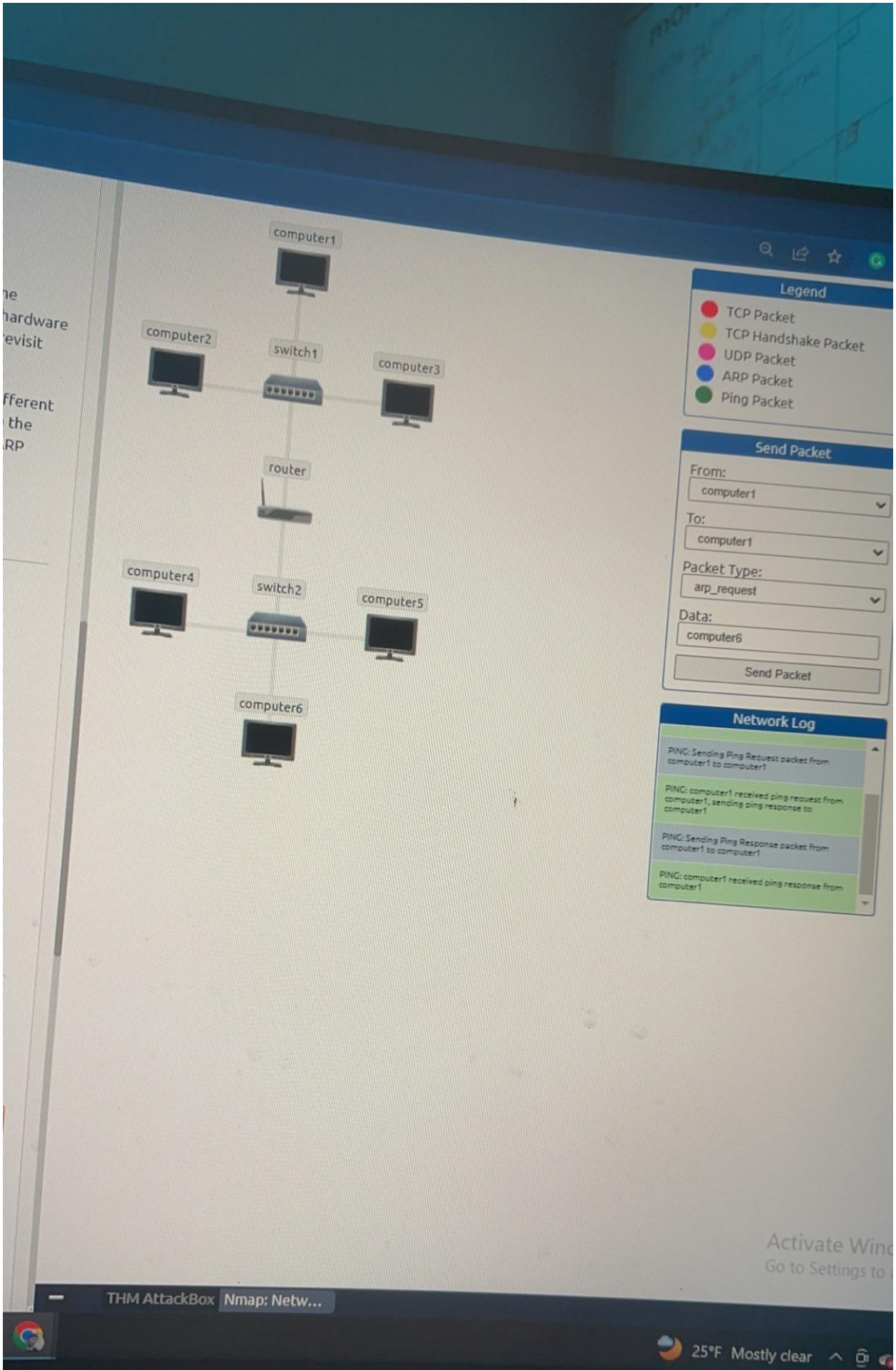
Mike Macancela
Nmap Lab


computer1
computer2
switch1
computer3
router
computer4
switch2
computer5
computer6
Legend
TCP Packet
TCP Handshake Packet
UDP Packet
ARP Packet
Ping Packet
Send Packet
From:
computer1
To:
computer1
Packet Type:
arp_request
Data:
computer6
Send Packet
Network Log
PING: Sending Ping Request packet from computer1 to computer1
PING: computer1 received ping request from computer1, sending ping response to computer1
PING: Sending Ping Response packet from computer1 to computer1
PING: computer1 received ping response from computer1
THM AttackBox
Nmap: Netw...
25°F Mostly clear

ackMe | Introduction to SIEM × TryHackMe | Nmap Live Host Dis × +

tryhackme.com/room/nmap01

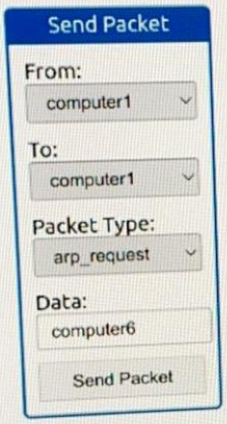
rt of active reconnaissance, we want to discover more information about a group of hosts or about a subnet. If you are connected to
et, you would expect your scanner to rely on ARP (Address Resolution Protocol) queries to discover live hosts. An ARP query aims to
ess (MAC address) so that communication over the link-layer becomes possible; however, we can use this to infer that the host is onli
ayer in Task 4.)

u are in Network A, you can use ARP only to discover the devices within that subnet (10.1.100.0/24). Suppose you are connected to a s
the subnet of the target system(s). In that case, all packets generated by your scanner will be routed via the default gateway (router)
ems on another subnet; however, the ARP queries won't be routed and hence cannot cross the subnet router. ARP is a link-layer proto
kets are bound to their subnet.

k on the "View Site" button to start the network simulator. We will use this simulator to answer the questions in tasks 2, 4, and 5.

swer the questions below

nd a packet with the following:



- 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)

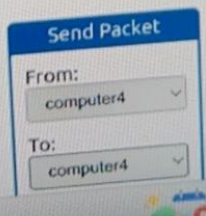
How many devices can see the ARP Request? Correct Answer

4

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

n

Send a packet with the following:



TryHackMe | Introduction to SIE

TryHackMe | Nmap Live Host Dis

tryhackme.com/room/nmap01

computer6

Send Packet

- 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

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

n

Correct

Send a packet with the following:

Send Packet

From:

computer4

To:

computer4

Packet Type:

arp_request

Data:

computer6

Send Packet

- 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

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

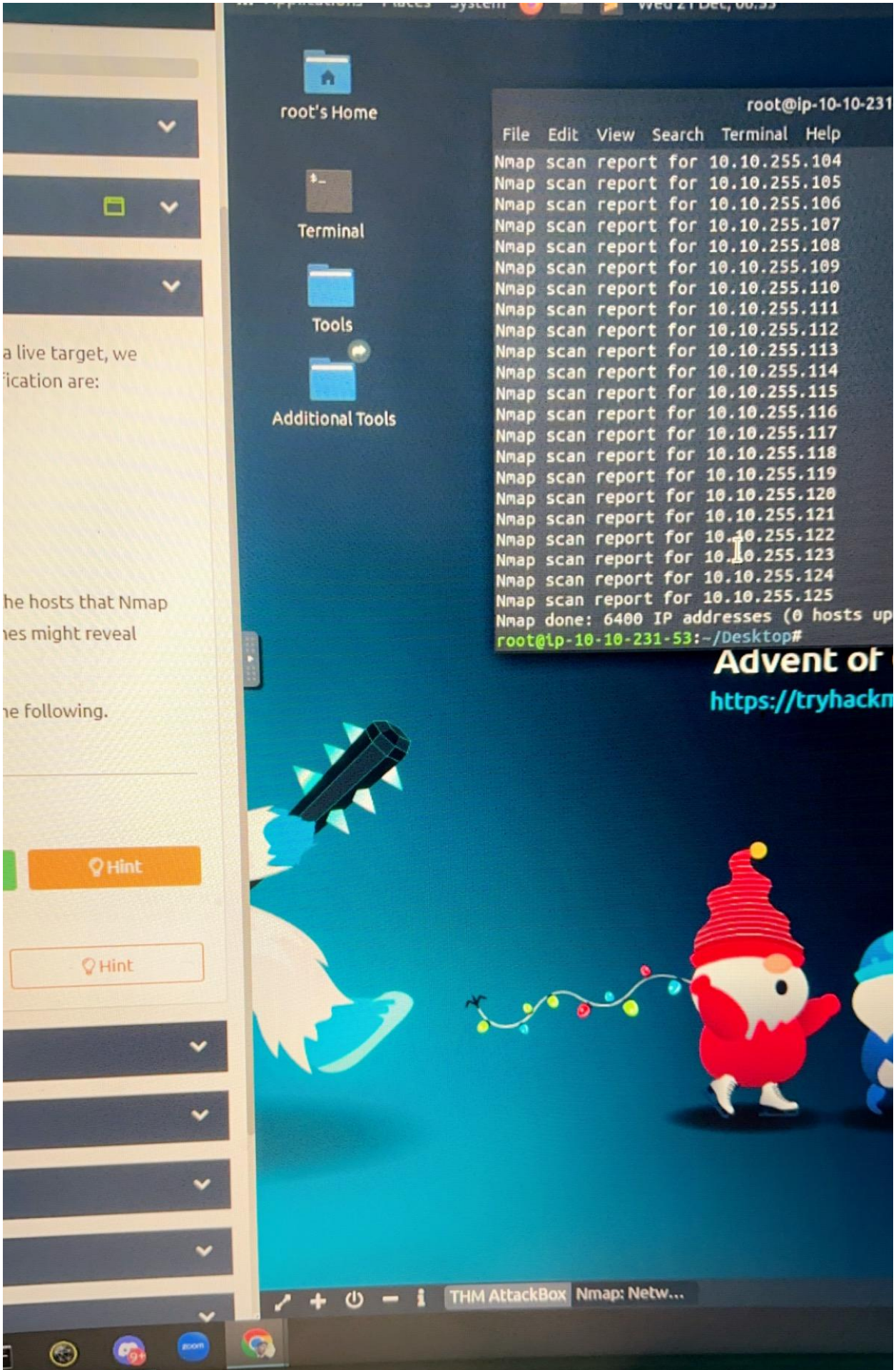
y

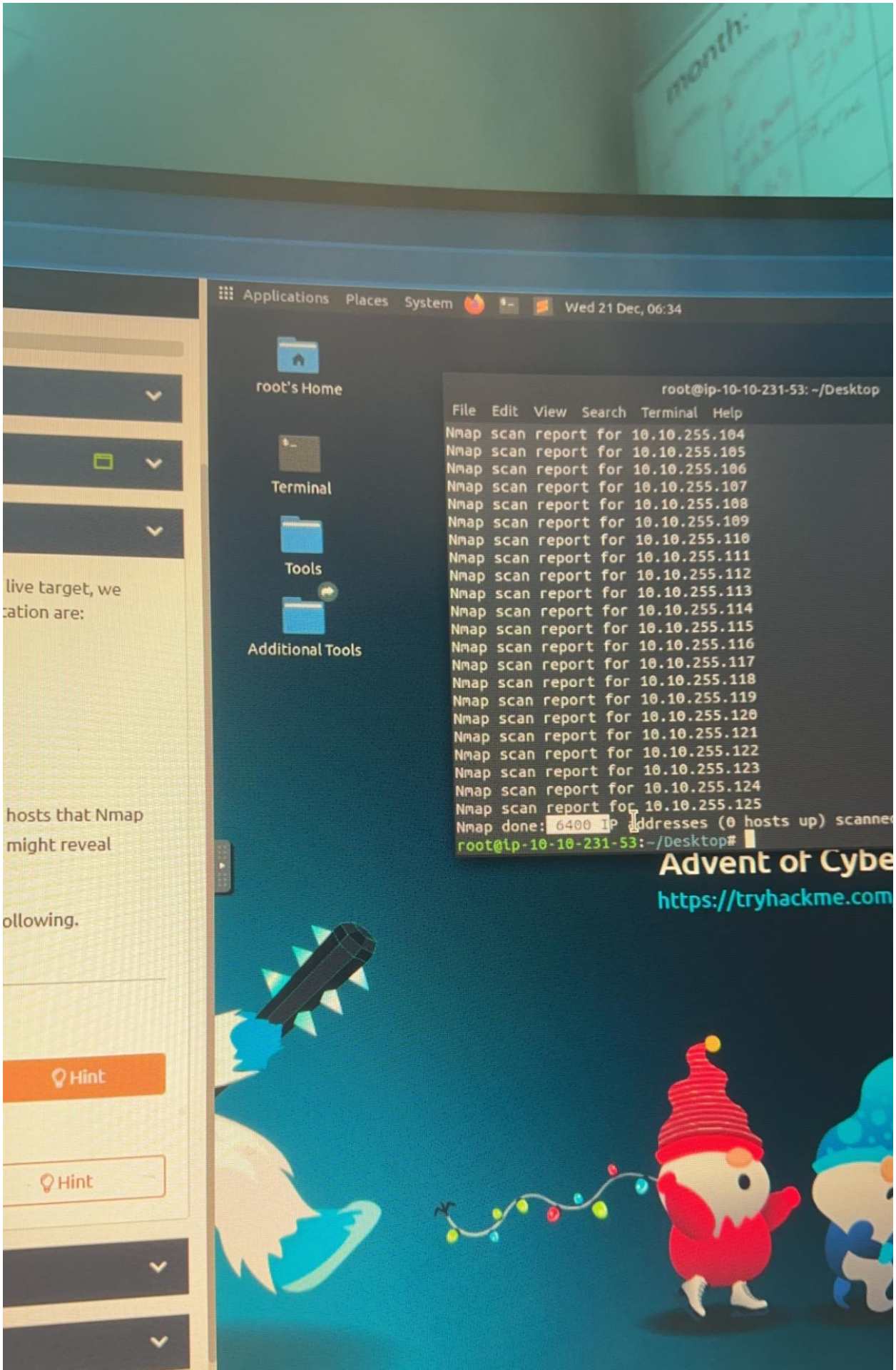
Correct An

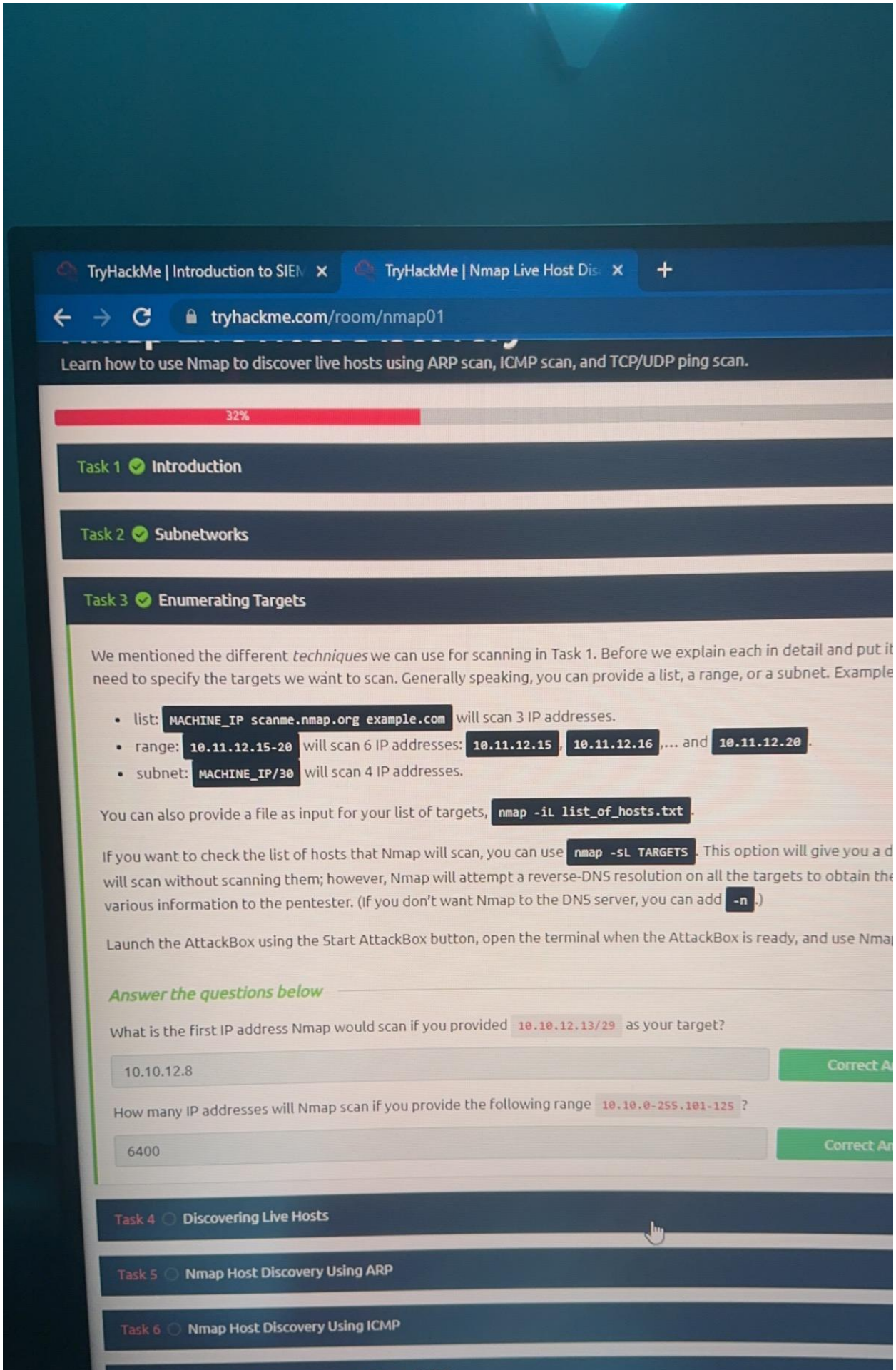
Task 3 Enumerating Targets

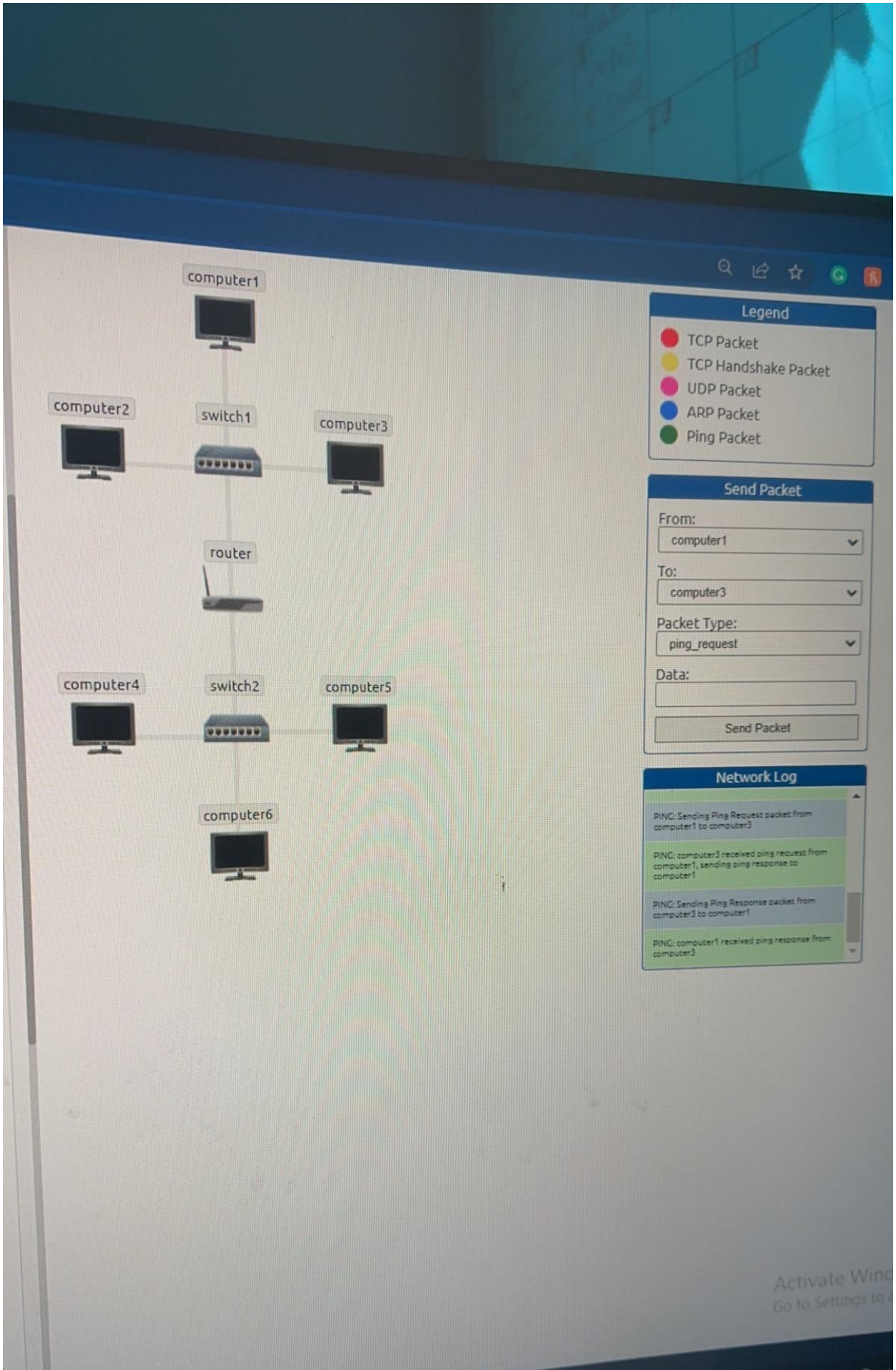
Task 4 Discovering Live Hosts

Type here to search


root's Home
Terminal
Tools
Additional Tools
root@ip-10-10-231
File Edit View Search Terminal Help
Nmap scan report for 10.10.255.104
Nmap scan report for 10.10.255.105
Nmap scan report for 10.10.255.106
Nmap scan report for 10.10.255.107
Nmap scan report for 10.10.255.108
Nmap scan report for 10.10.255.109
Nmap scan report for 10.10.255.110
Nmap scan report for 10.10.255.111
Nmap scan report for 10.10.255.112
Nmap scan report for 10.10.255.113
Nmap scan report for 10.10.255.114
Nmap scan report for 10.10.255.115
Nmap scan report for 10.10.255.116
Nmap scan report for 10.10.255.117
Nmap scan report for 10.10.255.118
Nmap scan report for 10.10.255.119
Nmap scan report for 10.10.255.120
Nmap scan report for 10.10.255.121
Nmap scan report for 10.10.255.122
Nmap scan report for 10.10.255.123
Nmap scan report for 10.10.255.124
Nmap scan report for 10.10.255.125
Nmap done: 6400 IP addresses (0 hosts up
root@ip-10-10-231-53:~/Desktop#
Advent of
https://tryhackm
a live target, we
fication are:
he hosts that Nmap
nes might reveal
ne following.
Hint
Hint
THM AttackBox
Nmap: Netw...


Applications Places System Wed 21 Dec, 06:34
root's Home
Terminal
Tools
Additional Tools
root@ip-10-10-231-53: ~/Desktop
File Edit View Search Terminal Help
Nmap scan report for 10.10.255.104
Nmap scan report for 10.10.255.105
Nmap scan report for 10.10.255.106
Nmap scan report for 10.10.255.107
Nmap scan report for 10.10.255.108
Nmap scan report for 10.10.255.109
Nmap scan report for 10.10.255.110
Nmap scan report for 10.10.255.111
Nmap scan report for 10.10.255.112
Nmap scan report for 10.10.255.113
Nmap scan report for 10.10.255.114
Nmap scan report for 10.10.255.115
Nmap scan report for 10.10.255.116
Nmap scan report for 10.10.255.117
Nmap scan report for 10.10.255.118
Nmap scan report for 10.10.255.119
Nmap scan report for 10.10.255.120
Nmap scan report for 10.10.255.121
Nmap scan report for 10.10.255.122
Nmap scan report for 10.10.255.123
Nmap scan report for 10.10.255.124
Nmap scan report for 10.10.255.125
Nmap done: 6400 IP addresses (0 hosts up) scanned
root@ip-10-10-231-53:~/Desktop#
Advent of Cybe
https://tryhackme.com
live target, we
cation are:
hosts that Nmap
might reveal
ollowing.
Hint
Hint


TryHackMe | Introduction to SIE
TryHackMe | Nmap Live Host Dis
tryhackme.com/room/nmap01
Learn how to use Nmap to discover live hosts using ARP scan, ICMP scan, and TCP/UDP ping scan.
32%
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
need to specify the targets we want to scan. Generally speaking, you can provide a list, a range, or a subnet. Example
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 d
will scan without scanning them; however, Nmap will attempt a reverse-DNS resolution on all the targets to obtain the
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
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 A
How many IP addresses will Nmap scan if you provide the following range 10.10.0-255.101-125 ?
6400
Correct An
Task 4 Discovering Live Hosts
Task 5 Nmap Host Discovery Using ARP
Task 6 Nmap Host Discovery Using ICMP


computer1
computer2
switch1
computer3
router
computer4
switch2
computer5
computer6
Legend
TCP Packet
TCP Handshake Packet
UDP Packet
ARP Packet
Ping Packet
Send Packet
From:
computer1
To:
computer3
Packet Type:
ping_request
Data:
Send Packet
Network Log
PING: Sending Ping Request packet from computer1 to computer3
PING: computer3 received ping request from computer1, sending ping response to computer1
PING: Sending Ping Response packet from computer3 to computer1
PING: computer1 received ping response from computer3

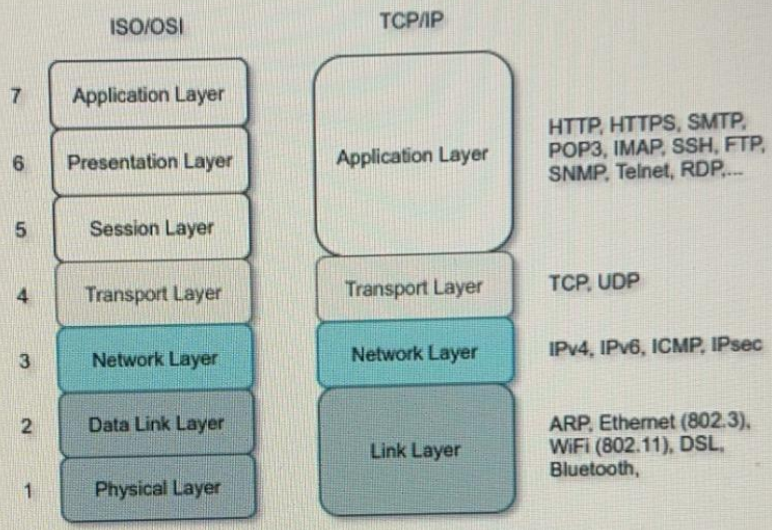
TryHackMe | Introduction to SIEM × TryHackMe | Nmap Live Host Dis × +

tryhackme.com/room/nmap01

k 4 Discovering Live Hosts

t's revisit the TCP/IP layers shown in the figure next. We will leverage the protocols to discover the live hosts. Startin

- ARP from Link Layer
- ICMP from Network Layer
- TCP from Transport Layer
- UDP from Transport Layer



Before we discuss how scanners can use each in detail, we will briefly review these four protocols. ARP has one purpos address on the network segment and asking the computer with a specific IP address to respond by providing its MAC (

ICMP has many types. ICMP ping uses Type 8 (Echo) and Type 0 (Echo Reply).

If you want to ping a system on the same subnet, an ARP query should precede the ICMP Echo.

Although TCP and UDP are transport layers, for network scanning purposes, a scanner can send a specially-crafted pack check whether the target will respond. This method is efficient, especially when ICMP Echo is blocked.

If you have closed the network simulator, click on the "View Site" button in Task 2 to display it again.

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?

TryHackMe | Introduction to SIE

TryHackMe | Nmap Live Host Dis

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 — Corre

What is the type of packet that computer1 received before being able to send the ping?

arp response — Correc

How many computers responded to the ping request?

1 — Correct

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 A

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

computer 5 — Correct A

Send another Ping Request. Did it require new ARP Requests? (Y/N)

n — Correct An

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

Type here to search

TryHackMe | Introduction to SIEM | TryHackMe | Nmap Live Host Dis

tryhackme.com/room/nmap01

02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.2? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.3? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.4? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.5? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	ARP Announcement for 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.7? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.8? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.9? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.10? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.11? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.12? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.13? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.14? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.15? Tell 10.10.210.6

Address Resolution Protocol: Protocol Packets: 1207 · Displayed: 512 (42.4%) Profile: Defaul

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 switch2, and router.

How many devices are you able to discover using ARP requests?

3

Correct Ans

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

Created by tryhackme and strategos

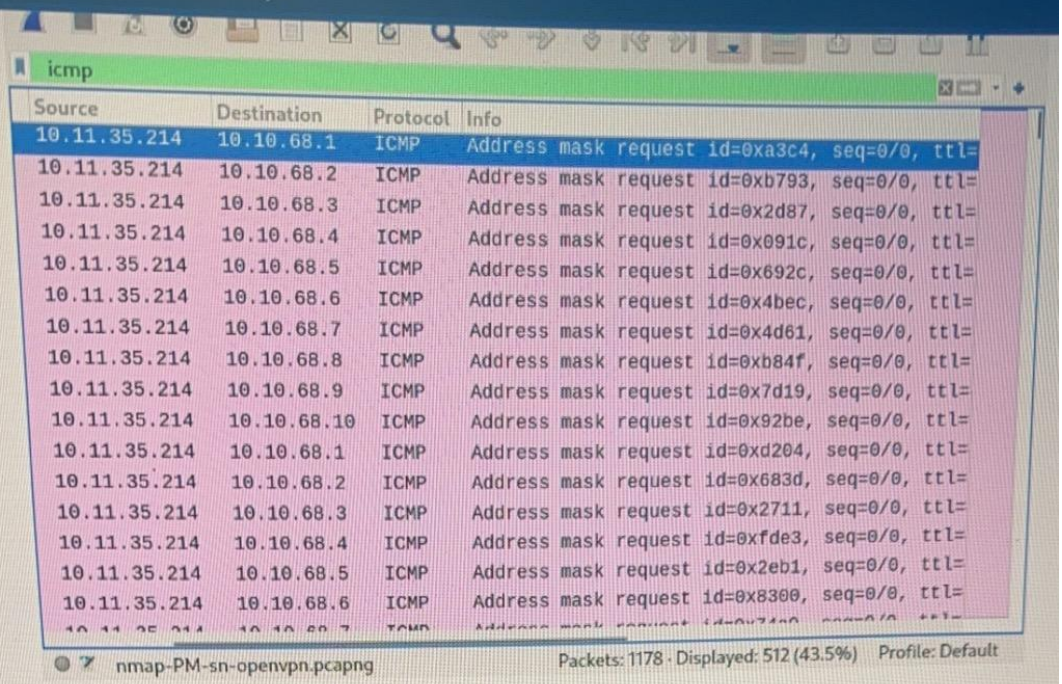
This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 66105 users are in here a days old.

Type here to search

TryHackMe | Introduction to SIE

TryHackMe | Nmap Live Host Dis

tryhackme.com/room/nmap01



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

Task 8 Using Reverse-DNS Lookup

Task 9 Summary

Created by tryhackme and strategos

This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 66105 users are in here and this r
days old.

Type here to search

TryHackMe | Introduction to SIEM | TryHackMe | Nmap Live Host Dis

tryhackme.com/room/nmap01

10.11.35.214	10.10.68.7	UDP	57190 → 40125 Len=40
10.11.35.214	10.10.68.8	UDP	57190 → 40125 Len=40
10.11.35.214	10.10.68.9	UDP	57190 → 40125 Len=40
10.11.35.214	10.10.68.10	UDP	57190 → 40125 Len=40
10.11.35.214	10.10.68.1	UDP	57192 → 40125 Len=40
10.11.35.214	10.10.68.2	UDP	57192 → 40125 Len=40
10.11.35.214	10.10.68.3	UDP	57192 → 40125 Len=40
10.11.35.214	10.10.68.4	UDP	57192 → 40125 Len=40
10.11.35.214	10.10.68.5	UDP	57192 → 40125 Len=40
10.11.35.214	10.10.68.6	UDP	57192 → 40125 Len=40

nmap-PU-sn-openvpn.pcapng Packets: 1118 · Displayed: 602 (53.8%) Profile: Default

Masscan

On a side note, Masscan uses a similar approach to discover the available systems. However, to finish its network scan quickly, Masscan is q
with the rate of packets it generates. The syntax is quite similar: `-p` can be followed by a port number, list, or range. Consider the followir

- `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?

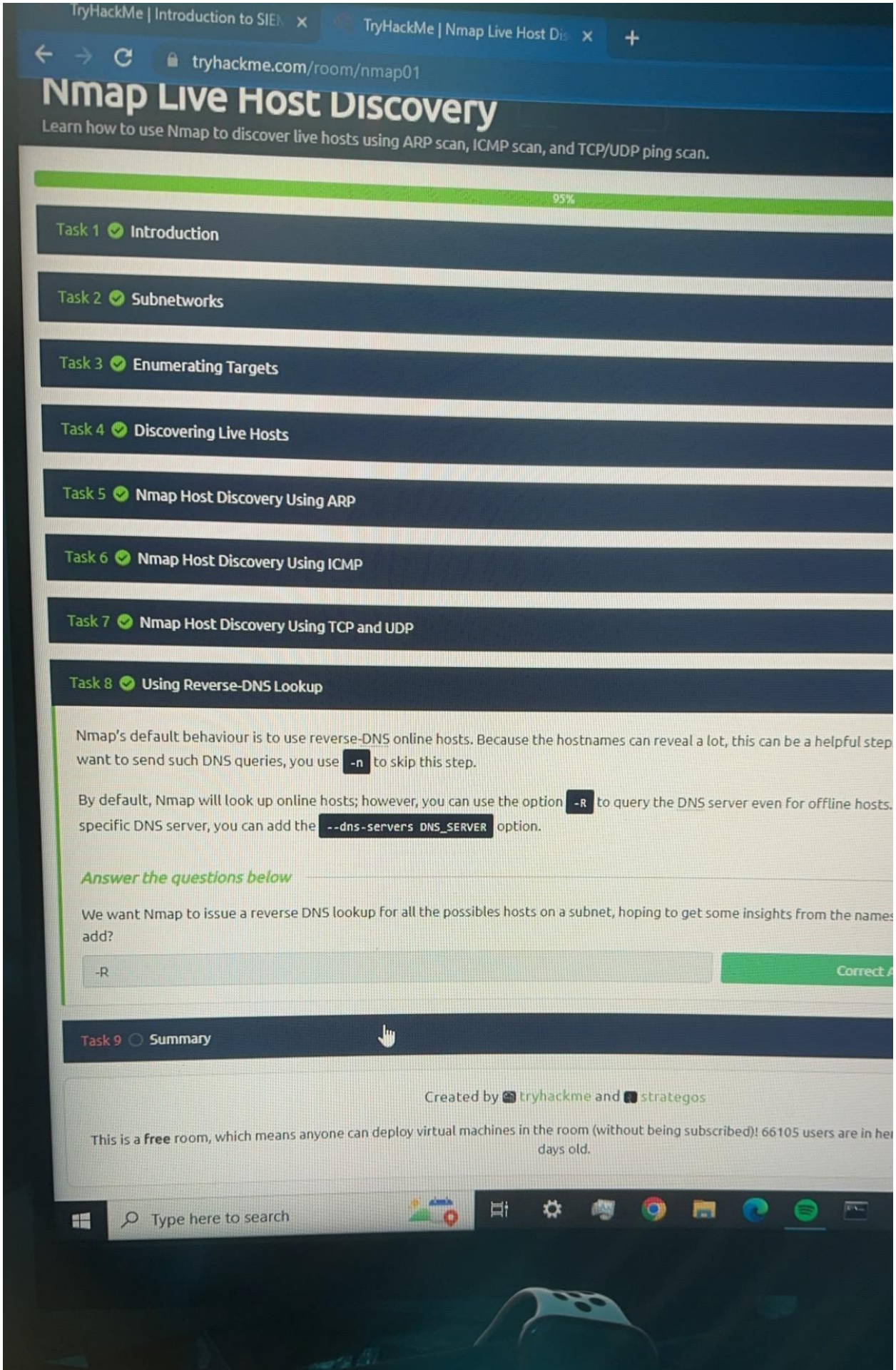
-PS23 — Correct Answer

Task 8 Using Reverse-DNS Lookup

Task 9 Summary

Created by tryhackme and strategos

This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 66105 users are in here and this
days old.


TryHackMe | Introduction to SIE
TryHackMe | Nmap Live Host Dis
tryhackme.com/room/nmap01
Nmap Live Host Discovery
Learn how to use Nmap to discover live hosts using ARP scan, ICMP scan, and TCP/UDP ping scan.
95%
Task 1 Introduction
Task 2 Subnetworks
Task 3 Enumerating Targets
Task 4 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
Nmap's default behaviour is to use reverse-DNS online hosts. Because the hostnames can reveal a lot, this can be a helpful step
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.
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
add?
-R
Correct A
Task 9 Summary
Created by tryhackme and stratego
This is a free room, which means anyone can deploy virtual machines in the room (without being subscribed)! 66105 users are in he
days old.
Type here to search

tryhackme.com/room/nmap01

Nmap Live Host Discovery

Learn how to use Nmap to discover live hosts using ARP scan, ICMP scan, and TCP/UDP ping scan.

100%

- Task 1 Introduction
- Task 2 Subnetworks
- Task 3 Enumerating Targets
- Task 4 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

Created by tryhackme and strategos

This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 66105 days old.

Type here to search