Abertay University

Banner grabbing and Nmap exercises Ethical Hacking lab exercise.

Note : - The location of the tools folder in the University labs is \\hannah\Tools\pentest

Note that Information contained in this document is for educational purposes.

.

Contents

.

.

1 MANUAL BANNER GRABBING

Often, a pen tester wants to ensure that the services that they have found are "real" (sometimes scanners can give false results) and if they are the service they expect. For example, if we find that port 21 is open, we will often assume that it is FTP because 21 is the standard port number. However, it is easy to run a service such as a web server on port 21 (or any other port) rather than its standard port (e.g. 80 for HTTP). Users may try to hide services by using unusual port numbers. So it is important that we know what the service actually is so that we can formulate an attack correctly.

An easy way of collecting information about a service is to *manually* connect to it using a simple tool and view the response from the service (termed the banner). Banners generally give lots of information about the service.

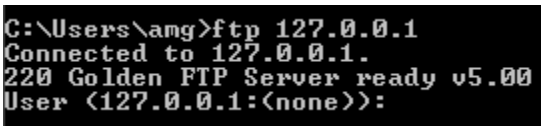
The following exercises will illustrate some generic manual banner grabbing techniques. If a protocol is unknown then a pen tester would have to research it or test using these generic techniques.

1.1 FTP BANNER GRABBING.

FTP is an acronym for File Transfer Protocol. As the name suggests, FTP is used to transfer files between computers on a network. We will set up an FTP server on our Windows desktop and then connect to it and grab the banner. There are many different FTP servers but they all *normally* listen on port 21.

- From the **tools** folder, **install and then run** "**Golden FTP Server**".
- From the Windows start menu, run **cmd**

Now connect to the ftp server using **ftp 127.0.0.1**, the server version should be shown in the banner.



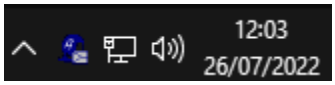
During a pen test, we would normally research this version to see if it has any known vulnerabilities.

1.2 E-MAIL BANNER GRABBING (SMTP PORT 25 AND POP3 PORT 110)

The Argosoft E-Mail server provides standard E-mail i.e. SMTP (port 25) and POP3 (Port 110). **SMTP is the major e-mail sending protocol and POP3 is one of the e-mail receiving protocols**. Argosoft is very old software but will quickly allow us to examine the protocols without installing and configuring something large like the industry standard Microsoft Exchange. Argosoft also allows webmail from a browser (normally port 80). We will run Argosoft and then examine the banners.

- Install and run the **Argosoft E-mail server** from the tools folder (**agsmail.exe**).
- Then run it from the desktop.

- Note that after it runs, you can control it from the toolbar (bottom right hand of Windows) as shown below.



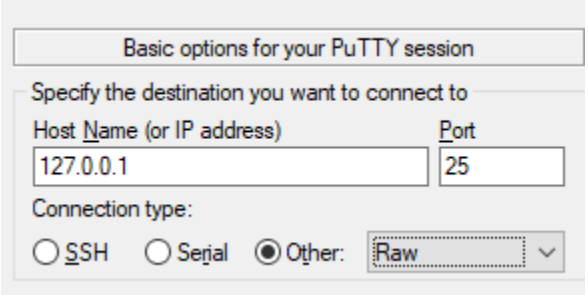
- **Right-click on the icon** to control the server. In our case, we only need to make sure that it is running.

PuTTY is an open source SSH and telnet client that has been developed for Windows. It allows for simple raw connections to any port.

We will now use **PuTTY** to create a raw connection to the ports and view the banners. Putty is installed by default in the specialist labs.

- From the Windows **Start menu**, run **PuTTY**.

- Connect to SMTP using a **RAW** connection to port 25 (SMTP) as shown below: -



The banner illustrating the version should be shown.

Note:

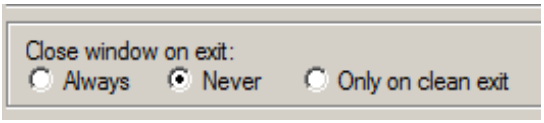
If you can speak SMTP "language" i.e. the SMTP protocol, you can send an e-mail using the raw connection. E.g. Type in HELO.

- In a similar manner, connect to **port 110** and get the **POP3** banner.

1.3 WEB SITE BANNER GRABBING.

Banner grabbing a web server is not as easy as this. After the connection is made, we need to issue a command before a web server responds with a banner. We can now connect to the Argosoft e-mail server web interface.

- Use PuTTY to connect to port 80 but make sure that you select **Never** close on exit as shown below: -



- Then issue the following HTTP command (copy and paste it for ease).

HEAD / HTTP/1.1

Then press the ENTER button TWICE.

You should be able to scroll back to the top of the window and read the banner showing the version.

- Use a browser and go to to http://127.0.0.1, this should show the **Argosoft** Webmail interface.

There are many other services that return banners when we connect. These can give useful information on the type of service and can often give the version.

Further reading

- https://securitytrails.com/blog/banner-grabbing
- https://www.hackingarticles.in/multiple-ways-to-banner-grabbing/

1.4 BANNER GRABBING EXERCISES

Using the banner grabbing techniques previously shown,

- **Switch on Server 1** and try to grab the banner for port **22** on **192.168.10.1** (note that port 22 is normally SSH and should be in this case).

- Try to grab the banner for **port 8000** on **192.168.10.1**.

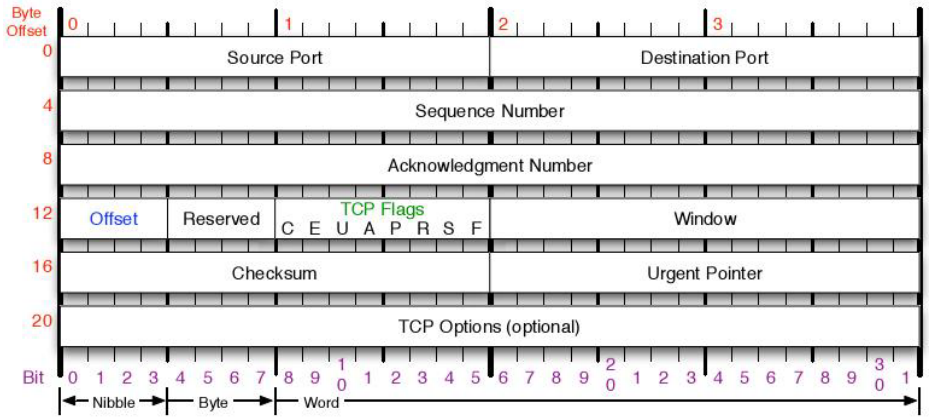
2 SOME REMINDERS

2.1 REMINDER - THE BASICS OF PORT SCANNING

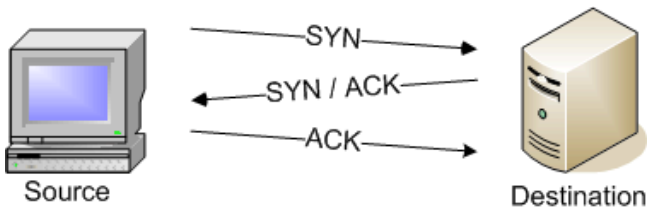
Nmap can be used for many purposes, however, its main uses are to:-

- Determine whether the target is switched on.
- Determine the open ports on a target.
- Determine the services running on a target.
- Determine the version of the services running on a target.
- Determine the operating system running on a target.

Background material was covered in the lecture but some references are shown below: -



The basic TCP three way handshake is shown below: -



SYN Scan	http://www.networkuptime.com/nmap/page3-2.shtml
TCP connect scan	http://www.networkuptime.com/nmap/page3-3.shtml
FIN Scan	http://www.networkuptime.com/nmap/page3-4.shtml
Xmas tree scan	http://www.networkuptime.com/nmap/page3-5.shtml
Null Scan	http://www.networkuptime.com/nmap/page3-6.shtml

2.2 A REMINDER OF OUR TARGET NETWORK

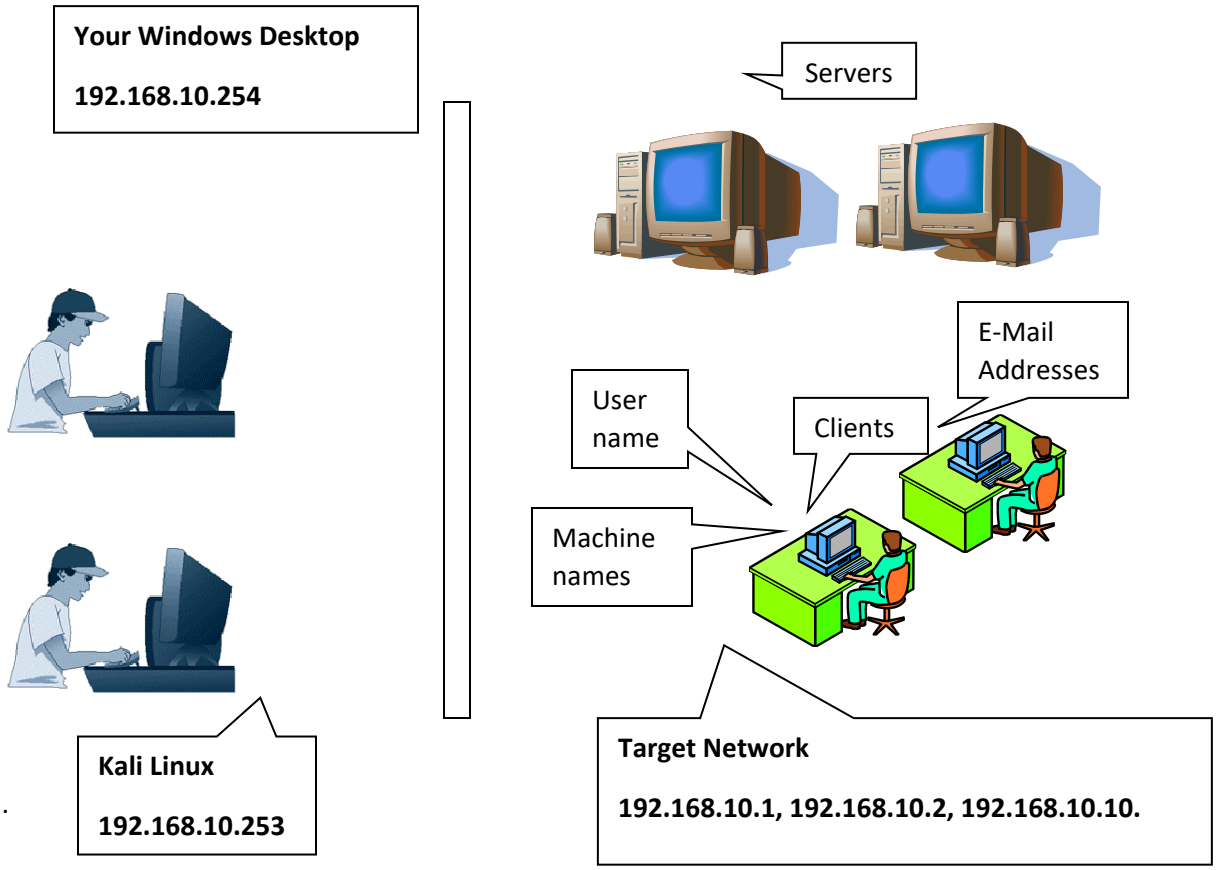
The IP addresses we are going to test are **192.168.10.1, 192.168.10.2**, **192.168.10.10**. The network is a client / server thus users must log on to a Windows server and the machines must be joined to the domain.

The pen tester has been given a special account to log in with on Client1 (the credentials are test/test123).

A note: - remember the reality of this situation.

In the real situation, we would not have physical access to login to these machines. Note that domain controllers ie. Server1 and Server2 will only allow login from Administrators by default anyway (in case you try!)

Our objective over the next few weeks is to investigate the target. A diagram is shown below: -



We only have one client on our network but in the real case, there would be lots of machines logged in. The Servers have details of all these computers and users etc under Active Directory (see video given previously "**A look at a Windows Server**" details).

3 NMAP SCANNING

- Firstly, make sure that **Server1** and **Server2** is running (using the snapshot **booted**) so that we scan them. Also, switch off Kali for the moment.

3.1 INTRODUCTION TO NMAP

NMAP is a multifaceted utility which is primarily used to scan a range of IP addresses, identify active systems, determine which ports on those systems are open, and attempt to identify the respective operating systems.

Like all security tools, nmap can be used defensively by a network manager or penetration tester to identify weaknesses that need to be corrected. It may also be used offensively by an attacker probing for vulnerabilities to exploit. Nmap is **the** industry standard scanner.

NMAP is free software and can be downloaded. It was originally written to run on Linux but is now available for several platforms including Windows. To illustrate how in-depth this tool is, there are several books written about using it (http://nmap.org/book/toc.html).

3.2 WAYS OF RUNNING NMAP

Nmap is a command-prompt based program but a GUI (Zenmap) has been created to assist in using the package. Note that using the standard settings in Zenmap would **NOT** normally be used by a security specialist. Also, using basic settings would run the risk of crashing target machines or devices.

This handout will deal with the command prompt switches to ensure that the basics of using nmap are covered. Using the command prompt version means that scripting (or Windows batch files) is possible. Zenmap is NOT used by professional pen testers for this reason.

Note: -

Scans can take a long time and there may be a lot of machines to test so a pen tester will normally script a network scan and let the scans run.

- Under Windows, **open a command prompt** (**cmd**).

Note: -

Nmap is installed under Kali linux as well so you could do these exercises using it if you like. You should be comfortable using either Linux or Windows. Note that if you are using Kali then you must use **sudo**.

3.3 NMAP PING SCANNING.

To perform a simple ping scan, the switch -sn or -sP can be used. Note that -sP is a legacy switch but probably easier to remember.

- Try the following: -

nmap -sn 192.168.10.1

nmap -sP 192.168.10.2

3.4 NMAP ARP SCANNING.

Remember that ICMP pings can be blocked by the firewall so an ARP scan is often used. This is not the easiest command line to remember!

- Try the following: -

nmap -sP -PR 192.168.10.1

3.5 A SAMPLE NMAP FULL CONNECT (VANILLA) SCAN

This form of port scanning is the most basic from of TCP port scanning. It uses the full TCP connect (i.e. SYN, SYN/ACK, ACK). A sample output against a home router is shown below : -

```
nmap -sT 10.0.0.1

Starting Nmap 4.68 ( http://nmap.org ) at 2008-08-09 13:59 GMT
Standard Time
Interesting ports on 192.168.10.1:
Not shown: 1713 closed ports
PORT     STATE SERVICE
80/tcp   open  http
5190/tcp open  aol
MAC Address: 00:0F:B5:A1:23:24 (Netgear)

Nmap done: 1 IP address (1 host up) scanned in 1.360 seconds

C:\Program Files\Nmap>
```

Note the **MAC address** has been determined and a guess at the manufacturer is also shown. Port 80 (web server for admin) and port 5190 is open (this is common for a Netgear home router).

A sample output against a Windows 10 machine is shown below : -

```
nmap -sT 10.0.0.10

Starting Nmap 4.68 ( http://nmap.org ) at 2008-08-12 10:57 GMT
Standard Time
All 1715 scanned ports on 10.0.0.10 are filtered
MAC Address: 00:01:6C:E2:D4:A7 (Foxconn)

Nmap done: 1 IP address (1 host up) scanned in 44.250 seconds

C:\Program Files\Nmap>
```

Note:-

The word "filtered" essentially means firewalled. Since all ports are closed, we can guess that the Windows firewall is on.

3.5.1 Getting help

To get basic help on nmap switches type **nmap** without any switches.

nmap

- Get detailed help by typing,

nmap --help

3.5.2 NMAP full connect (vanilla) scanning exercises

- Run an nmap **vanilla** scan against your main Windows desktop (i.e. 127.0.01)
- Now run an nmap **vanilla** scan against **Server1** (i.e. 192.168.10.1).

Note that pressing SPACEBAR during a scan will show the progress.

What ports are being scanned? The default is 1-1025 and every **registered** higher port.

- Open the file **C:\Program Files (x86)\Nmap\nmap-services** in notepad (or notepad++) to see the ports that are being scanned by nmap by default.
- Now do a vanilla scan against **192.168.10.1 but only check port 80** (it should be **open** meaning that a web server is running). Note that the -p switch allows us to specify a specific port (or ports).

- From your Windows desktop, use a browser to prove that it is a web server that is actually running on this IP address (i.e. browse to **http://192.168.10.1** using the browser).

Note: -

NMAP will first ping a machine to see if it is on. A commonly used switch by pen testers is **-pN** which means that nmap will not ping first. This is for stealth reasons.

3.6 SYN SCANNING

A SYN scan only partially completes the three-way handshake. SYN scanning is deemed to be dangerous since leaving so many connections hanging can crash a target. This is highly unlikely with modern operating systems but IOT devices often have older operating systems and legacy operating systems are not that uncommon so care should be taken during a pen test not to crash these devices.

The following is a SYN scan against a Windows XP machine with the firewall off.

```
nmap -sS 192.168.10.21

Starting Nmap 4.68 ( http://nmap.org ) at 2008-08-12 11:00 GMT
Standard Time
Interesting ports on 192.168.10.10:
Not shown: 1712 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:01:6C:E2:D4:A7 (Foxconn)

Nmsap done: 1 IP address (1 host up) scanned in 1.157 seconds
```

For backward compatibility, Windows 2000 and subsequent Microsoft operating systems continue to support the original NetBIOS ports (135 and 137). But with Windows 2000 and beyond, Microsoft has moved their NetBIOS services to port 445. For reference, the following is a good article on NetBIOS.

http://www.windowsdevcenter.com/pub/a/windows/2004/05/11/netbios.html

3.6.1 SYN Scanning exercises

- Using nmap, run **SYN** scans against the virtual machines **192.168.10.1** and **192.168.10.2**

3.7 UDP SCANNING

UDP scanning sends a “dataless” UDP header to each port in the default list. The responses from this header are used to determine the UDP port status. nmap functions as following: -

- An ICMP Unreachable error response indicates that the port is closed
- Other ICMP errors indicate that the port is filtered
- UDP bases services (DHCP, DNS and SNMP) may respond. This indicates that the port is open.
- If after several attempts of communication no response is received, the port will be marked as open|filtered. This could mean that packet filtering may be blocking communication with an otherwise open port.

Note:

A penetration tester would normally script Nmap UDP scans since they are extremely slow.

- To illustrate the slow speed, run the following.

nmap -sU 192.168.10.1

- Let it run for a few seconds then **press the space bar** to see the progress (it is very slow!).

- After about 30 seconds, press **Ctrl/C** to exit the scan.

3.8 SOME USEFUL NMAP SWITCHES

The following are commonly used switches.

-h	Help summary
-v	Be verbose (i.e. tell us what you know)
-v -v	Be extremely verbose (i.e. tell us everything you know)
-n	Don't do DNS reverse lookup (i.e. don't try to convert IP address to a name). This can increase the speed of scans
-T	These allow us to control the speed of the scan. The possible values are - paranoid (0)|sneaky (1)|polite (2)|normal (3)|aggressive (4) |insane (5). Eg. T paranoid or T 0
-p *ports*	-p 80 (web server port) -p 1-80 (try ports 1-80) -p 1-65535 (try all ports)
-o	Output to a file :- oN normal output e.g. -oN myhost.txt oX xml output e.g. –oX myhost.xml oG "grepable". E.g. –oG myhost.gnmap oA output to all above formats e.g.-oA myfile

3.8.1 Exercise

- Run a **nmap UDP** scan against **ports 40-60** and be very verbose.

3.9 IDENTIFYING OPERATING SYSTEMS AND APPLICATIONS.

If you ran Nmap against a remote machine and it might tell you that ports 25/tcp, 80/tcp, and 53/udp are open. Using its nmap-services database of about 2,200 well-known services, Nmap would report that those ports probably correspond to a mail server (SMTP), web server (HTTP), and name server (DNS) respectively. This lookup is usually accurate although most services can be configured for any port. Nmap can also attempt to guess at the service version and operating system. E.g. It tries to tell whether a router is a Netgear or a Linksys or whether machine is running Windows or Linux.

The major switches used are : -

-sV	Enable version detection.
-O	Guess at the operating system
-A	Enables OS detection and Version detection, Script scanning and Traceroute. **Be careful, most times we don't want the script scanning because it tries active hacking attacks.**
--osscan-guess	When Nmap is unable to detect a perfect OS match, it sometimes offers up near-matches as possibilities. This option will guess more aggressively and is normally required to be in the command line as well as the O option.

A sample output against a home router is shown below : -

```
nmap -sS -sV -T5 192.168.10.1

Starting Nmap 4.68 ( http://nmap.org ) at 2008-08-09 14:11 GMT
Standard Time
Interesting ports on 192.168.10.1:
Not shown: 1713 closed ports
PORT     STATE SERVICE    VERSION
80/tcp   open  http       Netgear DG834G router http config
5190/tcp open  tcpwrapped
MAC Address: 00:0F:B5:A1:23:24 (Netgear)
Service Info: Device: router
```

Note: -

If you are trying to get the operating system, it is normal to use both **-O** and **--osscan-guess** in the command line.

3.10 OPERATING SYSTEM AND APPLICATION IDENTIFICATION EXERCISES

- **Ensure that Server2 is running.**

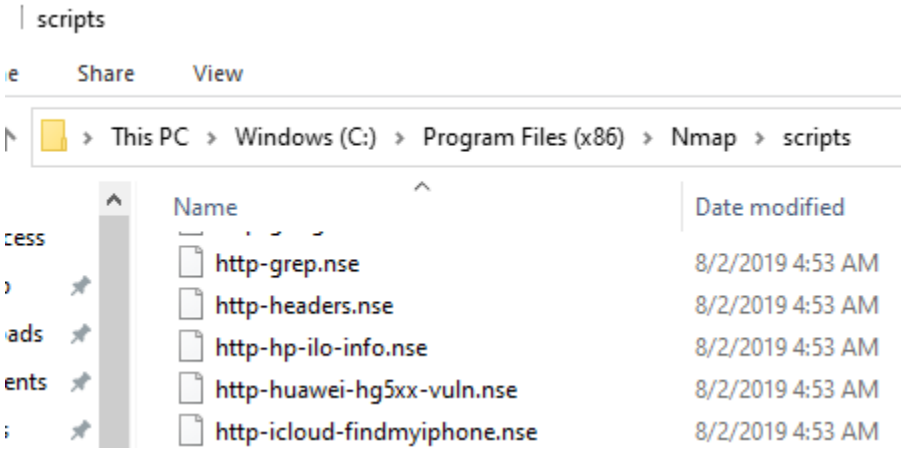
- In a single nmap command line, scan port 80 (web server port) on the virtual machine **192.168.10.2** (i.e. Server2) and also detect **the version** of the web Server that is running.

- Use the **-O** and **--osscan-guess** switches to detect the operating system that is running on **Server2** virtual machine (**this will illustrate the issues involved in detecting modern operating systems**).

3.11 NMAP SCRIPTS

The Nmap Scripting Engine (NSE) is one of Nmap's most powerful and flexible features. It allows users to write (and share) simple scripts (using the Lua programming language) to automate a wide variety of networking tasks. Those scripts are executed in parallel with the speed and efficiency you expect from Nmap. Users can rely on the growing and diverse set of scripts distributed with Nmap, or write their own to meet custom needs.

- Have a look at the available nmap scripts held in the folder "**C:\Program Files (x86)\Nmap\scripts**".



To run the script, use the syntax

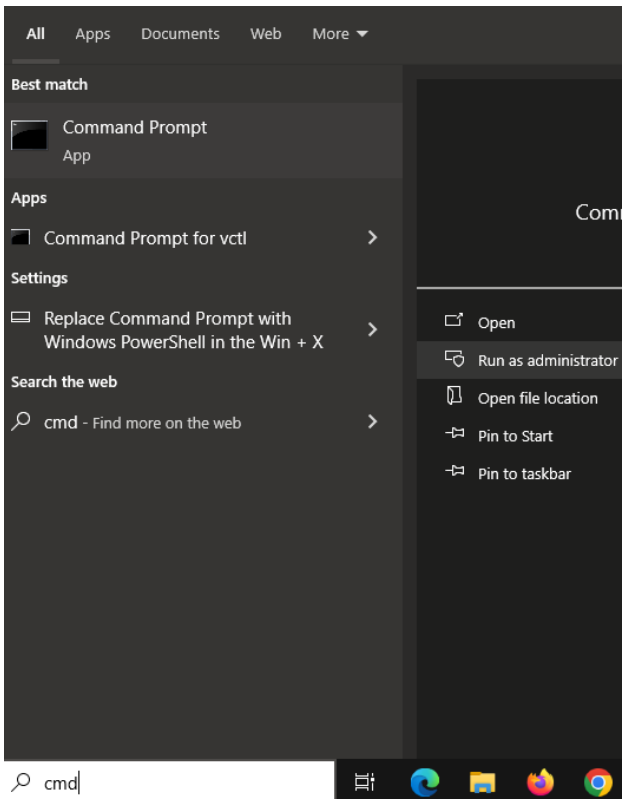
nmap --script *scriptname target*

For example, run the following from a command prompt. You should see the web server banners.

```
C:\>nmap --script http-headers 192.168.10.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-08-17 10:23 GMT
Nmap scan report for 192.168.10.1
Host is up (0.00073s latency).
Not shown: 981 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
53/tcp   open  domain
79/tcp   open  finger
80/tcp   open  http
| http-headers:
|   Date: Tue, 17 Aug 2021 09:23:42 GMT
|   Server: Apache
|   X-Powered-By: PHP/5.6.30
|   Vary: User-Agent
|   Connection: close
|   Content-Type: text/html; charset=UTF-8
|
|_  (Request type: HEAD)
```

- Try the **smtp-commands** script against **192.168.10.1**

To update the scripts, you must **run a command prompt as administrator**



then type: -

nmap --script-updatedb

Nmap has a banner grabbing script, (note this can take a little time to run. Have patience!).

nmap -sV --script=banner 192.168.10.1

You should see all the open ports and all the banners that the script has found. Exam these.

To scan with a set of scripts,

nmap -sV --script=smb* 192.168.10.1

To Gather page titles from HTTP services from the subnet,

nmap --script=http-title 192.168.10.1

Find web apps from known paths on the subnet,

nmap --script=http-enum 192.168.10.0/24

There are many scripts that are simple but helpful when examining larger networks. Note the many of these scripts are particularly noisy and can crash services and systems. Some scripts will actively attempt hacks which is often undesirable. A pen tester would normally not “blanket” run a set of scripts.

To scan using default safe scripts,

nmap -sV -sC 192.168.10.1

Note that there is an excellent tutorial on nmap scripts here: -

https://www.tecmint.com/use-nmap-script-engine-nse-scripts-in-linux/

3.12 ABOUT NMAP FIN, NULL AND XMAS TREE SCANS (NO PRACTICAL)

The main advantage to these scan types is that they can get through certain non-stateful firewalls and packet filtering routers. Such firewalls try to prevent incoming TCP connections (while allowing outbound ones) by blocking any TCP packets with the SYN bit set and ACK cleared. The NULL, FIN, and Xmas scans clear the SYN bit and thus bypasses those rules.

Another advantage is that these scan types are “more stealthy”. However, most modern IDS products can be configured to detect them. For information, The flags are:-

FIN scan (-sF)

Null scan (-sN)

Xmas scan (-sX)

In our case, there is no advantage in running them but it useful to know that they can be used.

- You may wish to try these on the virtual machines.

3.13 ABOUT NMAP IDLE SCANS (NO PRACTICAL)

The following examples skips host discovery and instructs an idle Scan using the IP 192.168.10.100 as the zombie device to scan ports 80, 21 and 20 of the target 192.168.10.1.

Note that this will NOT work in our case,

nmap -Pn -sI 192.168.10.100 -p 80,21,20 192.168.10.1

For the attack to work, the zombie device must be running an operating system that uses a predictable IPID sequence. Modern Windows, Solaris and Linux are two operating systems that are not vulnerable to this type of behaviour. i.e. they can’t be used since it doesn’t increment.

4 BATCH SCRIPTING AN ENTIRE NETWORK SCAN

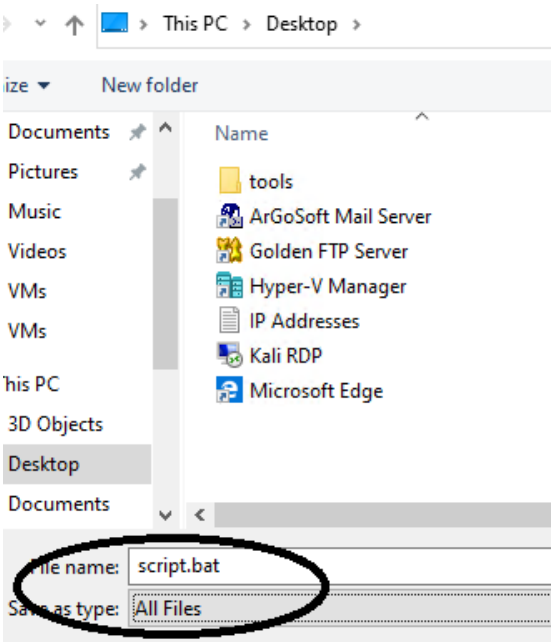
In the real situation, a penetration tester will have many machines to scan. In this case, it is preferable to automate the scans using a script. Nmaps scans are very slow to run so to save time, we will only scan the **first 10000 ports** (in the real case, all ports 1-65535 should be scanned). For your coursework, you would probably want to use a similar script.

Before running the script, ensure that you have Server1 and Server2 on!

- Under Windows, **run notepad**
- Now create the following file.

```
nmap -sT -p 1-10000 -v -v -T5 -sV -O --osscan-guess --script=banner -oN 192.168.10.1TCP.txt 192.168.10.1
nmap -sU -p 1-500 -v -v --scan-delay 1s -sV --script=banner -oN 192.168.10.1UDP.txt 192.168.10.1
nmap -sT -p 1-10000 -v -v -T5 -sV -O --osscan-guess --script=banner -oN 192.168.10.2TCP.txt 192.168.10.2
nmap -sU -p 1-500 -v -v --scan-delay 1s -sV --script=banner -oN 192.168.10.2UDP.txt 192.168.10.2
```

- Save the file on your desktop as **script.bat** (you will need to choose **All Files** in the **Save as type). See below.**



- From a command prompt in the Desktop folder, run the nmap script using the following: -

script.bat

You may want to ensure that you understand each of the switches in the script.

This will take some time to run (**This took approx 35 mins in room 4511 in September 2023**) so you may wish to have a break while it runs.

After a while, you should see the nmap text output files appear on your desktop as the script runs.

- **Open and examine the contents of the created files using notepad.**

Note: - Save these files for later use and analysis.

4.1 ANALYSING THE SCAN RESULTS

Note that every scan will be different and in the real case, you would have to research any open ports and protocols that you have not come across before.

We will analyse what our script output means next week but think about the following: -

- What services are running that you recognize?
- What ports are giving banners?
- What are the operating systems?
- What web servers are running and on what ports?
- What is the domain name of the machine?
- Are any of the machines running a DNS Server?
- You will find services and versions. In the real case, we would Google for their exploitability.

5 OPTIONAL EXERCISES

5.1 MASSCAN

Masscan is installed under Kali linux and is reported to be the fastest Internet port scanner. It produces results similar to nmap, but uses asynchronous transmission. Masscan uses a custom TCP/IP stack.

Under Azure, anything other than simple port scans will cause conflict with the local TCP/IP stack.

- There is a good video demo at https://www.youtube.com/watch?v=mJTLlfCjTxg&ab_channel=AlpineSecurity and an Excellent Tutorial at https://securitytrails.com/blog/masscan

Note that the following commands do not work under Azure but it is good to be aware of masscan.

The following shows how to specify TCP ports and UDP ports

sudo masscan -p 1-1000 192.168.10.1
sudo masscan -p U:1-1000 192.168.10.1

To get banners, use the –banners switch: -

sudo masscan -p80 --banners 192.168.10.1

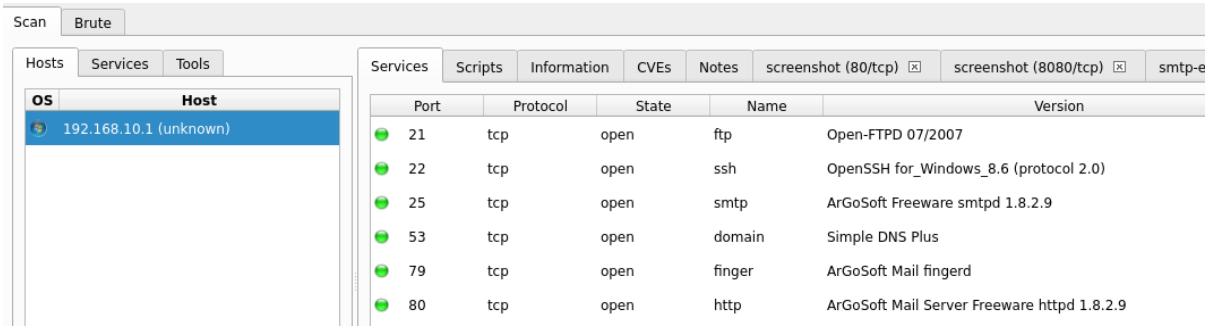
Reference: - https://tools.kali.org/information-gathering/masscan

5.2 LEGION

Legion is a tool within Kali Linux that uses several different packages to both scan and grab banners.

sudo legion

This tool is worth looking at. It gives a lot of information regarding banners. It also screenshots ant web pages that are found. It also does several other things such as password cracking. It takes a while to run.



5.3 NMAP AT AN INTERVIEW.

NMAP is such a commonly used pen testing tool that questions on its usage normally crop up at an interview. The following are common questions that have been compiled. **If you think that you would be interested in going for a pen testing job in the future, you should attempt these research exercises.**

There are also lots of NMAP cheatsheets that you can refer to e.g. https://www.stationx.net/nmap-cheat-sheet/

Source for answers to the following questions : - https://allabouttesting.org/most-asked-nmap-interview-questions-asked-by-big-companies/

Q1. Write a ping scan command in Nmap.

Q2. Write a Nmap command to scan targets from a file.

Q3. How to write Nmap command for specific ports and services?

Q4. How to scan a target using default scripts?

Q5. How to scan a target using a TCP SYN scan? List out advantages for the same.

Q7. How to scan a target from a specific interface?

Q8. How to scan a target using a UDP scan? List out advantages for the same.

Q9. How to write a Nmap script to scan a target for service detection?

Q10. How to exclude specific IPs from the range of IP or whole subnet of IP?

Q11. Write nmap query for OS detection.

Q12. How to write a Nmap script to scan the target for version detection?

Q13. Explain the Aggresive Detection command in Nmap.

Q14.How do you update the Nmap script database on your local computer?

Q15. Write the Nmap script for the ping scan using UDP.

Q16. How to write a Nmap script to spoof Mac Address of attacker?

Q17. Write Nmap command to scan IPv6 target.

Q18. Write a Nmap command to extract whois information.

Q19. Write a command to print a summary while sending and receiving every packet.

Q20. List out command options of Nmap for Firewall/IDS Evasion and Spoofing.

5.4 PORT NUMBERS AT AN INTERVIEW.

A typical pen tester interview will involve questions about ports and port numbers. The following are sample questions.

Q. What Is a Port Number?

A port number is part of the addressing information used to identify the senders and receivers of messages. Port numbers are most commonly used with TCP/IP connections. Home network routers and computer software work with ports and sometimes allow you to configure port number settings. These port numbers allow different applications on the same computer to share network resources simultaneously.

Q. What is the range of ports or how many ports are there?

Port numbers can vary from 0 to 65535.

Q. Why are port numbers just up to 65536?

This is because limitation in TCP/IP stacks where the port field is just 16bit size. So we get 2^16 ports which is equal to 65536.

Q. What are the well-known ports?

Well known ports are from 0 to 1023(total 2^10=1024 ports)

Q. What are the Registered Ports (Range: 1024 to 49151)

These are commonly used by a specific service such as Oracle database listener (1521), MySql (3306), Microsoft Terminal server (3389) etc.

Q. What are the Dynamic and/or Private Ports. (Range: 49152 to 65535)

These ports can't be registered by IANA. This is used for custom or temporary purposes and for automatic allocation of short-lived (or ephemeral) ports which is used internally by application/processes.

Q. What is meant by default port?

A default port is a designated port for particular well-known service.

Q. Can we change default port for a service(example Apache, squid)?

Yes. It is normally a configuration setting.

Q. How would find out which ports are open?

netstat -an|more

Specific port numbers are often asked. Here are some important port numbers to remember.

20-FTP Data (For transferring FTP data)

21-FTP Control (For starting FTP connection)

22-SSH (For secure remote administration which uses SSL to encrypt the transmission)

23-Telnet (For insecure remote administration

25-SMTP (Mail Transfer Agent for e-mail server such as SEND mail)

53- DNS (Special service which uses both TCP and UDP)

68-DHCP

69-TFTP (Trivial file transfer protocol uses udp protocol for connection less transmission of data)

80 -HTTP/WWW (apache)

88-Kerberos

110-POP3 (Mail delivery Agent)

123-NTP (Network time protocol used for time syncing uses UDP protocol)

137-NetBIOS (nmbd)

139,138,445-SMB-Samba (smbd)

143-IMAP

161-SNMP (For network monitoring)

389-LDAP (For centralized administration)

443-HTTPS (HTTP+SSL for secure web access)

5.5 CREATING HTML REPORTS FROM NMAP

https://securityboulevard.com/2021/01/converting-nmap-xml-files-to-html-with-xsltproc/

5.6 EVADING FIREWALLS USING NMAP.

Nmap has a large range of uses depending on the situation. One example is Firewall evasion

https://nmap.org/book/man-bypass-firewalls-ids.html