Exp No: 08 [A]

NMAP SCANS

AIM:

To discover live hosts using Nmap scans on the TryHackMe platform. Room link: https://tryhackme.com/room/nmap01.

Introduction

When targeting a network, we need an efficient tool to handle repetitive tasks. The tool we rely on is Nmap. The first question about finding live computers is answered in this room. This room is the first series of four rooms dedicated to Nmap. The 2nd question abt running services is answered in next Nmap rooms.

This room is the first of four in this Nmap series. These 4 rooms are also part of the Network Security module

- Nmap Live Host Discovery
- Nmap Basic Port Scans
- Nmap Advanced Port Scans
- Nmap Post Port Scans

We can introduce 2 scanners, arp-scan & nmap-scan, & explain how they overlap with part of Nmap's Host discovery.

Now, we will use Nmap to discover

Nmap to discover System & Services active

Subnetworks: A network segment is a grp of Computers linked through a shared medium like an ethernet switch / wifi access point.

In IP networks, a Subnetworks, typically consists of one/more network segments connected together & configured to use the same router.

Requests within a Subnet
(4 - computer Subnet)
Send packet

From:
computer 1

TO:
computer 1

packet type:
arp_request

Data:
Computer 6
Send packet

* From Computer 1
* to Computer 1 (to replicate it is broadcast).
* packet type : "ARP Request"
* Data : Computer 6.

How many
Did Compute
Enume
targets
. list
Disco
. AR
. I
. T
. C

How many devices can see the ARP Request? 4

Did Computer6 reply to ARP Request? (Y/N) Y

Sending Packets b/w Subnets

Send Packet

From:
Computer 4

To:
Computer 4

Packet type:
arp_request

Data:
computer 6

Send packet

* From computer 4
* To computer 4.
* Packet type: ARP Request
* Data: computer6.

Enumerating targets

targets can be specified in 3 ways

- list
- Range
- Subnet

Discovering live hosts

TCP/IP layers

- ARP from link layer
- ICMP from Network layer
- TCP from transport layer
- UDP from transport layer

NMAP Host Delivery using ARP

Nmap typically uses a ping scan to find live hosts & then proceeds to scan those live hosts.

TCP ACK Ping

Nmap as a privileged user. If you attempt this as an unprivileged user, Nmap will perform a 3-way handshake by default.

UDP Ping

you can also employ UDP to check if the host is online. Unlike TCP SYN Ping, sending a UDP packet to an open port typically does not elicit a response.

Student observation

1. which TCP ping scan does not require a previleged account?
   TCP SYN ping
2. Which TCP ping scan requires a privileged account?
   TCP ACK ping
3. Which option do you need to add to Nmap to run a TCP SYN ping scan on the telnet port.
   -PS23

4. what is to use hosts -PP
5. what to u hosts -PM

Result

TCP & comple

4. What is the option required to tell Nmap to use ICMP address stamp to discover live hosts
   -PP

5. What is the option required to tell Nmap to use ICMP address Mask to discover live hosts
   -PM

Result:
Thus we have learned how ARP, ICMP, TCP & UDP can detect live hosts by completing this room.

22/x 8/60

Exp No: 8B

Wireless LAN using CISCO packet tracker

AIM: configuration of wireless lan using CISCO packet tracker.

Design a topology with 3 PCs connected from linkeys wireless routers.

Perform following configuration

- Configure static IP on PC wireless Router
- Set SSID to Mother Network
- 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.

Step1: click on wireless Router

- Next click on wireless tab & set default SSID to mother network.
- Now Select wireless Security & change Security mode to WEP.
- Set Key 1 to 0123456789.
- Double click on PC Select Desktop tab click on IP configuration select static IP & set IP as given below:

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.
.then connect
do so cl
Pc wirele
.Click on
.It will as
& click c
wireless
and PC
.Repeat
PC-
PC

Student
1. what
SSID
wirele
&

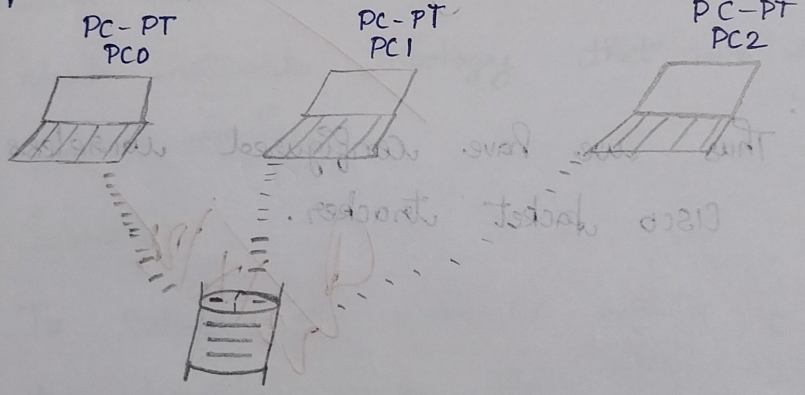
PC2 192.168.0.4 255.255.255.0 192.168.0.1

.then connect PC's from wireless router. TO do so click Pc select Desktop click on Pc wireless.

.click on connect tab & click on refresh button.

.It will ask for WAP key insert 0123456789 & click connect. It will connect you with wireless router. then the system is connected and PC I card is active.

.Repeat same process on PCI & PC2.



linksys - WRT300N
wireless router 0.

Student observation

1. what is SSID of a wireless Router?

SSID [Service set identifier] is the name of a wireless network that helps devices identify & connect to a specific wifi network.

2. What is a security key in wireless router?
A security key is used to protect the wireless network & ensure only authorized users can connect.

3. configuring a simple wireless LAN.
- connect the access point to network & power it ON.
- log in to router's admin page
- Set SSID
- Choose a security mode
- Set a security key.
- Connect devices using SSID & password.

Result:
Thus we have configured wireless LAN using Cisco packet tracker.

12/X/24

EXP NO: 9 Subnetting

AIM:
imple
Packet T
ore could
Subnets ,
a limit
to cre
Creating
Select
Select
blank
add
Subnetti
To
to
addres
route
Config
Right
will
rou
#
#