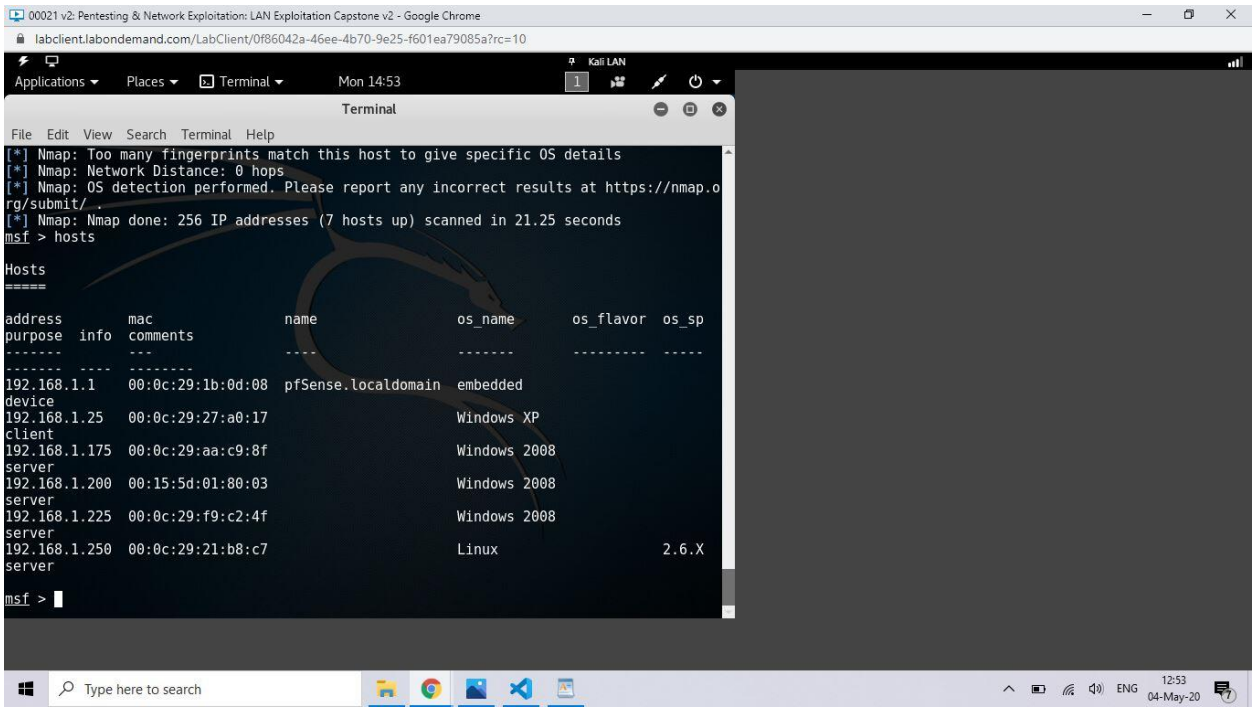
Zack Heaton
Cyber Security Bootcamp Denver University
04-05 May 2020
Homework Week 19
Penetration Testing

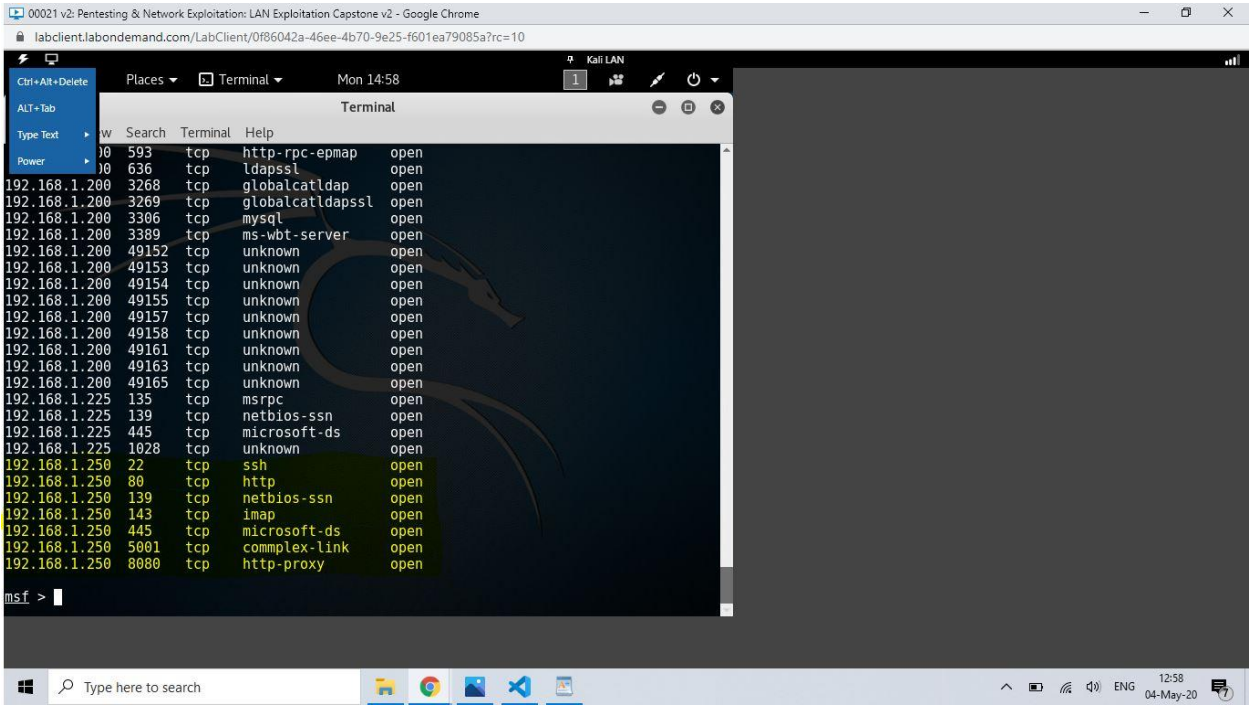
The instructions for this assignment indicate that I should provide screenshots for host discovery, verification of Scan Data, Target Host Service Enumeration, and Exploitation of a Linux Host. I have included those screenshots below.

Host Discovery



Screenshot 19-1

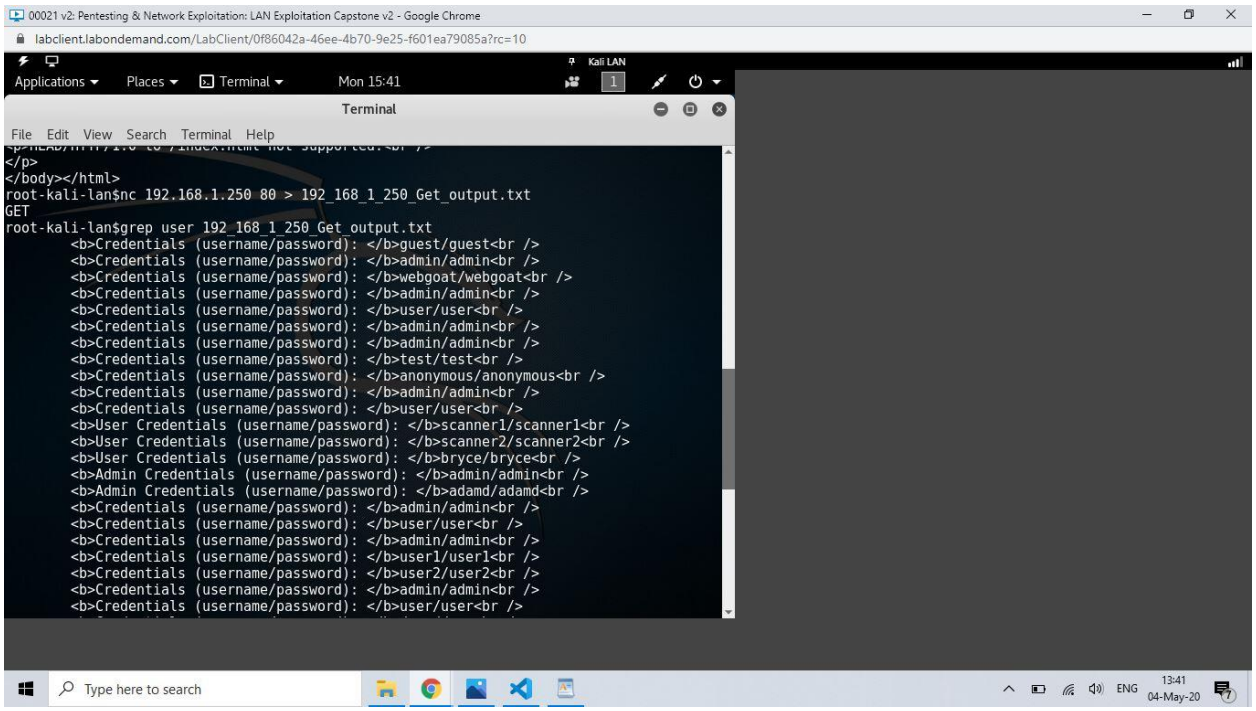
Notes: You can see that the commands up until this point got me to see all the hosts using the IP Addresses on the 192.168.1.0/24 subnetwork. Looking forward in the assignment where I will be exploiting a Linux machine I will focus my attention specifically on IP Address 192.168.1.250 because it is clearly the only Linux choice on this particular subnetwork. In order to do this I typed [services] into the msfconsole that shows the potential vulnerabilities. Those are visible in screenshot 19-2 below. One thing about 19-2 is that when I ran [services] it gave me the potential vulnerabilities for the whole subnet. In order to highlight the important parts I used snipping tool to highlight in yellow the potential vulnerabilities of 192.168.1.250. You can clearly see in the screenshot that ports 22, 80, 139, 143, 445, 5001, and 8080. They're all assigned the protocol TCP but are named different titles. That information may come into play in a later section.



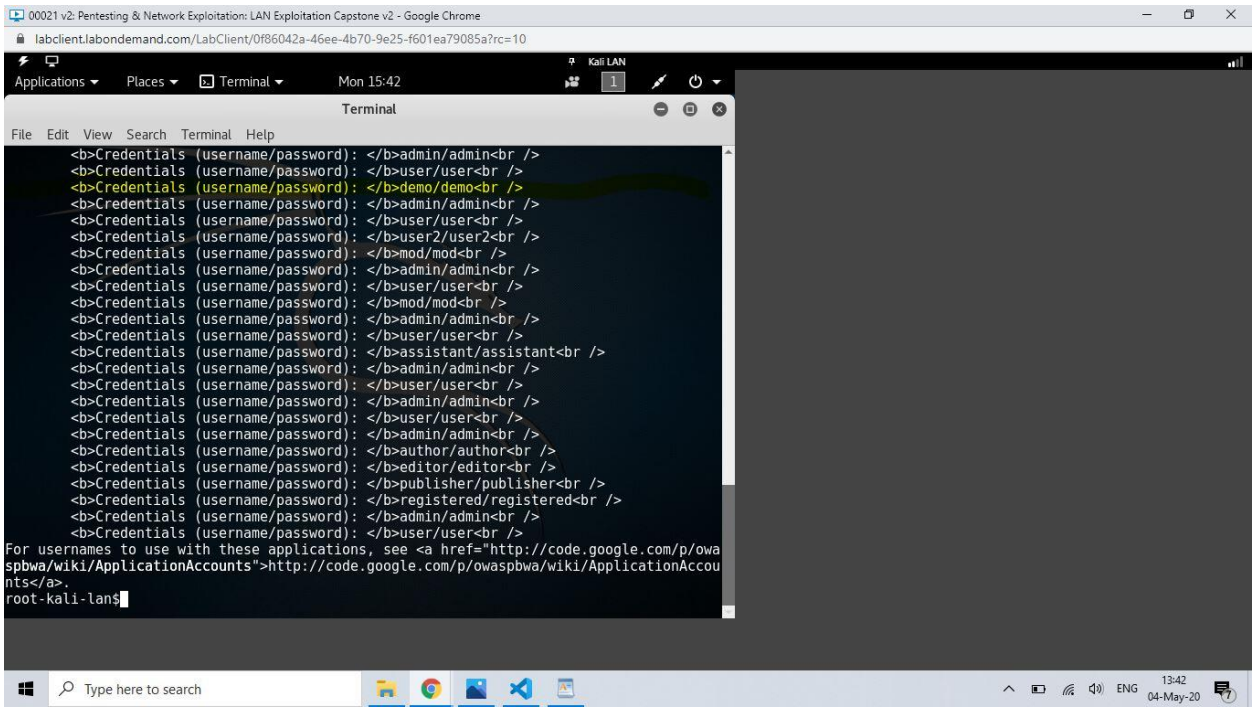
Screenshot 19-2

Verification of Scan Data

The next step for this assignment is to verify that the scan data is real. This would mean that we have to get out of Metasploit and actually probe some of the information that we got. The directions more or less helped out by indicated how and where but the rest was on us. In Screenshot 19-2 we can see that IMAP port 143 is open. Using Netcat and telnet we could verify that which is what you are looking at in Screenshot 19-3,4, and 5.

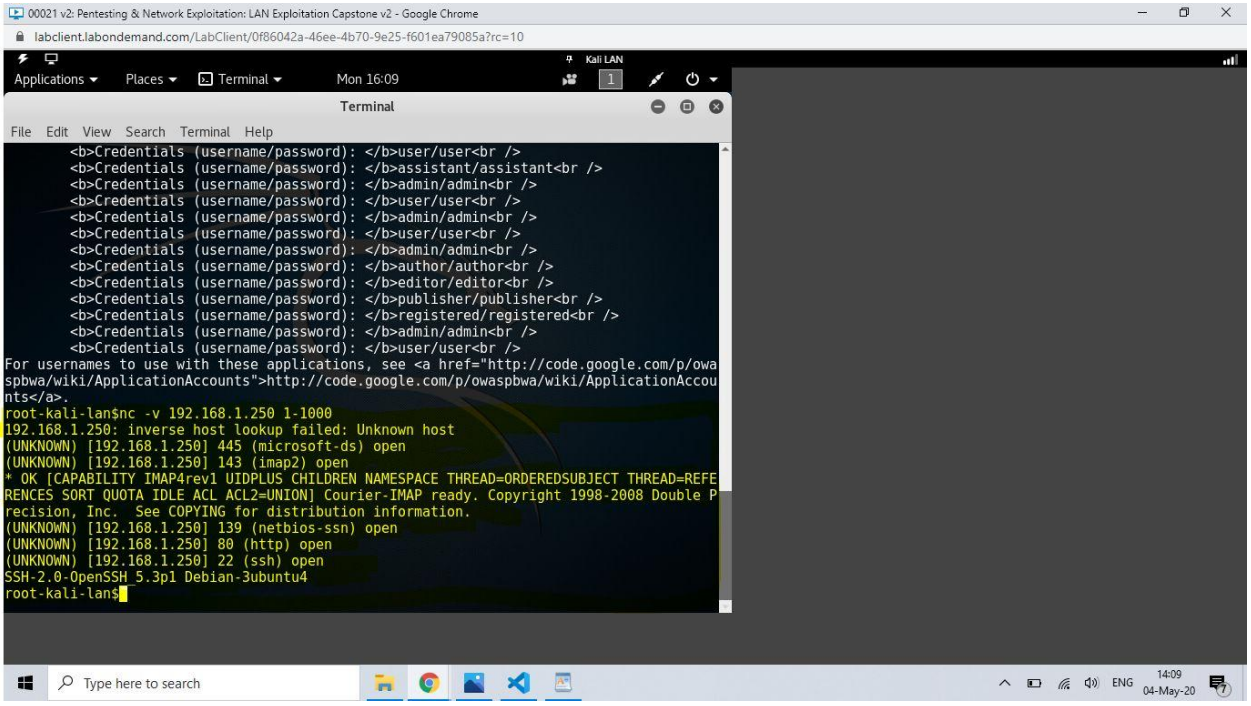


Screenshot 19-3



Screenshot 19-4

*In screenshot 19-4 the yellow line indicates the cutoff spot from 19-3. It was too big to get in one screenshot.



Screenshot 19-5

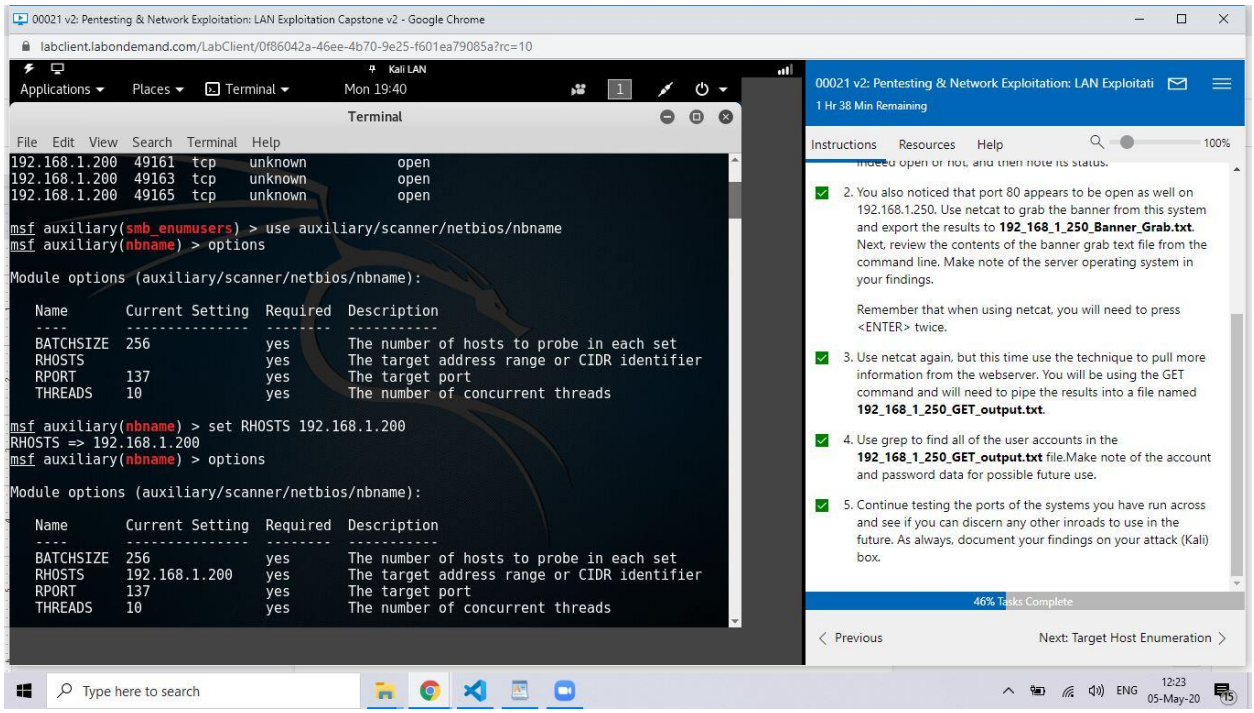
I would like to take an opportunity to explain a little further what is going on in screenshots 19-3,4,and 5. In screenshots 19-3, and 4 you can see that sending the telnet command to port 143 we were able to establish a connection. We were then able to use netcat on port 80 and output the data from out connection. Using the grep command to go through the data we were able to retrieve usernames and passwords in clear text. We could further test the vulnerability of the metasploit can from earlier by running a verbose netcat on the first 1000 ports of 192.168.1.250. This revealed what we already knew but it's now confirmed harder than Han Solo in Carbonite.

Target Host Service Enumeration

In this section we will use the confirmed information and return to metasploit to actually go in and target one of Windows devices from earlier, specifically the XP device on 192.168.1.200. This section will focus a lot more on enumerating the different ways to get information out of vulnerable systems whereas the next section is more about specifically exploiting. This section will have a lot of screenshots that explain each tactic and what it revealed. The next section based on Linux Exploitation will assume that the idea has been explained here and understood that those steps preceded the shorter section on Linux Exploitation.

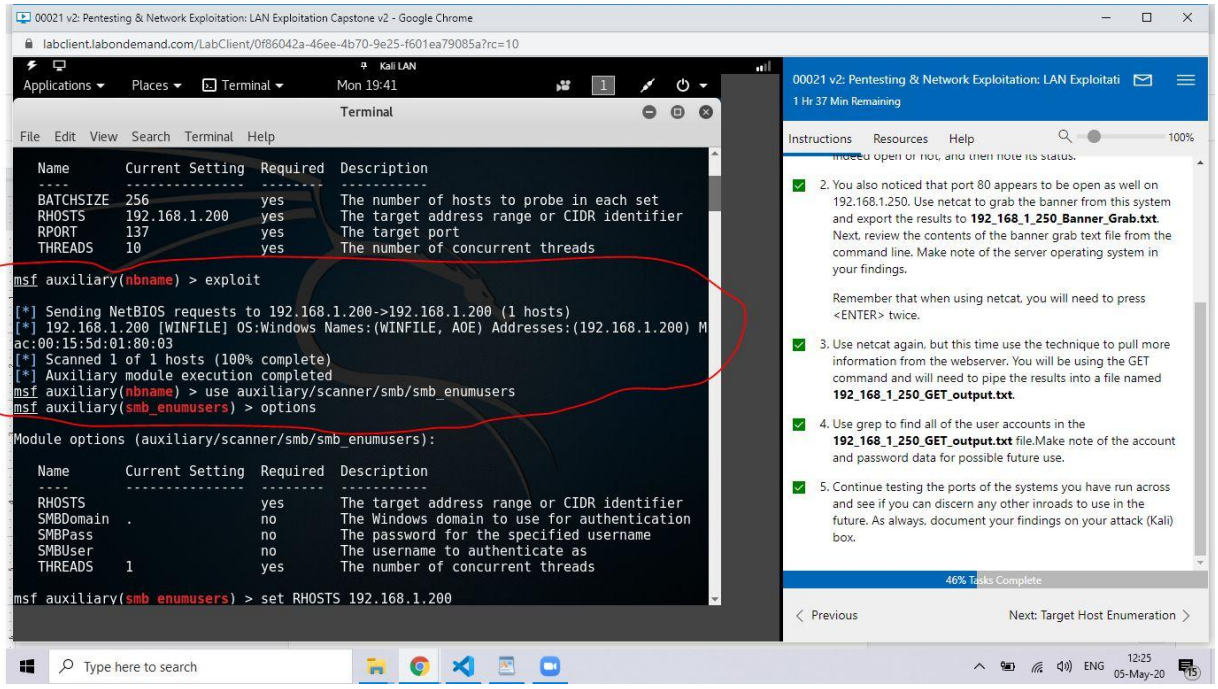
It is important to note that the way the particular exploits were chosen for this enumeration process is that the directions indicated to be looking for NetBios and SMB vulnerabilities. That information propelled the decision to probe [sbname], [smb_enumerusers], [enumshares], [smb2], and [smb_version]. In the process of setting up these exploits there are a few minor steps such as running the options command to see if the exploit is RHOST or RHOSTS. It is also helpful in order to analyze which parts of the exploit need to be set in order to successfully execute the exploit. Below in screenshot 19-6 you can see an example of running the options

command highlights what needs to be set and the actual setting of RHOSTS for this particular example. In order to save the space and confusion of extra screenshots it should be assumed that this step was performed to yield the results in future screenshots.



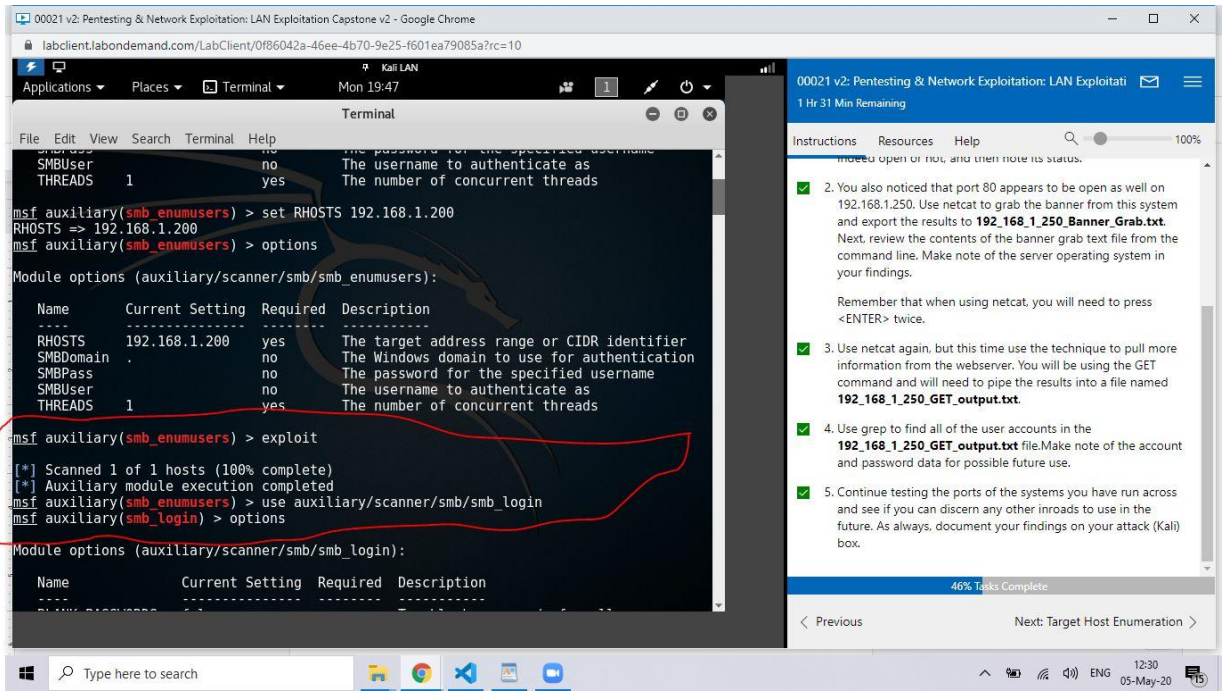
Screenshot 19-6

SBNAME - Running this exploit provided us some information about the host. You can see that in screenshot 19-7.



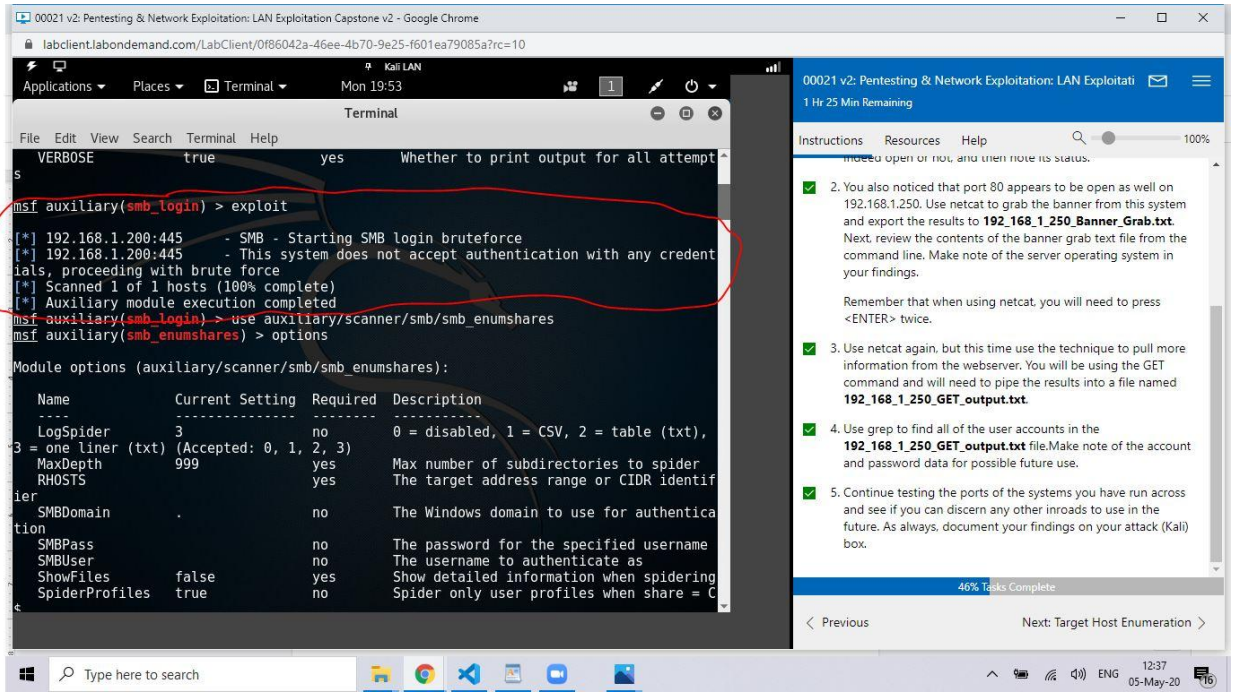
Screenshot 19-7

SMB_ENUMERUSERS - This exploit confirmed the connection but it did not provide us with any user information. This is shown in screenshot 19-8.



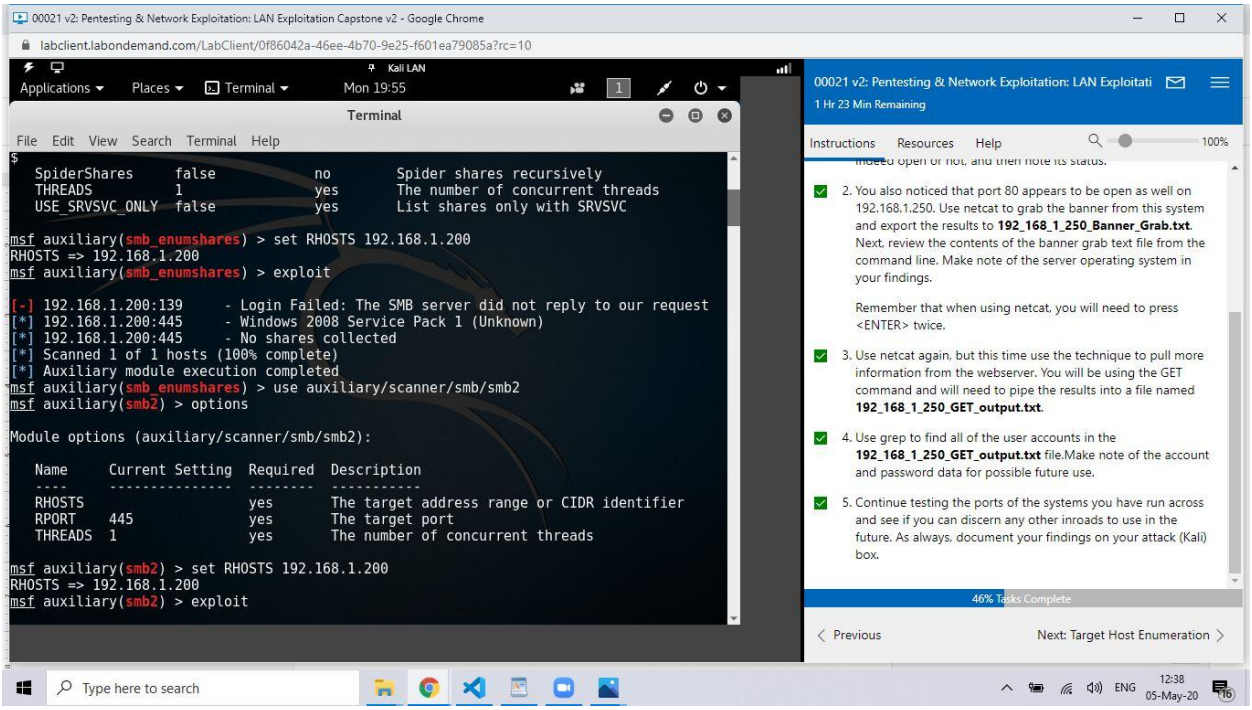
Screenshot 19-8

SMB_LOGIN - This told us that the attack was successful but that there were no credentials that could be brute forced. This simply tells us that there is a way and to keep going. This is shown in screenshot 19-9.



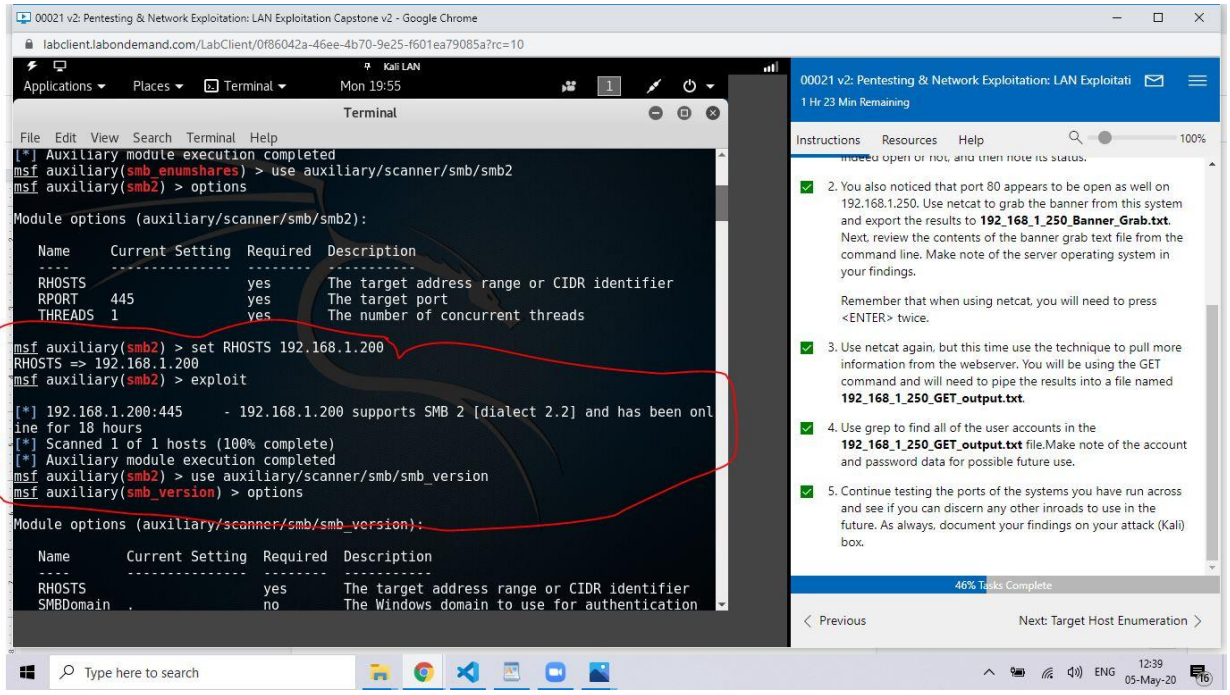
Screenshot 19-9

ENUMSHARES - This didn't give us anything from the smb server but it did provide the operating system and operating service pack which was Windows XP 2008 Service Pack 1. This is shown in screenshot 19-10.



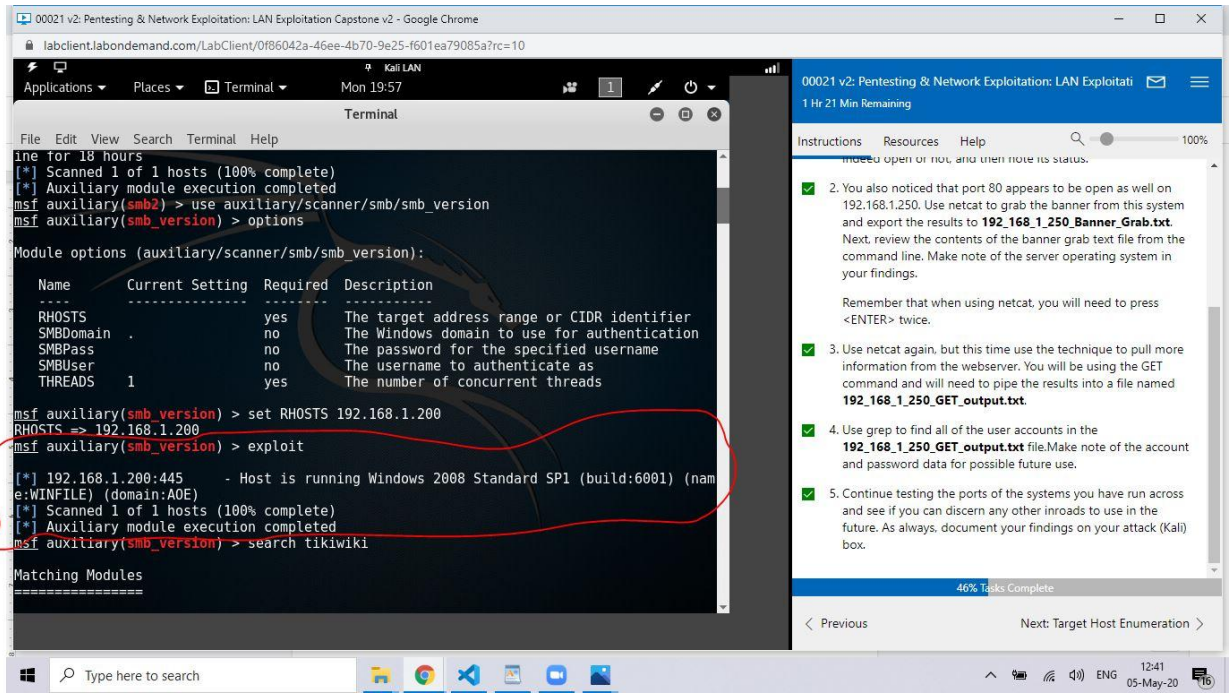
Screenshot 19-10

SMB2 - This provided some excellent information that the server is active and has been in use for the last 18 hours. In screenshot 19-11 below you can see the output received from this exploit.



Screenshot 19-11

SMB_VERSION - This added information to our what we know about the operating system and included that the service pack one is actually build number 6001. It also told us that the server has a domain of AOE and it is named WINFILE. This can all be seen in screenshot 19-12.



Screenshot 19-12

There are very possibly and likely more exploits that could be used on this Windows XP machine and more particularly the smb server. We could continue to enumerate and make this list longer but we have a lot of information. In order to continue the assignment there is a provided summary of the information discovered below and gears will be switched to exploiting a linux host as the assignment demands.

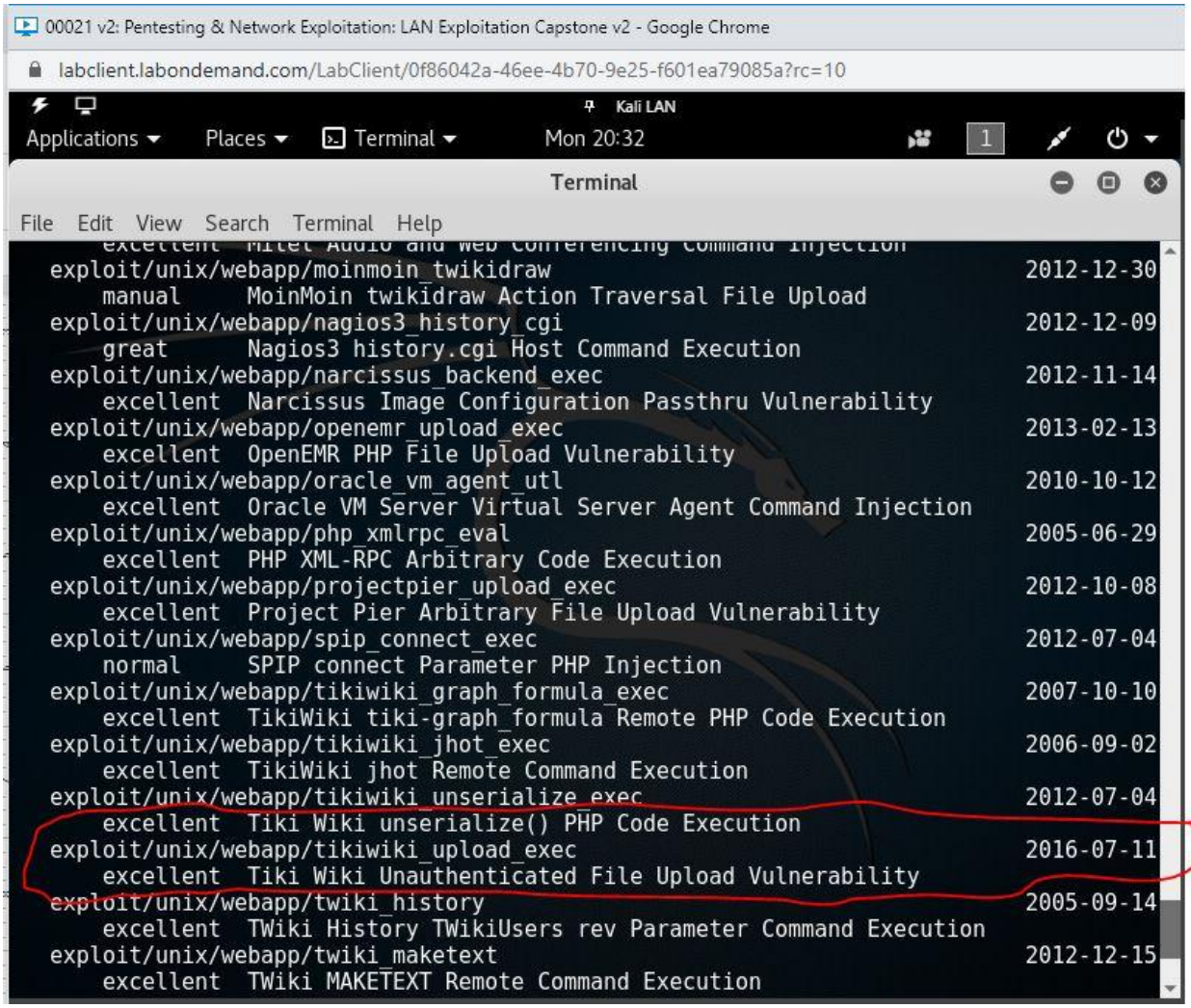
Operating System: Windows XP Service Pack One Build Number 6001
Domain - AOE
Name of Machine - WINFILE
Samba Server - Yes, 3.4.7
Support SMB? - Yes, SMB2
Vulnerabilities/Protections: System does not accept authentication with any credentials (no brute force).

Exploitation of a Linux Host

In the above section the process of enumeration is laid out as plain as possible. In this section a few of those steps will be glossed over here but there were enumeration steps and investigative actions not mentioned here. The reasoning behind that is because to include them would put the screenshots in the thirties and this makes the report simply more clean. Those details would be available upon request if needed.

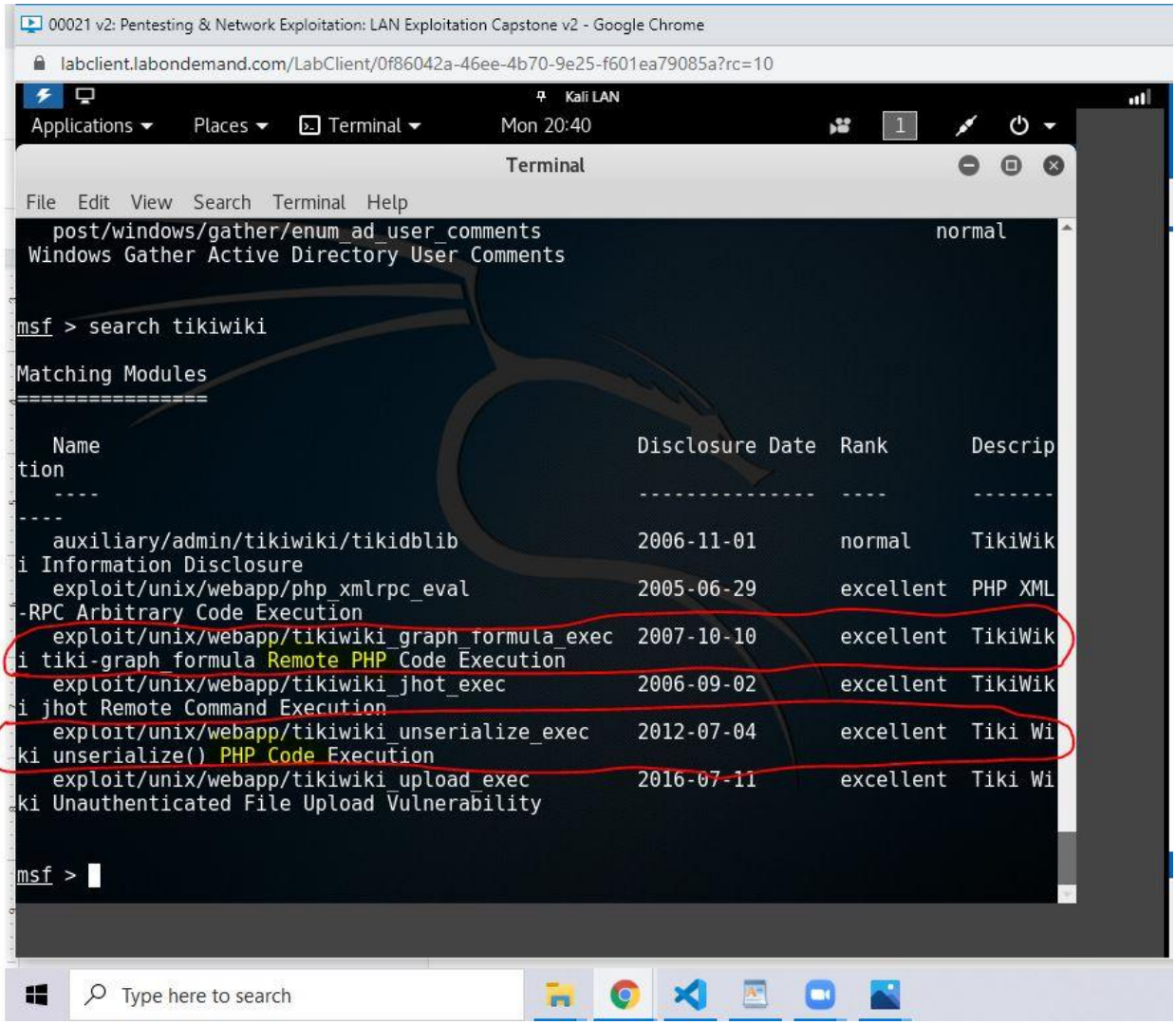
The directions indicated that we should be looking for a “specific wiki and php exploit”. The general idea of finding that would be to use the [search] function with specific criteria. There were a few different steps but the first one that yielded worthy results was to type in [search linux wiki]. The search function is operating on all the machines on the subnet and limiting the results to Linux helped to filter some of the output. That said, the output was still quite a lot of information and needed to be sorted. A lot of analysis went into that but one of the attempts was the idea of analyzing the date in which the exploits were made. One of the most recent exploits was created on 11 July 2016 which is not that old at all and very new compared to the others.

That particular exploit had the tag “PHP” in its name and also referred to a wiki called “TikiWiki”. The particular result in the data is shown below in screenshot 19-13.



Screenshot 19-13

After discovering the name Tiki Wiki there were some other searches and enumeration steps. The best result was when all letters were left lowercase and combined into one word. This yielded the result in screenshot 19-4 which is on the next page.

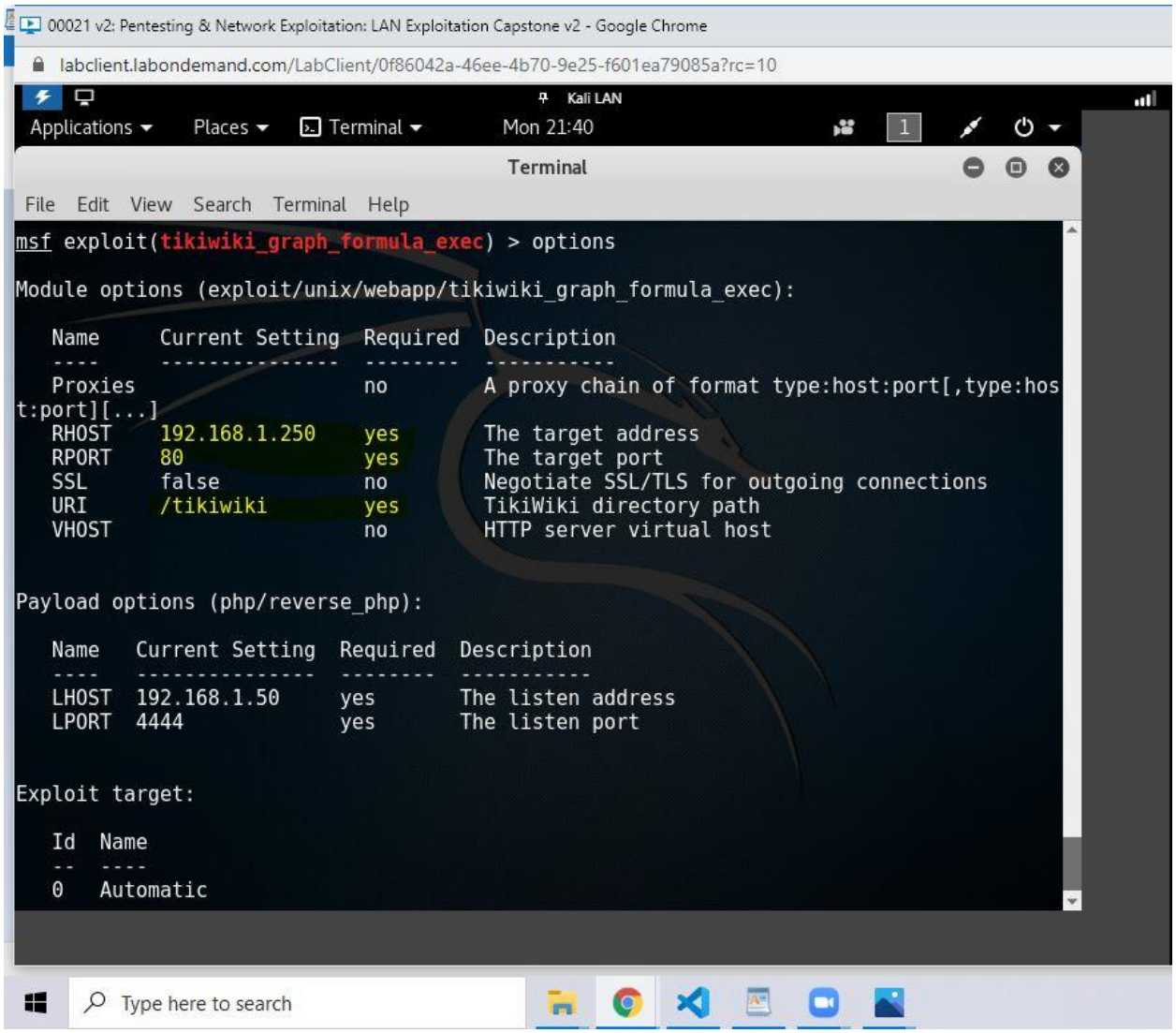


Screenshot 19-14

The results of the search for [tikiwiki] gave a few exploits that may/may not work but the list was certainly starting to filter down to a potential winner. A strange piece that there is no explanation for at this time is that the original PHP exploit that led to this search was not on the final list. There is one made on 11 July 2016 but it is not the same as the earlier one.

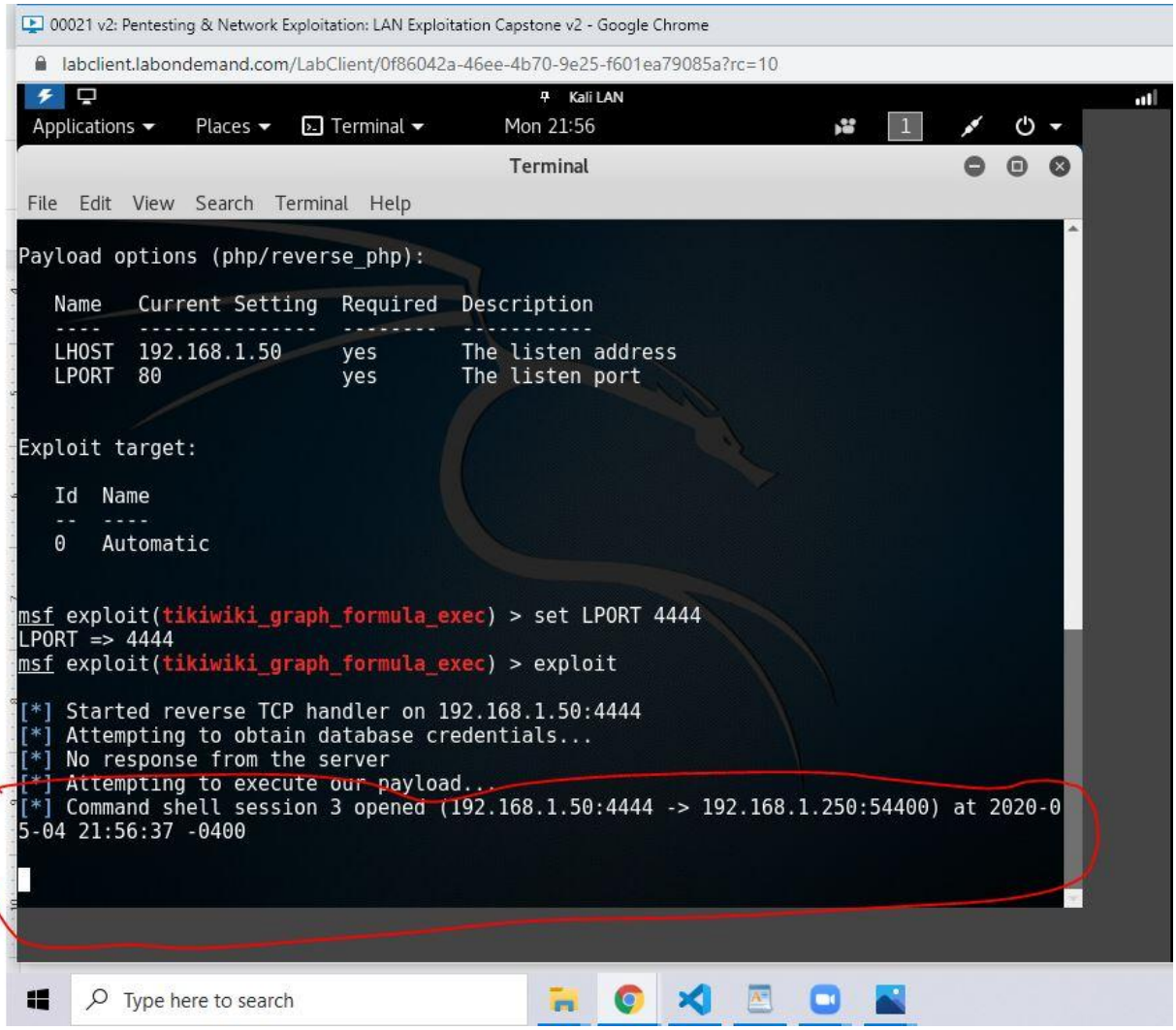
That was of little consequence. It is clear in screenshot 19-14 that there were two PHP exploits for tikiwiki. They are highlighted and circled. The decision was made to use the Remote_PHP on the basis that it was first in order and because the word “remote” was in the title. This ended up either being skill or luck to which the jury has yet.to return to court.

Once that exploit was chosen the next step was similar to the enumeration above but for clarity’s sake is included here with the command [options]. All of the options were set although there was some strangeness with having to change the LPORT each time from 80 to 4444 and back in order to get the exploit to happen. Screenshot 19-15 was taken before. The next step after modifying the options would be to [exploit].

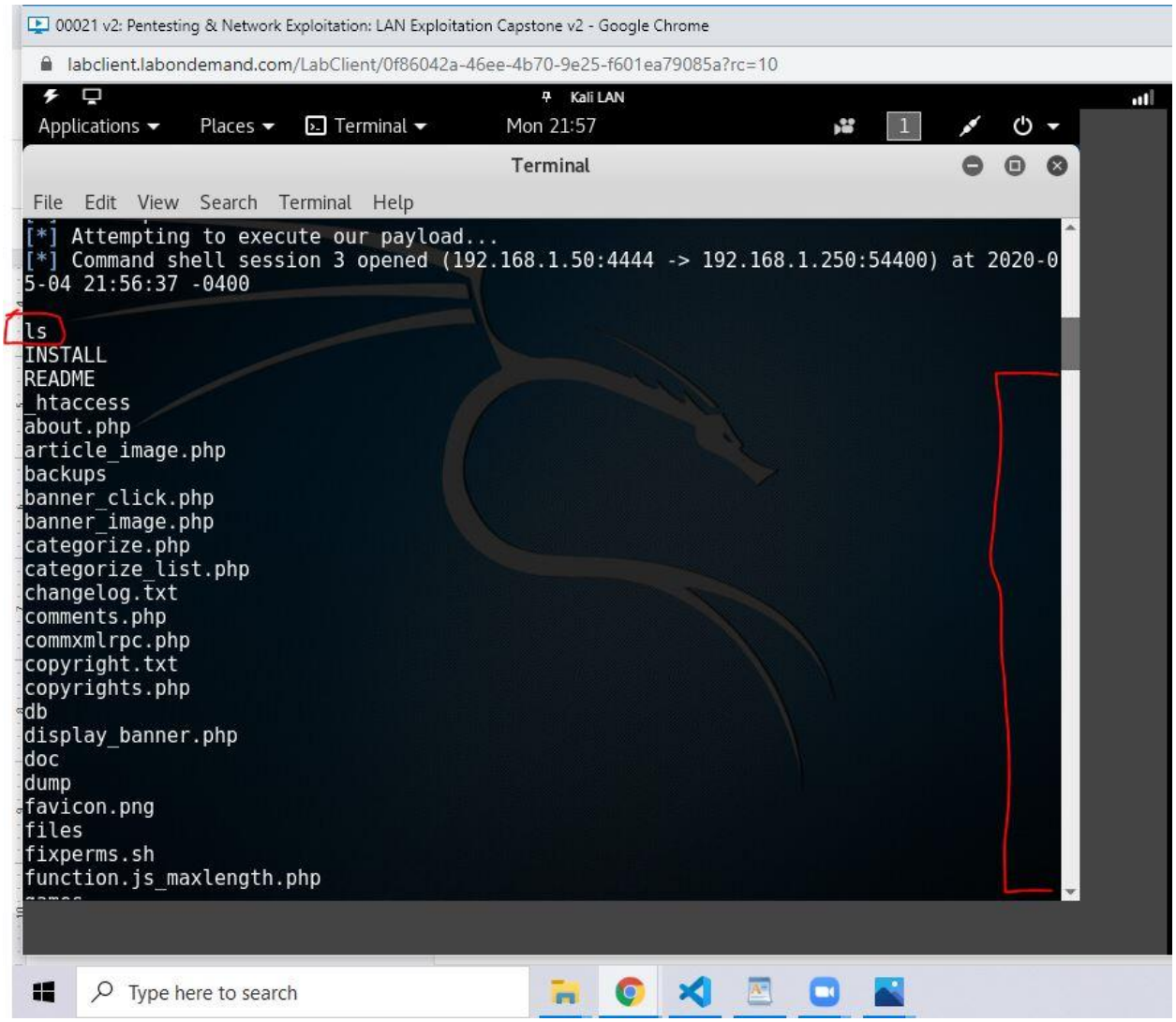


Screenshot 19-15

Once the options were set the [exploit] command was issued and a php command shell was opened up into the TikiWiki part of the Linux machine. The open command line is visible in screenshot 19-16. In order to prove that the command line not only open but also function there is also screenshot 19-17 that shows the beginning of an ls command. You can see that the list command produced a lot of directories and files by looking at the scroll bar on the right and how far up it is from the bottom after just running the command one time. Had this been more than a homework assignment my next logical step would have been to copy those files off of that machine to one of my own and then begin to analyze what data it contained.



Screenshot 19-16



Screenshot 19-17