CSC 436 Fall 2020 – Take-Home Final

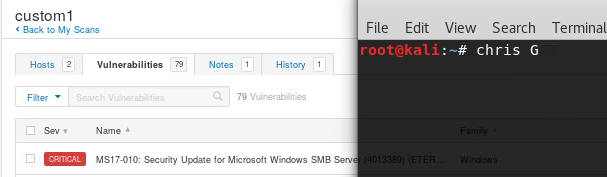
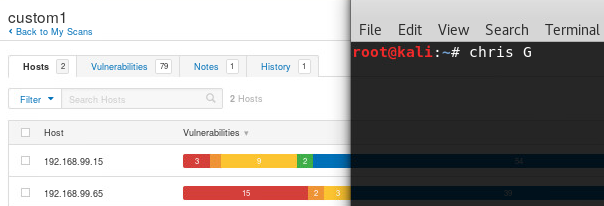
Use the IA lab environment to perform these tasks on the vApp called **CSC436-Brbr-Final**. Provide all necessary screenshots. Where appropriate, include a written response as well. Assume screenshots are required for each question. **Number your responses clearly; responses without numbers will not be graded.**

Total points: 60

**Your targets: 192.168.99.15, 192.168.99.65**

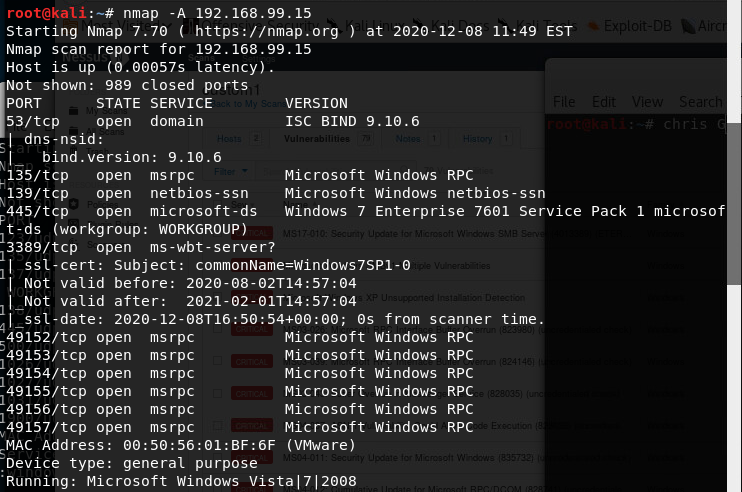
1. Run OpenVas or Nessus on the target. The username is **user** and password is **useruser** for both. Do a scan and generate a the report. Show the report from each scanner. What is one item to explore and why? This doesn’t mean you will be successful with it, but the vuln report gives you a reason to pursue it. *6 points*

One item to explore would be the eternalblue vuln which is present on both boxes,

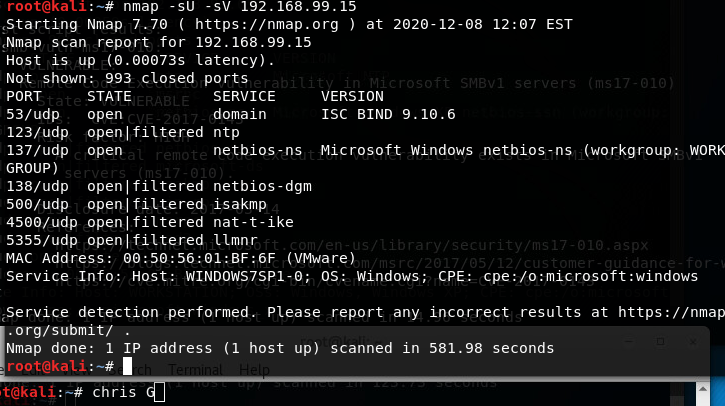


1. Use nmap to identify all the open ports on the targets. Use multiple scans to try to ensure you do not miss some ports. *6 points*

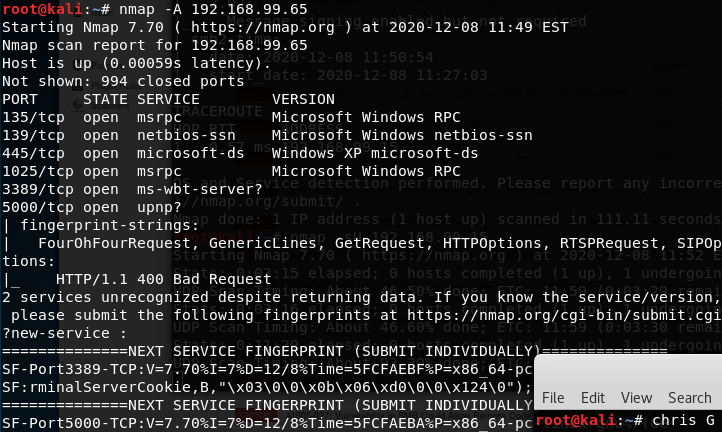
192.168.99.15 TCP



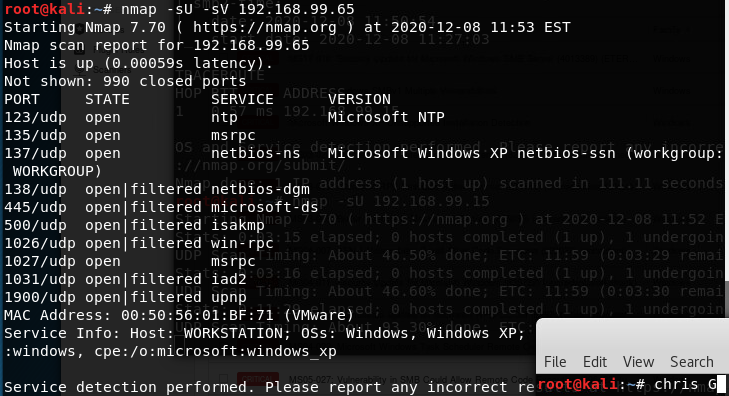
192.168.99.15 UDP



192.168.99.65 TCP

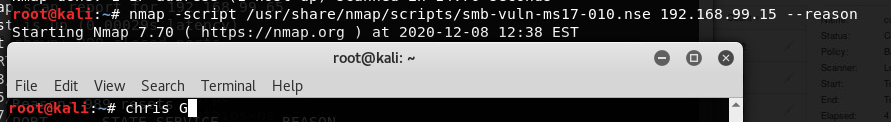


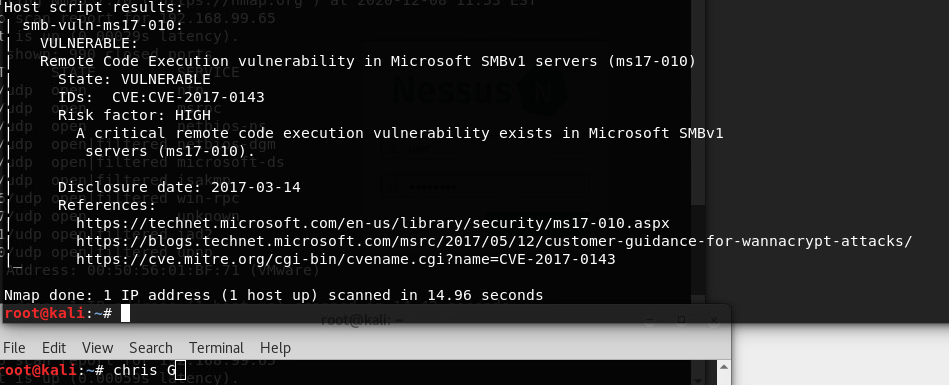
192.168.99.65 UDP



1. Use script reason with nmap on each target E.g. nmap –script vuln ip --reason. Is there a CVE recommended, and if so what? *6 points*

Recommended: CVE-2017-0143



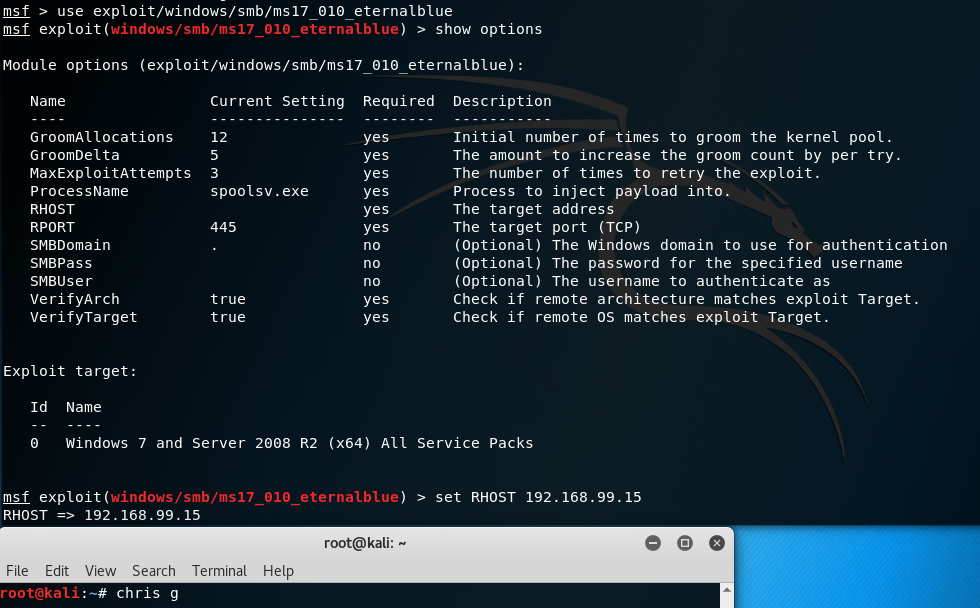


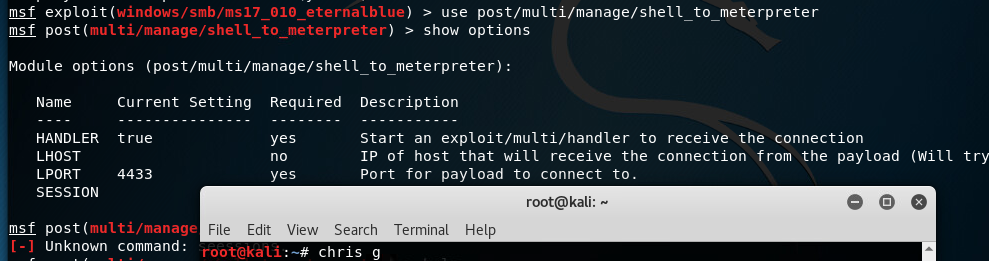
1. Use an exploit method or tool, such as Metasploit, to compromise one of the targets. Explain how you figured out how to do this exploit *8 points*

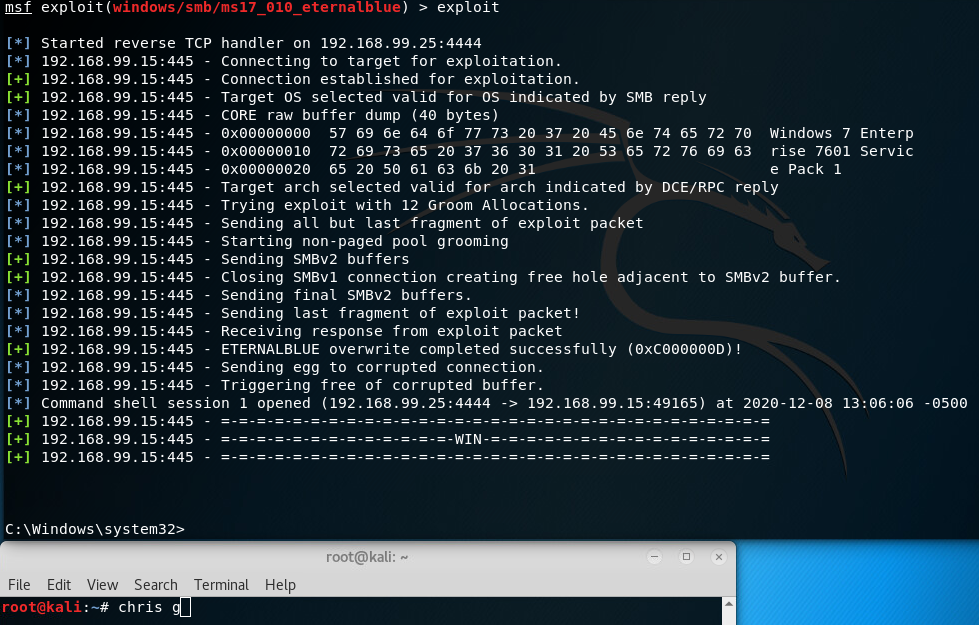
I used the eternalblue exploit from the metasploit db, meant for windows 7 smb servers to execute the default payload (reverse\_tcp\_shell). After getting the shell I used a post exploitation module to elevate the shell to a meterpreter,, and moved the meterpreter shell into a more stable process to continue with the post exploitation stuff.

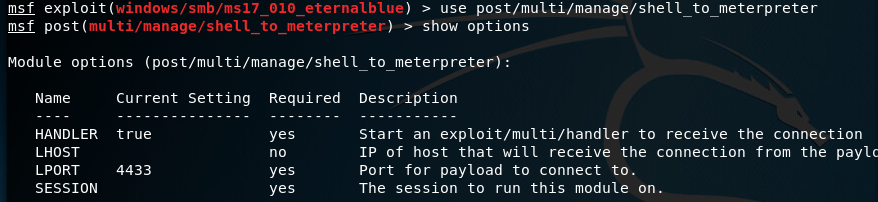
I figured out how to do this during one of the early labs, after discovering the vulnerability in a scan report, it was trial and error getting the payload to work… never occurred to me that msf had a default payload until hours later.

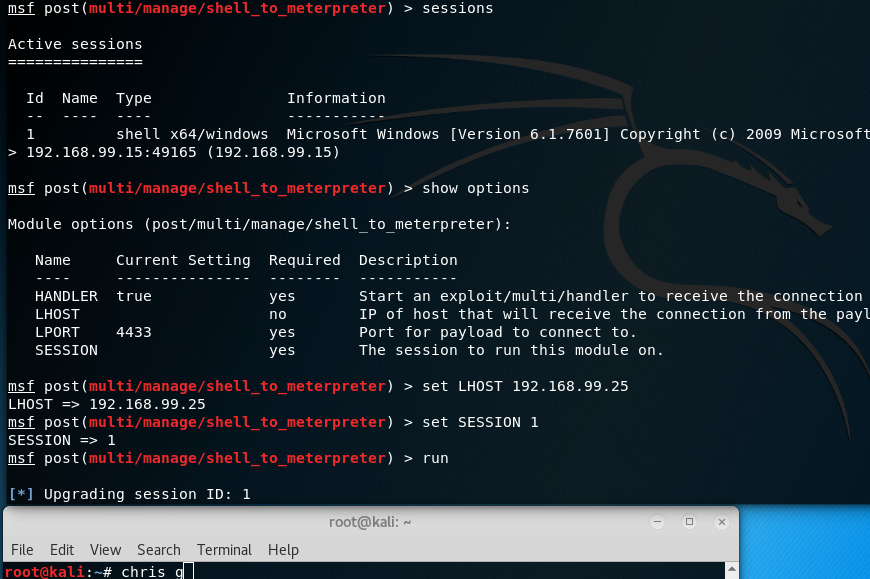
In 2020.3 it displays the payload when calling “set payload” without args, I wasn’t sure how to display that selection using another means but I don’t imagine it’s a major issue.

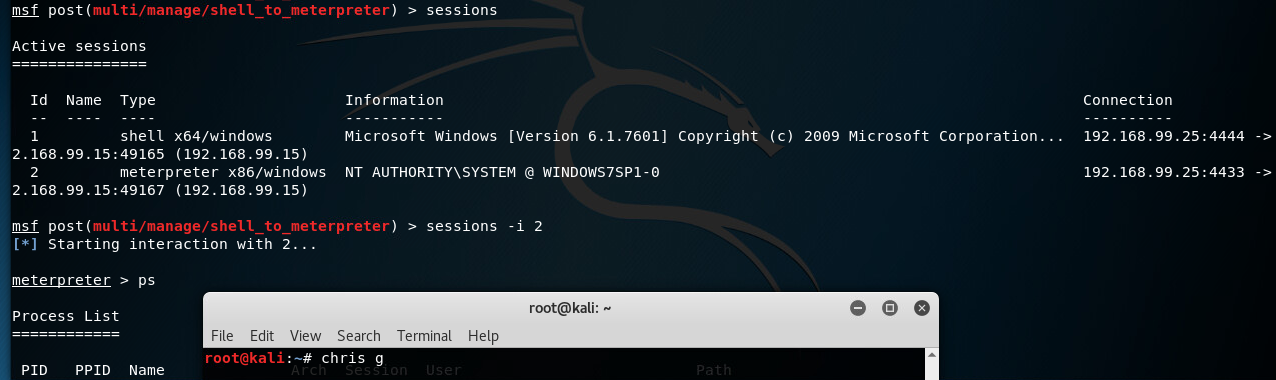






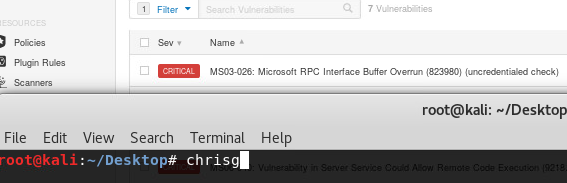




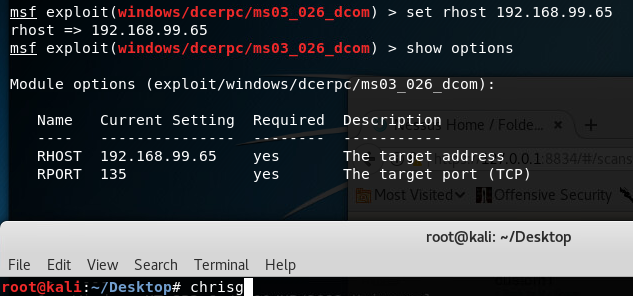


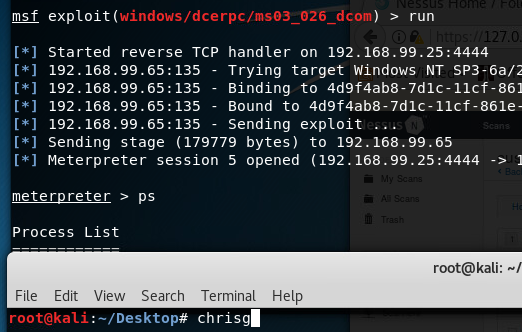
1. Gain entry into the other target using an exploitation method or tool, such as Metasploit. Explain why you selected this method. *8 points*

192.168.99.65: eternalblue has failed me on this machine. :,(

I found this exploit by filtering the results in nessus to display exploits available in the metasploit framework, and looking only at the remaining machine. I tried everything starting from the bottom, the top one was the one that did it.

Identified the corresponding module in Metasploit, and it popped a meterpreter.



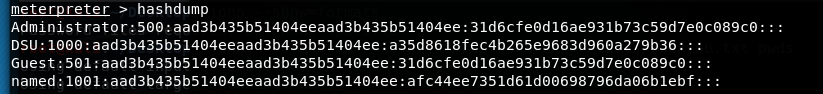


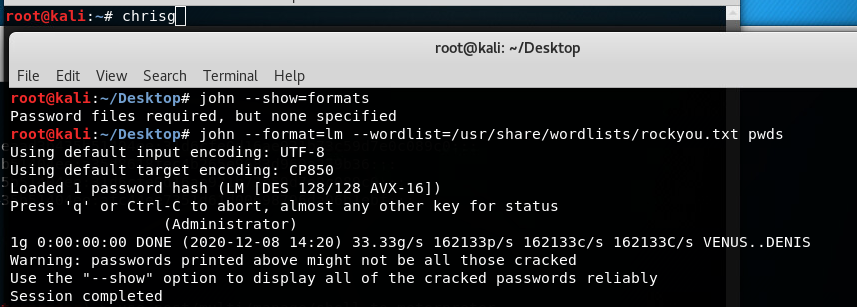
1. Perform a hashdump and crack the passwords for one machine. *6 points*

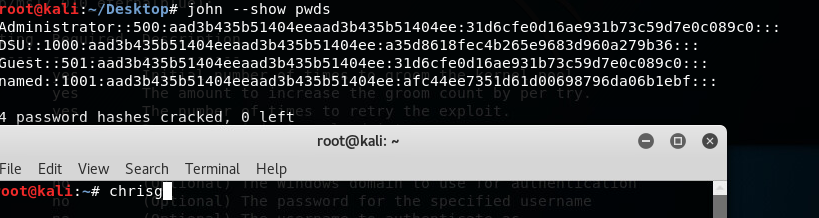
Possible ways to do this include but are not limited to the following:

* + Do this by using **hashdump** inside Meterpreter.
  + Use John or other tool to crack the password

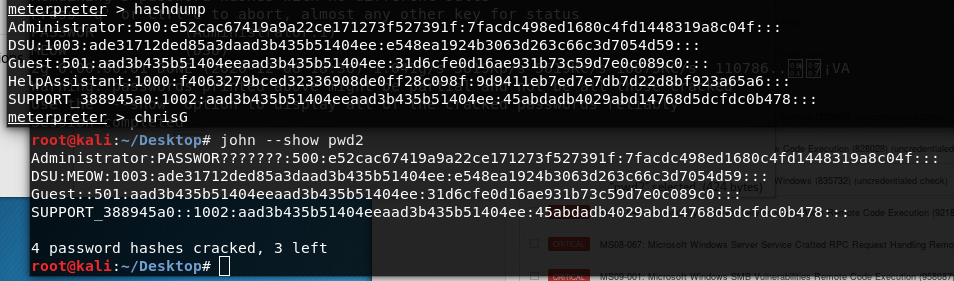
From 192.168.99.15



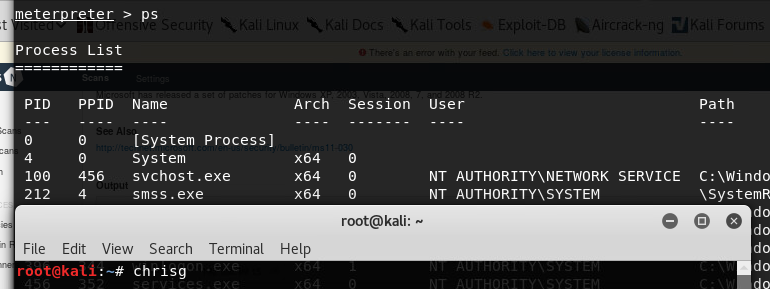


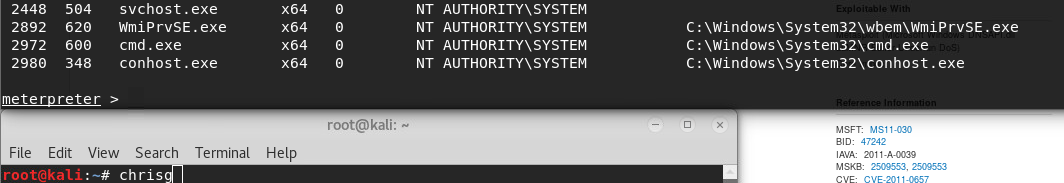


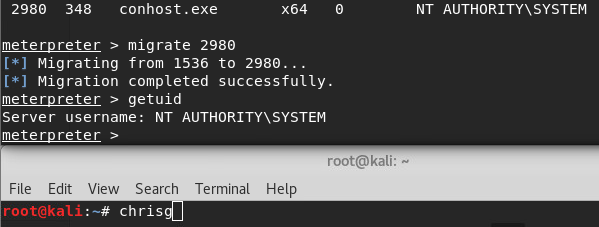
All passwords for …99.15 are blank, “aad3b43…” etc. **Passwords for …99.65:**

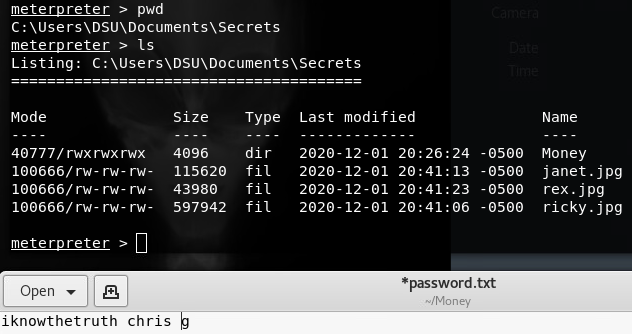
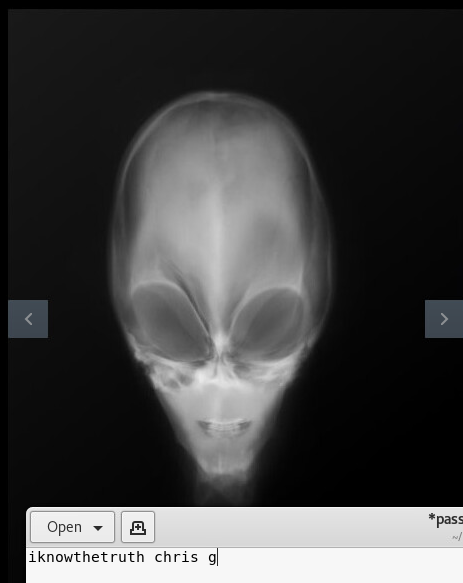


1. Use Meterpreter to view available processes and migrate to one with system level privileges. Show that your have system level privs. *6 points*

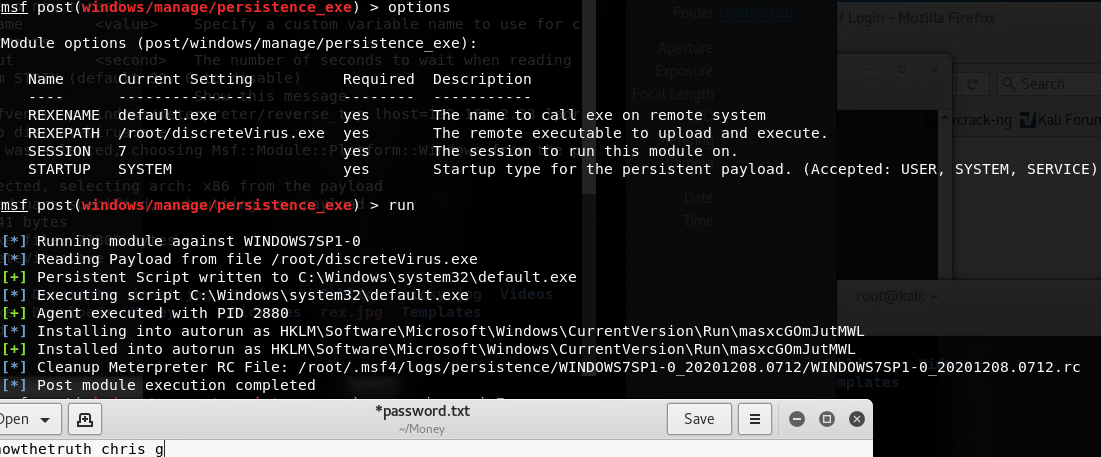


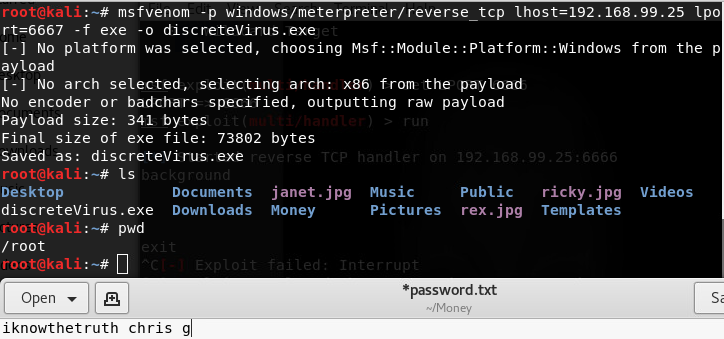




1. Uncle Craig has a very important X-ray on one of the machines, and your client – who is his employer – has asked you to find and retrieve it from his work machine, which is one of the two Windows machines. (He uses both.) What does the X-ray show, and what is its significance? Include screenshot of the X-ray. Once you do this, be sure to provide a couple screenshots, showing how you obtained Uncle Craig’s X-ray. *6 points.*

I used the download command to download his money, but I found something much more valuable than money. Uncle Craig is an Alien. Or he is an alien murderer, as he confesses to possessing the body one way or another.

1. Establish persistence in one of your targets. There are many ways you could achieve this. Include screenshots **and** explain how you achieved this. Restart your target and show you still have access. *8 points*



***Screenshot Requirements***

Your username must be visible. You may have your name in the background in an open .txt document or similar. If screenshots are submitted without this, there will be a 50% reduction in points. Do NOT add your name by typing it in Paint.

Screenshots should be edited to only contain the application and content requested; overly large screenshots that include extra material such as other applications, etc., will result in a reduction in available points. Screenshots must be readable. Any problems with tiny, unreadable screenshots will be resolved quickly with a 0.