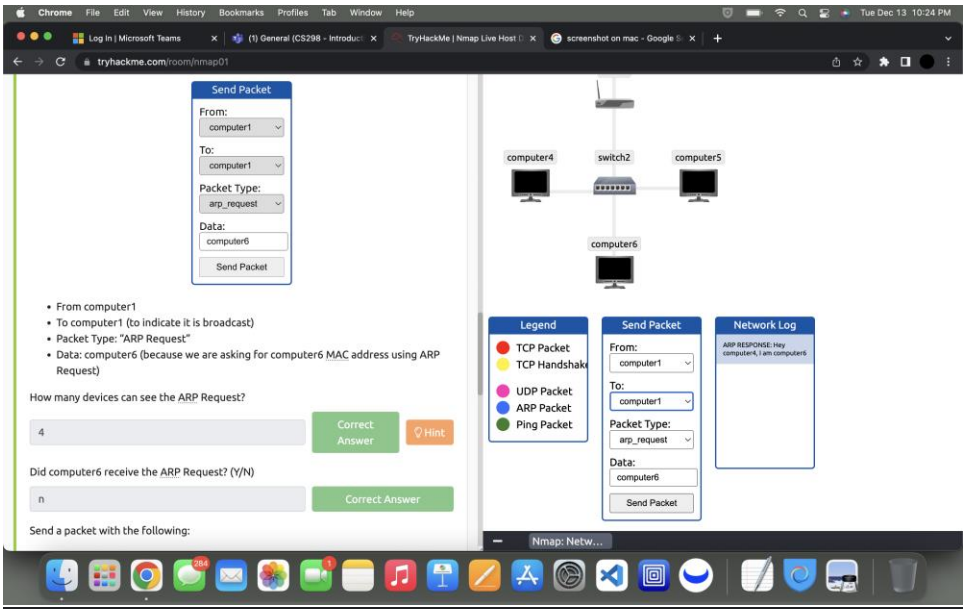
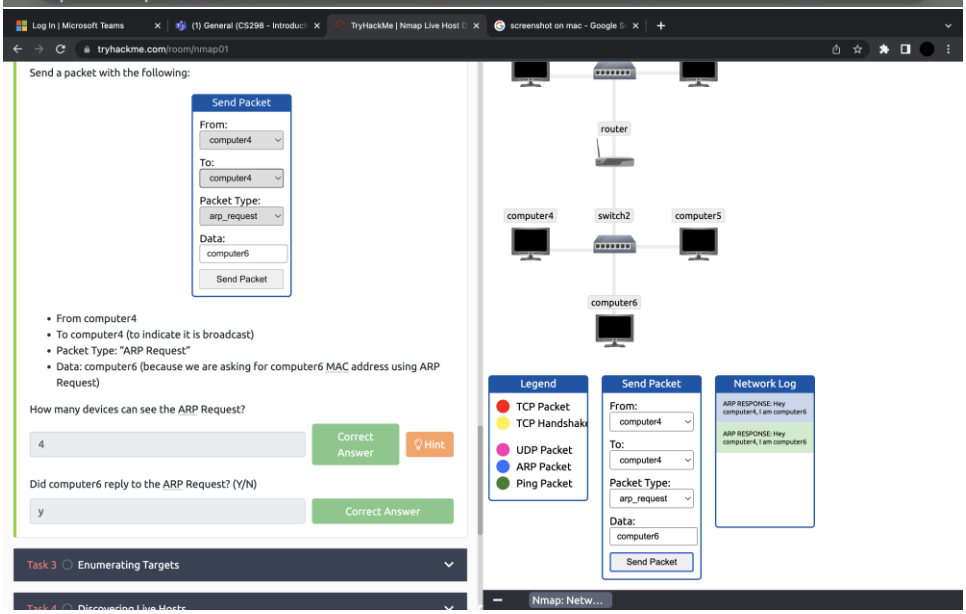
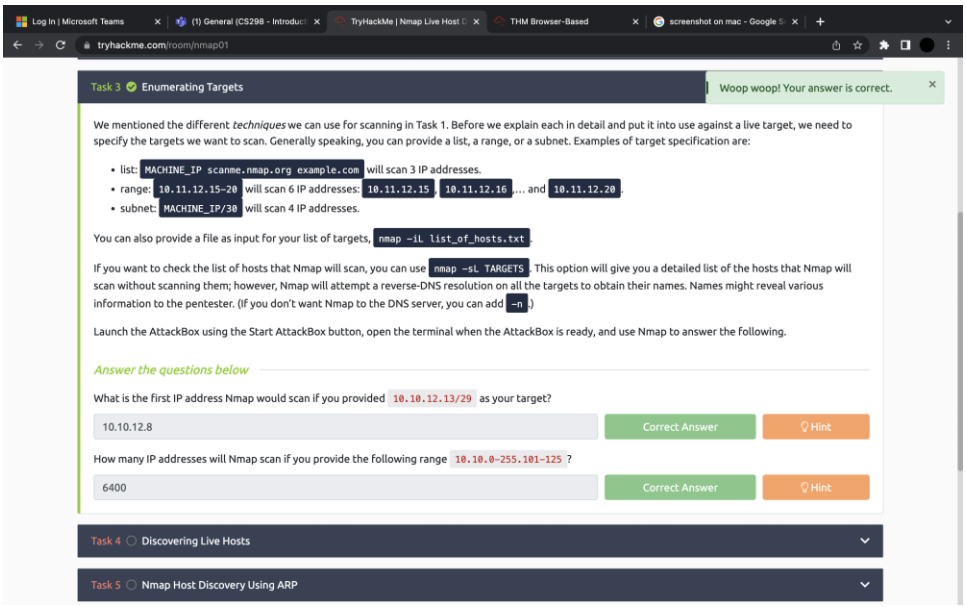
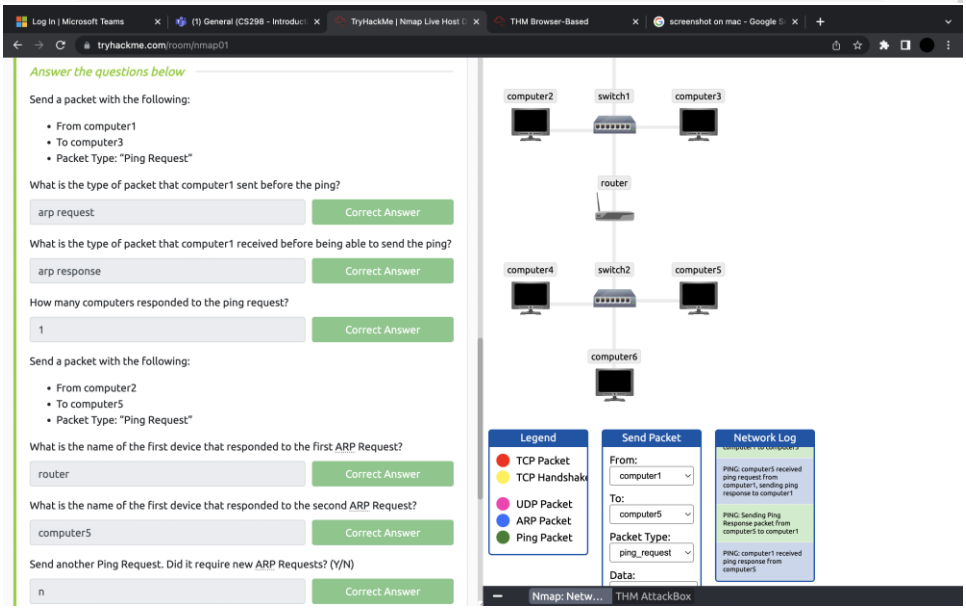
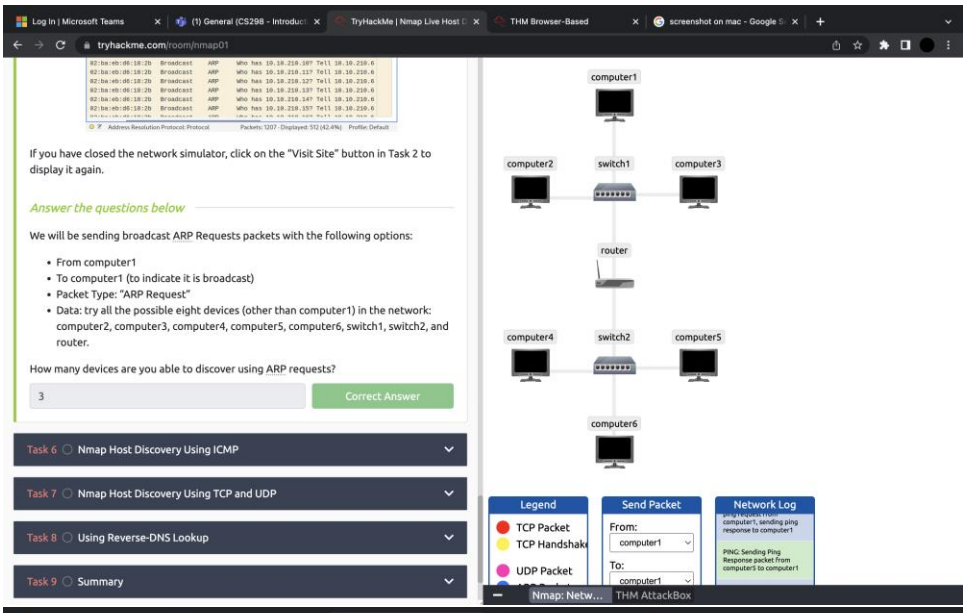
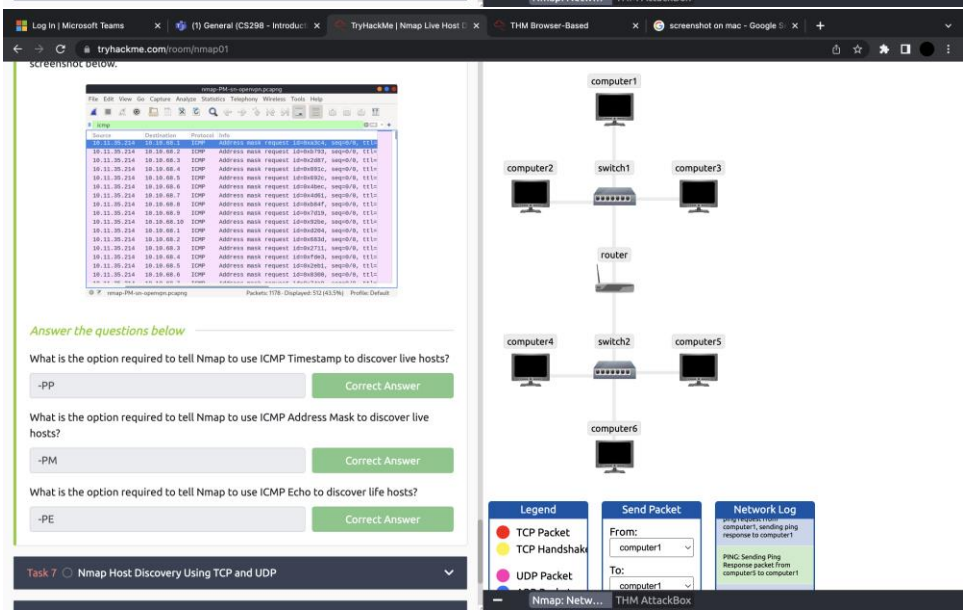

Chrome File Edit View History Bookmarks Profiles Tab Window Help
Tue Dec 13 10:24 PM
Log In | Microsoft Teams
(1) General (CS298 - Introduct
TryHackMe | Nmap Live Host D
screenshot on mac - Google S
tryhackme.com/room/nmap01
Send Packet
From:
computer1
To:
computer1
Packet Type:
arp_request
Data:
computer6
Send Packet
computer4
switch2
computer5
computer6
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:
Legend
TCP Packet
TCP Handshake
UDP Packet
ARP Packet
Ping Packet
Send Packet
From:
computer1
To:
computer1
Packet Type:
arp_request
Data:
computer6
Send Packet
Network Log
ARP RESPONSE: Hey computer4, I am computer6
Nmap: Netw...

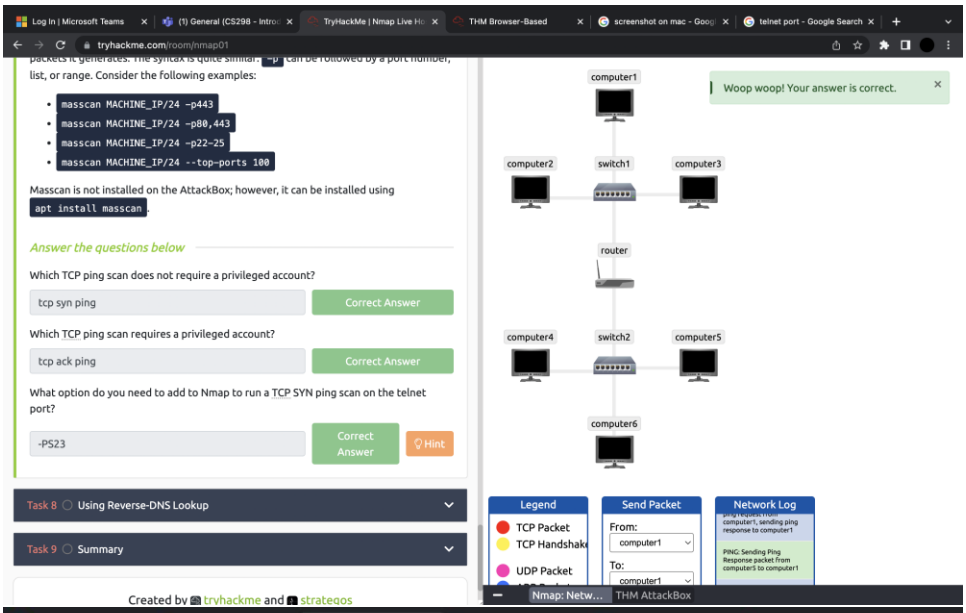

Log In | Microsoft Teams
(1) General (CS298 - Introduct
TryHackMe | Nmap Live Host D
screenshot on mac - Google S
tryhackme.com/room/nmap01
Send a packet with the following:
Send Packet
From:
computer4
To:
computer4
Packet Type:
arp_request
Data:
computer6
Send Packet
router
computer4
switch2
computer5
computer6
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
Legend
TCP Packet
TCP Handshake
UDP Packet
ARP Packet
Ping Packet
Send Packet
From:
computer4
To:
computer4
Packet Type:
arp_request
Data:
computer6
Send Packet
Network Log
ARP RESPONSE: Hey computer4, I am computer6
ARP RESPONSE: Hey computer4, I am computer6
Nmap: Netw...

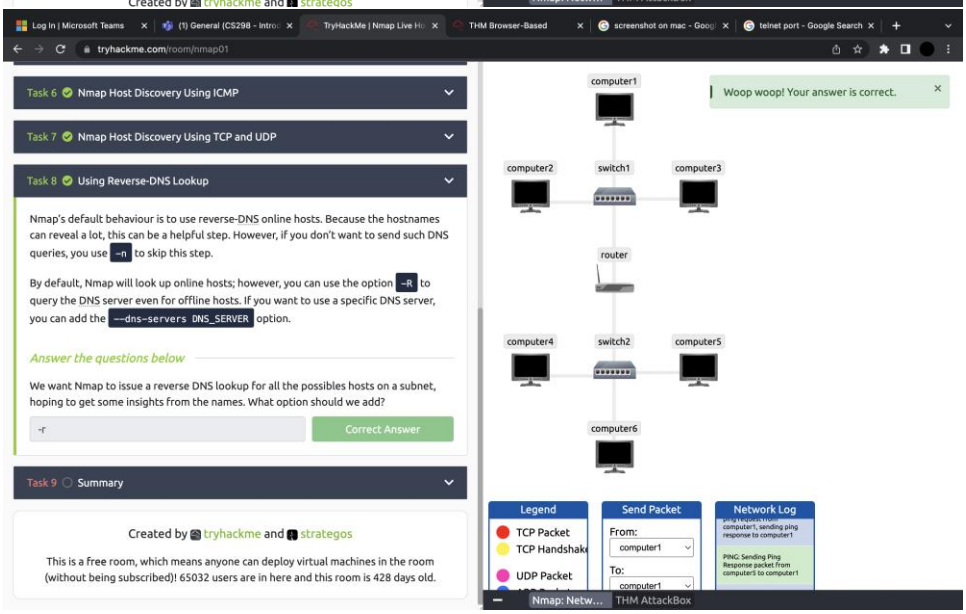

Log In | Microsoft Teams
(1) General (CS298 - Introduct
TryHackMe | Nmap Live Host D
THM Browser-Based
screenshot on mac - Google S
tryhackme.com/room/nmap01
Task 3 Enumerating Targets
Woop woop! Your answer is correct.
We mentioned the different techniques we can use for scanning in Task 1. Before we 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 scanme.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.
You can also provide a file as input for your list of targets, nmap -iL list_of_hosts.txt.
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?
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
Task 5 Nmap Host Discovery Using ARP

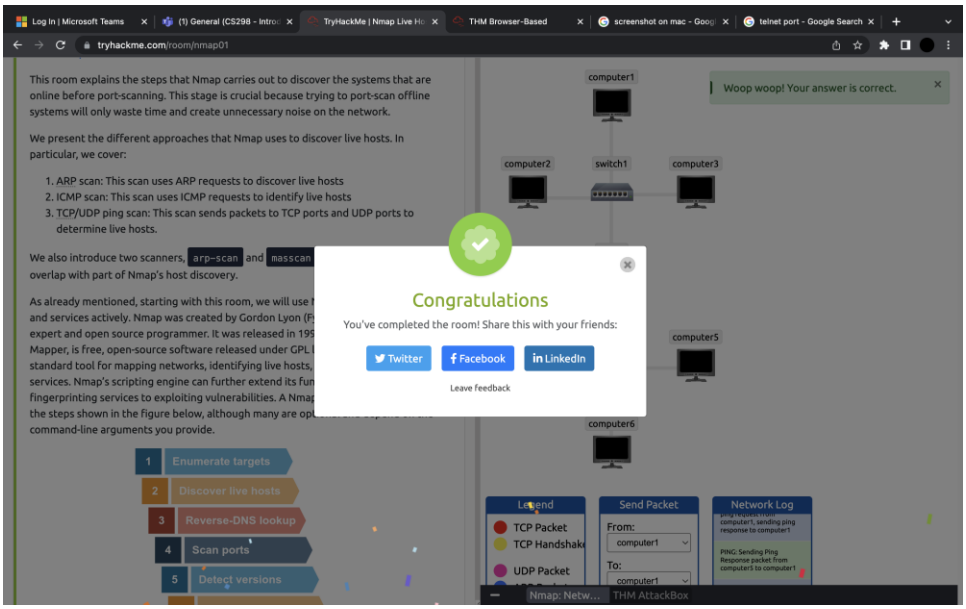

Log In | Microsoft Teams
(1) General (CS298 - Introduct
TryHackMe | Nmap Live Host D
THM Browser-Based
screenshot on mac - Google S
tryhackme.com/room/nmap01
Answer the questions below
Send a packet with the following:
From computer1
To computer3
Packet Type: "Ping Request"
What is the type of packet 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
computer2
switch1
computer3
router
computer4
switch2
computer5
computer6
Legend
TCP Packet
TCP Handshake
UDP Packet
ARP Packet
Ping Packet
Send Packet
From:
computer1
To:
computer5
Packet Type:
ping_request
Data:
Network Log
PING: computer5 received ping request from computer1, sending ping response to computer1
PING: Sending Ping Response packet from computer5 to computer1
PING: computer1 received ping response from computer5
Nmap: Netw...
THM AttackBox


Log In | Microsoft Teams
(1) General (CS298 - Introduct
TryHackMe | Nmap Live Host D
THM Browser-Based
screenshot on mac - Google S
tryhackme.com/room/nmap01
If you have closed the network simulator, click on the "Visit Site" button in Task 2 to display it again.
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
Task 7 Nmap Host Discovery Using TCP and UDP
Task 8 Using Reverse-DNS Lookup
Task 9 Summary
computer1
computer2
switch1
computer3
router
computer4
switch2
computer5
computer6
Legend
TCP Packet
UDP Packet
Send Packet
From:
computer1
To:
computer1
Network Log
PING: Sending Ping Response packet from computer5 to computer1
Nmap: Netw...
THM AttackBox


Log In | Microsoft Teams
(1) General (CS298 - Introduct
TryHackMe | Nmap Live Host D
THM Browser-Based
screenshot on mac - Google S
tryhackme.com/room/nmap01
screenshot below.
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 life hosts?
-PE
Correct Answer
Task 7 Nmap Host Discovery Using TCP and UDP
computer1
computer2
switch1
computer3
router
computer4
switch2
computer5
computer6
Legend
TCP Packet
UDP Packet
Send Packet
From:
computer1
To:
computer1
Network Log
PING: Sending Ping Response packet from computer5 to computer1
Nmap: Netw...
THM AttackBox


Log In | Microsoft Teams
(1) General (CS298 - Intro
TryHackMe | Nmap Live Ho
THM Browser-Based
screenshot on mac - Goog
telnet port - Google Search
tryhackme.com/room/nmap01
list, or range. Consider the following examples:
masscan MACHINE_IP/24 -p443
masscan MACHINE_IP/24 -p80,443
masscan MACHINE_IP/24 -p22-25
masscan MACHINE_IP/24 --top-ports 100
Masscan is not installed on the AttackBox; however, it can be installed using apt install masscan.
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
Task 9 Summary
Created by tryhackme and stratogos
Woop woop! Your answer is correct.
computer1
computer2
switch1
computer3
router
computer4
switch2
computer5
computer6
Legend
TCP Packet
TCP Handshake
UDP Packet
Send Packet
From:
computer1
To:
computer1
Network Log
PING: Sending Ping Response packet from computer5 to computer1
Nmap: Netw...
THM AttackBox


Log In | Microsoft Teams
(1) General (CS298 - Intro
TryHackMe | Nmap Live Ho
THM Browser-Based
screenshot on mac - Goog
telnet port - Google Search
tryhackme.com/room/nmap01
Task 6 Nmap Host Discovery Using ICMP
Task 7 Nmap Host Discovery Using TCP and UDP
Task 8 Using Reverse-DNS Lookup
Nmap's default behaviour is to use reverse-DNS online hosts. Because the hostnames can reveal a lot, this can be a helpful step. However, if you don't want to send such DNS queries, you use -n to skip this step.
By default, Nmap will look up online hosts; however, you can use the option -R to query the DNS server even for offline hosts. If you want to use a specific DNS server, you can add the --dns-servers DNS_SERVER option.
Answer the questions below
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?
-r
Correct Answer
Task 9 Summary
Created by tryhackme and stratogos
This is a free room, which means anyone can deploy virtual machines in the room (without being subscribed)! 65032 users are in here and this room is 428 days old.
Woop woop! Your answer is correct.
computer1
computer2
switch1
computer3
router
computer4
switch2
computer5
computer6
Legend
TCP Packet
TCP Handshake
UDP Packet
Send Packet
From:
computer1
To:
computer1
Network Log
PING: Sending Ping Response packet from computer5 to computer1
Nmap: Netw...
THM AttackBox


Log In | Microsoft Teams
(1) General (CS298 - Intro
TryHackMe | Nmap Live Ho
THM Browser-Based
screenshot on mac - Goog
telnet port - Google Search
tryhackme.com/room/nmap01
This room explains the steps that Nmap carries out to discover the systems that are online before port-scanning. This stage is crucial because trying to port-scan offline systems will only waste time and create unnecessary noise on the network.
We present the different approaches that Nmap uses to discover live hosts. In particular, we cover:
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.
We also introduce two scanners, arp-scan and masscan
overlap with part of Nmap's host discovery.
As already mentioned, starting with this room, we will use
and services actively. Nmap was created by Gordon Lyon (F
expert and open source programmer. It was released in 199
Mapper, is free, open-source software released under GPL
standard tool for mapping networks, identifying live hosts,
services. Nmap's scripting engine can further extend its fun
fingerprinting services to exploiting vulnerabilities. A Nmap
the steps shown in the figure below, although many are opt
command-line arguments you provide.
1 Enumerate targets
2 Discover live hosts
3 Reverse-DNS lookup
4 Scan ports
5 Detect versions
Congratulations
You've completed the room! Share this with your friends:
Twitter
Facebook
LinkedIn
Leave feedback
Woop woop! Your answer is correct.
computer1
computer2
switch1
computer3
computer5
computer6
Legend
TCP Packet
UDP Packet
Send Packet
From:
computer1
To:
computer1
Network Log
PING: Sending Ping Response packet from computer5 to computer1
Nmap: Netw...
THM AttackBox