بحث شامل عن ++++ الهكر ++++

الفهرس

14- ما هي أهم الأشياء التي يبحث عنها الهاكرز ؟

15- ما هي أهم الاحتياطات التي يجب اتخاذها للحماية من الهاكرز ؟

16- ازاي اعرف ان الصورة متلغمة "يعنى مدموج فيها باتش"؟

17- كيف تعرف ان جهازك مخترق مهم جدا..

18- كيف تحمي جهازك من الاختراق بدون برامج..

19- اقوى جاسوس من الاستخبارات الامريكية في جهازك الحق واحذفة ..

20- من أشهر برامج الحماية (فير وول Firewall). .

21- من أشهربرامج مقاومة الفيروسات..

22- في النهاية يجب توخي الحذر الشديد من الجميع في التعامل مع ما يلي..

المقدمة

الكثير منا يتعرض لعملية الأختراق دون أن يعلم ما هية الأختراق وكيف يمكن أن يتم أختراق الأجهزة ، وللأسف هناك الكثير من الناس يتعرضون لعملية الأختراق (التجسس) بصفه مستمرة دون أن يشعروا بذلك

لذلك تم وضع هذا البحث الشامل بين إيديكم لنتعلم كيف نواجه هذا الخطر الخفى حيث إن هذا البحث يتناول الكثير من التساؤلات التى تدور فى أذهان الكثير منا عن هذه القرصنه ، وكيف يستطيع الهاكر الدخول إلى الأجهزة والعبث بها، وكيفية الحمايه من الأختراق ، والمنافذ والثغرات التى يستطيع منها الهاكر الدخول إلى الأجهزة وقرصنتها

نرجوا من الله أن ينال رضاكم

ما هي عملية الهاكينج أو التجسس ؟

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

من هم الهاكرز ؟

هم الأشخاص الذين يخترقون الأجهزة فيستطيعون مشاهدة ما بها من ملفات أو سرقتها أو تدمير الجهاز أو التلصص ومشاهدة ما تفعله على شبكة الإنترنت..

ما هي الأشياء التي تساعدهم على اختراق جهازك ؟

١ - وجود ملف باتش أو تروجان

لا يستطيع الهكر الدخول إلى جهاز الكمبيوتر إلا عن طريق ملف الباتش أو التروجان الموجود بجهاز الضحية.

ملف الباتش :

وهو ملف يجب إرساله للضحية و يجب على الضحية فتحه أيضا حتى يفتح عند الضحيه منفذ (port) ثم يستطيع الهكر اختراقه و التحكم فى جهازه و السيطرة عليه

و أى برنامج باتش يحتوى على 4 أشياء أساسية و هى :-

1- *ملف الباتش* server : وهو ملف يجب إرساله للضحية و يجب على الضحية فتحه أيضا حتى يفتح عنده منفذ (port) ومنه يتم اختراقه..

2- *ملف* Edit server : وهو لوضع إعدادات الباتش أو تغييرها.

3- *ملف البرنامج الأساسي* Client: وهوالبرنامج الذي يتصل الهاكر من خلاله بالضحية و يتحكم في جهازه..

4- *ملفات الـ* dll *وغيرها* : وهي التي تساعد البرنامج على التشغيل ومن دونها لا يعمل البرنامج..

كما ان أي باتش دائما ما يكون امتداده ب name.exe حيث Name تعني اسم السيرفر و .exe تعني امتداده، و الأمتداد عبارة عن شيء خاص لتشغيل الملف

فمثلا

دائما ما يكون امتداد الصور بهذه الامتدادات(.... JPG – BMP – GIF- Jpeg) ويكون امتداد ملفات الورد (DOC) وملفات الأكسل(XLS) و يكون أمتداد الفلاش(...,wsf)

و يكون أمتداد ملفات القراءة (... , html , txt , doc , pdf)

وملفات الأغاني *MP3* (WAV)

و امتداد ملفات الفيديو (... AVI – ASF – MPG - mpeg).

لذلك فإن امتداد البرامج الأساسية أو ما يطلق عليها البرامج التنفيذية بالطبع دائما ما يكون امتدادها (EXE) لذلك عند إرسال ملف الباتش لا يتم إرساله كما هو بصيغته الأساسية .exe بل يتم إخفائه بأستخدام أحد الصيغ (صيغة الصورة أو الأغانى أو الفيديو.....) للتحايل في إرساله حيث يمكنك إرساله مدمج مع صوره أو ملف يتم تنصيبه عن طريق بعض البرامج ، و من الممكن تغير امتداد الباتش عن طريق الدوس حتى لا يشك الضحية..

يستطيع الهاكر من خلال هذا البرنامج التنصت و تسجيل وحفظ كل ما يتم كتابته على لوحة المفاتيح.

و من هذه البرامج برنامج يدعى Invisible KeyLloger *و هو برنامج يستطيع* ان يحتفظ في ملف مخفي بكل ما قمت بكتابته على لوحة المفاتيح مصحوبة بالتاريخ والوقت الذي قمت فيه بعمليات الكتابة هذه ، حيث سيمكنك ا لإطلاع على الملف المسجل به كل ما تم كتابته على لوحة مفاتيح الحاسب والتي لن يستطيع أحد معرفة مكانه إلا واضعه .

٢ - *الاتصال بشبكة الإنترنت*

لا يستطيع الهاكرالدخول إلى جهاز الضحية إلا عن طريق أتصال الضحية بالأنترنت

فإذا أحس الضحية بإن شخص ما يخترقه يقوم بسرعة بفصل الأتصال بالأنترنت لأن بمجرد فصل الأنترنت و عودة الأتصال به مرة أخرى يتغيرIP address الخاص بك

فمثلاً

إذا كان رقمك 212.123.123.200 بعد فصل الأنترنت و العودة يتغير ليصبح كالأتى

212.123.123.366 لاحظ التغير فى الجزء الأخير من 200 بقى 366

٣ - *برنامج التجسس*

يستطيع الهاكر الدخول إلى جهاز الضحية عن طريق أستخدام بعض البرامج التى تساعده على الأختراق

و من أشهرها:

Web Cracker 4

Net Buster

Net Bus Haxporg

Net Bus 1.7

Girl Friend

BusScong

BO Client and Server

Hackers Utility

ويوجد بعض البرامج الحديثة التي نزلت ولاترى من قبل برامج الحماية من الفيروسات هي:

BEAST

CIA122b

OptixPro

NOVA

و غيرها من البرامج الشهيرة و طبعا البرامج التي صممها الهاكر بأنفسهم على لغة برمجة معينة فبالتالي يمكنهم ان يضيفوا عليها أشياء لا ترى من قبل برامج الحماية.

كيف يتمكن الهاكر من الدخول إلى جهازك ؟

عندما يتعرض جهاز الكمبيوتر للإصابة بملف التجسس وهو " الباتش أو التروجان" فإنه على الفور يقوم بفتح بورت(port) 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!!

عند الإصابة بملف الباتش يحدث التالى :-

1-يتجه إلى ملف تسجيل النظام (registry) حيث ان النظام في كل مرة عندما تقوم بتشغيل الويندوز يقوم الويندز بتشغيل البرامج المساعدة في ملف تسجيل النظام مثل برامج الفيروسات وغيرها.

2-يقوم بفتح ملف اتصال داخل الجهاز المصاب تمكن برنامج الهاكر من الدخول إلى جهازك و التجسس عليه.

3-يقوم بعملية التجسس وذلك بتسجيل كل ما يحدث أو عمل أشياء أخرى على حسب ما يريد.

و هذا يعني ان الجهاز إذا أصيب فإنه يصبح مهيأ للإختراق.

كيف يتمكن الهاكر من الدخول إلى جهاز كمبيوتر بعينه ؟

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

١ - إذا كان هذا الكمبيوتر يحتوي على ملف التجسس " الباتش ".

٢ - إذا كان الهاكر يعرف رقم الآي بي أدرس (IP Address) الخاص بهذا الشخص...

3- اتصال الضحية بالإنترنت ومعرفة الهاكر بكيفية استخدام برنامج التجسس والاختراق من خلاله!

ما هو رقم الآي بي أدرس (IP (internet protocol :-

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..

ورقم الآي بي متغير وغير ثابت فهو يتغير مع كل دخول إلى الإنترنت .. بمعنى آخر لنفرض أنك اتصلت بالانترنت

ونظرت إلى رقم الآي بي الخاص بك فوجدت أنه :212.123.123.200

ثم خرجت من الانترنت أو أقفلت الاتصال ثم عاودت الاتصال بعد عدة دقائق فإن الرقم يتغير ليصبح كالتالي: 212.123.123.366

لاحظ التغير في الأرقام الأخيرة : الرقم 200 أصبح 366

كيف يصاب جهازك بملف الباتش أو التروجان أو حتى الفيروسات ؟

الطريقة الأولى:

أن يصلك ملف التجسس من خلال شخص عبر المحادثة أو الشات وهي أن يرسل لك أحد الهاكر 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:

أن يصلك الباتش من خلال رسالة عبر البريد الإلكتروني لا تعلم مصدر الرسالة ولا تعلم ماهية الشخص المرسل و يقول أدخل على الرابط التالى فتقوم بالدخول و من ثم الأصابة بملف الباتش.

الطريقة الرابعة:

إنزال برامج أو ملفات من مواقع مشبوهة مثل المواقع الغير أخلاقيه أو المواقع التي تساعد على تعليم التجسس !

الطريقة الخامسة:

الدخول إلى مواقع مشبوهة مثل المواقع الغير أخلاقية حيث أنه بمجرد دخولك إلى هذه المواقع فإنه يتم تنزيل الملف في جهازك بواسطة كوكيز لا تدري عنها!!

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!

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) أو كاشف رقم الآي بي وهو برنامج يقوم الهاكر باستخدامه للحصول على أرقام الآي بي التي تتعلق بالأجهزة المضروبة التي تحتوي على ملف التجسس (الباتش)

حيث 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:

212.224.123.10

212.224.123.100

لاحظ آخر رقمين وهما: 10 / 100

فيطلب منه البحث عن كمبيوتر مضروب (يحتوي على ملف الباتش) بين أجهزة الكمبيوتر الموجودة بين رقمي الآي بي

أدرس التاليين: 212.224.123.10 و 212.224.123.100

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

212.224.123.50

212.224.123.98

212.224.123.33

212.224.123.47

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!

كيف تعرف الآى بى الخاص بك ؟

بالنسبة لويندوز ٩٨ , ME

من قائمة START نختار RUN ثم نكتب الأمر التالي winipcfg

أما بالنسبة لويندوز XP

من قائمة START نختار RUN ثم نكتب الأمر التالي cmd /k ipconfig

كيف تستخرج رقم الآى بى الخاص بالهاكر ؟

من قائمة START ثم RUN وتكتب command أو cmd (for XP)

سوف تفتح شاشه الدوس السوداء

تكتب هذا الأمر netstat -n

مع ملاحظة المسافة بين الشرطة و الكلمة netstat -n

بعد كتابه الأمر سوف يظهر لك الشكل الأتي:-

Proto ---- Local Address ---- Foreign Addres ---- State

Local Address: هذا رقم الآي بي الخاص فيك أنت

Foreign Address: هذا رقم الآي بي الخاص بالهكر

State : يشير إلى رقم الهكر ويبقى مكتوب فيه TIME_WAIT و الرقم الموجود أمامه هو رقم الهكر

* سوف تجد فى الفورن ادرس ... ارقام مقدم الخدمه لك ..مع رقم البورت او المنفذ .. وهنا يجب ان تنتبه لان الحاله تكون كالاتى

State	ForeignAddress
Established	212.123.234.200:8080

اى ان الارقام لمقدم الخدمه هى

212.123.234.200

ثم تاتى بعدها نقطتين فوق بعض ... ياتى بعدها رقم البورت وهو8080

وهذا وضع طبيعى جدا ... ثم تاتى كلمه ... ستات ... اى الحاله وتحتها كلمه.. اشتبلش .. اى الاتصال تام .. وهذا ايضا طبيعى .

* المهم فى الامر ليس من الضرورى أن تجد كلمة time-wait فأحياناً لاتجدها و لكن إن وجدت أى رقم اى بى غريب ... وتتاكد من ذلك برقم المنفذ .. وهو الذى ياتى بعد النقطتين التى فوق بعض ... مثال

Foreign Adress State

212.100.97.50:12345 Established

انظر الى رقم .. الاى . بى ... ورقم المنفذ .. رقم الاى بى غريب.. ورقم المنفذ هو منفذ لبرنامج تجسس .. وحاله الاتصال تام مع جهازك.. اى انه بالفعل يوجد شخص الان فى داخل جهازك يتجسس عليك

...اكتب رقم المنفذ ... وهو ...البورت ... 12345 .... ثم اتجه الى قائمه البورتات الموجود فى الموقع تحت عنوان ارقام البورتات المستخدمه فى برامج التجسس وابحث عن اسم البرنامج لكى تعرف الملف

المصاب به جهازك لتنظيفه

*- مع ملاحظه انه فى حاله انزالك لبرنامج او استخدام اى برامج تشات..سوف تجد رقم الاى بى اما الخاص بالموقع الذى تقم بانزال البرنامج منه .. او رقم الاى بى الخاص بالشخص الذى تتحدث اليه ..وكما سبق ان قلنا فهذه احدى الطرق التى تستخدم لمعرفه رقم الاى . بى ... لاى جهاز يستخدم برامج التشات

و إليكم قائمة بأرقام البورتات المستخدمة من قِبل برامج الإختراق:-

2 Death

7 echo

21 TCP Blade Runner, Doly Trojan, Fore, FTP trojan, Invisible FTP, Larva, WebEx

23 TCP Tiny Telnet Server

25 TCP Antigen, Email Password ,WinSpy, ProMail trojan,Shtrilitz,

Stealth, Tapiras, Terminator

31 TCP Agent 31, Hackers Paradise, Masters Paradise

0037 Net bus

48 DRAT

41 TCP DeepThroat

50 DRAT

53 TCP DNS

58 TCP DMSetup

79 TCP Firehotcker

80 TCP Executor

81 Bifrost

00103 Net bus

110 TCP ProMail trojan

121 TCP JammerKillah

123 Net Controller

129 TCP Password Generator Protocol

137 TCP Netbios name (DoS attacks)

138 TCP Netbios datagram (DoS attacks)

139 TCP Netbios session (DoS attacks)

146 Infector

146 (UDP) Infector

421 TCP TCP Wrappers

456 TCP Hackers Paradise

531 TCP Rasmin

555 TCP Ini-Killer, Phase Zero, Stealth Spy

605 Secret Service

666 TCP Attack FTP, Satanz Backdoor

777 Aim Spy

911 TCP Dark Shadow

0954 Net bus

999 TCP DeepThroat

1000 Der Spacher 3

1001 Der Spacher 3

1001 TCP Silencer, WebEx

1010 (Doly Trojan 1.30 Subm.Cronc)

1011 TCP Doly Trojan

1012 TCP Doly Trojan

1015 (Doly Trojan 1.5 Subm.Cronco)

1020 Vampire

1024 TCP NetSpy

1027 TCP ICQ

1029 TCP ICQ

1032 TCP ICQ

1033 Netspy

1037 Net bus

1042 Bla1.1

1045 TCP Rasmin

1050 MiniCommand

1080 TCP Used to detect Wingate sniffers.

1090 TCP Xtreme

1095 RAT

1097 RAT

1098 RAT

1099 RAT

1170 TCP Psyber Stream Server, Voice

1176 Net bus

1200 (UDP) NoBackO

1201 (UDP) NoBackO

1207 SoftWAR

1234 TCP Ultors Trojan

1243 TCP BackDoor-G, SubSeven

1245 TCP VooDoo Doll

1269 Maverick's Matrix

1313 NETrojan

1349 UDP BO DLL

FTP99CMP 1492 TCP

1509 PsyberStreaming Serve Nikhil G

1600 TCP Shivka-Burka

1807 TCP Spy المرسل

1969 NETrojan

1981 TCP Shockrave

1999 TCP BackDoor

2000 OpC BO

2001 Der Spaeher 3

2001 TCP Trojan Cow

2023 TCP Ripper

2115 TCP Bugs

2140 TCP Deep Throat, The Invasor

2283 HVL Rat5

2300 Xplorer

2565 TCP Striker

2583 TCP WinCrash

2716 The Prayer

2773 SubSeven

2801 TCP Phineas Phucker

2989 UDP Rat

3024 TCP WinCrash

3037 Net bus

3129 TCP Masters Paradise

3150 TCP Deep Throat, The Invasor

3360 Painrat

3456 Terror Trojan

3460 Poison

3700 TCP al of Doom

3791 (Total Eclypse FTP)

4092 TCP WinCrash

4242 Virtual Hacking Machine

10103 Net bus

43002 Net bus

4567 TCP File Nail

4590 TCP ICQTrojan

4950 IcqTrojan

5000 TCP Bubbel, Back Door Setup, Sockets de Troie

5001 TCP Back Door Setup, Sockets de Troie

5011 OOTLT

5031 NetMetropolitan

5321 TCP Firehotcker

5400 TCP Blade Runner

5401 TCP Blade Runner

5402 TCP Blade Runner

5521 IllusionMailer

5550 XTCP 2.0 + 2.01

5555 TCP ServeMe

5556 TCP BO Facil

5557 TCP BO Facil

5569 TCP Robo-Hack

5637 PC Crasher

5638 PC Crasher

5742 TCP WinCrash

6037 Net bus

6272 Secret Service

6346 Shl

6400 TCP The Thing

6667 ScheduleAgent

6669 Host Control

6670 TCP DeepThroat

6711 SubSeven

6712 SubSeven

6713 SubSeven

6771 TCP DeepThroat

6776 TCP BackDoor-G, SubSeven

6883 DeltaSource DarkStar)

6912 Shitheep

6939 TCP Indoctrination

6969 TCP GateCrasher, Priority

7000 TCP Remote Grab

7215 SubSeven

7300 TCP NetMonitor

7301 TCP NetMonitor

7306 TCP NetMonitor

7307 TCP NetMonitor

7308 TCP NetMonitor

7789 TCP Back Door Setup, ICKiller

8037 Net bus

8787 Back Orifice 2000

8897 HackOffice

8989 Rcon

9872 TCP al of Doom

9873 TCP al of Doom

9874 TCP al of Doom

9875 TCP al of Doom

9989 TCP iNi-Killer

9999 The Prayer

10067 TCP al of Doom

10086 Syphillis

10103 Net bus

10167 TCP al of Doom

10520 TCP Acid Shivers

10607 TCP Coma

10666 (UDP) Ambush

11000 TCP Senna Spy

11050 Host Control

11223 TCP Progenic trojan

12076 TCP GJamer

12223 TCP Hack´99 KeyLogger

12345 TCP GabanBus, NetBus, Pie Bill Gates, X-bill

12346 TCP GabanBus, NetBus, X-bill

12349 BioNet

12361 TCP Whack-a-mole

12362 TCP Whack-a-mole

12623 (UDP) DUN Control

12631 TCP WhackJob

12701 Eclipse 2000

13000 TCP Senna Spy

16484 Mosucker

16772 ICQ Revenge

16969 TCP Priority

17777 Nephron

19864 ICQ Revenge

20000 TCP Millennium

20001 TCP Millennium

20034 TCP NetBus 2 Pro

20103 Net bus

20203 Chupacabr

20331 Bla

21544 TCP GirlFriend

21554 GirlFriend

22222 TCP Prosiak

23456 TCP Evil FTP, Ugly FTP

26274 UDP Delta Source

27374 SubSeven

27573 SubSeven

29891 UDP The Unexplained

30029 TCP AOL Trojan

30100 TCP NetSphere

30101 TCP NetSphere

30102 TCP NetSphere

30303 TCP Sockets de Troie

30999 Kuang

31337 TCP Baron Night, BO client, BO2, Bo Facil

31337 UDP BackFire, Back Orifice, DeepBO

31338 TCP NetSpy DK

31338 UDP Back Orifice, DeepBO

31339 TCP NetSpy DK

31666 TCP BOWhack

31785 Hack'a'tack

31787 Hack'a'tack

31789 TCP Hack'A'Tack

32418 Acid Battery

33333 TCP Prosiak

33911 Trojan Spirit 2001 a

34324 TCP BigGluck, TN

34555 (UDP) Trinoo

35555 (UDP) Trinoo

37651 YAT

40412 TCP The Spy

40421 TCP Agent 40421, Masters Paradise

40422 TCP Masters Paradise

40423 TCP Masters Paradise

40425 TCP Masters Paradise

40426 TCP Masters Paradise

47262 UDP Delta Source

50505 TCP Sockets de Troie

50766 TCP Fore

52317 Acid Battery 2000

53001 TCP Remote Windows Shutdown

54283 SubSeven

54320 (Back Orifice 2000 default port)

54321 TCP School Bus

57341 NetRaider

60000 TCP Deep Throat

61348 Bunker_Hill

61466 Telecommando

61603 Bunker_Hill

63485 Bunker_Hill

65000 Devil 1.03

65432 The Traitor

65432 (UDP) The Traitor

66670 Deepthroat

73313 Net bus

83313 Net bus

92003 Net bus

93313 Net bus

عندما يقوم شخص بمحاولة التهكير عليك يقوم بالحصول على رقم الآي بي الخاص بك بواسطة عدة طرق :-

الطريقة الأولى : استخراج الهاكر أي بي الخاص بك من خلال الماسنجر

في البداية يرسل الهاكر للضحية أي ملف أو صورة أو أي شيء بحجم يزيد عن ٢٥ كيلوبايت وبعد وصولها بنجاح يقوم الهاكر بفتح الدوس وطريقه فتحه كالآتي

من قائمة START ثم يختار RUN ويكتب command أو cmd (for XP)
سوف تفتح شاشه الدوس السوداء

يكتب فيها الأمر netstat -n
مع ملاحظة المسافة بين الشرطة و الكلمة netstat -n

بعد كتابه الأمر يظهر الشكل الأتي للهاكر :-

Proto ---- Local Address ---- Foreign Address ---- State

Local Address: هذا رقم الآي بي الخاص بالهكر
Foreign Address: هذا رقم الآي بي الخاص بالضحية
State : يشير إلى رقم الضحية ويبقى مكتوب فيه TIME_WAIT و الرقم الموجود أمامه هو رقم الضحية

الطريقة الثانية : بدون تحميل برامج أو أي شي يقوم الهاكر بإستخدام برنامج جدار نار

مثل:

Fire Wall

ZONE ALARM

BLACK ICE

١ - يأخذ الـ IP الخاص به (الهاكر) ثم

2 - يكتب الـ IP الخاص به بالشكل هذا http://127.0.0.1

٣ - بعد ما تحول الـ IP الخاص بالهكر لصورة لينك أو وصلة تطلب من الضحية الضغط عليه

٤ - الباتش اللي عند الضحية راح يدفعه ناحية الهاكر ناحية اتصال جهازك بالنت

الطريقة الثالثة : استخراج الهكر أي بي الخاص بك من خلال الايميل

يقوم الهاكر بإرسال إيميل للضحية لكى يحصل على IP و فيكتب الايميل ويزيد عليه الأمر confirm.TO

فإذا فرضنا إن أيميلك XXX@hotmail.com

يقوم الهاكر بإضافة كلمة confirm.TO بعد عنوان البريد الخاص بالضحية فيصبح XXX@hotmail.com.confirm.TO

وعندما يقوم الضحية بفتح الرسالة يأتى للهاكر رسالة تخبره أن الضحية فتحت الرسالة وبنفس اللحظة التى تقوم الضحية بفتح الرسالة و التى تكون رقم الآي بي الخاص بالهاكر فيقوم بأستخراج IP الخاص بالضحية كما وضحنا سابقاً .

لذلك ينصح بعدم فتح أى رسالة مجهولة المصدر أو الضغط على أى لينك بها

الطريقة الرابعة : استخراج الهاكر أي بي الخاص بك من خلال الايميل أيضاً

لنفرض أن الضحية أرسلت رسالة إلى شخص ما و أراد هذا الشخص أن يعرف ال IP الخاص بالمرسل من الرسالة ((HOTMAIL)) فيقوم بالتالى :

من بريد الـ HOTMAIL أختر options

ثم اختر Mail Display Settings

ثم اختر message headers

وغير الاختيار إلى advanced

فيروح الشخص لرسالة الضحية و يحصل على IP وبعض المعلومات الأخرى

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:

1- الحصول على المال من خلال سرقة المعلومات البنكية مثل أرقام الحسابات أو البطاقات الائتمانية.
2- 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!!
3- الحصول على ملفات جميلة مثل ملفات الأركامكس أو الباور بوينت أو الأصوات أو الصور أو...

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

5- الحصول على الرموز السرية للبريد الإلكتروني ليتسنى له التجسس على الرسائل الخاصة أو سرقة اسم البريد الإلكتروني بأكملها!!

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

7- الانتقام من أحد الأشخاص وتدمير جهازه بهدف قهره أو إذلاله..

ما هي أهم الاحتياطات التي يجب اتخاذها للحماية من الهاكرز ؟

١ - 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..

2- التأكد من تحديث الانتي فيروس كل أسبوع على الأقل

(شركة نورتون تطرح تحديث كل يوم أو يومين)

3- التأكد من أن Firewall على وضعية on

4- وضع Anti-Virus جيد و انا انصح بوضع انتي فيرس الشمسية (Avira)

5- لا تظل مدة طويلة متصل بالشبكة بحيث لو ان احد قام بالدخول عليك لا يستطيع أن يخرب فى جهازك فعند خروجك و دخولك مره اخرى للشبكة يغير آخر رقم من الاي بي.

6 - لا تدخل إلى المواقع المشبوهة مثل المواقع التي تعلم التجسس والمواقع التي تحارب الحكومات أو المواقع التي تحوي أفلاماً وصوراً لا أخلاقية 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!!

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

8 - 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 ذوي الامتدادين مثل (ahmed.pif.jpg) أو (.bat أو .dll أو.com)
وتكون أمثال هذه الملفات عبارة عن برامج تزرع ملفات التجسس في جهازك فيستطيع الهاكرز بواسطتها من الدخول على جهازك وتسبب الأذى والمشاكل لك..

9 - عدم الاحتفاظ بأية معلومات شخصية في داخل جهازك كالرسائل الخاصة أو الصور الفوتوغرافية أو الملفات المهمة وغيرها من المعلومات البنكية مثل أرقام الحسابات أو البطاقات الائتمانية....

10 - قم بوضع أرقام سرية على ملفاتك المهمة حيث لا يستطيع فتحها سوى من يعرف الرقم السري فقط وهو أنت و سوف نشرحها

11- حاول قدر الإمكان أن يكون لك عدد معين من الأصدقاء عبر الإنترنت وتوخي فيهم الصدق والأمانة والأخلاق.

12 - حاول دائماً تغيير كلمة السر بصورة دورية فهي قابلة للاختراق ويفضل أن تكون كلمة السر أرقام وحروف ورموز يصعب تخمينها .

13- تأكد من رفع سلك التوصيل بالإنترنت بعد الانتهاء من استخدام الإنترنت.

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

15- قم بمسح cookies أول بأول من جهازك هي عبارة عن ملفات يرسلها الموقع لمتصفحك و هي عبارة عن ملف مكتوب لا يستطيع أي موقع قراءته غير هذا الموقع و قد يكون به كلمات سر موقع أو اشتراك... وهي مزعجه في بعض الأحيان حيث أنها تسجل كل المواقع التي دخلتها و كل الصفحات التي شاهدتها و مدة مشاهدة كل صفحه....

* ويمكن مسح الكوكيز عن طريق الذهاب المجلد الخاص بها و حذف الملفات التي به C:\WINDOWS\Cookies و حذف الملفات التي توجد داخل هذا المجلد

* أو من قائمة Start نختار Run ونكتب فيها Cookies ثم OK ستظهر نافذة نمحو كل ما فيها

16- لا تخزن كلمات المرور أو كلمات سر على جهازك مثل كلمة المرور لاشتراكك في الانترنت أو البريد الكتروني أو .....

17- إذا لاحظت حدوث اي شيء غريب مثل خلل في اي برامج أو خروج و دخول السي دي افصل الاتصال بالانترنت فورا و تأكد من نظافة الجهاز.

18- أغلق خاصية الاكمال التلقائي من انترنت اكسبلورر .. ولا تسمح بحفظ كلمات المرور في النماذج .

19- لا تدخل بريدك أو أيّ من معلوماتك الخاصة من مقاهي الانترنت نهائيا .. فهناك برامج تعمل بشكل مخفي تحفظ جميع النماذج التي تقوم بتعبئتها دون أن تشعر.

20- غيّر كلمات مرورك بين فترة وأخرى .. وينصح أن تكون الكلمة مكونة من حروف وأرقام كثيرة يصعب تخمينها ، لأن هناك برامج تقوم بتجريب الآلاف من كلمات المرور وتعمل مسح على مدار الساعة .. فيدخل المخترق اسم المستخدم للبرنامج ويطلب منه تخمين كلمة المرور ..

* فإذا كانت كلمة المرور سهلة مثل هذه 12345 فسوف يحصل عليها في وقت قياسي

* ولكن إذا كانت كلمة المرور صعبة مثل Rhjju665dTpl,Q:4#6;/.gf9 فسوف يكون من الصعب جدا أن يكتشفها البرنامج بالتخمين ولو بعد 100 سنة وتزداد الصعوبة أكثر إذا أضيف في كلمة المرور أحرف أخرى باللغة العربية في المواقع التي تسمح بذلك.

21- لا تستخدم كلمة مرور موحّدة .. بل اجعل كلمة مرور بريدك تختلف عن معرفك بالساحة .. وأيضا تختلف عن معرفك في المنتديات الأخرى .. ولو استطعت أن تجعل لكل منتدى أو بريد كلمة مرور مختلفة فافعل .. وضع جدولا لكلمات المرور على مكتبك وليس في جهازك .

22- احذر من مواقع الكراكات والسيريالات والمواقع غير الموثوقة ففيها برامج يتم تحميلها في الخلفية أثناء تصفح الموقع .. وهي تتحدّث بشكل مستمر .. وأحيانا تفشل برامج السباي وير في مقاومتها أو القضاء عليها .. وكذلك عند تركيب كراك لبرنامج فكثير من هذه الكراكات يحتوي على باتش يمكن أن يكون عند تشغيله ثغرة خطيرة في جهازك.

23- للعلم مواقع المراسلة التي ظهرت مؤخرا وشارك فيها كثير من الأعضاء .. من السهل جدا جدا للعاملين بتلك المواقع .. الاطلاع على محتويات الرسائل الموجودة بها .. ولذا إذا استخدمتها فكن على حذر .. فالرسائل الواردة إليك والمرسلة منك عن طريقها مكشوفة بنسبة 100%!!

24- على أسوأ الاحتمالات لا تترك بيانات أو ملفات أو مستندات خاصة بك في بريدك الالكتروني .. بل بادر بمسحها أو الاحتفاظ بها في جهازك .. وأيضا يفضّل أن تحفظ ملفاتك الشخصية الخاصة

والتي لا ترغب أن يطّلع عليها أحد في فلاش ديسك أو هارديسك خارجي .. وتقوم بفصلها عند الاتصال بالانترنت ..

25- ما يقوله جوجل صحيح .....فإذا قمت بعمل بحث على موقع ووجدت جوجل يحذرك من هذا الموقع لا تدخل على هذا الموقع لأنه قد يضر بجهازك.....فقد يحتوى على برمجيات خبيثة وسوف تنزل على جهازك من دون أن تشعر وسوف تكون بذلك ضحية لأى هاكر.

26- المواقع الموجودة فى رسايل الـ spam مواقع خطيرة...يمكن أن تحتوى على برمجيات خبيثة.

27- الأبتعاد عن برنامجى ICQ و IRC لأنهم يسهلوا عملية الأختراق.

28- انصح كل عضو ان يكون له 3 ايميلات واحد منها مخصص للشبكة و يفضل ان يكون على الجي ميل حتى لا يستخدم في الماسينجرات و ايميل اخر للماسينجر و ايميل للمراسلات الخاصة حتى ان تم سرقة باسورد ايميل الماسينجر لا يكون هناك ضرر معين و ان يكون الايميل المخصص للشبكة بأي اسم غير اسمك الحقيقي كما انصح الجميع عند ارسال ايميلات لعدة اصدقاء ان يتم وضع الايميلات في خانة BCC حتى لا يرى الجميع ايميلات الاخرين و تكون فرصة ثمينة لمن يخترق احدى هذه الايميلات.

29- جميع الأجهزة المتصلة بالشبكة عرضة للإصابة بالفيروسات في حالة مشاركة الملفات فيما بينها أو في حالة مشاركة الاتصال بالإنترنت بينها. لذلك يجب تعطيل وظيفة تبادل الملفات والطابعات وتفعيل الدخول إلى الجهاز بكلمة سر حتى يتم تجنب المخاطر إلى حد كبير..

30- المتصفح الذى تقوم بأستخدامه سواء انترنت اكسبلورر او فاير فوكس او غيره ....لابد أن يكون أحدث نسخة موجودة

31- تفريغ قائمة my recent document لأنها أول ما يلهث إليه لص المعلومات هو آخر ملفات تعاملت معها مؤخراً وما بها من معلومات فيبحث عنها على القائمة سالفة الذكر

* لتفريغ هذه القائمة ننقر بزر الماوس الأيمن على أي مكان خال فوق شريط المهام أسفل الديسك توب ثم نختار Propertiesثم start menu ثم نضغط زر customize ثم advanced ثم زر clear list ثم نضغط ok مرتين.

32- جميع مراسلات الشبكة تتم من خلال ايميل الشبكة ali@paldf.net او webmaster@paldf.net لذلك في حال وصول رسالة على ايملك من غير هذين الايميل اهمالها و عدم التجاوب معها.

كيف تعرف ان الصورة المرسلة لك ملغمة "أى مدموج فيها باتش"؟

اولاً لابد أن نعرف بوجود صيغ تنفيذية وصيغ غير تنفيذية

فالصورة التى تكون صيغتها غير تنفيذية مثل bmb , png , jpg , jpeg , gif

لكن إذا وجدنا صورة صيغتها مثلا dll , cox , com , exe , bat , pif , vbs , , scr dif , shs

فهذه صيغ تنفيذية ومنها نعرف أنها ليست صورة ...وانها تروجان ومدموج معها صورة

كيف تعرف ان جهازك مخترق مهم جدا :-

الطريقة الأولى

نفتح قائمة أبدأ

ثم نختار Run

ثم نكتب الامر التالى

system.ini

ثم نضغط ok

بعد ذلك سوف تظهر لنا مفكرة note pad بها بعض الاوامر كما بالصورة

اذا ظهر لك رقم 850 كما هو محدد بالصورة فان جهازك سليم 100 % وغير معرض للاختراق

أما اذا ظهر لك الرمز WOA

فهذا يعنى ان جهازك مخترق وبه ملفات تجسس وسهل جدا ان يتم إختراقة فى أى وقت

ويفضل أن تقوم بمحو الملفات الخاصة بأسرع وقت حتى لا يتم نقلها أو نقوم بعمل باسورد

الطريقة الثانية

1- إذهب إلى قائمة أبدا start ثم تشغيل أختر run

2- ثم فى Run اكتب Cmd

3- ثم اكتب هذا الأمر netstat –a ولاحظ المسافه بين حرف (T) وعلامه (-)

4- ثم اضغط (Enter)

5- سيتم عرض جميع المنافذ المفتوحه في جهازك والتي تكون بعد الرمز(:) مباشره اما ما قبل الرمز فهو اسم الكمبيوتر الخاص بك الذي تم تعريفه عند تجهيز شبكه الاتصال

6- والان قارن ارقام المنافذ التي تظهر لك مع ارقام المنافذ التاليه وهي المنافذ التي يفتحها في العاده ملف (الباتش) التي ببرامج التجسس او التخريب ...

فأن وجدت رقم من ضمن ارقام المنافذ فان جهازك قد اخترق من قبل هكر وعليك في هذا الحالة التخلص اولا من ملف التجسس ثم بعد ذلك عليك باغلاق المنافذ المفتوحه ....

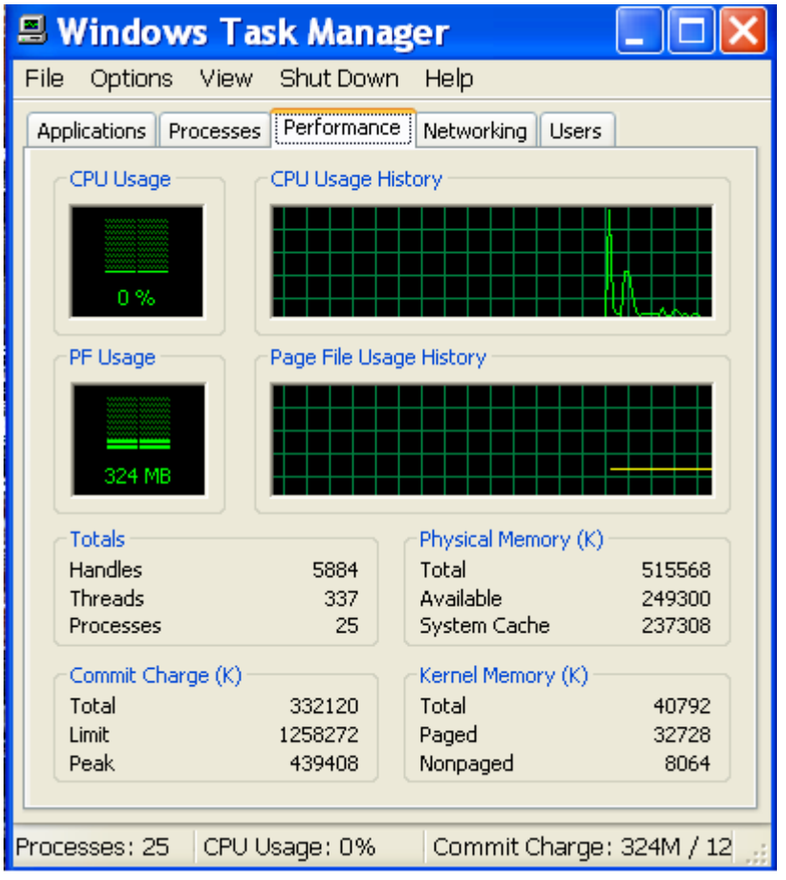
وان لم تجد رقم من هذه الأرقام في تقرير الدوس فان جهازك في أمان ولم يتم اختراقه

10034 -1045 – 4590 – 6711 -7300 – 7301 - 7306 - 7303 - 7308 -30029 – 30100 - 30101 - 30102 – 31337 – 30338 – 31339 – 31666 – 54320- 54321 - 6711- 6776 - 1234 – 1999 – 0 - 43002 - 5401 - 0954 - 1176 - 0037- 1037 - 6037 - 3037 - 8037 - 92003 - 00103 - 10103 - 20103 - 73313 - 83313 - 93313

الطريقة الثالثة

عند الضغط على الأزرار (Alt + ctrl + Delete) ..

سوف تفتح معك نافذة إدارة المهام



اذا وجدت الرسم البياني المشابة لمخطط القلب بالاعلى..

مرتفع ويمشي بخط مستقيم .. أعرف ان جهازك مهكر , ولتقم بعمل الفورمات فورااااا.

كيف تحمي جهازك من الاختراق بدون برامج :-

عندما تكتشف أن جهازك مخترق الأفضل أن تقوم بعمل فورمات للجهاز لأن أحياناً ملفات الباتش تجدد نفسها حتى لو حذفتها أما إذا لم تستطع أو لا تريد عمل الفورمات
فعليك أتباع الأتى:-

هناك عدة طرق تستخدم لسد المنافذ فى جهازك التى تساعد على الأختراق :

الطريقة الأولى:-

قم بحذف ملف الباتش الذى يساعد على الأختراق بواسطة ملف تسجيل النظام **Registry**
و ذلك بأتباع الطريقة الأتية :-

1- من قائمة Start نختار Run
2- ثم نكتب في خانة التشغيل Run الأمر regedit
3- ثم نفتح المجلدات التالية حسب الترتيب في قائمة : Register Editor

HKEY_LOCAL_MACHINE

Software

Microsoft

Windows

Current Version

Run أو Run once

- والآن من نافذة تسجيل النظام Registry Editor انظر إلي يمين النافذة بالشاشة المقسومة ستشاهد تحت قائمة Names أسماء الملفات التي تعمل مع قائمة بدء التشغيل ويقابلها في قائمة Dataعناوين الملفات .

- لاحظ الملفات جيدا فإن وجدت ملف لايقابلة عنوان بالـ Data أو قد ظهر أمامه سهم صغير <--- فهو ملف تجسس إذ ليس لـه عنوان معين بالويندوز

و إذا لم تجده تحقق من الملفات إذا وجدت أسم غريب أبحث عنه فى جوجل سوف يعطيك معلومات عن الملف إن كان ضار أم لا .

- فإذا وجدت ملف إختراق تخلص منه بالضغط على الزر الأيمن للفارة ثم Delete

**** لو وجدت أحدى العناوين الأتية الموجودة فى Date أحذفها :-**

NET POWER

C:\WINDOWS\NET POWER.EXE /nomsg

Explorer32

C:\WINDOWS\Expl32.exe

ole C:\WINDOWS\SYSTEM.ljsgz.exe

***** و كذلك ملفات التجسس التالية :-**

الملف الأول

Back Oriface

طريقة التخلص من هذا الملف:

1- من قائمة البداية Start اختر Run و اكتب Regedit ثم Ok

2- من القائمة على اليسار اختر

HKEY_LOCAL_MACHINE ----- ثم Software ----- ثم Microsoft -----

ثم Windows ----- ثم Current Version ----- ثم Run أو احياناRun Once .

3- اسم الملف Server وهو متغيير من مكان لآخر ولكن امتداده دائما EXE لكن يمكنك معرفته

كون اسم الملف Server وتظهر بعده مسافة ومن ثم exe عندما تجد الملف الغه تماما..

الملف الثاني

Net Busالنسخة قبل 2000

هو الاكثر انتشارا على الشبكة .حجمه 470 كيلو بايت يستخدم المنافذ 12345 و المنافذ 12346و هو يمكن المخترق من السيطرة شبه الكاملة على جهازك.

طريقة التخلص من الملف:

1- من قائمة Start اختر Run و اكتب Regedit ثم OK

2- من القائمة على اليسار اختر

HKEY_LOCAL_MACHINE ----- ثم Software ----- ثم Microsoft -----

ثم Windows ----- ثم Current Version ----- ثم Run services

3- ابحث في القائمة على اليمين عن NBsvr.exe هذا هو اسم الملف في الغالب هكذا انت على علم ان جهازك مصاب .. و عليك بالعلاج التالي .وحتى و ان لم تجد الملف السابق اكمل الخطوات التالية.

4- انتقل إلى HKEY_LOCAL_USER ثم ابحث عن مجلد اسمه NetBus Server اضغط على المجلد بزر الفأرة الايمن اختر DELETE

5- ثم اختر إعادة تشغيل الجهاز بوضع دوس DOS

6- اكتب Cd Winodw ثم إدخال Enter لتنتقل إلى مجلد الوندو ثم اكتب CD system ثم إدخال Enter لتنتقل إلى مجلد النظام و من ثم اكتب Del NBSvr.exe ثم إدخال لحذف الملف ، Del NBHelp.dllو اخيرا أكتب Del Log.txt ثم Enter لحذف الملف كذلك . واعد تشغيل جهازك.

الملف الثالث

Heack'a Tack'a

يستخدم بروتوكل FTP مما يصعب الوصول اليه.يستخدم المنافذ رقم 31785 و 31787 و 31789 و 31791

طريقة التخلص من الملف:

1- من قائمة Start اختر Run و اكتب Regedit ثم OK

2- من القائمة على اليسار اختر

HKEY_LOCAL_MACHINE ----- ثم Software ----- ثم Microsoft -----

ثم Windows ----- ثم Current Version ----- ثم Run أو احياناRun Once .

3-ابحث عن Explorer32 و الذي يوافق المسار C:\WINDOWS\Expl32.exe و قم بحذفه

الملف الرابع

NetSphere

يستخدم المنافذ TCP 30100 - TCP 30101-TCP 30102

طريقة التخلص من الملف:

1- - من قائمة Start اختر Run و اكتب Regedit ثم OK

2- من القائمة على اليسار اختر

HKEY_LOCAL_MACHINE ----- ثم Software ----- ثم Microsoft -----

ثم Windows ----- ثم Current Version ----- ثم Run .

3- ابحث في الجهه اليمنى عنc:\windows\system\nssx.exe

4- احذف هذا الملف . و اعد تشغيل الجهاز بواسطه الضغط على CTRL+ALT+DELETE

الملف الخامس

Net Bus Ver 1.6 & 1.7

تعريف :

الحقيقة ان النت باص أو أتوبيس الشبكة من أسهل برامج الاختراق و أشهرها لانتشار ملفه الخادم ..أو المسمى بالسيرفر ..

التخلص منه :

النت باص يستخدم الباتش سيرفر و يختبئ في الريجستري..

وللتخلص منه اتبع الآتي :

يجب أولا إطفاء الجهاز وتشغيله في وضعية السيف مود " safe mode "

اتجه للريجسترى ثم ابحث عن الملف الآتي :

:c:\windows\patch.exe

ثم قم بمسحه واعد تشغيل الجهاز مره أخرى

الملف السادس

Net Bus 2000

تعريف :

برنامج النت باص 2000 يستخدم السيرفر العادي وهو " server.exe " و لكن يمكن تغير الاسم وهو يسجل نفسه و لاكن في منطقه أخرى في الريجستري ..

التخلص منه :

للتخلص من البرنامج قم بالبحث عن الملف و لاكن بدلا من HKEY_LOCAL_MACHIN

اتجه إلى HKEY_LOCAL_USERS

ثم ابحث عن :

الكلمة التي تحتها خط هي الخادم للبرنامج أو السيرفر .. ان وجدتها قم بإطفاء الجهاز و إعادة تشغيله في وضع السيف مود (Safe Mode) ثم تخلص من الملف واعد تشغيل الجهاز

الملف السابع

Master Paradise

تعريف:

يعتبر هذا البرنامج سيد برامج الاختراق ... ويختبئ أيضا في الريجستري

التخلص من الملف :

اتجه للريجسترى ثم ابحث عن امتداد الملف:

"C:\windowds\nameofthe.exe“

عندما تجد هذا الملف في الريجستري قم بمسحه

الملف الثامن

ICQ Torjan

تعريف:

يقوم هذا الملف بعمل ثغره للمخترقين داخل جهازك مما يساعدهم على اختراق جهازك باستخدام السيرفر الخاص بالاسكيو ..وعندما تصاب بالملف يقوم الملف بتغير الاسكيو الحقيقي لديك ICQ.exe و إبعاده وتغير اسمه ليصبحICQ2.EXE

التخلص منه :

يمكن التخلص من الملف بكل سهوله اتجه إلى الملف الخاص بالاسكيو وقم بحذف ملف الاسكيو ICQ.EXE ثم قم بتعديل اسم الاسكيو الحقيقي ICQ2.EXE إلى ICQ.EXE

الملف التاسع

VBS.Freelink or freelink

وهو يعتبر دودة مشفرة يعمل تحت اي وندوز تدعم لغه الـ VB scrypting حتى وندوز 98 ووندوز2000 . ومعظم طرق دخولة الى جهازك عن طريق ال E-MAIL ويكون عنوان الـ E-MAILالقادم اليك هو Check this وتكون الرسالة المصاحبة لهذا العنوان هي Have fun with these links. Bye فاذا قمت بفتح الرسالة فإنه يقوم مباشرة بتحميل ملفين على جهازك هما:

c:\windows\links.vbs

c:\windows\system\rundll.vbs

ايضا يضيف الجزء التالي الى جهازك على الـ

window registry

----windows----microsoft----Software----HKEY_LOCAL_MACHINE

CurrentVersion----Run----Rundll=RUNDLL.VBS

وبعد التمكن من جهازك سوف يعرض على الشاشة صندوق صغير بالعنوان التالي

:

Free XXX linksوتحت العنوان تظهر الرسالة التالية:

This will add a shortcut to free XXX links on your desktop.

Do you want to continue

بعد ذلك يقوم هذا البرنامج بالبحث عن برامج المحادثة CHAT التالية:

MIRC32.exe

Pirch98.exe

ويعدل الملفات التالية

SCRIPT.INI

EVENTS.INI

وذلك حتى يتمكن من ارسال الـ LINKS.VBS الى اجهزة اخرى اثناء عملية المحادثات بين المستخدمين CHATTING والاسماء المستعارة لهذا البرنامج التي يتخفى بها هي:

VBS

Freelink

freelink

كيف تعرف ان هذا البرنامج موجود في جهازك وطريقة التخلص منه

اولا

قم بالبحث عن الملفات التالية:

LINKS.VBS

RUNDLL.VBS

ثانيا

قم بألغاء تلك الملفات من جميع الدرايفات التي على جهازك.

ثالثا

قم ايضا بحذف الجزء التالي من الـ win regitry باستخدام الامر regedit والجزء المراد حذفة هو

HKEY_LOCAL_MACHINE----Software----microsoft----windows----
Curr entVersion----Run\Rundll=RUNDLL.VBS

الملف العاشر

Back Orifice 2000

وهو متمكن من وندوز95 ووندوز 98 ووندوز ان تي
ولهذا البرنامج نسختين الاولى تسمى النسخة الامريكية وهي فقط اكبر حجما من النسخة الاخرى بالكيلوبايت ايضا لهذة النسخة ميزة اخرى تعرف بـ DES encryption

اما النسخة الثانية فتسمى النسخة الدولية
و الاسماء المستعارة لهذا البرنامج التي يتخفى بها هي:

BO2K

backdoor.BO2K

طريقة معرفة وجودة في جهازك والتخلص منه يوجد الان برنامج واحد لحمايتك من هذا البرنامج تجده في الموقع التالي :

http://www.spiritone.com/~cbenson/current_projects/backorifice/backorifice.htm

الملف الحادى عشر

Zipped_files or explorezip Trojan

وهذا البرنامج خطير من ناحية فتكه في الملفات فقد لا تجد ملف كان بالامس موجود وهو ايضا متمكن من وندوز 95 ووندوز 98 ووندوز ان تي . وهو يستطيع نشر نفسه بنفسه باستخدام الـ E-MAIL فاذا قمت بفتحة من الـ E-MAIL فإنه سوف يعرض الرسالة التالية:

Cannot open file; it does not appear to be a valid archive. If this is part of a ZIP backup set, insert the last disk of the backup set and try again.
Please press F1 for help.

وعندما يتمكن من نشر نفسة باستخدام الـ E-MAIL فإنه يقوم بارسال نفسه مرة اخرى تحت اسم Zipped_files.exe الي جميع العناوين التي استقبلت منهم رسائل سابقة مرفقا معها الكلمات السرية والباس وورد وتحت العنوان التالي:

Hi, (username)!
I recieved your email and I shall send you a reply ASAP.
Till then, take a look at this attached zip docs.
Bye.

ايضا سوف يقوم هذا البرنامج بالغاء جميع الملفات لديك والمنتهية بالاحرف التالية

DOC,,XLS,,EXE,,PPT,,CPP وللاسف فانة صعب جدا ان تستعيد تلك الملفات باستخدام الامر undelete

الاسماء المستعارة لهذا البرنامج التي يتخفى تحتها هي

worm.explore.zip

win32.explore

explore.zip

طريقة معرفة وجودة في جهازك والتخلص منه فقط لمستخدمي وندوز95 ووندوز 98 قم بالضغط على CTRL+ ALT+ DEL وعند ظهور شاشة الاغلاق ولاحظت ظهور احدى هذه الملفات فانه موجود في جهازك والملفات هي:

Zipped_files

Explore

_setup

ويجب ان تفرق بين اسم الملف السابق Explore وبين المتصفح Explorer فاذا لاحظت احدى هذه الملفات السابقة فقم مباشرة بالغاء الملفات التالية:

C:\windows_setup.exe

C:\windows\Explore.exe

بعد ذلك قم بالغاء الاسطر التالية والموجودة في

WIN.INI باستخدام الامر msconfig والاسطر هي:

run=setup.exe

run=c:\windows\system\explore.exe

ايضا قم بالغاء السطر التالي باستخدام الامر

regedit

----Windows----Microsoft----Software----HKEY_CURRENT_USER

CurrentVersion----Windows----Run

الملف الثاني عشر

Promail.Trojan

انتشر كثيرا هذا البرنامج بطريقة الـ freeware و الـ shareware

وقد انتشر تحت هذا الاسم promll121.zip

وهو ملف غير مضغوط داخل هذا الملف promail.exe

فاذا قمت بتحميلة على جهازك وقمت بعد تحميلة بالاشتراك مع اي شركة لخدمات البريد الالكترونية فان جميع المعلومات التي اعطيتها لهذه الشركة إضافة الى كلمة السر الخاصة بك يقوم هذا البرنامج بارسالها الى عنوان بريدي اخر غير معروف اي بطريقة عشوائيه

فكلما قمت بعملية اشتراك مع اي شركة اخرى لخدمات البريد الالكتروني فان البرامج يقوم بنفس العملية السابقة . فقط اذا كان لديك هذا البرنامج Promail قم مباشرة بالغاءه.

الملف الثالث عشر

BackDOOR.G

وهو ايضا يحتاج الى خادم لتشغيلة

ويوجد اصدارين من هذا البرنامج.

للتخلص من الاصدار الاول قم مباشرة بالبحث عن الملفات التالية وحذفها:

DATA2.EXE

TINURAK.EXE

WATCHING.DLL

وللتخلص من الاصدار الثاني قم مباشرة بالبحث عن الملفات التالية وحذفها

WINDOW.EXE

NODLL.EXE

SERVER_33.DLL

الملف الرابع عشر

K2PS.EXE

فقط يستطيع التمكن من وندوز95 ووندوز 98 وقد انتشر عن طريق البريد الالكتروني تحت اسم K2PS.EXE

حيث تقول رسالته الخبيثة أن هناك فيروس اسمة TX-500 وانه برنامج مضاد لهذا الفيروس . طبعا كما تعرف هذة مجرد كذبة ليتمكن من الدخول وسرقة معلومات اشتراكك مع مقدم خدمة الانترنت بالاضافة الى كلمة السر الخاصة بك والغريب في هذا البرنامج أنه لا يكتفي بسرقة الباسوورد بل يغير الباسوورد فلا تستطيع الدخول مرة ثانية الى الشبكة اليس خطير هذا البرنامج .

والطريقة المفضلة اذا احسست بهذا التغير قم مباشرة بتغير كلمة السر.

ثم ابحث عن هذه الملفات واحذفها مباشرة

K2PS.EXE

K2PS.CFG

ثم باستخدام الامر regedit قم بحذف:

HKEY_LOCAL_MACHINE ----Software---- Microsoft ----Window----

CurrentVersion---- C:\WINDOWS\SYSTEM\K2PS.EXE

الملف الخامس عشر

Win32.PrettyPark

هذا البرنامج يستطيع الانتشار ايضا عن طريق البريد الالكتروني فعند تنفيذه سوف يقوم بارسال نفسه الى العناوين الموجوده في الـ windows address book وسوف يخبر المستخدمين الموجودين على ال IRC عن اعدادت النظام وكلمات السر . وسوف يقوم بنسخ نفسة داخل الـ windows system directory مع الملف files32.VXD ايضا سوف يقوم بتسجيل نفسة داخل الـ HKEY_CLASSES_ROOT تحت أسم

exefile\shell\open\command\files32.vxd

فقط قم بالغاء ذلك الاسم باستخدام الامر

regedit

الطريقة الثانية :-

- بواسطة الأمر : msconfig

- انقر على زر البدء Start

- اكتب في خانة التشغيل Run الأمر التالي msconfig

- سوف تظهر لك نافذة System Configuration Utility

- اختر من هذه النافذة من أعلى قسم Start up

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

- أفحص هذه البرامج جيدا بالنظر فإن شككت بوجود برامج غريبة لم تقم أنت بتثبيتها بجهازك فقم بإلغاء الإشارة الظاهرة بالمربع الصغير المقابل لها فبذلك تكون قد أوقفت عمل البرنامج التجسسي أو غيره من البرامج الغير مرغوب بها.

الطريقة الثالث :-

- بواسطة مشغل الدوس : Dos

هذه الطريقة كانت تستخدم قبل ظهور الويندوز لإظهار ملفات التجسس مثل الباتش والتروجان وهي من أسهل الطرق:

-افتح الدوس عن طريق :

start→programs→accessories→command prompt

- أكتب الأمر التالي : dir patch

إذا لم يوجد ملف الباتش سوف يقول لك أن الملف غير موجود (the file is not found)

- إن وجدت ملف الباتش فقم بمسحة بالطريقة التالية أكتب فى الشاشة السوداء : del patch*.*

الطريقة الرابعة :-

- هذه الطريقه تستطيع تقفيل جميع البورتات (الثغرات الامنيه) الموجوده بكل الاجهزه :-

1- إذهب إلى قائمة أبدا start ثم تشغيل run

2- ثم اكتب الامر التالي command.com

3- ستظهر لك نافذة اكتب فيها هذه الكلمة ping host ثم أضغط Enter

4- ثم أكتب ping port ثم أضغط Enter

5- ثم إنتظر و أكتب ping port1027 ثم أضغط Enter

6- و إنتظر ثم إكتب ping port80 ثم أضغط Enter

7- ثم اكتب ping أو ping proxy أو ping ***** ثم أضغط Enter

8- ثم اكتب ping port و أضغط Enter

* انتظر لفترة تقريباً من 15الى20دقيقة واذا لم تختفي النافذة قم باغلاقها واعد تشغيل الجهاز.

الطريقة الخامسة :-

- لأخفاء جهازك من الشبكة بدون برنامج :-

1- إذهب إلى قائمة أبدا start ثم تشغيل run

2- فى Run اكتب Cmd سوف تظهر شاشة سوداء

3- اكتب هذا الأمر net Config Server /hidden:yes

4- ثم انتظر نصف ساعة و ستجد ان جهازك قد اختفى من الشبكة مع العلم ان ذلك لا يأثر على الـ Share او إذا كنت تستخدم برنامج مثل الـ Pcany Where أو Net Support

5- و للتراجع عن هذا الأمر اكتب فى الشاشة السوداء Net Config Server /hidden:no

6- ثم انتظر نصف ساعة واعمل Restart للجهاز وسوف يظهر الجهاز كما كان

ملحوظه

وهذا الأمر تم تجربتة على نسخة Xp /sp2

وتم تجربتة ايضا على شبكة بنظام Domain و على شبكة بنظام WorKGruop وتم بنجاح

أهمية هذه الحركة

عندما تقوم بإخفاء جهازك عن الشبكة المحلية أو حتى العالمية سيكون من سابع المستحيلات أن يتم

إختراق جهازك إلا من أفضل مخترقين العالم ربما فهذه الحركة مهمه لكل واحد يشبك على الإنترنت أو حتى على شبكة محلية أو أي شبكة .

الطريقة السادسة :-

- ايقاف خاصية مشاركة الملفات :

1- إذهب إلى قائمة أبدا start ثم settings ثم control panal

2- ثم أدخل network connections

3- أضغط click right ثم properties

4- أحذف علامة صح من أمام أختيار

file and printer sharing for Microsoft networks

5- ثم أضغط ok

الطريقة السابعة :-

- لأغلاق ثغرات الوندوز إكس بي ~ ويندوز ~ Xp فقط :-

1- إذهب إلى قائمة أبدا start ثم تشغيلrun

2- فى Run اكتب Cmd

3- ثم أكتب netstat -ano لترى المنافذ المفتوحه

فيه حوالي 17 منفذ مفتوح وفي حالة استماع listen

4- قم بنسخ الأوامر التالية وألصقها في الدوس

sc config policyagent start= disabled

sc config ssdpsrv start= disabled

sc config messenger start= disabled

sc config w32time start= disabled

sc config netbt start= disabled

exit

الطريقة الثامنة :-

- لأغلاق جميع البورتات والمنافذ المفتوحه بجهازك لحمايتك من الاختراق من قبل الهكرز :-

1- إذهب إلى قائمة أبدا start ثم تشغيل run

2- فى Run اكتب ftp –rc

- و بهذا تكون تكون قد اغلقت جميع البورتات المفتوحه بجهازك .

الطريقة التاسعة :-

- اخفاء IP الخاص بجهازك ب 4 خطوات وبدون برامج :-

رقم IPهو رقم جهازك علي الشبكة ويعتمد الهاكرز علي رقم الأي للدخول الى جهازك

لاخفاء الـ IP اتبع التالي ..

1- إذهب إلى قائمة أبدا start ثم تشغيلrun

2- فى Run اكتب Command

3- ثم أكتب drwatson ثم إضغط Enter

وسوف تظهر لك صورة رأس شخص شعره اصفرعلى شريط المهام....

واذا أردت اظهار الأي بي فقط اغلق اطار الدكتور واطسون.

اقوى جاسوس من الاستخبارات الامريكية في جهازك احذفة :-

- قامت الاستخبارت الامريكية بزراعة هذا الجاسوس في انظمة الاكس بي طبعا

- وظيفه هذا الجاسوس

يقوم بارسال كل المعلومات الموجودة في الداخل اضافة الى كل العمليات التي نقوم بها في حواسيبنا الشخصية

- للتخلص منه قم بالأتى :-

1- إذهب إلى قائمة أبدا start ثم تشغيلrun

2- فى Run اكتب Cmd

3- ثم أكتب net user

إذا كانت النتيجة كالتالي :- Support_388945a0 أذن server موجود فى نظام تشغيلك

ثم قم بكتابة الأمر التالى مع مراعاة الفواصل :-

net user SUPPORT_388945a0 /delete

ثم أكتب الأمر Exit

و للتأكد من الحذف قم بأعادة الخطوات الأولى ستجد أنه تم حذفه

من أشهر برامج الحماية (فير وول) :-

هناك عدة برامج للحماية منها

BlackICE Defender v2.5 co

Norton Internet Security 2001 v 2.5 Family Edition

Tiny Personal Firewall 2.0.14

Zone alarm

Intruder Alert '99

من أشهربرامج مقاومة الفيروسات:-

تعددت برامج الحماية من الفيروسات لكن هناك مجموعة تعد الشهيرة فى هذه البرامج

Mcafee

Norton Anti-Virus

Pc-cillin

AntiViral Toolkit Pro (AVP) Gold

AntiViral

Norton Anti-Virus 2001

Cleaner V.3.2

Avira personnel

في النهاية يجب توخي الحذر الشديد من الجميع في التعامل مع ما يلي:-

اولا :-

E-MAIL

*يجب الحرص الشديد على كلمة السر وتغيرها من فترة الى اخرى

*عدم فتح الرسائل اذا لم تعرف مضمونها او اذا لم تعرف عنوان الشخص المرسل

* ايضا تجنب اعطاء عنوانك البريدي لاي شخص او شركة غير معروفين لديك

*بعض الرسائل القادمة الى البريد الالكتروني تاتي بعناوين مغرية ومشوقة لفتح هذة الرسائل ولكن لا تقوم بفتحها بل قم مباشرة بالغاءها وكما لاحظت من ان كثير من برامج الاختراق والفيروسات تستطيع الدخول الى جهازك عن طريق البريد الالكتروني

* ايضا قم دائما بتنظيف بريدك من الرسائل القديمه والغير مهمة.

ثانيا :-

GAMES

يجب الحرص ايضا من التعامل من العاب الكمبيوتر خاصة التي تحتاج إلى تشات من الموقع او التي تكون تحت عنواين مشبوهة مثل وألعاب اليانصيب للحظ السعيد وغيرها من الالعاب

ثالثا :-

SCREEN SAVERS

احرص ايضا من تحميل الـ SCREEN SAVERS من الانترنت لانه قد يكون مرفق معها بعض الفيروسات او برامج الاختراق . ايضافة الى انها قد تؤثر على جهازك فبعض المشاكل التي تواجة اجهزتنا يكون سببها هو الـ SCREEN SAVERS

رابعا :-

SOFTWARES

لا تقوم بتحميل برامج عن طريق الانترنت من شركات ضعيفة او غير معروفة في عالم الكمبيوتر ايضا حاول دائما تحميل البرامج خارج ال سي درايف اي باستخدام CD-Writer او باستخدام Zip-drive

خامسا :-

chat

تجنب التعامل مع برامج المحادثة الأتيه وايضا يفضل حذفها من الجهاز واذكر منها :-

ICQ ------ MIRC ------ FREETEL ------ NETMEETING ------ irc