

# Active reconnaissance

## Introduction :

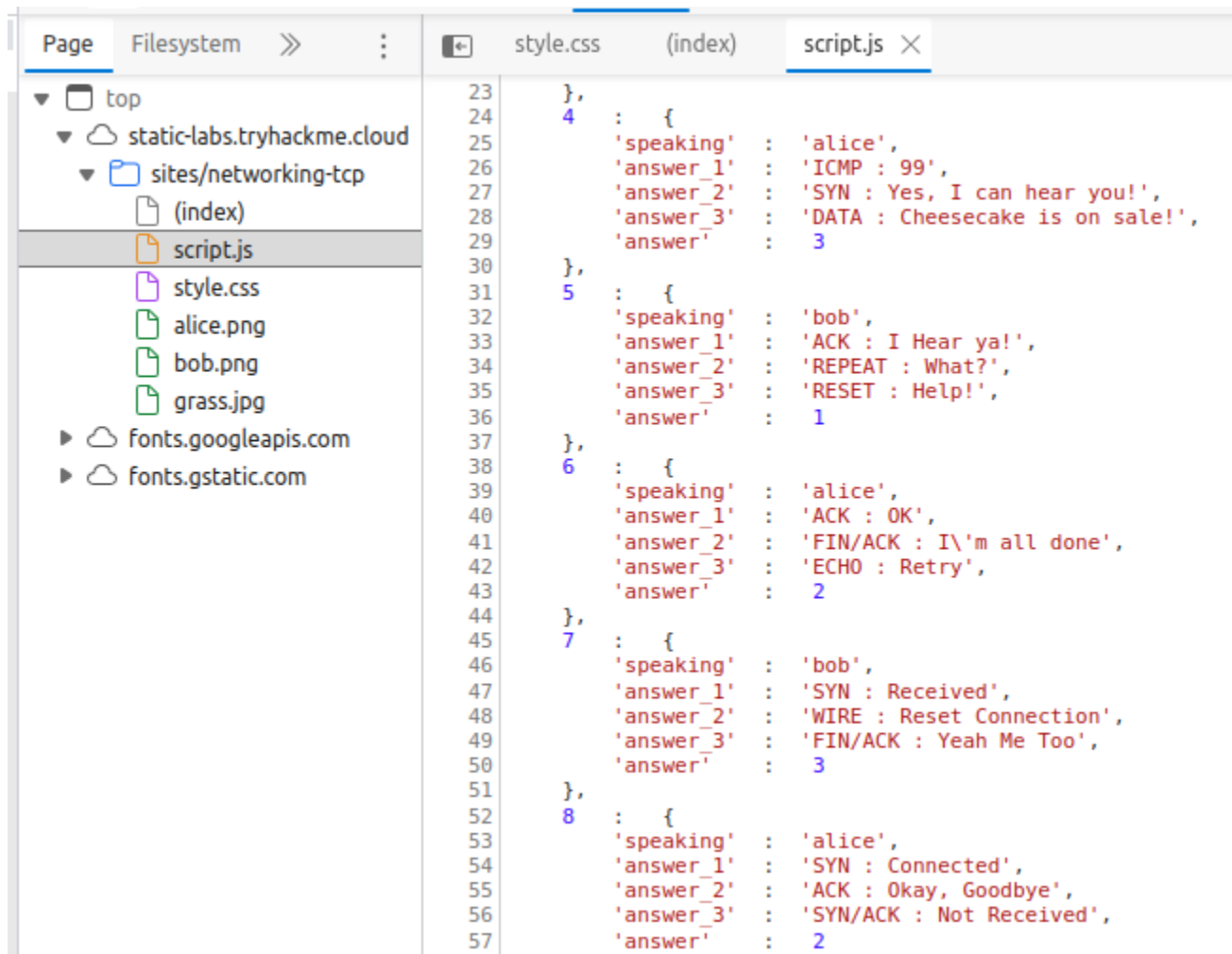
Active reconnaissance is a technique used in ethical hacking and cybersecurity to gather information about a target system or network by actively engaging with it. This means that the attacker sends packets or probes to the target system, which can elicit a response that can be used to gather information .

## ( The second part )Web Browse

Browse to the following website and ensure that you have opened your Developer Tools on AttackBox Firefox, or the browser on your computer. Using the Developer Tools, figure out the total number of questions.

- When you entered the page, you interacted with the questions until the flag appeared
- There were 8 questions

The answer : 8



```
23 },
24 4 : {
25   'speaking' : 'alice',
26   'answer_1' : 'ICMP : 99',
27   'answer_2' : 'SYN : Yes, I can hear you!',
28   'answer_3' : 'DATA : Cheesecake is on sale!',
29   'answer' : 3
30 },
31 5 : {
32   'speaking' : 'bob',
33   'answer_1' : 'ACK : I Hear ya!',
34   'answer_2' : 'REPEAT : What?',
35   'answer_3' : 'RESET : Help!',
36   'answer' : 1
37 },
38 6 : {
39   'speaking' : 'alice',
40   'answer_1' : 'ACK : OK',
41   'answer_2' : 'FIN/ACK : I\'m all done',
42   'answer_3' : 'ECHO : Retry',
43   'answer' : 2
44 },
45 7 : {
46   'speaking' : 'bob',
47   'answer_1' : 'SYN : Received',
48   'answer_2' : 'WIRE : Reset Connection',
49   'answer_3' : 'FIN/ACK : Yeah Me Too',
50   'answer' : 3
51 },
52 8 : {
53   'speaking' : 'alice',
54   'answer_1' : 'SYN : Connected',
55   'answer_2' : 'ACK : Okay, Goodbye',
56   'answer_3' : 'SYN/ACK : Not Received',
57   'answer' : 2
58 }
```

## **(The third part ) Ping**

The ping command sends an Internet Control Message Protocol (ICMP) Echo Request packet to the target host and waits for an ICMP Echo Reply packet. If the target host is reachable, it will send an Echo Reply packet back to the source host. The ping command will then display the round-trip time (RTT) for the echo request and reply packets.

**Which option would you use to set the size of the data carried by the ICMP echo request?**

The answer : -s

**What is the size of the ICMP header in bytes?**

The answer : 8

**Does MS Windows Firewall block ping by default? (Y/N)**

The answer : y

**Deploy the VM for this task and using the AttackBox terminal, issue the command . How many ping replies did you get back?**

ping -c 10 10.10.235.224

The answer : 10

---

## **(Part Four ) Traceroute**

Traceroute is a network diagnostic tool used to trace the path that a packet takes from a source to a destination on an IP network. It does this by sending packets with increasing Time To Live (TTL) values. Each router that the packet passes through decrements the TTL value by one. When the TTL value reaches zero, the router sends an ICMP Time Exceeded message back to the source.

**In Traceroute A, what is the IP address of the last router/hop before reaching tryhackme.com?**

The answer : 172.67.69.208

**In Traceroute B, what is the IP address of the last router/hop before reaching tryhackme.com?**

The answer : 104.26.11.229

**In Traceroute B, how many routers are between the two systems?**

The answer : 26

**Start the attached VM from Task 3 if it is not already started. On the AttackBox, run . Check how many routers/hops are there between the AttackBox and the target VM.traceroute 10.10.235.224**

The answer : NO answer needed

## (Fifth part ) Telnet

Telnet is a network protocol that allows a user to connect to a remote computer and control it as if they were sitting at the keyboard. It is a text-based protocol, so all communication is done in text form

Start the attached VM from Task 3 if it is not already started. On the AttackBox, open the terminal and use the telnet client to connect to the VM on port 80. What is the name of the running server?

The answer : **Apache**

What is the version of the running server (on port 80 of the VM)?

The answer : **2.4.10**

---

## (Part Six) Netcat

**Netcat (often abbreviated to nc)** is a computer networking utility for reading from and writing to network connections using TCP or UDP. It is a versatile tool that can be used for a variety of purposes, including:

Port scanning: Netcat can be used to scan ports on a remote host to see if they are open.

File transfer: Netcat can be used to transfer files between hosts.

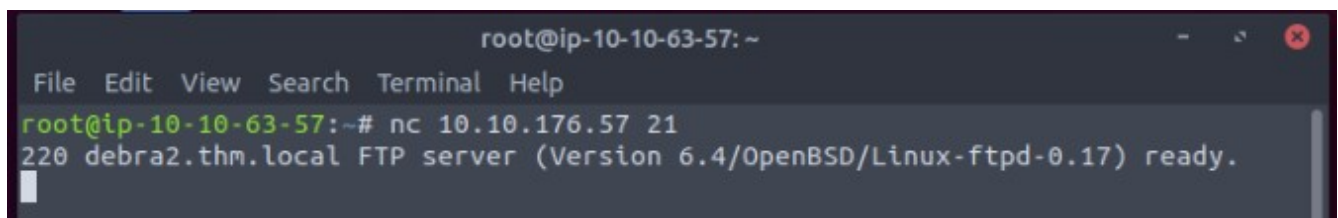
Remote command execution: Netcat can be used to execute commands on a remote host.

Tunneling: Netcat can be used to create a tunnel between two hosts.

Denial-of-service attacks: Netcat can be used to launch denial-of-service attacks.

Start the VM and open the AttackBox. Once the AttackBox loads, use Netcat to connect to the VM port 21. What is the version of the running server?

The answer :**0.17**



```
root@ip-10-10-63-57: ~  
File Edit View Search Terminal Help  
root@ip-10-10-63-57:~# nc 10.10.176.57 21  
220 debra2.thm.local FTP server (Version 6.4/OpenBSD/Linux-ftpd-0.17) ready.  
█
```

## Putting It All Together

In this room, we have covered many various tools. It is easy to put a few of them together via a shell script to build a primitive network and system scanner. You can use to map the path to the target, to check if the target system responds to ICMP Echo, and to check which ports are open and reachable by attempting to connect to them. Available scanners do this at much more advanced and sophisticated levels, as we will see in the next four rooms with . `traceroute ping telnet`

Command	Example
ping	<code>ping -c 10 MACHINE_IP</code> on Linux or macOS
ping	<code>ping -n 10 MACHINE_IP</code> on MS Windows
traceroute	<code>traceroute MACHINE_IP</code> on Linux or macOS
tracert	<code>tracert MACHINE_IP</code> on MS Windows
telnet	<code>telnet MACHINE_IP PORT_NUMBER</code>
netcat as client	<code>nc MACHINE_IP PORT_NUMBER</code>
netcat as server	<code>nc -lvnp PORT_NUMBER</code>



**Well we are done, congratulations**  
**Thank you for reading the report to the end .**

**BY: Abdelwahab Ahmed Shandy**