NAME: UDAYA SANKAR C ROLL NO: 231901058

Ex.no:8

Date:10.9.2024

NMAP TO DISCOVER LIVE HOSTS AIM:

To study Nmap tool using TryHackMe platform.

TASK 1 – INTRODUCTION:



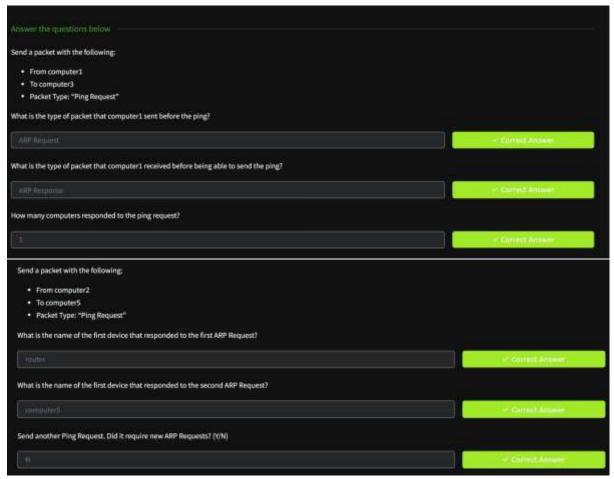
TASK 2 – SUBNETWORKS:

Anywer the questions below	
Send a picket with the hollowing:	
Send Paties	
From	
- Probugnitor	
To: computerY ==	
Packet Type:	
MI, Priced V	
Dota: computerti	
Sant Point	
Francomputed	
To computer((to indicate it is broadcast) Packet Type: 'APP Dequest' To computer(to indicate it is broadcast)	
Cata-computer6 (because we are asking for computer6 MAC address using ARP Request)	
How many devices can see the ASP Request?	
	ESHIONIES E164
Bild computer6 receive the ARP Request? (Y/W)	
u"	
Send a packet with the following:	
Send Packet	
From	
computers	
To:	
Packet Type:	
all_mand	
Dota: conjudeti	
Switt Packet	
9	
Fron computer4	
To computer4 tto indicate it is broadcast! Packet Type "NPP kequest"	
Data: computer6 (because we are asking for computer6 MAC address using ARP Request)	
How many devices can see the ARP Request?	
	A bined Market
Did computer6 reply to the ARP Request? (VIN)	
	V Exhaust shapes (

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 t	argets we want
to scan. Generally speaking, you can provide a list, a range, or a subnet. Examples of target specification are:		
list: MACHINE_IP scanne.nmap.org example.com will scan 3 iP addresses.		
 range: 18.11.12.15-28 will scan 6 IP addresses: 18.11.12.15 , 18.11.12.16 , and 18.11.12.28. 		
submet: MADITAR_17/30 will scan 4 IP addresses.		
You can also provide a file as input for your list of targets, map -it list_of_hosts.tst -		
If you want to check the list of hosts that Nmap will scan, you can use *** -*** TAMOETS . This option will give you a detailed list of	f the hosts that Nmap will scan withou	it scanning them;
however, Nmap will attempt a reverse-DNS resolution on all the targets to obtain their names. Names might reveal various informations are consistent of the start	tion to the pentester. (If you don't wan	t Nmap to the
DNS server, you can add)		
Launch the AttackBox using the Start AttackBox button, open the terminal when the AttackBox is ready, and use Nmap to answer the	e following.	
Answer the questions below		
What is the first IP address Nmap would scan if you provided 30.10.12.13/29 as your target?		
	→, Carried Armover	P HINE
How many IP addresses will Nmap scan if you provide the following range 18.18.8-255.181-125?		
	< Correct Answer.	0-Hint-

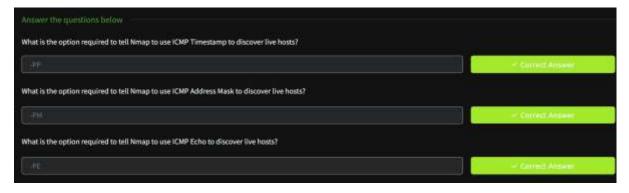
TASK4 - DISCOVERING LIVE HOSTS:



TASK 5 - NMAP HOST DISCOVERY USING ARP:



TASK 6 - NMAP HOST DISCOVERY USING ICMP:



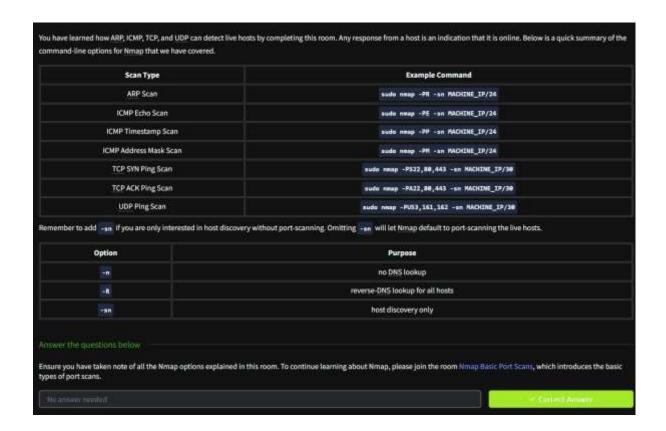
TASK 7 - NMAP HOST DISCOVERY USING TCP AND UDP:



TASK 8 - USING REVERSE-DNS LOOKUP:

e want Nmap to issue a reverse DNS lookup for all the possibles hosts on a subnet, hoping to get some i	nsights from the names. What option should we add?
	50 (
naver the questions below	
des-servers DMS_SERVER option.	
y default, Nmap will look up online hosts; however, you can use the option 🕒 to query the DNS server	even for offline hosts. If you want to use a specific DNS server, you can add the 🥞
se -m to skip this step.	
	s can be a helpful step. However, if you don't want to send such DNS queries, you

TASK 9 – SUMMARY:



RESULT:

Hence, Nmap to discover live hosts is studied.