iPenetrate Security Consulting

Volume 1, Issue 1337

December 6, 2004

NMAP THE UNIVERSE!

INSIDE THIS ISSUE:

How to Install Nmap	2
How Nmap is Used	2
Useful Flags	2
Information Nmap Provides	3
Nmap the News!	3
References	3
Port Scan Detection...	4

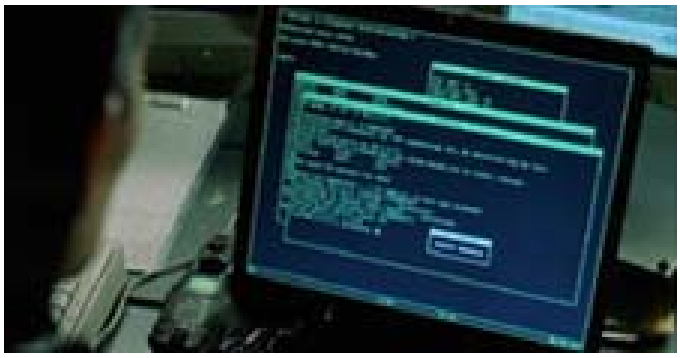
iPenetrate Team Members:

- Jason Chong jasc8@u.washington.edu
- Yarun Luon yaurn@u.washington.edu
- Ryan Prins rprins@u.washington.edu
- Anthony Trotter atrotter@u.washington.edu

WHAT IS NMAP?

Nmap is a tool that can be used by individuals that are curious about networks, network admins that want to see what is running on their networks, or for hackers that wish to use this tool maliciously. The Nmap tool is very easy to install and use on virtually any platform.

Nmap supports a large number of scanning techniques such as: UDP, TCP connect(), TCP SYN (half open), ftp proxy (bounce attack), ICMP (ping sweep), FIN, ACK sweep, Xmas Tree, SYN sweep, IP Protocol, and Null scan. It also offers a number of advanced features such as remote OS detection via TCP/IP fingerprinting, stealth scanning, dynamic delay and retransmission calculations, parallel scanning, detection of down hosts via parallel pings, decoy scanning, port filtering detection, direct (non-portmapper) RPC scanning, fragmentation scanning, and flexible target and port specification.



Nmap makes an appearance in "The Matrix Reloaded"

This tool is often used for networks exploration and also as a tool to check for security vulnerabilities. Nmap provides the user a list of open ports, services, and live hosts (based on used flags). With this information one can check the security of their network for holes that they may not have been aware of. However, on the flip side, a hacker could use this tool to find open ways to get into a system. With the addition of the random IP scan, this makes Nmap even more powerful for this use.

HOW NMAP WORKS

Nmap utilizes raw IP packets in innovative ways to determine what hosts are available on the networks, what services they are running, what OS they are running, and many more other characteristics of the hosts on the network. The most basic Nmap use, is testing what hosts are up and running, is performed by default. Nmap produces this information by sending ICMP request packets to specified hosts and waiting for a response. After determining if the host is alive or not, other options like OS detection can be performed with the use of TCP/IP fingerprinting, which determines characteristics of the OS and uses the information it discovers to create a fingerprint to match against known OS fingerprints in the Nmap database.

How to Insall Nmap

Users have many choices when choosing to install Nmap. Nmap supports multiple platforms, including more popular operating systems such as Linux, Mac OS X, and Microsoft Windows. Users also have the choice between source, binary, RPM, and zip distributions. The chosen package will depend on the user's operating system.

For Linux systems that support RPM, the user can install Nmap by simply running the commands:

```
rpm -vhU http://download.insecure.org/Nmap/dist/Nmap-3.75-1.i386.rpm
rpm -vhU http://download.insecure.org/Nmap/dist/Nmap-frontend-3.75-1.i386.rpm
```

Windows users will want to download either the source or zip distributions. If the zip distribution is chosen, the user need only unzip the file to his/her chosen folder, such as "C:\Program Files\Nmap-[version]." If the source distribution is chosen, the user will need to open the solution file (.sln) in Visual Studio and compile the code.

Unix/Linux and Mac users also have the option of using the source or binary distributions. To install the source distribution, download the tarball from the dist directory at http://download.insecure.org/Nmap/dist/?M=D. Accordingly, run the following commands:

```
bzip2 -cd Nmap-VERSION.tar.bz2 | tar xvf -
cd Nmap-VERSION
./configure
make
su root
make install
```

How Nmap is Used

"75% of all statistics are made up on the spot."

Nmap may be used for many purposes. In general, Nmap is used for network exploration and security auditing. Systems Administrators may use Nmap to analyze their network and perform penetration testing. On the other end of the spectrum, hackers may use Nmap to scan entire subnets for live computers, and accordingly determine the services that are running on a remote computer. In addition, Nmap can be used to determine the Operating System of a remote machine, or the types of packet filters and firewalls that are currently in use.

Nmap may also be used in conjunction with other tools to hack/audit a system. For example, a hacker may use Nmap to scan an entire network for live computers, scan the live computers for particular services, then use another tool, such as amap, to determine the versions of the services. The hacker may then proceed to research vulnerabilities for the chosen service, ultimately attacking the computer by taking advantage of the vulnerability.

Useful Flags

Nmap is a versatile tool with different scanning methods and different configurable options. Complete documentation can be found in the Nmap man pages or the html man pages. A link is included in the reference section. The following are several practical flags when using Nmap.

`-h` A brief usage of flags available to Nmap

`-O` `(dash big oh)` This option actives remote host identification via TCP/IP fingerprinting.

`-P0` `(dash big pee zero)` Does not try to ping hosts at all before scanning them. This allows the scanning of networks that do not allow ICMP echo requests (or responses) through their firewall. Useful for sites like Microsoft.com.

`-T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane>` Scan speed in order from slowest to fastest.

Example Usage:

```
Nmap –O –P0 –T Insane www.dhs.gov
```

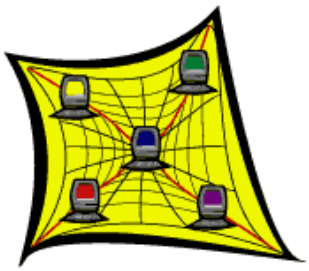
Information Nmap Provides

As mentioned above, Nmap is a tool used to perform network penetration tests as well as computer security through the use of port scanning. The type of information that Nmap can provide include:

- Open ports on the host computer (TCP, UDP…)
- Filtered or Unfiltered ports
- Version of the host OS
- Live hosts vs. Dead hosts
- What services are running (application name and version)
- Firewall information (rulesets)
- Packet filtering information
- Information on the service protocol running
- What IP protocols are supported on a host

Etc…

With the vast amount of information that Nmap provides to its users, it is apparent that computer security personnel can utilize this tool to test their own networks, but another use for Nmap is to collect information on potential hosts that could be targeted maliciously by hackers or crackers. Nmap provides a multitude of information to those that know how to utilize the various flags that can be used as options with the basic "Nmap" command.



This picture was called "internet.gif"
Which leads me to believe that the internet has only 5 computers

Nmap The News!

Nmap may be most famous for its appearance in The Matrix Reloaded; Trinity attempts to hack into the mainframe of a power plant by first using Nmap to discover vulnerabilities, and secondly running a fictional program entitled SSHnuke to exploit the vulnerability (Trinity actually uses a real life loophole entitled "SSH1CRC32." Nmap also appeared in a less known movie, Battle Royale, starring the lovely Go Go from Kill Bill: Volume 1.

Nmap has also appeared in many magazines, including Linux Journal and Information Week. In addition, Microsoft now lists Nmap among a list of 7 recommended security tools, and even insists that Nmap should be run daily. This is particularly interesting, considering that with the release of Windows XP SP2, Nmap was crippled. Fortunately, Nmap developers created a workaround to this problem.

"Nmap is like that toy you didn't have when you were a kid that everybody else had and played with. Now you seek your revenge on those people by hacking their networks."

References

HTML version of Nmap man page:
http://www.insecure.org/Nmap/data/Nmap_manpage.html

If Microsoft owned Nmap:
http://www.counterhack.net/base_clippy_image.html

Ways to hide your OS fingerprint:
http://voodoo.somoslopeor.com/papers/nmap.html#LSOLUTIONS
http://www.securiteam.com/windowsntfocus/5OP0E0A1FC.html

iPenetrate Security Consulting

c/o Network Analysis Team
1 Unsecured Network Way
Your Problem, State of Confusion 10110

Phone: Don't call us, we'll call you.
Fax: What's a fax?
E-mail: We don't own computers.

We're not on the web! So, don't look for us.

We penetrate your network so you don't have to!

iPenetrate

Once again iPenetrate is back to bring you the latest and greatest in network security!

As you well know, we are the same chums that brought you "Warwalking in the U-District: Uncensored" and "IPsec and You!" As you can see from our last two seminars, we are passionate about security and how it affects us as users and our data. Nothing is worse than losing all of that hard worked data because of some hax0r!

Like many of you, we all have home computers and networks and our data is extremely important to us. Because of this, we don't get out much and we get lonely quite frequently. So, if you see us twitch in the light, that is why. Sunlight is foreign to us. However, our network packets are always there to keep us company. Even when we do not understand what they are telling us.

So, if you are in need of some network consulting, or if you would like to be our friend, please take a look at our contact information. Yes, we realize that it is sparse, but that is how we like it! If you do like what you see in this handout and the corresponding presentation please let us know. We're trying to keep our presentation to around 15 minutes, so holler at us if we go over. Now it is time for us to run back into our blackened holes that we call our lives.

Port Scan Detection and OS Un-identification

Actually preventing a port scan can be difficult, since a port scan is just a collection of IP packets sent to different ports of a host. An Intrusion Detection Systems (IDS) can detect these port scans by recognizing the pattern that all the host ports are being probed from the same recipient address. However this can become tricky if the user administering the port scan is using infrequent or random time intervals for each port pinged.

Because malicious users can customize attacks that exploit that particular operating system, having the operating system identified through fingerprinting can be a security risk. There are numerous ways to prevent this OS fingerprinting depending on the OS. For Windows NT systems, this can be done by editing registry keys. For Linux operators, patches to the Linux kernel are available that change the actual TCP/IP stack behavior. Another solution is to create an abundance of virtual devices that each have a specified OS fingerprint. Doing this will not only be time consuming for the malicious user to scan, but it could also lure the malicious user to a specific area of honeypots, all with a particular OS, and at the same time hiding your real OS.

Just some tall building that probably has a network or two inside.