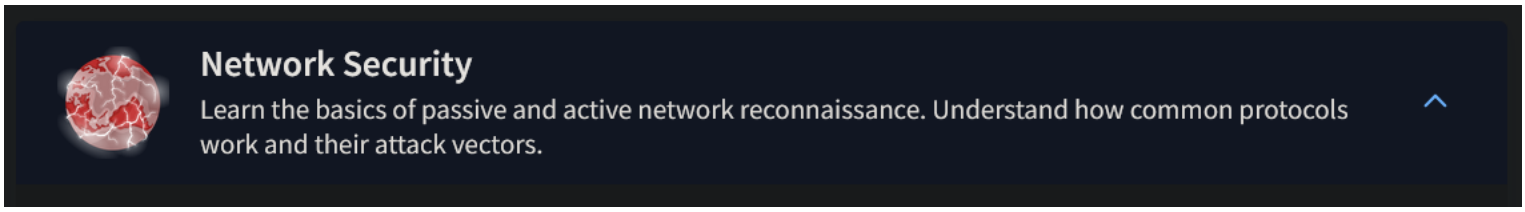
Directions:

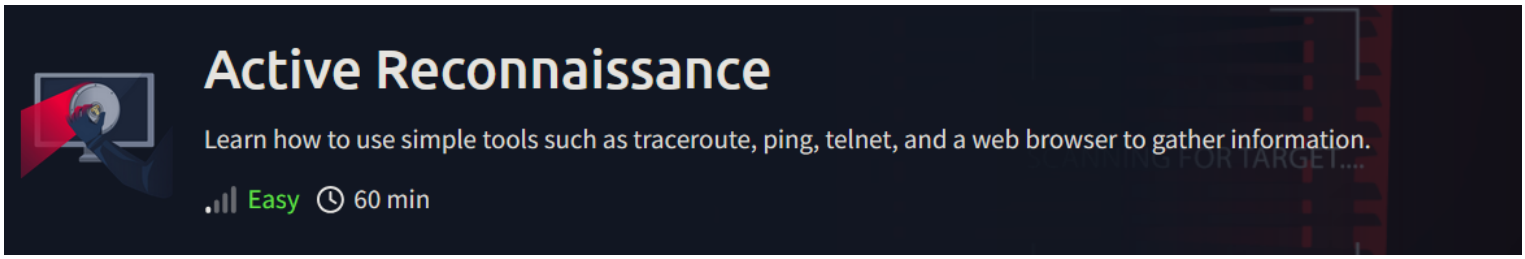


Compiled Summary of All rooms:

In this room, we focused on passive reconnaissance. In particular, we covered command-line tools, whois, nslookup, and dig. We also discussed two publicly available services DNSDumpster and Shodan.io. The power of such tools is that you can collect information about your targets without directly connecting to them. Moreover, the trove of information you may find using such tools can be massive once you master the search options and get used to reading the results.

Purpose	Commandline Example
Lookup WHOIS record	whois tryhackme.com
Lookup DNS A records	nslookup -type=A tryhackme.com
Lookup DNS MX records at DNS server	nslookup -type=MX tryhackme.com 1.1.1.1
Lookup DNS TXT records	nslookup -type=TXT tryhackme.com
Lookup DNS A records	dig tryhackme.com A
Lookup DNS MX records at DNS server	dig @1.1.1.1 tryhackme.com MX
Lookup DNS TXT records	dig tryhackme.com TXT

Learn more about DNS at DNS in Detail.

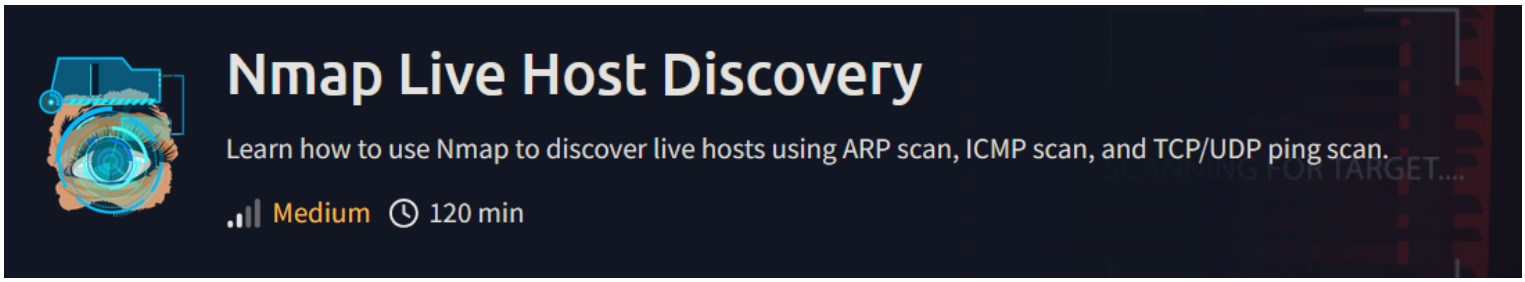


In this room, we have covered many various tools. It is easy to put a few of them together via a shell script to build a primitive network and system scanner. You can use traceroute to map the path to the target, ping to check if the target system responds to ICMP Echo, and telnet to check which ports are open and reachable by attempting to connect to them. Available scanners do this at much more advanced and sophisticated levels, as we will see in the next four rooms with nmap.

Command	Example
ping	ping -c 10 MACHINE_IP on Linux or macOS
ping	ping -n 10 MACHINE_IP on MS Windows
traceroute	traceroute MACHINE_IP on Linux or macOS
tracert	tracert MACHINE_IP on MS Windows
telnet	telnet MACHINE_IP PORT_NUMBER
netcat as client	nc MACHINE_IP PORT_NUMBER
netcat as server	nc -lvnp PORT_NUMBER

Although these are fundamental tools, they are readily available on most systems. In particular, a web browser is installed on practically every computer and smartphone and can be an essential tool in your arsenal for conducting reconnaissance without raising alarms. If you want to gain more profound knowledge of the Developer Tools, we recommend joining Walking An Application.

Operating System	Developer Tools Shortcut
Linux or MS Windows	Ctrl+Shift+I
macOS	Option + Command + I

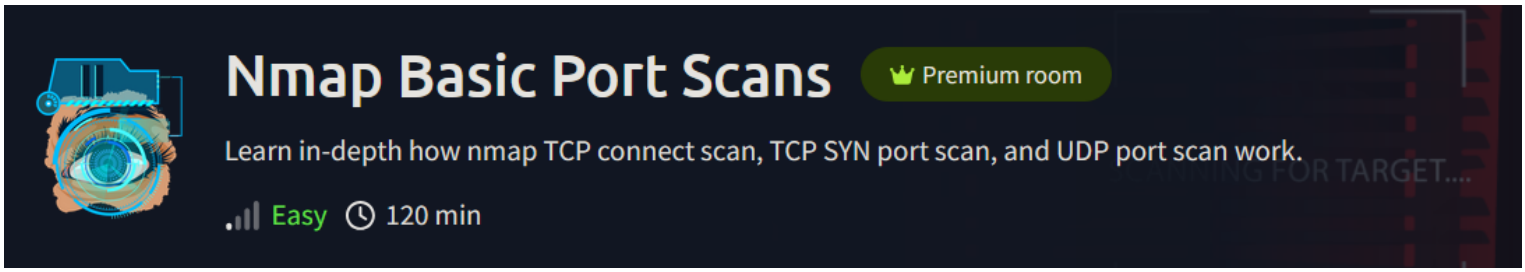


You have learned how ARP, ICMP, TCP, and UDP can detect live hosts by completing this room. Any response from a host is an indication that it is online. Below is a quick summary of the command-line options for Nmap that we have covered.

Scan Type	Example Command
ARP Scan	sudo nmap -PR -sn MACHINE_IP/24
ICMP Echo Scan	sudo nmap -PE -sn MACHINE_IP/24
ICMP Timestamp Scan	sudo nmap -PP -sn MACHINE_IP/24
ICMP Address Mask Scan	sudo nmap -PM -sn MACHINE_IP/24
TCP SYN Ping Scan	sudo nmap -PS22,80,443 -sn MACHINE_IP/30
TCP ACK Ping Scan	sudo nmap -PA22,80,443 -sn MACHINE_IP/30
UDP Ping Scan	sudo nmap -PU53,161,162 -sn MACHINE_IP/30

Remember to add -sn if you are only interested in host discovery without port-scanning. Omitting -sn will let Nmap default to port-scanning the live hosts.

Option	Purpose
-n	no DNS lookup
-R	reverse-DNS lookup for all hosts
-sn	host discovery only

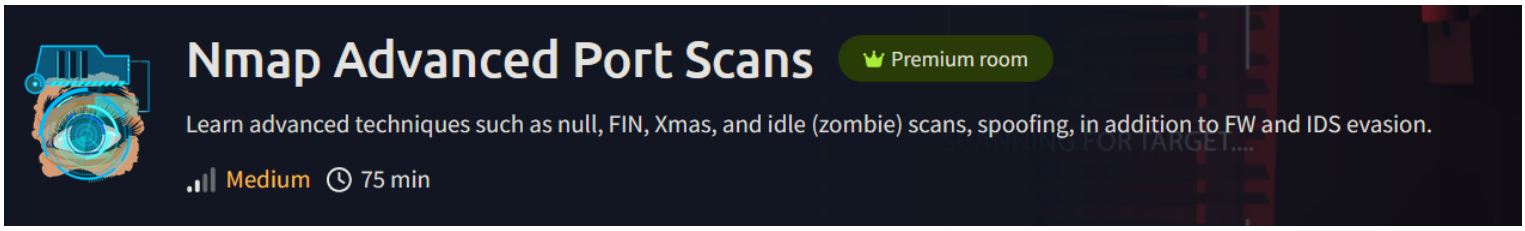


This room covered three types of scans.

Port Scan Type	Example Command
TCP Connect Scan	nmap -sT MACHINE_IP
TCP SYN Scan	sudo nmap -sS MACHINE_IP
UDP Scan	sudo nmap -sU MACHINE_IP

These scan types should get you started discovering running TCP and UDP services on a target host.

Option	Purpose
-p-	all ports
-p1-1023	scan ports 1 to 1023
-F	100 most common ports
-r	scan ports in consecutive order
-T<0-5>	-T0 being the slowest and T5 the fastest
--max-rate 50	rate <= 50 packets/sec
--min-rate 15	rate >= 15 packets/sec
--min-parallelism 100	at least 100 probes in parallel



This room covered the following types of scans.

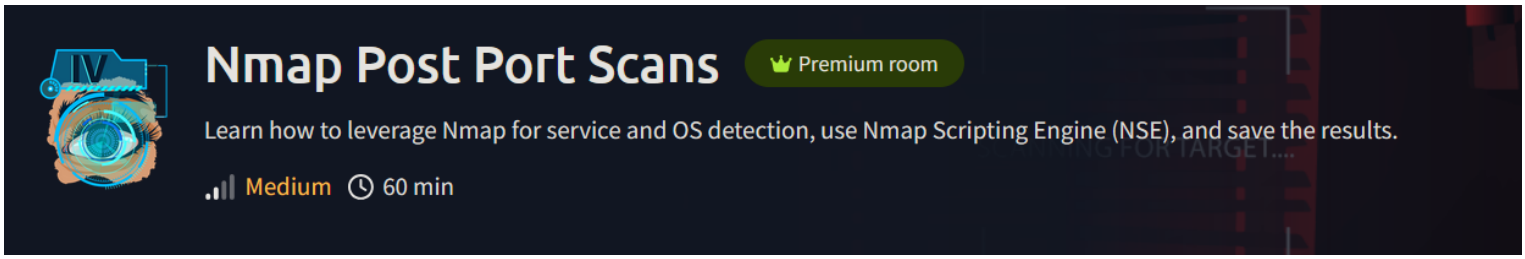
Port Scan Type	Example Command
TCP Null Scan	sudo nmap -sN MACHINE_IP
TCP FIN Scan	sudo nmap -sF MACHINE_IP
TCP Xmas Scan	sudo nmap -sX MACHINE_IP
TCP Maimon Scan	sudo nmap -sM MACHINE_IP
TCP ACK Scan	sudo nmap -sA MACHINE_IP
TCP Window Scan	sudo nmap -sW MACHINE_IP
Custom TCP Scan	sudo nmap --scanflags URGACKPSHRSTSYNFIN MACHINE_IP
Spoofed Source IP	sudo nmap -S SPOOFED_IP MACHINE_IP
Spoofed MAC Address	--spoof-mac SPOOFED_MAC
Decoy Scan	nmap -D DECOY_IP,ME MACHINE_IP
Idle (Zombie) Scan	sudo nmap -sI ZOMBIE_IP MACHINE_IP
Fragment IP data into 8 bytes	-f
Fragment IP data into 16 bytes	-ff

Option	Purpose
--source-port PORT_NUM	specify source port number
--data-length NUM	append random data to reach given length

These scan types rely on setting TCP flags in unexpected ways to prompt ports for a reply. Null, FIN, and Xmas scan provoke a response from closed ports, while Maimon, ACK, and Window scans provoke a response from open and closed ports.

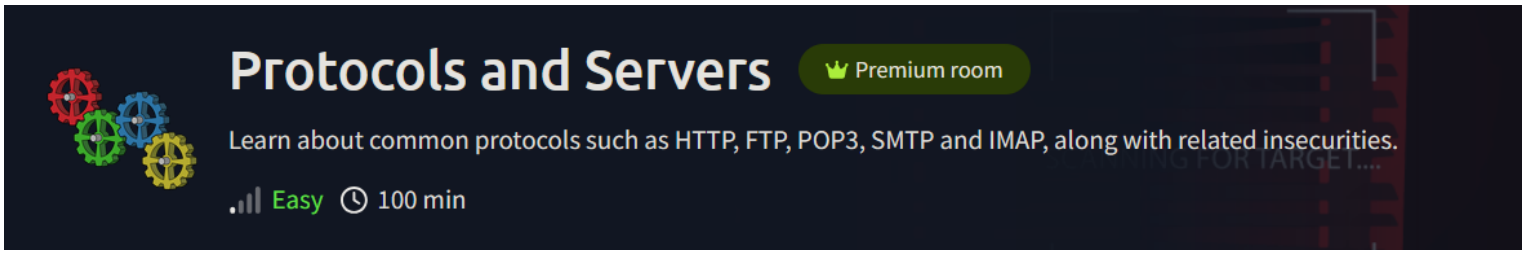
Option	Purpose
--reason	explains how Nmap made its conclusion
-v	verbose

Option	Purpose
-vv	very verbose
-d	debugging
-dd	more details for debugging



In this room, we learned how to detect the running services and their versions along with the host operating system. We learned how to enable traceroute and we covered selecting one or more scripts to aid in penetration testing. Finally, we covered the different formats to save the scan results for future reference. The table below summarizes the most important options we covered in this room.

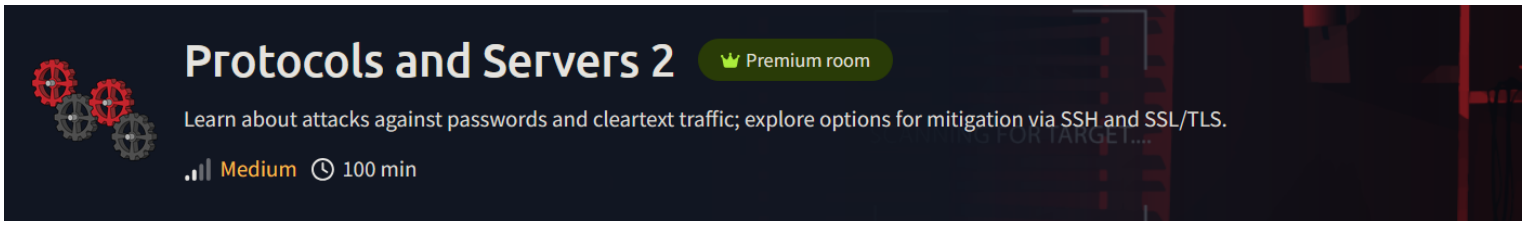
Option	**Meaning**
-sV	determine service/version info on open ports
-sV --version-light	try the most likely probes (2)
-sV --version-all	try all available probes (9)
-O	detect OS
--traceroute	run traceroute to target
--script=SCRIPTS	Nmap scripts to run
-sC or --script=default	run default scripts
-A	equivalent to -sV -O -sC --traceroute
-oN	save output in normal format
-oG	save output in grepable format
-oX	save output in XML format
-oA	save output in normal, XML and Grepable formats



This room covered various protocols, their usage, and how they work under the hood. Many other standard protocols are of interest to attackers. For instance, Server Message Block (SMB) provides shared access to files and printers between networks, and it can be an exciting target. However, this room intends only to give you a good knowledge of a few common protocols and how they work under the hood. One room or even a complete module can't cover all the network protocols.

It is good to remember the default port number for common protocols. Below is a summary of the protocols we covered, sorted in alphabetical order, along with their default port numbers.

Protocol	TCP Port	Application(s)	Data Security
FTP	21	File Transfer	Cleartext
HTTP	80	Worldwide Web	Cleartext
IMAP	143	Email (MDA)	Cleartext
POP3	110	Email (MDA)	Cleartext
SMTP	25	Email (MTA)	Cleartext
Telnet	23	Remote Access	Cleartext



This room covered various protocols, their usage, and how they work under the hood. Three common attacks are:

1. Sniffing Attack
2. MITM Attack
3. Password Attack

For each of the above, we focused both on the attack details and the mitigation steps.

Many other attacks can be conducted against specific servers and protocols. We will provide a list of some related modules.

- Vulnerability Research: This module provides more information about vulnerabilities and exploits.
- Metasploit: This module trains you on how to use Metasploit to exploit target systems.
- Burp Suite: This module teaches you how to use Burp Suite to intercept HTTP traffic and launch attacks related to the web.

It is good to remember the default port number for common protocols. For convenience, the services we covered are listed in the following table sorted by alphabetical order.

Protocol	TCP Port	Application(s)	Data Security
FTP	21	File Transfer	Cleartext
FTPS	990	File Transfer	Encrypted
HTTP	80	Worldwide Web	Cleartext
HTTPS	443	Worldwide Web	Encrypted
IMAP	143	Email (MDA)	Cleartext
IMAPS	993	Email (MDA)	Encrypted
POP3	110	Email (MDA)	Cleartext
POP3S	995	Email (MDA)	Encrypted
SFTP	22	File Transfer	Encrypted
SSH	22	Remote Access and File Transfer	Encrypted
SMTP	25	Email (MTA)	Cleartext

Protocol	TCP Port	Application(s)	Data Security
SMTPS	465	Email (MTA)	Encrypted
Telnet	23	Remote Access	Cleartext

Hydra remains a very efficient tool that you can launch from the terminal to try the different passwords. We summarize its main options in the following table.

Option	Explanation
-l username	Provide the login name
-P WordList.txt	Specify the password list to use
server service	Set the server address and service to attack
-s PORT	Use in case of non-default service port number
-V or -vV	Show the username and password combinations being tried
-d	Display debugging output if the verbose output is not helping