

LetsUpgrade

Cyber Security Essentials

Day 6 Assignment

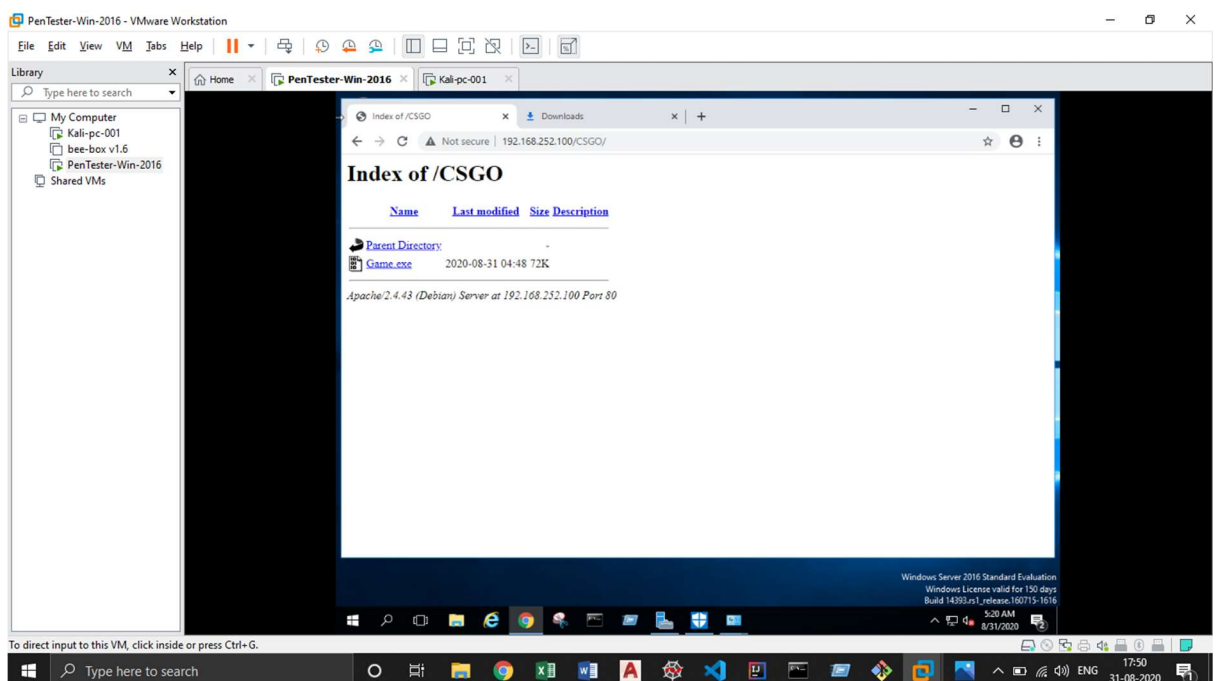
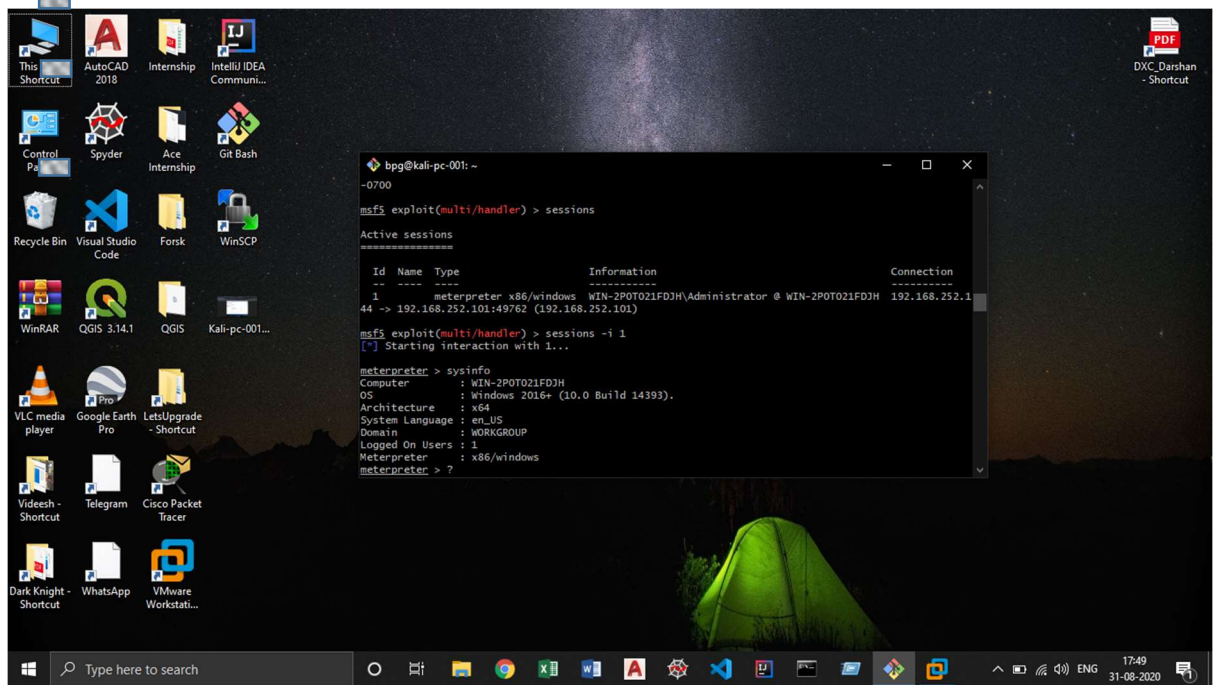
Darshan

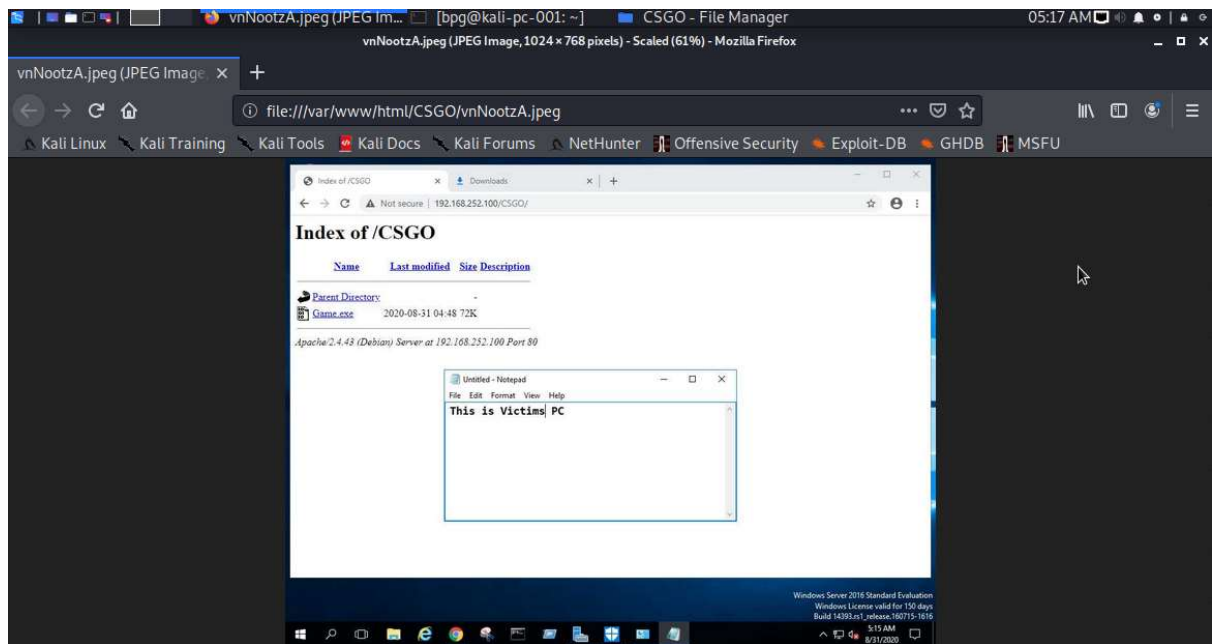
+91 7022086560

darshanbangera1612@gmail.com

1. Hacking Windows using Metasploit:

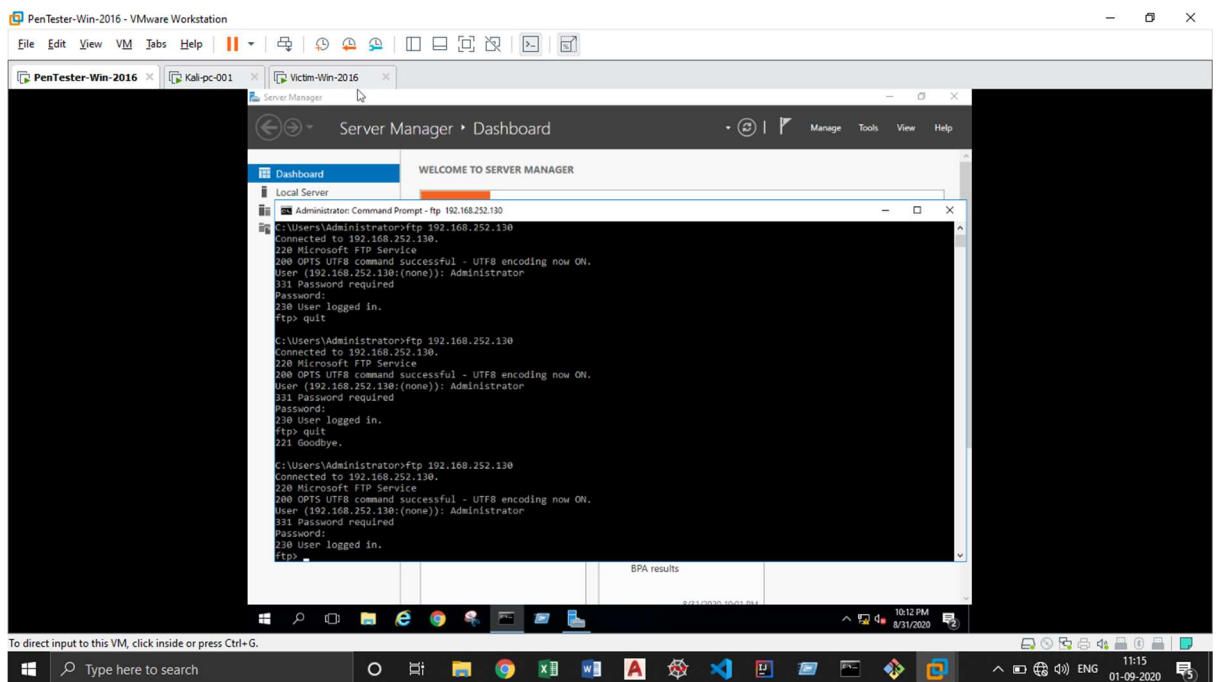
- Creating payload for Windows.
- Transferring the payload to the victim's machine.
- Exploit the victim's machine.



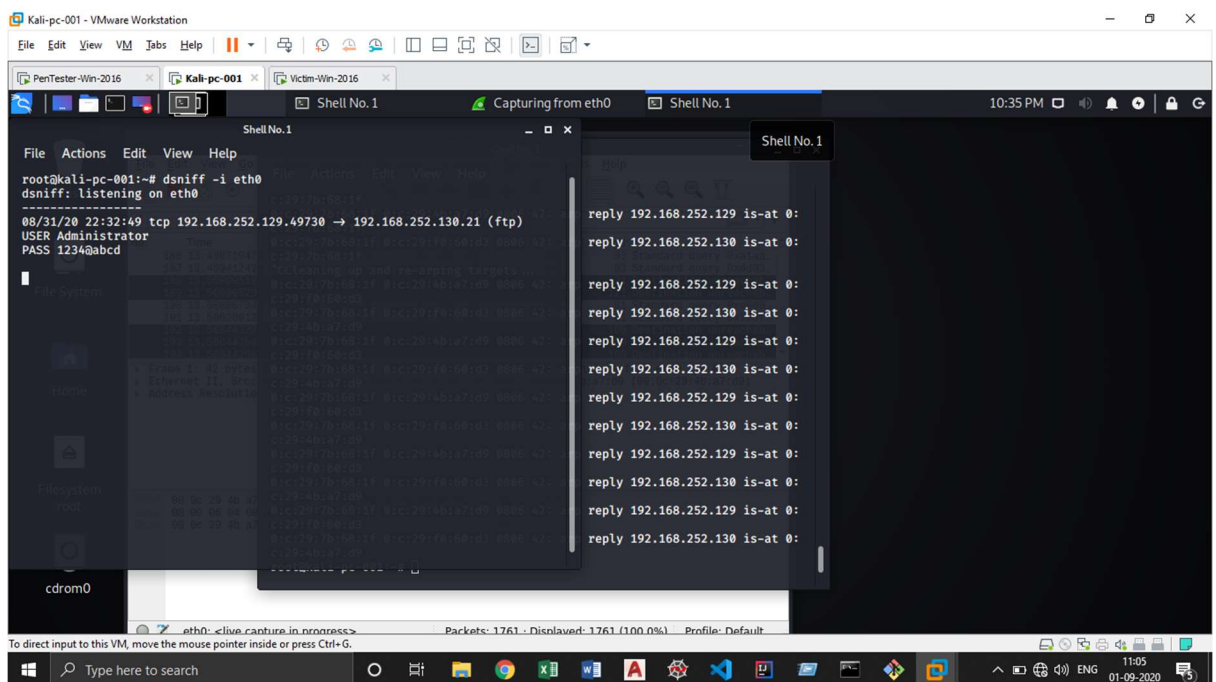


2. Man In TheMiddle Attack on FTP server:

- **Accessing FTP server on the client system using CMD**



- **Using dsniff**



- Using Wireshark

The screenshot shows a Kali Linux virtual machine environment. On the left, a terminal window displays the execution of a dnstiff attack:

```
root@kali-pc-001:~# dnstiff -i eth0
dnstiff: listening on eth0
08/31/20 22:32:49 tcp 192.168.252.2
USER Administrator
PASS 1234abcd
```

The main window shows Wireshark capturing traffic on the `eth0` interface. The packet list shows several packets, including a DNS query and response. The packet details pane shows the structure of the captured packets, including Ethernet II, Internet Protocol Version 4, and DNS.

No.	Time	Source	Destination	Protocol	Length	Info
3864	419.852717501	Vmware_c0:00:08	Broadcast	ARP	60	Who has 192.168.252.2
3865	419.975263667	192.168.252.129	192.168.252.2	DNS	84	Standard query 0x9464
3866	419.975263767	192.168.252.2	192.168.252.129	ICMP	112	Destination unreachable
3867	419.975263842	192.168.252.2	192.168.252.129	ICMP	112	Destination unreachable
3868	420.852846692	Vmware_c0:00:08	Broadcast	ARP	60	Who has 192.168.252.2
3869	421.774996591	Vmware_f0:60:d3	Vmware_f0:7a:3c	ARP	60	Who has 192.168.252.2
3870	421.774996941	Vmware_f0:60:d3	Vmware_f0:60:d3	ARP	60	192.168.252.2 is at 0
3871	422.381814724	Vmware_c0:00:08	Broadcast	ARP	60	Who has 192.168.252.2

The packet details pane for the selected packet (Frame 1) shows the following structure:

- Ethernet II, Src: Vmware_7b:68:1f (00:0c:29:7b:68:1f), Dst: Vmware_4b:a7:d9 (00:0c:29:4b:a7:d9)
 - Destination: Vmware_4b:a7:d9 (00:0c:29:4b:a7:d9)
 - ...0... = LG bit: Globally unique address (factory default)
 - ...0... = IG bit: Individual address (unicast)
 - Source: Vmware_7b:68:1f (00:0c:29:7b:68:1f)
 - ...0... = LG bit: Globally unique address (factory default)
 - ...0... = IG bit: Individual address (unicast)

The packet bytes pane shows the raw data of the packet:

```
0000 00 0c 29 4b a7 d9 00 0c 29 7b 68 1f 08 06 00 01 ...K... }{h...
0010 08 06 04 04 00 02 00 0c 29 7b 68 1f c0 a8 fc 81 ...K... }{h...
0020 00 0c 29 4b a7 d9 c0 a8 fc 82 ...K... }
```