A CASE STUDY

ON

NMAP - NETWORK MAPPER.

INTRODUCTION:

- **Nmap** (*Network Mapper*) is a security scanner, originally written by Gordon Lyon (also known by his pseudonym *Fyodor Vaskovich*),used to discover hosts and services on a computer network, thus building a "map" of the network.
- To accomplish its goal, Nmap sends specially crafted packets to the target host(s) and then analyzes the responses.
- The software provides a number of features for probing computer networks, including host discovery and service and operating-systemdetection.
- These features are extensible by scripts that provide more advanced service detection, vulnerability detection, and other features.
- Nmap can adapt to network conditions including latency and congestion during a scan. The Nmap user community continues to develop and refine the tool.
- Nmap started as a Linux-only utility,but porting to Windows, Solaris, HP-UX, BSD variants (including OS X), AmigaOS, and IRIXhave followed.Linux is the most popular platform, followed closely by Windows.

FEATURES:

Nmap features include:

- **Host discovery** – Identifying hosts on a network. For example, listing the hosts that respond to TCP and/or ICMP requests or have a particular port open.
- **Port scanning** – Enumerating the open ports on target hosts.

- Version detection – Interrogating network services on remote devices to determine application name and version number.
- **OS detection** – Determining the operating system and hardware characteristics of network devices.
- **Scriptable interaction with the target** – using Nmap Scripting Engine(NSE) and Lua programming language.

Nmap can provide further information on targets, including reverse DNS names, device types, and MAC addresses.

Uses of Nmap:

- Auditing the security of a device or firewall by identifying the network connections which can be made to, or through it.
- Identifying open ports on a target host in preparation for auditing.
- Network inventory, network mapping, maintenance and asset management.
- Auditing the security of a network by identifying new servers.
- Generating traffic to hosts on a network, response analysis and response time measurement.
- Finding and exploiting vulnerabilities in a network.

NMAP WITH EXAMPLES:

- Network scanning is done at the reconnaissance stage of a structured attack. A network scanner can provide an attacker with information on remote machines which are alive, and that the attacker can communicate with, as well as the services those systems are running.

- Scanning includes host sweeps/scans, OS scans, port scans and ping sweeps/scans. A host scan is typically done over an entire network, and reports machines which are alive on the network.

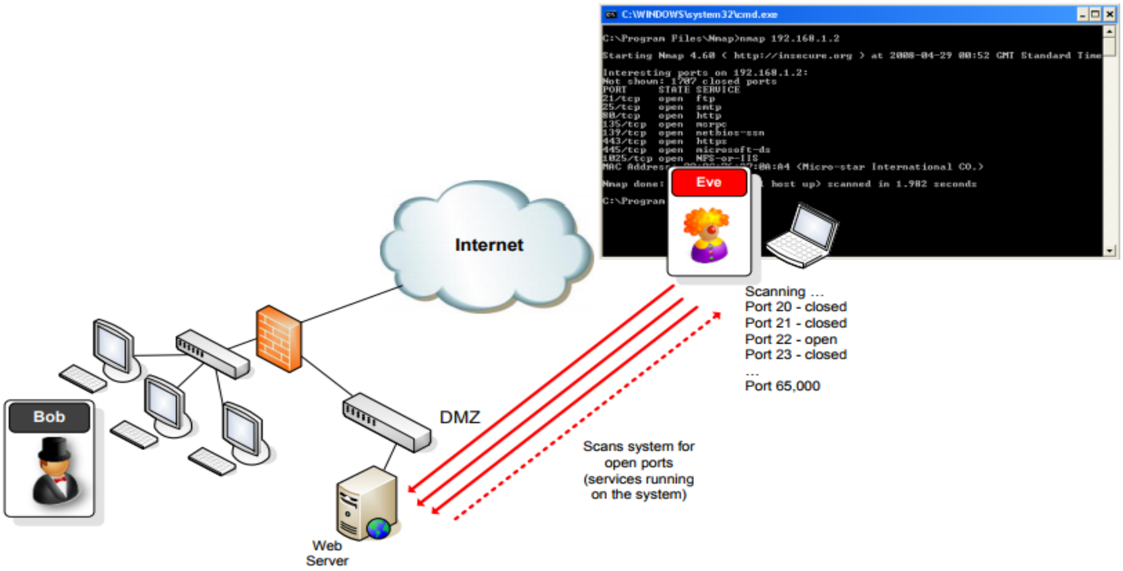
- A port scan is performed on a single, remote, host system, via its IP Address, and gives information on services running on the machine.

- Typically an attacker is also looking for which OS the system is running as well as any open TCP and UDP ports (services) which the attacker may be able to exploit.

- A network scanning tool, such as nmap, can be used to automatically probe the system for open ports, and give a report back to the attacker.

- To mitigate open ports which attackers could use to compromise the system, make sure only services which are necessary are running.

- Some server OSs have services running by default, such as HTTP (port 80) and FTP (ports 20 & 21) which should be removed when systems are installed. (The command line network utility netstat can be used to check which services are running on the same host).



```
C:\Program Files\Nmap>nmap 192.168.1.2

Starting Nmap 4.60 ( http://insecure.org ) at 2008-04-29 00:52 GMT Standard Time

Interesting ports on 192.168.1.2:
Not shown: 1707 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
MAC Addres            7:0A:A4 (Micro-star International CO.)

Nmap done:          1 host up) scanned in 1.982 seconds

C:\Program
```

Nmap can be used as a simple discovery tool, using various techniques (e.g. ARP pings, ICMP requests, TCP and/or UDP pings) to identify live devices on a network. All of these techniques are used when specifying the –sP switch in an Nmap command, for example:

Nmap –sP 192.168.1.0/24

This simple command will send various packets (ARP, ICMP, etc.) to every address within the 192.168.1.0/24 range, and will report any devices that respond. The results will look similar to those in the example below:

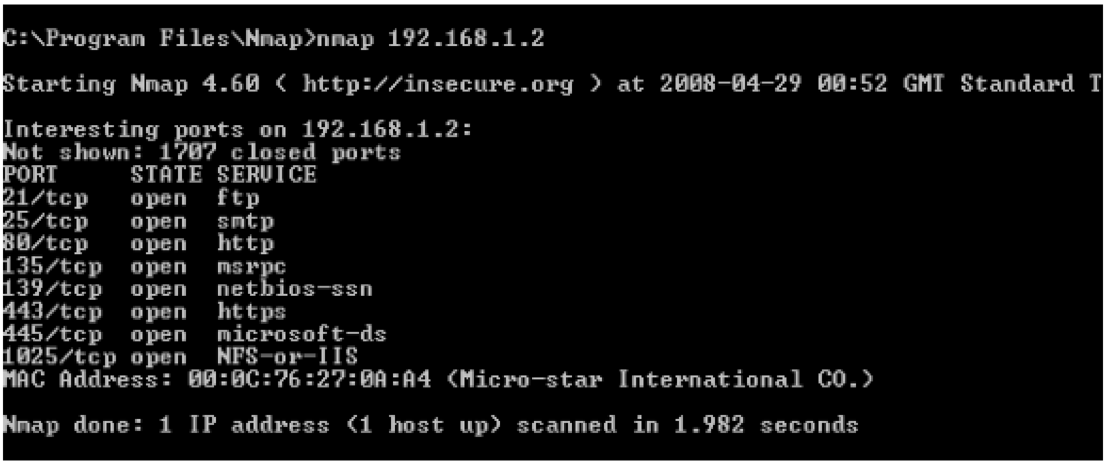
```
c:\>nmap -sP 192.168.1.0/24

Starting Nmap 5.51 ( http://nmap.org ) at 2011-06-05 18:27 GMT Daylight
Time
```

```
Nmap scan report for 192.168.1.1
Host is up (0.20s latency).
MAC Address: 38:E7:D8:BC:E6:E7 (HTC)
Nmap scan report for 192.168.1.3
Host is up.
Nmap scan report for 192.168.1.4
Host is up (0.31s latency).
MAC Address: 00:1C:DF:58:9D:0A (Belkin International)
Nmap scan report for 192.168.1.254
Host is up (0.0040s latency).
MAC Address: 00:14:7F:35:B3:58 (Thomson Telecom Belgium)
Nmap done: 256 IP addresses (4 hosts up) scanned in 12.10 seconds
```

USING WIRESHARK:

Start a Wireshark capture. Open a Windows command window, and perform a Host Scan (using ICMP packets) on a neighbours machine using nmap –sP [neighbours ip address] (do not scan the entire subnet). Stop the capture and filter the traffic for ARP and ICMP packets if necessary.



```
C:\Program Files\Nmap>nmap 192.168.1.2

Starting Nmap 4.60 ( http://insecure.org ) at 2008-04-29 00:52 GMT Standard T

Interesting ports on 192.168.1.2:
Not shown: 1707 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
1025/tcp  open  NFS-or-IIS
MAC Address: 00:0C:76:27:0A:A4 (Micro-star International CO.)

Nmap done: 1 IP address (1 host up) scanned in 1.982 seconds
```

Nmap command line reconnaissance tool

What's it running ?

Once it's identified the live devices, Nmap can be used to determine which TCP and UDP ports are open, closed or firewalled. Knowing which services are running, and which of those are essential to the running of the business, can help determine a network security baseline.

This baseline can serve as a starting point from which to identify any anomalies, allowing for swift investigation. Malware will often open ports on infected devices in order to send and/or receive data; malicious attackers will look for badly configured services (i.e., anonymously accessed FTP servers, unauthenticated administrative Web interfaces, etc.) and exploitable software. Nmap can help to identify any of these problems.

When scanning devices to determine which ports are open, there are various basic scanning options:

- **sS** –Performs a “stealth” TCP scan (that does not fully complete the “TCP three-way handshake,” and closes the connection once the service responds).

- **sT** –Performs a full TCP scan (a full connection is established with open TCP ports).

- **sU** –Performs a UDP scan (as UDP is a connectionless protocol, these scans can take significantly longer than TCP scans).

- **p** – Tells Nmap which ports to scan (e.g., –p1-65535 will specify every port).

These basic options can be used to give a quick overview of the open ports on any given device, for example:

```
c:\>nmap -sS -p1-65535 192.168.1.4

Nmap scan report for 192.168.1.4
Host is up (0.017s latency).
Not shown: 65520 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
912/tcp   open  apex-mesh
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
17500/tcp open  unknown
49152/tcp open  unknown
```

```
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49158/tcp open  unknown
49159/tcp open  unknown
MAC Address: 00:1C:DF:58:9D:0A (Belkin International)

Nmap done: 1 IP address (1 host up) scanned in 139.26 seconds
```

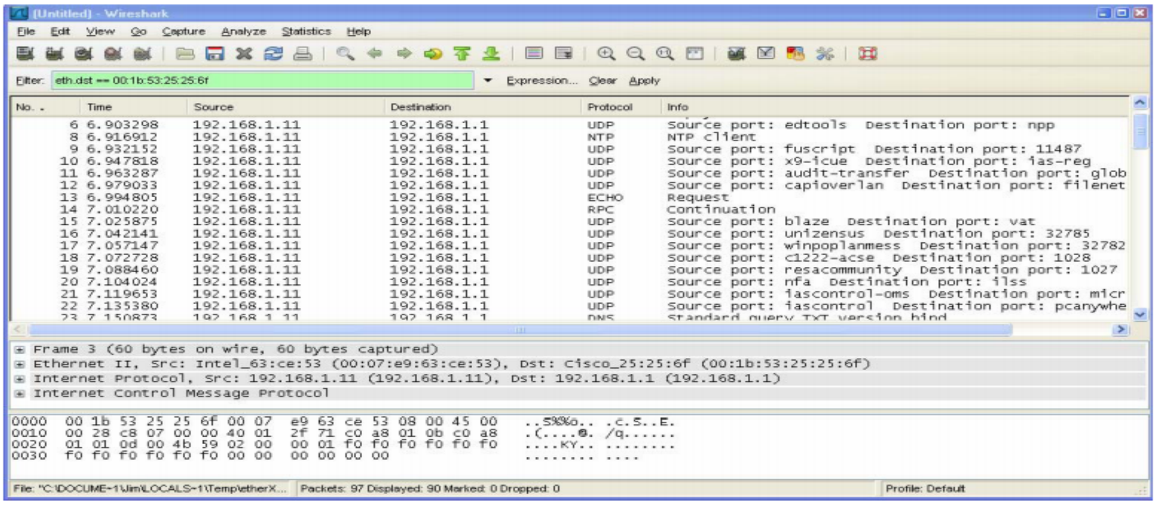
- Nmap includes an advanced option, “--top-ports”, which can be used to test only the most commonly seen ports. This can be used in conjunction with various advanced timing options to reduce the time needed to scan a large number of devices.

- Knowing which ports are open is only half the battle, but Nmap does have another weapon at its disposal: a huge database of service fingerprints. Nmap can connect to the open ports it discovers and attempt to identify the services running behind them. For the attacker, version information is critical to knowing whether a service is exploitable. By default, Nmap identifies services based on their entry in the Nmap services file (which was initially based on the IANA assigned ports list).

- As this isn’t always correct (What’s to stop an attacker from writing a virus that sends out data on the registered SMTP port?), the “-sV” switch can be used to tell Nmap to interrogate discovered open ports to determine software and version information.

Start a new Wireshark capture, and then perform a complete Port Scan (in this case a TCP SYN scan) and an Operating System Fingerprint on a neighbours machine using nmap –O [neighbours ip address] (do not scan more than a single machine).

The –O option should provide the OS running on the scanned machine. Stop the capture and filter for source address == your machines address if necessary. Notice the number and types of ports tried by the nmap port scan. The capture should look something like:



Filter: eth.dst == 00:1b:53:25:25:6f

```
No. .  Time        Source          Destination    Protocol  Info
     6 6.903298    192.168.1.11    192.168.1.1    UDP       Source port: edtools  Destination port: npp
     8 6.916912    192.168.1.11    192.168.1.1    NTP       NTP client
     9 6.932152    192.168.1.11    192.168.1.1    UDP       Source port: fuscript  Destination port: 11487
    10 6.947818    192.168.1.11    192.168.1.1    UDP       Source port: x9-icue  Destination port: ias-reg
    11 6.963287    192.168.1.11    192.168.1.1    UDP       Source port: audit-transfer  Destination port: glob
    12 6.979033    192.168.1.11    192.168.1.1    UDP       Source port: capioverlan  Destination port: filenet
    13 6.994805    192.168.1.11    192.168.1.1    ECHO      Request
    14 7.010220    192.168.1.11    192.168.1.1    RPC       Continuation
    15 7.025875    192.168.1.11    192.168.1.1    UDP       Source port: blaze  Destination port: vat
    16 7.042141    192.168.1.11    192.168.1.1    UDP       Source port: unizensus  Destination port: 32785
    17 7.057147    192.168.1.11    192.168.1.1    UDP       Source port: winpoplanmess  Destination port: 32782
    18 7.072728    192.168.1.11    192.168.1.1    UDP       Source port: c1222-acse  Destination port: 1028
    19 7.088460    192.168.1.11    192.168.1.1    UDP       Source port: resacommunity  Destination port: 1027
    20 7.104024    192.168.1.11    192.168.1.1    UDP       Source port: nfa  Destination port: ilss
    21 7.119653    192.168.1.11    192.168.1.1    UDP       Source port: iascontrol-oms  Destination port: micr
    22 7.135380    192.168.1.11    192.168.1.1    UDP       Source port: iascontrol  Destination port: pcanywhe
    23 7.150873    192.168.1.11    192.168.1.1    DNS       Standard query TXT version bind

⊞ Frame 3 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: Intel_63:ce:53 (00:07:e9:63:ce:53), Dst: Cisco_25:25:6f (00:1b:53:25:25:6f)
⊞ Internet Protocol, Src: 192.168.1.11 (192.168.1.11), Dst: 192.168.1.1 (192.168.1.1)
⊞ Internet Control Message Protocol

0000   00 1b 53 25 25 6f 00 07  e9 63 ce 53 08 00 45 00   ..S%%o.. .c.S..E.
0010   00 28 c8 07 00 00 40 01  2f 71 c0 a8 01 0b c0 a8   .(....@. /q......
0020   01 01 0d 00 4b 59 02 00  00 01 f0 f0 f0 f0 f0 f0   ....KY.. ........
0030   f0 f0 f0 f0 f0 f0 00 00  00 00 00 00               ........ ....

File: "C:\DOCUME~1\Jim\LOCALS~1\Temp\etherX...   Packets: 97 Displayed: 90 Marked: 0 Dropped: 0   Profile: Default
```

Nmap port scan

The scan above has identified the device as Microsoft Windows Server 2008, Windows Vista or Windows 7.

CONCLUSION:

Nmap is an extremely useful, free tool that can allow organisations to keep tabs on the state of their networks. Running these types of scans on a regular basis can help maintain a reasonable level of assurance that:

1. You know what devices are on the network, and can easily discover if and when something new has been added.

2. You know what services are running on every device, and can easily discover if a service has been created (whether malicious or not).

3. You can use the information discovered to help mitigate some vulnerabilities on the network.