

١- توجد ملحوظة صغيرة و هامة : و هي أن ( الباتش ) له اسم في ( الريجستري ) ، و اسم آخر مختلف عن الثاني في فولدر ال (system) . في البداية ... هذا البرنامج يمكنك عمل اختراق 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) .

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

٣- و 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) .

٤- و أنا هقول لكم حته 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 شيء ما من هذا السيرفر .. مركزيين معي ؟ و لنفسرها معاً من يكون السيرفر ، و من يكون الكلاينت ، و هي شيء بديهي 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 لأخترق هذا الجهاز ... المهم و هو غرضي من هذا الموضوع و هو أنك لكي تتسلل الى جهاز الضحية فما هو مطلوب أولاً ألا أن يكون جهاز الضحية به أحد البورتات المذكورة سابقاً مفتوحة ، و ذلك لكي 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 لكي يجمع المعلومات التى يحتاجها لأخترق جهاز الضحية ، و هذا هو موضوعي اليوم عن ( كيفية البحث عن الباتشات الموجودة فى جهازك أن وجدت !!! ) ، و ليس ( كيفية الأخترق !!! ) ... و بهذا تكونون قد فهمتم الى حد ما المفهوم العام لهذه العملية .

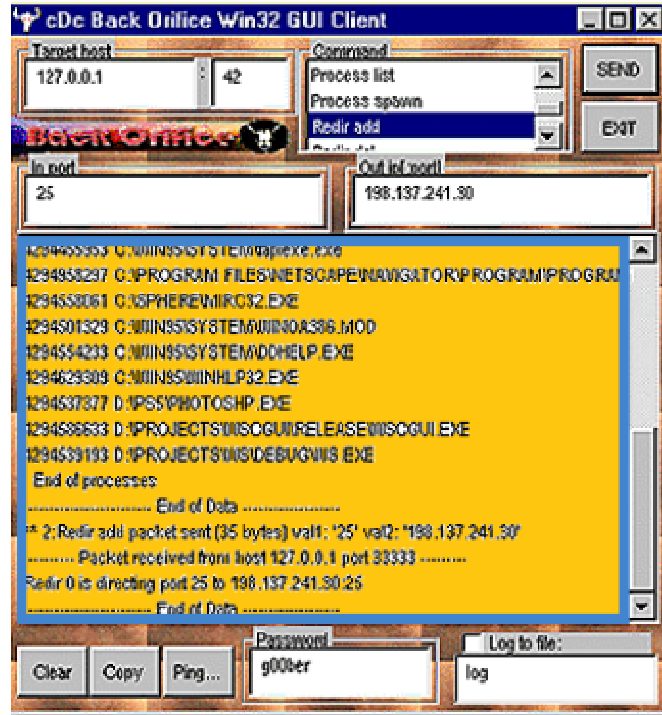
٥- لنفرض أنك وجدت عندك أحد الباتشات الخاصة بهذا البرنامج ، و تريد أزالته من جهازك ... فكيف ستكون الخطوات المتبعة لهذه العملية ؟ و هى كالتالى ....

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

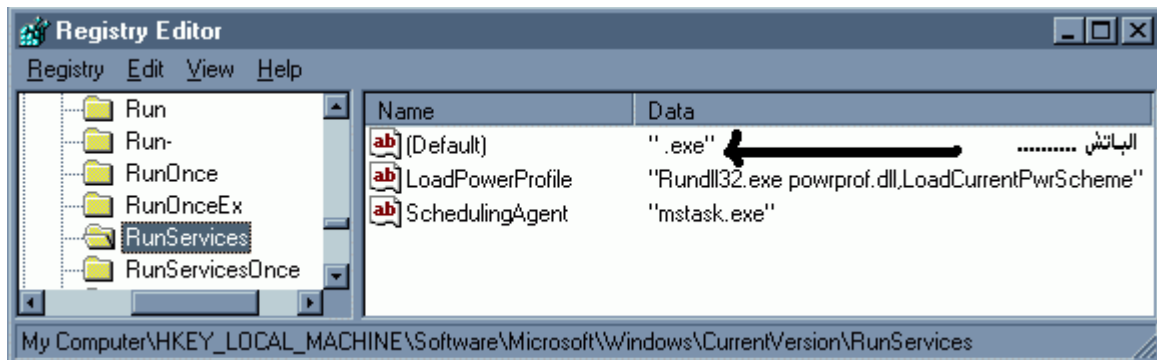
```
software\microsoft\windows\currentversion\run)
(hkey_local_machine\
```

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 إلا مكان هذا الباتش فى الويندوز ، و لكي تمسحه من جهازك فما عليك إلا 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 إذا 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 ) :-



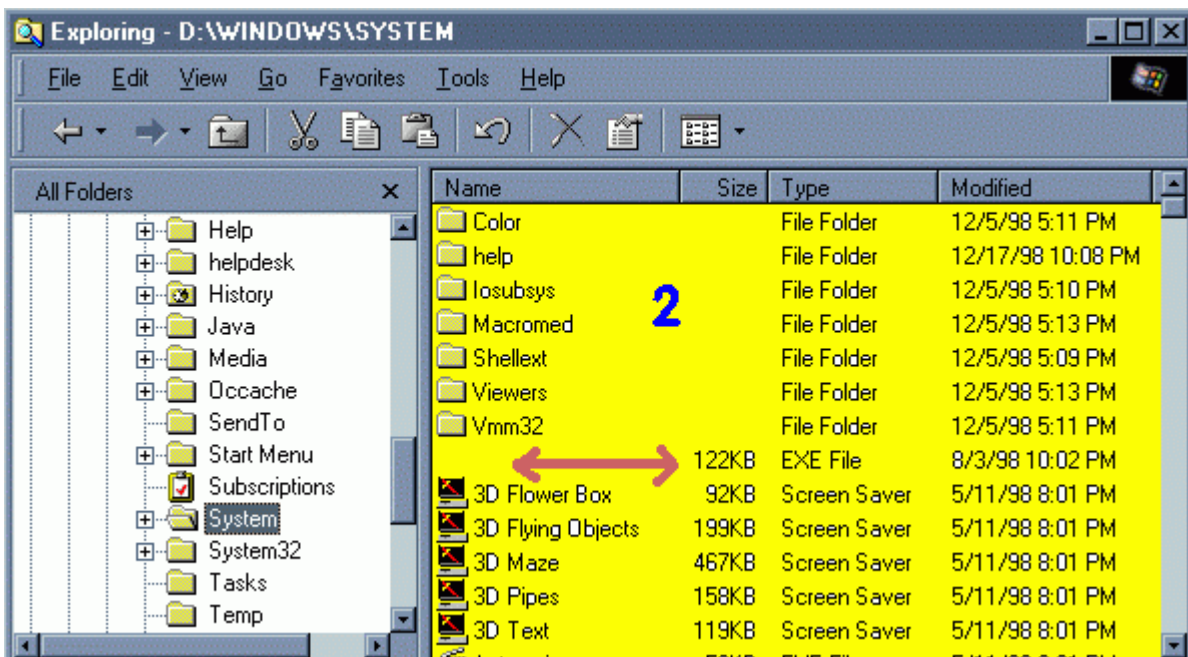
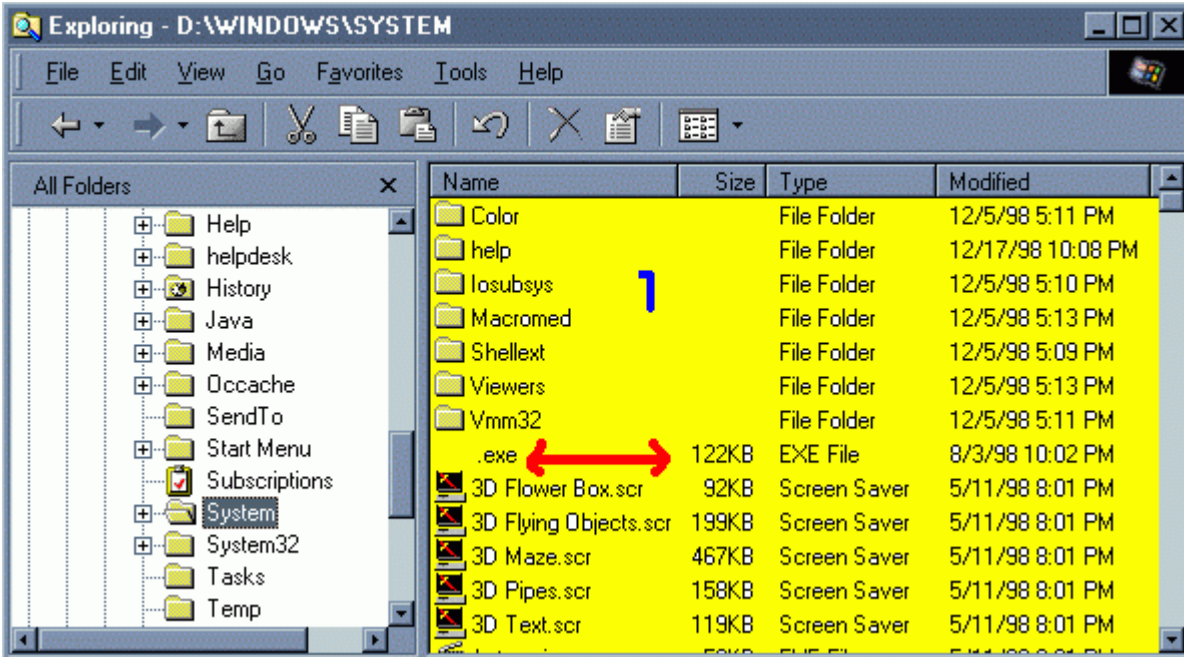
١- و الصورة السابقة طبعاً هي صورة للبرنامج ، و هذا البرنامج يعتبر أقوى و أخطر برنامج على مستوى برامج الأختراق . و هو قوى جداً فى التعامل مع الضحية و مفعوله سريع جداً .

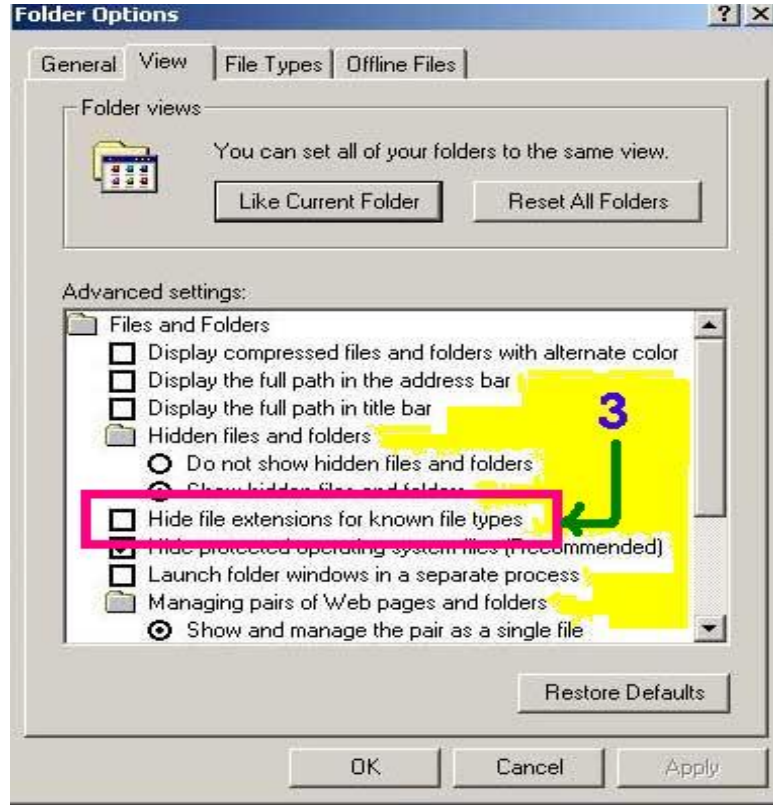


٢- بالنسبة لتفسير الصورة السابقة ، فهو كالتالى : غالباً و مع الأسف ما يكون ملف الباتش ليس له اسم أو مخفى ، و لكى تعرف مكانه ؛ فما عليك إلا بالذهاب الى الأمتداد التالى ، و كما هو موضح فى الصورة السابقة ...

software\microsoft\windows\currentversion\runtimeservices)  
( hkey\_local\_machine\

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





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

أرأيتم كم مرة كتبت العبارة ( هامة جداً ) ، و السبب هو أن (٩٩%) من مستخدمي الكمبيوتر لا يعلمون هذه الملحوظة و أهميتها ، و هي 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 في الصورة السابقة التي ستجد فيها الرقم (٣) مكتوب ، و عندما تفتحها ستجدني محدداً جملة (بمربع أحمر) ، و هي ما سأشرح أهميتها العظيمة الآن : و هذه العبارة يقصد بها ( أنها تسألك هل تريد أن تضع مع اسم كل ملف في الويندوز الأمتداد الخاص به ؟؟ بمعنى أنك لو عندك مثلاً صورة اسمها (١) و هي من النوع (gif) ؛ فأذا أزلت ( علامة الصح ) الموجودة بجانب العبارة الموجودة في الصورة فأنتك بهذا تقول للويندوز أجعل الصورة التي اسمها (١) و هي من النوع (gif) تكتب كالتالي (1.gif) : بأختصار ستجد كل ملفات الويندوز سواء صور أو أفلام أو كليببات أو غيره مكتوب معها ال (extension) الذي ينتمي لها ... و هدفي من هذا الموضوع هو أنك لو جعلت كل ملف مكتوب معه أمتداده فأنتك بهذا ستظهر ( كل الأعيب المخترقيين ) ، و الألاعيب التي أعنيها هي أن برنامج مثل ال ( back orifice) هذا إذا نزل لك باتش في جهازك من خلال هذا البرنامج ، فأمامك حل واحد لكى تتعرف على هذا الباتش و هو كما قلت لكم هو ( أنك تزيل علامة الصح )





١- 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  
(systemdll32) ، و ستجده طبعاً فى فولدر الويندوز و لكن باسم  
(systempatch.exe) . و طبعاً لكى تزيلون الباتش فأنتم عرفتموا الطريقة المتبعة  
لذلك .

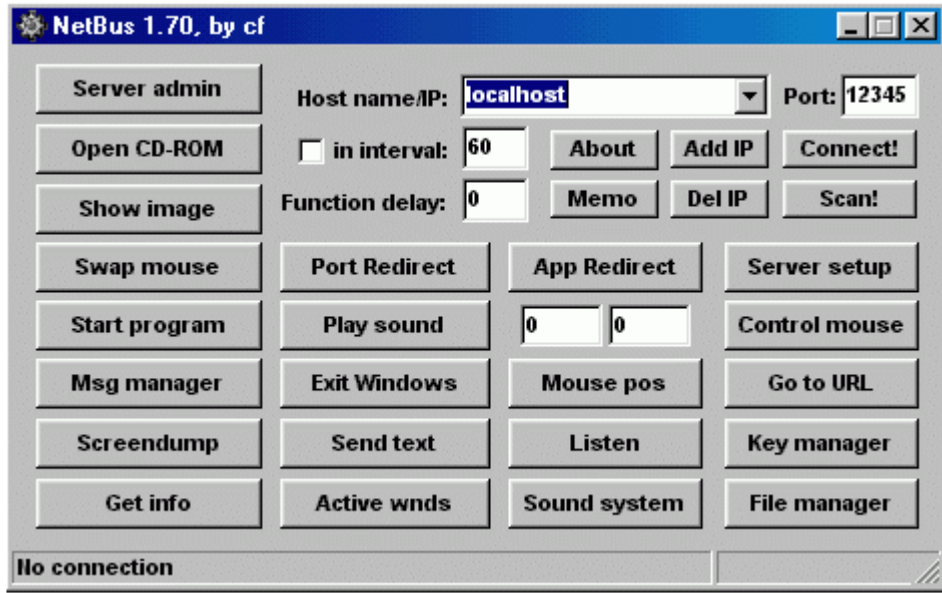
٢- و البورتات التى يتسلل منها هذا البرنامج : (٢١٤٠) و (٣١٥٠) ، و هى من  
النوع (udp) .

---

##برنامج الـ (netbus) :-

---





١- 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  
(patch.exe) ... سواء فى الريجستري ، أو فى فولدر ال (system) .

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

٢- بالنسبة للباتش الأول : لكي تعرف مكانه ؛ فما عليك إلا بالذهاب الى الأمتداد التالي :

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

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

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

software\microsoft\windows\currentversion\runtimeservices)  
( hkey\_local\_machine\

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

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

(hkey\_classes root)

و أبحث فيها على هذا الأسم (\\_dl) .

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

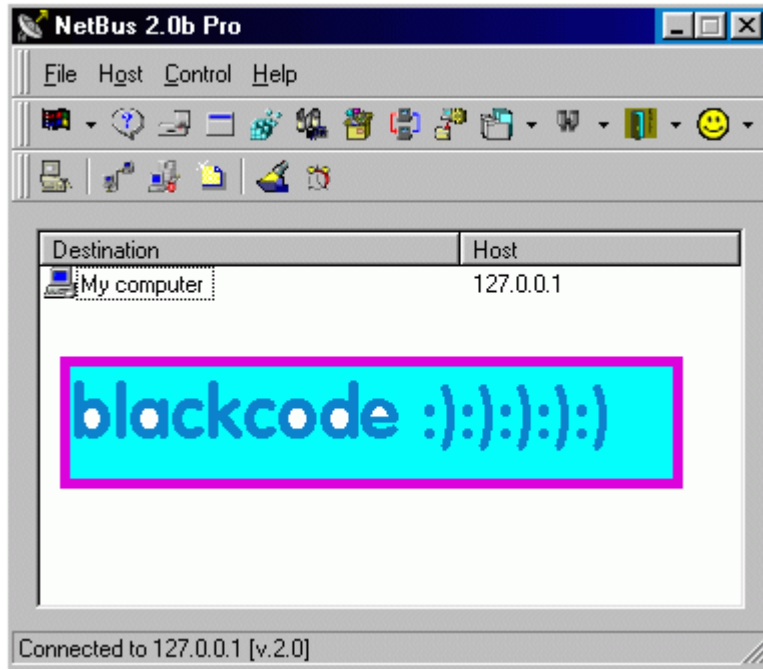
keyhook.dll  
keyhook.dl\_  
nbsetup.reg  
nb2setup.reg  
ntsetup.reg  
nt2setup.reg  
rundll.dl\_  
whack.exe

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

---

###برنامج الـ (netbus 2 pro) :-

---

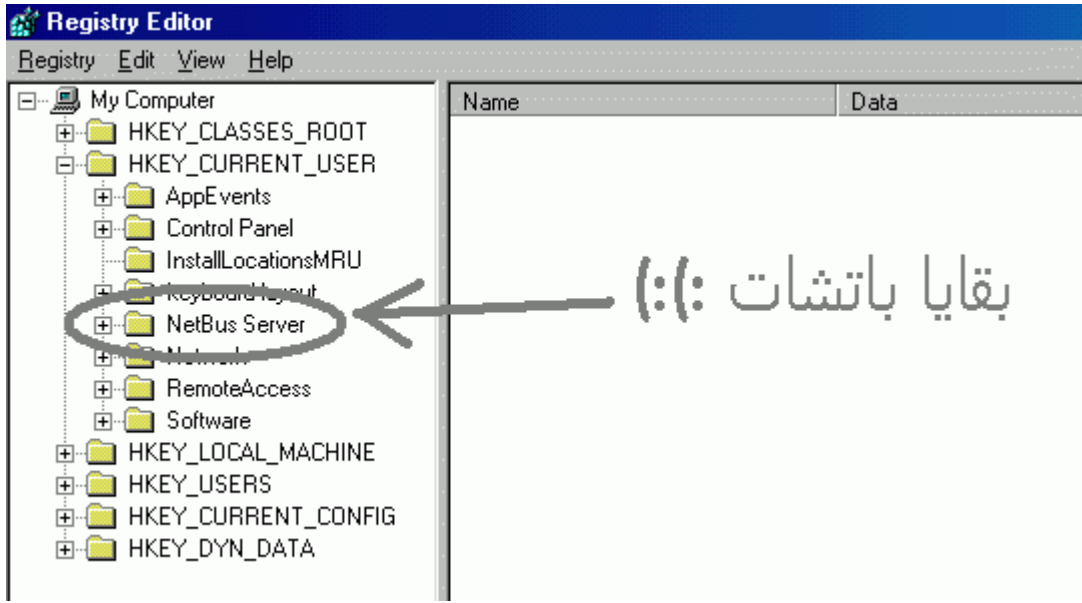


١- وفي الصورة السابقة ستجدون برنامج الـ (netbus 2 pro) : و هو نوع أحدث من البرنامج الذي سبق شرحه ، و هو يتسلل من البورته (٢٠٠٣٤) .

٢- ولكي تجد الباتش ، فأمامك طريقين : الطريق الأول ... و هو موضح في الصورة السابقة ، و الموجود في الأمتداد :

software\microsoft\windows\currentversion\runtimeservices)  
( hkey\_local\_machine\

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 :

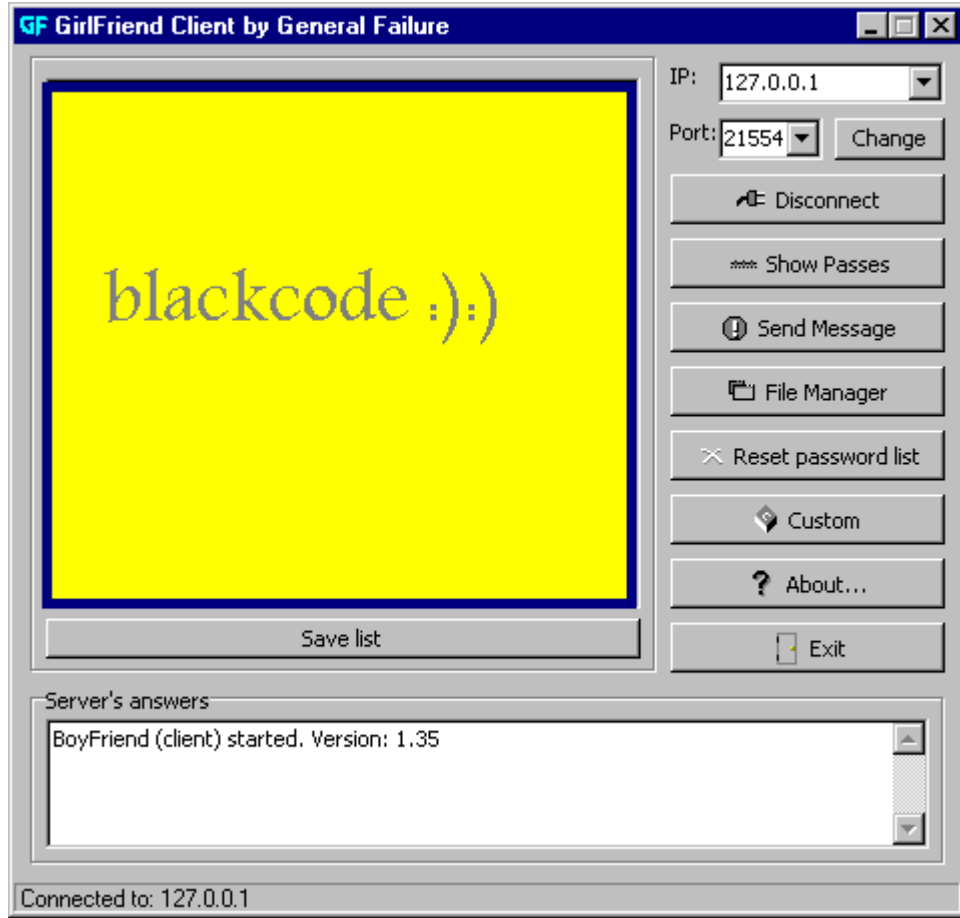
(hkey\_current\_user)

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

---

##برنامج الـ (girlfriend) :-

---



١- بالنسبة لتفسير الصورة السابقة ، فهو كالتالى : لكي 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  
(windll.exe) ... سواء فى الريجستري ، أو فى فولدر ال (system) .

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

---

###برنامج الـ (sockets de troie) :-

---



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

٢- و مع الأسف هذا البرنامج عيبه أنه يينزل باتشات كثيرة جداً في جهاز الضحية .

٣- الطريقة الأولى لأيجاد الباتش : ركزوا معي جيداً .. إذا طلعت لكم رسالة (error) : تقول لك أن الملف (setup32.dll) مفقود من ملف النظام الموجود في الويندوز ... فما عليك إلا بالذهاب الى الأمتداد التالي :

software\microsoft\windows\currentversion\runload)  
( hkey\_local\_machine\

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

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

c:\windows\rsrcload  
c:\windows\system\magadesk.dll.exe  
c:\windows\system\csmctrl32.exe

٥- و لكن على الرغم من كل هذا ألا أنك ستواجه مشكلة أخرى ، و هي الأخطر بالنسبة لى ... و السبب هو أنك مع الأسف بعد ما تمسح كل هذه الباتشات سواء من الريجستري أو الدوس ؛ ألا أنك ستواجه عدو أخطر و هو الفيروس الذى يضعه هذا البرنامج فى جهاز الضحية ، و وظيفة هذه الفيروسات هي أنك كل ما تعمل إعادة 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) :-

---



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

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

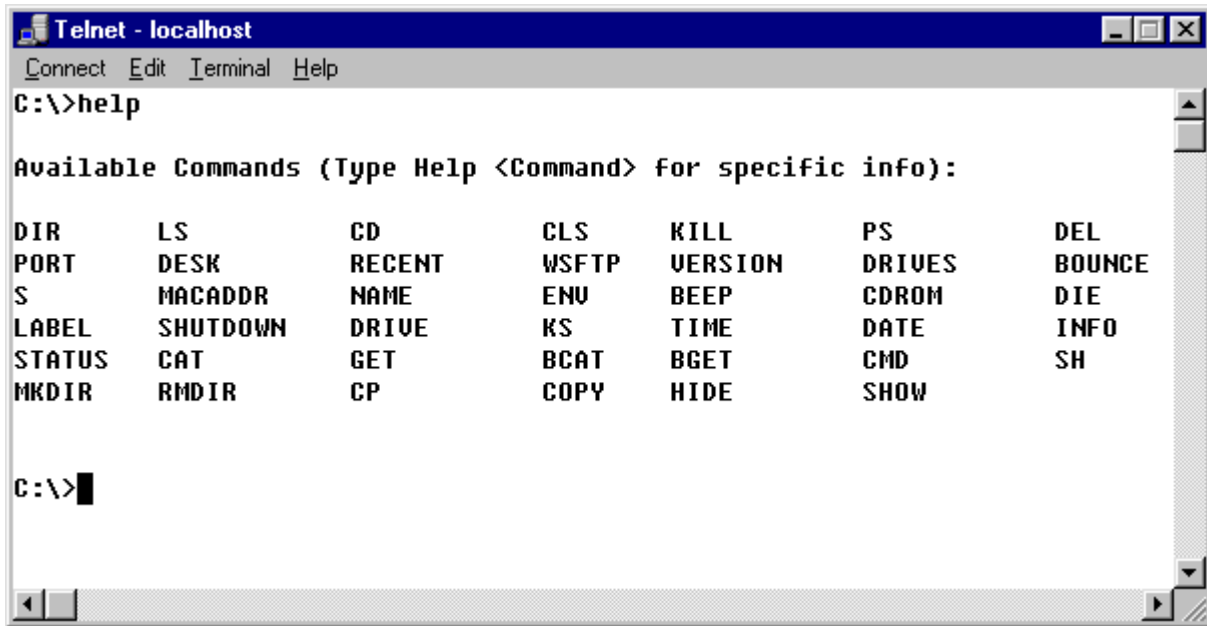
`software\microsoft\windows\currentversion\run`  
( `hkey_local_machine\`

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

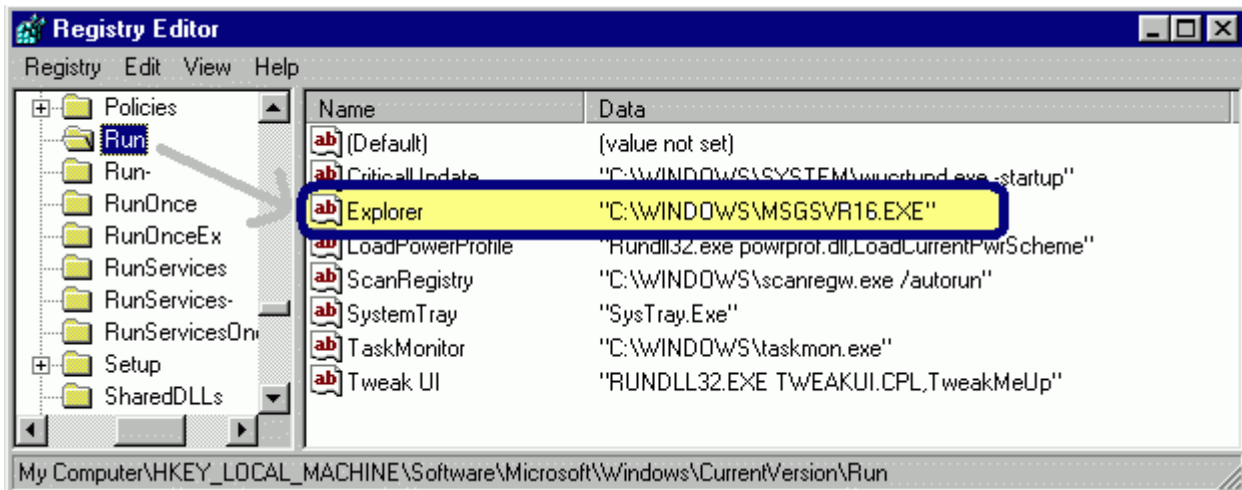
---

###برنامج الـ (acid shivers) :-

---



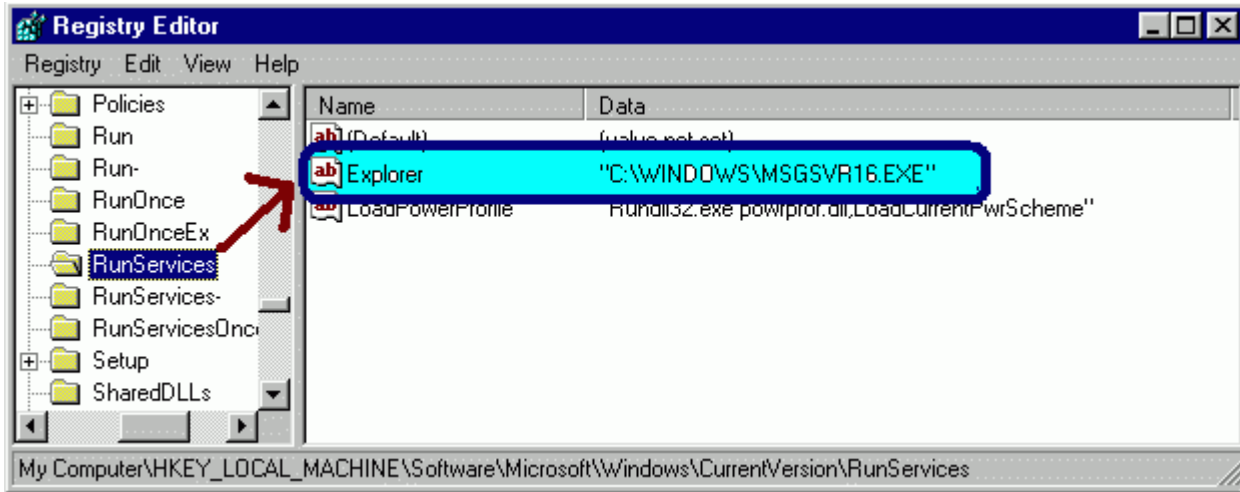
١- و البورتات التي يتسلل منها هذا البرنامج : (١٠٥٢٠) .... و هتستجبوا عندما ترون صورة البرنامج السابقة ؛ حيث أن الأسم لا يدل على صورة البرنامج .



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

software\microsoft\windows\currentversion\run)  
( hkey\_local\_machine\

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



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

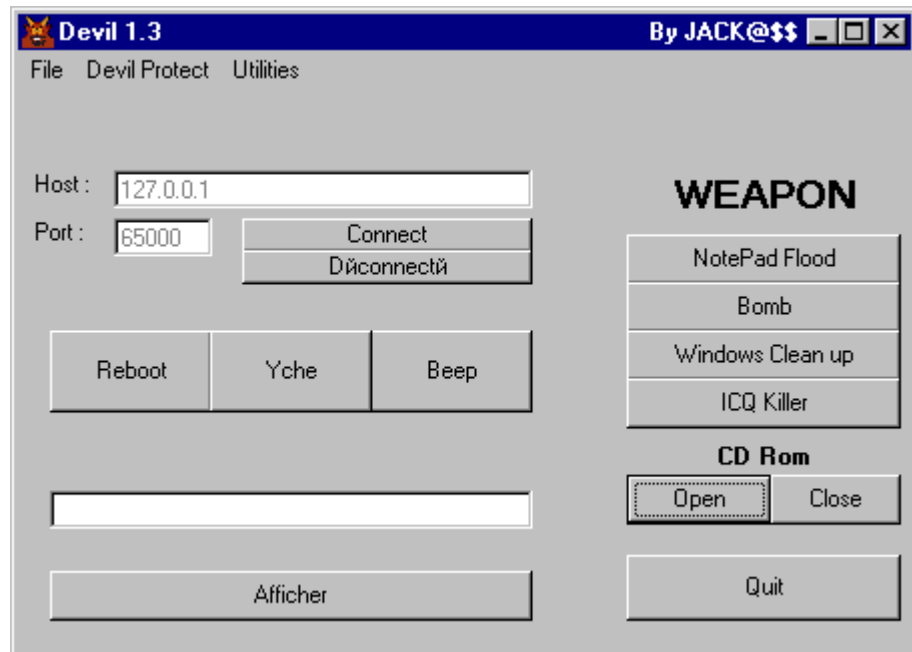
software\microsoft\windows\currentversion\runservices)  
( hkey\_local\_machine\

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

---

##برنامج ال- (devil) :-

---



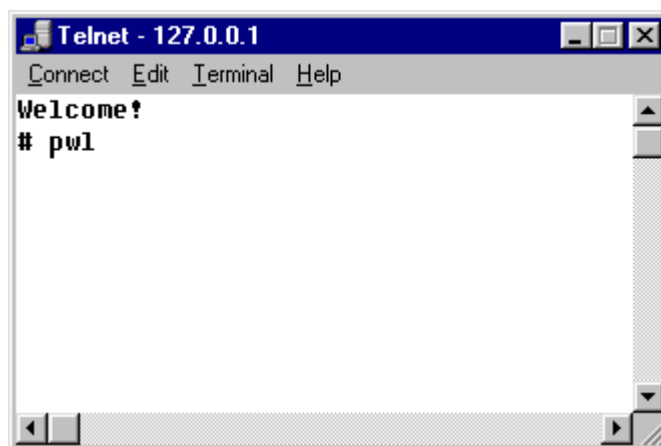
١- و البورتات التي يتسلل منها هذا البرنامج : (٦٥٠٠٠) .

٢- و هذا البرنامج بالذات فهو لا يمثل أية خطورة ... و لكي تسمح الباتش الخاص به ؛ فستجده في ملف ال (system) الموجود في الويندوز ، و اسمه هو . (icqflood.exe)

---

###برنامج الـ (big gluck) :-

---



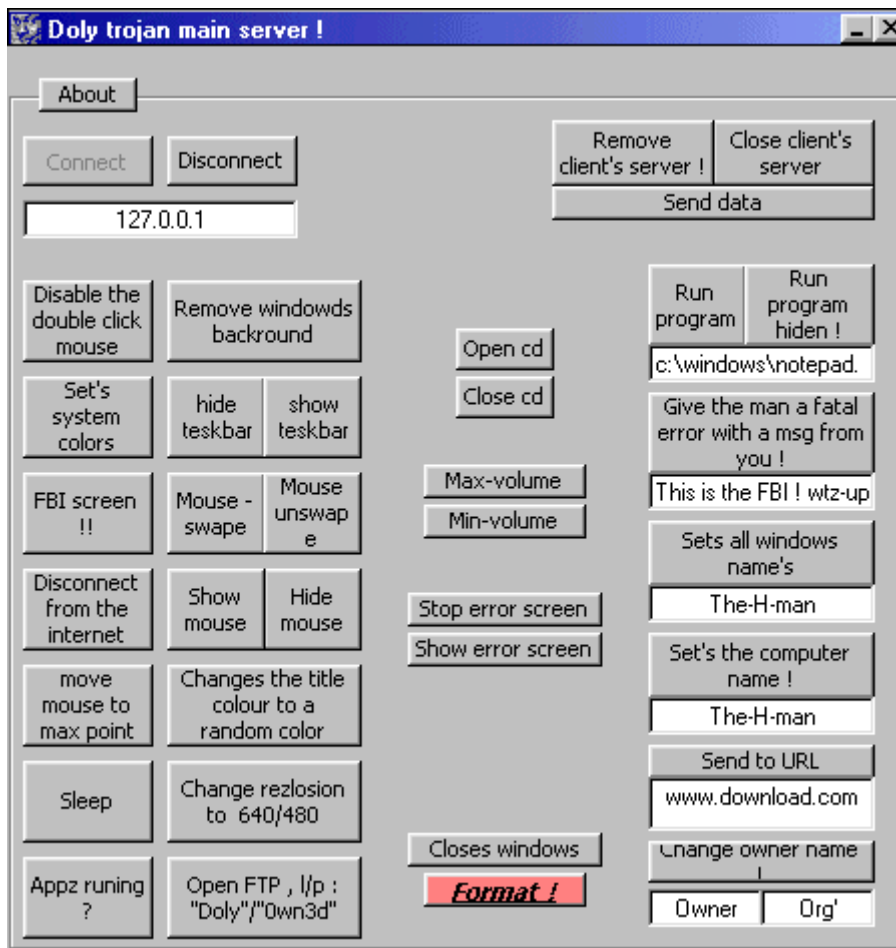
١- و البورتات التي يتسلل منها هذا البرنامج : (٣٤٣٢٤) . و هذا البرنامج مخصص فقط لسرقة كلمات السر الموجودة في جهاز الضحية .

٢- و لكي تجد الباتش ، فأمامك طريقين : الطريق الأول ... و هو موضح في الصورة السابقة ، و الموجود في الأمتداد :

software\microsoft\windows\currentversion\runtservices)  
( hkey\_local\_machine\

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

##برنامج الـ (doly Trojan) :-



١- و البورتات التي يتسلل منها هذا البرنامج : (١٠١١) .

٢- بالنسبة لتفسير الصورة السابقة ، فهو كالتالي : لكي تعرف مكانه ؛ فما عليك إلا بالذهاب الى الأمتداد التالي :

software\microsoft\windows\currentversion\run)  
( hkey\_local\_machine\

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

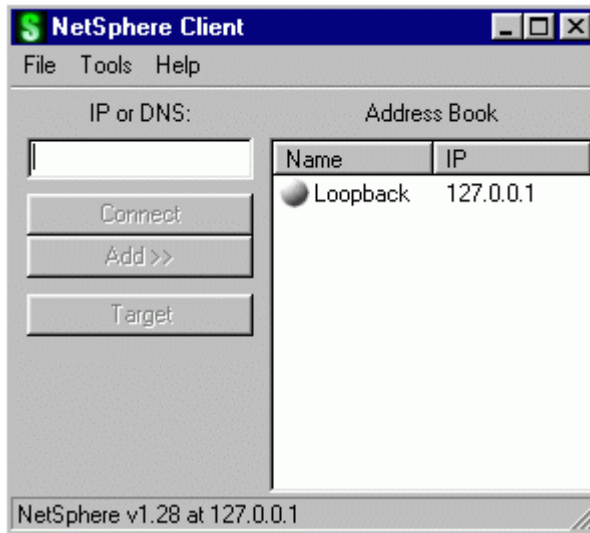
٣- أو من الممكن أن تجده في هذا الأمتداد ، و بنفس الأسم :

software\microsoft\windows\currentversion\run)  
( hkey\_local\_user\

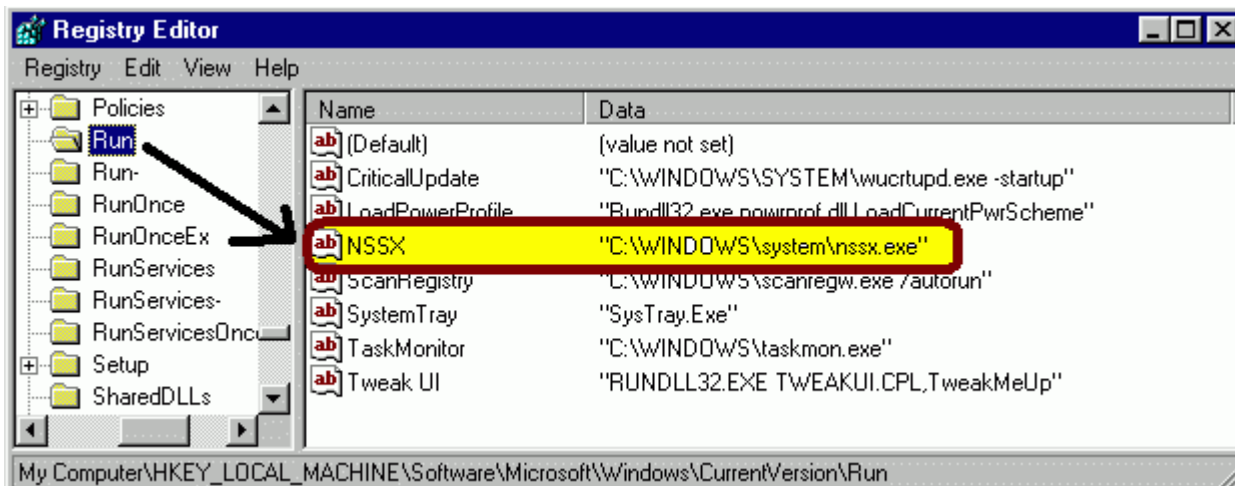
---

###برنامج الـ (netsphere) :-

---



١- و البورتات التي 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 أي شخص فيك هذا البرنامج فأنا أقول لك أنك مش هتعرف تخلص من شره .



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

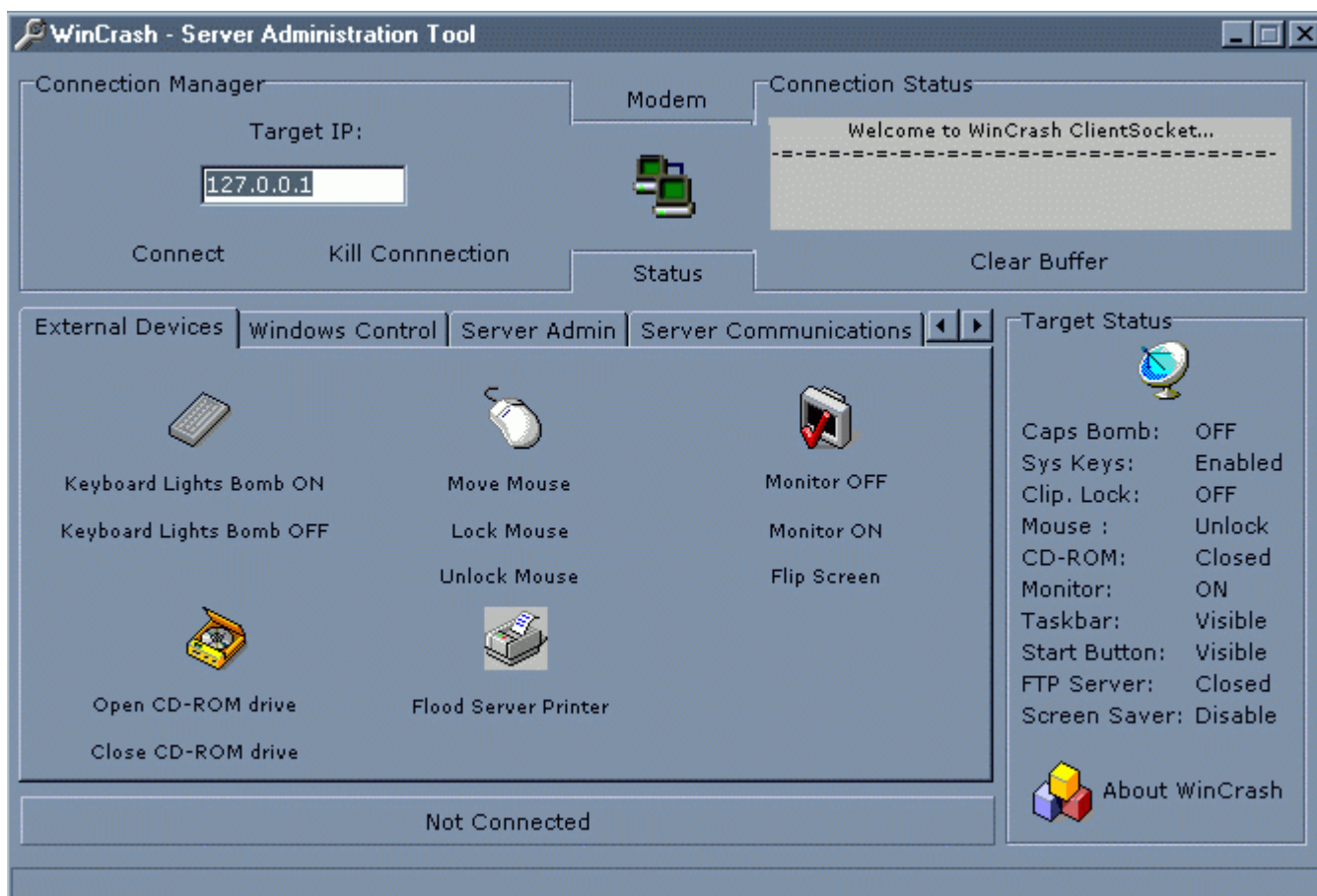
**software\microsoft\windows\currentversion\run)**  
**( hkey\_local\_machine\**

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

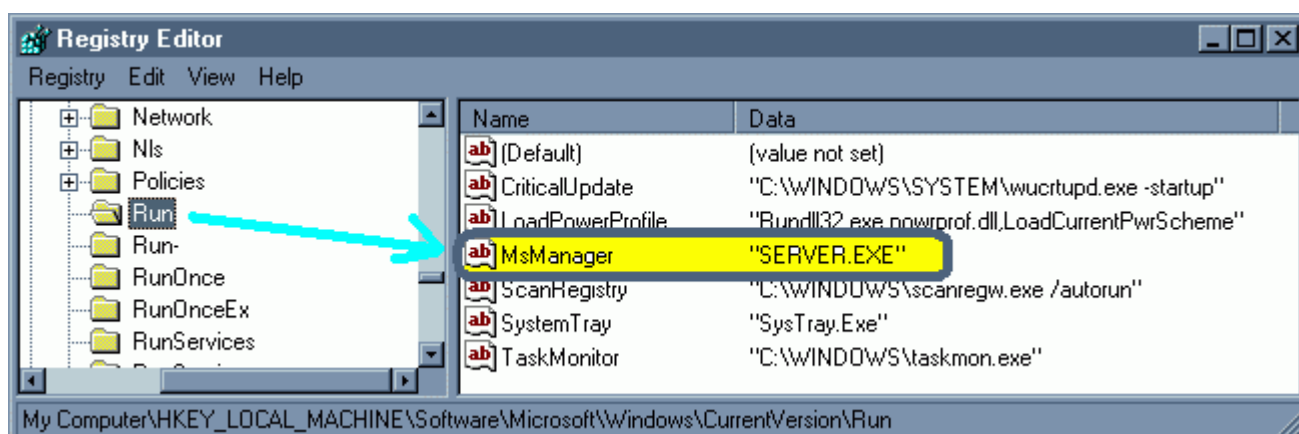
---

##برنامج الـ (wincrash) :-

---



١- و البورتات التي يتسلل منها هذا البرنامج : (٥٧٤٢) .



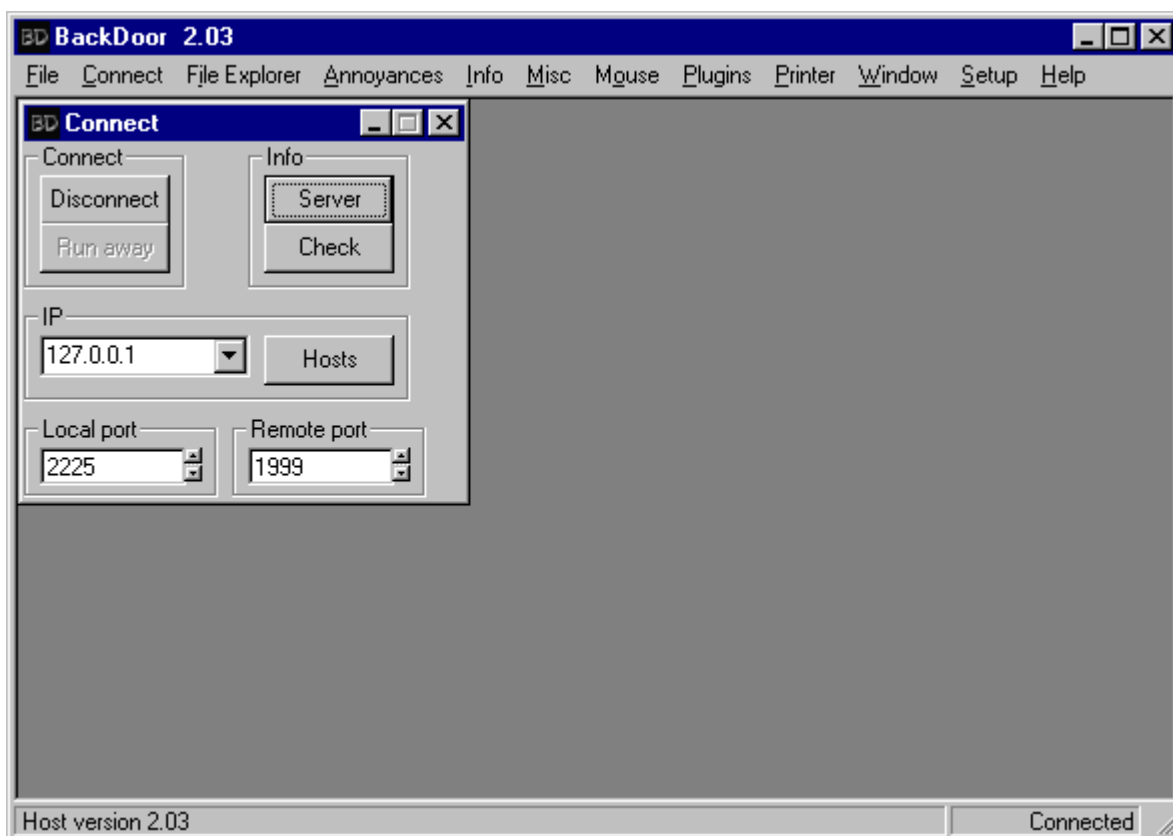
٢- بالنسبة لتفسير الصورة السابقة ، فهو كالتالي : لكي تعرف مكانه ؛ فما عليك إلا بالذهاب الى الامتداد التالي :



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 التي يتسلل منها هذا البرنامج : (١٩٩٩) . و عيب هذا البرنامج أنه خبيث ، و الخبائثة في حد ذاتها غالباً ما تكزن أداة قوية تمكن المخترق من التحكم بجهاز الضحية .

٢- بالنسبة لتفسير الصورة السابقة ، فهو كالتالي : لكي تعرف مكانه ؛ فما عليك إلا بالذهاب الى الأمتداد التالي :

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) :-



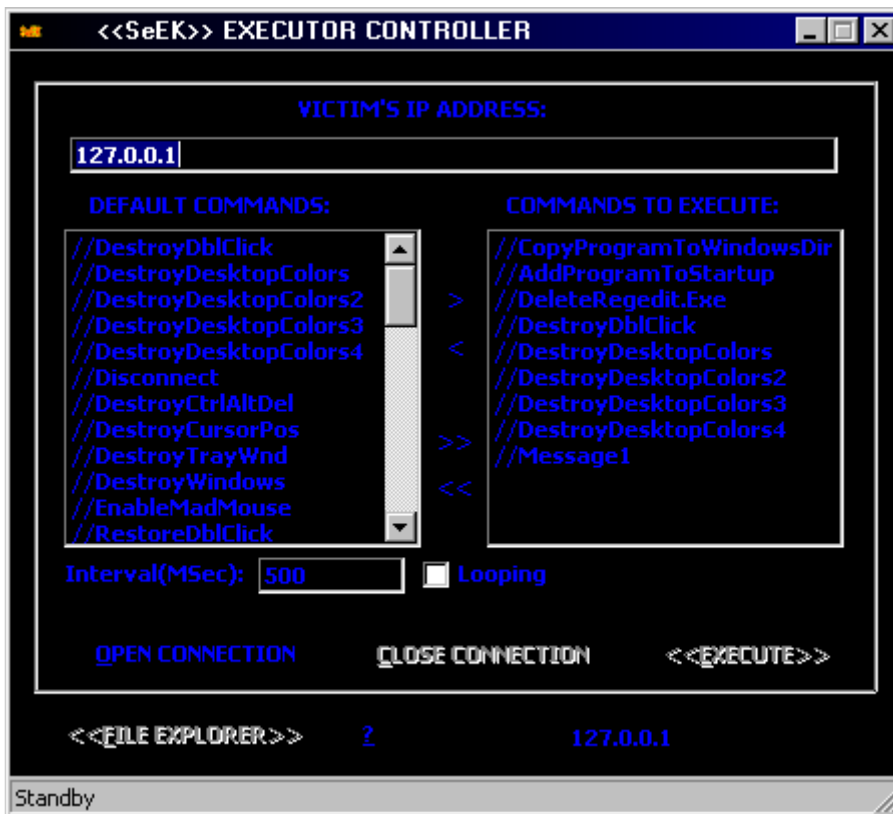
١- و البورتات التي يتسلل منها هذا البرنامج : (٥٤٠٠) و (٥٤٠١) و (٥٤٠٢) و (٢١) . و هذا البرنامج لي قصة طويلة معه ، و لكن كل ما أقوله لكم هو أن هذا البرنامج يعتبر برنامجي المفضل من بين برامج الأختراق .

٢- بالنسبة لتفسير الصورة السابقة ، فهو كالتالي : لكي تعرف مكانه ؛ فما عليك إلا بالذهاب الى الأمتداد التالي :

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) :-



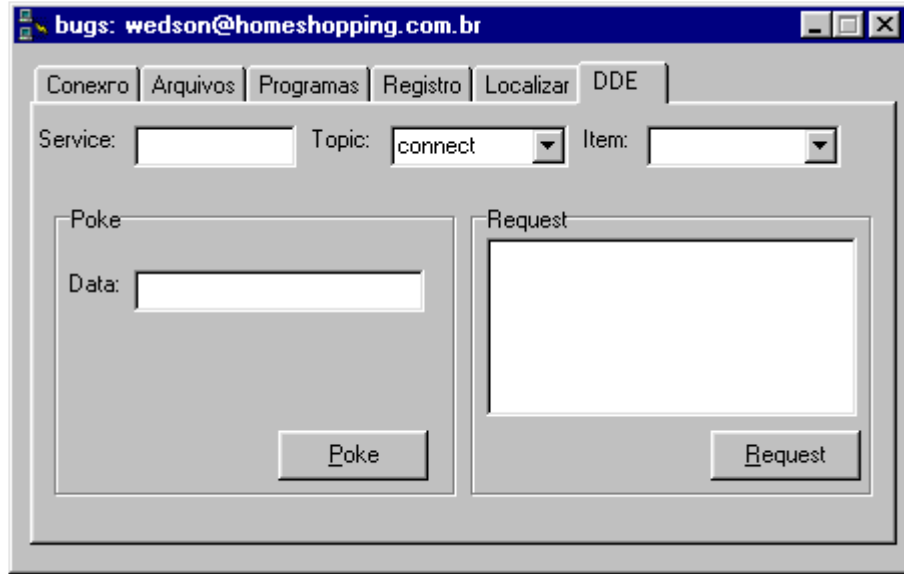
١- و البورتات التي يتسلل منها هذا البرنامج : (٨٠) .

٢- بالنسبة لتفسير الصورة السابقة ، فهو كالتالى : لكي 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) :-



١- و البورتات التي يتسلل منها هذا البرنامج : (٢١١٥) .

٢- بالنسبة لتفسير الصورة السابقة ، فهو كالتالى : لكي 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) .

**blackcode**