

TryHackMe – Nmap



An in depth look at scanning with Nmap, a powerful network scanning tool.

Task 1: Deploy

Deploy the VM in THM.

Task 2: Introduction

The more knowledge you have about a target system or network, the more options you have available. This makes it imperative that proper enumeration is carried out before any exploitation attempts are made.

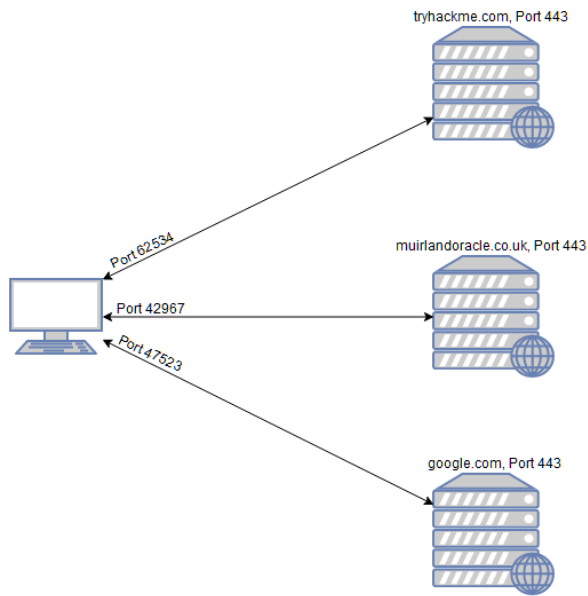
Say we have been given an IP (or multiple IP addresses) to perform a security audit on. Before we do anything else, we need to get an idea of the “landscape” we are attacking. What this means is that we need to establish which services are running on the targets.

For example, perhaps one of them is running a webserver, and another is acting as a Windows Active Directory Domain Controller. The first stage in establishing this “map” of the landscape is something called port scanning.

When a computer runs a network service, it opens a networking construct called a “port” to receive the connection. Ports are necessary for making multiple network requests or having multiple services available.

For example, when you load several webpages at once in a web browser, the program must have some way of determining which tab is loading which web page. This is done by establishing connections to the remote webserver using different ports on your local machine. Equally, if you want a server to be able to run more than one service (for example, perhaps you want your webserver to run both HTTP and HTTPS versions of the site), then you need some way to direct the traffic to the appropriate service.

Once again, ports are the solution to this. Network connections are made between two ports – an open port listening on the server and a randomly selected port on your own computer. For example, when you connect to a web page, your computer may open port 49534 to connect to the server’s port 443.



As in the previous example, the diagram shows what happens when you connect to numerous websites at the same time. Your computer opens up a different, high-numbered port (at random), which it uses for all its communications with the remote server.

Every computer has a total of **65535** available ports; however, many of these are registered as standard ports. For example, a HTTP Webservice can nearly always be found on port 80 of the server. A HTTPS Webservice can be found on port 443. Windows NETBIOS can be found on port 139 and SMB can be found on port 445. It is important to note; however, that especially in a CTF setting, it is not unheard of for even these standard ports to be altered, making it even more imperative that we perform appropriate enumeration on the target.

If we do not know which of these ports a server has open, then we do not have a hope of successfully attacking the target; thus, it is crucial that we begin any attack with a port scan. This can be accomplished in a variety of ways – usually using a tool called nmap.

Nmap can be used to perform many different kinds of port scan. However, the basic theory is this: nmap will connect to each port of the target in turn. Depending on how the port responds, it can be determined as being open, closed, or filtered (usually by a firewall). Once we know which ports are open, we can then look at enumerating which services are running on each port – either manually, or more commonly using nmap.

So, why nmap? The short answer is that it's currently the industry standard for a reason: no other port scanning tool comes close to matching its functionality (although some newcomers are now matching it for speed). It is an extremely powerful tool – made even more powerful by its scripting engine which can be used to scan for vulnerabilities, and in some cases even perform the exploit directly!

Question 1: What networking constructs are used to direct traffic to the right application on a server?

Answer: *Ports*

Question 2: How many of these are available on any network-enabled computer?

Answer: 65535

Question 3: How many of these are considered "well-known"? (These are the "standard" numbers mentioned in the task)

Answer: 1024

Task 3: Nmap Switches

Like most pentesting tools, nmap is run from the terminal. There are versions available for both Windows and Linux.

Nmap can be accessed by typing `nmap` into the terminal command line, followed by some of the "switches" (command arguments which tell a program to do different things) we will be covering below.

All you'll need for this is the help menu for nmap (accessed with `nmap -h`) and/or the nmap man page (access with `man nmap`). For each answer, include all parts of the switch unless otherwise specified. This includes the hyphen at the start (`h`).

Question 4: What is the first switch listed in the help menu for a 'Syn Scan'?

Answer: `-sS`

Question 5: Which switch would you use for a "UDP scan"?

Answer: `-sU`

Question 6: If you wanted to detect which operating system the target is running on, which switch would you use?

Answer: `-O`

Question 7: Nmap provides a switch to detect the version of the services running on the target. What is this switch?

Answer: `-sV`

Question 8: The default output provided by nmap often does not provide enough information for a pentester. How would you increase the verbosity?

Answer: `-v`

Question 9: Verbosity level one is good, but verbosity level two is better! How would you set the verbosity level to two? (Note: it's highly advisable to always use at least this option)

Answer: `-vv`

Question 10: We should always save the output of our scans -- this means that we only need to run the scan once (reducing network traffic and thus chance of detection), and gives us a reference to use when writing reports for clients. What switch would you use to save the nmap results in three major formats?

Answer: `-oA`

Question 11: What switch would you use to save the nmap results in a "normal" format?

Answer: `-oN`

Question 12: A very useful output format: how would you save results in a "grepable" format?

Answer: `-oG`

Question 13: Sometimes the results we're getting just aren't enough. 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?

Answer: `-A`

Question 14: Nmap offers five levels of "timing" template. These are essentially used to increase the speed your scan runs at. Be careful though: higher speeds are noisier and can incur errors! How would you set the timing template to level 5?

Answer: `-T5`

Question 15: We can also choose which port(s) to scan. How would you tell nmap to only scan port 80?

Answer: `-p 80`

Question 16: How would you tell nmap to scan ports 1000-1500?

Answer: `-p 1000-1500`

Question 17: A very useful option that should not be ignored: How would you tell nmap to scan all ports?

Answer: `-p-`

Question 18: How would you activate a script from the nmap scripting library?

Answer: `--script`

Question 19: How would you activate all of the scripts in the "vuln" category?

Answer: `--script=vuln`

Task 4: Scan Types – Overview

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

- TCP Connect Scans (**-sT**)
- SYN "Half-open" Scans (**-sS**)
- UDP Scans (**-sU**)

Additionally, there are several less common port scan types, some of which we will also cover (albeit in less detail). These are:

- TCP Null Scans (**-sN**)
- TCP FIN Scans (**-sF**)
- TCP Xmas Scans (**-sX**)

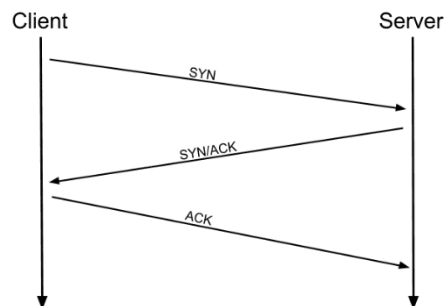
Most of these (with the exception of UDP scans) are used for very similar purposes, however, the way that they work differs between each scan. This means that, whilst one of the first three scans are likely to be your go-to in most situations, it's worth bearing in mind that other scan types exist.

In terms of network scanning, we will also look briefly at ICMP (or "ping") scanning.

Task 5: Scan Types – TCP Connect Scans

To understand TCP, Connect scans (**-sT**), it's important that you're comfortable with the *TCP three-way handshake*.

As a brief recap, the three-way handshake consists of three stages. First the connecting terminal (our attacking machine, in this instance) sends a TCP request to the target server with the SYN flag set. The server then acknowledges this packet with a TCP response containing the SYN flag, as well as the ACK flag. Finally, our terminal completes the handshake by sending a TCP request with the ACK flag set.



No.	Time	Source	Destination	Protocol	Length	Info
21	2.009477639	192.168.1.142	192.168.1.141	TCP	74	60516 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2310196 TSecr=0 WS=128
22	2.009847598	192.168.1.141	192.168.1.142	TCP	66	80 → 60516 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
23	2.009886244	192.168.1.142	192.168.1.141	TCP	54	60516 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0

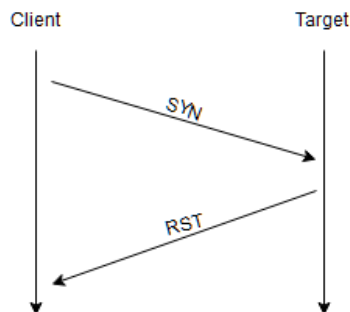
This is one of the fundamental principles of TCP/IP networking, but how does it relate to Nmap?

Well, as the name suggests, a TCP Connect scan works by performing the three-way handshake with each target port in turn. In other words, Nmap tries to connect to each specified TCP port, and determines whether the service is open by the response it receives.

For example, if a port is closed, [RFC 9293](#) states that:

"... If the connection does not exist (CLOSED), then a reset is sent in response to any incoming segment except another reset. A SYN segment that does not match an existing connection is rejected by this means."

In other words, if Nmap sends a TCP request with the *SYN* flag set to a **closed** port, the target server will respond with a TCP packet with the *RST* (Reset) flag set. By this response, Nmap can establish that the port is closed.



If, however, the request is sent to an *open* port, the target will respond with a TCP packet with the SYN/ACK flags set. Nmap then marks this port as being *open* (and completes the handshake by sending back a TCP packet with ACK set).

This is all well and good, however, there is a third possibility.

What if the port is open, but hidden behind a firewall?

Many firewalls are configured to simply **drop** incoming packets. Nmap sends a TCP SYN request and receives nothing back. This indicates that the port is being protected by a firewall and thus the port is considered to be *filtered*.

That said, it is very easy to configure a firewall to respond with a RST TCP packet. For example, in IPtables for Linux, a simple version of the command would be as follows:

```
iptables -I INPUT -p tcp --dport <port> -j REJECT --reject-with tcp-reset
```

This can make it extremely difficult (if not impossible) to get an accurate reading of the target(s).

Question 20: Which RFC defines the appropriate behavior for the TCP protocol?

Answer: RFC 9293

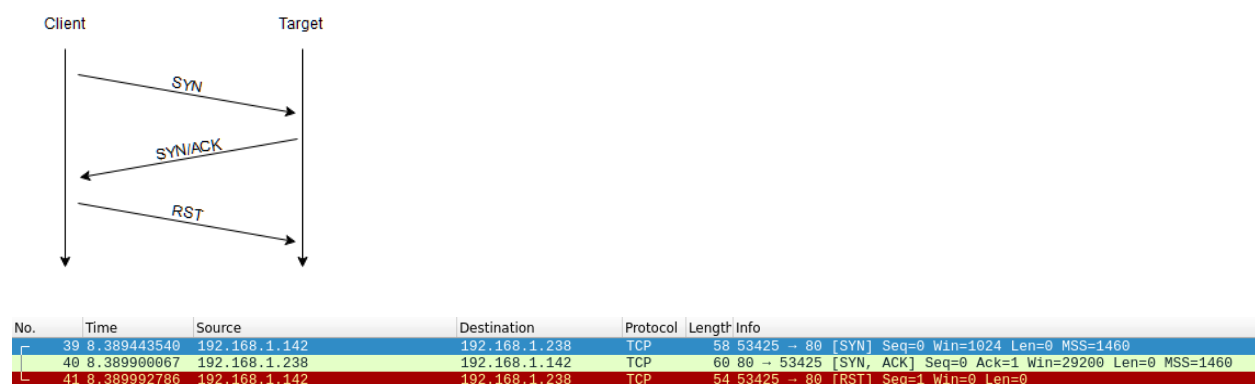
Question 21: If a port is closed, which flag should the server send back to indicate this?

Answer: RST

Task 6: Scan Types – SYN Scans

As with TCP scans, SYN scans (**-sS**) are used to scan the TCP port-range of a target or targets; however, the two scan types work slightly differently. SYN scans are sometimes referred to as "Half-open" scans, or "Stealth" scans.

Where TCP scans perform a full three-way handshake with the target, SYN scans sends back a RST TCP packet after receiving a SYN/ACK from the server (this prevents the server from repeatedly trying to make the request). In other words, the sequence for scanning an **open** port looks like this:



This has a variety of advantages for us as hackers:

- It can be used to bypass older Intrusion Detection systems as they are looking out for a full three-way handshake. This is often no longer the case with modern IDS solutions; it is for this reason that SYN scans are still frequently referred to as "stealth" scans.
- SYN scans are often not logged by applications listening on open ports, as standard practice is to log a connection once it's been fully established. Again, this plays into the idea of SYN scans being stealthy.
- Without having to bother about completing (and disconnecting from) a three-way handshake for every port, SYN scans are significantly faster than a standard TCP Connect scan.

There are, however, a couple of disadvantages to SYN scans, namely:

- They require sudo permissions^[1] in order to work correctly in Linux. This is because SYN scans require the ability to create raw packets (as opposed to the full TCP handshake), which is a privilege only the root user has by default.

- Unstable services are sometimes brought down by SYN scans, which could prove problematic if a client has provided a production environment for the test.

All in all, the pros outweigh the cons.

For this reason, SYN scans are the default scans used by Nmap *if run with sudo permissions*. If run **without** sudo permissions, Nmap defaults to the TCP Connect scan we saw in the previous task.

When using a SYN scan to identify closed and filtered ports, the exact same rules as with a TCP Connect scan apply.

If a port is closed then the server responds with a RST TCP packet. If the port is filtered by a firewall then the TCP SYN packet is either dropped, or spoofed with a TCP reset.

In this regard, the two scans are identical: the big difference is in how they handle *open* ports.

[1] SYN scans can also be made to work by giving Nmap the CAP_NET_RAW, CAP_NET_ADMIN and CAP_NET_BIND_SERVICE capabilities; however, this may not allow many of the NSE scripts to run properly.

Question 22: There are two other names for a SYN scan, what are they?

Answer: Half-Open, Stealth

Question 23: Can Nmap use a SYN scan without Sudo permissions (Y/N)?

Answer: N

Task 7: Scan Types – UDP Scans

Unlike TCP, UDP connections are *stateless*. This means that, rather than initiating a connection with a back-and-forth "handshake", UDP connections rely on sending packets to a target port and essentially hoping that they make it. This makes UDP superb for connections which rely on speed over quality (e.g. video sharing), but the lack of acknowledgement makes UDP significantly more difficult (and much slower) to scan. The switch for an Nmap UDP scan is (**-sU**)

When a packet is sent to an open UDP port, there should be no response. When this happens, Nmap refers to the port as being **open/filtered**. In other words, it suspects that the port is open, but it could be firewalled. If it gets a UDP response (which is very unusual), then the port is marked as *open*. More commonly there is no response, in which case the request is sent a second time as a double-check. If there is still no response, then the port is marked *open/filtered* and Nmap moves on.

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. This clearly identifies closed ports, which Nmap marks as such and moves on.

Due to this difficulty in identifying whether a UDP port is actually open, UDP scans tend to be incredibly slow in comparison to the various TCP scans (in the region of 20 minutes to scan the first 1000 ports, with a good connection). For this reason, 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>`. Will scan the top 20 most commonly used UDP ports, resulting in a much more acceptable scan time.

When scanning UDP ports, Nmap usually sends completely empty requests -- just raw UDP packets. That said, for ports which are usually occupied by well-known services, it will instead send a protocol-specific payload which is more likely to elicit a response from which a more accurate result can be drawn.

Question 24: If a UDP port doesn't respond to an Nmap scan, what will it be marked as?

Answer: open|filtered

Question 25: 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: Scan Types – NULL, FIN, Xmas

NULL, FIN and Xmas TCP port scans are less commonly used than any of the others we've covered already, so we will not go into a huge amount of depth here. All three are interlinked and are used primarily as they tend to be even stealthier, relatively speaking, than a SYN "stealth" scan. Beginning with NULL scans:

- 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.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	127.0.0.1	127.0.0.1	TCP	54	36717 → 80 [<None>] Seq=1 Win=1024 Len=0
2	0.000012387	127.0.0.1	127.0.0.1	TCP	54	80 → 36717 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Acknowledgment number: 0	
Acknowledgment number (raw): 0	
0101 = Header Length: 20 bytes (5)	
▼ Flags: 0x000 (<None>)	
0000.	= Reserved: Not set
...0.	= Nonce: Not set
... 0... ..	= Congestion Window Reduced (CWR): Not set
.... 0... ..	= ECN-Echo: Not set
.... ..0. ..	= Urgent: Not set
.... ...0. ..	= Acknowledgment: Not set
.... ... 0..	= Push: Not set
....0.	= Reset: Not set
....0.	= Syn: Not set
....0	= Fin: Not set

- 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 (usually used to gracefully close an active connection). Once again, Nmap expects a RST if the port is closed.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	127.0.0.1	127.0.0.1	TCP	54	33952 → 80 [FIN] Seq=1 Win=1024 Len=0
2	0.000013391	127.0.0.1	127.0.0.1	TCP	54	80 → 33952 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0

Acknowledgment number: 0	
Acknowledgment number (raw): 0	
0101 = Header Length: 20 bytes (5)	
▼ Flags: 0x001 (FIN)	
000.	= Reserved: Not set
...0	= Nonce: Not set
...0	= Congestion Window Reduced (CWR): Not set
...0	= ECN-Echo: Not set
...0	= Urgent: Not set
...0	= Acknowledgment: Not set
...0	= Push: Not set
...0	= Reset: Not set
...0	= Syn: Not set
...1	= Fin: Set

- 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. It's referred to as an xmas scan as the flags that it sets (PSH, URG and FIN) give it the appearance of a blinking Christmas tree when viewed as a packet capture in Wireshark.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	127.0.0.1	127.0.0.1	TCP	54	46664 → 80 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
2	0.000100904	127.0.0.1	127.0.0.1	TCP	54	80 → 46664 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0

Acknowledgment number: 0	
Acknowledgment number (raw): 0	
0101 = Header Length: 20 bytes (5)	
▼ Flags: 0x029 (FIN, PSH, URG)	
000.	= Reserved: Not set
...0	= Nonce: Not set
...0	= Congestion Window Reduced (CWR): Not set
...0	= ECN-Echo: Not set
...1	= Urgent: Set
...0	= Acknowledgment: Not set
...1	= Push: Set
...0	= Reset: Not set
...0	= Syn: Not set
...1	= Fin: Set

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 behaviour 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.

It's also worth noting that while RFC 793 mandates that network hosts respond to malformed packets with a RST TCP packet for closed ports, and don't respond at all for open ports; this is not always the case in practice. In particular Microsoft Windows (and a lot of Cisco network devices) are known to respond with a RST to any malformed TCP packet -- regardless of whether the port is actually open or not. This results in all ports showing up as being closed.

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. Whilst this is good in theory, most modern IDS solutions are savvy to these scan types, so don't rely on them to be 100% effective when dealing with modern systems.

Question 26: Which of the three shown scan types uses the URG flag?

Answer: *xmas*

Question 27: Why are NULL, FIN and Xmas scans generally used?

Answer: *Firewall Evasion*

Question 28: Which common OS may respond to a NULL, FIN or Xmas scan with a RST for every port?

Answer: *Microsoft Windows*

Task 9: Scan Types – ICMP Network Scanning

On first connection to a target network in a black box assignment, our first objective is to obtain a "map" of the network structure -- or, in other words, we want to see which IP addresses contain active hosts, and which do not.

One way to do this is by using Nmap to perform a so called "ping sweep". This is exactly as the name suggests: Nmap sends an ICMP packet to each possible IP address for the specified network. When it receives a response, it marks the IP address that responded as being alive. For reasons we'll see in a later task, this is not always accurate; however, it can provide something of a baseline and thus is worth covering.

To perform a ping sweep, we use the `-sn` switch in conjunction with IP ranges which can be specified with either a hyphen (`-`) or CIDR notation. i.e. we could scan the `192.168.0.x` network using:

- `nmap -sn 192.168.0.1-254`

or

- `nmap -sn 192.168.0.0/24`

The `-sn` switch tells Nmap not to scan any ports -- forcing it to rely primarily on ICMP echo packets (or ARP requests on a local network, if run with sudo or directly as the root user) to identify targets. In addition to the ICMP echo requests, the `-sn` switch will also cause nmap to send a TCP SYN packet to port 443 of the target, as well as a TCP ACK (or TCP SYN if not run as root) packet to port 80 of the target.

Question 29: How would you perform a ping sweep on the 172.16.x.x network (Netmask: 255.255.0.0) using Nmap? (CIDR notation)

Hint: The CIDR notation for a Class B network with a default netmask is /16

Answer: `nmap -sn 172.16.0.0/16`

Task 10: NSE Scripts – Overview

The Nmap Scripting Engine (NSE) is an incredibly powerful addition to Nmap, extending its functionality quite considerably. NSE Scripts are written in the *Lua* programming language, and can be used to do a variety of things: from scanning for vulnerabilities, to automating exploits for them. The NSE is particularly useful for reconnaissance, however, it is well worth bearing in mind how extensive the script library is.

There are many categories available. Some useful categories include:

- **safe**:- Won't affect the target
- **intrusive**:- Not safe: likely to affect the target
- **vuln**:- Scan for vulnerabilities
- **exploit**:- Attempt to exploit a vulnerability
- **auth**:- Attempt to bypass authentication for running services (e.g. Log into an FTP server anonymously)
- **brute**:- Attempt to bruteforce credentials for running services
- **discovery**:- Attempt to query running services for further information about the network (e.g. query an SNMP server).

A more exhaustive list can be found [here](#).

Question 30: What language are NSE scripts written in?

Answer: *Lua*

Question 31: Which category of scripts would be a very bad idea to run in a production environment?

Answer: *intrusive*

Task 11: NSE Scripts – Working with the NSE

In Task 3 we looked very briefly at the **--script** switch for activating NSE scripts from the **vuln** category using **--script=vuln**. It should come as no surprise that the other categories work in exactly the same way. If the command **--script=safe** is run, then any applicable safe scripts will be run against the target (Note: only scripts which target an active service will be activated).

o run a specific script, we would use **--script=<script-name>**, e.g. **--script=http-fileupload-exploiter**.

Multiple scripts can be run simultaneously in this fashion by separating them by a comma. For example: `--script=smb-enum-users,smb-enum-shares`.

Some scripts require arguments (for example, credentials, if they're exploiting an authenticated vulnerability). These can be given with the `--script-args` Nmap switch. An example of this would be with the `http-put` script (used to upload files using the PUT method). This takes two arguments: the URL to upload the file to, and the file's location on disk. For example:

```
nmap -p 80 --script http-put --script-args http-put.url='/dav/shell.php',http-put.file='./shell.php'
```

Note that the arguments are separated by commas, and connected to the corresponding script with periods (i.e. `<script-name>.<argument>`).

A full list of scripts and their corresponding arguments (along with example use cases) can be found [here](#).

Nmap scripts come with built-in help menus, which can be accessed using `nmap --script-help <script-name>`. This tends not to be as extensive as in the link given above, however, it can still be useful when working locally.

Question 32: What optional argument can the `ftp-anon.nse` script take?

Answer: `maxlist`

Task 12: NSE Scripts – Searching for Scripts

Ok, so we know how to use the scripts in Nmap, but we don't yet know how to *find* these scripts.

We have two options for this, which should ideally be used in conjunction with each other. 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 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.

```

muri@augury:/usr/share/nmap/scripts$ file script.db
script.db: ASCII text
muri@augury:/usr/share/nmap/scripts$ head script.db
Entry { filename = "acarsd-info.nse", categories = { "discovery", "safe", } }
Entry { filename = "address-info.nse", categories = { "default", "safe", } }
Entry { filename = "afp-brute.nse", categories = { "brute", "intrusive", } }
Entry { filename = "afp-ls.nse", categories = { "discovery", "safe", } }
Entry { filename = "afp-path-vuln.nse", categories = { "exploit", "intrusive", "vuln", } }
Entry { filename = "afp-serverinfo.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "afp-showmount.nse", categories = { "discovery", "safe", } }
Entry { filename = "ajp-auth.nse", categories = { "auth", "default", "safe", } }
Entry { filename = "ajp-brute.nse", categories = { "brute", "intrusive", } }
Entry { filename = "ajp-headers.nse", categories = { "discovery", "safe", } }

```

Nmap uses this file to keep track of (and utilize) 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`.

```

muri@augury:/usr/share/nmap/scripts$ grep "ftp" /usr/share/nmap/scripts/script.db
Entry { filename = "ftp-anon.nse", categories = { "auth", "default", "safe", } }
Entry { filename = "ftp-bounce.nse", categories = { "default", "safe", } }
Entry { filename = "ftp-brute.nse", categories = { "brute", "intrusive", } }
Entry { filename = "ftp-libopie.nse", categories = { "intrusive", "vuln", } }
Entry { filename = "ftp-proftpd-backdoor.nse", categories = { "exploit", "intrusive", "malware", "vuln", } }
Entry { filename = "ftp-syst.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "ftp-vsftpd-backdoor.nse", categories = { "exploit", "intrusive", "malware", "vuln", } }
Entry { filename = "ftp-vuln-cve2010-4221.nse", categories = { "intrusive", "vuln", } }
Entry { filename = "tftp-enum.nse", categories = { "discovery", "intrusive", } }

```

The second way to search for scripts is quite simply to use the `ls` command. For example, we could get the same results as in the previous screenshot by using `ls -l /usr/share/nmap/scripts/*ftp*`:

```

muri@augury:/usr/share/nmap/scripts$ ls -l /usr/share/nmap/scripts/*ftp*
-rw-r--r-- 1 root root 4530 Oct 12 14:29 /usr/share/nmap/scripts/ftp-anon.nse
-rw-r--r-- 1 root root 3253 Oct 12 14:29 /usr/share/nmap/scripts/ftp-bounce.nse
-rw-r--r-- 1 root root 3108 Oct 12 14:29 /usr/share/nmap/scripts/ftp-brute.nse
-rw-r--r-- 1 root root 3272 Oct 12 14:29 /usr/share/nmap/scripts/ftp-libopie.nse
-rw-r--r-- 1 root root 3290 Oct 12 14:29 /usr/share/nmap/scripts/ftp-proftpd-backdoor.nse
-rw-r--r-- 1 root root 3768 Oct 12 14:29 /usr/share/nmap/scripts/ftp-syst.nse
-rw-r--r-- 1 root root 6021 Oct 12 14:29 /usr/share/nmap/scripts/ftp-vsftpd-backdoor.nse
-rw-r--r-- 1 root root 5923 Oct 12 14:29 /usr/share/nmap/scripts/ftp-vuln-cve2010-4221.nse
-rw-r--r-- 1 root root 5736 Oct 12 14:29 /usr/share/nmap/scripts/tftp-enum.nse

```

Note the use of asterisks () on either side of the search term.*

The same techniques can also be used to search for categories of script. For example: `grep "safe" /usr/share/nmap/scripts/script.db`


```
muri@augury:/usr/share/nmap/scripts$ grep "safe" /usr/share/nmap/scripts/script.db
Entry { filename = "acarsd-info.nse", categories = { "discovery", "safe", } }
Entry { filename = "address-info.nse", categories = { "default", "safe", } }
Entry { filename = "afp-ls.nse", categories = { "discovery", "safe", } }
Entry { filename = "afp-serverinfo.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "afp-showmount.nse", categories = { "discovery", "safe", } }
Entry { filename = "ajp-auth.nse", categories = { "auth", "default", "safe", } }
Entry { filename = "ajp-headers.nse", categories = { "discovery", "safe", } }
Entry { filename = "ajp-methods.nse", categories = { "default", "safe", } }
Entry { filename = "ajp-request.nse", categories = { "discovery", "safe", } }
Entry { filename = "allseeingeye-info.nse", categories = { "discovery", "safe", "version", } }
```

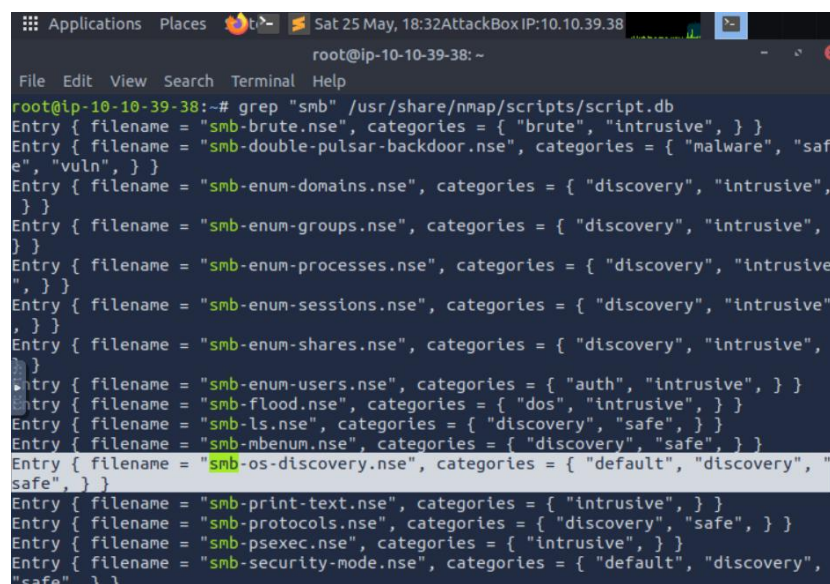
Installing New Scripts

We mentioned previously that the Nmap website contains a list of scripts, so, what happens if one of these is missing in the `scripts` directory locally? A standard `sudo apt update && sudo apt install nmap` should fix this; however, it's also possible to install the scripts manually by downloading the script from Nmap (`sudo wget -O /usr/share/nmap/scripts/<script-name>.nse https://svn.nmap.org/nmap/scripts/<script-name>.nse`). This must then be followed up with `nmap --script-updatedb`, which updates the `script.db` file to contain the newly downloaded script.

It's worth noting that you would require the same "updatedb" command if you were to make your own NSE script and add it into Nmap -- a more than manageable task with some basic knowledge of Lua!

Question 33: 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`



```
Applications Places Sat 25 May, 18:32 AttackBox IP:10.10.39.38
root@ip-10-10-39-38: ~
File Edit View Search Terminal Help
root@ip-10-10-39-38:~# grep "smb" /usr/share/nmap/scripts/script.db
Entry { filename = "smb-brute.nse", categories = { "brute", "intrusive", } }
Entry { filename = "smb-double-pulsar-backdoor.nse", categories = { "malware", "safe", "vuln", } }
Entry { filename = "smb-enum-domains.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-enum-groups.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-enum-processes.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-enum-sessions.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-enum-shares.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-enum-users.nse", categories = { "auth", "intrusive", } }
Entry { filename = "smb-flood.nse", categories = { "dos", "intrusive", } }
Entry { filename = "smb-ls.nse", categories = { "discovery", "safe", } }
Entry { filename = "smb-mbenum.nse", categories = { "discovery", "safe", } }
Entry { filename = "smb-os-discovery.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "smb-print-text.nse", categories = { "intrusive", } }
Entry { filename = "smb-protocols.nse", categories = { "discovery", "safe", } }
Entry { filename = "smb-psexec.nse", categories = { "intrusive", } }
Entry { filename = "smb-security-mode.nse", categories = { "default", "discovery", "safe", } }
```

Question 34: Read through this script. What does it depend on?

Answer: *smb-brute*

Commands:

locate smb-os-discovery.nse

```
root@ip-10-10-39-38:/# locate smb-os-discovery.nse
/usr/share/nmap/scripts/smb-os-discovery.nse
/var/lib/docker/overlay2/2d199c7783384d3e7736d37c79af646abb52d47edade257e9f6d0dd419
2156c0/diff/usr/share/nmap/scripts/smb-os-discovery.nse
/var/lib/docker/overlay2/f8cd9c5888da7cfc46b82e9040b91e479a8c531fa4e432de5c24e2b73f
57895f/diff/usr/share/nmap/scripts/smb-os-discovery.nse
root@ip-10-10-39-38:/#
```

Copy the location.

cat <file_location>

cat /usr/share/nmap/scripts/smb-os-discovery.nse

```
@xmloutput
<elem key="os">Windows Server (R) 2008 Standard 6001 Service Pack 1</elem>
-- <elem key="cpe">cpe:/o:microsoft:windows_2008::sp1</elem>
-- <elem key="lanmanager">Windows Server (R) 2008 Standard 6.0</elem>
-- <elem key="domain">LAB</elem>
-- <elem key="server">SQL2008</elem>
-- <elem key="date">2011-04-20T13:34:06-05:00</elem>
-- <elem key="fqdn">Sql2008.lab.test.local</elem>
-- <elem key="domain_dns">lab.test.local</elem>
-- <elem key="forest_dns">test.local</elem>

author = "Ron Bowes"
license = "Same as Nmap--See https://nmap.org/book/man-legal.html"
categories = {"default", "discovery", "safe"}
dependencies = {"smb-brute"}
```

Task 13: Firewall Evasion

We have already seen some techniques for bypassing firewalls (think stealth scans, along with NULL, FIN and Xmas scans); however, there is another very common firewall configuration which it's imperative we know how to bypass.

Your typical Windows host will, with its default firewall, block all ICMP packets. This presents a problem: not only do we often use *ping* to manually establish the activity of a target, Nmap does the same thing by default. This means that Nmap will register a host with this firewall configuration as dead and not bother scanning it at all.

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).

It's worth noting that if you're already directly on the local network, Nmap can also use ARP requests to determine host activity. Address Resolution Protocol (ARP) is responsible for finding the MAC (hardware) address related to a specific IP address. It works by broadcasting an ARP query, "Who has this IP address? Tell me." And the response is of the form, "The IP address is at this MAC address."

It's worth noting that if you're already directly on the local network, Nmap can also use ARP requests to determine host activity.

There are a variety of other switches which Nmap considers useful for firewall evasion. We will not go through these in detail, however, they can be found [here](#).

The following switches are of particular note:

- **-f**:- Used to fragment the packets (i.e. split them into smaller pieces) making it less likely that the packets will be detected by a firewall or IDS.
- An alternative to **-f**, but providing more control over the size of the packets: **--mtu <number>**, accepts a maximum transmission unit size to use for the packets sent. This *must* be a multiple of 8.
- **--scan-delay <time>ms**:- used to add a delay between packets sent. This is very useful if the network is unstable, but also for evading any time-based firewall/IDS triggers which may be in place.
- **--badsum**:- this is used to generate in invalid checksum for packets. Any real TCP/IP stack would drop this packet, however, firewalls may potentially respond automatically, without bothering to check the checksum of the packet. As such, this switch can be used to determine the presence of a firewall/IDS.

Question 35: Which simple (and frequently relied upon) protocol is often blocked, requiring the use of the -Pn switch?

Answer: ICMP

Question 36: Which Nmap switch allows you to append an arbitrary length of random data to the end of packets?

Answer: --data-length

Command:

man nmap

FIREWALL/IDS EVASION AND SPOOFING:

- f; --mtu <val>: fragment packets (optionally w/given MTU)
- D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
- S <IP_Address>: Spoof source address
- e <iface>: Use specified interface
- g/--source-port <portnum>: Use given port number
- proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxy
- data <hex string>: Append a custom payload to sent packets
- data-string <string>: Append a custom ASCII string to sent packets
- data-length <num>: Append random data to sent packets
- ip-options <options>: Send packets with specified ip options
- ttl <val>: Set IP time-to-live field
- spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
- badsum: Send packets with a bogus TCP/UDP/SCTP checksum

Task 14: Practical

Question 37: Does the target ip respond to ICMP echo (ping) requests (Y/N)?

Answer: N

Question 37: Perform an Xmas scan on the first 999 ports of the target -- how many ports are shown to be open or filtered?

Answer: 999

```
root@ip-10-10-39-38:/# nmap -p1-999 -sX 10.10.237.200 -vv
Starting Nmap 7.60 ( https://nmap.org ) at 2024-05-25 19:05 BST
Initiating ARP Ping Scan at 19:05
Scanning 10.10.237.200 [1 port]
Completed ARP Ping Scan at 19:05, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:05
Completed Parallel DNS resolution of 1 host. at 19:05, 0.00s elapsed
Initiating XMAS Scan at 19:05
Scanning ip-10-10-237-200.eu-west-1.compute.internal (10.10.237.200) [999 ports]
Completed XMAS Scan at 19:06, 21.11s elapsed (999 total ports)
Nmap scan report for ip-10-10-237-200.eu-west-1.compute.internal (10.10.237.200)
Host is up, received arp-response (0.00018s latency).
All 999 scanned ports on ip-10-10-237-200.eu-west-1.compute.internal (10.10.237.200)
) are open|filtered because of 999 no-responses
MAC Address: 02:1B:76:0F:DE:B5 (Unknown)

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 21.59 seconds
Raw packets sent: 1999 (79.948KB) | Rcvd: 2 (60B)
root@ip-10-10-39-38:/#
```

Question 38: There is a reason given for this -- what is it?

Note: The answer will be in your scan results. Think carefully about which switches to use -- and read the hint before asking for help!

Answer: No response

Question 39: Perform a TCP SYN scan on the first 5000 ports of the target -- how many ports are shown to be open?

Answer: 5

```
root@ip-10-10-39-38:/# nmap -p1-5000 -sS 10.10.237.200 -vv -Pn

Starting Nmap 7.60 ( https://nmap.org ) at 2024-05-25 19:10 BST
Initiating ARP Ping Scan at 19:10
Scanning 10.10.237.200 [1 port]
Completed ARP Ping Scan at 19:10, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:10
Completed Parallel DNS resolution of 1 host. at 19:10, 0.00s elapsed
Initiating SYN Stealth Scan at 19:10
Scanning ip-10-10-237-200.eu-west-1.compute.internal (10.10.237.200) [5000 ports]
Discovered open port 21/tcp on 10.10.237.200
Discovered open port 3389/tcp on 10.10.237.200
Discovered open port 80/tcp on 10.10.237.200
Discovered open port 135/tcp on 10.10.237.200
Discovered open port 53/tcp on 10.10.237.200
Increasing send delay for 10.10.237.200 from 0 to 5 due to 11 out of 24 dropped probes since last increase.
SYN Stealth Scan Timing: About 29.81% done; ETC: 19:12 (0:01:13 remaining)
Increasing send delay for 10.10.237.200 from 5 to 10 due to 11 out of 28 dropped probes since last increase.
```

Question 40: Deploy the ftp-anon script against the box. Can Nmap login successfully to the FTP server on port 21? (Y/N)

Answer: Y

```
Applications Places Sat 25 May, 19:16 AttackBox IP: 10.10.39.38
root@ip-10-10-39-38:/
File Edit View Search Terminal Help
root@ip-10-10-39-38:/# nmap --script=ftp-anon -p21 10.10.237.200 -vv

Starting Nmap 7.60 ( https://nmap.org ) at 2024-05-25 19:14 BST
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 19:14
Completed NSE at 19:14, 0.00s elapsed
Initiating ARP Ping Scan at 19:14
Scanning 10.10.237.200 [1 port]
Completed ARP Ping Scan at 19:14, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:14
Completed Parallel DNS resolution of 1 host. at 19:14, 0.00s elapsed
Initiating SYN Stealth Scan at 19:14
Scanning ip-10-10-237-200.eu-west-1.compute.internal (10.10.237.200) [1 port]
Discovered open port 21/tcp on 10.10.237.200
Completed SYN Stealth Scan at 19:14, 0.22s elapsed (1 total ports)
NSE: Script scanning 10.10.237.200.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 19:14
Completed NSE at 19:14, 30.02s elapsed
Nmap scan report for ip-10-10-237-200.eu-west-1.compute.internal (10.10.237.200)
Host is up, received arp-response (0.00015s latency).
Scanned at 2024-05-25 19:14:28 BST for 31s

PORT      STATE SERVICE REASON
21/tcp    open  ftp      syn-ack ttl 128
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ Can't get directory listing: TIMEOUT
MAC Address: 02:1B:76:0F:DE:B5 (Unknown)

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 19:14
Completed NSE at 19:14, 0.00s elapsed
```

```
Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 31.27 seconds
Raw packets sent: 3 (116B) | Rcvd: 3 (116B)
root@ip-10-10-39-38:/#
```

```
root@ip-10-10-39-38:/# ftp 10.10.237.200
Connected to 10.10.237.200.
220-FileZilla Server 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
Name (10.10.237.200:root): Anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp>
```

Happy Hacking! 🐱



Thanks and Regards,

ShadowGirl 🧑🏻💻 😊