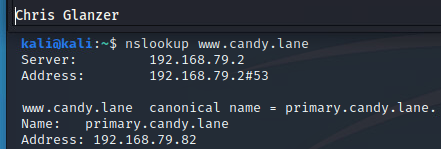
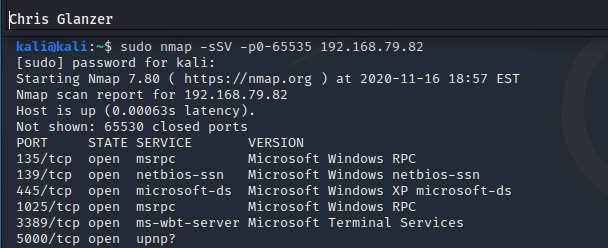
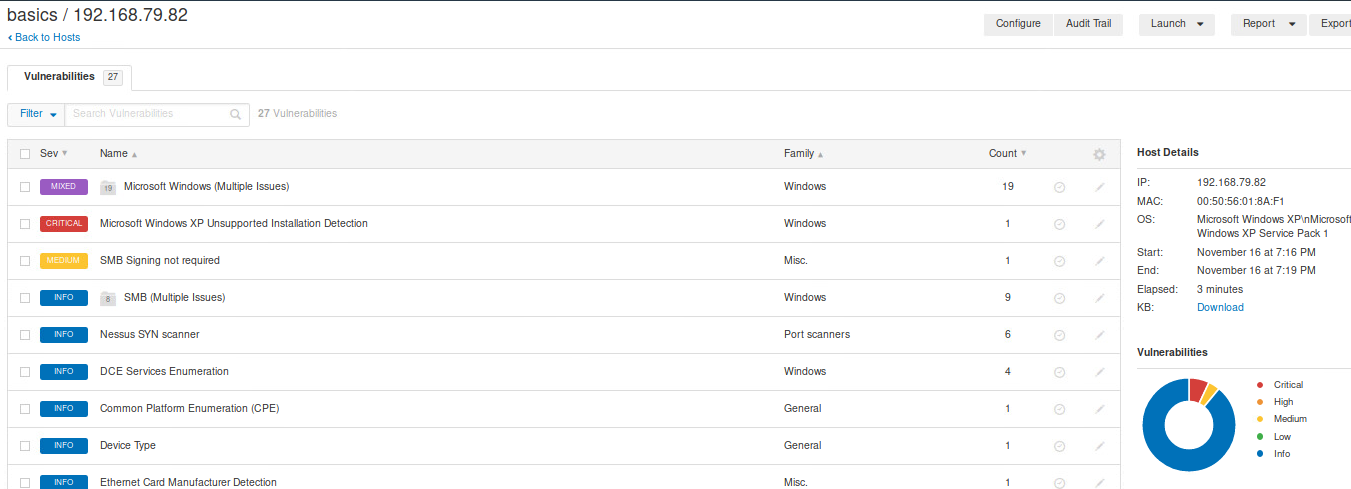
**CSC 436 Lab 11** – 30 points

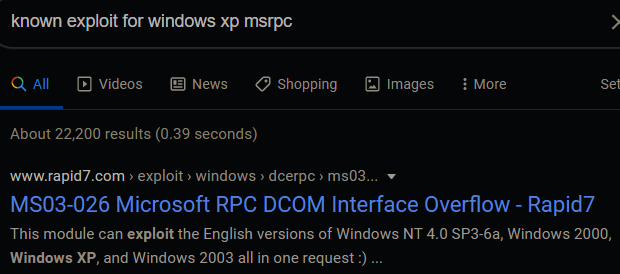
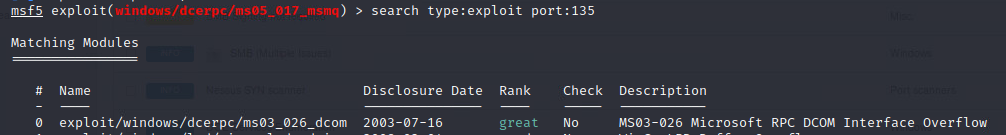
**Part 1: Candy.lane Adventures** *13 points*

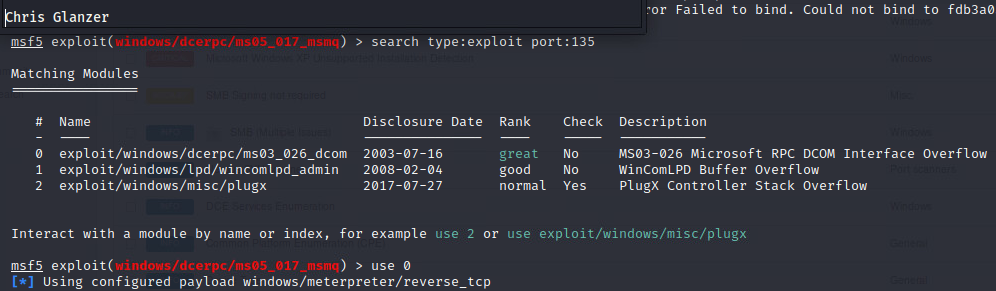
A. Show how you found the ip address for www.candy.lane.

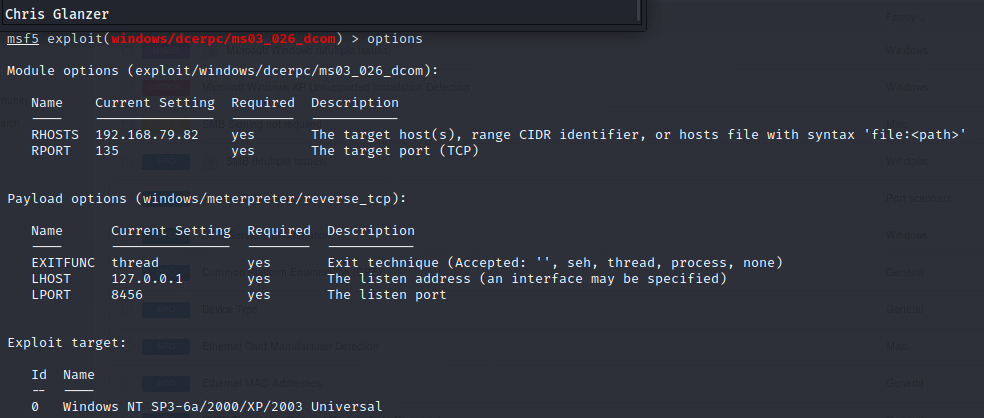
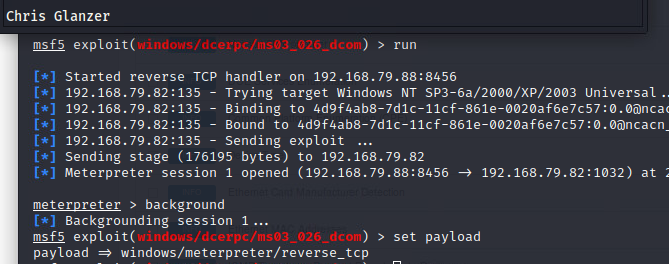
B. Show your use of nmap to identify open ports on candy.lane.

C. Show your use of Nessus/OpenVas/nmap to identify vulnerabilities on candy.lane. You are required to run a vulnerability scan and provide the screenshot, but you may use other methods as well to find vulnerabilities. Please describe and include up to two additional screenshots if this applies.

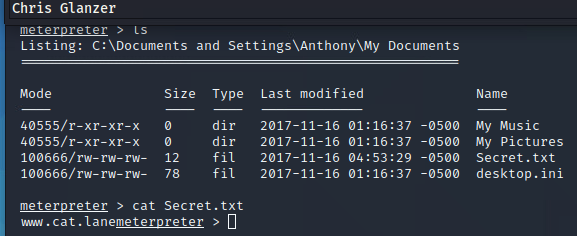
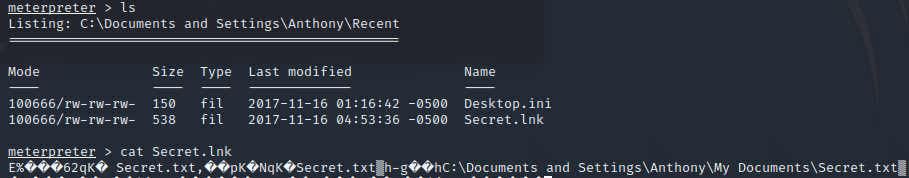
Both this lab and the last lab I spent a lot of time trying to connect dots between msf and nessus, but the first result when searching for the port number in Metasploit was the thing that worked.

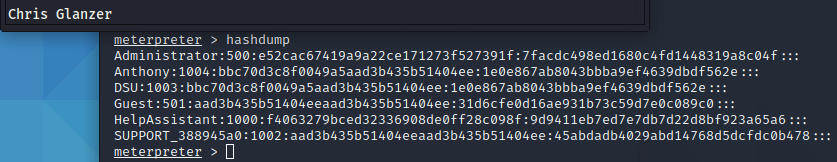
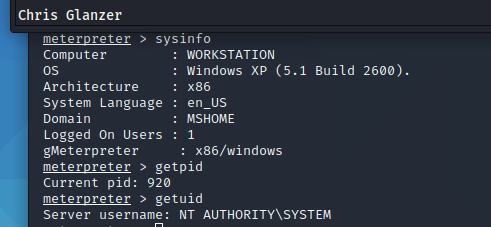
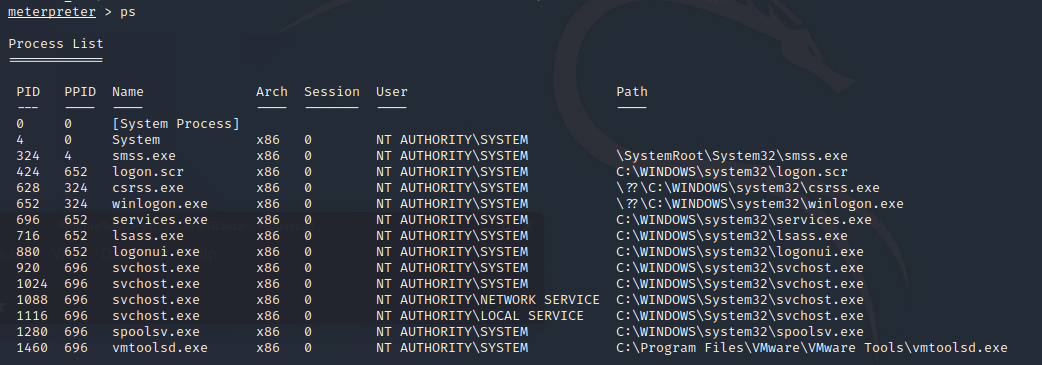


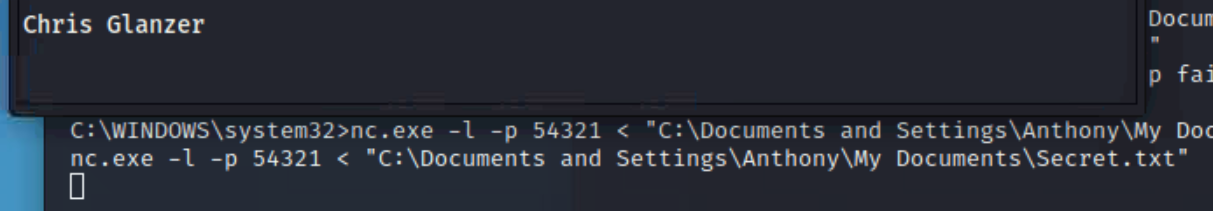
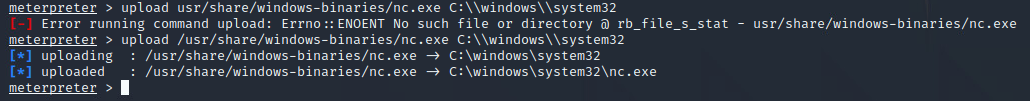
D. Show your use of Metasploit to compromise candy.lane. What is the exploit? What are the options? You may include two or three screenshots here.  
another note on this: I swear that I had tried using this exploit previously (as can be seen by the pre-set rhost) but it didn’t work. After a couple hours of fiddling around trying to find another way I tried it again found out that the lhost had defaulted to a loopback, **and I did not set a payload.** But somehow it popped a meterpreter. I just printed out the payload that was set. I’m not sure if this was left over from when I was trying earlier, or if it is default. But it’s what was set.

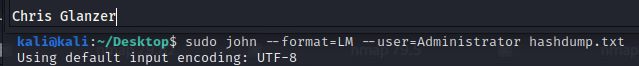
E. Obtain a meterpreter shell on candy.lane. You may upgrade if need be. Refer to our lecture content on upgrading meterpreter and alternate ways of doing so.

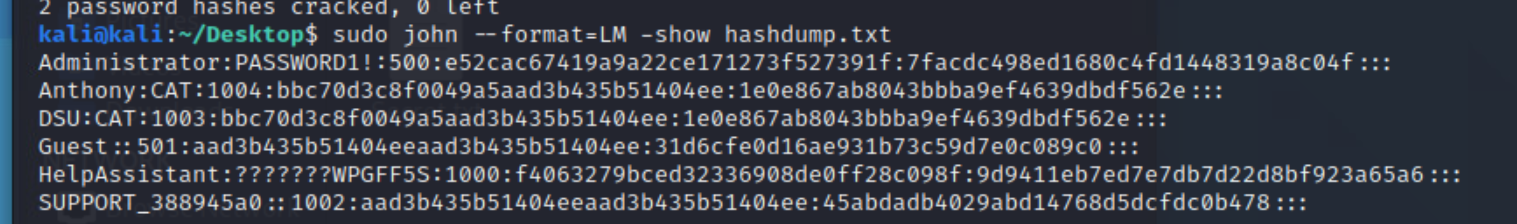
This screencap ^ has the payload printed at the bottom, after I backgrounded the meterpreter session.

F. Navigate and find the confidential secret.   


G. Use five meterpreter commands. You may use two or three screenshots here if necessary.

H. Upload Netcat to your target. Execute Netcat on the target and use it to download a file. Show that the file downloaded successfully. 

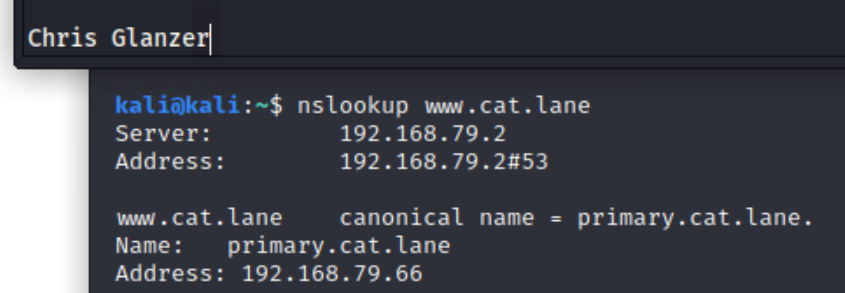
I. Obtain passwords for users. Your method of doing this will vary, and it is at your discretion is to how you perform this.



**Part 2: Candy.lane Redux** *12 points*

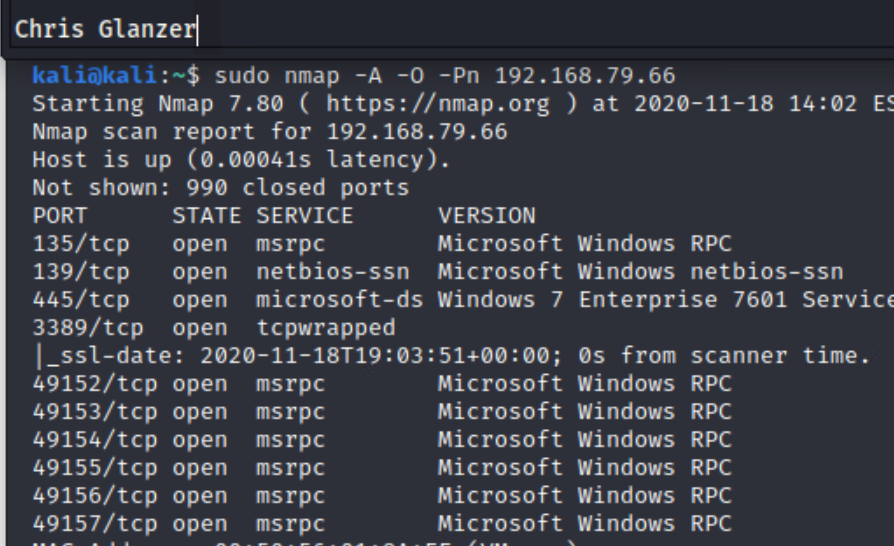
Preface: There is another target owned by the same business. Can you find it? There are a couple ways. First, you could use some of the techniques in our earlier phases to find the location. You also might find information in the candy.lane machine. *Hint:* Try looking in My Documents.

1. How did you find the ip address for the new target?

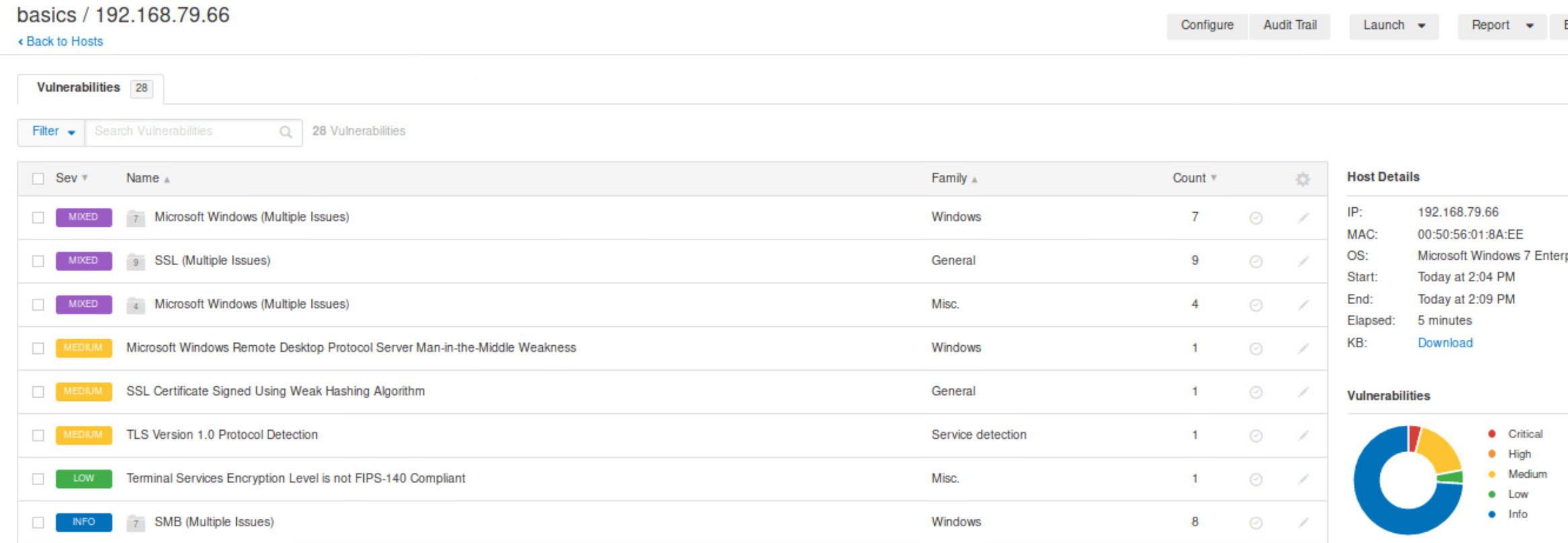


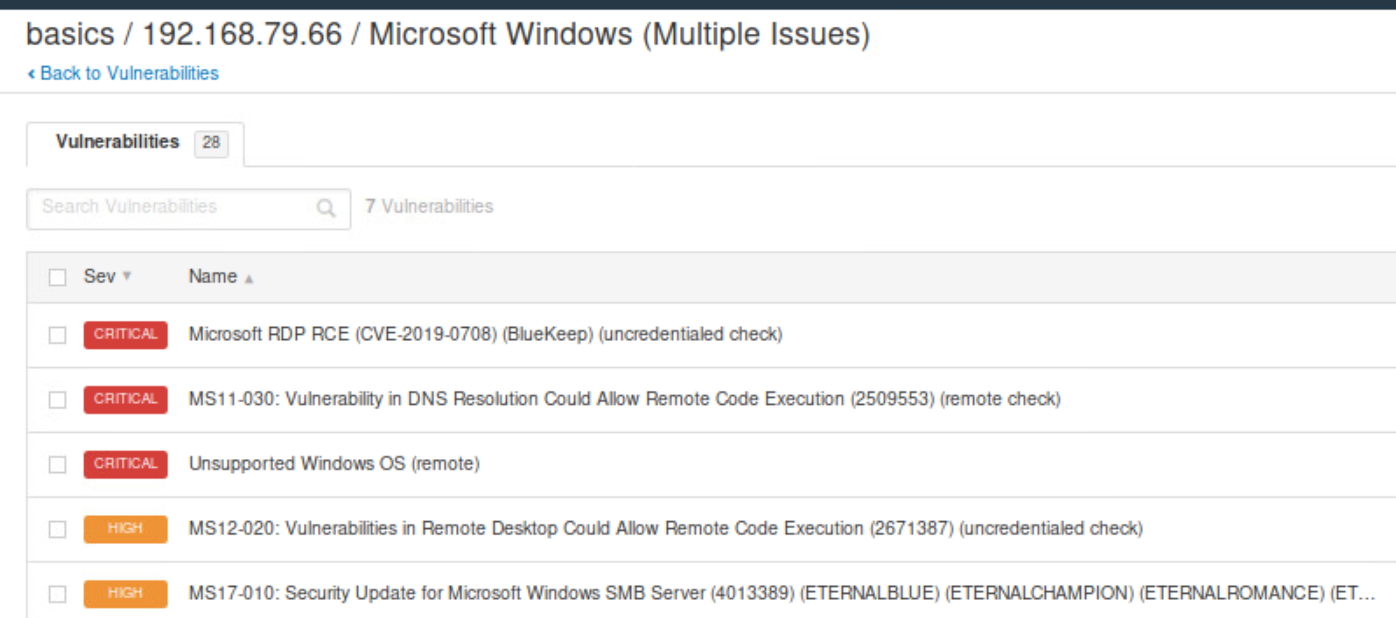
Also used dig, but this was same info, just more concise

B. Show your use of nmap to identify open ports for this target.



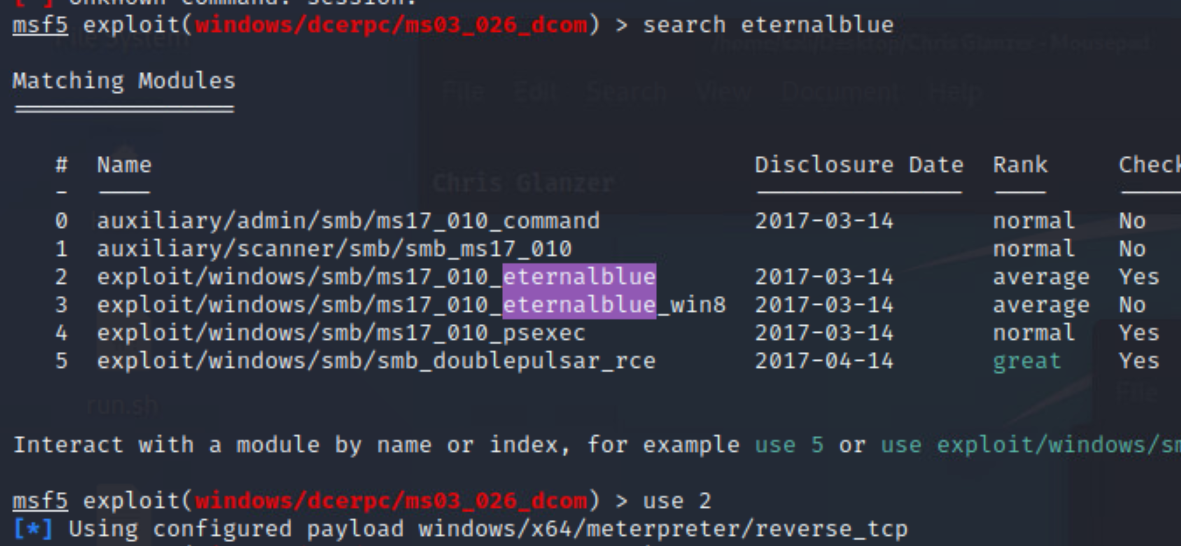
C. Show your use of Nessus/OpenVas/nmap to identify vulnerabilities on the target. You are required to run a vulnerability scan and provide the screenshot, but you may use other methods as well to find vulnerabilities. Please describe and include up to two additional screenshots if this applies.

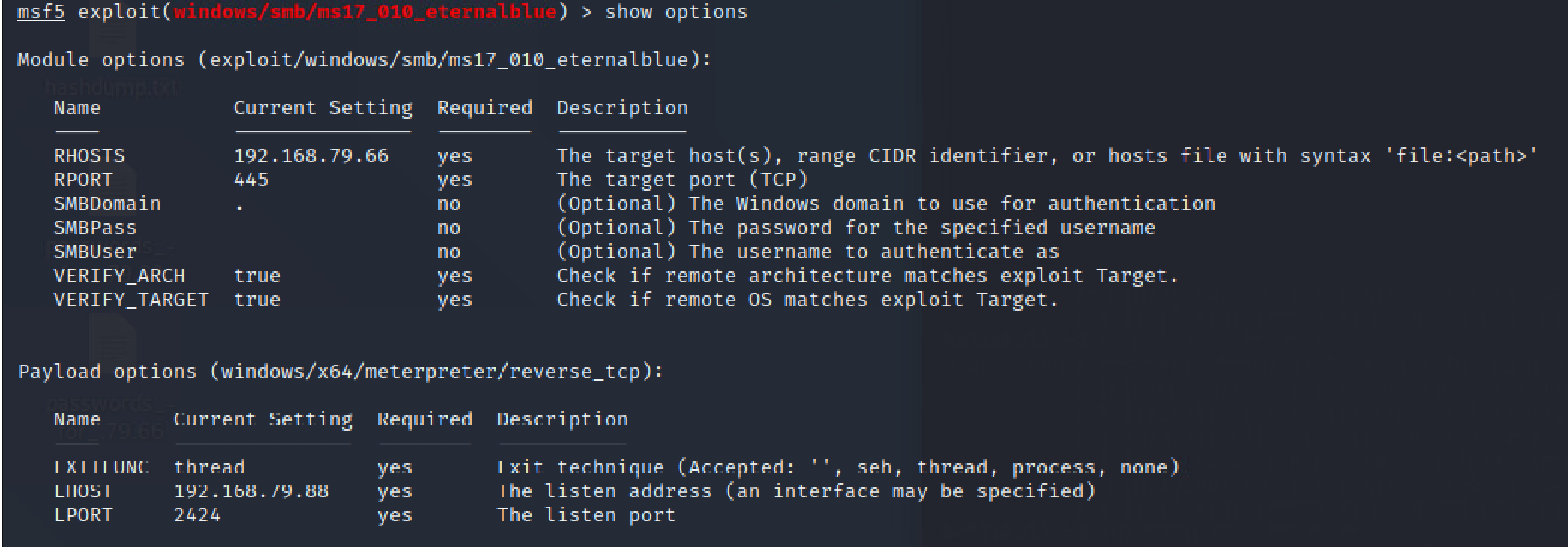


****

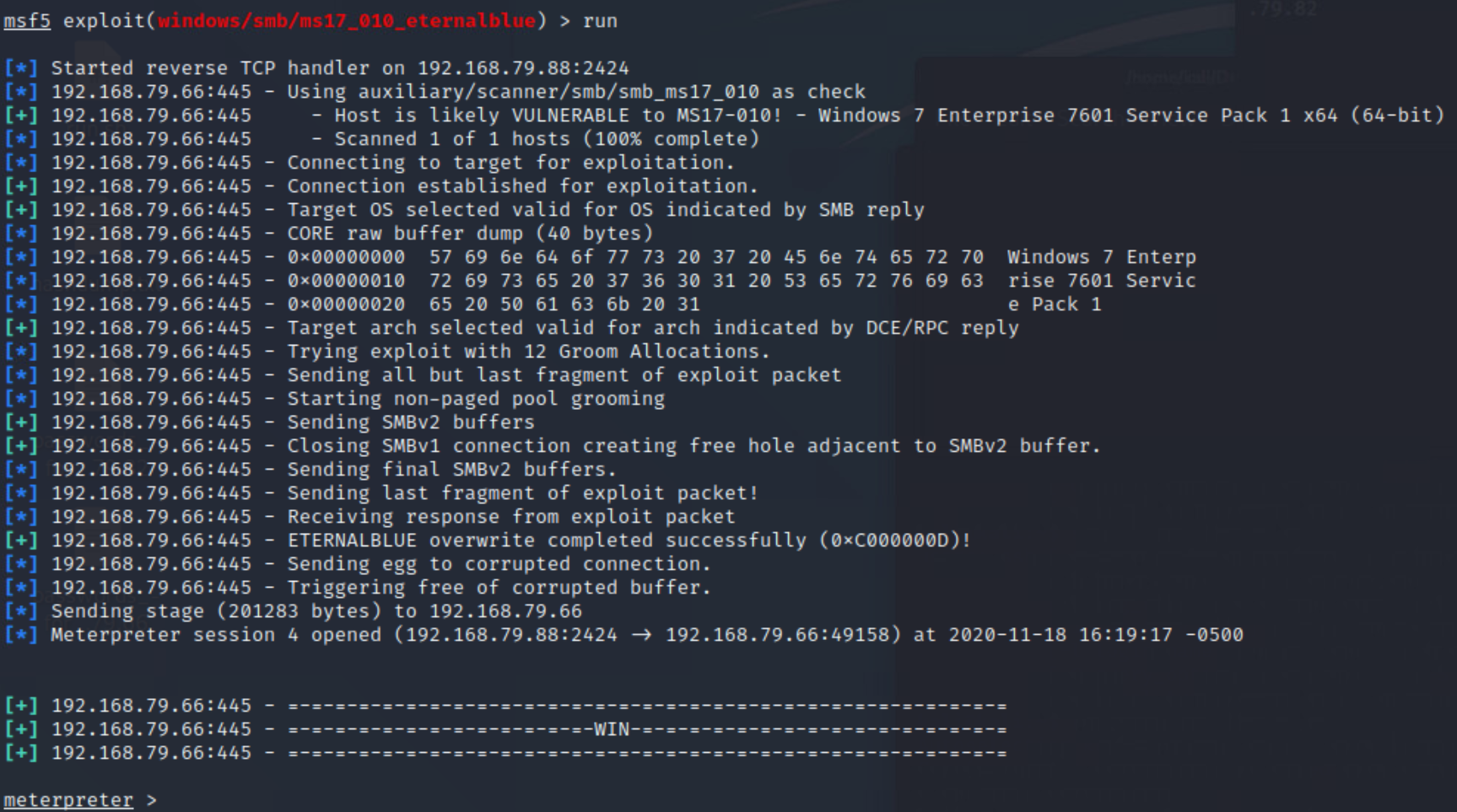
**Ayyyy Eternalblue Spotted.**

D. Show your use of Metasploit to compromise the target. In this case, you may open up the machine if you wish to and interact with it. (Hint: You may need a password to do this.) That way you can make use of client side attacks. For instance, you might give the user a link to click on, and you could simulate that yourself. If you find a password that works, you might also attempt to pass the hash. How you compromise this is up to you. You may certainly use multiple screenshots here.

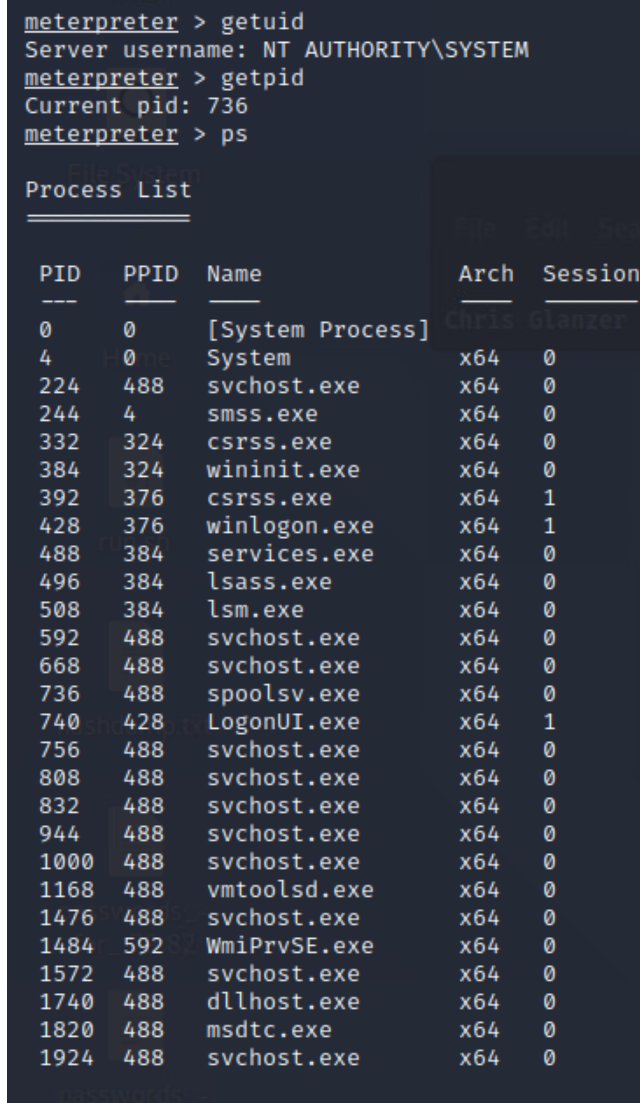


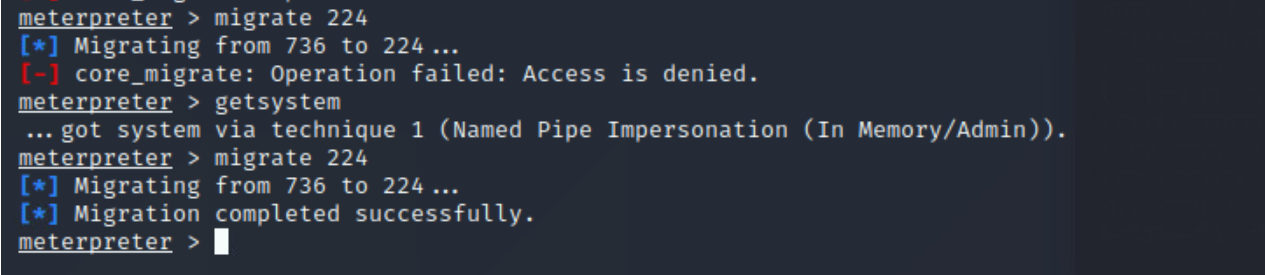


E. Obtain a meterpreter shell. Partial credit for other shells is available.



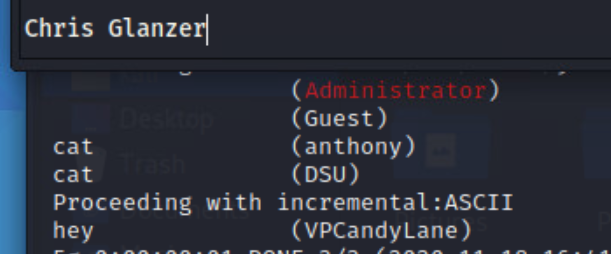
F. Use five meterpreter commands. You may use two or three screenshots here if necessary.

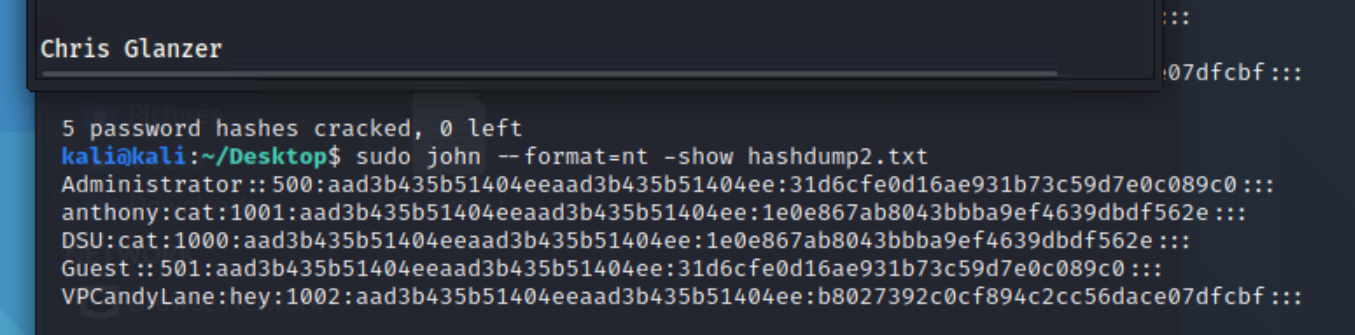




I made a mistake migrating to this process and had to rerun the exploit, as I lost my privs and couldn’t re-escelate

H. Obtain passwords for users.





**Part 3: Questions** *5 points*

\*\*\*Screenshots are not acceptable for these questions. Provide typed responses.

A. List all the domains you found. You should find at least two.   
[www.candy.lane](http://www.candy.lane)

Primary.candy.lane  
[www.cat.lane](http://www.cat.lane)

Primary.cat.lane

B. List all the IP addresses you found. Provide identifying information, e.g. ports open. Can you identify any services or software (versions)? Expect reduced credit if specific software and specific versions are not identified.

192.168.79.82

Microsoft Windows XP (Windows 2000 LAN Manager)

NetBios name: Workstation

Port: service/Version

135: Microsoft Windows RPC

139: Microsoft Windows Netbios-ssn

445: Windows XP Microsoft-ds

1025: Microsoft Windows RPC

3389: Microsoft Terminal Services (rdp)

5000: No version information available. Nmap hesitantly identifies this as upnp (used by printers) but it looks to me like an http1.1 webservice, which when navigated to via a browser does in fact serve a blank web page.

192.168.79.66

Windows 7 Enterprise 7601 Service Pack 1 (Windows 7 Enterprise 6.1)

Netbios name: WINDOWS7SP1-1

Port: service/Version

135: Microsoft Windows RPC

139: Microsoft Windows Netbios-ssn

445: Windows 7 Enterprise 7601 Service Pack 1 Microsoft-ds (workgroup: WORKGROUP)

1025: Microsoft Windows RPC

3389: Microsoft Terminal Services (rdp) (TCPwrapped)

49152: Microsoft Windows RPC

49153: Microsoft Windows RPC

49154: Microsoft Windows RPC

49155: Microsoft Windows RPC

49156: Microsoft Windows RPC

49157: Microsoft Windows RPC

192.168.79.2

Windows 7 Enterprise 7601 Service Pack 1 (Windows 7 Enterprise 6.1)

Netbios name: WINDOWS7SP1-0

Port: service/Version

53: DNS/ ISC BIND 9.10.6

135: Microsoft Windows RPC

139: Microsoft Windows Netbios-ssn

445: Windows XP Microsoft-ds

1025: Microsoft Windows RPC

3389: Microsoft Terminal Services (rdp) (through SSL)

49152: Microsoft Windows RPC

49153: Microsoft Windows RPC

49154: Microsoft Windows RPC

49155: Microsoft Windows RPC

49156: Microsoft Windows RPC

49157: Microsoft Windows RPC

192.168.79.5

Windows 8.1 Enterprise 9600 (Windows 8.1 Enterprise 6.3)

Netbios name: WINDOWS8-0

Port: service/Version

135: Microsoft Windows RPC

139: Microsoft Windows Netbios-ssn

445: Windows XP Microsoft-ds

554: rtsp (service ID is hesitant… version not identified)

2869: Microsoft HTTPAPI httpd2.0 (SSDP/UPnP)

3389: Microsoft Terminal Services (rdp) (through SSL)

10243: Microsoft HTTPAPI httpd2.0 (SSDP/UPnP)

49152: Microsoft Windows RPC

49153: Microsoft Windows RPC

49154: Microsoft Windows RPC

49155: Microsoft Windows RPC

49156: Microsoft Windows RPC

49157: Microsoft Windows RPC

49158: Microsoft Windows RPC

C. Where does the DNS come from? What do you know about it?

Comes from …79.2 . I ran an nmap scan on it, as seen above. I can rdp in. I attempted a zone transfer but it failed. Not 100% certain that it wasn’t my own user error though – since I’ve never done one before. The nmap scan was included above. I ran a nessus scan, but nothing looked capable of granting me access.

**Bonus** *Point Varies based on quality*

1. What is the Candy Lane bank routing number? (This is not on one of the above two targets.) Notes: You do not need to use Metasploit here, although you could attempt it. Show how you found it. Use sufficient screenshots and commentary to describe your process.

**Deliverable**

* Turn in a PDF/DOC/DOCX that has requested responses. Screenshots must be cropped appropriately and readable to be accepted. Please respond to all questions, numbering the responses that you provide.
* **Your name must be visible in screenshots, as shown in example on page 1.**