

CS23532-COMPUTER NETWORKS-LAB MANUAL

Practical -8

Name: Tharunraj

RegNo:230701362

AIM:- To Discover Live Hosts Using Nmap Scans (ARP, ICMP, TCP/UDP) on the TryHackMe Platform
Room Link :<https://tryhackme.com/room/nmap01>

This experiment outlines the processes that Nmap takes before port-scanning to find which systems are online. **This stage is critical since attempting to port-scan offline systems will merely waste time and create unneeded network noise** (because it is active recon)

The following is the information that will be covered in an attempt to discover live hosts:

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.

There will be two scanners introduced:

1. arp-scan
2. masscan

Nmap (Network Mapper) — It is a well-known tool for mapping networks, **locating live hosts**, and **detecting running services**. Nmap's scripting engine can be used to extend its capabilities, such as **fingerprinting services** and **exploiting flaws**.

The scans typically follow the steps represented in the image below, but several are optional and are conditional on the “command-line” options provided prior to the scan:

1

Enumerate targets

2

Discover live hosts

3

Reverse-DNS lookup

4

Scan ports

5

Detect versions

6

Detect OS

7

Traceroute

8

Scripts

9

Write output

Task 1:Introduction

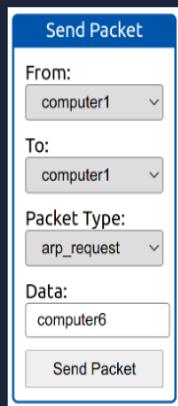
Some of these questions will require the use of a static site to answer the task questions, while others require the use of the AttackBox.

No answer needed

✓ Correct Answer

Task 2:Subnetworks

Send a packet with the following:



- 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

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

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

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

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

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

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

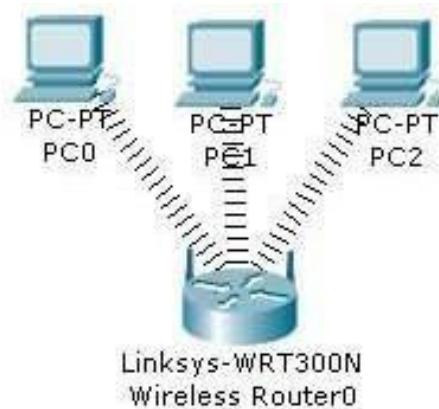
✓ Correct Answer

RESULT:

Thus To Discover Live Hosts Using Nmap Scans (ARP, ICMP, TCP/UDP) on the TryHackMe Platform Room has been executed successfully.

AIM:-b) Configuration of Wireless LAN using CISCO Packet Tracer.

Design a topology with three PCs connected from Linksys Wireless routers.



Perform following configuration:-

- Configure Static IP on PC and Wireless Router
- Set SSID to MotherNetwork
- Set IP address of router to 192.168.0.1, PC0 to 192.168.0.2, PC1 to 192.168.0.3 and PC2 to 192.168.0.4.
- Secure your network by configuring WAP key on Router
- Connect PC by using WAP key

To complete these tasks follow these step by step instructions:-

Step1:- Click on wireless router,

- Select Administration tab from top Menu, set username and password to admin and click on Save Setting.



- Next click on wireless tab and set default SSID to MotherNetwork.
- Now Select wireless security and change Security Mode to WEP



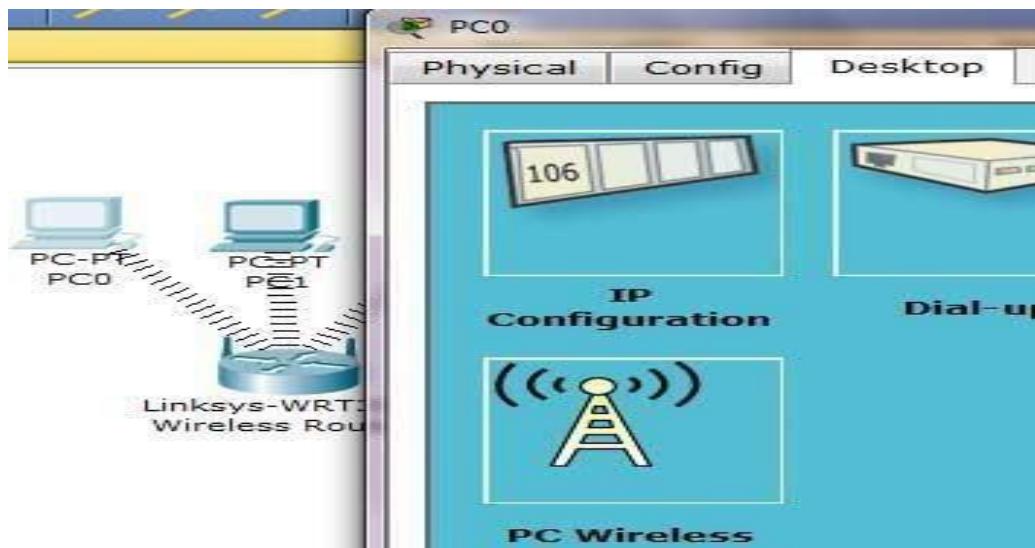
- Set Key1 to 0123456789



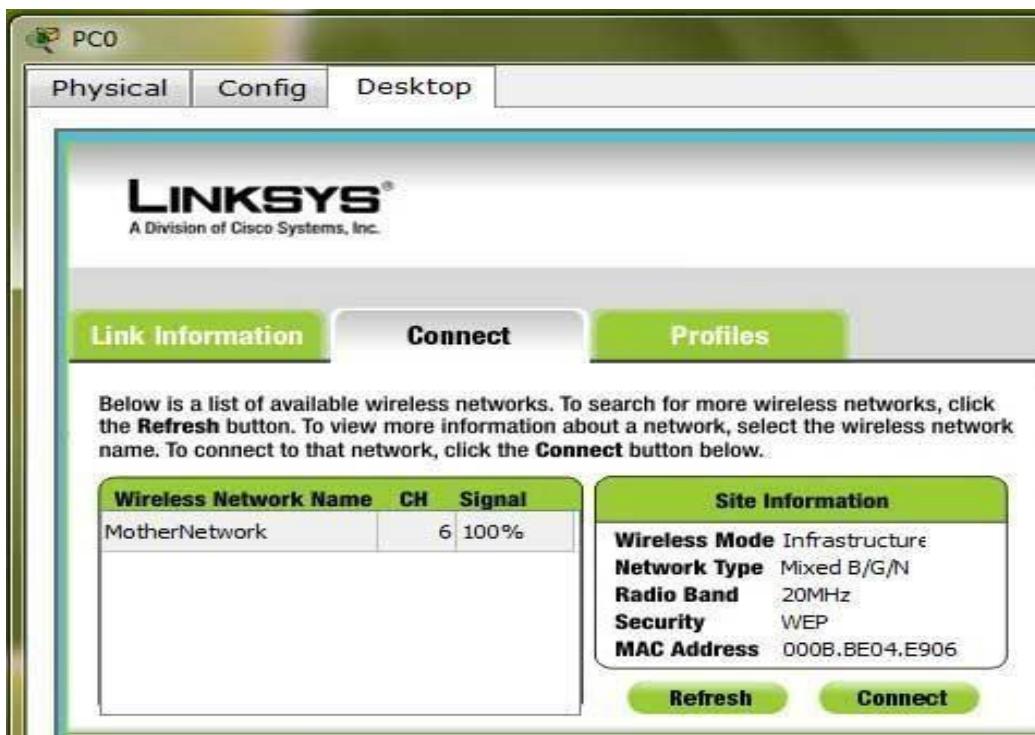
- Again go in the end of page and Click on Save Setting
- Now we have completed all given task on Wireless router. Now configure the static IP on all three PC's
- Double click on pc select Desktop tab click on IP configuration select Static IP and set IP as given below

PC	IP	Subnet Mask	Default Gateway
PC0	192.168.0.2	255.255.255.0	192.168.0.1
PC1	192.168.0.3	255.255.255.0	192.168.0.1
PC2	192.168.0.4	255.255.255.0	192.168.0.1

- Now it's time to connect PC's from Wireless router. To do so click PC select Desktop click on PC Wireless

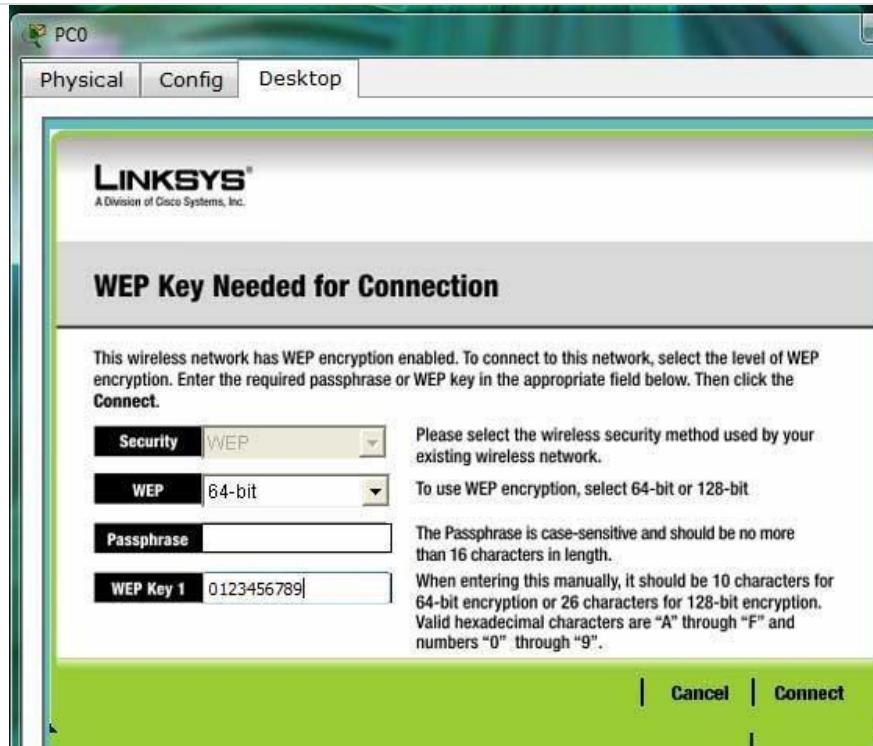


- Click on connect tab and click on Refresh button



As you can see in image that Wireless device is accessing MotherNetwork on CH 6 and signal strength is 100%. In left side you can see that WEP security is configured in network. Click on connect button to connect MotherNetwork

- It will ask for WAP key insert 0123456789 and click connect



It will connect you with wireless router.

As you can see in image below that system is connected. And PCI card is active.



- Repeat same process on PC1 and PC2.

Student observation:

1.What is SSID of a wireless router?

SSID (Service Set Identifier) is the name of a wireless network broadcast by a router or access point.

It helps users identify and connect to the correct Wi-Fi network.

2.What is a security key in wireless router?

A security key (Wi-Fi password) is used to secure the wireless network and prevent unauthorized access.

Common types include WPA2 or WPA3 keys.

3.Configure a simple Wireless LAN in your lab using a real access point and write down the configurations in your notebook.

Connect the access point to the network, log in to its admin page, and set the SSID, security type (WPA2), and password.

Assign IP addresses (e.g., 192.168.1.x) to connected devices; verify connectivity using the ping command.

RESULT:

Thus Configuration of Wireless LAN using CISCO Packet Tracer has been executed successfully