

Name : Ritesh Lakhani
Enrollment No : 22010101099

Metasploit Room

Task 1 Introduction to Metasploit

Metasploit is the most widely used exploitation framework. Metasploit is a powerful tool that can support all phases of a penetration testing engagement, from information gathering to post-exploitation.

Metasploit has two main versions:

- **Metasploit Pro:** The commercial version that facilitates the automation and management of tasks. This version has a graphical user interface (GUI).
- **Metasploit Framework:** The open-source version that works from the command line. This room will focus on this version, installed on the AttackBox and most commonly used penetration testing Linux distributions.

The Metasploit Framework is a set of tools that allow information gathering, scanning, exploitation, exploit development, post-exploitation, and more. While the primary usage of the Metasploit Framework focuses on the penetration testing domain, it is also useful for vulnerability research and exploit development.

The main components of the Metasploit Framework can be summarized as follows;

- **msfconsole:** The main command-line interface.
- **Modules:** supporting modules such as exploits, scanners, payloads, etc.
- **Tools:** Stand-alone tools that will help vulnerability research, vulnerability assessment, or penetration testing. Some of these tools are msfvenom, pattern_create and pattern_offset. We will cover msfvenom within this module, but pattern_create and pattern_offset are tools useful in exploit development which is beyond the scope of this module.

This room will cover the main components of Metasploit while providing you with a solid foundation on how to find relevant exploits, set parameters, and exploit vulnerable services on the target system. Once you have completed this room, you will be able to navigate and use the Metasploit command line comfortably.

Press the **Start Machine** button below.

Start the AttackBox by pressing the **Start AttackBox** button at the top of this page to complete tasks and answer the questions. The AttackBox machine will start in Split-Screen view. If it is not visible, use the blue **Show Split View** button at the top of the page.

Answer the questions below

No answer needed

No answer needed

✓ Correct Answer

Task 2 Main Components of Metasploit

If you wish to familiarize yourself further with these modules, you can find them under the modules folder of your Metasploit installation. For the AttackBox these are under `/opt/metasploit-framework/embedded/framework/modules`

Answer the questions below

What is the name of the code taking advantage of a flaw on the target system?

Exploit

✓ Correct Answer

What is the name of the code that runs on the target system to achieve the attacker's goal?

Payload

✓ Correct Answer

What are self-contained payloads called?

Singles

✓ Correct Answer

Is "windows/x64/pingback_reverse_tcp" among singles or staged payload?

Singles

✓ Correct Answer

Task 3 MfsConsole

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/admin/http/dlink_dir_300_600_exec_noauth	2013-02-04	normal	No	D-Link DIR-600 / DIR-300 Unauthenticated Remote
1	auxiliary/admin/http/netgear_r6700_pass_reset	2020-06-15	normal	Yes	Netgear R6700v3 Unauthenticated LAN Admin Passw
2	auxiliary/dos/cisco/ios_telnet_rocem	2017-03-17	normal	No	Cisco IOS Telnet Denial of Service
3	auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof	2010-12-21	normal	No	Microsoft IIS FTP Server Encoded Response Overf
4	auxiliary/scanner/ssh/juniper_backdoor	2015-12-20	normal	No	Juniper SSH Backdoor Scanner
5	auxiliary/scanner/telnet/brocade_enable_login		normal	No	Brocade Enable Login Check Scanner
6	auxiliary/scanner/telnet/lantronix_telnet_password		normal	No	Lantronix Telnet Password Recovery
7	auxiliary/scanner/telnet/lantronix_telnet_version		normal	No	Lantronix Telnet Service Banner Detection
8	auxiliary/scanner/telnet/satel_cmd_exec	2017-04-07	normal	No	Satel Iberia SenNet Data Logger and Electricity
9	auxiliary/scanner/telnet/telnet_encrypt_overflow		normal	No	Telnet Service Encryption Key ID Overflow Detec
10	auxiliary/scanner/telnet/telnet_login		normal	No	Telnet Login Check Scanner
11	auxiliary/scanner/telnet/telnet_ruggedcom		normal	No	RuggedCom Telnet Password Generator
12	auxiliary/scanner/telnet/telnet_version		normal	No	Telnet Service Banner Detection
13	auxiliary/server/capture/telnet		normal	No	Authentication Capture: Telnet

Interact with a module by name or index, for example use 13 or use auxiliary/server/capture/telnet

msf6 >

Please remember that exploits take advantage of a vulnerability on the target system and may always show unexpected behavior. A low-ranking exploit may work perfectly, and an excellent ranked exploit may not, or worse, crash the target system.

Answer the questions below

How would you search for a module related to Apache?

search apache

✓ Correct Answer

Who provided the auxiliary/scanner/ssh/ssh_login module?

todb

✓ Correct Answer

🔍 Hint

Task 4 Working With Modules

```
msf6 > sessions

Active sessions
=====

  Id  Name      Type      Information                                     Connection
  --  -
  1    meterpreter x64/windows NT AUTHORITY\SYSTEM @ JON-PC 10.10.44.70:4444 -> 10.10.12.229:49163 (10.10.12.229)
  2    meterpreter x64/windows NT AUTHORITY\SYSTEM @ JON-PC 10.10.44.70:4444 -> 10.10.12.229:49186 (10.10.12.229)

msf6 > sessions -i 2
[*] Starting interaction with 2...

meterpreter >
```

Answer the questions below

How would you set the LPORT value to 6666?

set LPORT 6666

✓ Correct Answer

How would you set the global value for RHOSTS to 10.10.19.23 ?

setg RHOSTS 10.10.19.23

✓ Correct Answer

What command would you use to clear a set payload?

unset PAYLOAD

✓ Correct Answer

What command do you use to proceed with the exploitation phase?

exploit

✓ Correct Answer

Task 5 Summary

Task 5 ✓ Summary

As we have seen so far, Metasploit is a powerful tool that facilitates the exploitation process. The exploitation process comprises three main steps; finding the exploit, customizing the exploit, and exploiting the vulnerable service.

Metasploit provides many modules that you can use for each step of the exploitation process. Through this room, we have seen the basic components of Metasploit and their respective use.

It would be best if you also had used the ms17_010_eternalblue exploit to gain access to the target VM.

In the following rooms, we will cover Metasploit and its components in more detail. Once completed, this module should give you a good understanding of the capabilities of Metasploit.

Answer the questions below

No answer needed.

No answer needed

✓ Correct Answer

Name: Ritesh Lakhani


Enrollment No: 22010101099

Nessus Tool :

Task 1:

Introduction about nessus

Task 1 Introduction



Nessus vulnerability scanner is exactly what you think is its! A vulnerability scanner!
It uses techniques similar to Nmap to find and report vulnerabilities, which are then, presented in a nice GUI for us to look at.
Nessus is different from other scanners as it doesn't make assumptions when scanning,
like assuming the web application is running on port 80 for instance.

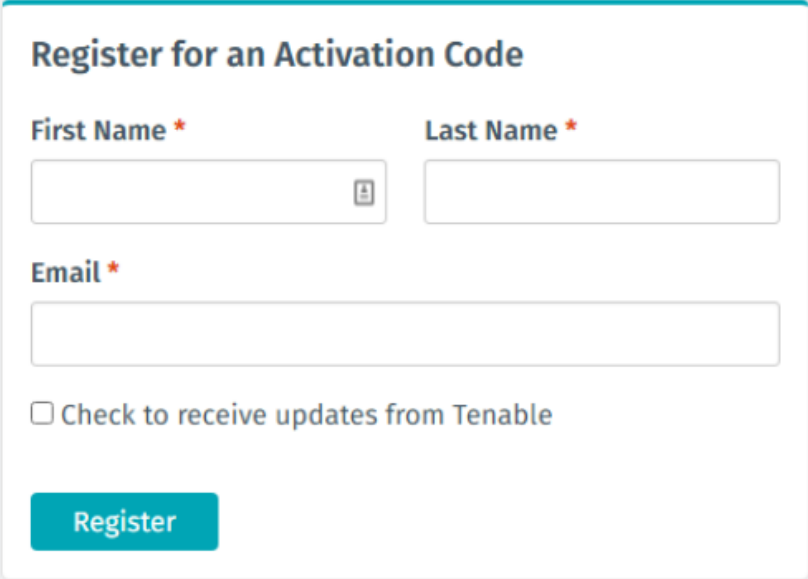
Nessus offers a free and paid service, in which some features are left out from the free to make you more inclined to buy the paid service.
Their pricing is similar to Burp Suite, so unless you got some spare change, we will be just be using their free version.

You can check out their pricing options here: <https://www.tenable.com/products/nessus>

Task 2:

Installation step :

Step #1



The image shows a registration form titled "Register for an Activation Code". It contains three input fields: "First Name" with a red asterisk, "Last Name" with a red asterisk, and "Email" with a red asterisk. The "First Name" field has a small user icon on its right side. Below the email field is a checkbox labeled "Check to receive updates from Tenable". At the bottom of the form is a teal button labeled "Register".

Goto <https://www.tenable.com/products/nessus/nessus-essentials> and register an account.

Click on url and register your self then it shows download button click on it and download the Nessus.

Step #2

 [Nessus-8.12.1-debian6_amd64.deb](#)

Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3, 2018, 2019, 2020 AMD64

42.9 MB

Oct 29, 2020

[Checksum](#)

We will then download the Nessus-8.12.1-debian6_amd64.deb file

Save it to your **/Downloads/** folder

No answer needed

✓ Correct Answer

Step #3

In the terminal we will navigate to that folder and run the following command:

`sudo dpkg -i package_file.deb`

Remember to replace **package_file.deb** with the file name you downloaded.

```
A root ~/Downloads
$ sudo dpkg -i Nessus-8.12.1-debian6_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 366461 files and directories currently installed.)
Preparing to unpack Nessus-8.12.1-debian6_amd64.deb ...
Unpacking nessus (8.12.1) ...
Setting up nessus (8.12.1) ...
Unpacking Nessus Scanner Core Components...

- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://kali:8834/ to configure your scanner
```

No answer needed

✓ Correct Answer

After downloading perform given command and install Nessus

Step #4

We will now start the Nessus Service with the command:

`sudo /bin/systemctl start nessusd.service`

```
A root ~/Downloads
$ sudo /bin/systemctl start nessusd.service
```

No answer needed

✓ Correct Answer

Now for starting run above code

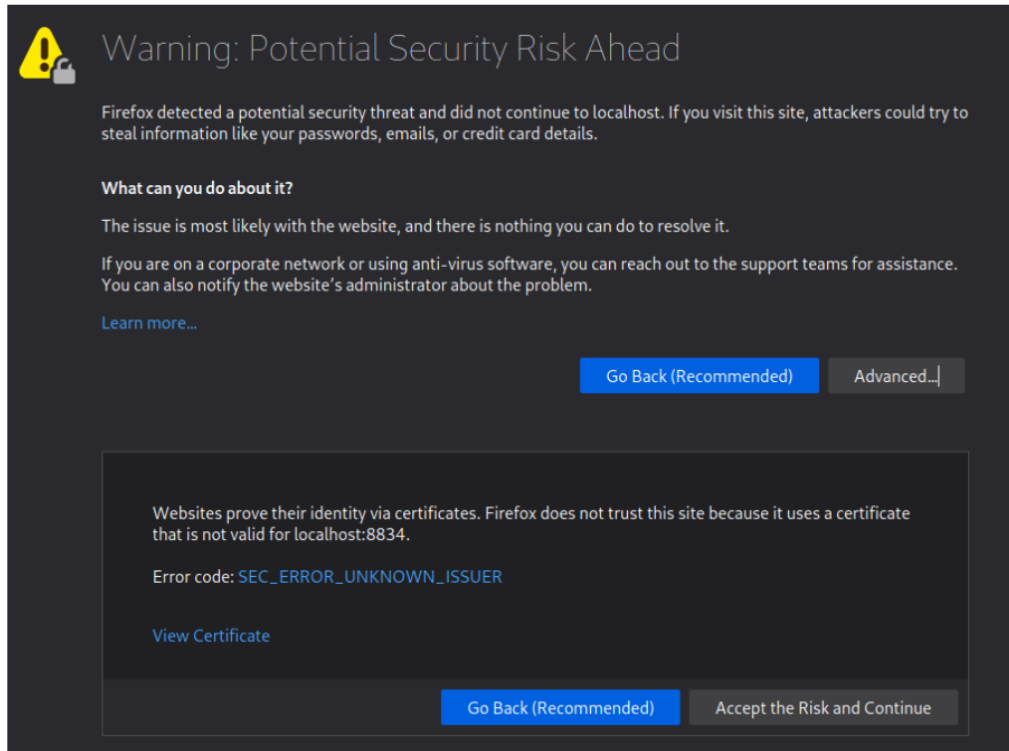
Step #5

Open up Firefox and goto the following URL:

<https://localhost:8834/>

You may be prompted with a security risk alert.

Click **Advanced...** -> **Accept the Risk and Continue**



Now go to that url and start the Nessus

Then follow steps accordingly

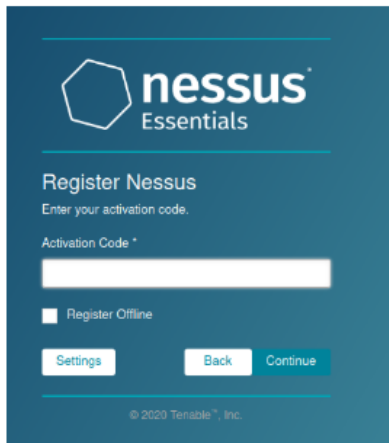
Step #6

Next, we will set up the scanner.

Select the option **Nessus Essentials**



Clicking the **Skip** button will bring us to a page, which we will input that code we got in the email from Nessus.



No answer needed

✓ Correct Answer

Step #7

Fill out the **Username** and **Password** fields. Make sure to use a strong password!

No answer needed

✓ Correct Answer

Step #8

Nessus will now install the **plugins** required for it to function.

This will take some time, which will depend on your internet connection and the hardware attached to your VM.

If the progress bar appears to be **not moving**, it means you do not have **enough space** on the VM to install.

No answer needed

✓ Correct Answer

Log in with the account credentials you made earlier.

No answer needed ✓ Correct Answer


You have now successfully installed **Nessus**!

No answer needed ✓ Correct Answer

Task 3:


Navigations and Scans

DISCOVERY




Host Discovery
A simple scan to discover live hosts and open ports.


VULNERABILITIES




Basic Network Scan
A full system scan suitable for any host.




Advanced Scan
Configure a scan without using any recommendations.




Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.




Malware Scan
Scan for malware on Windows and Unix systems.




Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.




Web Application Tests
Scan for published and unknown web vulnerabilities.




Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.




Badlock Detection
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.




Bash Shellshock Detection
Remote and local checks for CVE-2014-4271 and CVE-2014-7169.




DHROWN Detection
Remote checks for CVE-2016-0803.




Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.




Shadow Brokers Scan
Scan for vulnerabilities disclosed in the Shadow Brokers leaks.




Spectre and Meltdown
Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754.



WannaCry Ransomware
Remote and local checks for MS17-010.



Hippie20 Remote Scan
A remote scan to fingerprint hosts potentially running the Tweek stack in the network.



ZeroLogon Remote Scan
A remote scan to detect Microsoft Netlogon Elevation of Privilege (ZeroLogon).

Answer the questions below

What is the name of the **button** which is used to launch a scan?

New Scan

✓ Correct Answer

🔍 Hint

What side menu option allows us to create **custom templates**?

Policies

✓ Correct Answer

🔍 Hint

What menu allows us to change **plugin** properties such as hiding them or changing their severity?

Plugin Rules

✓ Correct Answer

🔍 Hint

In the '**Scan Templates**' section after clicking on '**New Scan**', what scan allows us to see simply what hosts are alive?

Host Discovery

✓ Correct Answer

One of the most useful scan types, which is considered to be '**suitable for any host**'?

Basic Network Scan

✓ Correct Answer

What scan allows you to '**Authenticate to hosts and enumerate missing updates**'?

Credentialed Patch Audit

✓ Correct Answer

What scan is specifically used for scanning **Web Applications**?

Web Application Tests

✓ Correct Answer

Task 4: Scanning

Create a new '**Basic Network Scan**' targeting the deployed VM. What option can we set under '**BASIC**' (on the left) to set a time for this scan to run? This can be very useful when network congestion is an issue.

Schedule

✓ Correct Answer

Under '**DISCOVERY**' (on the left) set the '**Scan Type**' to cover ports 1-65535. What is this type called?

Port scan (all ports)

✓ Correct Answer

What '**Scan Type**' can we change to under '**ADVANCED**' for lower bandwidth connection?

Scan low bandwidth links

✓ Correct Answer



With these options set, launch the scan.

No answer needed

✓ Correct Answer

After the scan completes, which '**Vulnerability**' in the '**Port scanners**' family can we view the details of to see the open ports on this host?

Nessus SYN scanner

✓ Correct Answer

What **Apache HTTP Server Version** is reported by Nessus?

2.4.99

✓ Correct Answer

🔍 Hint

Task 5 : Scanning A WebApp

(Running this Scan will take some time to complete, please be patient)

Answer the questions below

What is the plugin id of the plugin that determines the HTTP server type and version?

10107

✓ Correct Answer

🔍 Hint

What authentication page is discovered by the scanner that transmits credentials in cleartext?

login.php

✓ Correct Answer

🔍 Hint

What is the file extension of the config backup?

.bak

✓ Correct Answer

🔍 Hint

Which directory contains example documents? (This will be in a php directory)

/external/phpids/0.6/docs/examples/

✓ Correct Answer

🔍 Hint

What vulnerability is this application susceptible to that is associated with X-Frame-Options?

Clickjacking

✓ Correct Answer

🔍 Hint

Name : Ritesh Lakhani

EnrollmentNo:22010101099

Task 1 : Introduction

Room completed (100%)

This room explains the steps that *Nmap* carries out to discover the systems that are online before port-scanning. This stage is crucial because trying to port-scan offline systems will only waste time and create unnecessary noise on the network.

We present the different approaches that *Nmap* uses to discover live hosts. In particular, we cover:

1. **ARP** scan: This scan uses **ARP** requests to discover live hosts
2. **ICMP** scan: This scan uses **ICMP** requests to identify live hosts
3. **TCP/UDP** ping scan: This scan sends packets to **TCP** ports and **UDP** ports to determine live hosts.

We also introduce two scanners, **arp-scan** and **masscan**, and explain how they overlap with part of *Nmap*'s host discovery.

As already mentioned, starting with this room, we will use *Nmap* to discover systems and services actively. *Nmap* was created by Gordon Lyon (Fyodor), a network security expert and open source programmer. It was released in 1997. *Nmap*, short for Network Mapper, is free, open-source software released under GPL license. *Nmap* is an industry-standard tool for mapping networks, identifying live hosts, and discovering running services. *Nmap*'s scripting engine can further extend its functionality, from fingerprinting services to exploiting vulnerabilities. A *Nmap* scan usually goes through the steps shown in the figure below, although many are optional and depend on the command-line arguments you provide.



Answer the questions below

Some of these questions will require the use of a static site to answer the task questions, while others require the use of the AttackBox and the target VM.

No answer needed

✓ Correct Answer

Task 2 Subnetworks :

Answer the questions below

Send a packet with the following:

Send Packet

From:
computer1

To:
computer1

Packet Type:
arp_request

Data:
computer6

Send Packet

- From computer1
- To computer1 (to indicate it is broadcast)
- Packet Type: "ARP Request"
- Data: computer6 (because we are asking for computer6 MAC address using ARP Request)

How many devices can see the ARP Request?

4

✓ Correct Answer

🔍 Hint

Did computer6 receive the ARP Request? (Y/N)

N

✓ Correct Answer

Send a packet with the following:

Send Packet

From:
computer4

To:
computer4

Packet Type:
arp_request

Data:
computer6

Send Packet

- From computer4
- To computer4 (to indicate it is broadcast)
- Packet Type: "ARP Request"
- Data: computer6 (because we are asking for computer6 MAC address using ARP Request)

How many devices can see the ARP Request?

4

✓ Correct Answer

🔍 Hint

Did computer6 reply to the ARP Request? (Y/N)

Y

✓ Correct Answer

Task 3 : Enumerating Targets

We mentioned the different *techniques* we can use for scanning in Task 1. Before we explain each in detail and put it into use against a live target, we need to specify the targets we want to scan. Generally speaking, you can provide a list, a range, or a subnet. Examples of target specification are:

- list: `MACHINE_IP scanme.nmap.org example.com` will scan 3 IP addresses.
- range: `10.11.12.15-20` will scan 6 IP addresses: `10.11.12.15`, `10.11.12.16`, ..., and `10.11.12.20`.
- subnet: `MACHINE_IP/30` will scan 4 IP addresses.

You can also provide a file as input for your list of targets, `nmap -iL list_of_hosts.txt`.

If you want to check the list of hosts that Nmap will scan, you can use `nmap -sL TARGETS`. This option will give you a detailed list of the hosts that Nmap will scan without scanning them; however, Nmap will attempt a reverse-DNS resolution on all the targets to obtain their names. Names might reveal various information to the pentester. (If you don't want Nmap to the DNS server, you can add `-n`.)

Launch the AttackBox using the Start AttackBox button, open the terminal when the AttackBox is ready, and use Nmap to answer the following.

Answer the questions below

What is the first IP address Nmap would scan if you provided `10.10.12.13/29` as your target?

✓ Correct Answer

🔍 Hint

How many IP addresses will Nmap scan if you provide the following range `10.10.0-255.101-125`?

✓ Correct Answer

🔍 Hint

Task 4 : Discovering Live Hosts

Answer the questions below

Send a packet with the following:

- From computer1
- To computer3
- Packet Type: "Ping Request"

What is the type of packet that computer1 sent before the ping?

ARP Request

✓ Correct Answer

What is the type of packet that computer1 received before being able to send the ping?

ARP Response

✓ Correct Answer

How many computers responded to the ping request?

1

✓ Correct Answer

Send a packet with the following:

- From computer2
- To computer5
- Packet Type: "Ping Request"

What is the name of the first device that responded to the first ARP Request?

router

✓ Correct Answer

What is the name of the first device that responded to the second ARP Request?

computer5

✓ Correct Answer

Send another Ping Request. Did it require new ARP Requests? (Y/N)

N

✓ Correct Answer

Task 5 : Nmap Host Discovery Using ARP

02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.15? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.15? Tell 10.10.210.6
Address Resolution Protocol: Protocol Packets: 1207 - Displayed: 512 (42.4%) Profile: Default			

If you have closed the network simulator, click on the "Visit Site" button in Task 2 to display it again.

Answer the questions below

We will be sending broadcast ARP Requests packets with the following options:

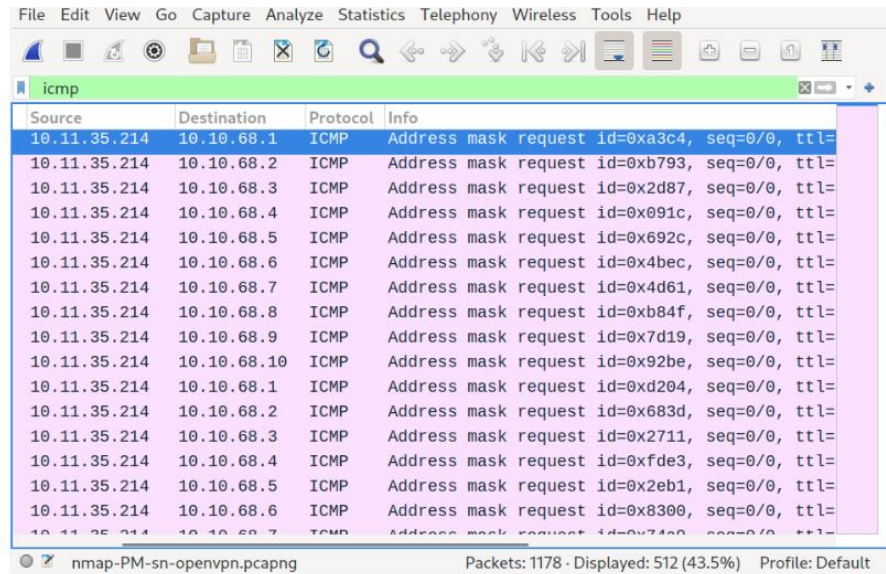
- From computer1
- To computer1 (to indicate it is broadcast)
- Packet Type: "ARP Request"
- Data: try all the possible eight devices (other than computer1) in the network: computer2, computer3, computer4, computer5, computer6, switch1, switch2, and router.

How many devices are you able to discover using ARP requests?

3

✓ Correct Answer

Task 6 : Nmap Host Discovery Using ICMP



The image shows a Wireshark packet capture window with the filter 'icmp'. The packet list shows 20 ICMP address mask requests from source 10.11.35.214 to various destinations in the 10.10.68.1-10.10.68.10 range. The packet details pane shows the structure of an ICMP address mask request.

Source	Destination	Protocol	Info
10.11.35.214	10.10.68.1	ICMP	Address mask request id=0xa3c4, seq=0/0, ttl=
10.11.35.214	10.10.68.2	ICMP	Address mask request id=0xb793, seq=0/0, ttl=
10.11.35.214	10.10.68.3	ICMP	Address mask request id=0x2d87, seq=0/0, ttl=
10.11.35.214	10.10.68.4	ICMP	Address mask request id=0x091c, seq=0/0, ttl=
10.11.35.214	10.10.68.5	ICMP	Address mask request id=0x692c, seq=0/0, ttl=
10.11.35.214	10.10.68.6	ICMP	Address mask request id=0x4bec, seq=0/0, ttl=
10.11.35.214	10.10.68.7	ICMP	Address mask request id=0x4d61, seq=0/0, ttl=
10.11.35.214	10.10.68.8	ICMP	Address mask request id=0xb84f, seq=0/0, ttl=
10.11.35.214	10.10.68.9	ICMP	Address mask request id=0x7d19, seq=0/0, ttl=
10.11.35.214	10.10.68.10	ICMP	Address mask request id=0x92be, seq=0/0, ttl=
10.11.35.214	10.10.68.1	ICMP	Address mask request id=0xd204, seq=0/0, ttl=
10.11.35.214	10.10.68.2	ICMP	Address mask request id=0x683d, seq=0/0, ttl=
10.11.35.214	10.10.68.3	ICMP	Address mask request id=0x2711, seq=0/0, ttl=
10.11.35.214	10.10.68.4	ICMP	Address mask request id=0xfde3, seq=0/0, ttl=
10.11.35.214	10.10.68.5	ICMP	Address mask request id=0x2eb1, seq=0/0, ttl=
10.11.35.214	10.10.68.6	ICMP	Address mask request id=0x8300, seq=0/0, ttl=
10.11.35.214	10.10.68.7	ICMP	Address mask request id=0x74d0, seq=0/0, ttl=

nmmap-PM-sn-openvpn.pcapng Packets: 1178 · Displayed: 512 (43.5%) Profile: Default

Answer the questions below

What is the option required to tell Nmap to use ICMP Timestamp to discover live hosts?

-PP

✓ Correct Answer

What is the option required to tell Nmap to use ICMP Address Mask to discover live hosts?

-PM

✓ Correct Answer

What is the option required to tell Nmap to use ICMP Echo to discover live hosts?

-PE

✓ Correct Answer

Task 7 : Nmap Host Discovery Using TCP and UDP

Masscan

On a side note, Masscan uses a similar approach to discover the available systems. However, to finish its network scan quickly, Masscan is quite aggressive with the rate of packets it generates. The syntax is quite similar: `-p` can be followed by a port number, list, or range. Consider the following examples:

- `masscan MACHINE_IP/24 -p443`
- `masscan MACHINE_IP/24 -p80,443`
- `masscan MACHINE_IP/24 -p22-25`
- `masscan MACHINE_IP/24 --top-ports 100`

Masscan is not installed on the AttackBox; however, it can be installed using `apt install masscan`.

Answer the questions below

Which TCP ping scan does not require a privileged account?

TCP SYN Ping

✓ Correct Answer

Which TCP ping scan requires a privileged account?

TCP ACK Ping

✓ Correct Answer

What option do you need to add to Nmap to run a TCP SYN ping scan on the telnet port?

-PS23

✓ Correct Answer

🔍 Hint

Task 8 : Using Reverse-DNS Lookup

Task 8 🟢 Using Reverse-DNS Lookup

Nmap's default behaviour is to use reverse-DNS online hosts. Because the hostnames can reveal a lot, this can be a helpful step. However, if you don't want to send such DNS queries, you use `-n` to skip this step.

By default, Nmap will look up online hosts; however, you can use the option `-R` to query the DNS server even for offline hosts. If you want to use a specific DNS server, you can add the `-dns-servers DNS_SERVER` option.

Answer the questions below

We want Nmap to issue a reverse DNS lookup for all the possible hosts on a subnet, hoping to get some insights from the names. What option should we add?

-R

✓ Correct Answer

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

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
<code>-n</code>	no DNS lookup
<code>-R</code>	reverse-DNS lookup for all hosts
<code>-sn</code>	host discovery only

Answer the questions below

Ensure you have taken note of all the Nmap options explained in this room. To continue learning about Nmap, please join the room [Nmap Basic Port Scans](#), which introduces the basic types of port scans.

No answer needed

✓ Correct Answer