الهكرز

اسالة تطرح نفسها:

١. ما هي عملية الهاكرز أو التجسس ؟
٢. من هم الهاكرز ؟
٣. ما هي الأشياء التي تساعدهم على اختراق جهازك ؟
٤. كيف يتمكن الهاكر من الدخول إلى جهازك ؟
٥. كيف يتمكن الهاكر من الدخول إلى جهاز كمبيوتر بعينه ؟
٦. ما هو رقم الآي بي أدرس ؟
٧. كيف يصاب جهازك بملف الباتش أو التروجان أو حتى الفيروسات ؟
٨. كيف يختار الهاكر الجهاز الذي يود اختراقه ؟
٩. ما هي أشهر برامج الهاكرز ؟
١٠. كيف تعرف إذا كان جهازك مخترقاً أم لا ؟
١١. ما هي أهم الاحتياطات التي يجب اتخاذها للحماية من الهاكرز ؟
١٢. ما هي أهم الأشياء التي يبحث عنها الهاكرز ؟
١٣. ما هي أشهر طريقة للكشف عن ملفات التجسس ؟

الشرح:

١. ما هي عملية الهاكنك أو التجسس ؟

تسمى باللغة الإنكليزية .. (Haking) وتسمى باللغة العربية عملية التجسس أو الاختراق
حيث يقوم أحد الأشخاص الغير مصرح لهم بالدخول إلى نظام التشغيل في جهازك بطريقة غير شرعية ولأغراض غير سوية مثل التجسس أو السرقة أو التخريب حيث يتاح للشخص المتجسس (الهاكر) أن ينقل أو يمسح أو يضيف ملفات أو برامج كما أنه بإمكانه أن يتحكم في نظام التشغيل فيقوم بإصدار أوامر مثل إعطاء أمر الطباعة أو التصوير أو التخزين ..

٢. من هم الهاكرز ؟

هم الأشخاص الذين يخترقون جهازك فيستطيعون مشاهدة ما به من ملفات أو سرقتها أو تدمير جهازك أو التلصص ومشاهدة ما تفعله على شبكة الإنترنت..

٣. ما هي الأشياء التي تساعدهم على اختراق جهازك ؟

أ وجود ملف باتش أو تروجان

لا يستطيع الهاكر الدخول إلى جهازك إلا مع وجود ملف يسمى (patch) أو(trojan) في جهازك وهذه الملفات هي التي يستطيع الهاكر بواسطتها الدخول إلى جهازك الشخصي حيث يستخدم الهاكر أحد برامج التجسس التي ترتبط مع ملف الباتش الذي يعمل كـ (ريسيفر) يستطيع أن يضع له الهاكر (إسم مستخدم) و(رمز سري) تخوله أن يكون هو الشخص الوحيد الذي يستطيع الدخول إلى جهازك وكذلك يستطيع أن يجعل جهازك مفتوحاً فيستطيع أي هاكر أن يدخل إلى جهازك

ب الاتصال بشبكة الإنترنت

لا يستطيع الهاكر أن يدخل إلى جهازك إلا إذا كنت متصلاً بشبكة الإنترنت
أما إذا كان جهازك غير متصل بشبكة الإنترنت أو أي شبكة أخرى فمن
المستحيل أن يدخل أحد إلى جهازك سواك
ولذلك إذا أحسست بوجود هاكر في جهازك فسارع إلى قطع الاتصال بخط
الإنترنت بسرعة حتى تمنع الهاكر من مواصلة العبث والتلصص في جهازك

ت برنامج التجسس

حتى يتمكن الهاكر العادي من اختراق جهازك لابد أن يتوافر معه برنامج
يساعده على الاختراق
ومن أشهر واهم واقوى برامج الهاكرز فى الوقت الحالي:-

١) البرورات (prorat)

٢) الاوبتكس (optix)

٣) Web Cracker 4

٤) Net Buster

٥) NetBus Haxporg

٦) Net Bus 1.7

٧) Girl Friend

٨) BusScong

٩) BO Client and Server

٤. كيف يتمكن الهاكر من الدخول إلى جهازك ؟

عندما يتعرض جهاز الكمبيوتر للإصابة بملف التجسس وهو (الباتش أو التروجان او الخادم) فإنه على الفور يقوم بفتح بورت (port) أو منفذ داخل جهازك فيستطيع كل من لديه برنامج تجسس أن يقتحم جهازك من خلال هذا الملف الذي يقوم بفتح منطقة أشبه بالنافذة السرية التي يدخل منها اللصوص وهم الهاكرز !!

٥. كيف يتمكن الهاكر من الدخول إلى جهاز كمبيوتر بعينه ؟

لا يستطيع الهاكر أن يخترق جهاز كمبيوتر بعينه إلا إذا توفرت عدة شروط وهي:

أ. إذا كان هذا الكمبيوتر يحوي ملف التجسس (الباتش)

ب. إذا كان الهاكر يعرف رقم الآي بي أدرس الخاص بهذا الشخص

ت. اتصال الضحية بالإنترنت

ث. معرفة الهاكر بكيفية استخدام برنامج التجسس والاختراق من خلاله

بمعنى آخر إذا كان جهاز الكمبيوتر سليماً ولا يحوي أي ملفات باتش فمن المستحيل أن يدخل عليه أي هاكر عادي حتى لو كان يعرف رقم الآي بي أدرس ما عدا المحترفين فقط وهم قادرون على الدخول بأية طريقة وتحت أي مانع ولديهم طرقهم السرية في الولوج إلى مختلف الأنظمة

وإذا كان الهاكر لا يعرف رقم الآي بي أدرس الخاص بك فإنه لن يستطيع الدخول إلى جهازك حتى لو كان جهازك يحوي ملف الباتش

٦. ما هو رقم الآي بي أدرس ؟

هو العنوان الخاص بكل مستخدم لشبكة الإنترنت أي أنه الرقم الذي يُعَّرف مكان الكمبيوتر أثناء تصفح شبكة الإنترنت وهو يتكون من (٤) أرقام وكل جزء منها

يشير إلى عنوان معين فأحدها يشير إلى عنوان البلد والتالي يشير إلى عنوان الشركة الموزعة والثالث إلى المؤسسة المستخدمة والرابع هو المستخدم ..

ولذلك ينصح بعدم استخدام بعرض برامج المحادثة مثل (الآيسكيو)ICQ لأنه يقوم بإظهار رقم الآي بي بشكل دائم حتى مع إخفائه فيتمكن الهاكر من استخدامه في الدخول إلى جهاز الشخص المطلوب مع توافر شرط وهو أن يحتوي كمبيوتر هذا الشخص على منفذ أو ملف تجسس (باتش)

٧. كيف يصاب جهازك بملف الباتش أو التروجان أو حتى الفيروسات ؟

الطريقة الأولى :

أن يصلك ملف التجسس من خلال شخص عبر المحادثة أو (الجات) وهي أن يرسل أحد الهاكر لك صورة أو ملف يحتوي على الباتش أو التروجان

ولابد أن تعلم أنه بإمكان الهاكر أن يغرز الباتش في صورة أو ملف فلا تستطيع معرفته إلا باستخدام برنامج كشف الباتش أو الفيروسات حيث تشاهد الصورة أو الملف بشكل طبيعي ولا تعلم أنه يحتوي على باتش أو فيروس ربما يجعل جهازك عبارة عن شوارع يدخلها الهاكر والمتطفلون

الطريقة الثانية :

أن يصلك الباتش من خلال رسالة عبر البريد الإلكتروني لا تعلم مصدر الرسالة ولا تعلم ماهية الشخص المرسل فتقوم بتنزيل الملف المرفق مع الرسالة ومن ثم فتحه وأنت لا تعلم أنه سيجعل الجميع يدخلون إلى جهازك ويتطفلون عليك ..

الطريقة الثالثة :

إنزال برامج أو ملفات من مواقع مشبوهة مثل المواقع الجنسية أو المواقع التي تساعد على تعليم التجسس

الطريقة الرابعة :

الدخول إلى مواقع مشبوهة مثل المواقع الجنسية حيث أنه بمجرد دخولك إلى الموقع فإنه يتم تنزيل الملف في جهازك بواسطة ملف الباتش لا تدري عنه حيث يقوم أصحاب مثل هذه المواقع بتفخيخ الصفحات فعندما يرغب أحد الزوار في الدخول إلى هذه الصفحات تقوم صفحات الموقع بإصدار أمر بتنزيل ملف التجسس في جهازك

٨. كيف يختار الهاكر الجهاز الذي يود اختراقه ؟

بشكل عام لا يستطيع الهاكر العادي من اختيار كمبيوتر بعينه لاختراقه إلا إذا كان يعرف رقم الآي بي أدرس الخاص به كما ذكرنا سابقاً فإنه يقوم بإدخال رقم الآي بي أدرس الخاص بكمبيوتر الضحية في برنامج التجسس ومن ثم إصدار أمر الدخول إلى الجهاز المطلوب !!
وأغلب المخترقين يقومون باستخدام برنامج مثل (IP Scan) كاشف رقم الآي بي وهو برنامج يقوم الهاكر باستخدامه للحصول على أرقام الآي بي التي تتعلق بالأجهزة المضروبة التي تحتوي على ملف التجسس (الباتش)

يتم تشغيل البرنامج ثم يقوم المخترق بوضع أرقام آي بي افتراضيه .. أي أنه يقوم بوضع رقمين مختلفين فيطلب من الجهاز البحث بينهما فمثلاً يختار هذين الرقمين :

217.164.123.10

217.164.123.100

لاحظ آخر رقمين وهما : ١٠ و ١٠٠

فيطلب منه البحث عن كمبيوتر يحوي منفذ (كمبيوتر مضروب) بين أجهزة الكمبيوتر الموجودة بين رقمي الآي بي أدرس التاليين :
217.164.123.10 و 217.164.123.100

وهي الأجهزة التي طلب منه الهاكر البحث بينها !

بعدها يقوم البرنامج بإعطائه رقم الآي بي الخاص بأي كمبيوتر مضروب يقع ضمن النطاق الذي تم تحديده مثل :

217.164.123.50

217.164.123.98

217.164.123.33

217.164.123.47

فيخبره أن هذه هي أرقام الآي بي الخاصة بالأجهزة المضروبة التي تحوي منافذ أو ملفات تجسس فيستطيع الهاكر بعدها من أخذ رقم الآي بي ووضعه في برنامج التجسس ومن ثم الدخول إلى الأجهزة المضروبة

٩. ما هي أشهر برامج الهاكرز ؟

أ netbus1.70

من أقدم البرامج في اختراق السيرفرات وهو الأكثر شيوعا بين مستخدمي المايكروسوفت شات وهو برنامج به العديد من الإمكانيات التي تمكن الهاكر من التحكم بجهاز الضحية وتوجد نسخ مختلفة أكثر حداثة من النت باس وكل نسخه منها أكثر تطوراً من الأخرى ..

ب SUB 7

برنامج ممتاز وغني عن التعريف .. تستطيع التحكم وتنسيق السيرفر ليعمل كيفما تشاء سواء من تغيير شكل او طريقة عمل وهو ممتاز في مجال الاختراق بالبرامج ..

ت ******** Utility

برنامج مفيد ورهيب للهاكرز وخاصة المبتدئين والمحترفين حيث أنه يمتلك أغلب وأفضل إمكانيات مختلف برامج الهاكرز ويمكن من خلاله كسر الكلمات السرية للملفات المضغوطة وفك تشفير الملفات السرية المشفرة وكذلك تحويل عناوين المواقع الى أرقام آي بي والعكس كما به العديد من الإمكانيات والمميزات التي يبحث عنها الكثير من الهاكرز ..

ث Back Orifice

برنامج غني عن التعريف لما لفيروسه من انتشار بين أجهزة مستخدمي الانترنت ولكن حتى تستطيع اختراق أحد الأجهزة لابد أن يكون جهازك ملوثاً بنفس الفيروس المستخدم ..

ج Deep Throat 2.0

يقوم هذا البرنامج بمسح الملف (سيستري) ويقوم باستبداله بالسيرفر الخاص به وهذا البرنامج فيه ميزة وهي أنك تستطيع التحكم في المواقع اللي يزورها الضحية وتقوم بتوجيهه لأي مكان ترغب وبإمكان المتحكم غلق وفتح الشاشة وكذلك استخدامه عن طريق برنامج الإف تي بي ..

ح porter

برنامج يعمل Scan على ارقام الـ IP و الـ Ports

خ pinger

برنامج يعمل (Ping) لمعرفة إذا كان الضحية أو الموقع متصلاً بالإنترنت أم لا ...

د ultrascan-15.exe

أسرع برنامج لعمل Scan على جهاز الضحية لمعرفة المنافذ المفتوحة التي يمكنك الدخول إليه منها ...

ذ Zip Cracker

هذا البرنامج الصغير تستطيع من خلاله كسر كلمات سر الملفات المضغوطة والمحمية بباسوورد ..

ر Girl Friend

برنامج قام بعمله شخص يدعى بـ(الفاشل العام) ومهمته الرئيسية والخطيرة هي سرقة جميع كلمات السر الموجودة في جهازك بما قفيها باسوورد الأيميل وكذلك إسم المستخدم والرمز السري الذي تستخدمه لدخول الإنترنت ..

١٠. كيف تعرف إذا كان جهازك مخترقاً أم لا ؟

في البداية تستطيع أن تعرف إذا كان جهازك مخترقاً من خلال معرفة التغيرات التي يحدثها الهاكرز في نظام التشغيل مثل فتح وغلق الشاشة تلقائياً أو وجود ملفات جديدة لم يدخلها أحد أو مسح ملفات كانت موجودة أو فتح مواقع إنترنت أو إعطاء أمر للطابعة بالإضافة إلى العديد من التغيرات التي تشاهدها وتعرفها وتعلم من خلالها عن وجود متطفل يستخدم جهازك ..
هذه الطريقة تستطيع من خلالها أن تعرف هل دخل أحد المتطفلين إلى جهازك أم أن جهازك سليم

افتح قائمة (Start) و منها اختر أمر .(Run)

اكتب التالي regedit

ثم اختر (HKEY_CURRENT_CONFIG)

منه اختر (SOFTWARE)
منه (FONTS)
منه (MICROSOFT)
منه (WINDOWS)
منه (CURRENTVERSION)

ستجد على يمينك في الشاشة قوائم (NAME) و(TYPE) و (DATA) وفيها معلومات عن الملف وامتداد الملف او البرنامج حيت ان ملف التجسس ليس لة لا معلومات ولا امتداد جددة ثم احذفه
ولزيادة الاطمانان كرر العملية مع

ONCE
SERVICES
SERVICES ONCE

١١. ما هي أهم الاحتياطات التي يجب اتخاذها للحماية من الهاكرز ؟

أ- استخدم أحدث برامج الحماية من الهاكرز والفيروسات وقم بعمل مسح دوري وشامل على جهازك في فترات متقاربة خصوصاً إذا كنت ممن يستخدمون الإنترنت بشكل يومي

ب- لا تدخل إلى المواقع المشبوهة مثل المواقع التي تعلم التجسس والمواقع التي تحارب الحكومات أو المواقع التي تحوي أفلاماً وصوراً خليعة لأن الهاكرز يستخدمون أمثال هذه المواقع في إدخال ملفات التجسس إلى الضحايا حيث يتم تنصيب ملف التجسس (الباتش) تلقائياً في الجهاز بمجرد دخول الشخص إلى الموقع

ت- عدم فتح أي رسالة إلكترونية من مصدر مجهول لأن الهاكرز يستخدمون رسائل البريد الإلكتروني لإرسال ملفات التجسس إلى الضحايا

ث- عدم استقبال أية ملفات أثناء (الشات) من أشخاص غير موثوق بهم وخاصة إذا كانت هذه الملفات تحمل امتداد (exe) مثل (love.exe) أو أن تكون ملفات من ذوات الامتدادين مثل (ahmed.pif.jpg) وتكون أمثال هذه الملفات عبارة عن برامج تزرع ملفات التجسس في جهازك فيستطيع الهاكرز بواسطتها من الدخول على جهازك وتسبيب الأذى والمشاكل لك

ج عدم الاحتفاظ بأية معلومات شخصية فى داخل جهازك كالرسائل الخاصة أو الصور الفوتوغرافية أو الملفات المهمة وغيرها من معلومات بنكية مثل أرقام الحسابات أو البطاقات الائتمانية

ح قم بوضع أرقام سرية على ملفاتك المهمة حيث لا يستطيع فتحها سوى من يعرف الرقم السري فقط وهو أنت

خ حاول قدر الإمكان أن يكون لك عدد معين من الأصدقاء عبر الإنترنت وتوخى فيهم الصدق والأمانة والأخلاق .

د حاول دائماً تغيير كلمة السر بصورة دورية فهي قابلة للاختراق

ذ- تأكد من رفع سلك التوصيل بالإنترنت بعد الإنتهاء من استخدام الإنترنت

ر- لا تقم بإستلام أي ملف وتحميله على القرص الصلب في جهازك الشخصي إن لم تكن متأكدا من مصدره .

١٢. ما هي أهم الأشياء التي يبحث عنها الهاكرز ؟

بعض الهاكرز يمارسون التجسس كهواية وفرصة لإظهار الإمكانيات وتحدي الذات والبعض الآخر يمارس هذا العمل بدافع تحقيق عدة أهداف تختلف من هاكر لآخر ونذكر منها ما يلي :

أ- الحصول على المال من خلال سرقة المعلومات البنكية مثل أرقام الحسابات أو البطاقات الائتمانية .

ب- الحصول على معلومات أو صور شخصية بدافع الابتزاز لأغراض مالية أو انحرافية كتهديد بعض الفتيات بنشر صورهن على الإنترنت إذا لم يستجبن لمطالب انحرافية أو مالية !!

ت الحصول على ملفات جميلة مثل ملفات الأركامكس أو الباور بوينت أو الأصوات أو الصور أو ...

ث إثبات القدرة على الاختراق ومواجهة العقبات وفرصة للافتخار بتحقيق نصر في حال دخول الهاكر على أحد الأجهزة أو الأنظمة المعلوماتية ..

ج الحصول على الرموز السرية للبريد الإلكتروني ليتسنى له التجسس على الرسائل الخاصة أو سرقة إسم البريد الإلكتروني بأكمله !!

ح الحصول على الرمز السري لأحد المواقع بهدف تدميره أو التغيير في محتوياته ..

خ الانتقام من أحد الأشخاص وتدمير جهازه بهدف قهره أو إذلاله ..

١٣. ما هي أشهر طريقة للكشف عن ملفات التجسس ؟

هناك العديد من الطرق للكشف عن وجود ملفات التجسس في جهازك ..

الطريقة الأولى : برامج الكشف عن ملفات التجسس والفيروسات

استخدام أحد برامج الكشف عن ملفات التجسس وكذلك الحماية من التجسس والهاكرز عن طريق عمل جدار ناري يمنع دخول المتطفلين ...

من أشهر وأفضل برامج الكشف عن ملفات التجسس :

أ- Norton internet security

ب- Zone alarm

ت MacAfee firewall

ث The Cleaner

ومن أشهر وأفضل برامج الحماية من الهاكرز :

أ ZoneAlarm

ب LockDown 2000

ت Jammer

ث Internet Alert 99

ج Tiny Personal Firewall

الطريقة الثانية : بواسطة ملف تسجيل النظام : Registry

١) انقر على زر البدء . Start

٢) أكتب في خانة التشغيل Run الأمر rigedit :

٣) افتح المجلدات التالية حسب الترتيب في قائمة Registery Editor

- HKEY_LOCAL_MACHINE
- Software
- Microsoft
- Windows
- Current Version
- Run

٤) والآن من نافذة تسجيل النظام Registry Editor انظر الي يمين النافذة بالشاشة المقسومة ستشاهد تحت قائمة Names أسماء الملفات التي تعمل مع قائمة بدء التشغيل ويقابلها في قائمة Data عناوين الملفات .

٥) لاحظ الملفات جيدا فإن وجدت ملف لايقابلة عنوان بالـ Data او قد ظهر أمامة سهم صغير ---> فهو ملف تجسس إذ ليس له عنوان معين بالويندوز

٦) تخلص منه بالضغط على الزر الأيمن للفارة ثم Delete

الطريقة الثالثة : بواسطة الأمر msconfig:

١) انقر على زر البدء Start

٢) اكتب في خانة التشغيل Run الأمر التالي:

msconfig

٣) سوف تظهر لك نافذة System Configuration Utility

٤) اختر من هذه النافذة من أعلى قسم Start up

٥) ستظهر لك شاشة تعرض البرامج التي تبدأ العمل مباشرة مع بدء تشغيل الجهاز .

٦) إفحص هذة البرامج جيدا بالنظر فإن شككت بوجود برامج غريبة لم تقم أنت بتثبيتها بجهازك فقم بالغاء الإشارة الظاهرة بالمربع الصغير المقابل له فتكون بذلك قد أوقفت عمل البرنامج التجسسي أو غيره من البرامج الغير مرغوب بها .

الطريقة الرابعة : بواسطة مشغل الدوس : Dos

هذة الطريقة كانت تستخدم قبل ظهور الويندوز لإظهار ملفات التجسس مثل الباتش والتروجانز وهي من اسهل الطرق :

١) افتح الدوس من محث MSDos بقائمة البدء Start

٢) أكتب الأمر التالي
(C:/Windows\dir patch.* e)

٣) إن وجدت ملف الباتش فقم بمسحة بالطريقة التالية :

C:\Windows\delete patch.*

٤) ممكن من خلال كتابه الامر netstat من خلال الدوس

****
****
*****
**

وبهذا انتهت محاضرات
(الهكر من هو وكيف يخترق وكيفية الوقاية منه)
وأرجو من الله عز وجل أن أكون قد وفقت
في إيصال المعلومات بطريقة سهلة
ومبسطة للغاية والله
ولي التوفيق

المهندس
سهيل نجم الدين نوري