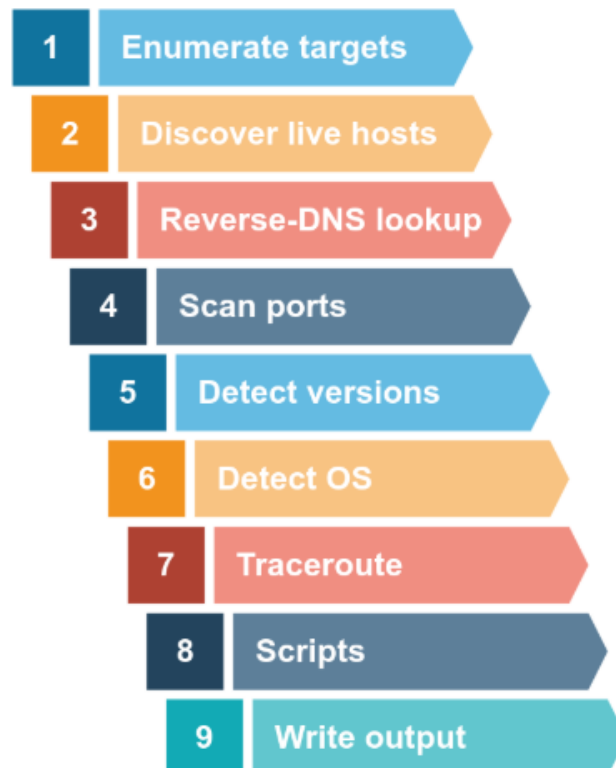


Lab Practical 13:

1. Nmap Live Host Discovery

Perform nmap lab in tryhackme website

- Task 1 : Introduction

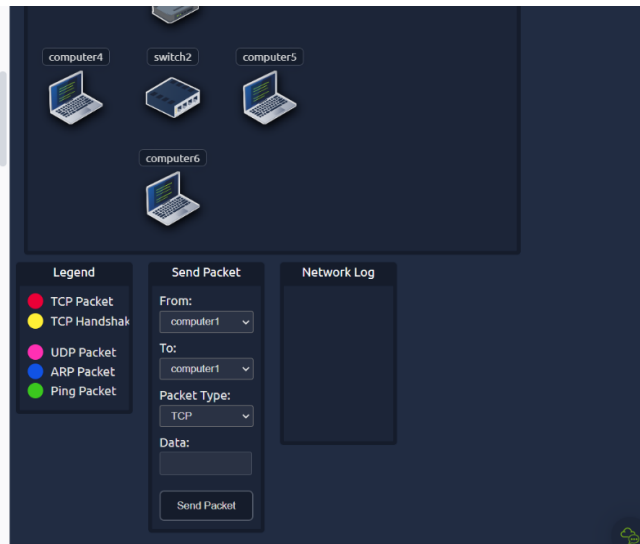
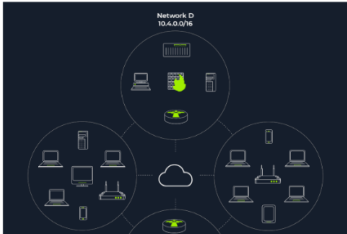


- Task 2 : Subnetworks

Task 2 Subnetworks

Let's review a couple of terms before we move on to the main tasks. A *network segment* is a group of computers connected using a shared medium. For instance, the medium can be the Ethernet switch or WiFi access point. In an IP network, a *subnetwork* is usually the equivalent of one or more network segments connected together and configured to use the same router. The network segment refers to a physical connection, while a subnetwork refers to a logical connection.

In the following network diagram, we have four network segments or subnetworks. Generally speaking, your system would be connected to one of these network segments/subnetworks. A subnetwork, or simply a subnet, has its own IP address range and is connected to a more extensive network via a router. There might be a *firewall* enforcing security policies depending on each network.



The interface shows a network diagram with four computers (computer4, computer5, computer6) and a switch (switch2) connected to a central cloud. Below the diagram is a legend for packet types: TCP Packet (red), TCP Handshake (yellow), UDP Packet (pink), ARP Packet (blue), and Ping Packet (green). To the right of the legend is a 'Send Packet' section with fields for 'From:' (computer1), 'To:' (computer1), 'Packet Type:' (TCP), and 'Data:'. A 'Send Packet' button is at the bottom. To the right of the 'Send Packet' section is a 'Network Log' section.

Date: 07/03/2025

1. Question -1

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



2. Question -2

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)

Answer:

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**

A-1 : Address range(10.10.12.8 to 10.10.12.15)

A-2 : (0-255)=256 & (101-125) = 25

256*25=6400

Answer the questions below

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

10.10.12.8

✓ Correct Answer

💡 Hint

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

6400

✓ Correct Answer

💡 Hint

▪ **Task -4 : Discovering Live Hosts**

Q-1:

- **A-1 : Arp request would be send to find reciver**
- **A-2 : Arp response send back to computer1**
- **A-3 : Only receiver will response ping request,(in our case it's computer3)**

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?

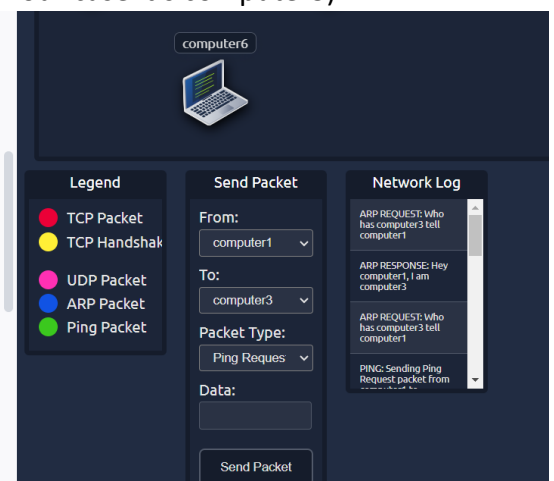
ARP Response

✓ Correct Answer

How many computers responded to the ping request?

1

✓ Correct Answer



Q-2:

- **A-1** : Router will be respond to computer1 that reciver is not found in local network.
- **A-2** : computer5 will send second Arp response.
- **A-3** : Only Once Arp Request is send to located computer5.

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?

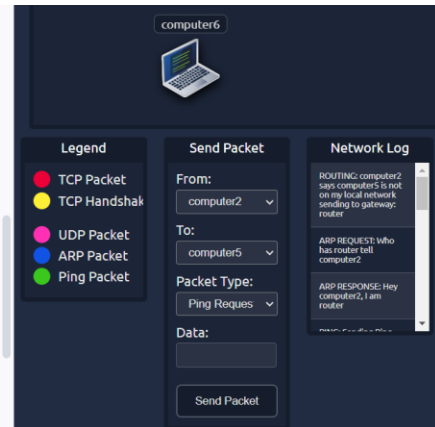
computer5

✓ Correct Answer

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

N

✓ Correct Answer



Task -5 : Nmap Host Discovery Using ARP

A-1: connected device only will receive arp request (hear it is Computer2,computer3,and router)

Answer the questions below

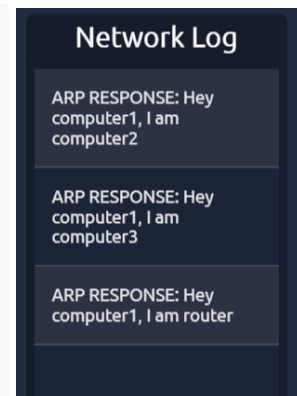
We will be sending broadcast ARP Requests packets with the following options:

- 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

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

Date: 07/03/2025

Task -7 : Nmap Host Discovery Using TCP and UDP

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

Nmap's default behaviour is to use reverse-DNS on live 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 live 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.

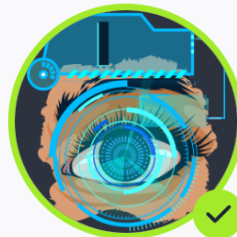
Answer the questions below

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

Task -9 : Summary



Congratulations on completing Nmap Live Host Discovery!!! 🎉

Points earned

🎯 160

Completed tasks

✅ 9

Room type

👤 Walkthrough

Difficulty

📶 Medium

Streak

🔥 1

2. Nessus

Learn how to set up and use Nessus, a popular vulnerability scanner

Task 1: Introduction

Nessus is a widely used vulnerability scanning tool in the field of cyber security and security testing. Nessus is a platform developed by Tenable that scans for security vulnerabilities in devices, applications, operating systems, cloud services, and other network resources. It is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer, that you have connected with any network. It does this by running over 1200 checks on a given computer, to see if any of these attacks could be used to break into the computer or otherwise harm it.

Task 2: Installation

1. Download Nessus:

- Navigate to the <https://www.tenable.com/downloads/nessus> page
- Choose the appropriate version for your operating system and Download

2. Install Nessus:

- Open a terminal and navigate to the directory where the Nessus package was downloaded.
- Run the following command:

```
(kali㉿kali)-[~]  
$ cd Downloads  
  
(kali㉿kali)-[~/Downloads]  
$ sudo dpkg -i ./Nessus-10.8.3-ubuntu1604_amd64.deb
```

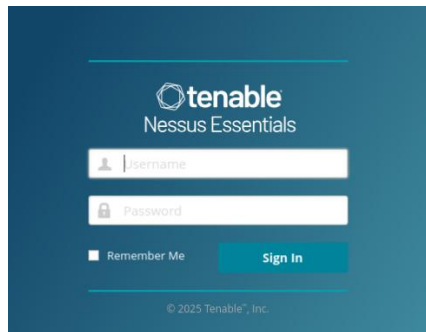
3. Start Nessus Service:

- start the Nessus service by following command:

```
(kali㉿kali)-[~/Downloads]  
$ sudo systemctl start nessusd.service  
[sudo] password for kali:  
  
(kali㉿kali)-[~/Downloads]  
$
```

4. Access Nessus Web Interface:

- Open a web browser and navigate to <https://localhost:8834>.
- Follow the setup instructions to create an administrator account and activate Nessus using the activation code obtained during the download process.

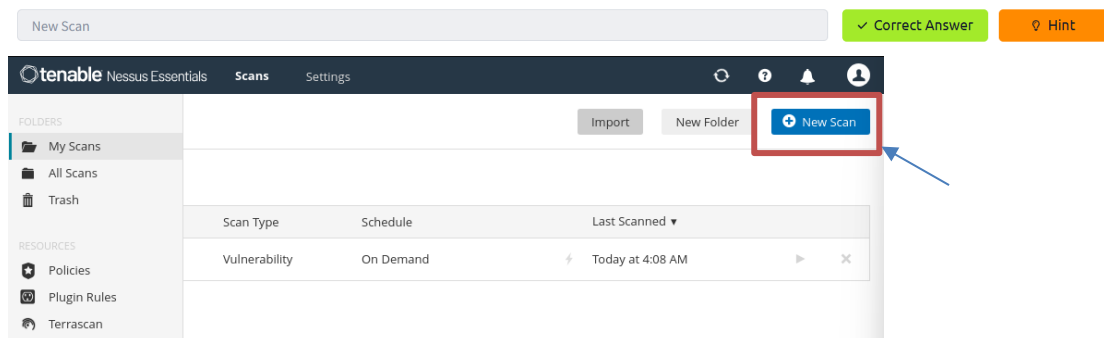


Task 3: Navigation and Scans

Answer below Questions:

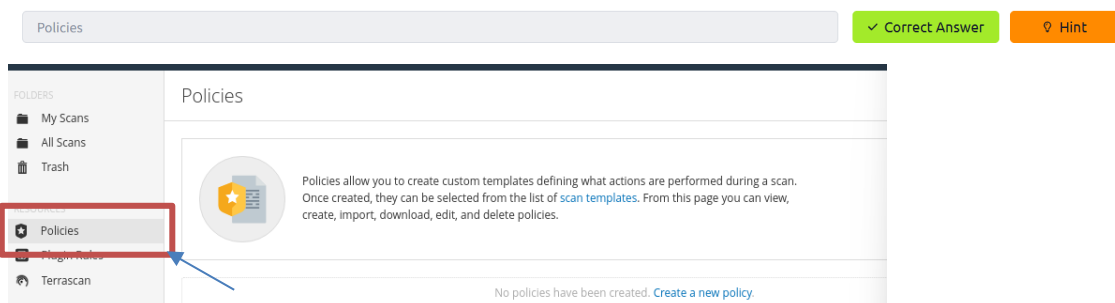
1. Q1 :

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



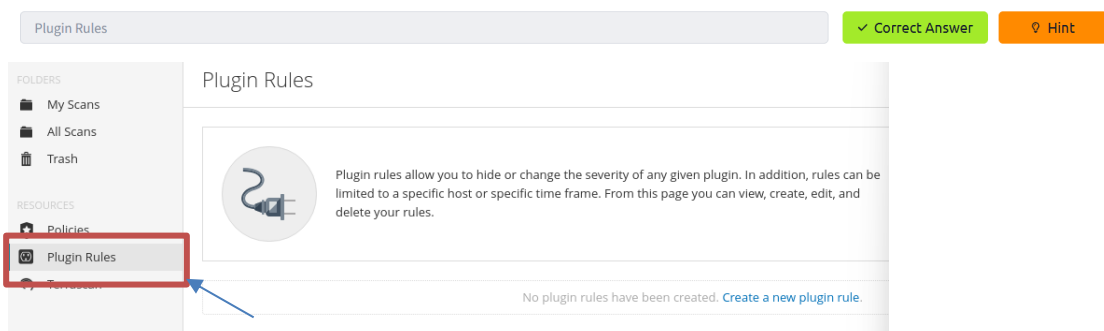
2. Q2:

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



3. Q3:

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



Date: 07/03/2025

4. Q4:

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

Scanner

DISCOVERY



Host Discovery

A simple scan to discover live hosts and open ports.

5. Q5:

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

Basic Network Scan

✓ Correct Answer

VULNERABILITIES



Basic Network Scan

A full system scan suitable for any host.

6. Q6:

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

Credentialed Patch Audit

✓ Correct Answer



Credentialed Patch Audit

Authenticate to hosts and enumerate missing updates.

7. Q7:

What scan is specifically used for scanning Web Applications?

Web Application Tests

✓ Correct Answer



Web Application Tests

Scan for published and unknown web vulnerabilities using Nessus Scanner.

Date: 07/03/2025

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.

Answer below Questions:

1. Q1 :

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

Settings **Plugins**

BASIC
General
Schedule
Notifications
DISCOVERY
REPORT
ADVANCED

Enabled

NOTE: Only one schedule can be enabled. Any other scheduled scans will be disabled. Upgrade to Nessus Professional

Frequency: Once
Starts: 05:00 2025-02-02
Timezone: America/New York
Summary: Once on Sunday, February 2nd, 2025 at 5:00 AM

2. Q2:

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

Settings **Plugins**

BASIC
DISCOVERY
REPORT
ADVANCED

Scan Type: Port scan (all ports)

General Settings:

3. Q3:

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

Scan low bandwidth links ✓ Correct Answer

Settings **Credentials** **Plugins**

BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED

Scan Type

Scan low bandwidth links
Default
Scan low bandwidth links
Custom
2 simultaneous checks per host (max)

4. Q4:

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



Date: 07/03/2025

5. Q5:

What Apache HTTP Server Version is reported by Nessus?

2.4.99

✓ Correct Answer

🔍 Hint

Task 5: Scanning a Web Application!

Run a Web Application scan on the VM!

1. Q1:

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

10107

✓ Correct Answer

🔍 Hint

INFO	HTTP Server Type and Version	Web Servers	1
Plugin Details			
Severity:	Info		
ID:	10107		
Version:	1.141		
Type:	remote		
Family:	Web Servers		
Published:	January 4, 2000		
Modified:	October 30, 2020		

2. Q2:

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

login.php

✓ Correct Answer

🔍 Hint

3. Q3:

What is the file extension of the config backup?

.bak

✓ Correct Answer

🔍 Hint

4. Q4:

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

/external/phpids/0.6/docs/examples/

✓ Correct Answer

🔍 Hint

5. Q5:

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

Clickjacking

✓ Correct Answer

🔍 Hint

Sev ▼	CVSS ▼	VPR ▼	EPSS ▼	Name ▲
MEDIUM	4.3 *			Web Application Potentially Vulnerable to Clickjacking