EXP NO: 08 Nmap using tryhackme platform

DATE: 10.09.2024

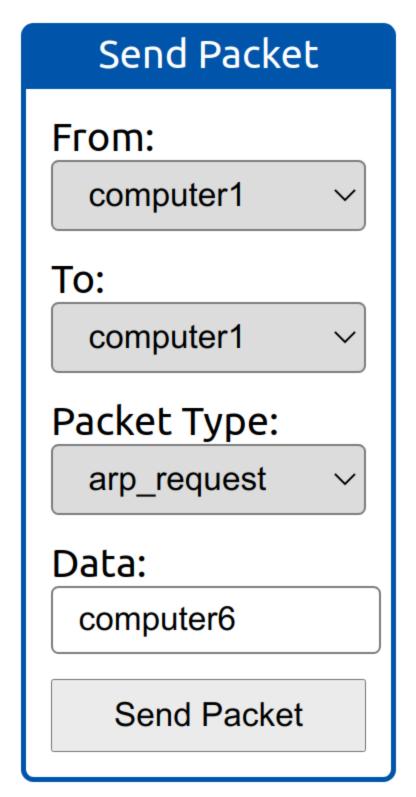
Nmap Live Host Discovery

AIM:

To use Nmap to discovery live hosts using ARP Scan ,ICMP scan , and TCP/UDP Ping Scan in the tryhackme platform.

TASK: 2 - SUBNETWORKS:

Send a packet with following



- 1.From computer1
- 2.To computer1 (to indicate it is broadcast)
- 3.Packet Type: "ARP Request"

4.Data : computer6 (because we are asking for computer6 MAC address using ARP Request)

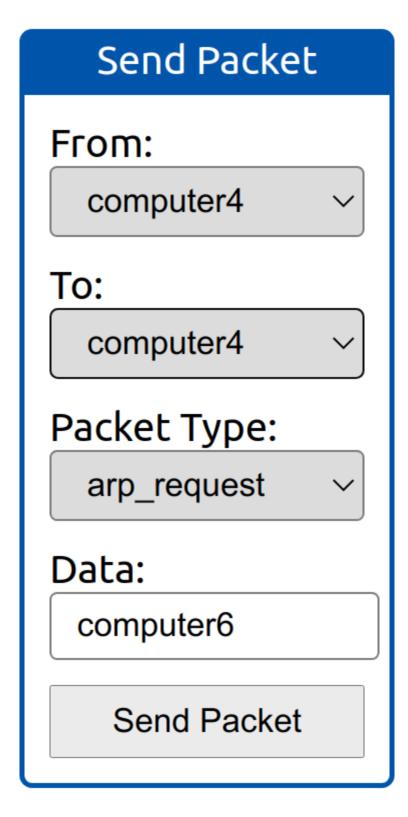
How many devices can see the ARP Request?

Ans:4

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

Ans : N

Send a packet with the following:



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

How many devices can asee the ARP Request?

Ans:4

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

Ans: Y

TASK - 3: Enumerating Targets

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

Ans: 10.10.12.8

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

Ans: 6400

TASK - 4 : Discovering Live Hosts

Send a packet with following:

1.From computer1

2.To computer3

3.Packeet Type: "Ping Request"

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

Ans : ARP Resquest

How many computers responded to the ping request?

Ans: 1

Send a packet with following:

1.From computer2

2.To computer5

3.Packet Type: "Ping Request"

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

Ans : router

What is the name of the first device that responded to the second ARP Request? Computer5

Send another Ping request Did it required new ARP Requests? (Y/N)

Ans: N

TASK - 5: Nmap Host Discovery Using ARP

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?

Ans: 3

TASK - 6: Nmap Host Discovery Using ICMP

Nmap Host Discovery Using ICMP:

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

Ans:-PP

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

Ans:-PM

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

Ans:-PE

TASK - 7: Nmap Host Discovery Using TCP and UDP

Which TCP ping scan does not require a privileged account?

Ans: TCP SYN Ping

Which TCP ping scan requires a privileged account?

Ans: TCP ACK Ping

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

Ans:-PS23

TASK - 8 : Using Reverse - DNS Lookup

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

Ans:-R

RESULT:

Nmap to discover live host usng ARP scan ,ICMP scan and TCP/UDP ping scan in the tryhackme platform.