

CyberHost Internship Assignment 1

Name : George David D

Assignment 1 : Nmap

Date : 05/09/23

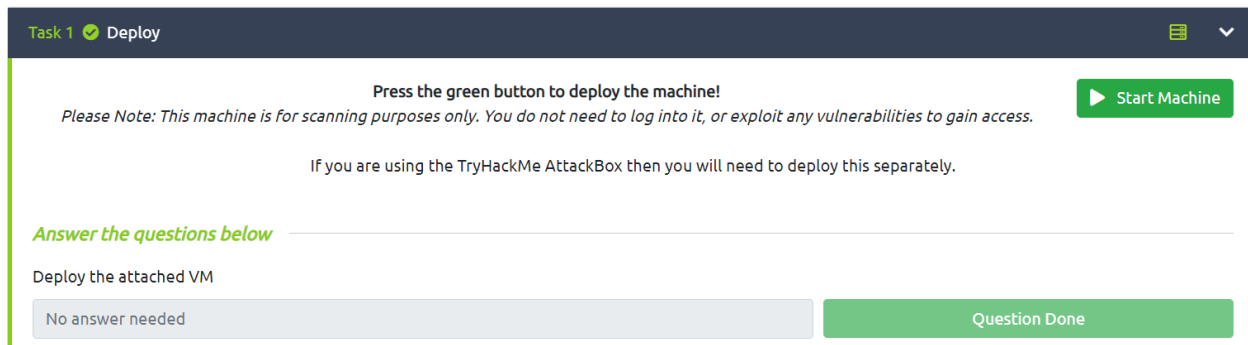
What is Nmap?

Nmap is a network analyzing tool. It is a short form of Network mapper; it is an open-source tool for scanning the network to find open ports for security audits its available in cross-platforms such as Windows (Zenmap GUI) and Linux distributions.

What are Ports?

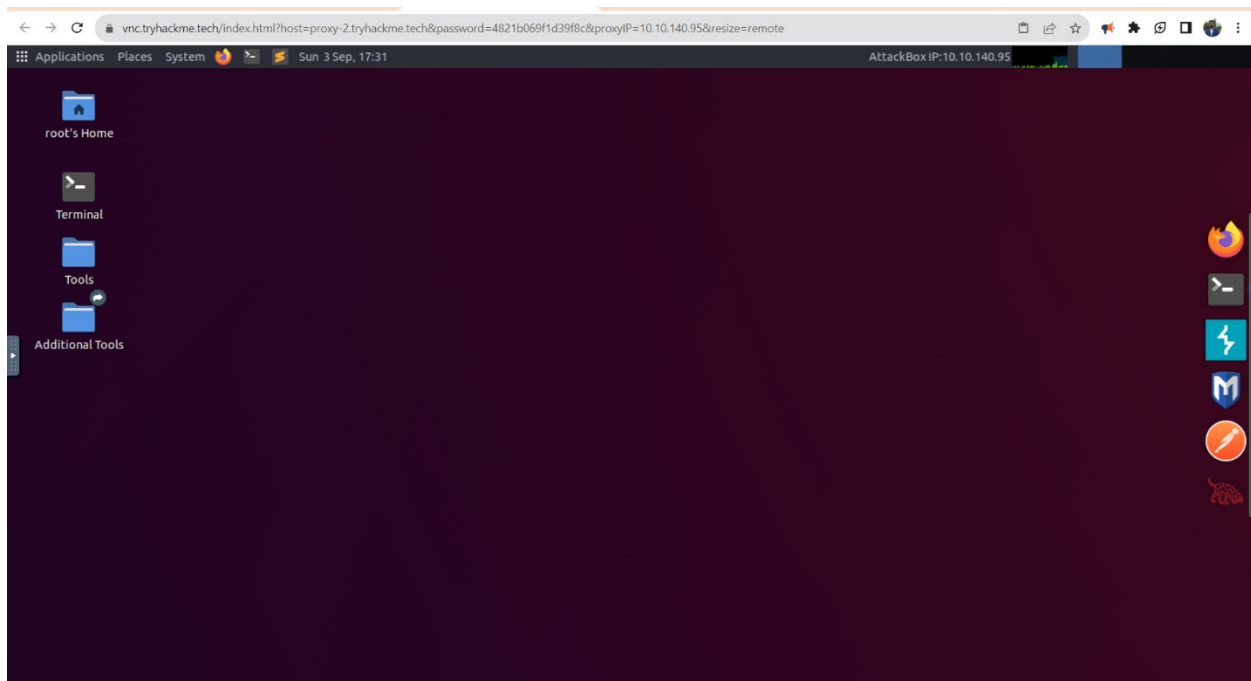
Port numbers are specific numbers in networking to route network traffic to specific processes within the network

Task 1-Deploy



The screenshot shows a task interface with a dark header bar containing 'Task 1' with a green checkmark and the word 'Deploy'. Below the header, there is a green button labeled 'Start Machine' with a play icon. A note states: 'Please Note: This machine is for scanning purposes only. You do not need to log into it, or exploit any vulnerabilities to gain access.' Below this, it says 'If you are using the TryHackMe AttackBox then you will need to deploy this separately.' A section titled 'Answer the questions below' contains a question 'Deploy the attached VM'. Below the question are two buttons: a grey one labeled 'No answer needed' and a green one labeled 'Question Done'.

1. First, I joined the room
2. Then I clicked to start the machine and start the attack box button.
3. It will open a browser-based Linux operating system



Task 2- Introduction

I am using my machine's IP address as a target IP. The first step of gathering data on the machine is to find out what services are running on the machine. do this by scanning its ports. A machine needs to have certain ports open to run certain services, and by scanning its ports can figure out which services it runs by looking at which ports are open. Every computer has 65535 available ports, of which many are registered as standard ports. HTTP for example, runs on port 80, while HTTPS runs on port 443.

Nmap is a tool that provides us with the power to do quick and efficient port scanning.

Answer the questions below

What networking constructs are used to direct traffic to the right application on a server?

Ports

How many of these are available on any network-enabled computer?

65535

How many of these are considered "well-known"? (These are the "standard" numbers mentioned in the task)

1024

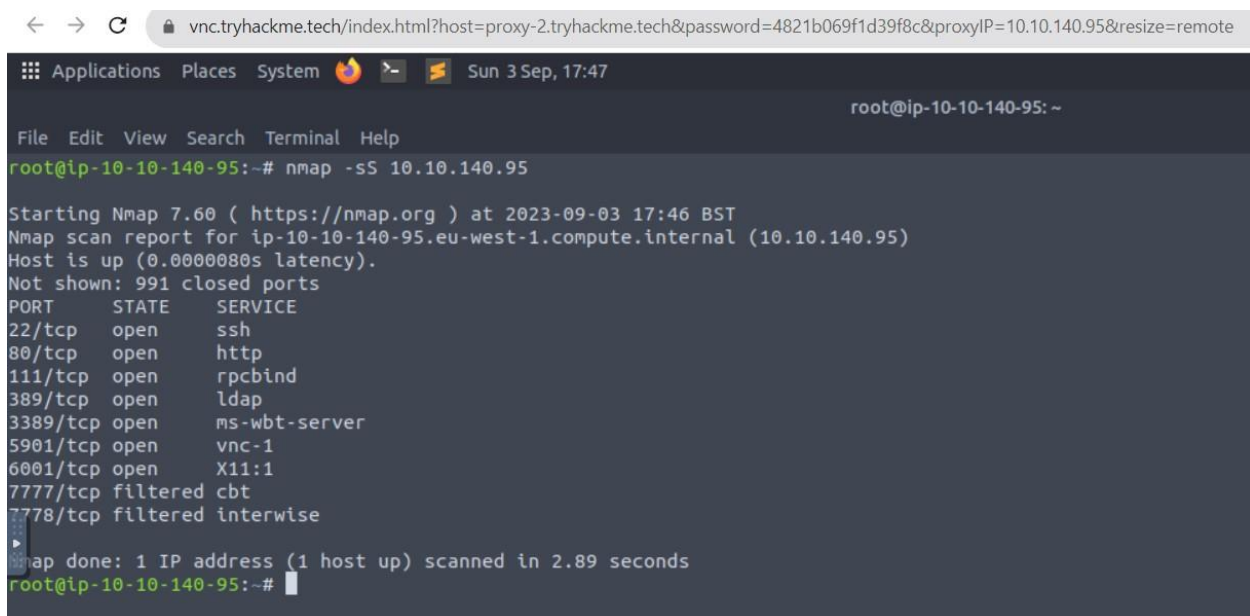
Task-3 network switches

Nmap -h or man Nmap This command is used to know about Nmap commands.

Answer the questions below

What is the first switch listed in the help menu for a 'Syn Scan' (more on this later!)?

-sS



The screenshot shows a terminal window with the following content:

```
← → ↻ vnc.tryhackme.tech/index.html?host=proxy-2.tryhackme.tech&password=4821b069f1d39f8c&proxyIP=10.10.140.95&resize=remote
Applications Places System Sun 3 Sep, 17:47
root@ip-10-10-140-95: ~
File Edit View Search Terminal Help
root@ip-10-10-140-95:~# nmap -sS 10.10.140.95

Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-03 17:46 BST
Nmap scan report for ip-10-10-140-95.eu-west-1.compute.internal (10.10.140.95)
Host is up (0.0000080s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
389/tcp   open  ldap
3389/tcp  open  ms-wbt-server
5901/tcp  open  vnc-1
6001/tcp  open  X11:1
7777/tcp  filtered cbt
7778/tcp  filtered interwise

Nmap done: 1 IP address (1 host up) scanned in 2.89 seconds
root@ip-10-10-140-95:~#
```

Which switch would you use for a "UDP scan"?

-sU

```
← → ↻ vnc.tryhackme.tech/index.html?host=proxy-2.tryhackme.tech&password=4821b069f1d39f8c&proxyIP=10.10.140.95&resize=remote

Applications Places System 🔥 🖱️ 🚪 Sun 3 Sep, 17:50

root@ip-10-10-140-95: ~

File Edit View Search Terminal Help

root@ip-10-10-140-95:~# nmap -sU 10.10.140.95

Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-03 17:49 BST
Nmap scan report for ip-10-10-140-95.eu-west-1.compute.internal (10.10.140.95)
Host is up (0.0000090s latency).
Not shown: 996 closed ports
PORT      STATE      SERVICE
68/udp    open|filtered dhcpc
111/udp   open       rpcbind
631/udp   open|filtered ipp
5353/udp  open|filtered zeroconf

Nmap done: 1 IP address (1 host up) scanned in 2.77 seconds
root@ip-10-10-140-95:~#
```

If you wanted to detect which operating system the target is running on, which switch would you use?

-sO

```
← → ↻ vnc.tryhackme.tech/index.html?host=proxy-2.tryhackme.tech&password=4821b069f1d39f8c&proxyIP=10.10.140.95

Applications Places System 🔥 🖱️ 🚪 Sun 3 Sep, 17:51

root@ip-10-10-140-95: ~

File Edit View Search Terminal Help

root@ip-10-10-140-95:~# nmap -sO 10.10.140.95

Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-03 17:51 BST
Nmap scan report for ip-10-10-140-95.eu-west-1.compute.internal (10.10.140.95)
Host is up (0.000011s latency).
Not shown: 249 closed protocols
PROTOCOL STATE      SERVICE
1         open       icmp
2         open|filtered igmp
6         open       tcp
17        open       udp
103       open|filtered pim
136      open|filtered udplite
255      open|filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 2.72 seconds
root@ip-10-10-140-95:~#
```

Nmap provides a switch to detect the version of the services running on the target. What is this switch?

-sV

```
root@lp-10-10-140-95:~# nmap -v 10.10.140.95
```

```
Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-03 17:53 BST
Nmap scan report for lp-10-10-140-95.eu-west-1.compute.internal (10.10.140.95)
Host is up (0.0000080s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh            OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http           WebSockify Python/3.6.9
111/tcp   open  rpcbind       2-4 (RPC #100000)
389/tcp   open  ldap          OpenLDAP 2.2.X - 2.3.X
3389/tcp   open  ms-wbt-server xrdp
5901/tcp   open  vnc            VNC (protocol 3.8)
6001/tcp   open  X11            (access denied)
77/tcp    filtered cbt
78/tcp    filtered interwise
Service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
_
SFPort80-BCP:V=7.60XI=7ND=9/3KTime=64F4BA0FNP=x86_64-pc-linux-gnuXr(GetRe
SF:=quest,290,"HTTP/1.1|x20405|x20Method|x20Allowed|xnServer|x20W
SF:=ebSockify|x20Python/3|.6|.9|r|nDate:x20Sun,x2003|x20Sep|x2020z|x2016
SF:=f:rsst|x20ContentLength|x20content-Type|x20text/html;ch
SF:=set=utf-8|n|nContent-Length:x20472|n|n|n-IDOCTYPE|x20HTML|x20PUBLIC
SF:=x20"-//W3C/DTD/x20HTML|x204.01/EH|n|x20|x20|x20|x20|x20|x20|x20
SF:=x20"/www.w3.org/TR/html4/strict.dtd">|n<html>|n|x20|x20|x20
SF:=x20<head>|n|x20|x20|x20|x20|x20|x20|x20<xmeta>|x20http-equiv="Conten
SF:=Type"|x20content="text/html;charset=utf-8">|n|x20|x20|x20|x20|x20
SF:=x20|x20<title>Error|x20response</title>|n|x20|x20|x20|x20</head>|n
SF:=x20|x20|x20|x20<body>|n|x20|x20|x20|x20|x20|x20|x20<h1>Error|x20res
SF:=ponse</h1>|n|x20|x20|x20|x20|x20|x20|x20<p>Error|x20code:x20405</p
SF:=|n|x20|x20|x20|x20|x20|x20|x20|x20<p>Message:x20Method|x20Not|x20Allo
SF:=wed.</><p/>|n|x20|x20|x20|x20|x20|x20|x20<p>Error|x20code|x20explanat
SF:=ion:x20405|x20->x20specified|x20method|x20is|x20invalid|x20for|x20this
SF:=x20resource</><p/>|n|x20|x20|x20|x20</body><n</html>|n")%r(HTTPOptions,
SF:=2B8,"HTTP/1.1|x20501|x20Unsupported|x20method|x20('OPTIONS'|)|r)nServ
SF:=er:x20WebSockify|x20Python/3|.6|.9|r|nDate:x20Sun,x2003|x20Sep|x2020
SF:=23|x2016:53:35|x20GMT|nConnection:x20Close|nContent-Type:x20text/
```

The default output provided by Nmap often does not provide enough information for a pen tester. How would you increase the verbosity?

-v

```
vnc.tryhackme.tech/index.html?host=proxy-2.tryhackme.tech&password=4821b069f1d39f8c&proxyIP=10.10.140.95&resize=remote
Applications  Places  System  Sun 3 Sep, 17:58  root@ip-10-10-140-95: ~

File Edit View Search Terminal Help

root@ip-10-10-140-95:~# nmap -sU -v 10.10.140.95

Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-03 17:57 BST
Initiating Parallel DNS resolution of 1 host. at 17:57
Completed Parallel DNS resolution of 1 host. at 17:57, 0.00s elapsed
Initiating UDP Scan at 17:57
Scanning ip-10-10-140-95.eu-west-1.compute.internal (10.10.140.95) [1000 ports]
Discovered open port 111/udp on 10.10.140.95
Completed UDP Scan at 17:57, 2.68s elapsed (1000 total ports)
Nmap scan report for ip-10-10-140-95.eu-west-1.compute.internal (10.10.140.95)
Host is up (0.0000080s latency).
Not shown: 996 closed ports
PORT      STATE      SERVICE
8/udp     open|filtered dhcpc
111/udp   open       rpcbind
631/udp   open|filtered ipp
653/udp   open|filtered zeroconf

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.78 seconds
Raw packets sent: 1072 (31.032KB) | Rcvd: 2136 (91.484KB)

root@ip-10-10-140-95:~#
```

Verbosity level one is good, but verbosity level two is better! How would you set the verbosity level to two?

-vv

```
vnc.tryhackme.tech/index.html?host=proxy-2.tryhackme.tech&password=4821b069f1d39f8c&proxyIP=10.10.140.95&resize=remote
Applications Places System Sun 3 Sep, 18:03
root@ip-10-10-140-95: ~
File Edit View Search Terminal Help
root@ip-10-10-140-95:~# nmap -sU -vv 10.10.140.95

Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-03 17:59 BST
Initiating Parallel DNS resolution of 1 host. at 17:59
Completed Parallel DNS resolution of 1 host. at 17:59, 0.00s elapsed
Initiating UDP Scan at 17:59
Scanning ip-10-10-140-95.eu-west-1.compute.internal (10.10.140.95) [1000 ports]
Increasing send delay for 10.10.140.95 from 0 to 50 due to 33 out of 108 dropped probes since last increase.
Increasing send delay for 10.10.140.95 from 50 to 100 due to 11 out of 35 dropped probes since last increase.
Increasing send delay for 10.10.140.95 from 100 to 200 due to 11 out of 22 dropped probes since last increase.
Discovered open port 111/udp on 10.10.140.95
UDP Scan Timing: About 22.82% done; ETC: 18:02 (0:01:45 remaining)
UDP Scan Timing: About 47.88% done; ETC: 18:02 (0:01:29 remaining)
UDP Scan Timing: About 62.70% done; ETC: 18:02 (0:01:07 remaining)
UDP Scan Timing: About 77.18% done; ETC: 18:02 (0:00:42 remaining)
Completed UDP Scan at 18:03, 192.02s elapsed (1000 total ports)
Nmap scan report for ip-10-10-140-95.eu-west-1.compute.internal (10.10.140.95)
Host is up, received localhost-response (0.000064s latency).
Scanned at 2023-09-03 17:59:54 BST for 192s
Not shown: 996 closed ports
Reason: 996 port-unreaches
PORT      STATE      SERVICE    REASON
68/udp    open|filtered dhcpc      no-response
111/udp   open       rpcbind    udp-response ttl 64
631/udp   open|filtered ipp        no-response
5353/udp  open|filtered zeroconf   no-response

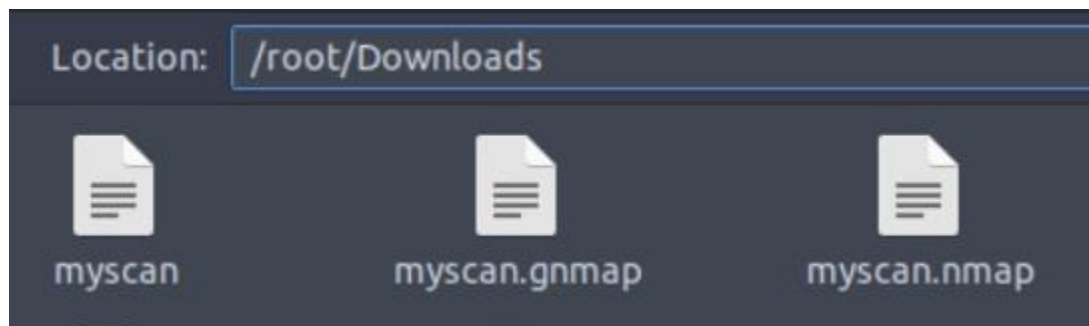
Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 192.10 seconds
Raw packets sent: 1093 (31.714KB) | Rcvd: 2175 (93.222KB)
root@ip-10-10-140-95:~#
```

What switch would you use to save the Nmap results in three major formats?

-oA

```
root@ip-10-10-140-95:~# nmap -oA /root/Downloads/myscan

Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-03 18:16 BST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.05 seconds
root@ip-10-10-140-95:~#
```

```
File Edit View Search Tools Documents Help
myscan.xml x
1 <?xml version='1.0' encoding='UTF-8' ?>
2 <!DOCTYPE nmaprun>
3 <?xml-stylesheet href='file:///usr/bin/.:/share/nmap/nmap.xsl' type='text/xsl'?>
4 <!-- Nmap 7.60 scan initiated Sun Sep  3 18:10:04 2023 as: nmap -oA /root/Downloads/myscan --
5 <nmaprun scanners='nmap' args='nmap -oA /root/Downloads/myscan' start='189161864' startstr='Sun Sep  3 18:10:04 2023' version='7.60' xmloutputversion='1.04'>
6 <scaninfo type='syn' protocol='tcp' numservices='1000'
  services='1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,135,139,143-144,146,161,163,179,199,211-212,222,254-256,259,264,
  >
7 <verbose level='0' />
8 <debugging level='0' />
9 <runstats><finished time='189161864' timestr='Sun Sep  3 18:10:04 2023' elapsed='0.00' summary='Nmap done at Sun Sep  3 18:10:04 2023; 0 IP addresses (0 hosts up)
  scanned in 0.00 seconds' exit='success' /><hosts up='0' down='0' total='0' />
10 </runstats>
11 </nmaprun>
```

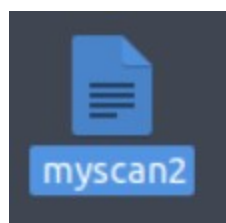
What switch would you use to save the nmap results in a “normal” format?

-oN

```
myscan1 x
1 # Nmap 7.60 scan initiated Sun Sep  3 18:21:55 2023 as: nmap -oN /root/Downloads/myscan1
2 WARNING: No targets were specified, so 0 hosts scanned.
3 # Nmap done at Sun Sep  3 18:21:55 2023 -- 0 IP addresses (0 hosts up) scanned in 0.05 seconds
```

A very useful output format: how would you save results in a “grepable” format?

-oG



If we don't care about how loud we are, we can enable "aggressive" mode. This is a shorthand switch that activates service detection, operating system detection, a traceroute and common script scanning. How would you activate this setting?

-A

```
Applications Places System Mon 4 Sep, 11:20
root@ip-10-10-169-123: ~
File Edit View Search Terminal Help
root@ip-10-10-169-123:~# nmap -A 10.10.169.123

Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-04 11:16 BST
Nmap scan report for ip-10-10-169-123.eu-west-1.compute.internal (10.10.169.123)
Host is up (0.0000080s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:
  2048 3d:51:f2:f2:68:2a:5c:27:46:fd:f6:f0:a9:38:27 (RSA)
  256 63:de:38:2a:d8:f0:66:87:fe:ce:76:7a:94:59:7d:10 (ECDSA)
  256 32:d4:01:22:15:e6:bb:01:2f:51:60:04:f8:3d:60:7f (EdDSA)
80/tcp    open  http         WebSockify Python/3.6.9
fingerprint-strings:
  GetRequest:
    HTTP/1.1 405 Method Not Allowed
    Server: WebSockify Python/3.6.9
    Date: Mon, 04 Sep 2023 10:17:01 GMT
    Connection: close
    Content-Type: text/html; charset=utf-8
    Content-Length: 472
    <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
    "http://www.w3.org/TR/html4/strict.dtd">
    <html>
    <head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
    <title>Error response</title>
    </head>
    <body>
    <h1>Error response</h1>
    <p>Error code: 405</p>
    <p>Message: Method Not Allowed.</p>
    <p>Error code explanation: 405 - Specified method is invalid for this resource.</p>
    </body>
    </html>
  HTTPOptions:
    HTTP/1.1 501 Unsupported method ('OPTIONS')
    Server: WebSockify Python/3.6.9
    Date: Mon, 04 Sep 2023 10:17:01 GMT
```

Nmap offers five levels of "timing" templates. These are essentially used to increase the speed of your scan runs at. How would you set the timing template to level 5?

-T5

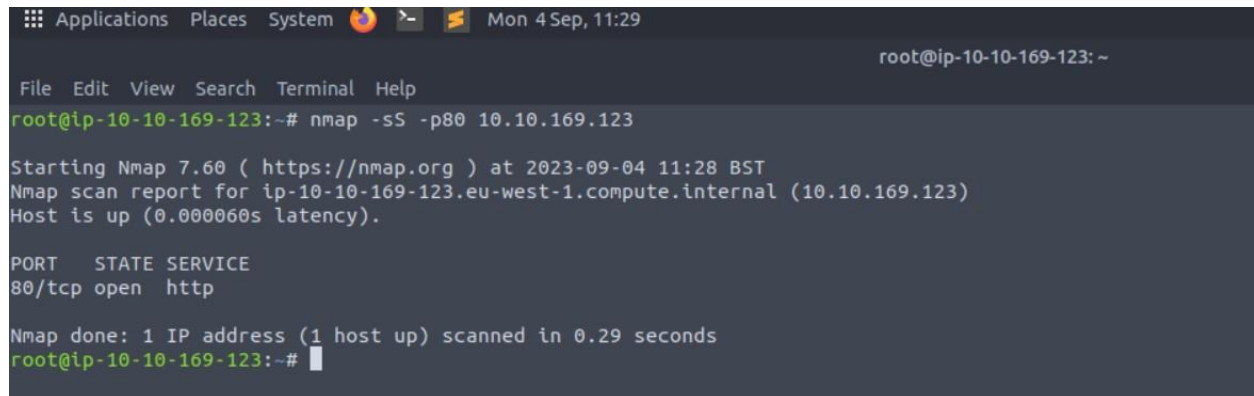
```
root@ip-10-10-169-123:~# nmap -sU -T5 10.10.169.123

Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-04 11:26 BST
Nmap scan report for ip-10-10-169-123.eu-west-1.compute.internal (10.10.169.123)
Host is up (0.0000080s latency).
Not shown: 930 closed ports, 69 open|filtered ports
PORT      STATE SERVICE
111/udp   open  rpcbind

Nmap done: 1 IP address (1 host up) scanned in 1.51 seconds
root@ip-10-10-169-123:~#
```


We can also choose which port(s) to scan. How would you tell Nmap to only scan port 80?

-p 80

A terminal window with a dark background and light text. The title bar shows 'Applications Places System' and the date 'Mon 4 Sep, 11:29'. The prompt is 'root@ip-10-10-169-123: ~'. The command 'nmap -sS -p80 10.10.169.123' is entered. The output shows 'Starting Nmap 7.60 (https://nmap.org) at 2023-09-04 11:28 BST', 'Nmap scan report for ip-10-10-169-123.eu-west-1.compute.internal (10.10.169.123)', 'Host is up (0.000060s latency).', and a table with columns 'PORT', 'STATE', and 'SERVICE' showing '80/tcp open http'. It concludes with 'Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds' and returns to the prompt.

```
Applications Places System Mon 4 Sep, 11:29 root@ip-10-10-169-123: ~
File Edit View Search Terminal Help
root@ip-10-10-169-123:~# nmap -sS -p80 10.10.169.123

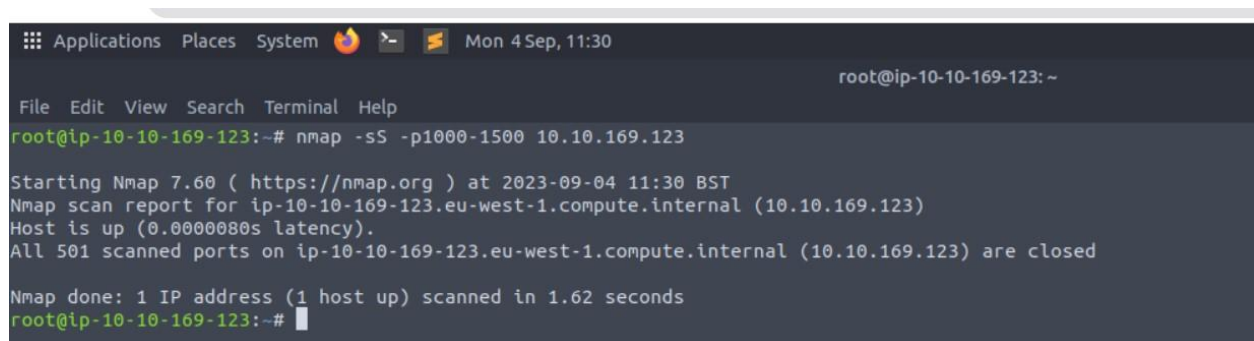
Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-04 11:28 BST
Nmap scan report for ip-10-10-169-123.eu-west-1.compute.internal (10.10.169.123)
Host is up (0.000060s latency).

PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
root@ip-10-10-169-123:~#
```

How would you tell Nmap to scan ports 1000–1500?

-p 1000–1500

A terminal window with a dark background and light text. The title bar shows 'Applications Places System' and the date 'Mon 4 Sep, 11:30'. The prompt is 'root@ip-10-10-169-123: ~'. The command 'nmap -sS -p1000-1500 10.10.169.123' is entered. The output shows 'Starting Nmap 7.60 (https://nmap.org) at 2023-09-04 11:30 BST', 'Nmap scan report for ip-10-10-169-123.eu-west-1.compute.internal (10.10.169.123)', 'Host is up (0.000080s latency).', and 'All 501 scanned ports on ip-10-10-169-123.eu-west-1.compute.internal (10.10.169.123) are closed'. It concludes with 'Nmap done: 1 IP address (1 host up) scanned in 1.62 seconds' and returns to the prompt.

```
Applications Places System Mon 4 Sep, 11:30 root@ip-10-10-169-123: ~
File Edit View Search Terminal Help
root@ip-10-10-169-123:~# nmap -sS -p1000-1500 10.10.169.123

Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-04 11:30 BST
Nmap scan report for ip-10-10-169-123.eu-west-1.compute.internal (10.10.169.123)
Host is up (0.000080s latency).
All 501 scanned ports on ip-10-10-169-123.eu-west-1.compute.internal (10.10.169.123) are closed

Nmap done: 1 IP address (1 host up) scanned in 1.62 seconds
root@ip-10-10-169-123:~#
```

How would you tell Nmap to scan all ports?

-p-

```
Applications Places System Mon 4 Sep, 17:24 root@ip-10-10-88-231: ~
File Edit View Search Terminal Help
root@ip-10-10-88-231:~# nmap -p- 10.10.88.231

Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-04 17:14 BST
Nmap scan report for ip-10-10-88-231.eu-west-1.compute.internal (10.10.88.231)
Host is up (0.000047s latency).
Not shown: 65526 closed ports
PORT      STATE      SERVICE
22/tcp    open      ssh
80/tcp    open      http
111/tcp   open      rpcbind
389/tcp   open      ldap
3389/tcp  open      ms-wbt-server
5901/tcp  open      vnc-1
6001/tcp  open      X11:1
7777/tcp  filtered  cbt
7878/tcp  filtered  interwise

Nmap done: 1 IP address (1 host up) scanned in 552.58 seconds
root@ip-10-10-88-231:~#
```

How would you activate a script from the Nmap scripting library (lots more on this later!)?

-- Script

```

root@ip-10-10-169-123:~# nmap -sV --script=banner 10.10.169.123

Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-04 11:50 BST
Nmap scan report for ip-10-10-169-123.eu-west-1.compute.internal (10.10.169.123)
Host is up (0.00000080s latency).
Not shown: 991 closed ports
PORT      STATE      SERVICE      VERSION
22/tcp    open      ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
|_banner: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7
80/tcp    open      http         WebSockify Python/3.6.9
|_fingerprint-strings:
|   GetRequest:
|       HTTP/1.1 405 Method Not Allowed
|       Server: WebSockify Python/3.6.9
|       Date: Mon, 04 Sep 2023 10:50:07 GMT
|       Connection: close
|       Content-Type: text/html; charset=utf-8
|       Content-Length: 472
|       <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
|       "http://www.w3.org/TR/html4/strict.dtd">
|       <html>
|       <head>
|       <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
|       <title>Error response</title>
|       </head>
|       <body>
|       <h1>Error response</h1>
|       <p>Error code: 405</p>
|       <p>Message: Method Not Allowed.</p>
|       <p>Error code explanation: 405 - Specified method is invalid for this resource.</p>
|       </body>
|       </html>
|   HTTPOptions:
|       HTTP/1.1 501 Unsupported method ('OPTIONS')
|       Server: WebSockify Python/3.6.9
|       Date: Mon, 04 Sep 2023 10:50:07 GMT

```

How would you activate all of the scripts in the “vuln” category?

Answer: — script=vuln

```

root@ip-10-10-169-123:~# nmap -sS --script=vuln 10.10.169.123

```

Task 4 Scan Types — Overview

When port scanning with Nmap, there are three basic scan types. These are:

TCP Connect Scans (-sT)

```
File Edit View Search Terminal Help
root@ip-10-10-169-123:~# nmap -sT 10.10.169.123

Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-04 12:07 BST
Nmap scan report for ip-10-10-169-123.eu-west-1.compute.internal (10.10.169.123)
Host is up (0.00017s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp    open  rpcbind
389/tcp    open  ldap
3389/tcp   open  ms-wbt-server
5901/tcp   open  vnc-1
6001/tcp   open  X11:1
7777/tcp   open  cbt
7778/tcp   open  interwise

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
root@ip-10-10-169-123:~#
```

SYN “Half-open” Scans (-sS)

```
Applications Places System Mon 4 Sep, 12:08 root@ip-10-1
File Edit View Search Terminal Help
root@ip-10-10-169-123:~# nmap -sS 10.10.169.123

Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-04 12:08 BST
Nmap scan report for ip-10-10-169-123.eu-west-1.compute.internal (10.10.169.123)
Host is up (0.000028s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp    open  rpcbind
389/tcp    open  ldap
3389/tcp   open  ms-wbt-server
5901/tcp   open  vnc-1
6001/tcp   open  X11:1
7777/tcp   filtered cbt
7778/tcp   filtered interwise

Nmap done: 1 IP address (1 host up) scanned in 2.79 seconds
root@ip-10-10-169-123:~#
```

UDP Scans (-sU)

```
File Edit View Search Terminal Help
root@ip-10-10-169-123:~# nmap -sU 10.10.169.123

Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-04 12:09 BST
Nmap scan report for ip-10-10-169-123.eu-west-1.compute.internal (10.10.169.123)
Host is up (0.0000090s latency).
Not shown: 996 closed ports
PORT      STATE      SERVICE
68/udp    open|filtered dhcpc
111/udp   open          rpcbind
631/udp   open|filtered ipp
5353/udp  open|filtered zeroconf

Nmap done: 1 IP address (1 host up) scanned in 2.76 seconds
root@ip-10-10-169-123:~#
```

Additionally, there are several less common port scan types:

TCP Null Scans (-sN)

```
root@ip-10-10-169-123:~# nmap -sN 10.10.169.123

Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-04 12:12 BST
Nmap scan report for ip-10-10-169-123.eu-west-1.compute.internal (10.10.169.123)
Host is up (0.000037s latency).
Not shown: 991 closed ports
PORT      STATE      SERVICE
22/tcp    open|filtered ssh
80/tcp    open|filtered http
111/tcp   open|filtered rpcbind
389/tcp   open|filtered ldap
3389/tcp  open|filtered ms-wbt-server
5901/tcp  open|filtered vnc-1
6001/tcp  open|filtered X11:1
7777/tcp  open|filtered cbt
7778/tcp  open|filtered interwise

Nmap done: 1 IP address (1 host up) scanned in 95.82 seconds
root@ip-10-10-169-123:~#
```

TCP FIN Scans (-sF)


```
Applications Places System Mon 4 Sep, 12:17 root@ip-10-10-169-123

File Edit View Search Terminal Help
root@ip-10-10-169-123:~# nmap -sF 10.10.169.123

Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-04 12:15 BST
Nmap scan report for ip-10-10-169-123.eu-west-1.compute.internal (10.10.169.123)
Host is up (0.000039s latency).
Not shown: 991 closed ports
PORT      STATE      SERVICE
22/tcp    open|filtered ssh
80/tcp    open|filtered http
111/tcp   open|filtered rpcbind
389/tcp   open|filtered ldap
3389/tcp  open|filtered ms-wbt-server
5901/tcp  open|filtered vnc-1
6001/tcp  open|filtered X11:1
7777/tcp  open|filtered cbt
7778/tcp  open|filtered interwise

Nmap done: 1 IP address (1 host up) scanned in 95.41 seconds
root@ip-10-10-169-123:~#
```

TCP Xmas Scans (-sX)

```
File Edit View Search Terminal Help
root@ip-10-10-169-123:~# nmap -sX 10.10.169.123

Starting Nmap 7.60 ( https://nmap.org ) at 2023-09-04 12:18 BST
Nmap scan report for ip-10-10-169-123.eu-west-1.compute.internal (10.10.169.123)
Host is up (0.000036s latency).
Not shown: 991 closed ports
PORT      STATE      SERVICE
22/tcp    open|filtered ssh
80/tcp    open|filtered http
111/tcp   open|filtered rpcbind
389/tcp   open|filtered ldap
3389/tcp  open|filtered ms-wbt-server
5901/tcp  open|filtered vnc-1
6001/tcp  open|filtered X11:1
7777/tcp  open|filtered cbt
7778/tcp  open|filtered interwise

Nmap done: 1 IP address (1 host up) scanned in 93.95 seconds
root@ip-10-10-169-123:~#
```


Task 5 Scan Types — TCP Connect Scans

Questions

Which RFC defines the appropriate behavior for the TCP protocol?

RFC 793

If a port is closed, which flag should the server send back to indicate this?

RST

Task 6 (SYN Scans)

Syn scans are very similar to TCP Connect scans. SYN scans are often referred to as “half-open”, or “stealth” scans. The difference is that SYN scans do not perform a full three-way handshake in the sense that they send back a RST TCP package in the third step, instead of a ACK. This prevents that the server will repeatedly try to make the request.

This can have different advantages:

Avoids detection. Some older intrusion detection system are only looking for a full three-way handshake.

Avoids logging. Standard practice is to log a connection once it has been fully established.

Quicker. Because we do not bother to establish a full connection, we increase port scan speed.

There are also two disadvantages:

They require sudo permissions.

They can bring down unstable services.

Because of these strong advantages SYN scans are the default scan type.

Questions

There are two other names for a SYN scan, what are they?

Answer: Half-Open, Stealth

Can Nmap use a SYN scan without Sudo permissions (Y/N)?

Answer: N

Task 7 (UDP Scans)

While TCP connections have a state initiated with a three-way handshake, UDP are stateless. This means that UDP connection send packets to the target port with a hope that they arrive, but no guarantee. Due to being stateless, UDP connections are very quick, but make them difficult and slower to quick.

The switch for an Nmap UDP scan is -sU.

Since UDP scans are so slow it's usually good practice to run an Nmap scan with --top-ports <number> enabled. For example, scanning with `nmap -sU --top-ports 20 <target>`. Now only the 20 most common ports get scanned.

When sending a UDP packet to an open UDP port there should be no response. Nmap can in this case only conclude that the port is either open or filtered. It suspect that the port is open, but it could still be firewalled. If it does receive a response the port is marked as open, but this does not happen often. When a packet is sent to a closed UDP port, the target should respond with an ICMP (ping) packet containing a message that the port is unreachable.

Questions

If a UDP port doesn't respond to an Nmap scan, what will it be marked as?

Answer: open|filtered

When a UDP port is closed, by convention the target should send back a “port unreachable” message. Which protocol would it use to do so?

Answer: ICMP

Task 8 (NULL, FIN and Xmas)

NULL, FIN and Xmas TCP port scans are not used as commonly as the previously discussed port scan types. What these three scan types have in common are that they are even stealthier than a SYN scan.

As the name suggests, NULL scans (-sN) are when the TCP request is sent with no flags set at all. As per the RFC, the target host should respond with a RST if the port is closed.

FIN scans (-sF) work in an almost identical fashion; however, instead of sending a completely empty packet, a request is sent with the FIN flag. Once again, Nmap expects a RST if the port is closed.

As with the other two scans in this class, Xmas scans (-sX) send a malformed TCP packet and expects a RST response for closed ports.

The expected response for open ports with these scans is also identical, and is very similar to that of a UDP scan. If the port is open then there is no response to the malformed packet. Unfortunately (as with open UDP ports), that is also an expected behavior if the port is protected by a firewall, so NULL, FIN and Xmas scans will only ever identify ports as being open|filtered, closed, or filtered. If a port is identified as filtered with one of these scans then it is usually because the target has responded with an ICMP unreachable packet.

That said, the goal here is, of course, firewall evasion. Many firewalls are configured to drop incoming TCP packets to blocked ports which have the SYN flag set (thus blocking new connection initiation requests). By sending requests which do not

contain the SYN flag, we effectively bypass this kind of firewall. However, most modern IDS solutions can deal with these scan types.

Questions

Which of the three shown scan types uses the URG flag?

Answer: xmas

Why are NULL, FIN and Xmas scans generally used?

Answer: Firewall Evasion

Which common OS may respond to a NULL, FIN or Xmas scan with a RST for every port?

Answer: Microsoft Windows

Task 9 (ICMP Network Scanning)

On connecting to a system, our first objective is to obtain a “map” of the network structure. In other words, we want to see which IP addresses contain active hosts, and which do not. Nmap can do this by running a “ping sweep”. What this means is that Nmap sends a ICMP packet to each possible IP address for the specified network. If it receives a response, it marks the address as being alive.

To perform a ping sweep, we use the -sn switch in conjunction with IP ranges.

Questions

How would you perform a ping sweep on the 172.16.x.x network (Netmask: 255.255.0.0) using Nmap? (CIDR notation)

Answer: `nmap -sn 172.16.0.0/16`

Task 10 (NSE Scripts — Overview)

NSE stands for Nmap Scripting Language. NSE can greatly improve the functionality of Nmap with the use of scripts written in the Lua programming language.

There are many categories of scripts available. A exhaustive list can be found [here](#).

Questions

What language are NSE scripts written in?

Answer: Lua

Which category of scripts would be a very bad idea to run in a production environment?

Answer: intrusive

Task 11 (NSE Scripts — Working with NSE)

To run a specific script, we would use:

`--script=http-fileupload-exploiter`

Multiple scripts can be run simultaneously in this fashion by separating them by a comma.

Questions

What optional argument can the `ftp-anon.nse` script take?

The answer can be found here:

<https://nmap.org/nsedoc/scripts/ftp-anon.html>

Answer: `maxlist`

Task 12 (NSE Scripts — Searching)

We know how to run scripts, but how to find them? There are two options:

The first is the page on the Nmap website (mentioned in the previous task) which contains a list of all official scripts.

The second is the local storage on your attacking machine. Nmap stores its scripts on Linux at `/usr/share/nmap/scripts`. All of the NSE scripts are stored in this directory by default -- this is where Nmap looks for scripts when you specify them.

There are two ways to search for these installed scripts. One is by using the `/usr/share/nmap/scripts/script.db` file. Despite the extension, this isn't actually a database so much as a formatted text file containing filenames and categories for each available script. Nmap uses this file to keep track of (and utilise) scripts for the scripting engine; however, we can also `grep` through it to look for scripts. For example:

```
grep "ftp" /usr/share/nmap/scripts/script.db
```

The second way to search for scripts is quite simply to use the `ls` command in the scripts folder. For example, we could get the same results as in the previous screenshot by using:

```
ls -l /usr/share/nmap/scripts/*ftp*.
```

Questions

Search for “smb” scripts in the `/usr/share/nmap/scripts/` directory using either of the demonstrated methods. What is the filename of the script which determines the underlying OS of the SMB server?

Answer: `smb-os-discovery.nse`

Read through this script. What does it depend on?

Scroll a bit down in the script. Then you will find the answer:

Dependencies of the `smb-os-discovery.nse` script

Answer: `smb-brute`

Task 13 (Firewall Evasion)

We have talked a lot about techniques for bypassing firewalls using stealthier scans. However, there is another common problem. Typical Windows hosts will because of its default firewall block all ICMP packets. This means that we can't use ping on

the network, and in addition nmap uses ICMP packets as well for scanning ports. Open ports will therefore not be detected.

We can bypass this problem by using the -Pn flag. This tells Nmap to avoid pinging hosts before

So, we need a way to get around this configuration. Fortunately Nmap provides an option for this: -Pn, which tells Nmap to not bother pinging the host before scanning it. This means that Nmap will always treat the target host(s) as being alive, effectively bypassing the ICMP block; however, it comes at the price of potentially taking a very long time to complete the scan (if the host really is dead then Nmap will still be checking and double checking every specified port).

Questions

Which simple (and frequently relied upon) protocol is often blocked, requiring the use of the -Pn switch?

Answer: ICMP

[Research] Which Nmap switch allows you to append an arbitrary length of random data to the end of packets?

Answer: --data-length

Task 14 (Practical)

Questions

Does the target ip respond to ICMP (ping) requests (Y/N)?

Answer: N

Perform an Xmas scan on the first 999 ports of the target — how many ports are shown to be open or filtered?

Answer: 999

There is a reason given for this — what is it?

Answer: No Response

Perform a TCP SYN scan on the first 5000 ports of the target — how many ports are shown to be open?

Answer: 5

Open Wireshark (see Cryillic's Wireshark Room for instructions) and perform a TCP Connect scan against port 80 on the target, monitoring the results. Make sure you understand what's going on.

Answer: No answer needed

Deploy the ftp-anon script against the box. Can Nmap login successfully to the FTP server on port 21? (Y/N)

Answer: Y