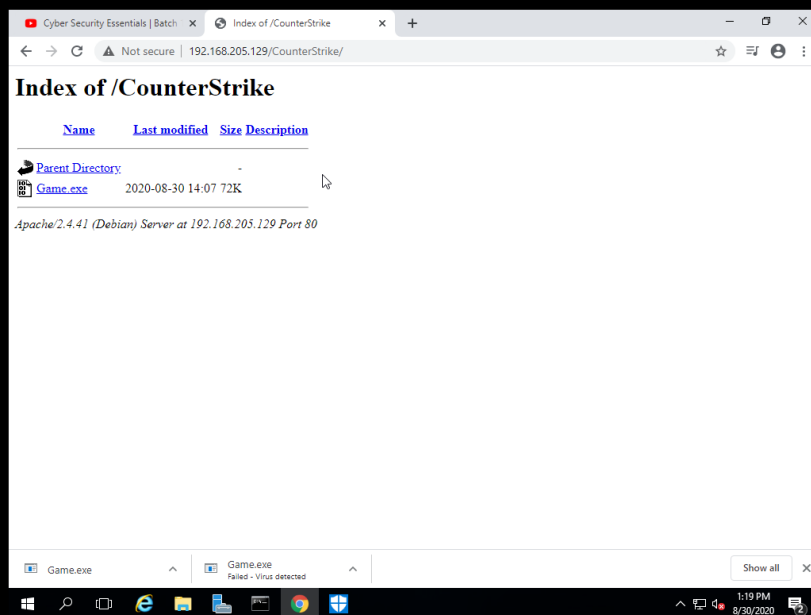
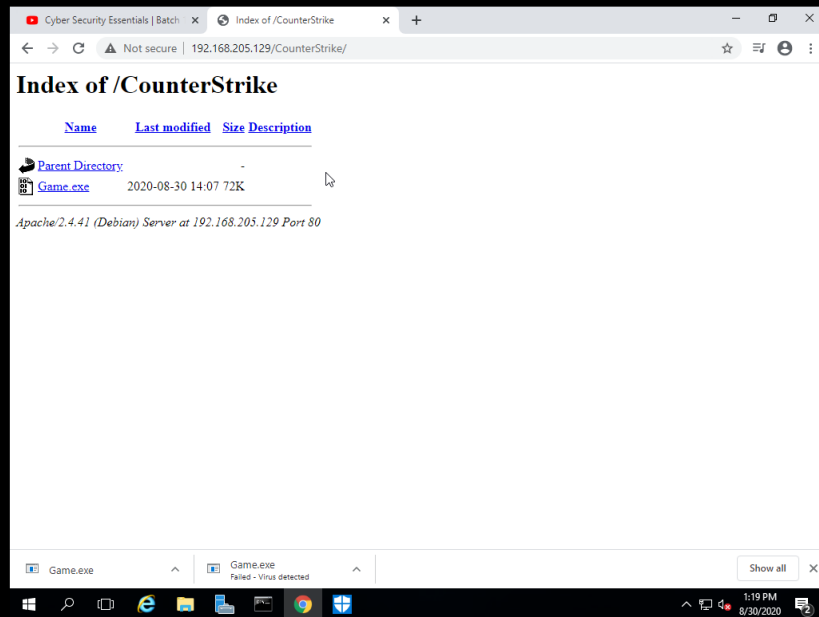


## Day 6 Assignment -

### Question 1:

1. Create payload for windows.
2. Transfer the payload to the victim's machine.
3. Exploit the victim's machine.

## Game.exe



Victim downloaded the exploit.

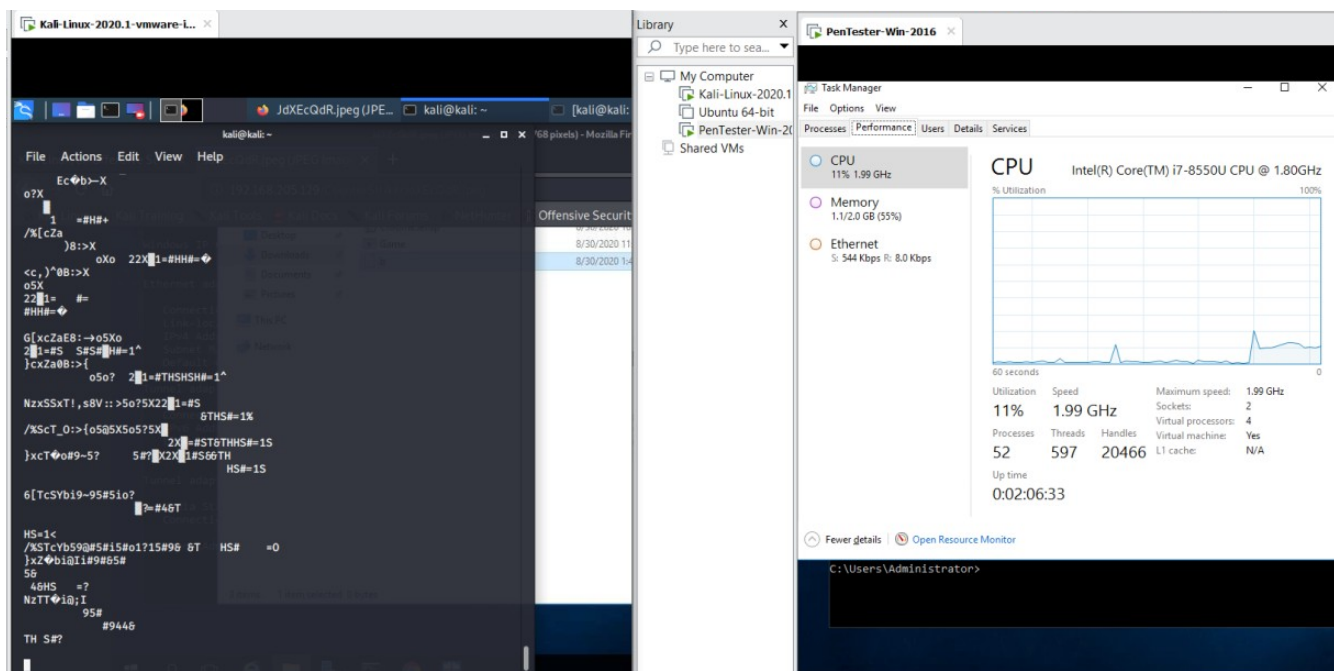
```
kali@kali: ~  
File Actions Edit View Help  
Name : Software Loopback Interface 1  
Hardware MAC : 00:00:00:00:00:00  
MTU : 4294967295  
IPv4 Address : 127.0.0.1  
IPv4 Netmask : 255.0.0.0  
IPv6 Address : ::1  
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff  
  
Interface 2  
===== Name : Intel(R) 82574L Gigabit Network Connection  
Hardware MAC : 00:0c:29:a4:1f:a6  
MTU : 1500  
IPv4 Address : 192.168.205.134  
IPv4 Netmask : 255.255.255.0  
IPv6 Address : fe80::e141:b4a6:f3ff:2161  
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff  
  
Interface 4  
===== Name : Teredo Tunneling Pseudo-Interface  
Hardware MAC : 00:00:00:00:00:00  
MTU : 1280  
IPv4 Address : 2001:0:348b:fb58:2049:2fca:3f57:3279  
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff  
IPv6 Address : fe80::205e:be4:3f57:3279  
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff  
  
Interface 9  
===== Name : Microsoft ISATAP Adapter #2  
Hardware MAC : 00:00:00:00:00:00  
MTU : 1280  
IPv4 Address : fe80::5efe:c0a8:cd86  
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

```
Type here to search  
My Computer  
Kali-Linux-2020.1  
Ubuntu 64-bit  
PenTester-Win-20  
Shared VMs  
Recycle Bin  
Downloads  
File Home Share View  
C:\Users\Administrator>ipconfig  
Windows IP Configuration  
  
Ethernet adapter Ethernet0:  
  
Connection-specific DNS Suffix . : localdomain  
Link-local IPv6 Address . . . . . : fe80::e141:b4a6:f3ff:2161%2  
IPv4 Address. . . . . : 192.168.205.131  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.205.2  
  
Tunnel adapter Teredo Tunneling Pseudo-Interface:  
  
Connection-specific DNS Suffix . :  
IPv6 Address. . . . . : 2001:0:348b:fb58:2049:2fca:3f57:327c  
Link-local IPv6 Address . . . . . : fe80::2049:2fca:3f57:327c%4  
Default Gateway . . . . . :  
  
Tunnel adapter isatap.localdomain:  
  
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . : localdomain  
  
C:\Users\Administrator>
```

```
JdXEcQdR.jpeg (JPEG Image, 1024 x 768 pixels) - Scaled (73%) - Mozilla Firefox  
JdXEcQdR.jpeg (JPEG Image, 1024 x 768 pixels) - Scaled (73%) - Mozilla Firefox  
192.168.205.129/CounterStrike/JdXEcQdR.jpeg 90%  
Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSF5  
Downloads  
Name Date modified Type Size  
ChromeSetup 8/30/2020 10:33 AM Application 1,205 KB  
Game 8/30/2020 11:33 AM Application 73 KB  
b 8/30/2020 1:42 PM Text Document 0 KB
```

```
Type here to search  
My Computer  
Kali-Linux-2020.1  
Ubuntu 64-bit  
PenTester-Win-20  
Shared VMs  
Recycle Bin  
Downloads  
File Home Share View  
C:\Users\Administrator>ipconfig  
Windows IP Configuration  
  
Ethernet adapter Ethernet0:  
  
Connection-specific DNS Suffix . : localdomain  
Link-local IPv6 Address . . . . . : fe80::e141:b4a6:f3ff:2161%2  
IPv4 Address. . . . . : 192.168.205.131  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.205.2  
  
Tunnel adapter Teredo Tunneling Pseudo-Interface:  
  
Connection-specific DNS Suffix . :  
IPv6 Address. . . . . : 2001:0:348b:fb58:2049:2fca:3f57:327c  
Link-local IPv6 Address . . . . . : fe80::2049:2fca:3f57:327c%4  
Default Gateway . . . . . :  
  
Tunnel adapter isatap.localdomain:  
  
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . : localdomain  
  
C:\Users\Administrator>
```

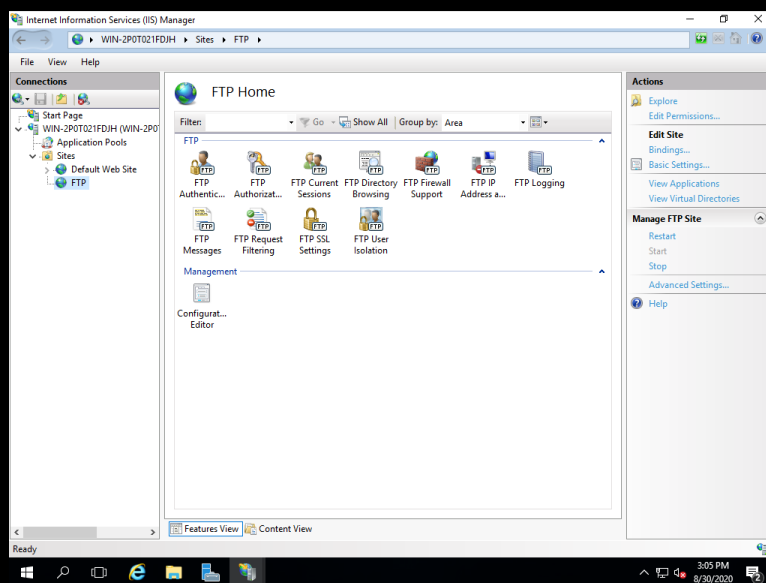
Attacker used payload to make the victim's machine busy.



## Question 2:

1. Create an FTP server
2. Access FTP server from windows command prompt
3. Do a mitm and username and password of FTP transaction using wireshark and dsniiff.

Creation of FTP server



### Accessing FTP using command prompt.

```
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>_
```

Dsniff caught the username and password during FTP transaction.

The image is a composite of three screenshots from a Kali Linux virtual machine, illustrating a network security exercise.

**Left Screenshot:** A Windows command prompt window titled "C:\WINDOWS\system32\cmd.exe". The user is connected to a Kali Linux VM via FTP. The command prompt shows the following output:

```

Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1

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

C:\Users\DAMISH>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\DAMISH>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\DAMISH>

```

**Middle Screenshot:** A Kali Linux terminal window showing the execution of a netmap scan on the target IP 192.168.205.134. The command is `nmap -sS 192.168.205.134`. The output shows a single open port, 21 (ftp).

```

kali@kali:~$ nmap -sS 192.168.205.134
Nmap scan report for 192.168.205.134
Host is up (0.0000s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
21/tcp    OPEN  ftp

```

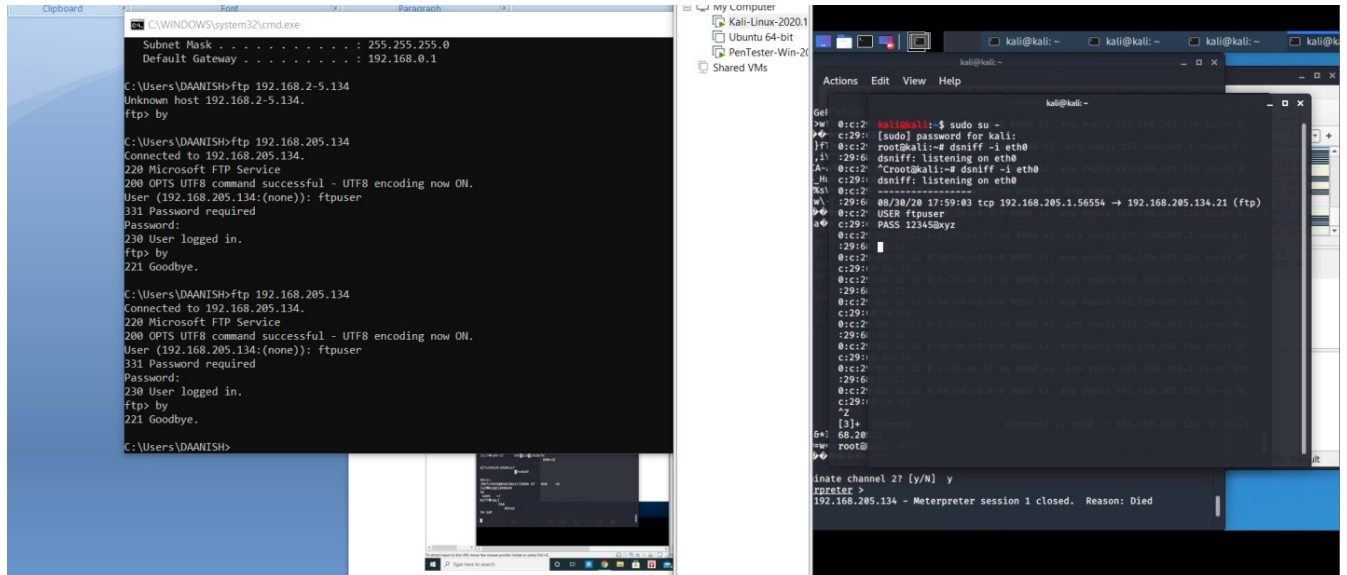
**Right Screenshot:** A Kali Linux terminal window showing the execution of a netmap scan on the target IP 192.168.205.134 with the `-u root` flag. The command is `nmap -sS 192.168.205.134 -u root`. The output shows a single open port, 22 (ssh).

```

kali@kali:~$ nmap -sS 192.168.205.134 -u root
Nmap scan report for 192.168.205.134
Host is up (0.0000s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    OPEN  ssh

```

Wireshark also caught the username and the password.



Thankyou!