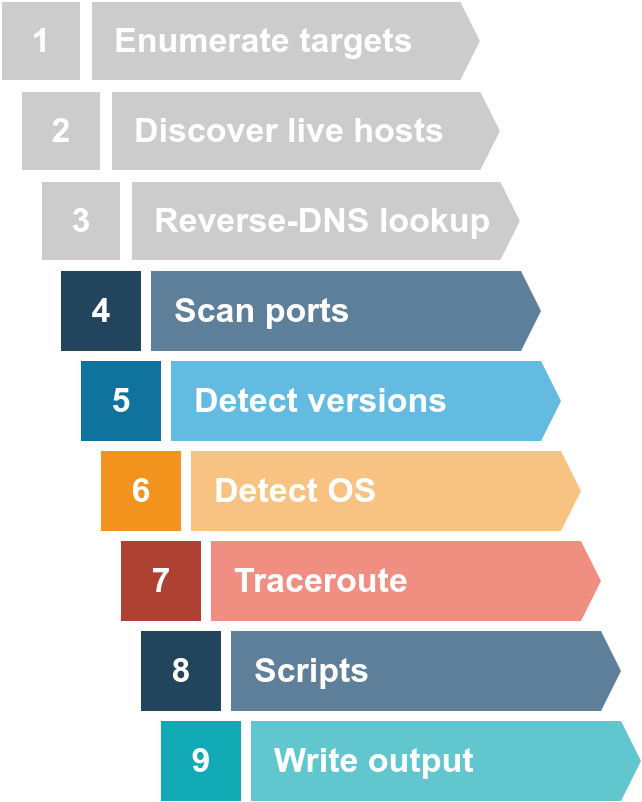
You have learned how ARP, ICMP, TCP, and UDP can detect live hosts by completing this room. Any response from a host is an indication that it is online. Below is a quick summary of the command-line options for Nmap that we have covered.

| **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 |



If you want to range Run nmap -sL -n 10.10.0-255.101-125.

Nmap considers the following six states:

1. **Open**: indicates that a service is listening on the specified port.
2. **Closed**: indicates that no service is listening on the specified port, although the port is accessible. By accessible, we mean that it is reachable and is not blocked by a firewall or other security appliances/programs.
3. **Filtered**: means that Nmap cannot determine if the port is open or closed because the port is not accessible. This state is usually due to a firewall preventing Nmap from reaching that port. Nmap’s packets may be blocked from reaching the port; alternatively, the responses are blocked from reaching Nmap’s host.
4. **Unfiltered**: means that Nmap cannot determine if the port is open or closed, although the port is accessible. This state is encountered when using an ACK scan -sA.
5. **Open|Filtered**: This means that Nmap cannot determine whether the port is open or filtered.
6. **Closed|Filtered**: This means that Nmap cannot decide whether a port is closed or filtered.

In particular, we need to focus on the flags that Nmap can set or unset. We have highlighted the TCP flags in red. Setting a flag bit means setting its value to 1. From left to right, the TCP header flags are:

1. **URG**: Urgent flag indicates that the urgent pointer filed is significant. The urgent pointer indicates that the incoming data is urgent, and that a TCP segment with the URG flag set is processed immediately without consideration of having to wait on previously sent TCP segments.
2. **ACK**: Acknowledgement flag indicates that the acknowledgement number is significant. It is used to acknowledge the receipt of a TCP segment.
3. **PSH**: Push flag asking TCP to pass the data to the application promptly.
4. **RST**: Reset flag is used to reset the connection. Another device, such as a firewall, might send it to tear a TCP connection. This flag is also used when data is sent to a host and there is no service on the receiving end to answer.
5. **SYN**: Synchronize flag is used to initiate a TCP 3-way handshake and synchronize sequence numbers with the other host. The sequence number should be set randomly during TCP connection establishment.
6. **FIN**: The sender has no more data to send.
7. This room covered three types of scans.

| **Port Scan Type** | **Example Command** |
| --- | --- |
| TCP Connect Scan | nmap -sT 10.10.194.86 |
| TCP SYN Scan | sudo nmap -sS 10.10.194.86 |
| UDP Scan | sudo nmap -sU 10.10.194.86 |

1. 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 |

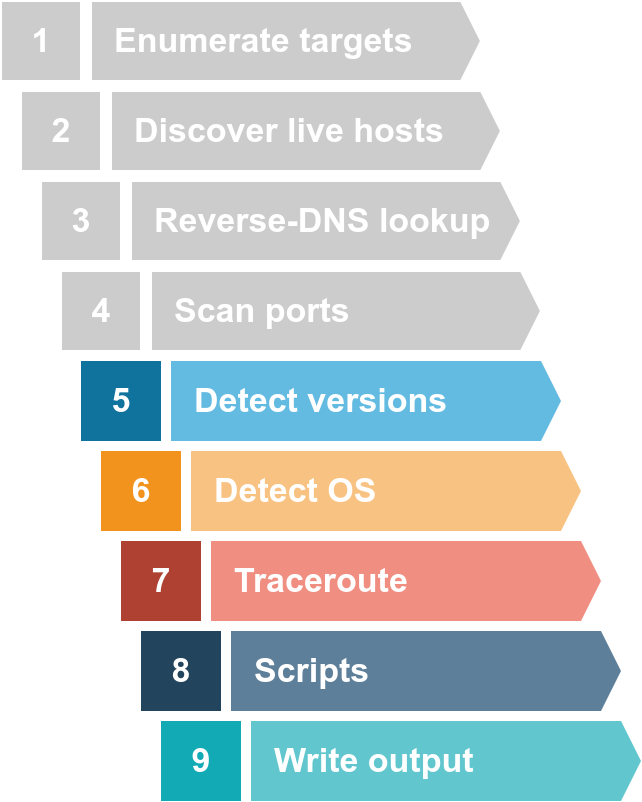
This room covered the following types of scans.

| **Port Scan Type** | **Example Command** |
| --- | --- |
| TCP Null Scan | sudo nmap -sN 10.10.33.170 |
| TCP FIN Scan | sudo nmap -sF 10.10.33.170 |
| TCP Xmas Scan | sudo nmap -sX 10.10.33.170 |
| TCP Maimon Scan | sudo nmap -sM 10.10.33.170 |
| TCP ACK Scan | sudo nmap -sA 10.10.33.170 |
| TCP Window Scan | sudo nmap -sW 10.10.33.170 |
| Custom TCP Scan | sudo nmap --scanflags URGACKPSHRSTSYNFIN 10.10.33.170 |
| Spoofed Source IP | sudo nmap -S SPOOFED\_IP 10.10.33.170 |
| Spoofed MAC Address | --spoof-mac SPOOFED\_MAC |
| Decoy Scan | nmap -D DECOY\_IP,ME 10.10.33.170 |
| Idle (Zombie) Scan | sudo nmap -sI ZOMBIE\_IP 10.10.33.170 |
| 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 |
| -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 |

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 |

In the next room of this module, we learn about various attacks against these protocols and servers along with mitigation steps.

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 |
| 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 |

nmap -sC -sV -p- -T4 --min-rate=9326 -vv [MACHINE IP]

Let’s break this command if it just passed up from your head 😅

* sC : run particular scripts on the target and check what all can happen there
* sV : check for the versions
* -p- : check all the ports
* -T4 : it is to speed up things(max is T5)
* — min-rate=9326 : nmap will send the packets at the rate of 9326 per second, this 9326 is just a random number that I got from my Twitter friend
* -vv this stand for very verbose(refers to details) output