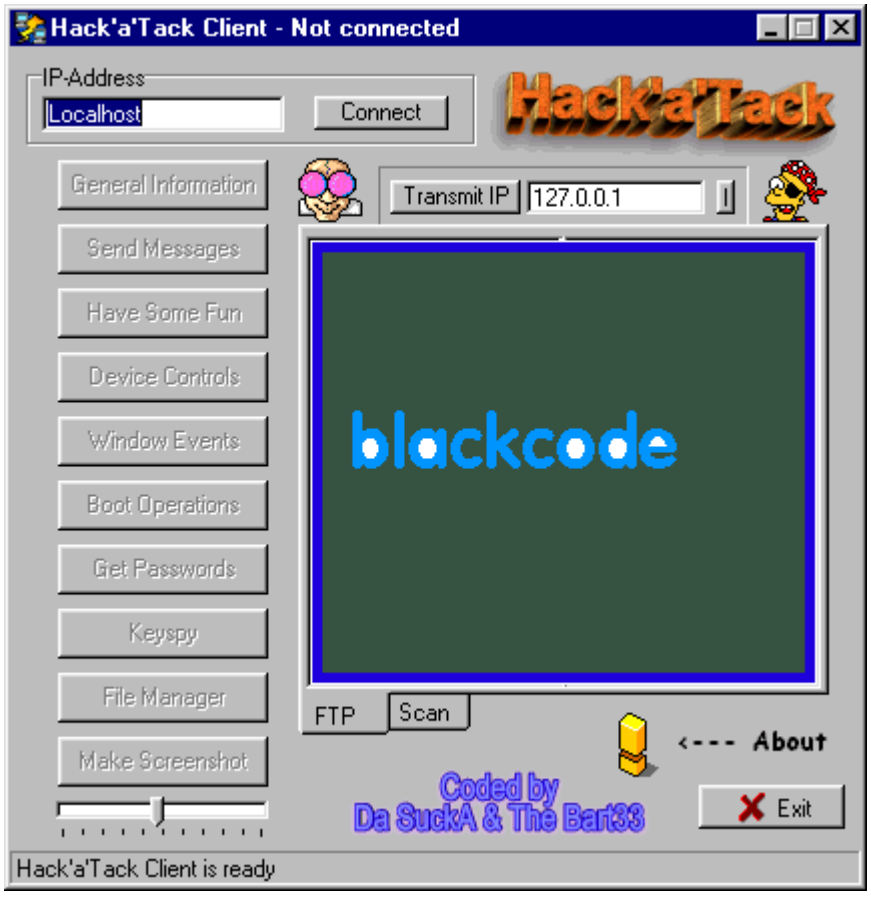
العنوان : أقوى درجات الحماية فى عالم الكمبيوتر و الأنترنت

##مقدمة الموضوع :-

هدفى من شرح هذا الموضوع المدعم بالصور العديدة هو أن أوفر أقصى درجة من الحماية لجميع مستخدمى الكمبيوتر . و لا تتعجبوا لأنى وضعت لكل برنامج من هذه البرامج صورة له ، و لكن لى أسبابى العديدة ، و أهمها هو أنكم من رؤية صورة البرنامج ستدركون مدى خطورته على أجهزتكم ، و هذا بالنسبة لكم يعتبر دليل مدعم لشرحى بهذا الموضوع المثيييييييييييييييييييير و البديييييييييييييييييييييع ، و هذا الشرح لا يوجد فيه أى نوع من الشك؛ لأن كل هذه البرامج التى سأشرحها بالأسفل جربتها بالفعل على ضحايا كثيرين ... و الى هيعمل ضجة بالفعل على مستوى المواقع ، و الفريد من نوعه فى الشرح و الأمكانات التى ستدركونها بصرف النظر عن هذه المقدمة ..... مع تمنياتى للجميع بالأستمتاع .

##برنامج الـ (hack'a'tack) :-



١ـتوجد ملحوظة صغيرة و هامة : و هى أن (الباتش) له اسم فى (الريجسترى) ، و اسم آخر مختلف عن الثانى فى فولدر ال (system) . فى البداية ... هذا البرنامج يمكنك عمل أختراق به على أى جهاز به: (windows 95) و (windows 98) و (windows me) ... لذلك أنصح بتحميل (windows 2000) أو (windows nt) أو (windows xp) أو (unix) أو (linux) .

٢ـثانياً ... لكى تتأكد من أن ملف السيرفر الخاص بالبرنامج ليس موجوداً فى جهازك ؛ فستجده فى فولد ال (windows) ، و اسمه هو (expl32.exe) . و عيب هذا الملف أنه يساعد بعض المخترقين على التعامل مع جهازك بسهولة .

٣ـو البورتات التى يستطيع البرنامج التسلل الى جهازك من خلالها : تنقسم الى قسمين : بورتات ال (tcp) و هى (٣١٧٨٥) و (٣١٧٨٧) ، أما بورتات ال (udp) و هى (٣١٧٨٩) و (٣١٧٩١) .

٤ـو أنا هقول لكم حتة جامدة من أخيكم blackcode ... و فكرة البرنامج أو الأختراق هنا بأختصار كالتالى : أنا من قبل كنت شرحت العلاقة بين ال (server) و ال (client) ، و لكنى سأشرحها هذه المرة لأهميتها بالنسبة لكم ... أنا كنت قلت أن ال (server) على سبيل المثال كمكتب مخصص لأنك تستعلم منه فقط عن أى

معلومات تحتاجها منهم ، أما ال (client) على سبيل المثال كعميل ما يريد أن يستفسر عن شئ ما من هذا السيرفر .. مركزيين معى ؟ و لنفسرها معاً من يكون السيرفر ، و من يكون الكلاينت ، و هى شئ بديهى لا يحتاج الى نوع من الذكاء : حيث أن البرنامج أو جهازك سيمثل ال (client) ، أما جهاز الضحية فهو يمثل ال (server) و السبب هو أنك أنت الذى تحتاج الى تجميع بعض المعلومات أو الأستفسار عن بعض المعلومات المطلوبة لأختراق هذا الجهاز ... المهم و هو غرضى من هذا الموضوع و هو أنك لكى تتسلل الى جهاز الضحية فما هو مطلوب أولاً ألا أن يكون جهاز الضحية به أحد البورتات المذكورة سابقاً مفتوحة ، و ذلك لكى يتسلل منها المخترق .. ثانياً و هو الأهم و هو أن البرنامج يقوم بوضع ال (server) أو ما يسميه البعض (الباتش) فى مكان معين فى جهاز الضحية لكى يجمع المعلومات التى يحتاجها لأختراق جهاز الضحية ، و هذا هو موضوعى اليوم عن (كيفية البحث عن الباتشات الموجودة فى جهازك أن وجدت !!!) ، و ليس (كيفية الأختراق !!!) ... و بهذا تكونون قد فهمتم الى حدٍ ما المفهوم العام لهذه العملية .

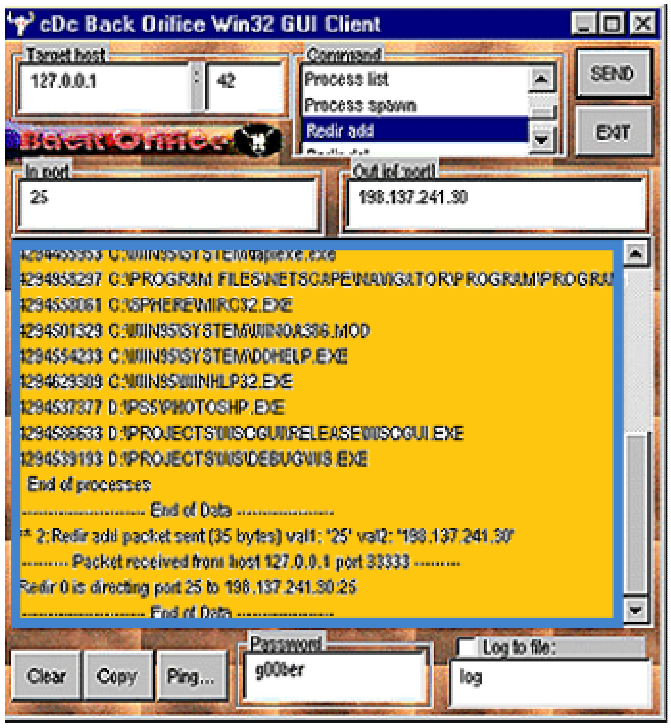
٥-لنفرض أنك وجدت عندك أحد الباتشات الخاصة بهذا البرنامج ، و تريد أزالته من جهازك ... فكيف ستكون الخطوات المتبعة لهذه العملية ؟ و هى كالتالى ....

٦-أذهب الى قائمة (start) ، ثم (run) ، ثم أكتب فيها الأمر (regedit) ، و اضغط (ok) ، و ستفتح لك شاشة مفصولة من المنتصف : فعلى اليسار أذا ضغطت على أى شئ فيها فستظهر محتوياته على اليمين ... المهم بعد أن تفتح لك الشاشة .. قم بالذهاب الى الأمتداد التالى ...

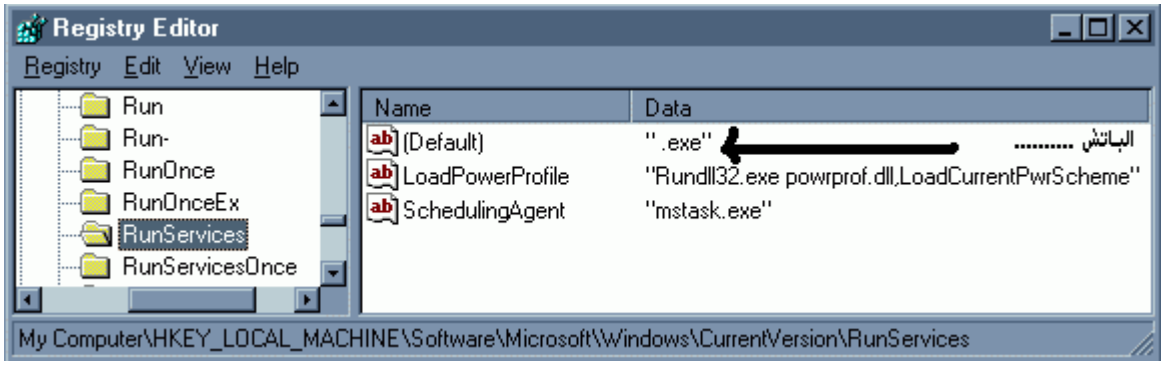
(hkey_local_machine\software\microsoft\windows\currentversion\run)

و عندما تضغط على (run)؛ ستجد على اليمين ملف اسمه (explorer32) ، و مكتوب أمامه هذا الأمتداد (c:\windows\expl32.exe) ... و هذا الأمتداد السابق ما هو ألا مكان هذا الباتش فى الويندوز ، و لكى تمسحه من جهازك فما عليك ألا أن تزليه كما تزيل أى ملف أو فولدر ، ثم تغلق الجهاز ، ثم شغل الجهاز مرة أخرى و لكن أدخل على شاشة الدوس السوداء ، و تأكد أنك على الأمتداد (c:\windows) ، و أذا لم تكن على الويندوز فأكتب الأمر (cd windows) و اضغط (enter) ... و أكتب الأمر التالى (del expl32.exe) و اضغط (enter) ، و اضغط بعدها (alt+ctrl+delete) ... و بهذا تصبح آمناً من مشاكل برنامج ال (hack'a'tack) .. أى خدمة يا باشاوات .

برنامج الـ (back orifice) :-



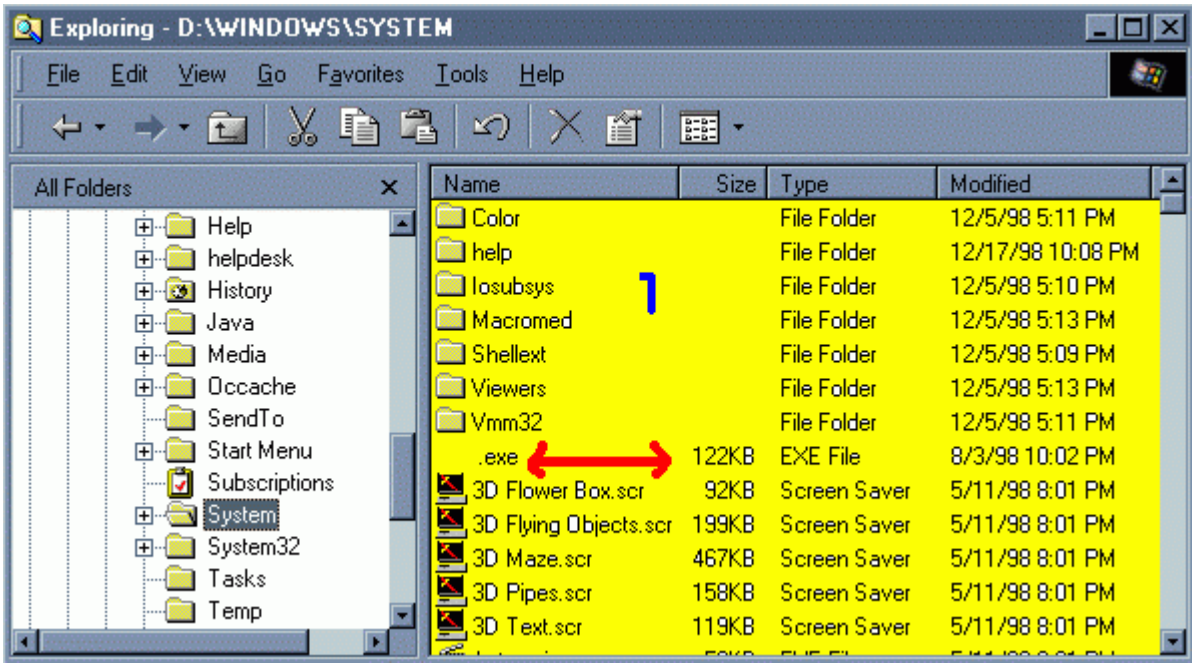
١ـ و الصورة السابقة طبعاً هى صورة للبرنامج ، و هذا البرنامج يعتبر أقوى و أخبث برنامج على مستوى برامج الأختراق . و هو قوى جداً فى التعامل مع الضحية و مفعوله سريع جداً .

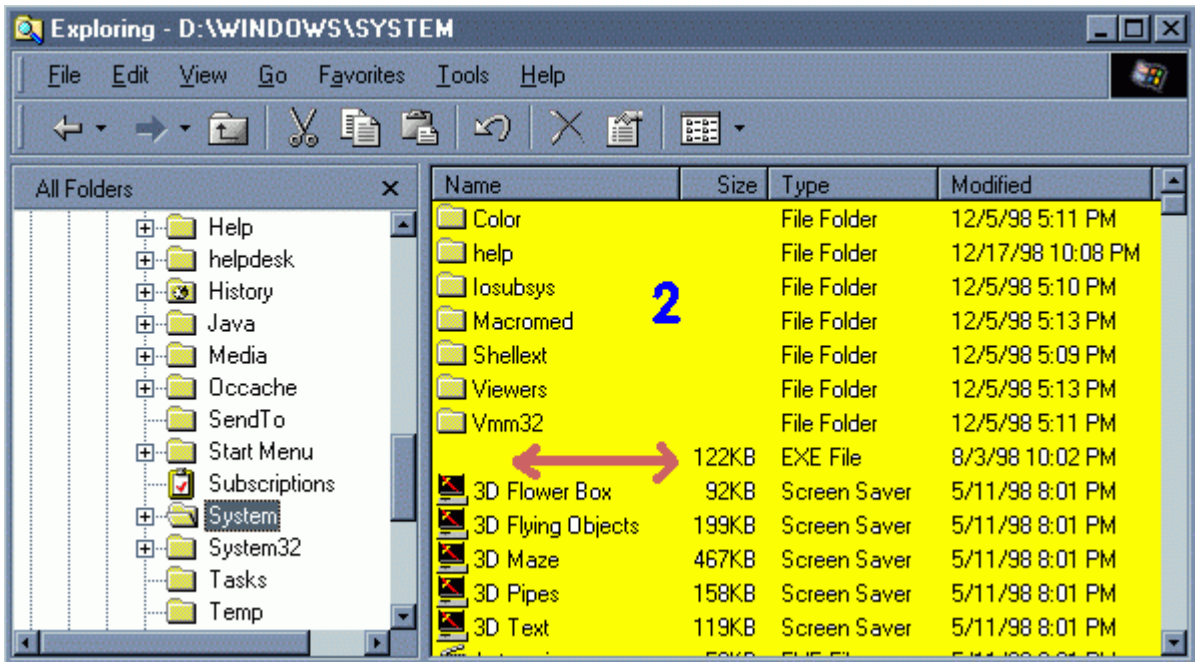


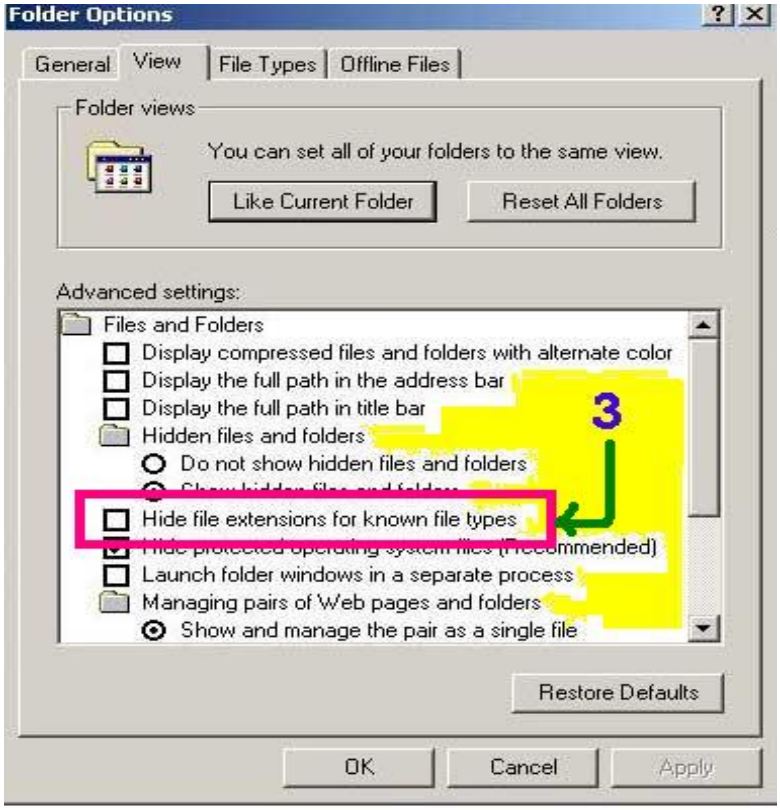
٢ـ بالنسبة لتفسير الصورة السابقة ، فهو كالتالى : غالباً و مع الأسف ما يكون ملف الباتش ليس له اسم أو مخفى ، و لكى تعرف مكانه ؛ فما عليك ألا بالذهاب الى الأمتداد التالى ، و كما هو موضح فى الصورة السابقة ...

(hkey_local_machine\software\microsoft\windows\currentversion\runservices)

و عندما تضغط على (runservice) ؛ ستجد على اليمين ملف ليس له اسم ، و هو مكتوب كالتالى (.exe) . و من المفروض أنا هذا المكان فى الريجسترى ليس من المسموح وجود أية ملفات فيه .







٣-ملحوظة هامة هامة هامة هامة هامة هامة جداً جداً جداً جداً جداً جداً جداً جداً جداً :

أرأيتم كم مرة كتبت العبارة (هامة جداً) ، و السبب هو أن (٩٩%) من مستخدمى الكمبيوتر لا يعلمون هذه الملحوظة و أهميتها ، و هى أنك عندما تفتح (my computer) ، ثم تضغط على (view) الموجودة أعلى اليسار ، ثم (folder options) ، و فيها من الأعلى ستجد قائمة (view) كما هو موضح فى الصورة السابقة التى ستجد فيها الرقم (٣) مكتوب ، و عندما تفتحها ستجدنى محدداً جملة (بمربع أحمر) ، و هى ما سأشرح أهميتها العظيمة الآن : و هذه العبارة يقصد بها (أنها تسألك هل تريد أن تضع مع اسم كل ملف فى الويندوز الأمتداد الخاص به ؟؟ بمعنى أنك لو عندك مثلاً صورة اسمها (١) و هى من النوع (gif) ؛ فأذا أزلت (علامة الصح) الموجودة بجانب العبارة الموجودة فى الصورة فأنك بهذا تقول للويندوز أجعلى الصورة التى اسمها (١) و هى من النوع (gif) تكتب كالتالى (1.gif) : بأختصار ستجد كل ملفات الويندوز سواء صور أو أفلام أو كليبات أو غيره مكتوب معها ال (extension) الذى ينتمى لها ... و هدفى من هذا الموضوع هو أنك لو جعلت كل ملف مكتوب معه أمتداده فأنك بهذا ستظهر (كل ألاعيب المخترقيين) ، و الألاعيب التى أعنيها هى أن برنامج مثل ال (back orifice) هذا أذا نزل لك باتش فى جهازك من خلال هذا البرنامج ، فأمامك حل واحد لكى تتعرف على هذا الباتش و هو كما قلت لكم هو (أنك تزيل علامة الصح)

الموجودة بجانب العبارة الموجودة فى الصورة رقم (٣) ، و سيظهر لك الباتش بالشكل المكتوب فى الصورة رقم (١) ... و لكن (أذا لم تزيل علامة الصح) فأن الملف سيظهر كما تراه فى الصورة رقم (٢) و لو حاولت أنك تساوى الملفات بجانب بعضها فلن تنجح العملية ، و السبب هو أن الباتش قد أخذ هذا الحيز و لكنه مخفى عن الأعين ... فهمتونى ؟؟؟ ..... و لكى تمسح الباتش من جهازك فما عليك ألا أن تزليه كما تزيل أى ملف أو فولدر ، ثم تغلق الجهاز ، ثم أفتح ال (windows explorer) ، و أذهب الى الأمتداد الذى تجد فيه ملفات النظام : أذا كنت عندك (ويندوز ٩٥) أو (ويندوز ٩٨) أو (ويندوز ميلينيوم) فأذهب الى هذا الأمتداد (c:\windows\system) ، أما أذا كنت عندك (ويندوز ٢٠٠٠) أو (ويندوز أن تى) أو (ويندوز أكس بى) فأذهب الى هذا الأمتداد (c:\windows\system32) ، و أول ما تفتح هذا الفولدر ستجد الصورة المكتوب بداخلها رقم (١) السابقة ، و أمسح الملف الذى تجدنى محدداً بجانبه سهم . و على فكرة ممكن تجدون الباتش بأسم ، و لكن لكى تكشفوه ستجدونه بدون أيقونه .... ماااااااااااشى يا أساتذة ؟؟

٤-و يتسلل هذا البرنامج من البورته (٣١٣٣٧) .

##برنامج الـ (deep throat) :-

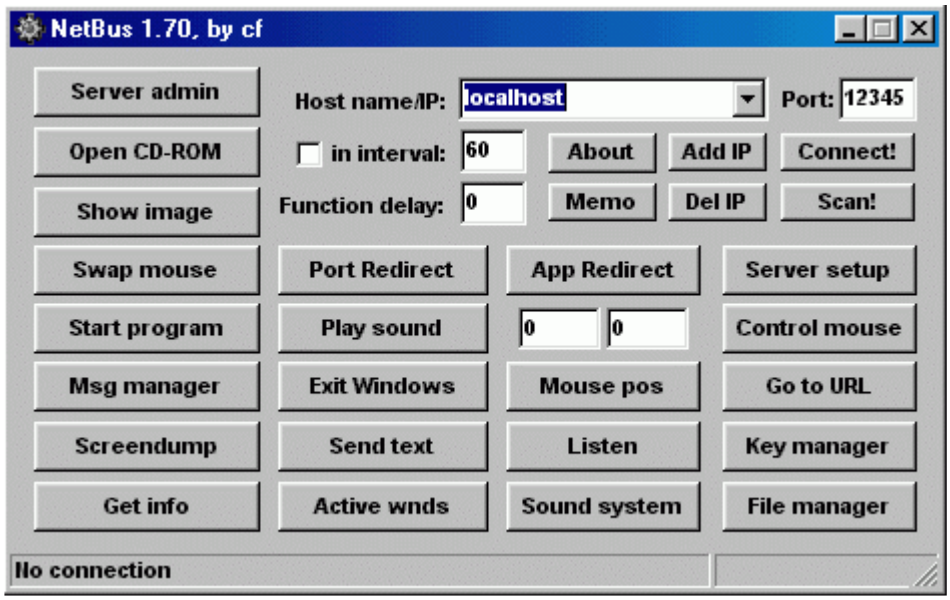
١ ـ بالنسبة لتفسير الصورة السابقة ، فهو كالتالى : لكى تعرف مكانه ؛ فما عليك ألا بالذهاب الى الأمتداد التالى :

(hkey_local_machine\software\microsoft\windows\currentversion\run)

و عندما تضغط على (run)؛ ستجد على اليمين الباتش ، و اسمه هو (systemdll32) ، و ستجده طبعاً فى فولدر الويندوز و لكن باسم (systempatch.exe) . و طبعاً لكى تزيلون الباتش فأنتم عرفتوا الطريقة المتبعة لذلك .

٢ـو البورتات التى يتسلل منها هذا البرنامج : (٢١٤٠) و (٣١٥٠) ، و هى من النوع (udp) .

##برنامج الـ (netbus) :-



١ـ بالنسبة لتفسير الصورة السابقة ، فهو كالتالى : لكى تعرف مكانه ؛ فما عليك ألا بالذهاب الى الأمتداد التالى :

(hkey_local_machine\software\microsoft\windows\currentversion\run)

و عندما تضغط على (run)؛ ستجد على اليمين الباتش ، و اسمه هو (patch.exe) ... سواء فى الريجسترى ، أو فى فولدر ال (system) .

٢ـ و البورتات التى يتسلل منها هذا البرنامج : (١٢٣٤٥) و (١٢٣٤٦) .

##برنامج الـ (whack-a-mole) :-

١-هذا البرنامج بالذات له قصة كبيرة ، و مع الأسف أيضاً يغفل عنها النسبة الأغلبية من مستخدمى الكمبيوتر ... و قصة هذا البرنامج تبدأ من خلال الألعاب التى يستمتعون بها الأغلبية من أجل التسلية : فمن المعروف أن الكثير يبحثون عن المواقع التى تقدم خدمة (اللعب من خلال الأنترنت مع صديق آخر) ، و مع الأسف يقع طرف فريسة للطرف الآخر ، و أيضاً يقع اللاعبان فريسة للموقع نفسه .
المشكلة هنا هى أن الكثير من الناس يلعبون مع البعض من الناس عن طريق النت لهدف واحد و هو القيام بعملية أختراق على الاعب الآخر . و هذا البرنامج الذى نتحدث عنه الآن يعتبر نوع من أنواع برامج ال (netbus) . و طبعاً له ميزة و عيب : بالنسبة للميزة الموجودة فى هذا البرنامج أنه يمكن المخترق من الدخول الى جهاز الضحية بسهولة جداً ، و عيبه أنه ينزل باتشات كثيرة فى جهاز الضحية . لذلك أحذر من اللعب مع شخص ليس محل ثقة عبر شبكة الأنترنت .

٢- بالنسبة للباتش الأول : لكى تعرف مكانه ؛ فما عليك ألا بالذهاب الى الأمتداد التالى :

(hkey_local_machine\software\microsoft\windows\currentversion\run)

و عندما تضغط على (run)؛ ستجد على اليمين الباتش ، و اسمه أما أن يكون (netbuster) و هو من أخطر الباتشات ، أو (syscopy) .

٣ـ بالنسبة للباتش الثانى : لكى تعرف مكانه ؛ فما عليك ألا بالذهاب الى الأمتداد التالى :

software\microsoft\windows\currentversion\runservices)
(hkey_local_machine\

و عندما تضغط على (runservice) ؛ ستجد على اليمين الباتش ، و اسمه أما أن يكون (rundll) ، أو (rundll32) .

٤ـ بالنسبة للباتش الثالث : لكى تعرف مكانه ؛ فما عليك ألا بالذهاب الى الأمتداد التالى :

(hkey_classes root)

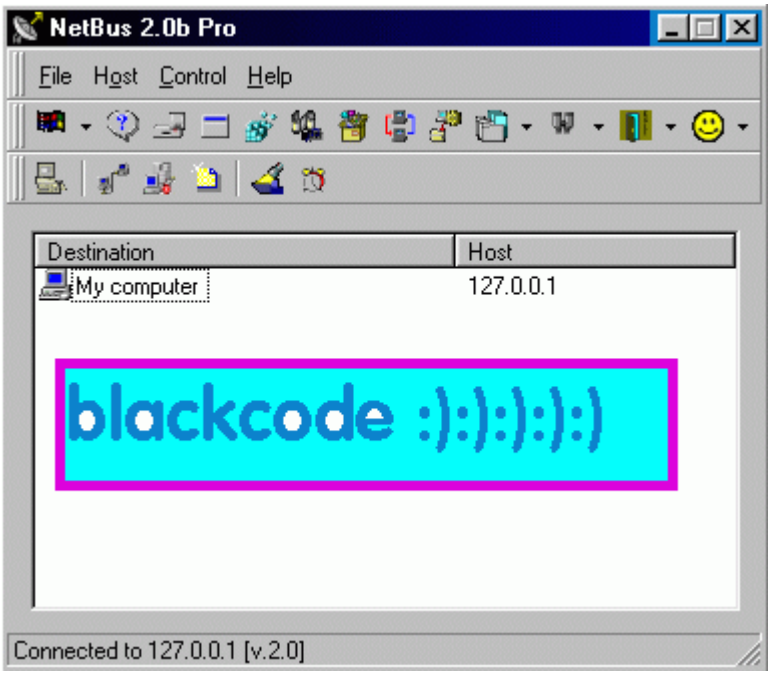
و أبحث فيها على هذا الأسم (\.dl_) .

٥ـ و أختصاراً : عندما تفتح شاشة الريجسترى ، اضغط على الزر الموجود فى لوحة المفاتيح و هو (F3) ، و أكتب فيه أسم كل ملف من هذه الملفات التى سأنكرها الآن ... و عندما تجد أحدهم ؛ فقم بأزالته فوراً ، و الأسماء كما تلى:

keyhook.dll
keyhook.dl_
nbsetup.reg
nb2setup.reg
ntsetup.reg
nt2setup.reg
rundll.dl_
whack.exe

٦ـ و البورتات التى يتسلل منها هذا البرنامج : (١٢٣٦١) و (١٢٣٦٢) .

##برنامج الـ (netbus 2 pro) :-

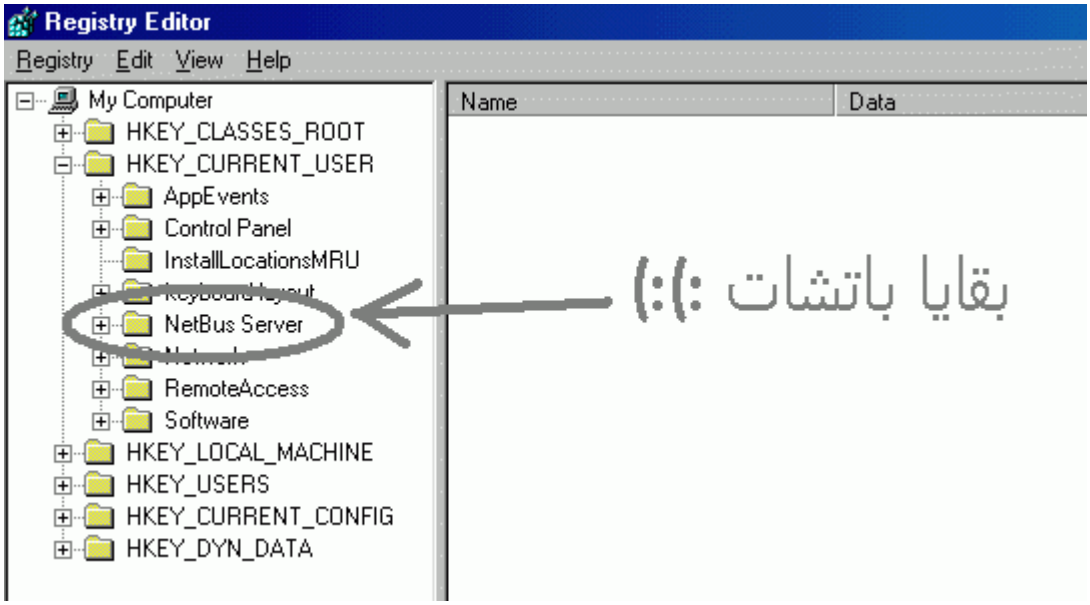


١ـو فى الصورة السابقة ستجدون برنامج الـ (netbus 2 pro) : و هو نوع أحدث من البرنامج الذى سبق شرحه ، و هو يتسلل من البورته (٢٠٠٣٤) .

٢ـو لكى تجد الباتش ، فأمامك طريقين : الطريق الأول ... و هو موضح فى الصورة السابقة ، و الموجود فى الأمتداد :

(hkey_local_machine\software\microsoft\windows\currentversion\runservices)

و عندما تضغط على (runservice) ؛ ستجد على اليمين الباتش ، و اسمه هو (nbsvr.exe) .

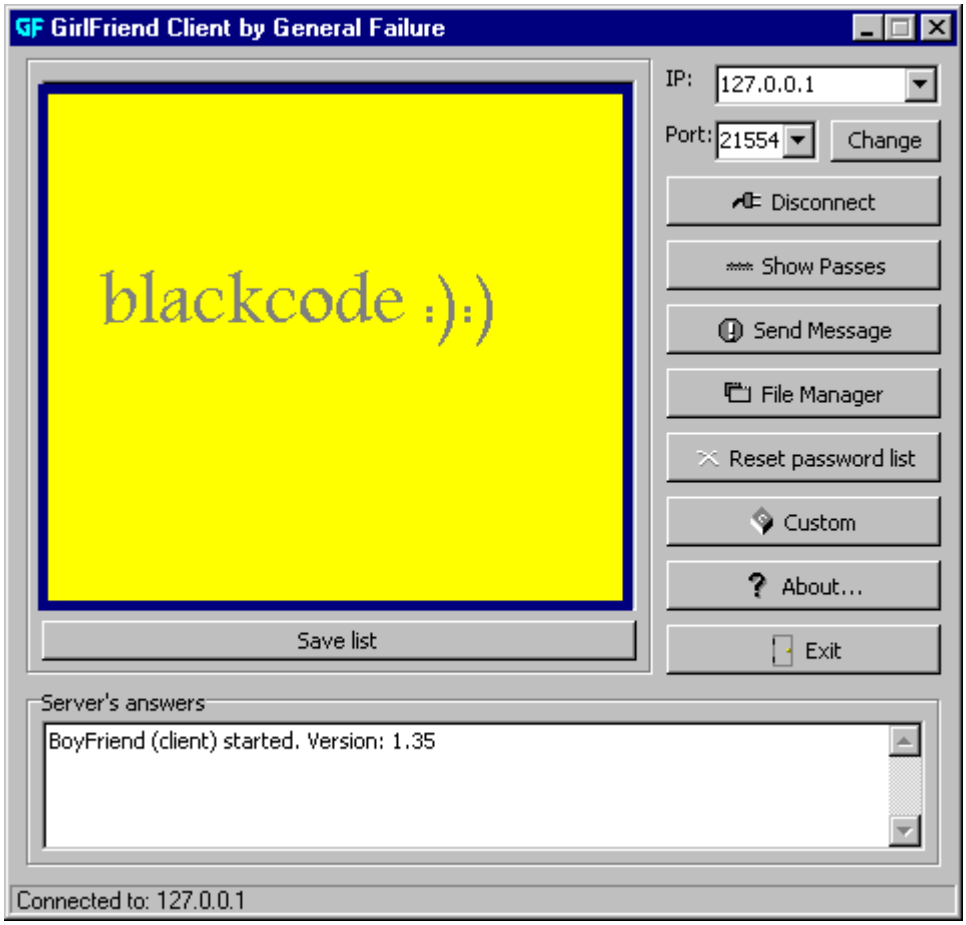


٣-أما الطريقة الثانية لأيجاد الباتش الثانى .... و هو موضح فى الصورة السابقة ، و الموجود فى الأمتداد :

(hkey_current_user)

٤- و البورتات التى يتسلل منها هذا البرنامج : (٢٠٠٣٤) .

##برنامج الـ (girlfriend) :-



١ - بالنسبة لتفسير الصورة السابقة ، فهو كالتالى : لكى تعرف مكانه ؛ فما عليك ألا بالذهاب الى الأمتداد التالى :

(hkey_local_machine\software\microsoft\windows\currentversion\run)

و عندما تضغط على (run)؛ ستجد على اليمين الباتش ، و اسمه هو (windll.exe) ... سواء فى الريجسترى ، أو فى فولدر ال (system) .

٢ - و البورتات التى يتسلل منها هذا البرنامج : (٢١٥٥٤) .

-_____

##برنامج الـــ (sockets de troie) :-

_____

١- و البورتات التى يتسلل منها هذا البرنامج : (٥٠٠٠) و (٥٠٠١) .

٢-و مع الأسف هذا البرنامج عيبه أنه بينزل باتشات كثيرة جداً فى جهاز الضحية .

٣-الطريقة الأولى لأيجاد الباتش : ركزوا معى جيداً .. أذا طلعت لكم رسالة (error) : تقول لك أن الملف (setup32.dll) مفقود من ملف النظام الموجود فى الويندوز ... فما عليك ألا بالذهاب الى الأمتداد التالى :

(hkey_local_machine\software\microsoft\windows\currentversion\runload)

و عندما تضغط على (run)؛ ستجد على اليمين الباتش ، و اسمه هو (mschv32) ... سواء فى الريجسترى ، أو فى فولدر ال (system) .

٤-الطريقة الثانية لأيجاد الباتش : أذا طلعت لكم رسالة (error) : تقول لك أن الملف (isapi32.dll)) مفقود من ملف النظام الموجود فى الويندوز ، و لكن هذه المرة مع الأسف توجد مشكلة ، و هى أن بمجرد دخول هذا الباتش الى جهاز الضحية فأنه ينسخ نفسه ثلاث مرات فى الويندوز ، و لكى تعرف طريقهم ... فما عليك ألا بالذهاب الى الأمتدادات التالية :

c:\windows\rsrcload
c:\windows\system\magadeskdll.exe
c:\windows\system\csmctrl32.exe

٥-و لكن على الرغم من كل هذا ألا أنك ستواجه مشكلة أخرى ، و هى الأخطر بالنسبة لى ... و السبب هو أنك مع الأسف بعد ما تمسح كل هذه الباتشات سواء من الريجسترى أو الدوس ؛ ألا أنك ستواجه عدو أخطر و هو الفيروس الذى يضعه هذا البرنامج فى جهاز الضحية ، و وظيفة هذه الفيروسات هى أنك كل ما تعمل أعادة تشغيل لجهازك فتقوم الفيروسات بتفعيل عمل الباتشات . و لكى تمسحها أمامك ثلاثة طرق .

٦-الطريقة الأولى لأزالة الفيروس ... أذهب الى :

software\microsoft\windows\currentversion\runload)
(hkey_local_machine\

٧-الطريقة الثانية لأزالة الفيروس ... أذهب الى :

software\microsoft\windows\currentversion\runload)
(hkey_local_machine\

٨-الطريقة الثالثة لأزالة الفيروس ... أذهب الى :

software\microsoft\windows\currentversion\runservicesload)
(hkey_local_machine\

##برنامج الـ (master's paradise) :-

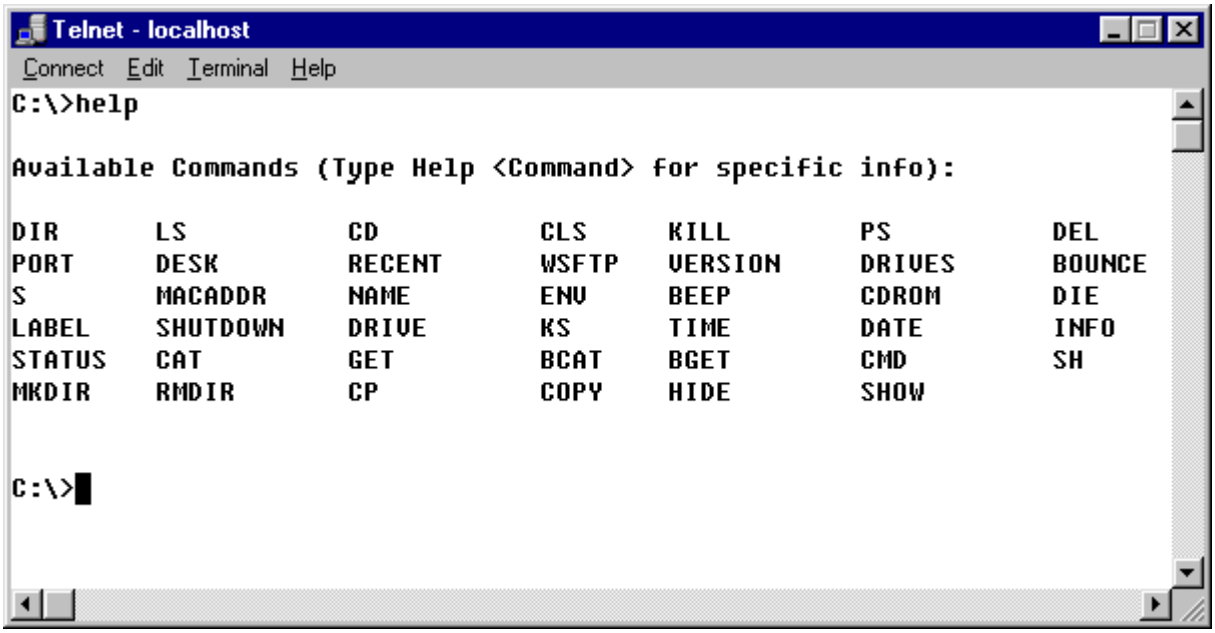
١ـ و البورتات التى يتسلل منها هذا البرنامج : (٣١٢٩) و (٤٠٤٢١) و (٤٠٤٢٢) و (٤٠٤٢٣) و (٤٠٤٢٦) .

٢ـ بالنسبة لتفسير الصورة السابقة ، فهو كالتالى : لكى تعرف مكانه ؛ فما عليك ألا بالذهاب الى الأمتداد التالى :

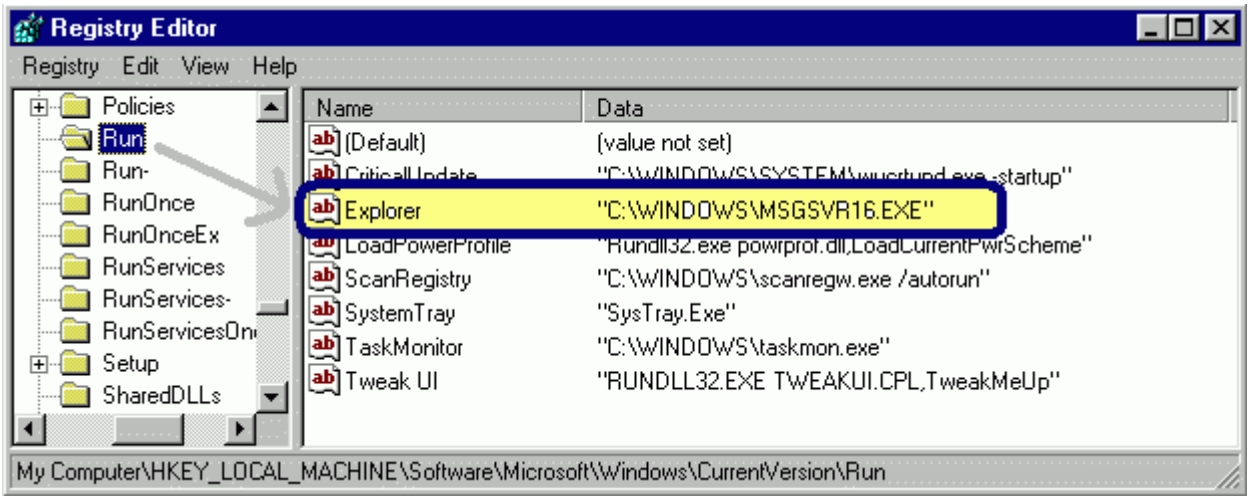
(hkey_local_machine\software\microsoft\windows\currentversion\run)

و عندما تضغط على (run)؛ ستجد على اليمين الباتش ، و اسمه هو (sysedit.exe) ... سواء فى الريجسترى ، أو فى فولدر ال (system) .

##برنامج الـ (acid shivers) :-



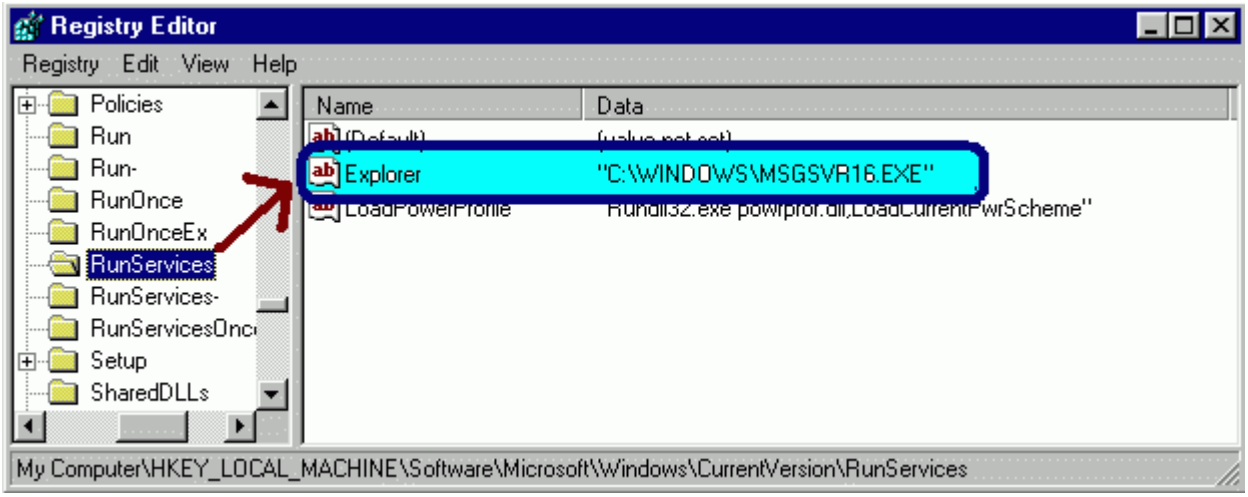
١ـ و البورتات التى يتسلل منها هذا البرنامج : (١٠٥٢٠) .... و هتستعجبوا عندما ترون صورة البرنامج السابقة ؛ حيث أن الأسم لا يدل على صورة البرنامج .



٢ـ بالنسبة لتفسير الصورة السابقة ، فهو كالتالى : لكى تعرف مكانه ؛ فما عليك ألا بالذهاب الى الأمتداد التالى :

(hkey_local_machine\software\microsoft\windows\currentversion\run)

و عندما تضغط على (run)؛ ستجد على اليمين الباتش ، و اسمه هو
(msgsvr16.exe) ... سواء فى الريجسترى ، أو فى فولدر ال (system) .

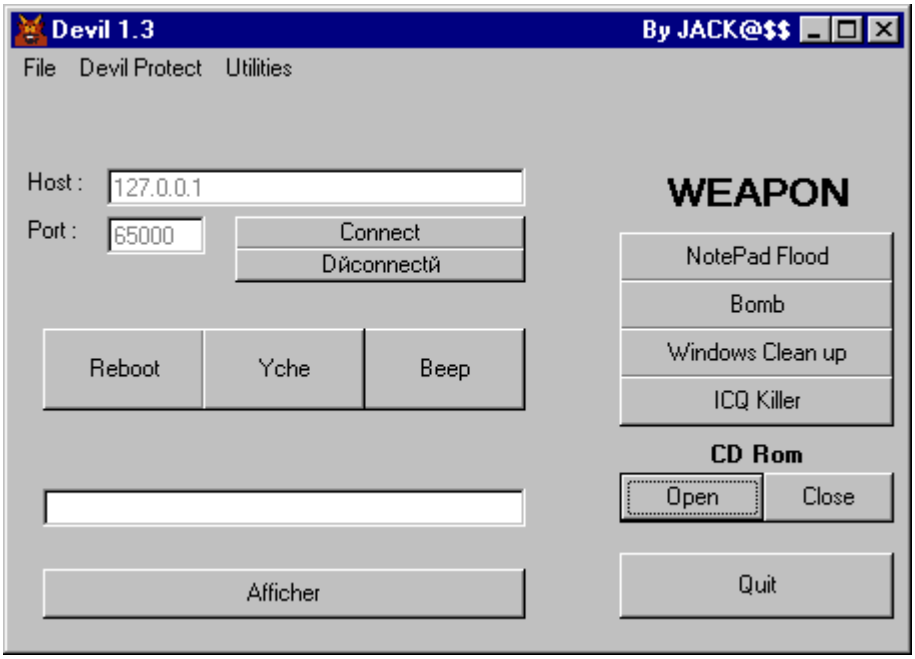


٣-أيضاً توجد طريقة أخرى: بالنسبة لتفسير الصورة السابقة ، فهو كالتالى : لكى
تعرف مكانه ؛ فما عليك ألا بالذهاب الى الأمتداد التالى :

software\microsoft\windows\currentversion\runservices)
(hkey_local_machine\

و عندما تضغط على (run)؛ ستجد على اليمين الباتش ، و اسمه هو
(msgsvr16.exe) ... سواء فى الريجسترى ، أو فى فولدر ال (system) .

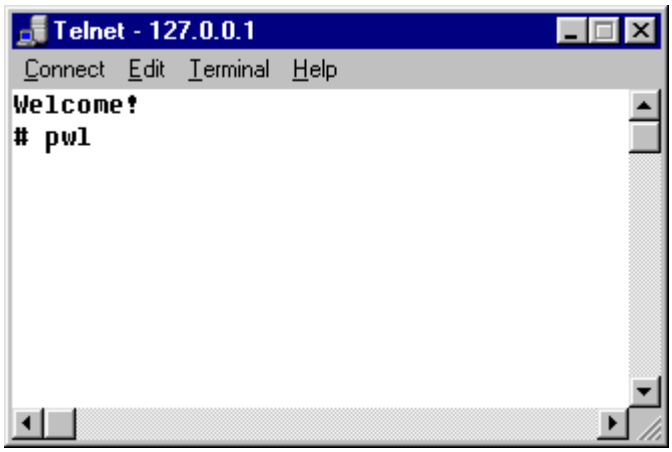
##برنامج الـ (devil) :-



١ـ و البورتات التى يتسلل منها هذا البرنامج : (٦٥٠٠٠) .

٢ـو هذا البرنامج بالذات فهو لا يمثل أية خطورة ... و لكى تمسح الباتش الخاص به ؛ فستجده فى ملف ال (system) الموجود فى الويندوز ، و اسمه هو (icqflood.exe) .

##برنامج الـ (big gluck) :-



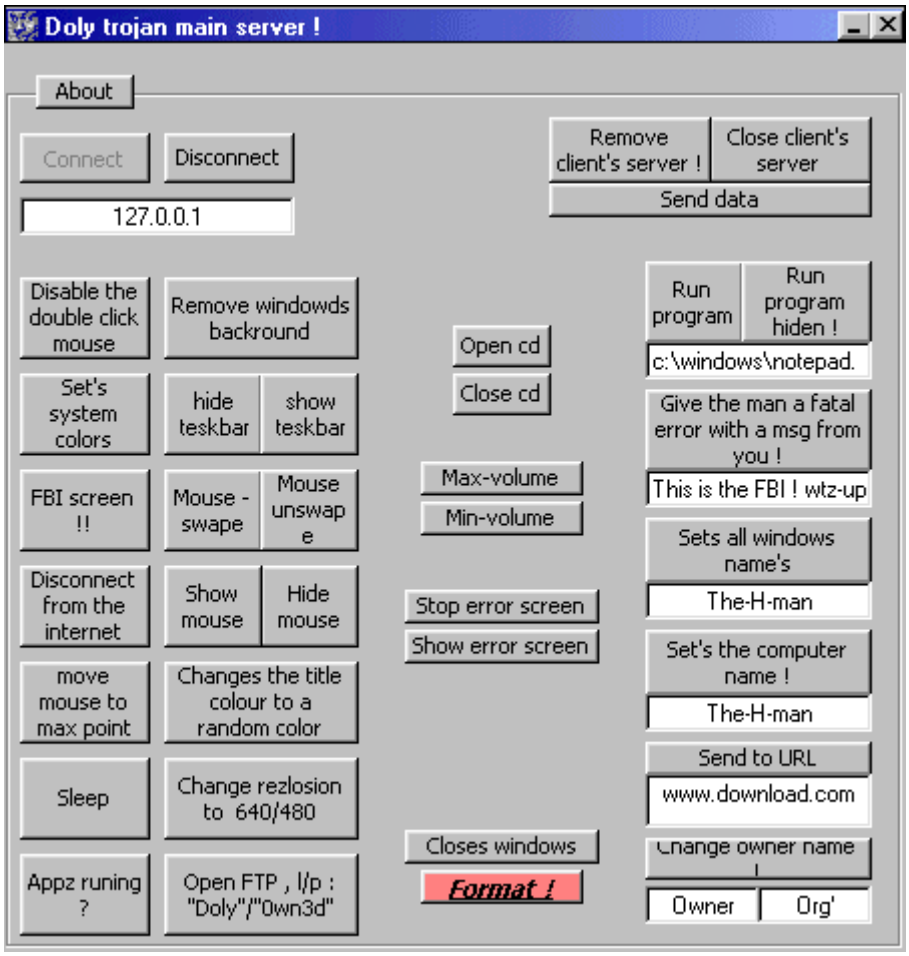
١ـ و البورتات التى يتسلل منها هذا البرنامج : (٣٤٣٢٤) . و هذا البرنامج مخصص فقط لسرقة كلمات السر الموجودة فى جهاز الضحية .

٢ـو لكى تجد الباتش ، فأمامك طريقين : الطريق الأول ... و هو موضح فى الصورة السابقة ، و الموجود فى الأمتداد :

(hkey_local_machine\software\microsoft\windows\currentversion\runservices)

و عندما تضغط على (runservice) ؛ ستجد على اليمين الباتش ، و اسمه هو (bg10.exe) .

##برنامج الـ (doly Trojan) :-



١ـ و البورتات التى يتسلل منها هذا البرنامج : (١٠١١) .

٢ـ بالنسبة لتفسير الصورة السابقة ، فهو كالتالى : لكى تعرف مكانه ؛ فما عليك ألا بالذهاب الى الأمتداد التالى :

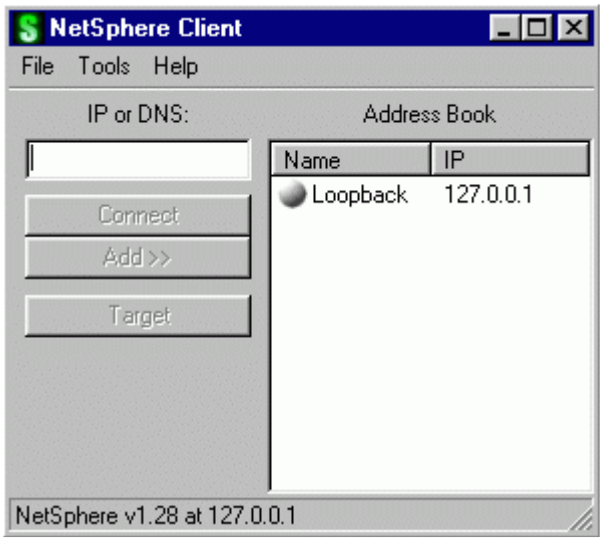
(hkey_local_machine\software\microsoft\windows\currentversion\run)

و عندما تضغط على (run)؛ ستجد على اليمين الباتش ، و اسمه هو (tesk.exe) .

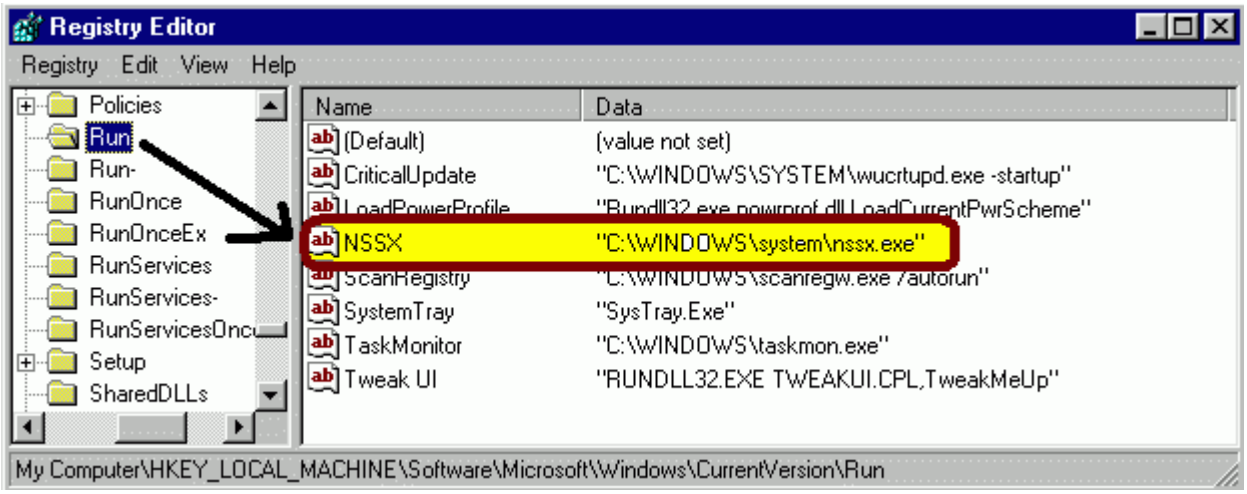
٣ـأو من الممكن أن تجده فى هذا الأمتداد ، و بنفس الأسم :

(hkey_local_user\software\microsoft\windows\currentversion\run)

##برنامج الـ (netsphere) :-



١ـ و البورتات التى يتسلل منها هذا البرنامج : (٣٠١٠١) و (٣٠١٠٢) و (٣٠١٠٣) .... و مش هقدر أقول لكم أكثر من (ربنا يكفيكم شر هذا البرنامج) . هو صحيح البرنامج من شكله تقول عليه ما لوش لازمة ؛ لكن فعلاً لو جرب أى شخص فيك هذا البرنامج فأنا أقول لك أنك مش هتعرف تخلص من شره .

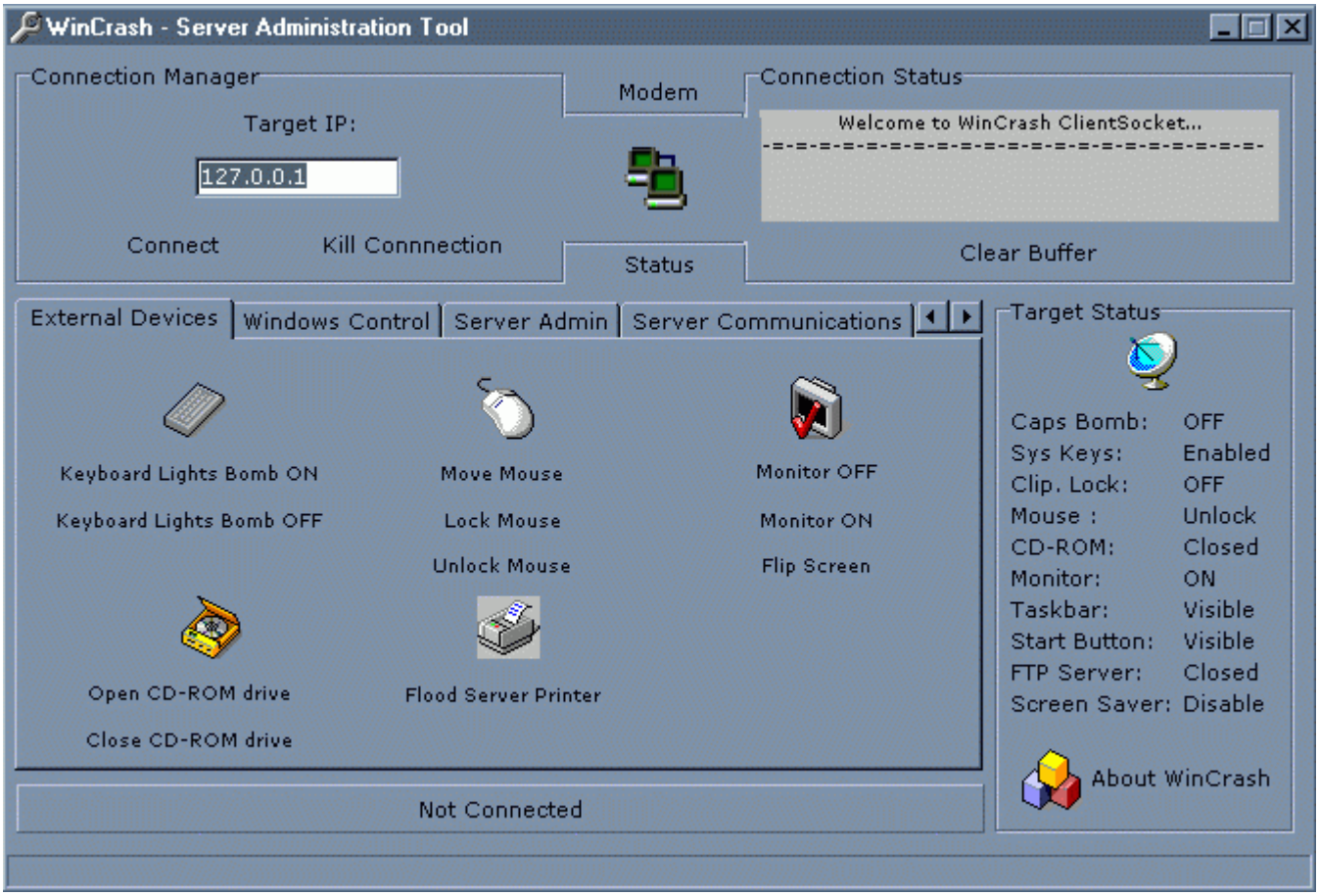


٢ـ بالنسبة لتفسير الصورة السابقة ، فهو كالتالى : لكى تعرف مكانه ؛ فما عليك ألا بالذهاب الى الأمتداد التالى :

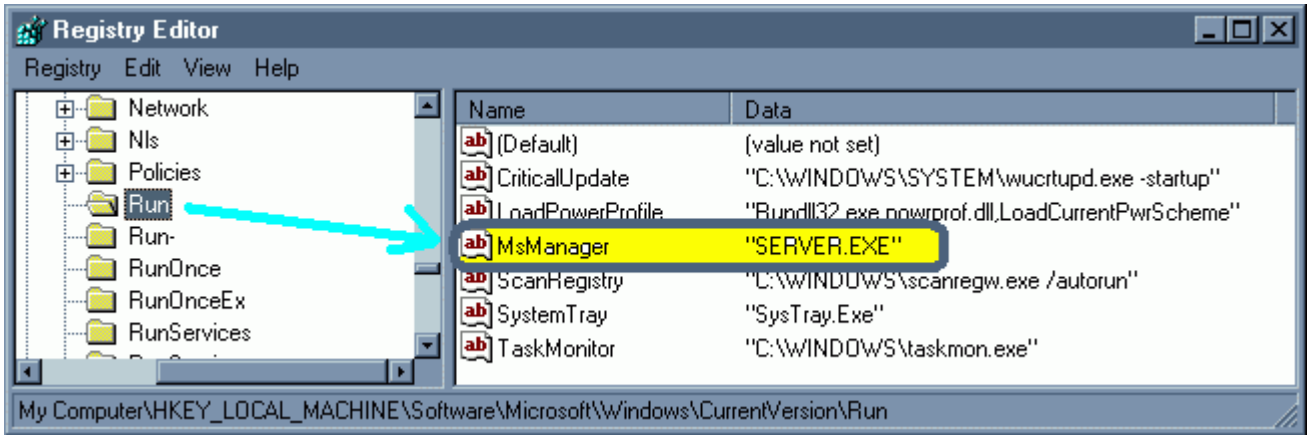
(hkey_local_machine\software\microsoft\windows\currentversion\run)

و عندما تضغط على (run)؛ ستجد على اليمين الباتش ، و اسمه هو (nssx) .

##برنامج الـ (wincrash) :-



١ـ و البورتات التى يتسلل منها هذا البرنامج : (٥٧٤٢) .

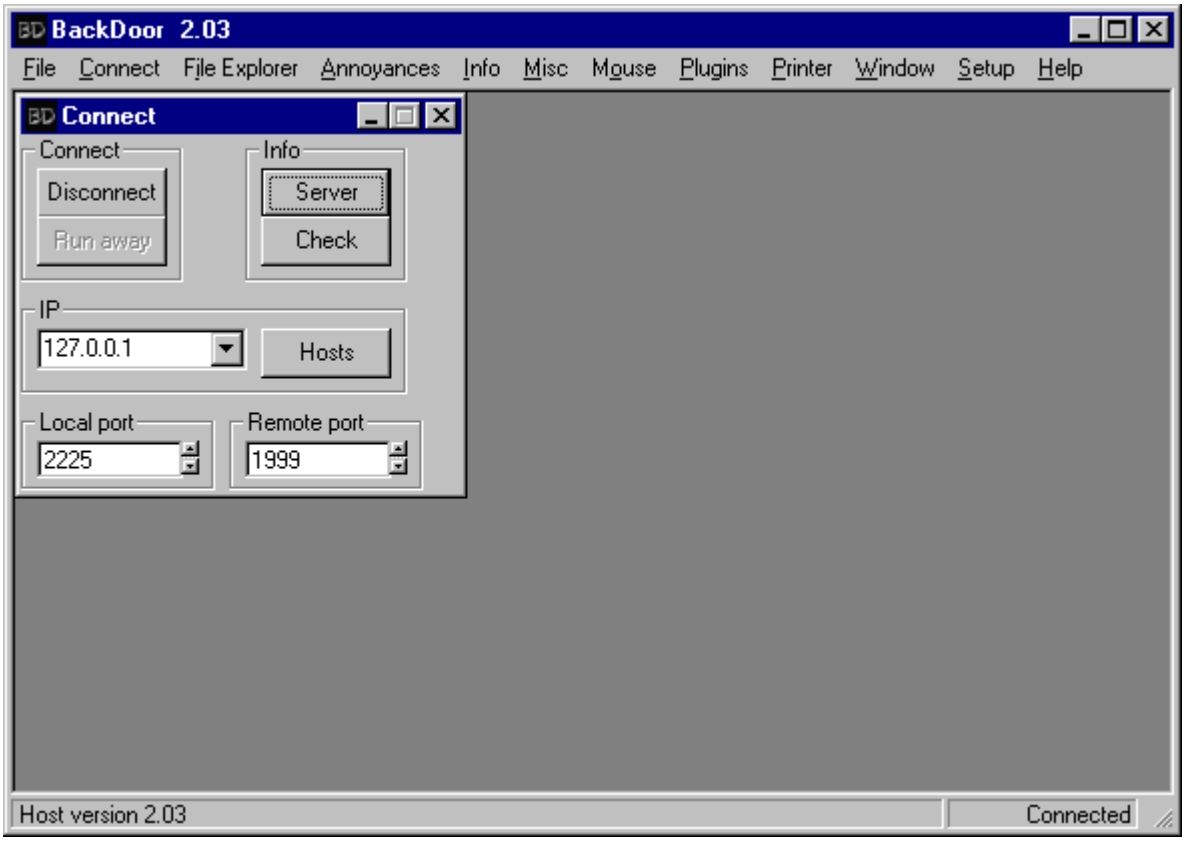


٢ـ بالنسبة لتفسير الصورة السابقة ، فهو كالتالى : لكى تعرف مكانه ؛ فما عليك ألا بالذهاب الى الأمتداد التالى :

software\microsoft\windows\currentversion\run)
(hkey_local_machine\

و عندما تضغط على (run)؛ ستجد على اليمين الباتش ، و اسمه هو (msmanager) .

##برنامج الـ (back door) :-



١- و البورتات التى يتسلل منها هذا البرنامج : (١٩٩٩) . و عيب هذا البرنامج أنه خبيث ، و الخباثة فى حد ذاتها غالباً ما تكزن أداة قوية تمكن المخترق من التحكم بجهاز الضحية .

٢- بالنسبة لتفسير الصورة السابقة ، فهو كالتالى : لكى تعرف مكانه ؛ فما عليك ألا بالذهاب الى الأمتداد التالى :

software\microsoft\windows\currentversion\run)
(hkey_local_machine\

و عندما تضغط على (run)؛ ستجد على اليمين الباتش ، و اسمه هو (icqnuke.exe) .

##برنامج الـ (blade runner) :-

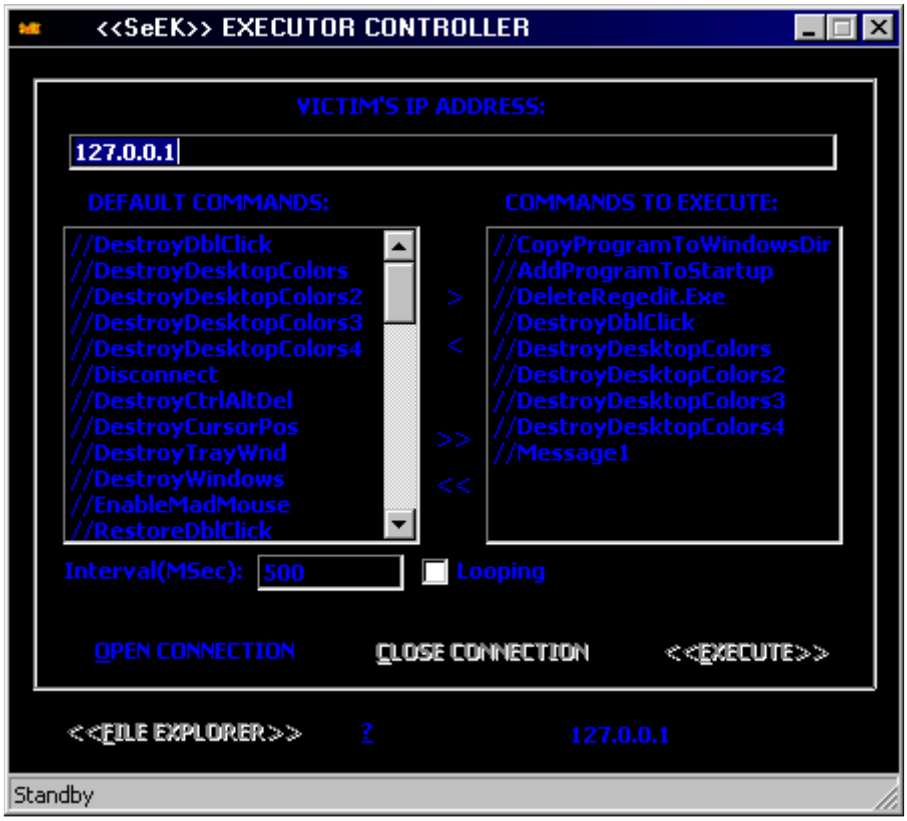
١- و البورتات التى يتسلل منها هذا البرنامج : (٥٤٠٠) و (٥٤٠١) و (٥٤٠٢) و (٢١) . و هذا البرنامج لى قصة طويلة معه ، و لكن كل ما أقوله لكم هو أن هذا البرنامج يعتبر برنامجى المفضل من بين برامج الأختراق .

٢-بالنسبة لتفسير الصورة السابقة ، فهو كالتالى : لكى تعرف مكانه ؛ فما عليك ألا بالذهاب الى الأمتداد التالى :

software\microsoft\windows\currentversion\run)
(hkey_local_machine\

و عندما تضغط على (run)؛ ستجد على اليمين الباتش ، و اسمه هو
. (server.exe)

##برنامج الـ (executer) :-



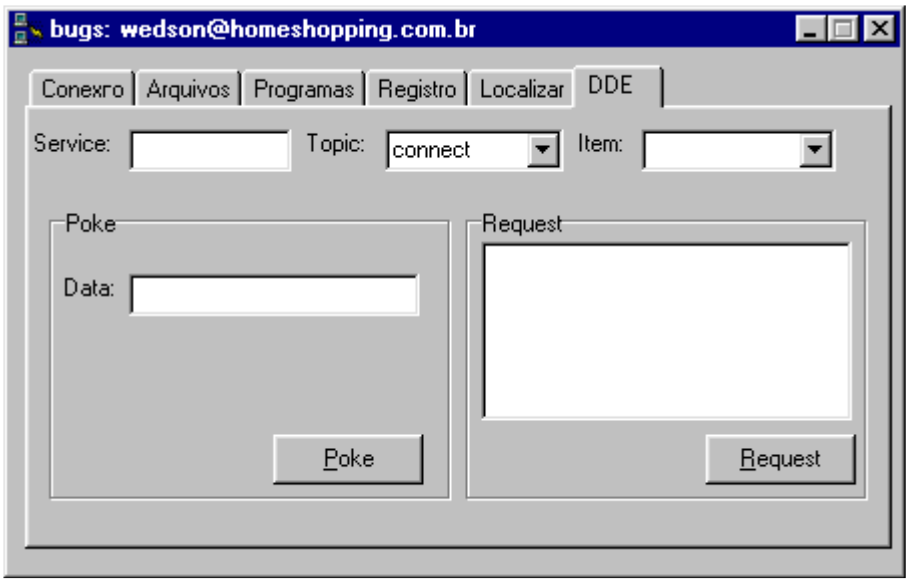
١ - و البورتات التى يتسلل منها هذا البرنامج : (٨٠) .

٢ - بالنسبة لتفسير الصورة السابقة ، فهو كالتالى : لكى تعرف مكانه ؛ فما عليك ألا بالذهاب الى الأمتداد التالى :

software\microsoft\windows\currentversion\run)
(hkey_local_machine\

و عندما تضغط على (run)؛ ستجد على اليمين الباتش ، و اسمه هو (exec.exe)
.

##برنامج الـ (bugs) :-



١ـ و البورتات التى يتسلل منها هذا البرنامج : (٢١١٥) .

٢ـ بالنسبة لتفسير الصورة السابقة ، فهو كالتالى : لكى تعرف مكانه ؛ فما عليك ألا بالذهاب الى الأمتداد التالى :

software\microsoft\windows\currentversion\run)
(hkey_local_machine\

و عندما تضغط على (run)؛ ستجد على اليمين الباتش ، و اسمه هو
. (bugs.exe)