Active Reconnaissance

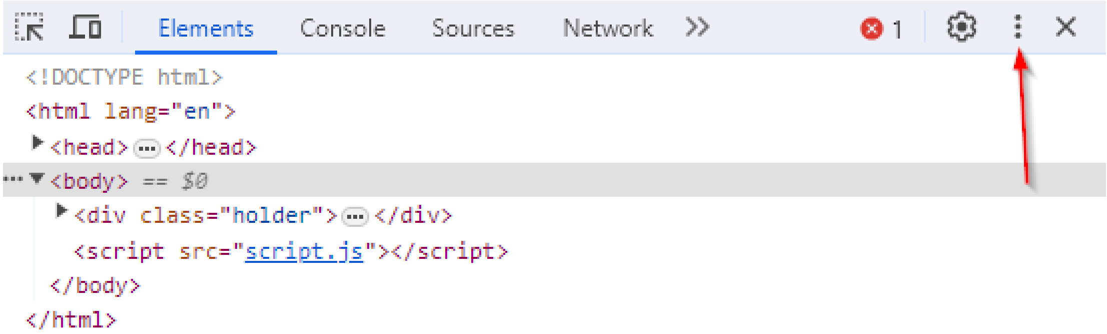
Learn how to use simple tools such as traceroute, ping, telnet, and a web browser to gather information

Task 1: Introduction

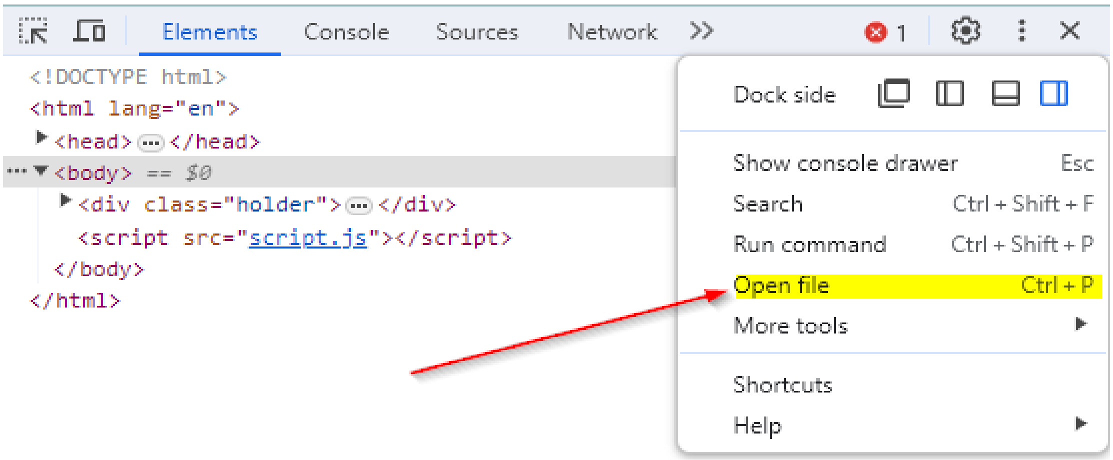
Active reconnaissance involves initiating contact with a target to gather information.

Task 2: Web Browser

- **"Ctrl+Shift+I"** on a PC will open the Developer Tools on a web page
- Click on the link to the website provided
- Open the developer tool using the shortcode above
- Click on the 3 dots and open the file

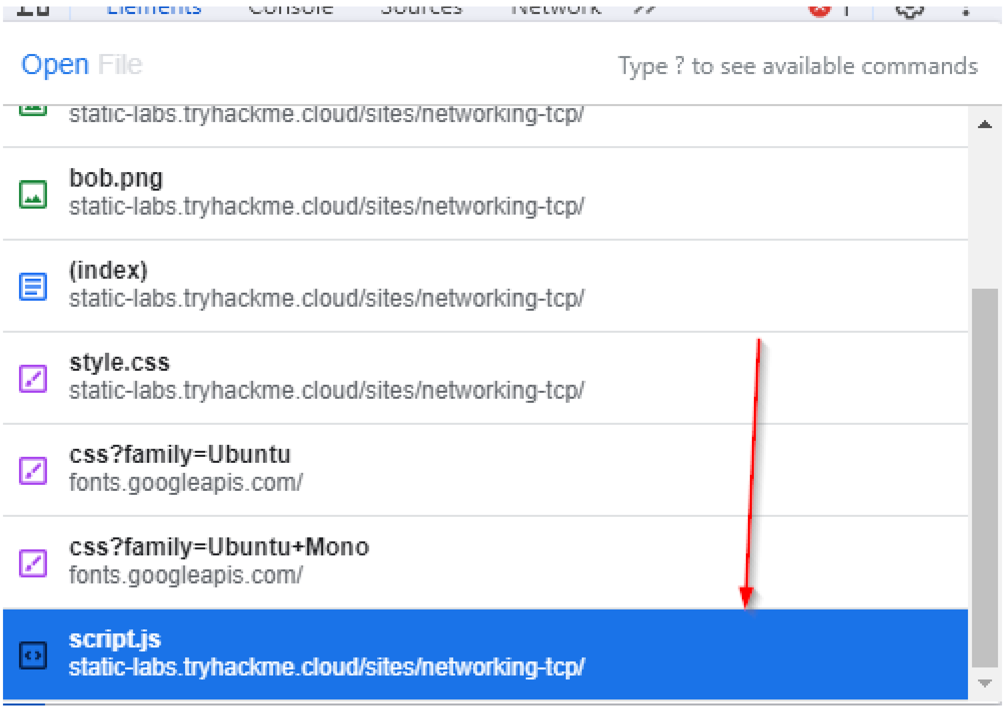


```
<!DOCTYPE html>
<html lang="en">
  <head>…</head>
  <body> == $0
    <div class="holder">…</div>
    <script src="script.js"></script>
  </body>
</html>
```



```
<!DOCTYPE html>
<html lang="en">
  <head>…</head>
  <body> == $0
    <div class="holder">…</div>
    <script src="script.js"></script>
  </body>
</html>
```

- Go to the script.js file



Open File

Type ? to see available commands

static-labs.tryhackme.cloud/sites/networking-tcp/

bob.png
static-labs.tryhackme.cloud/sites/networking-tcp/

(index)
static-labs.tryhackme.cloud/sites/networking-tcp/

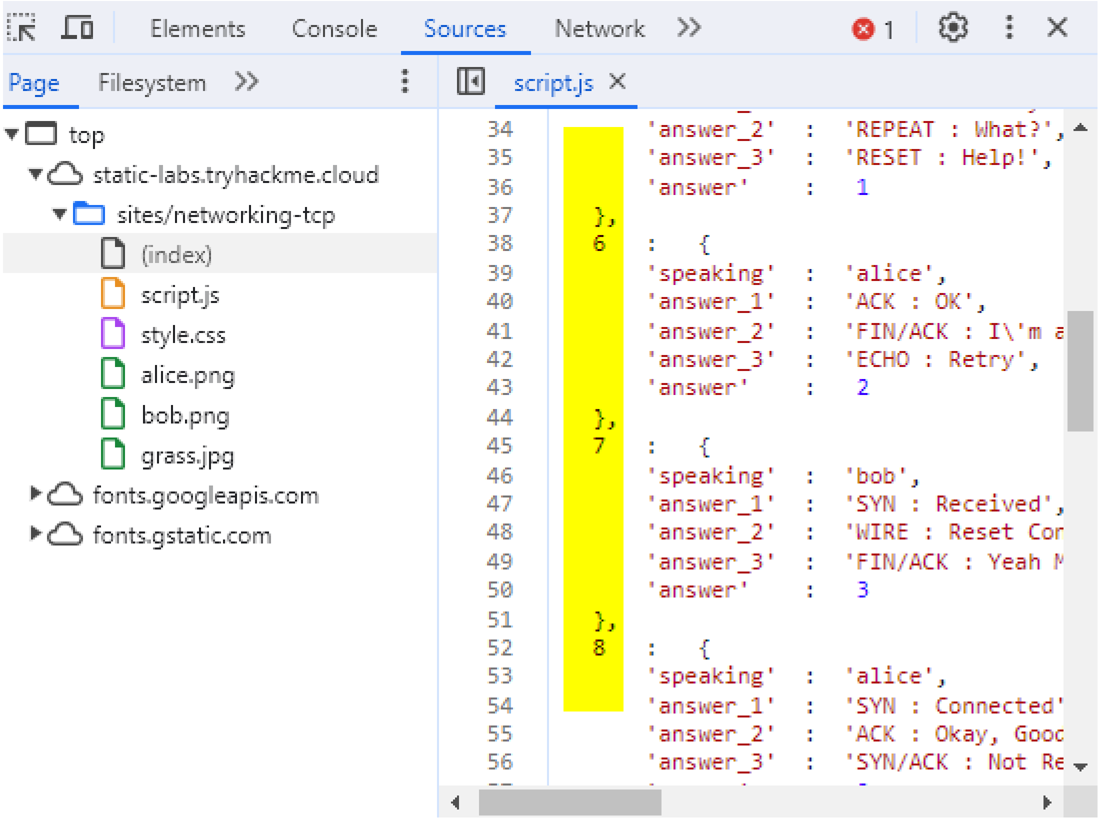
style.css
static-labs.tryhackme.cloud/sites/networking-tcp/

css?family=Ubuntu
fonts.googleapis.com/

css?family=Ubuntu+Mono
fonts.googleapis.com/

script.js
static-labs.tryhackme.cloud/sites/networking-tcp/

- Congratulations, You have your total number of questions



```
        'answer_2'  :  'REPEAT : What?',
        'answer_3'  :  'RESET : Help!',
        'answer'    :   1
    },
    6
        :   {
        'speaking'  :  'alice',
        'answer_1'  :  'ACK : OK',
        'answer_2'  :  'FIN/ACK : I\'m a
        'answer_3'  :  'ECHO : Retry',
        'answer'    :   2
    },
    7
        :   {
        'speaking'  :  'bob',
        'answer_1'  :  'SYN : Received',
        'answer_2'  :  'WIRE : Reset Cor
        'answer_3'  :  'FIN/ACK : Yeah M
        'answer'    :   3
    },
    8
        :   {
        'speaking'  :  'alice',
        'answer_1'  :  'SYN : Connected'
        'answer_2'  :  'ACK : Okay, Gooc
        'answer_3'  :  'SYN/ACK : Not Re
```

Question	Answer
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.	8

Task 3: Ping

- The syntax is **ping [options] <hostname or IP address>** **NOTE: USING OPTIONS IS OPTIONAL**
- Deploy the VM for this task.
- Go to the man page of Ping using “man ping”
- Enter the following command: **"ping -c 10 MACHINE_IP,"** where the "-c 10" option specifies that the ping command should send 10 ICMP echo requests to the specified MACHINE_IP address. NOTE: your MACHINE_IP changes to your actual machine if you have deployed your VM.

Question	Answer
Which option would you use to set the size of the data carried by the ICMP echo request?	-s
What is the size of the ICMP header in bytes?	8
Does MS Windows Firewall block ping by default? (Y/N)	y
Deploy the VM for this task and using the AttackBox terminal, issue the command ping -c “Your Machine IP”. How many ping replies did you get back?	10

Task 4: Traceroute

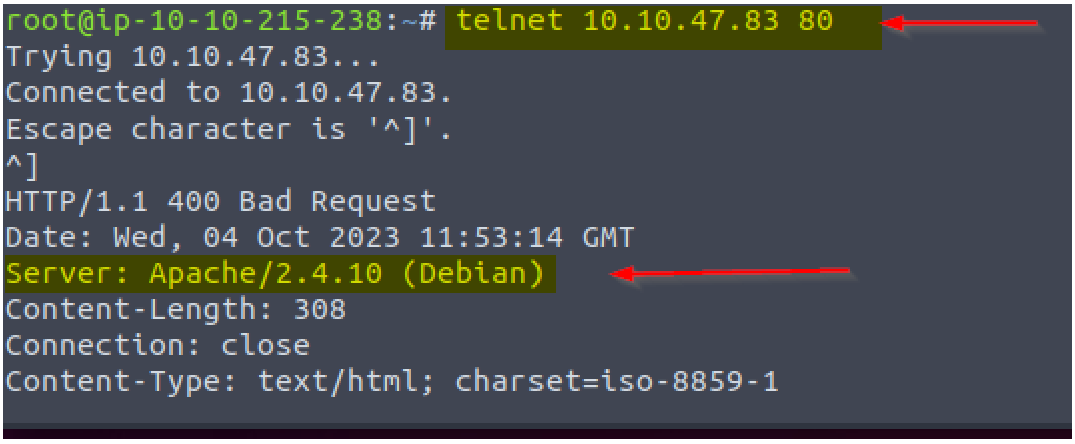
- Syntax is **traceroute [options] <hostname or IP address>**

Question	Answer
In Traceroute A, what is the IP address of the last router/hop before reaching tryhackme.com?	172.67.69.208
In Traceroute B, what is the IP address of the last router/hop before reaching tryhackme.com?	104.26.11.229
In Traceroute B, how many routers are between the two systems?	26

Task 5:Telnet

teletype network is a network protocol used for connecting to remote devices over a network. It allows you to establish a text-based, interactive session with a remote device via the command line interface (CLI) of that device. Its secure alternative is SSH

- Syntax is **telnet [options] [hostname or IP address] [port]**



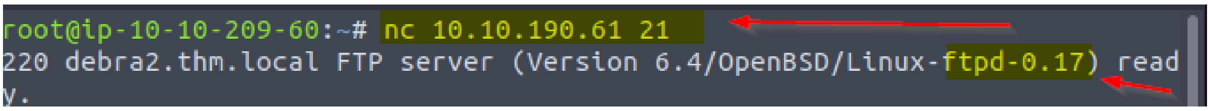
```
root@ip-10-10-215-238:~# telnet 10.10.47.83 80
Trying 10.10.47.83...
Connected to 10.10.47.83.
Escape character is '^]'.
^]
HTTP/1.1 400 Bad Request
Date: Wed, 04 Oct 2023 11:53:14 GMT
Server: Apache/2.4.10 (Debian)
Content-Length: 308
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

Question	Answer
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?	Apache
What is the version of the running server (on port 80 of the VM)?	2.4.10

Task 6: Netcat

Netcat, "nc," is a networking utility used for reading from and writing to network connections. It can function as a client that connects to a listening port or as a server that listens on a port over UDP or TCP.

- The syntax is **nc [options] [hostname] [port]**
- Common options and meanings are -l for listening mode, -n for numeric only, -v for verbose output and -p to specify port.
- For the task, type nc [hostname/IP address] [port]



```
root@ip-10-10-209-60:~# nc 10.10.190.61 21
220 debra2.thm.local FTP server (Version 6.4/OpenBSD/Linux-ftpd-0.17) read
y.
```

Question	Answer
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?	0.17

ADD THIS TO YOUR PERSONAL COMMAND LIST, THIS IS A CUE TO CREATE YOUR OWN TOOL BOX OR TOOL LIST

Command	Syntax
Ping on Linux or macOS	ping -c [Hostname]
Ping on MS Windows	ping -n [Hostname]
Traceroute on Linux or macOS	traceroute [Hostname]
Tracert on MS Windows	Tracert [Hostname]
telnet	telnet [Hostname] [Port Number]
netcat as client	nc [Hostname] [Port Number]
netcat as server	nc -lvnp PORT_NUMBER