Ex.no:8

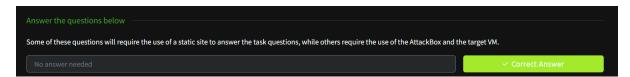
Date:10.9.2024

NMAP TO DISCOVER LIVE HOSTS

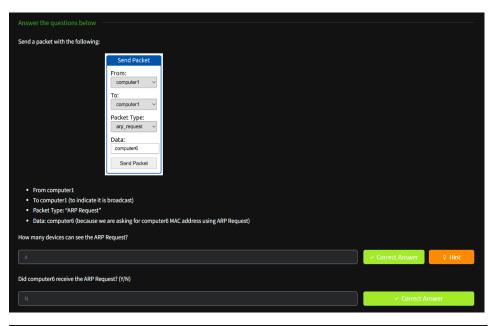
AIM:

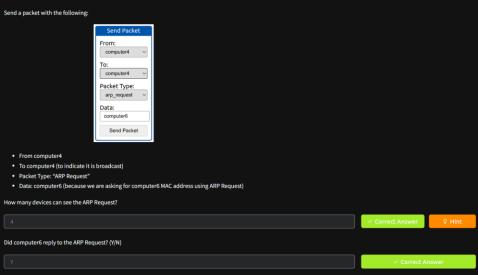
To study Nmap tool using TryHackMe platform.

TASK 1 – INTRODUCTION:



TASK 2 – SUBNETWORKS:





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 targets 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: 10.11.12.15-20 will scan 6 IP addresses: 10.11.12.15, 10.11.12.16, ... and 10.11.12.20.

• subnet: MACHINE_IP/30 will scan 4 IP addresses: 10.11.12.15, 10.11.12.16, ... and 10.11.12.20.

• subnet: MACHINE_IP/30 will scan 4 IP addresses: 10.11.12.15, 10.11.12.16, ... and 10.11.12.20.

If you want to check the list of hosts that Nmap will scan, you can use nmap -sL TARGETS. This option will give you a detailed list of the hosts that Nmap will scan without scanning them; however, Nmap will attempt a reverse-DNS resolution on all the targets to obtain their names. Names might reveal various information to the pentester. (If you don't want Nmap to the DNS server, you can add -n.)

Launch the AttackBox using the Start AttackBox button, open the terminal when the AttackBox is ready, and use Nmap to answer the following.

Answer the questions below

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

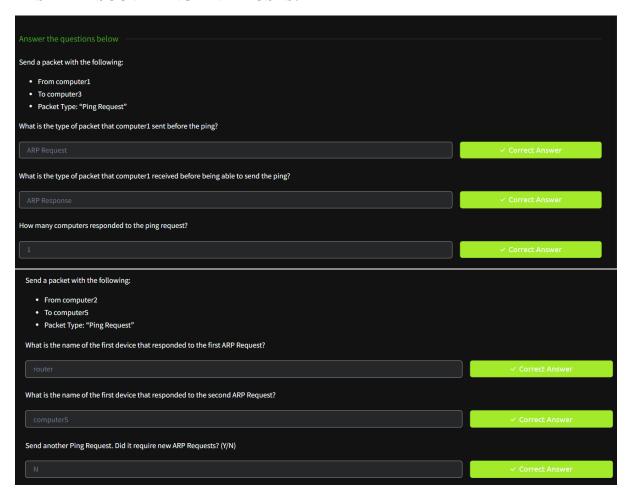
1010.12.8

V Correct Answer

• Hint

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

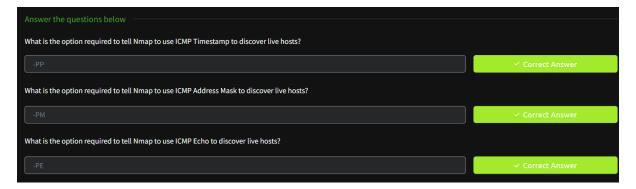
TASK4 - DISCOVERING LIVE HOSTS:



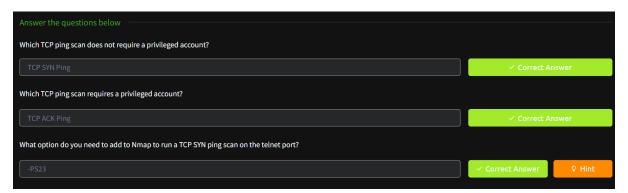
TASK 5 - NMAP HOST DISCOVERY USING ARP:



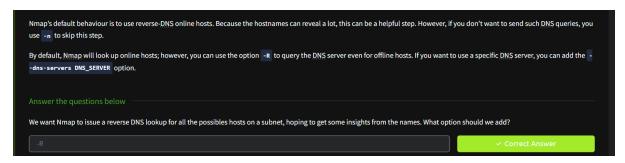
TASK 6 - NMAP HOST DISCOVERY USING ICMP:



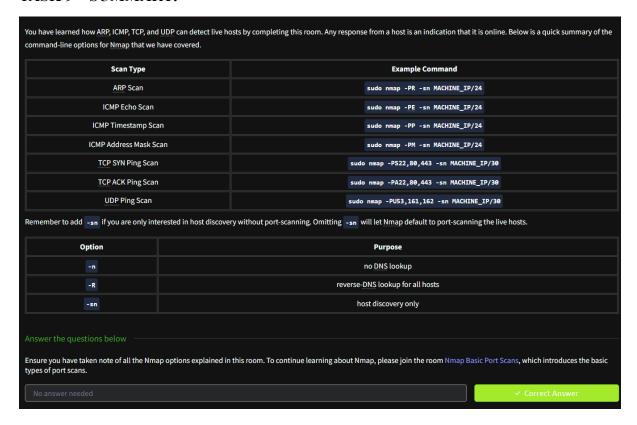
TASK 7 - NMAP HOST DISCOVERY USING TCP AND UDP:



TASK 8 - USING REVERSE-DNS LOOKUP:



TASK 9 – SUMMARY:



RESULT:

Hence, Nmap to discover live hosts is studied.