ITT-340 PEN Testing Report Guidelines

Direction: Use this example as a guideline to build your PEN Testing Report.

Cover Page

This is the start of your document and is used to impress the customer, so be creative. Create a cover page that is unique to your select organization. Follow GCU's APA Writing Guide for the proper format of a standard cover page**.**

Document Properties

This section is used to document any revisions to the report and who performed them. Additionally, this section documents the original author of the report.

Title	Salesforce Penetration Testing
Author	Liela Pressley

Versioning Control

Version	Date	Author	Changes
01	1/21/2024	Liela Pressley	Recon via recon-ng
02	1/31/2024	Liela Pressley	Scanning via Nmap and Netcat
03	1/31/2024	Liela Pressley	Vulnerability Scanning
04	2/4/2024	LP	Applied Exploitation
05	2/6/2024	LP	Custom Payload
06	2/10/2024	LP	Website Vulnerability Assessment
07	2/16/2024	LP	SQL Injection

Disclaimer: This document and its findings is a purely fictitious penetration testing report for the purpose of learning and training. All reconnaissance, password cracking, and exploiting was done in a sandbox environment consisting of virtual machines and does not represent any actual networks or systems of any organization.

Executive Summary

Complete this section of the report after finishing all phases of the penetration test. An executive summary is a very brief summary of the entire report, focusing on the test, not the details. You will finish this section after all testing and documentation has been completed.

Table of Contents

Complete this section of the report after finishing all phases of the penetration test.

Phase Testing (Main Headings)

Directions: For each phase of the PEN testers methodology, include the following subheadings:

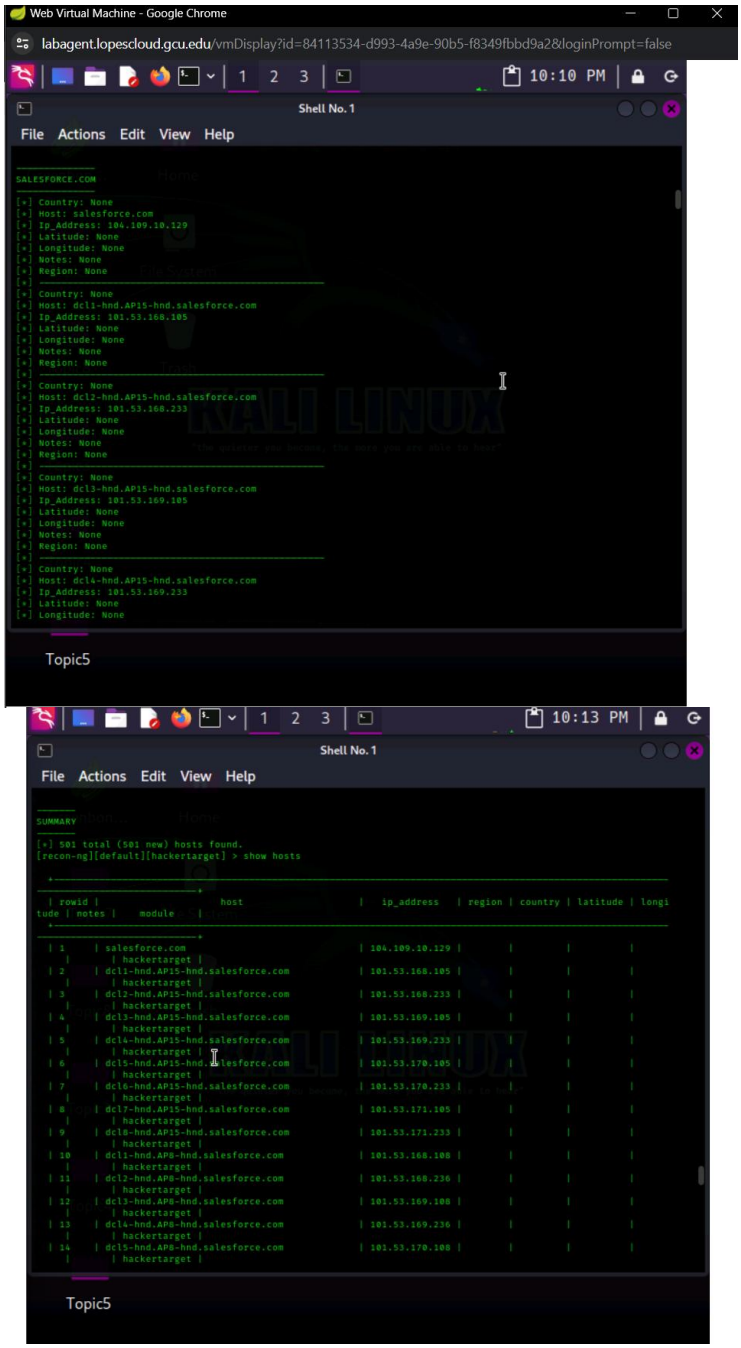
1.1 Recon Phase

Summary

This phase we utilized the recon automation tool, RECON-NG, to gather more in depth information such as IP addresses, host addresses, and PHI on major contacts from the Salesforce main office buildings.

Steps

Found over 501 IP addresses and host addresses but no other information was able to be found which is great from the pen tester perspective because they are taking extra steps to not make key infrastructure and info none viewable to the public.



Using one of the many modules, I found 7 Total contacts were found along with the town/state/country they are based in and their email address which totalled to about 25 records (due to duplicates).

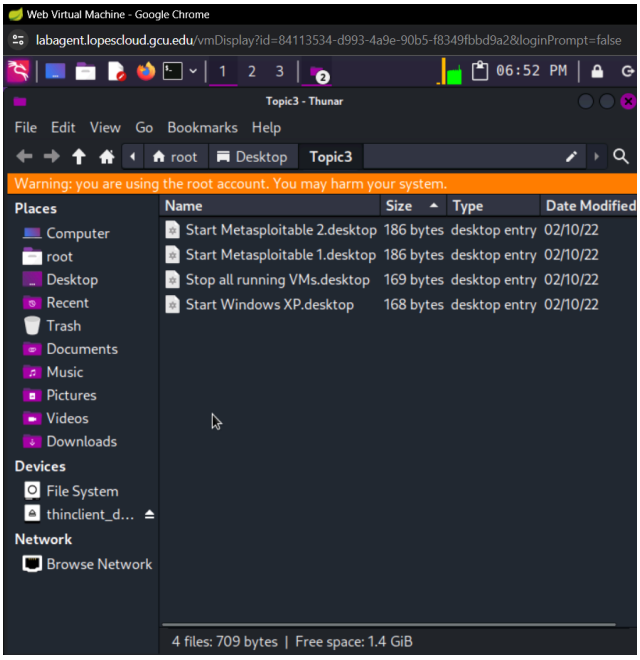
2.1 Recon Phase

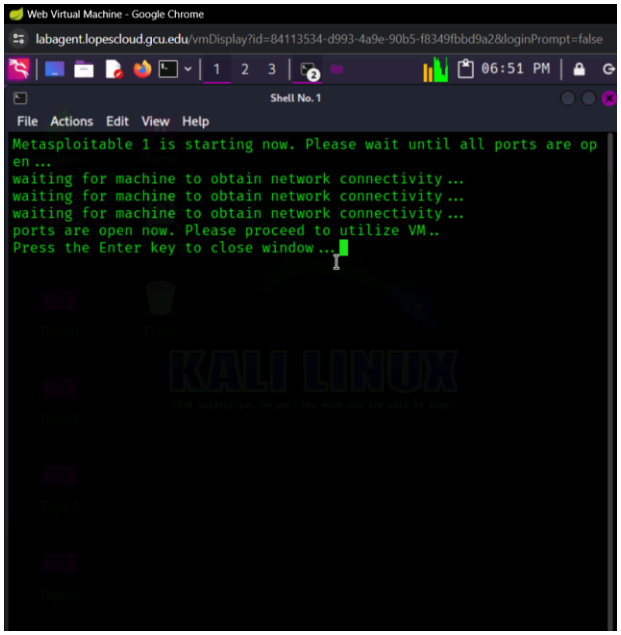
Summary

Using NMAP and netcat, we were able to find different IP addresses (virtual machines), scan for available ports that were both open and closed as well as find specific information about 3 different systems.

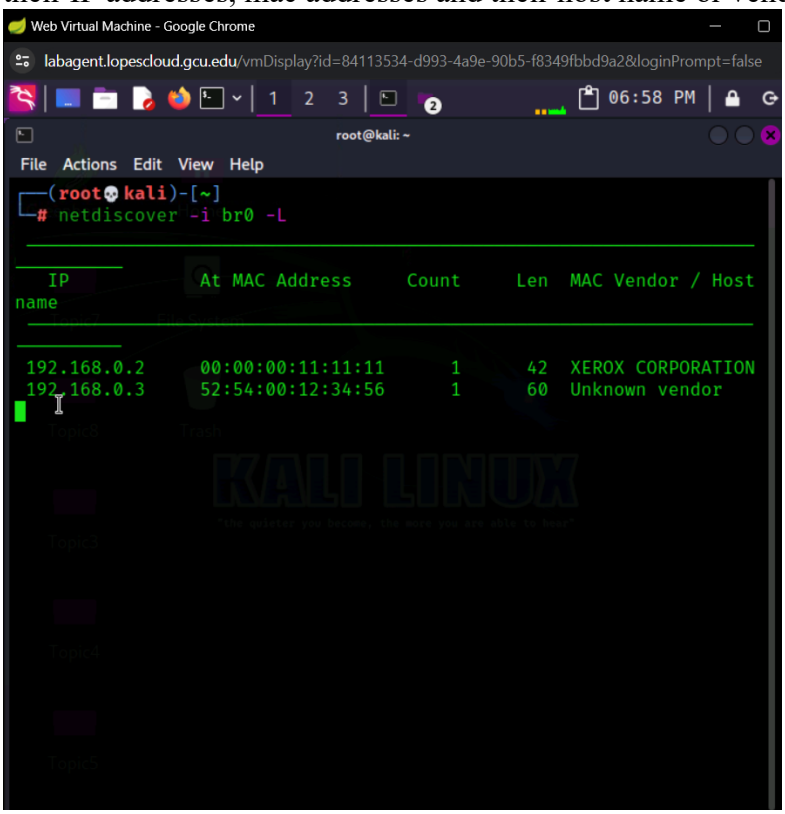
Steps

Started by launching all three VMs within my lopescloud: Metasploitable 1 and Windows



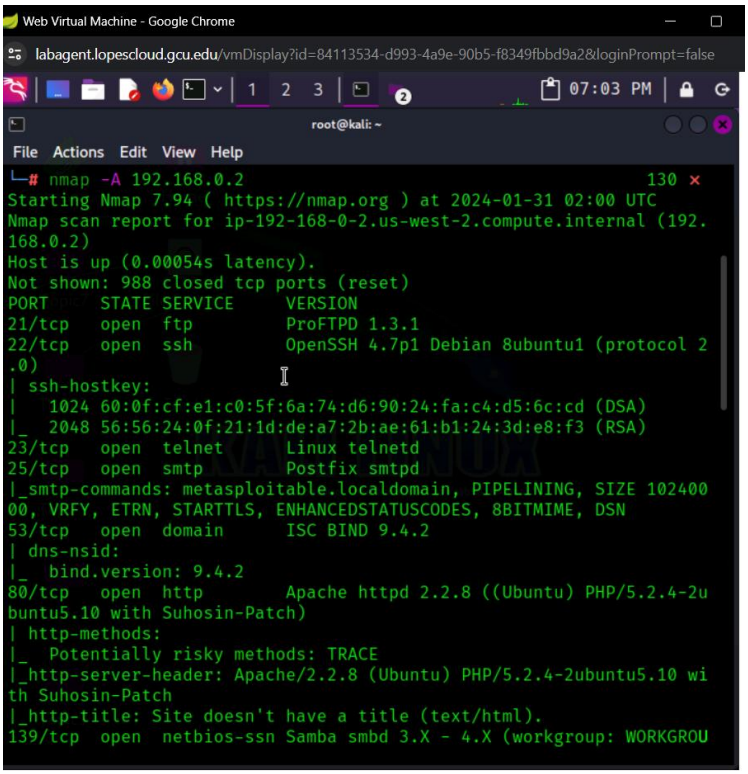


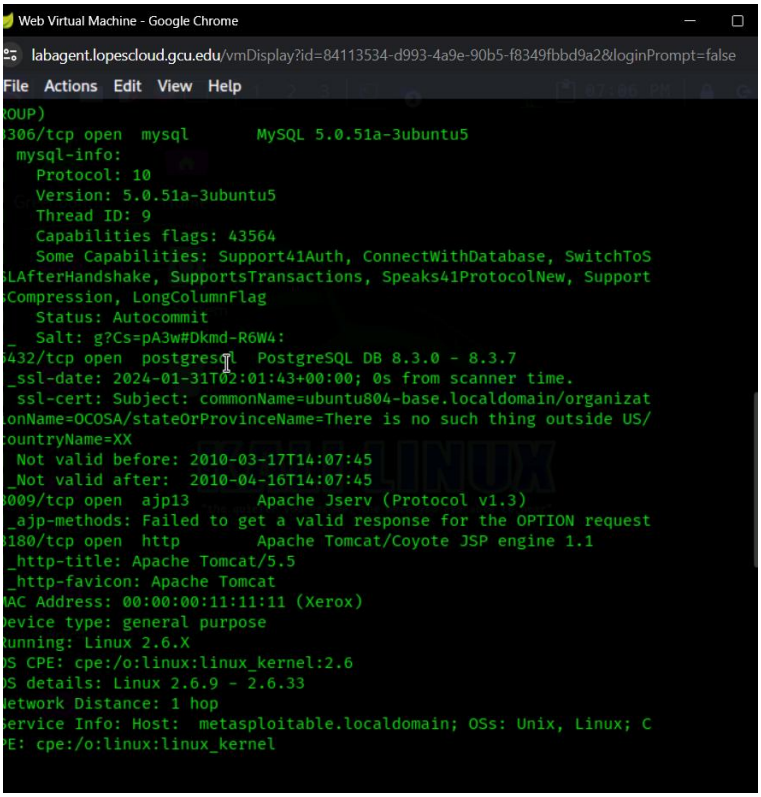
Using netdiscover I looked for different virtual machines on that were being hosted and found their IP addresses, mac addresses and their host name or vendor

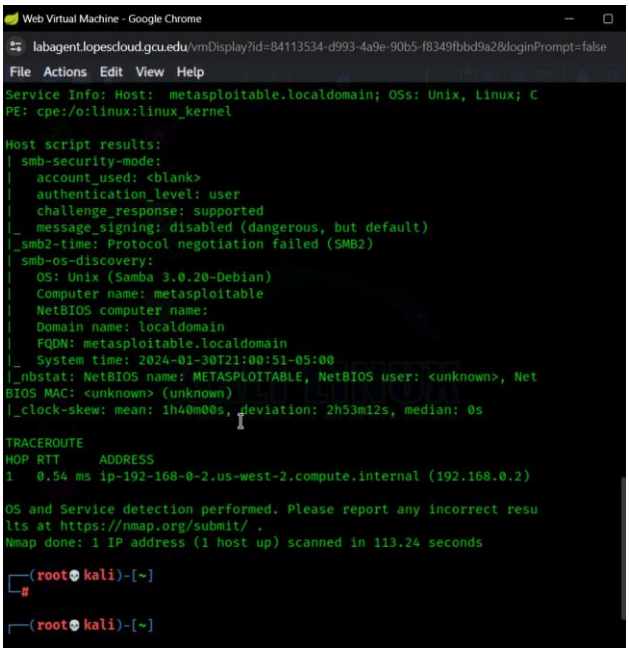


Using nmap -A does a general scan using different nmap tools at once to see what ports are open and additional info that could be grabbed.

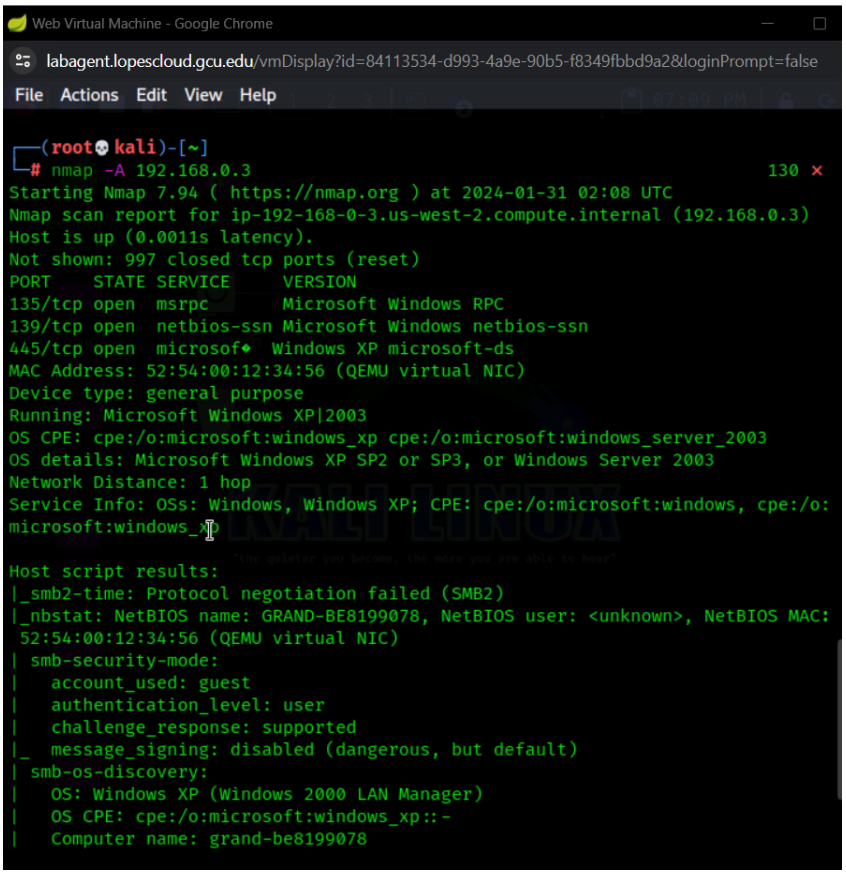
First was Metasploitable we found over 930 of the open and closed ports along with the service those ports are being used for and even the encryption keys that are being used to “secure the packets being transported”. It was able to share the OS details, how many hops to took, and even pull user account information, mac addresses, the domain, and netBIOs info. And provided a traceroute of how it arrived to the system.

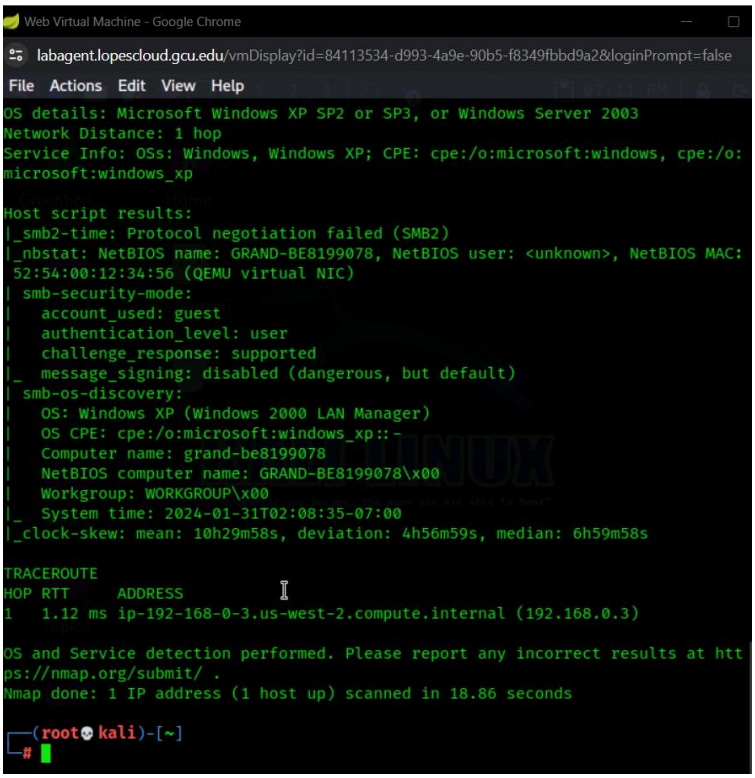




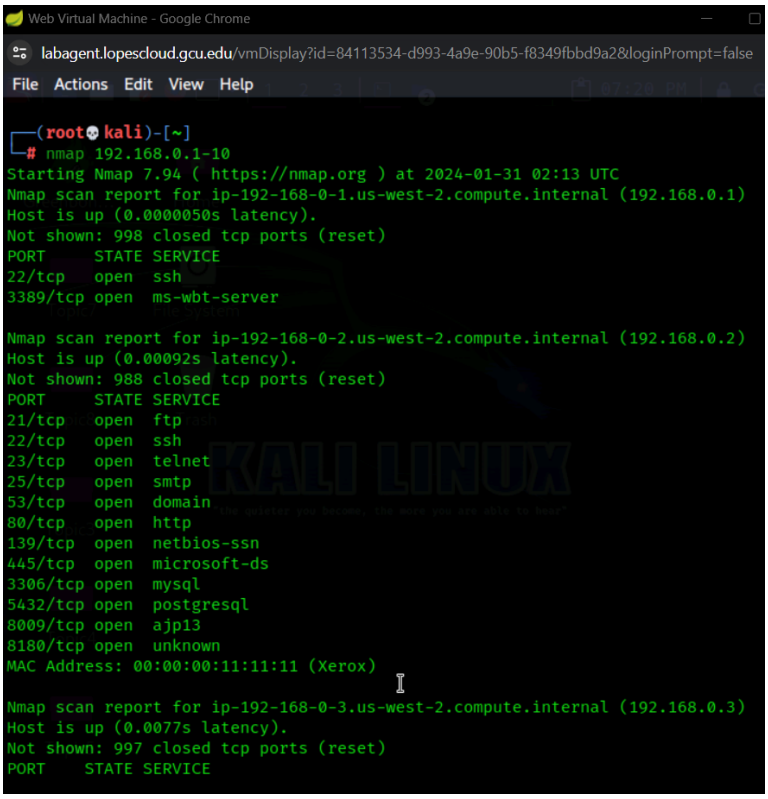


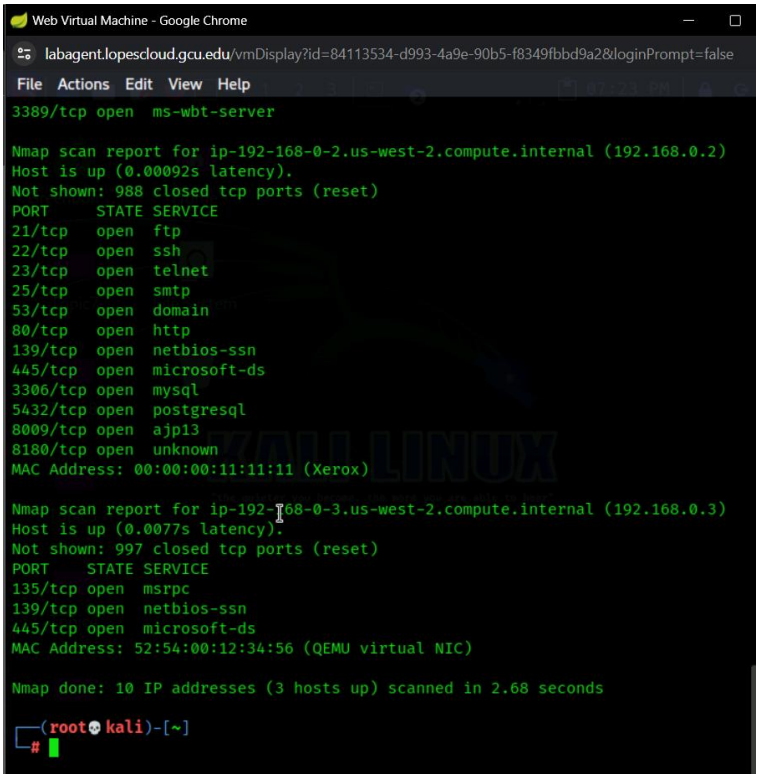
I ran the same test on the Windows VM ip address. It found 997 closed ports and 3 open ports that were tcp protocols, the MAC address, the device type, OS details, NetBIOs name, details about the user account on the system and traceroute/hops that it took in order to reach the vm.



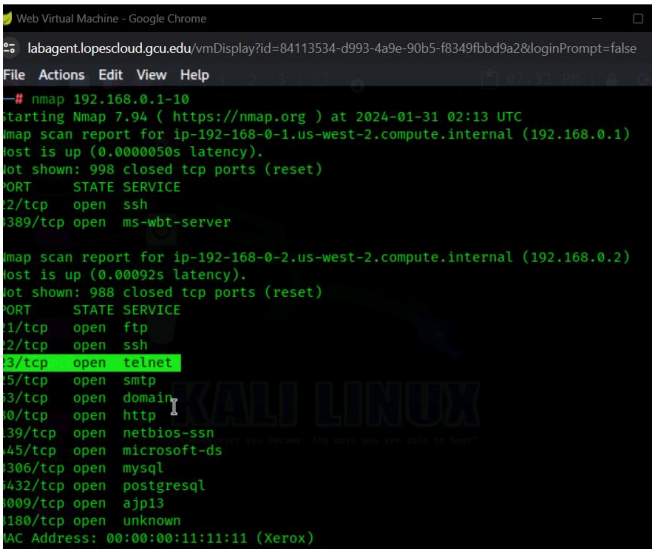


Using the command: nmap 192.168.0.1-10 I scanned for all ip addresses between 192.168.0.1 to 192.168.0.10. Nmap discovered a host with about 1000 ports (998 being closed) while 2 being open for ssh and wbt server in the ip address ending in .1 then it displaced the open ports for the ip ending in .2 and then the open ports for the ip address ending in .3. It concluded that there were 3 hosts up out of the 10 that were scanned.

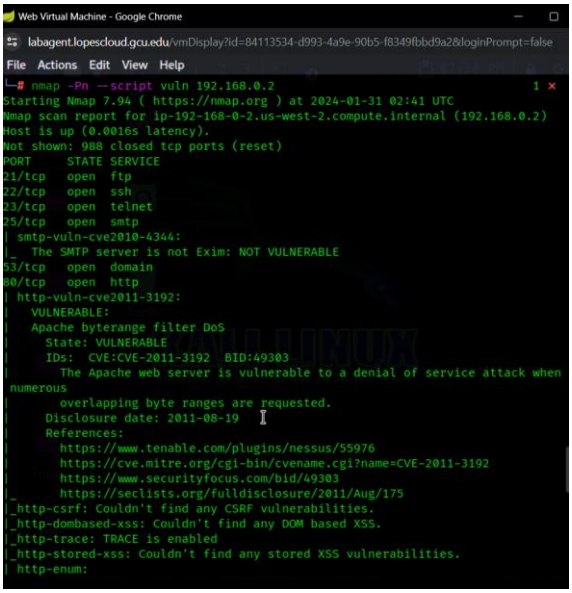


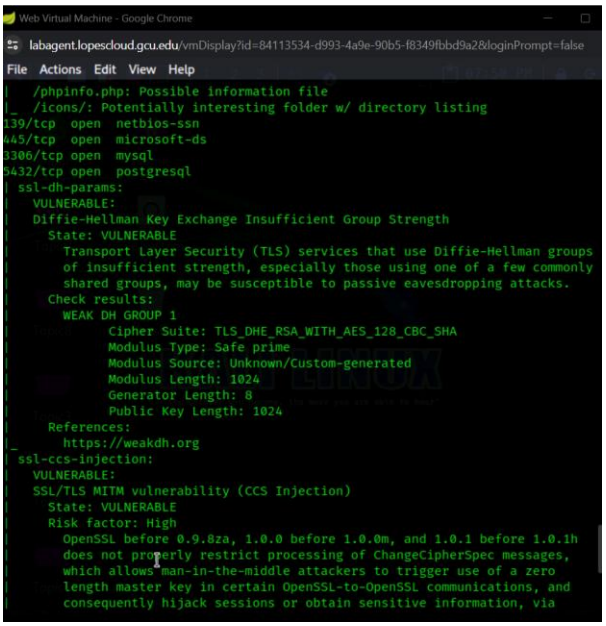


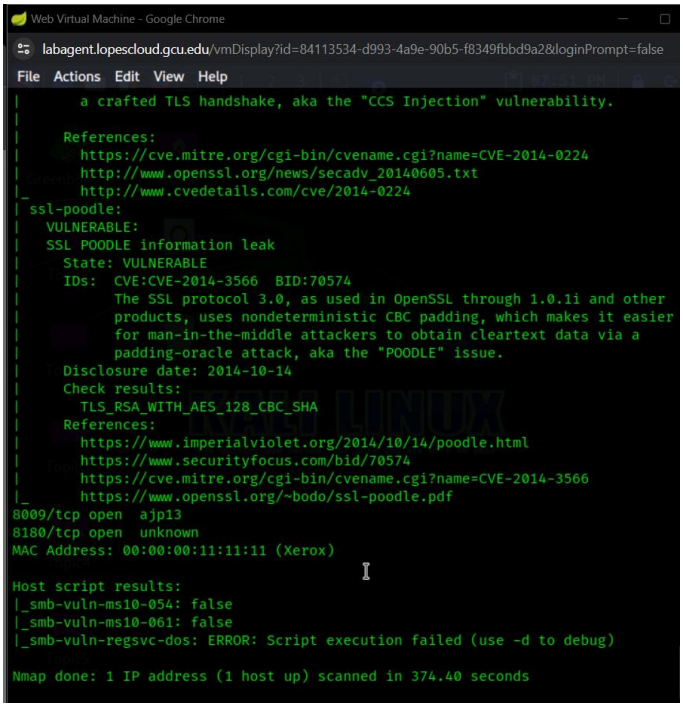
Using netcat we are going to try and see if we can access any files or information via telnet on the microsoft system on port 23 using the command nc 192.168.0.2 23



It didn't work so I moved on to a vulnerability nmap scan on metasploitable using the command: nmap -PN – script vuln 192.168.0.2





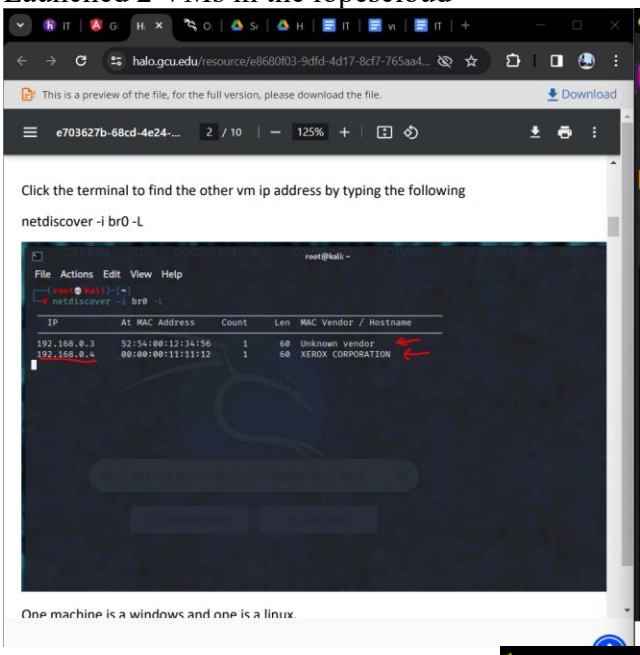


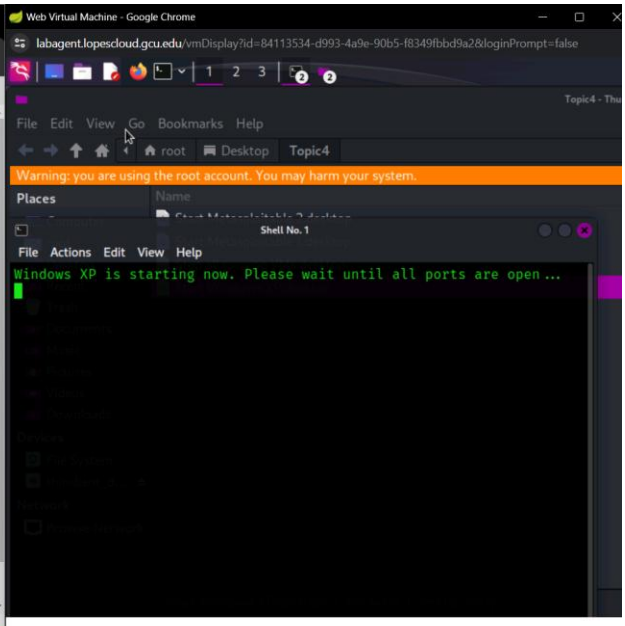
3.1 Vulnerability Scanning

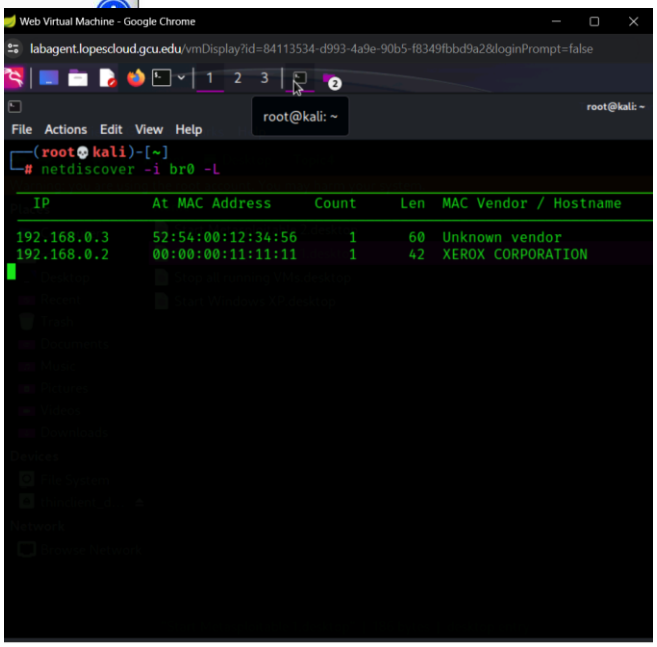
Summary

Steps

1. Launched 2 VMs in the lopescloud

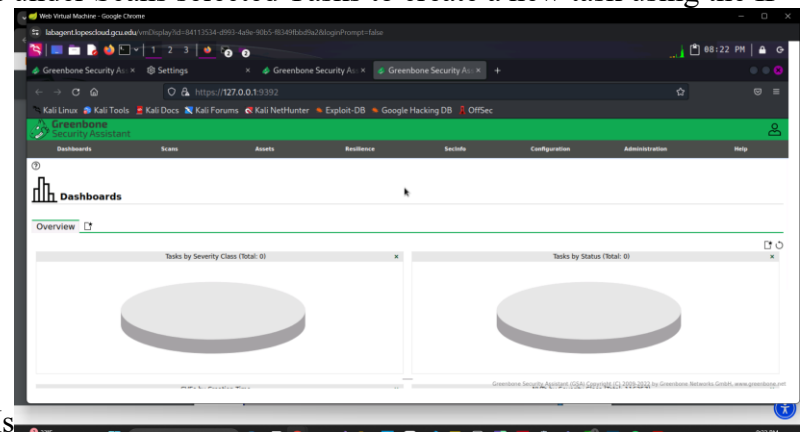




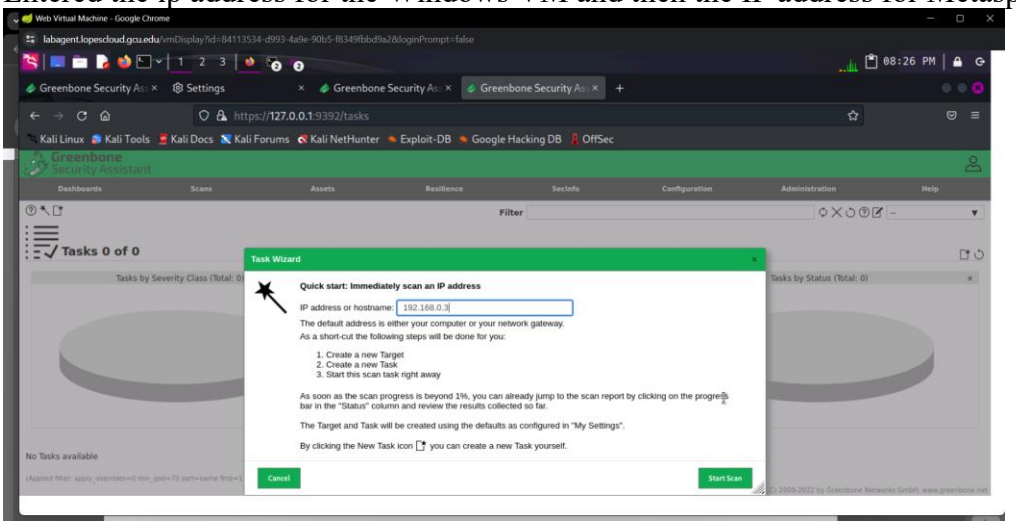


2. Used CMD to view the available VMS

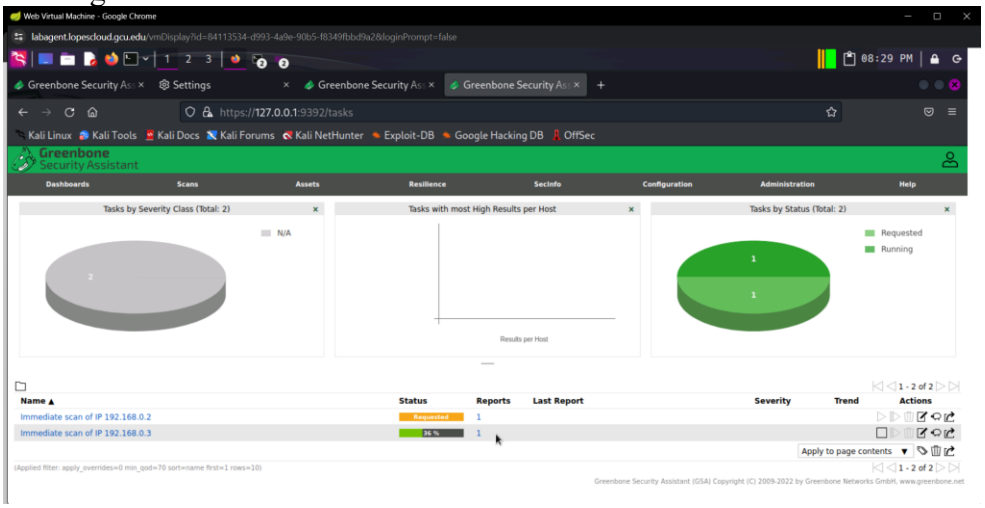
3. Opened Greenbone and under Scans selected Tasks to create a new task using the IP addresses from the VMs.



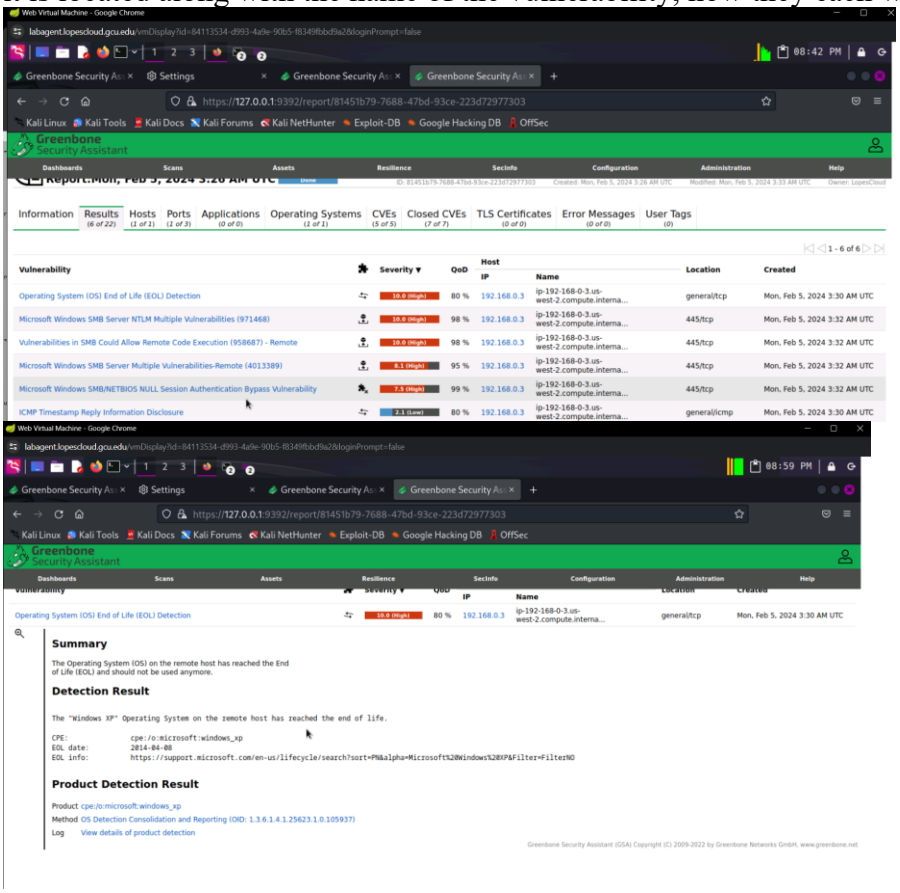
4. Entered the ip address for the Windows VM and then the IP address for Metasploitable :



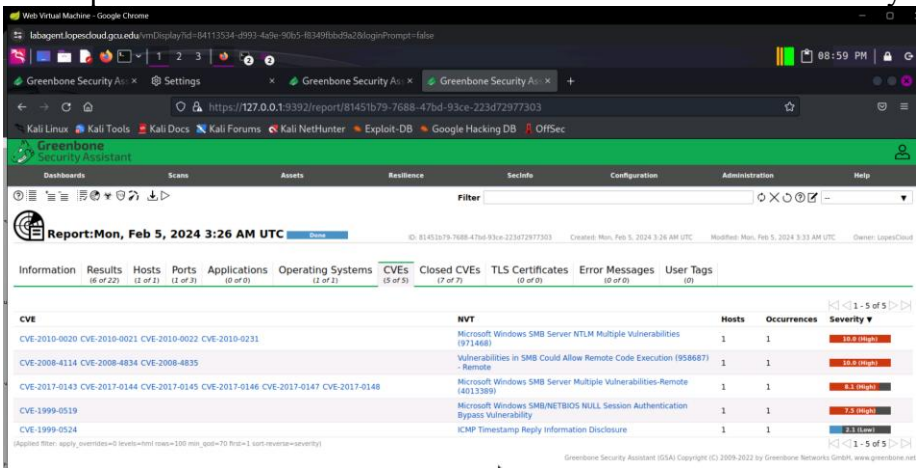
5. Waiting for the scans to load:



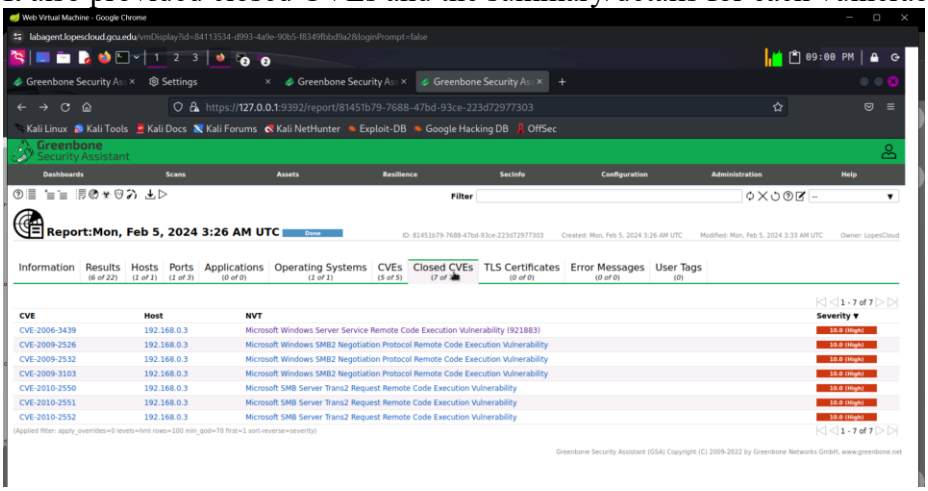
6. The Report for the Vulnerabilities in the Windows Scan revealed at least 5 severe vulnerabilities and 1 low vulnerability. Each Vulnerability provides the port/service that it is located along with the name of the vulnerability, how they each work, and a solution.



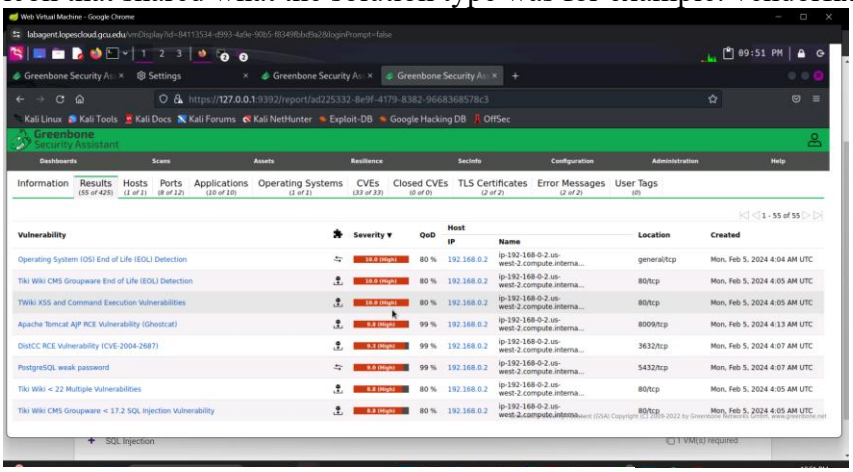
7. It also provided links to the exact CVE numbers for each vulnerability

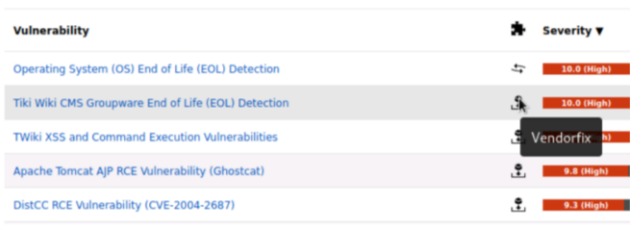


8. It also provided closed CVEs and the summary/details for each vulnerability.

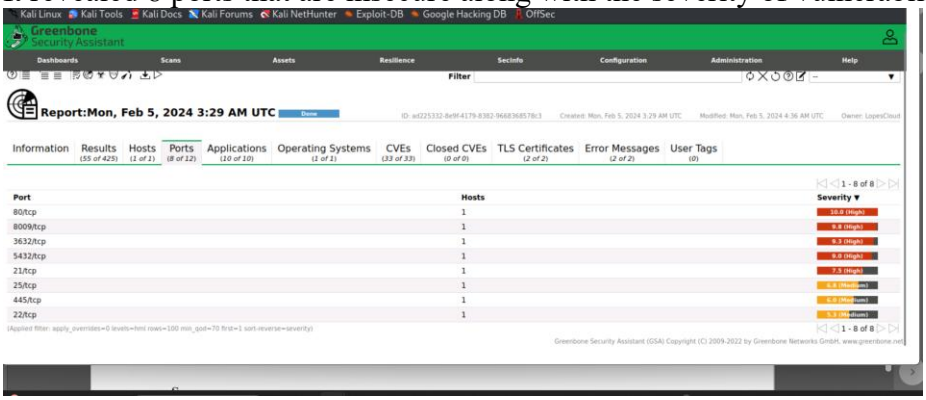


9. The Report for the Vulnerabilities in the Metasploitable Scan revealed at least 13 severe vulnerabilities, 36 medium and 6 low vulnerability. Each Vulnerability also presented an icon that shared what the solution type was for example: vendorfix, migration, etc.

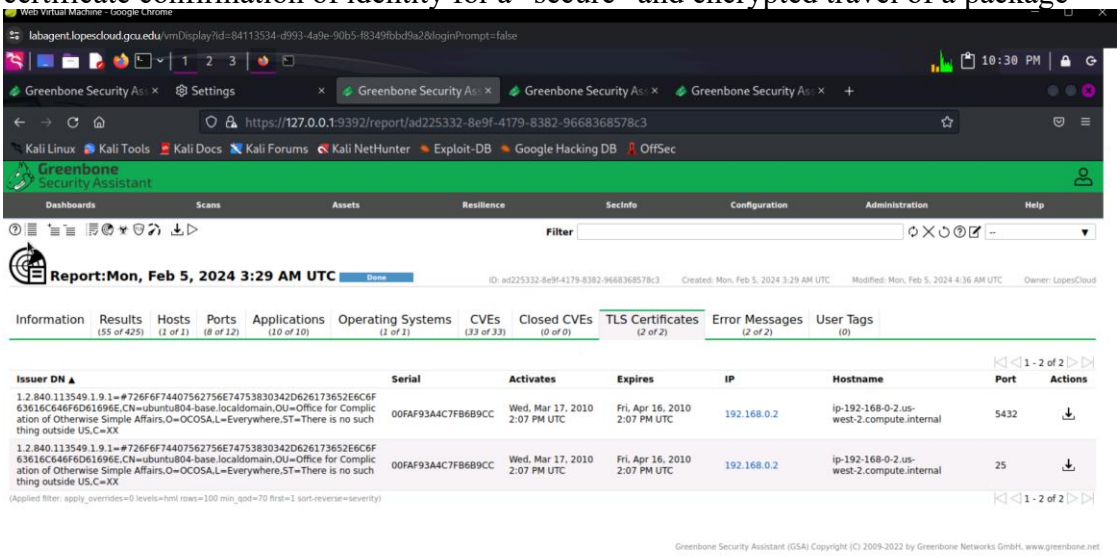




10. It revealed 8 ports that are insecure along with the severity of vulnerability.

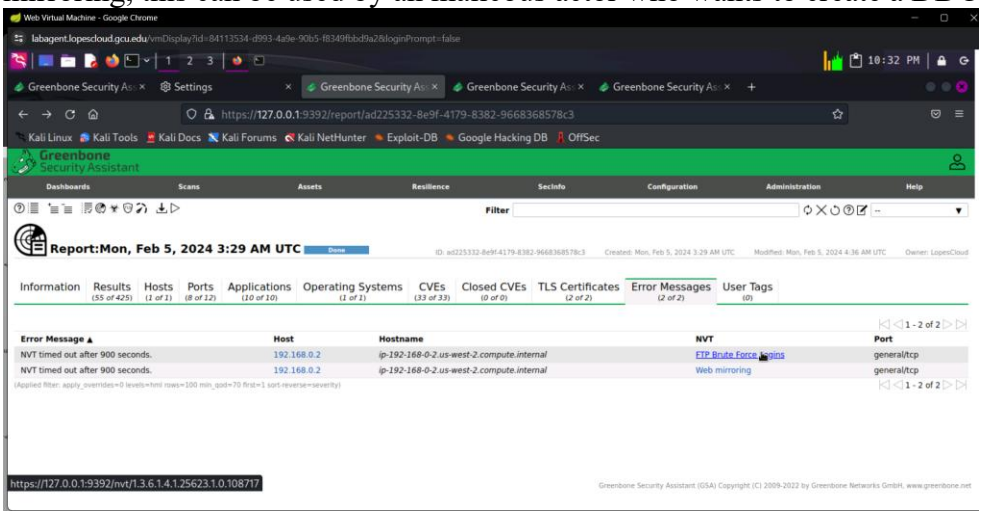


11. I was also able to view 2 TLS Certificates including the serial numbers which are actually certificate confirmation of identity for a “secure” and encrypted travel of a package



12. It also provided 2 error messages and the causes of error messages and how those errors were determined. One error was due to brute force attempts and the other was web

mirroring, this can be used by an malicous actor who wants to create a DDOS.

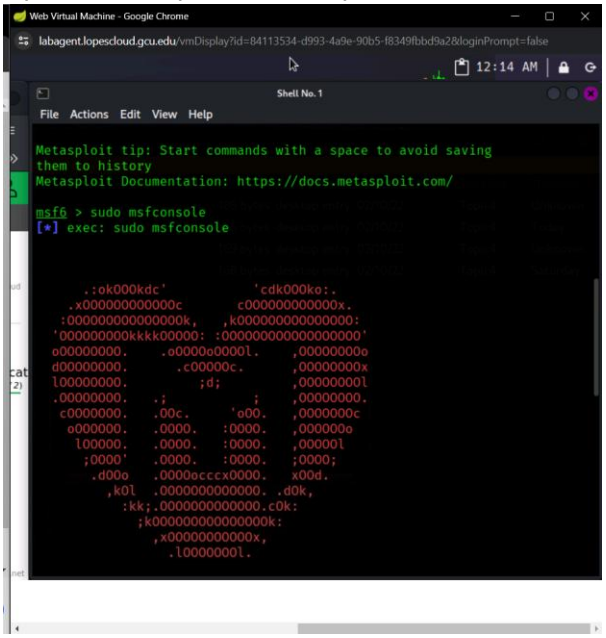


Applied Exploitation using Metasploit

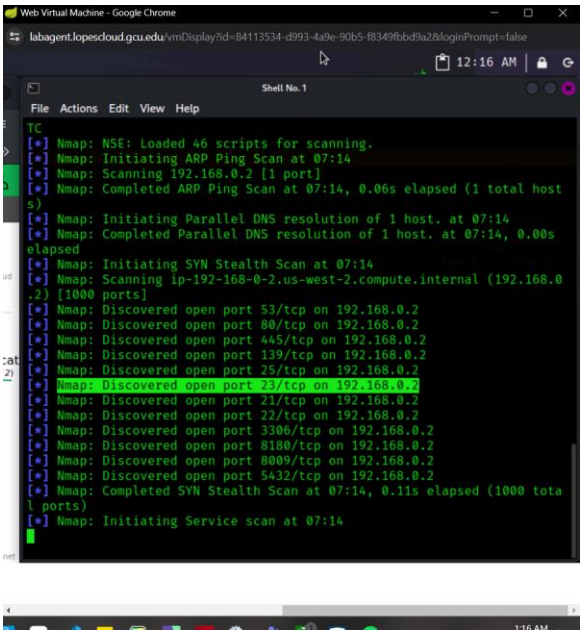
Summary

When looking for vulnerabilities I utilized the vulnerability scan for inspiration of what ports and vulnerabilities to keep an eye out for when using Metasploit. I then pursued the open ports: 23/telnetd, 25/tcp, and 5432/tcp postgresql.

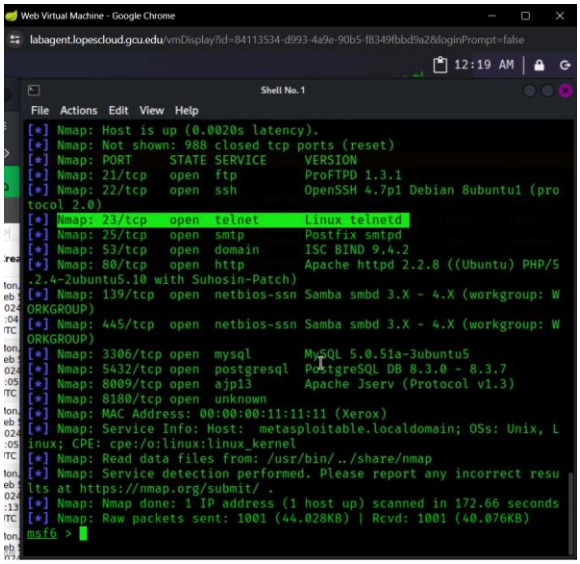
Opened metasploit with root permissions and did a nmap search for vulnerabilities under the llnux system



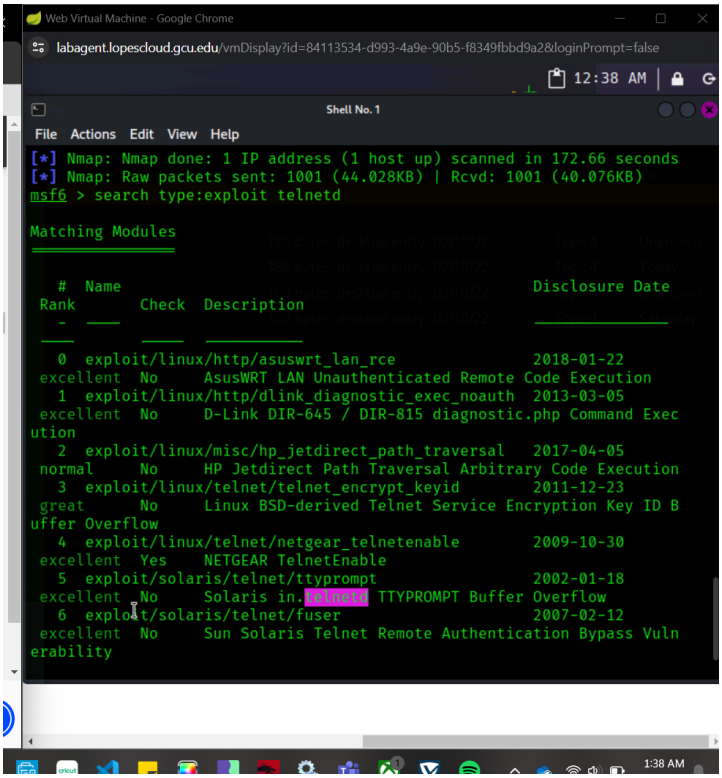
Found a series of open ports including the telnet port 23, decided to pursue this and scan for vulnerabilities



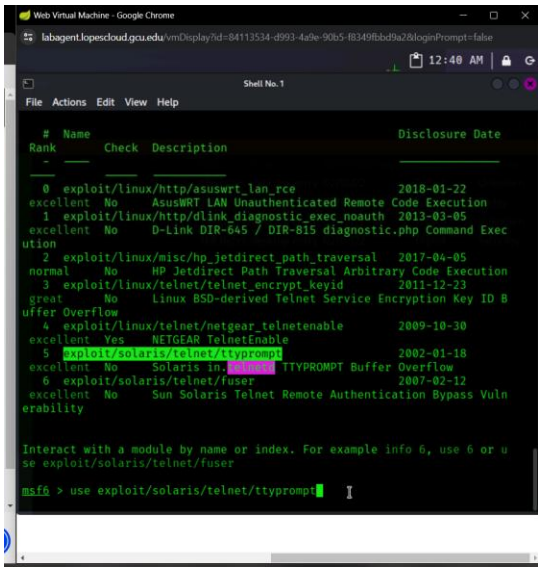
Metasploit also provides the exact service and a description which is going to be useful in this exploit and in future investigations.



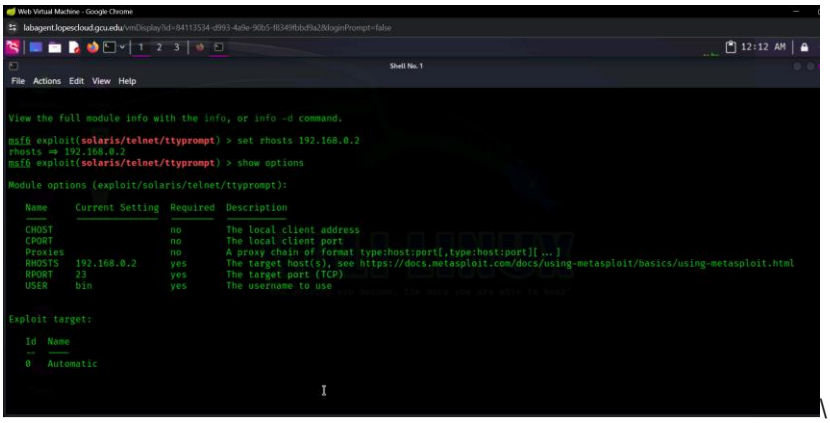
Did a specific search for exploits on telnetd and found 6 specific exploits including the Solaris in .telnet d which has the vulnerability from a buffer overflow



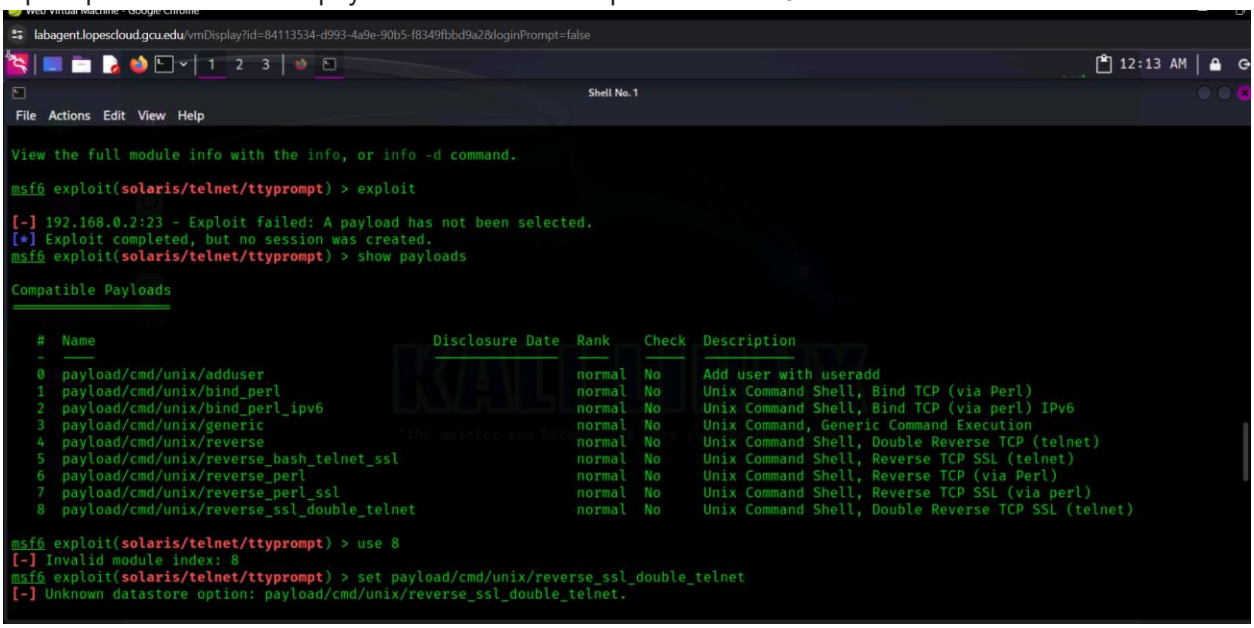
Typed in the option (5) that I wanted to pursue then typed options to see the list of module options



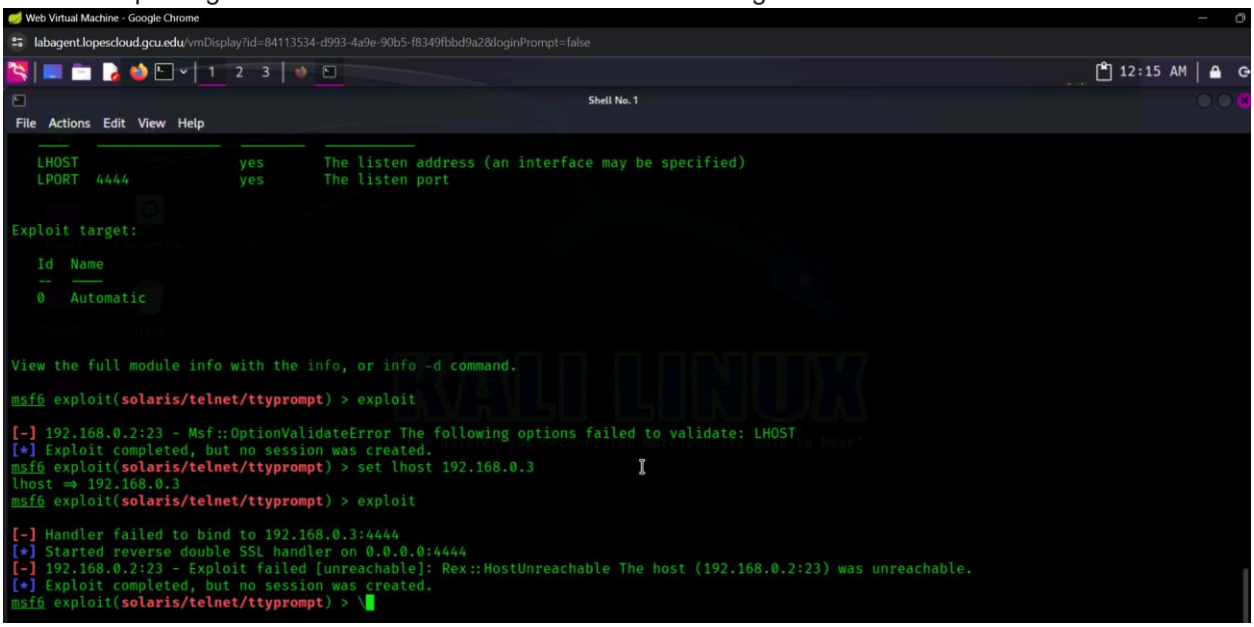
I then typed show options and then set the rhosts (targeted host) to 192.168.0.2 and showed options again to confirm.



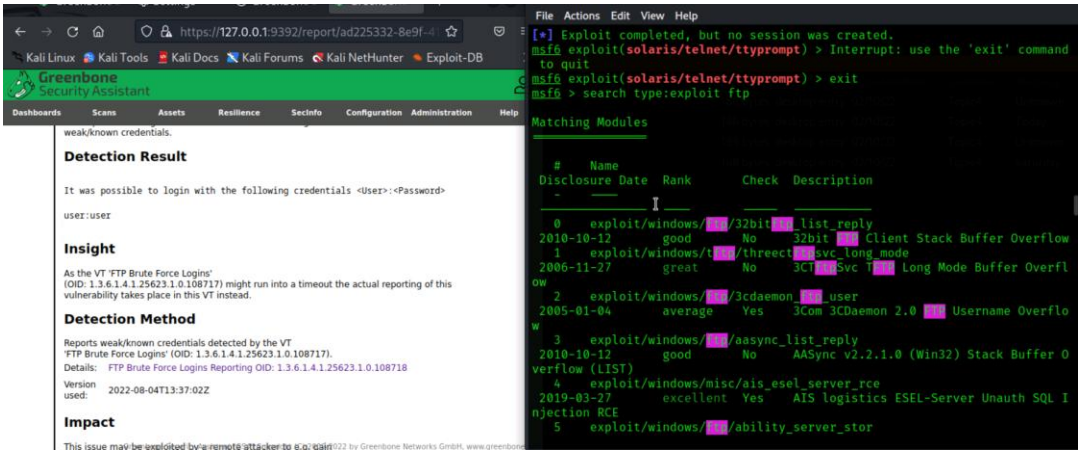
It prompted me to select a payload to use for the exploit so I used 8



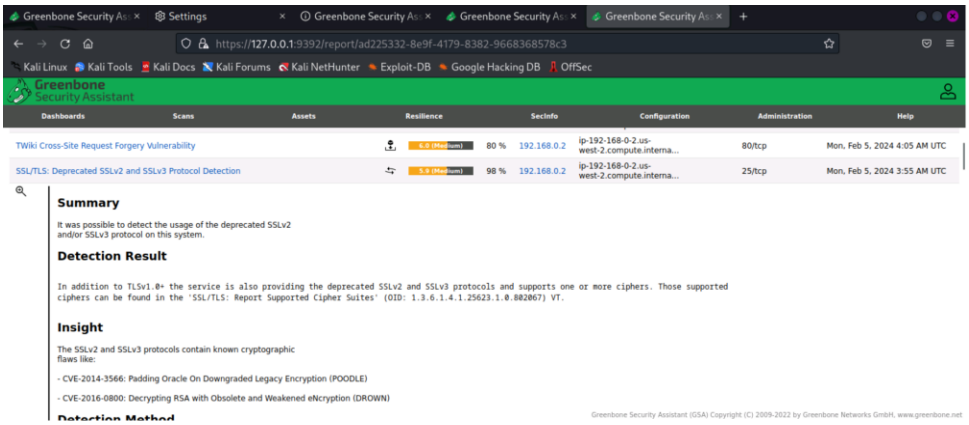
I tried to exploit again but it led me to a deadend as it was asking for more addresses



Exploiting a FTP vulnerability



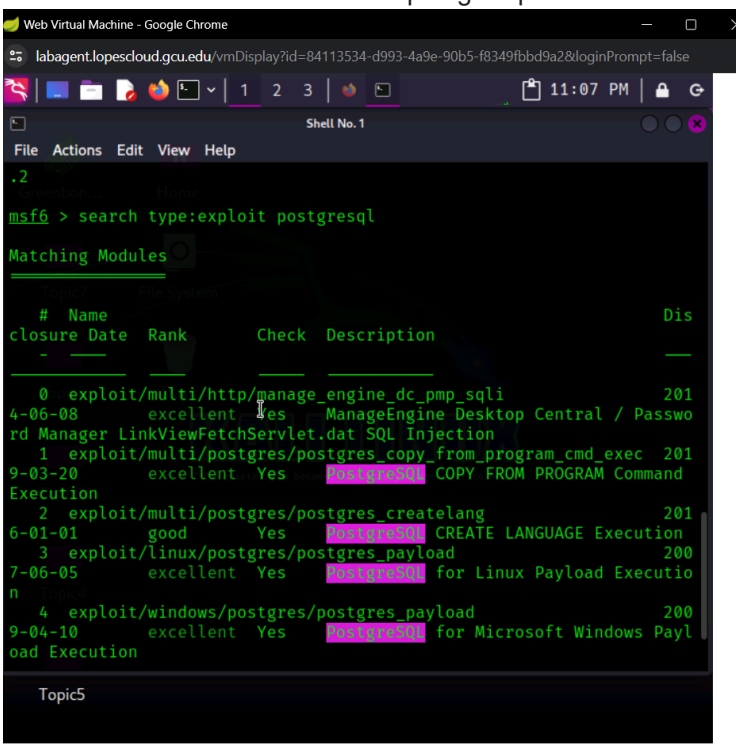
Going to aim for th 25/tcp port and exploit the SSL/TLS deprecated SSLv2 and SSLv3 Protocol Detection Vulnerability



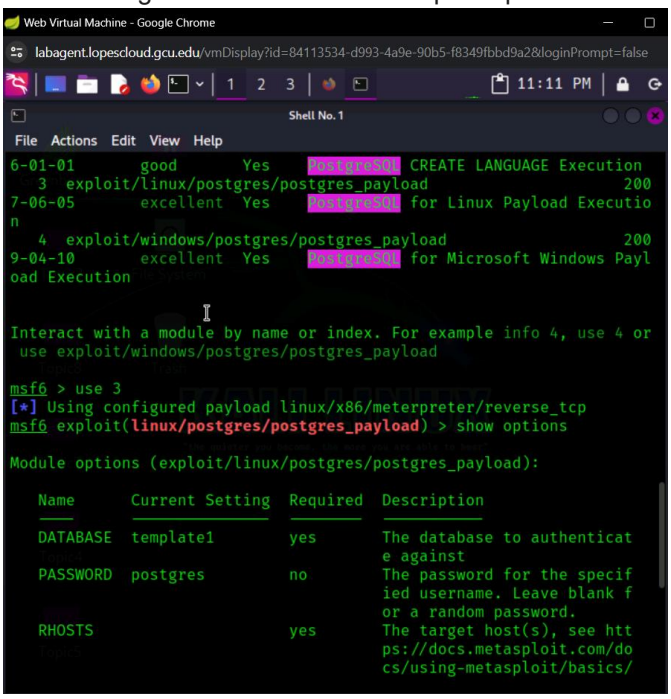
Decided to compare the list of services discovered by metasploit and compare it to the vulnerability scan to see what ports I can utilize and exploit

Decided to go for port 5432/tcp postgresql with the vulnerability of weak passwords

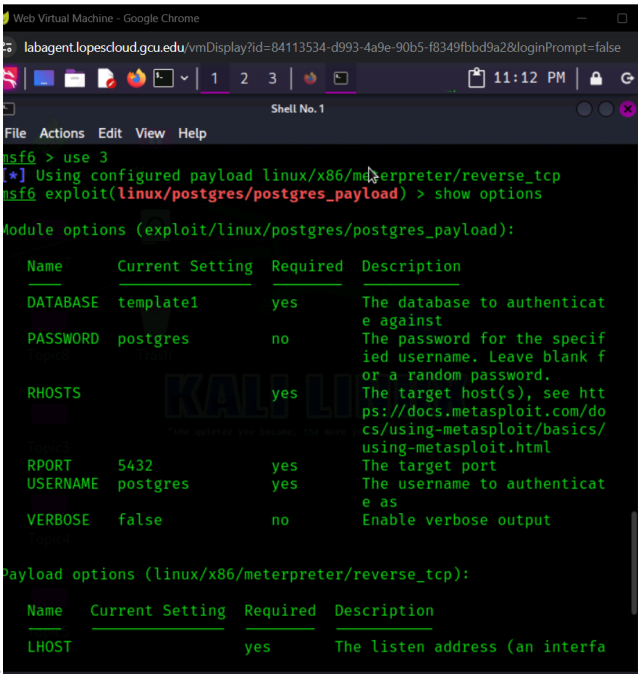
Searched for vulnerabilities under postgresql



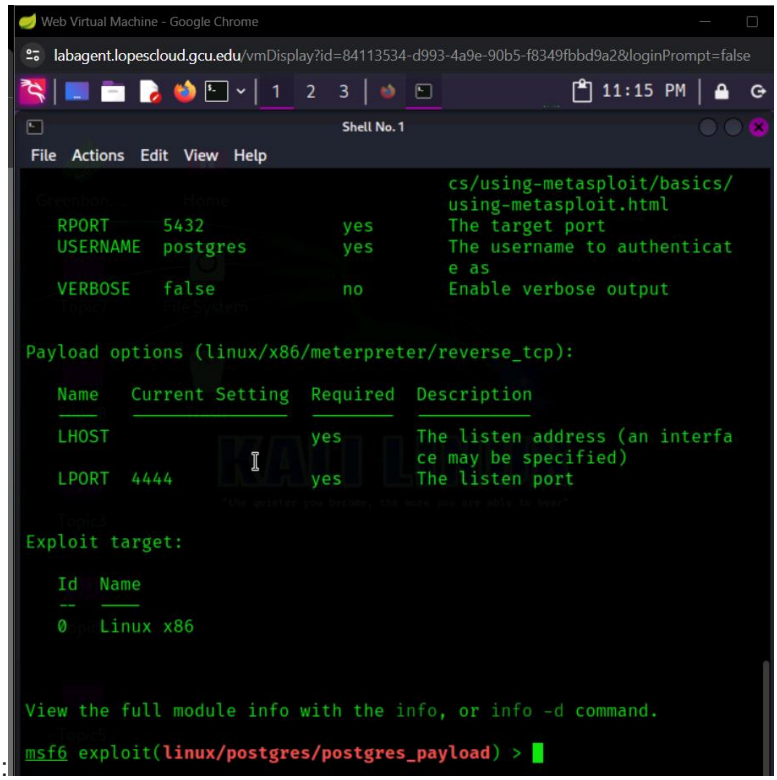
Decided to go with 3 then see the exploit options available



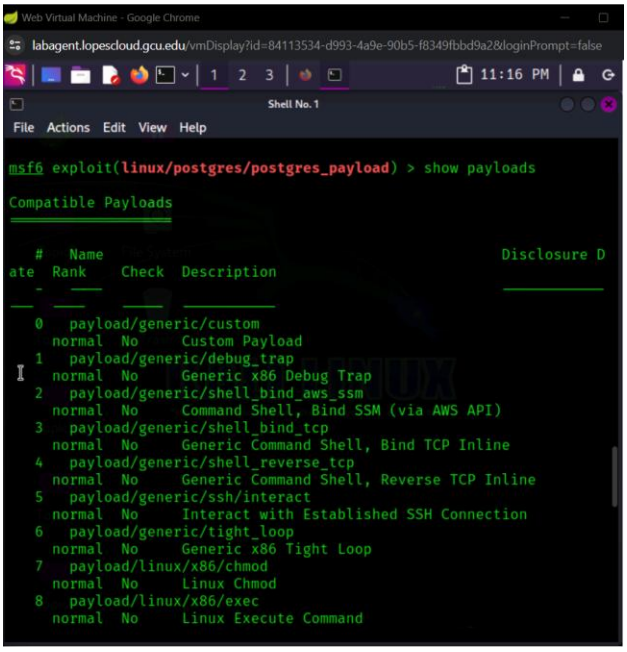
Discovered the database name to authenticate against, the password that can be used but it also told me that I can leave the password blank to access it and the username to use to login : postgres. It gave me the name of the port I was targeting: RPORT.



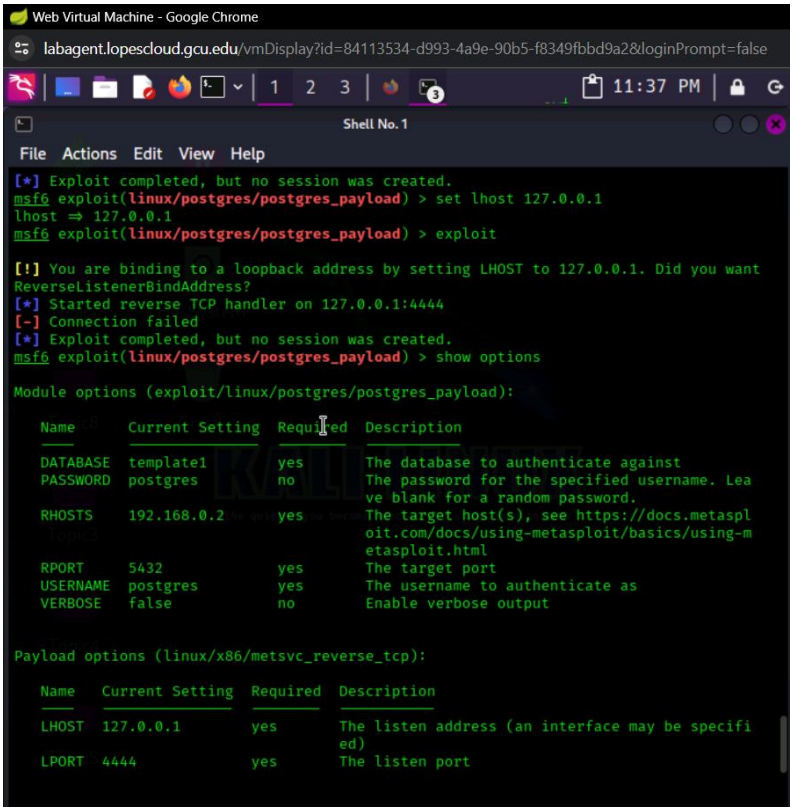
Provided payload options:



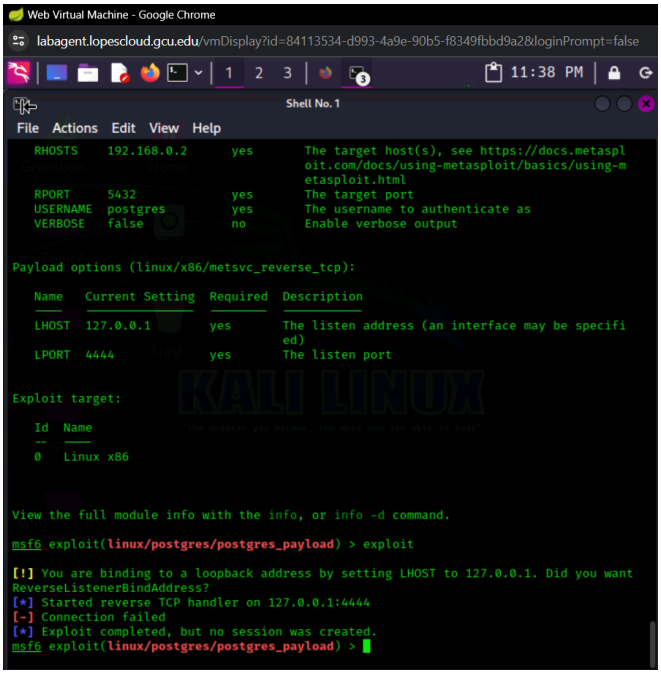
I then searched for payloads aka the pathways to the attack I could perform which provided me with 34 payload options to choose from:



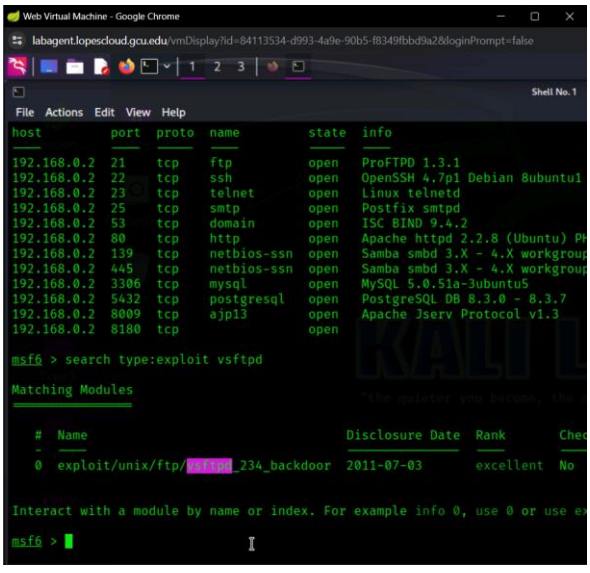
```
msf6 exploit(linux/postgres/postgres_payload) > set payload 19
payload ⇒ linux/x86/metsvc_reverse_tcp
msf6 exploit(linux/postgres/postgres_payload) > \
```



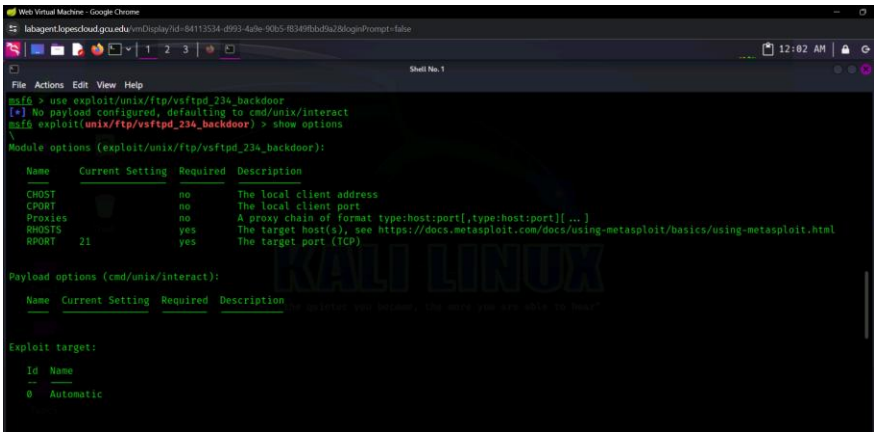
After setting the rhosts ip to the correct attack address and attempting to set my ip address as the lhost I was ready to perform the exploit. It performed but kept saying that the connection failed.



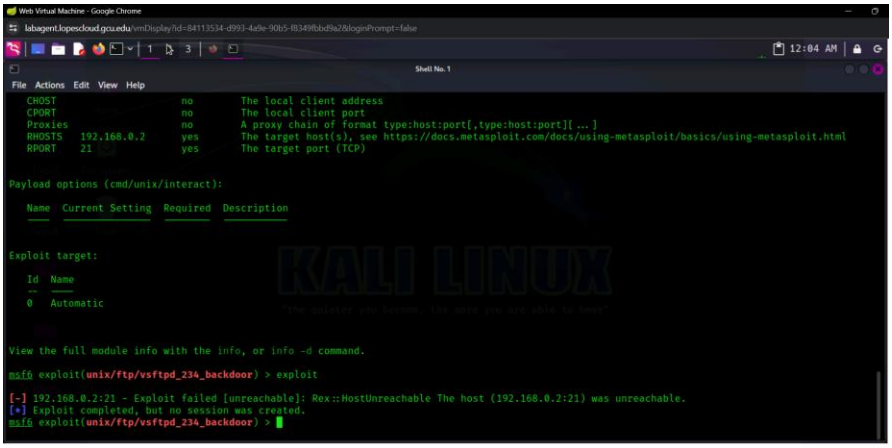
Decided to perform an exploit for vsftpd to implement a backdoor by first searching for it (noting that its in port 21).



Decided to use this exploit then show options from this exploits payload, then set the rhosts to the ip address of the target



After exploiting it with the assigned rhosts it provided me with this feedback:

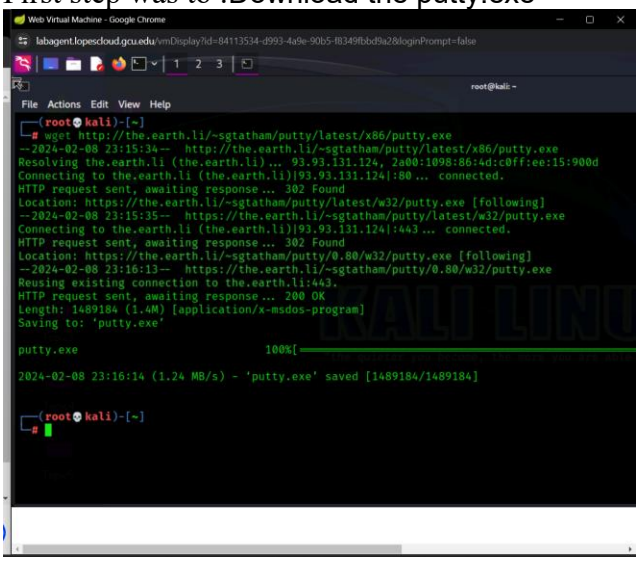


Custom Payload

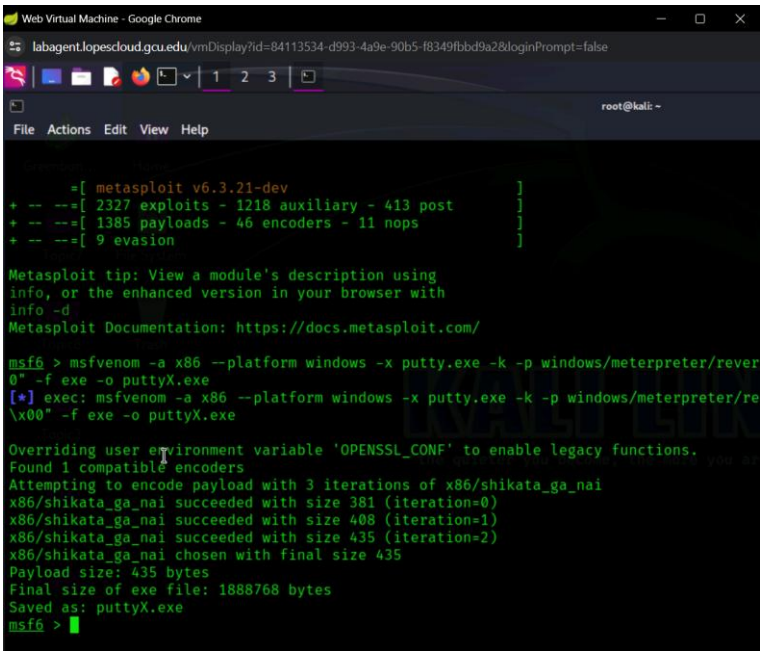
Summary: The goal was to use a reverse tcp handler in order to imitate utilizing a custom payload so that

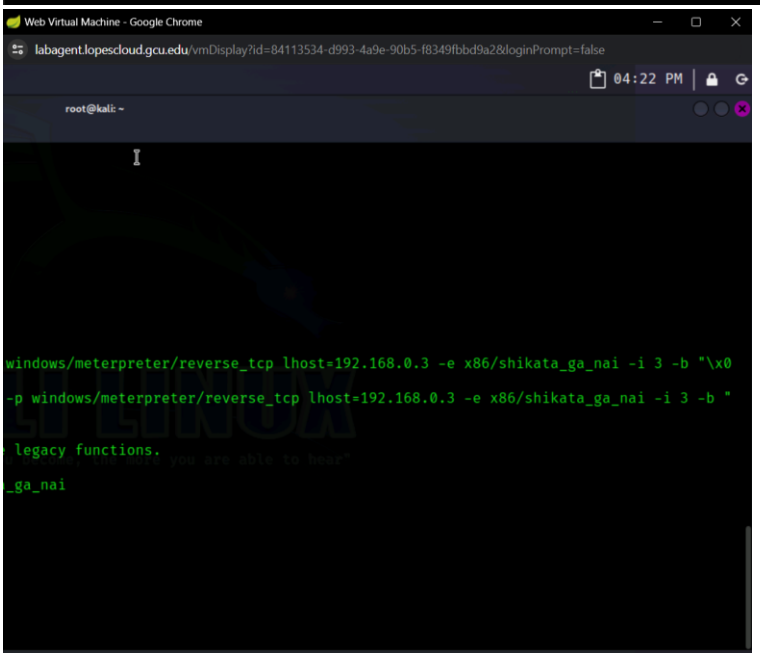
Steps:

First step was to :Download the putty.exe

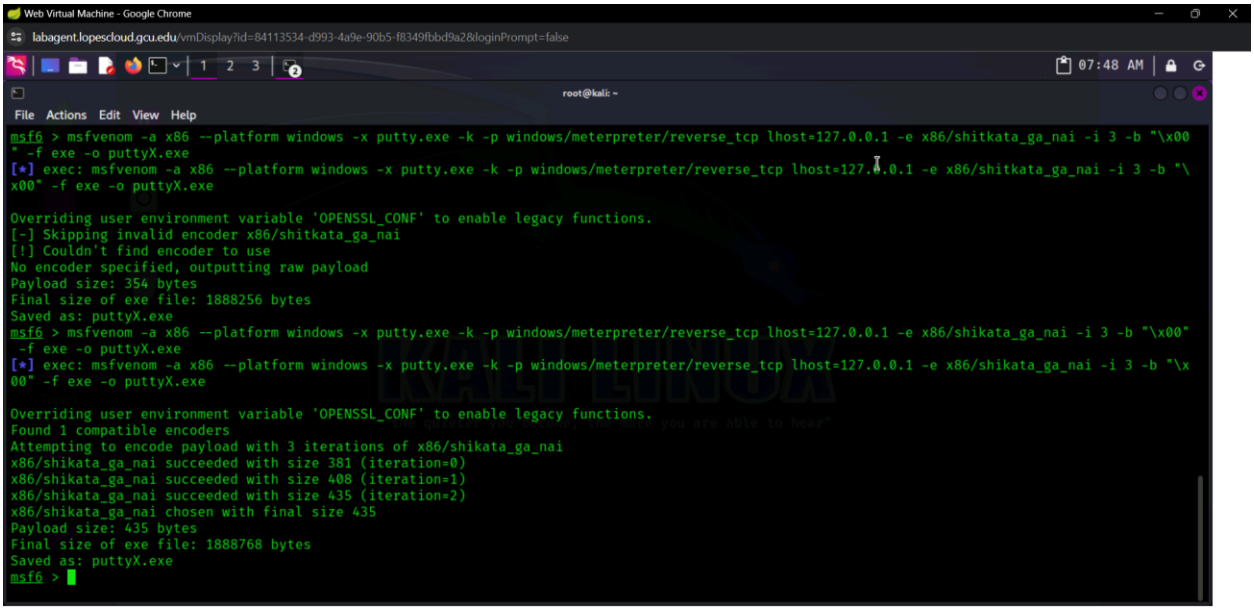


Then set a custom payload with a meterpreter reverse and backdoor to the windows vm: 127.0.0.1

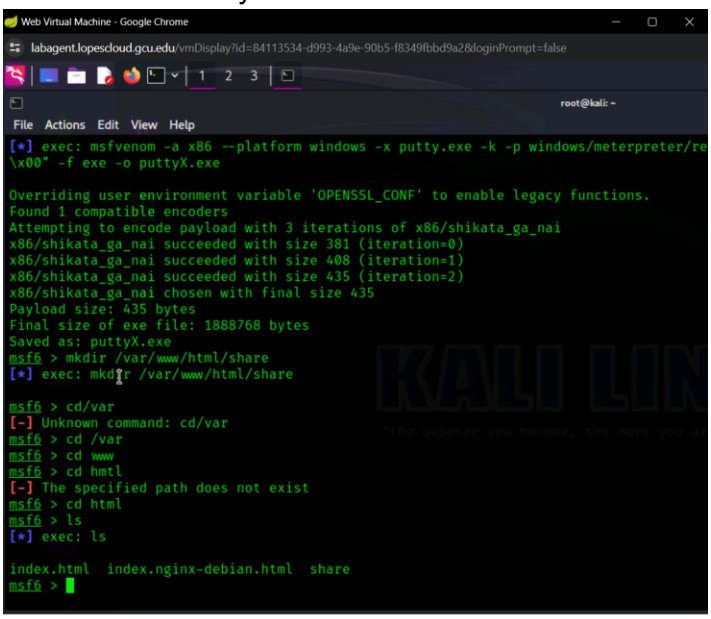




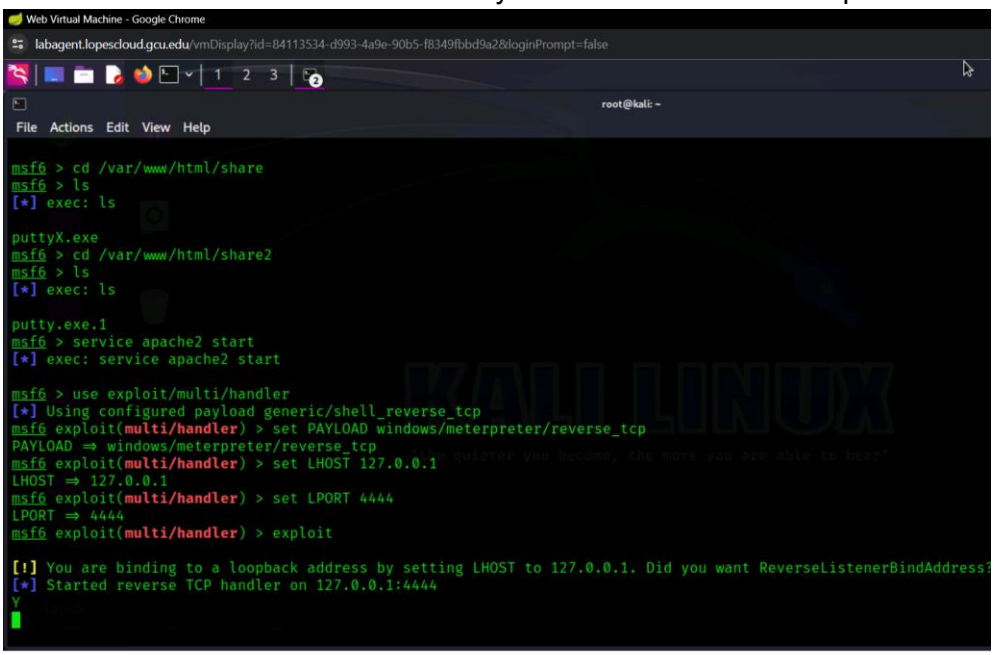
The putty executable file is not created but needs to be accessed by the windows vm:



Created a directory called share and then checked to ensure that it did exist:



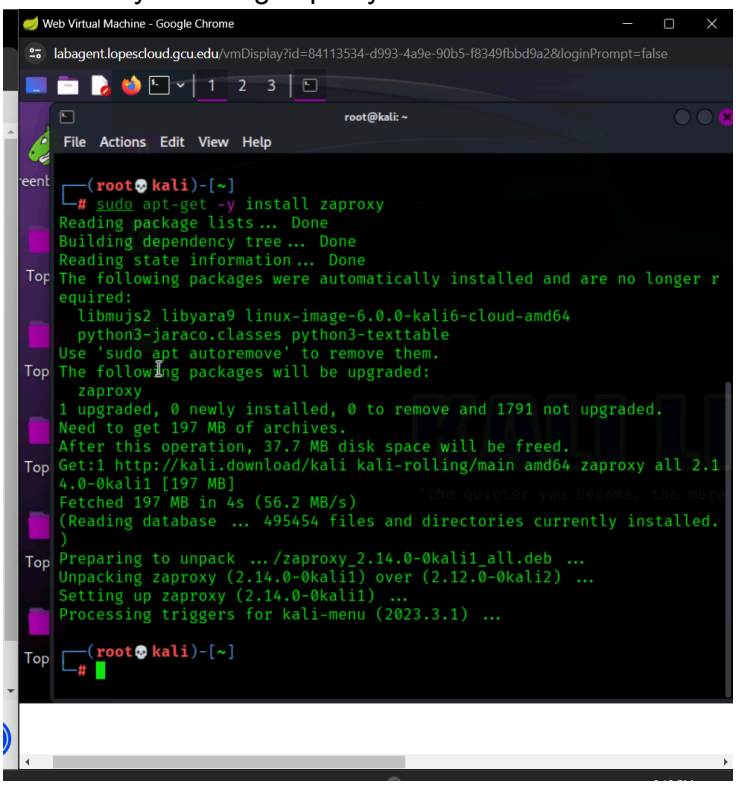
Realizing that i used the wrong ip address the first run I repeated all previous steps and had to use different file names. But was finally able to run the reverse tcp handler



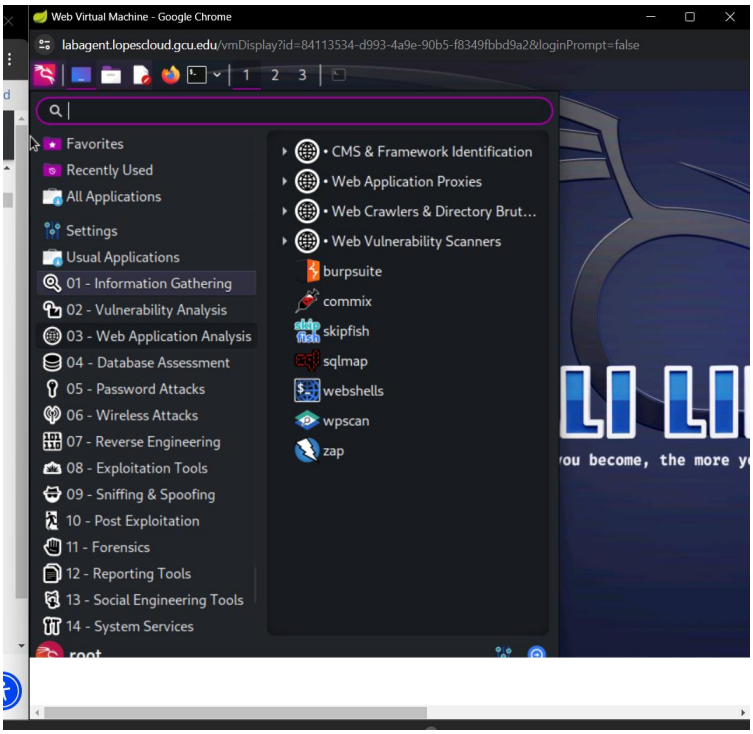
When trying to access the browser it said it was unable to connect but it could be because my host laptop was connected to a public wifi network or because I utilized the wrong port so I went back and changed the LPORT to 9392 but it caused the screen to become frozen.

Website Vulnerability Assessment

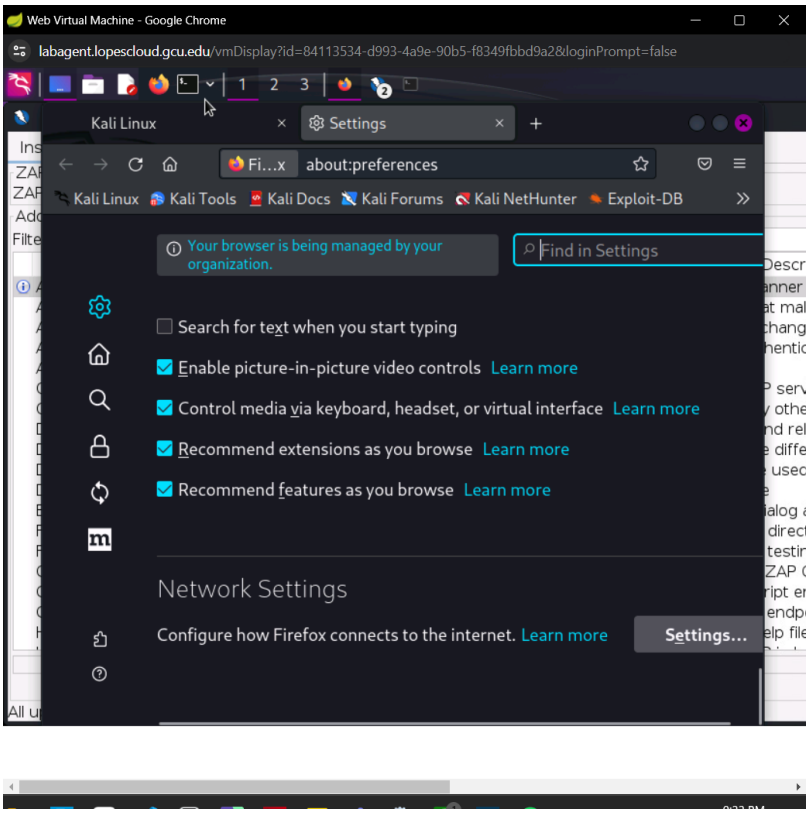
I started by installing zaproxy:

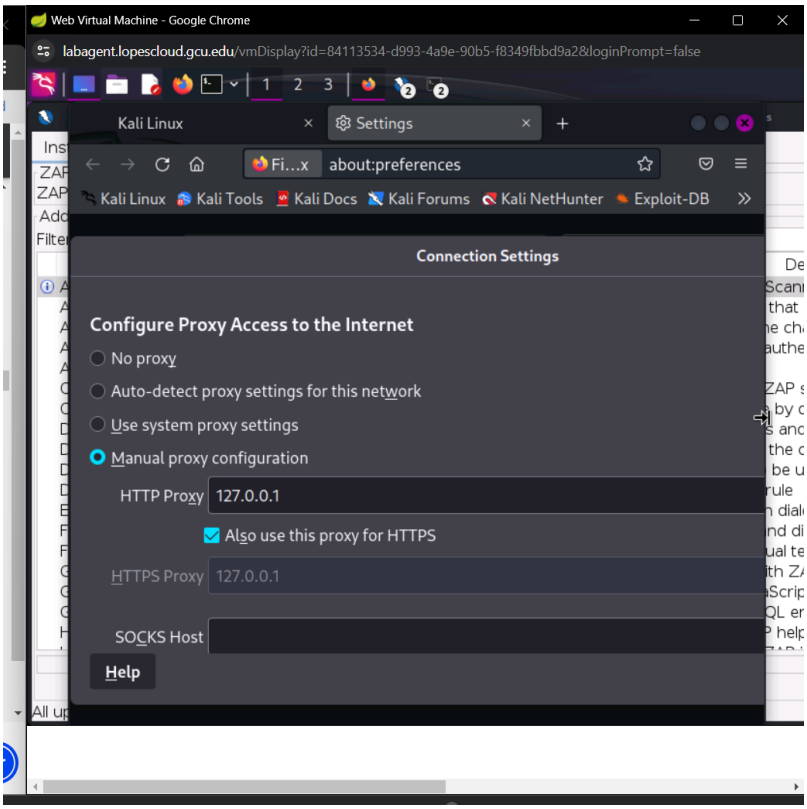


I then opened the application and my browser:



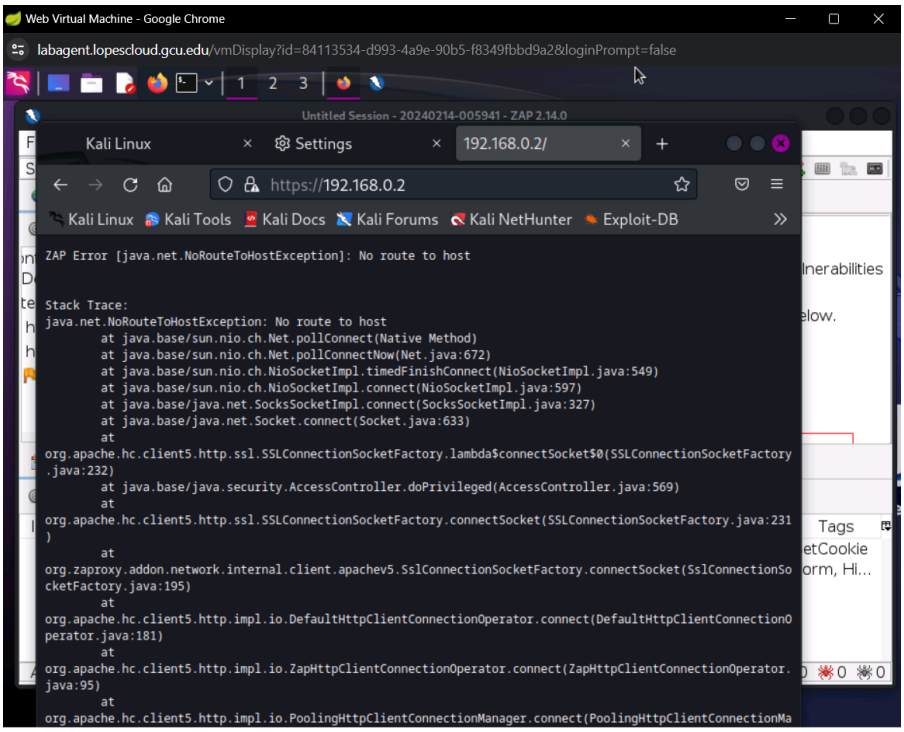
Before proceeding to any other steps I needed to make sure that the network settings were properly configured so that the LHOST was set my VM's local host: 127.0.0.1 and port 8080



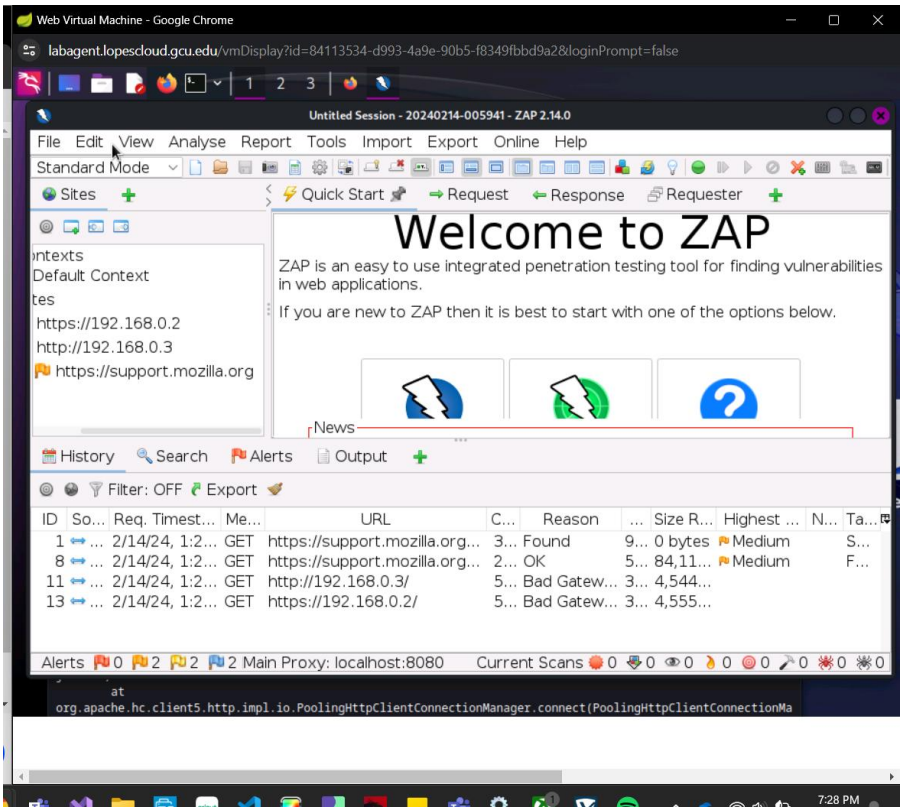


After configuring the settings I opened a new tab to go to the ip address for the metasploitable 2: 192.168.0.2.

After going to advanced and accepting the risk and continuing it led this error:

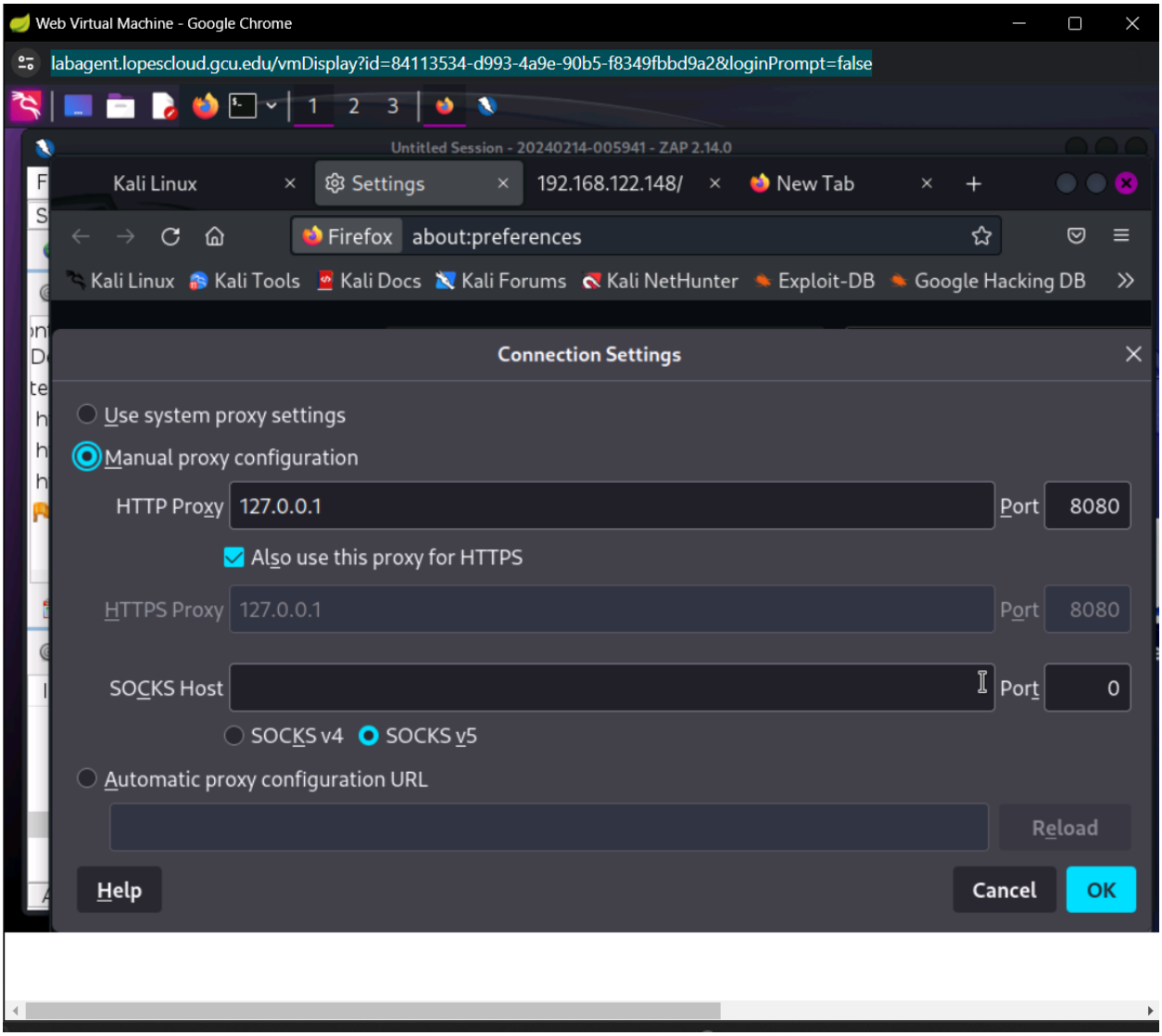


We are now able to see the requests on zap but they only showed the failed requests:



I checked my settings once again and even tried to restart my LopesCloud and restart the browser but it still led to the same failures- I am thinking the lab was malfunctioning or just down when trying to connect. I also tried different IP addresses just to makes sure it wasn't the one

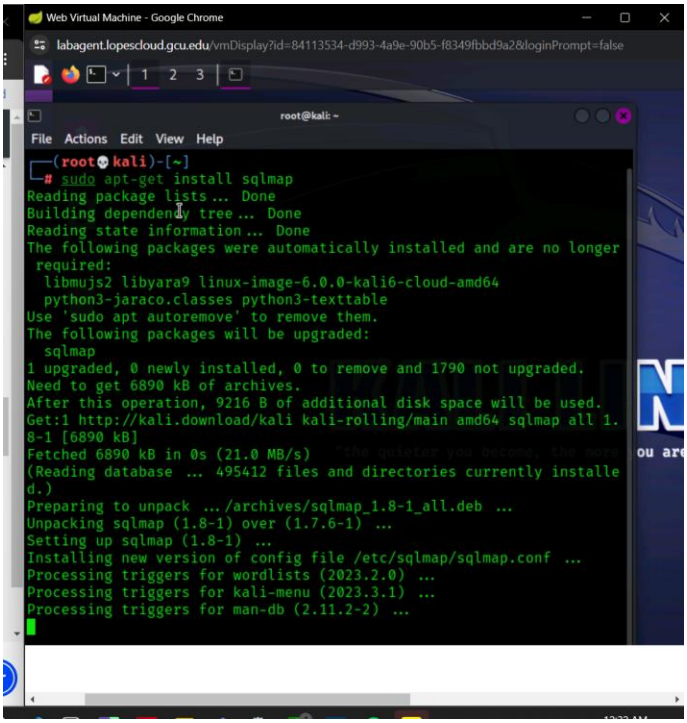
website. (192.168.0.3 and 192.168.0.2 and 192.168.122.148):



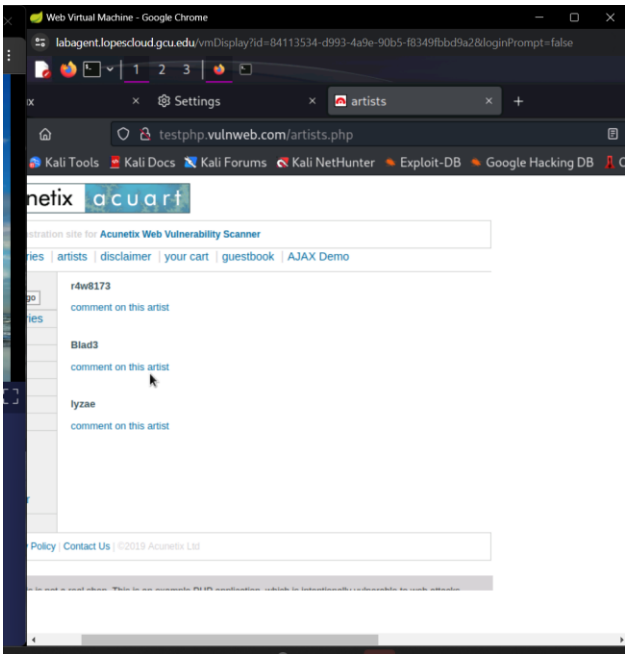
SQL Injection

Summary: To test the various vulnerabilities and/or bugs in the website's database structure and code, it is necessary for pen testers to perform a SQL injection test to see if code can be manipulated in order to obtain unauthorized access to the database and its data. Using the tool SWLMap we were able to extract user information and data about carts from the website.

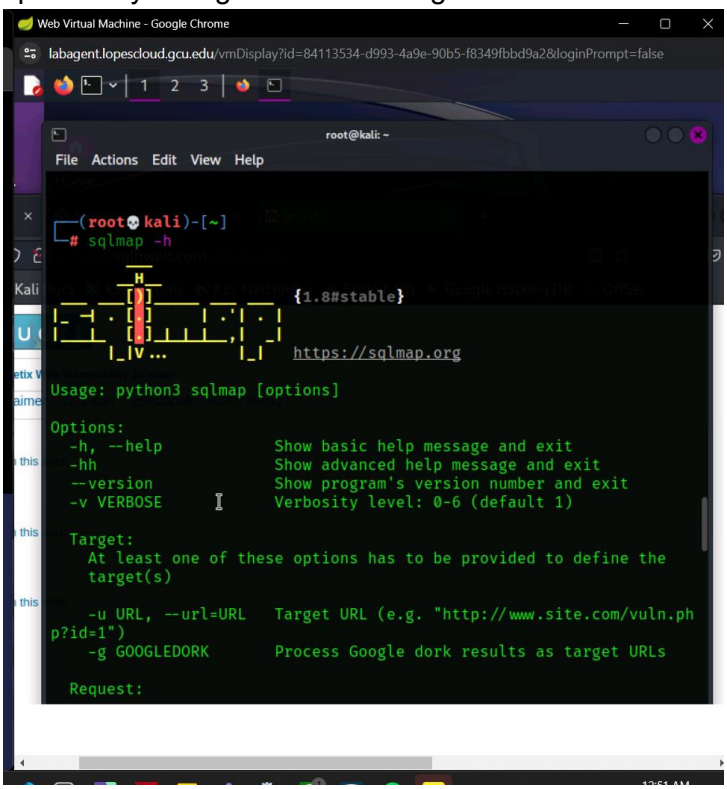
Installed sqlmap



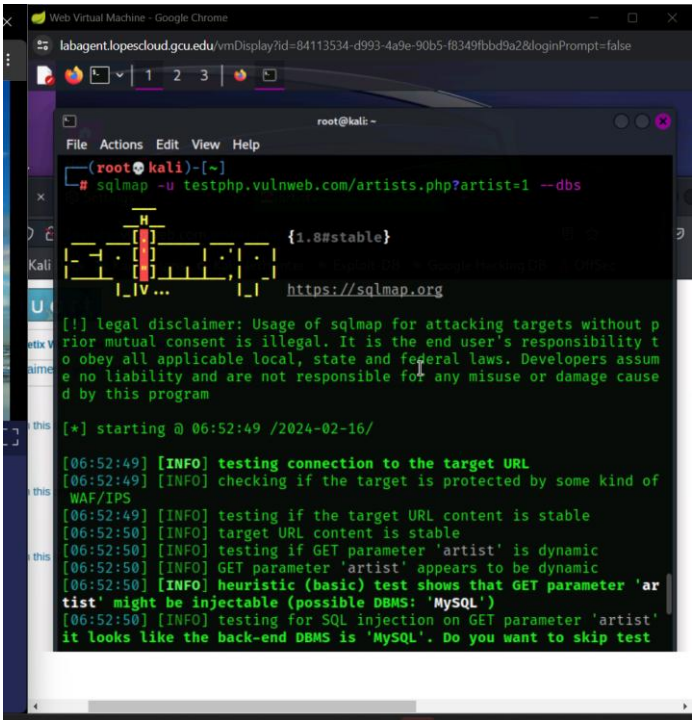
Went to the practice "vulnerable" site and took note of the url.



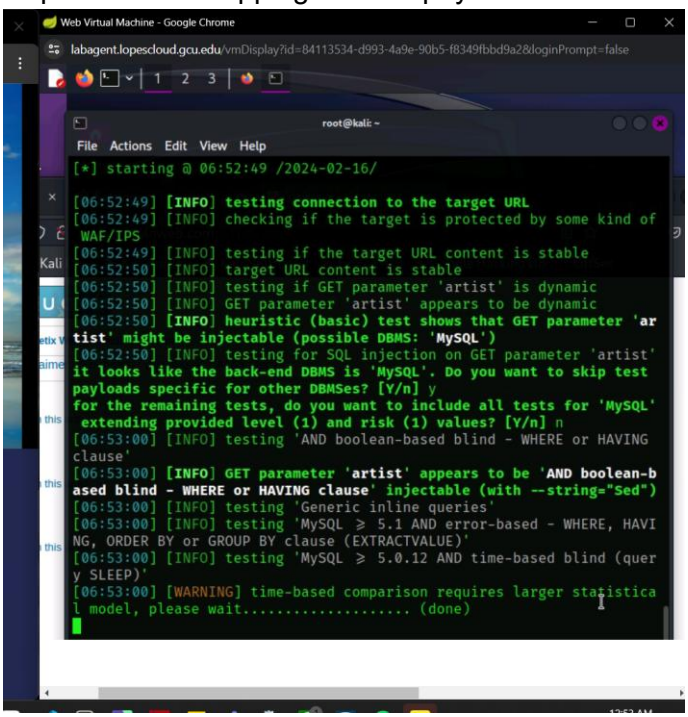
Opened the Help Menu in sqlmap in my cmd to get to know the different tools/functions specifically taking note of the Target functions.

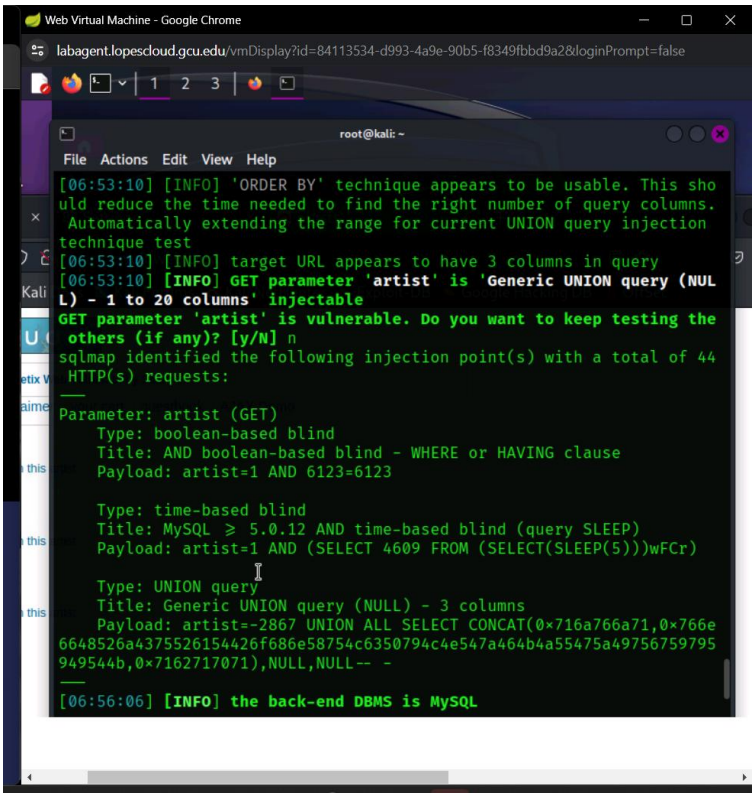


Utilized the website url then added additional code to access the database.

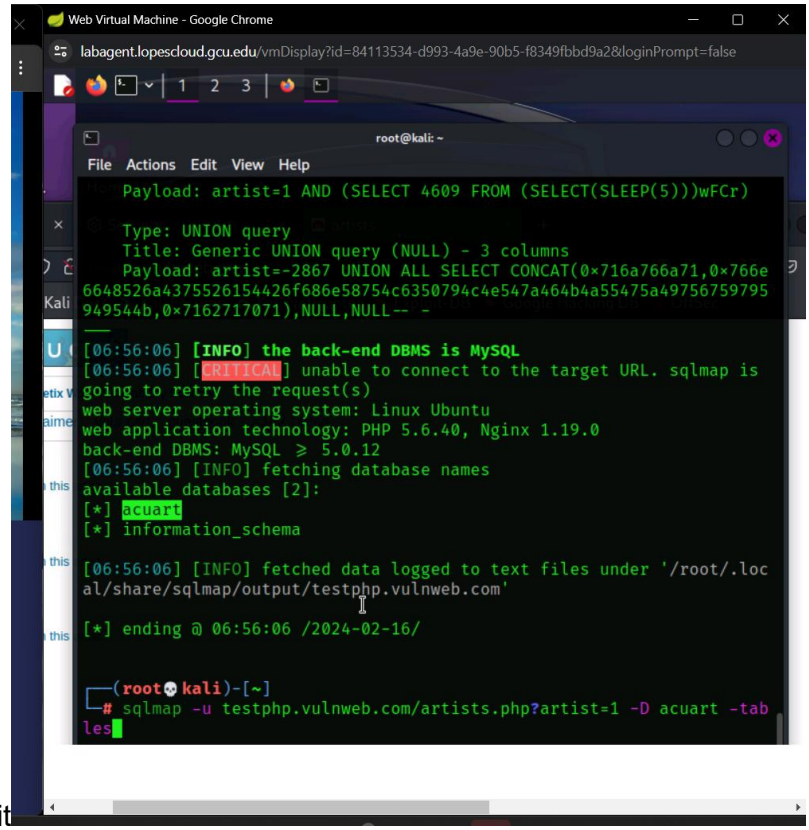


Replied Yes to skipping the test payloads and No to include all tests for MySqL

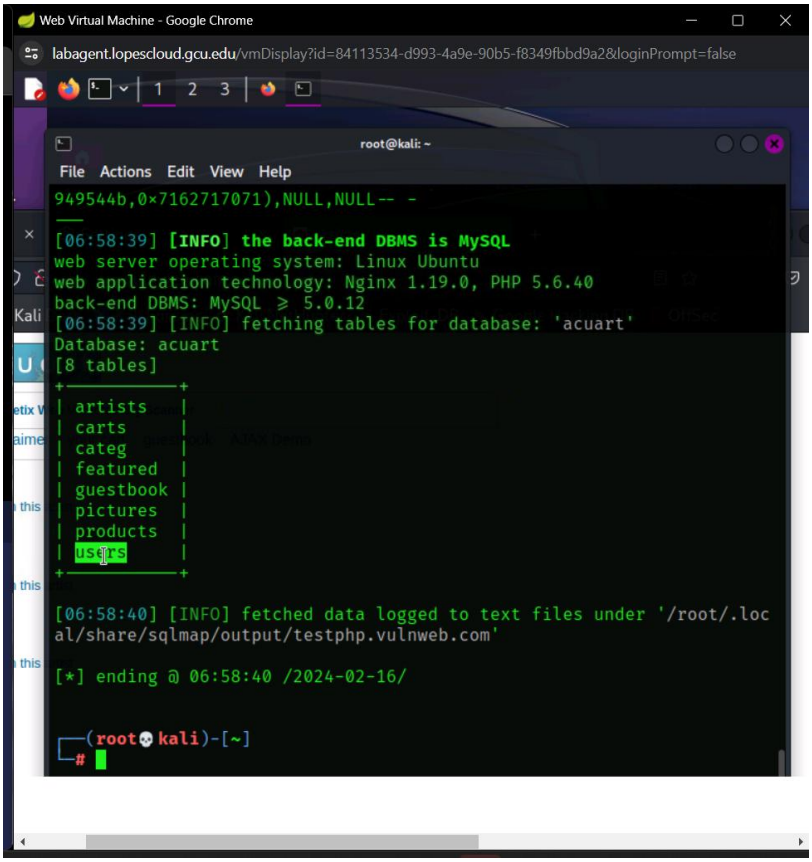




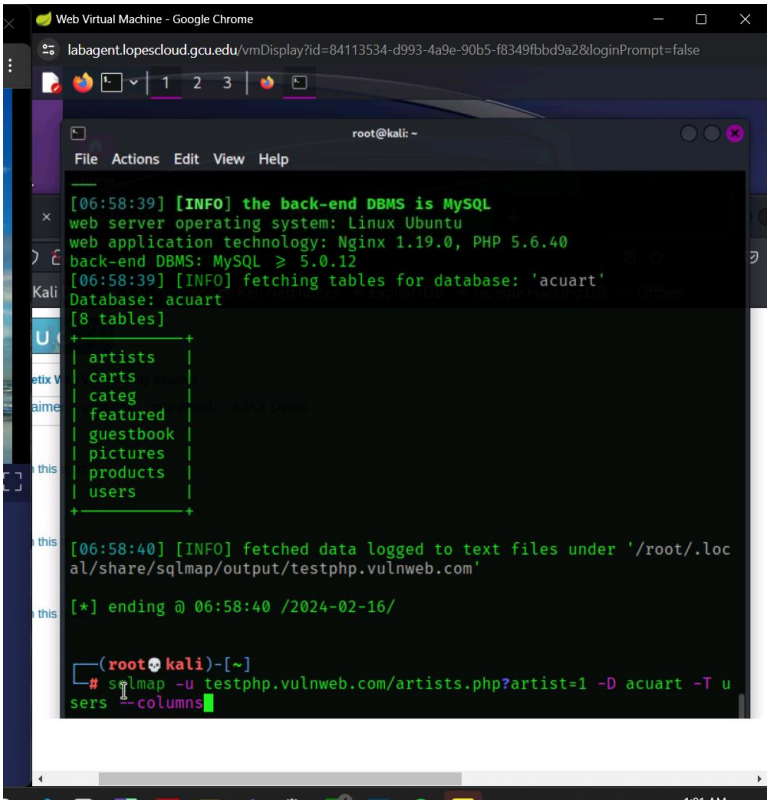
Discovered that Acuart is the file name for the database so we wanted to explore the tables inside it



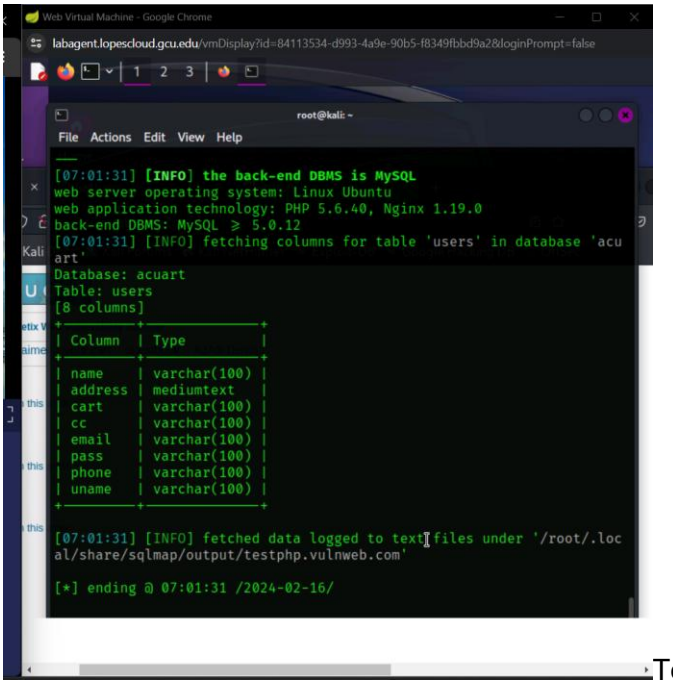
It revealed 8 categories to choose from, i then pursued the users column



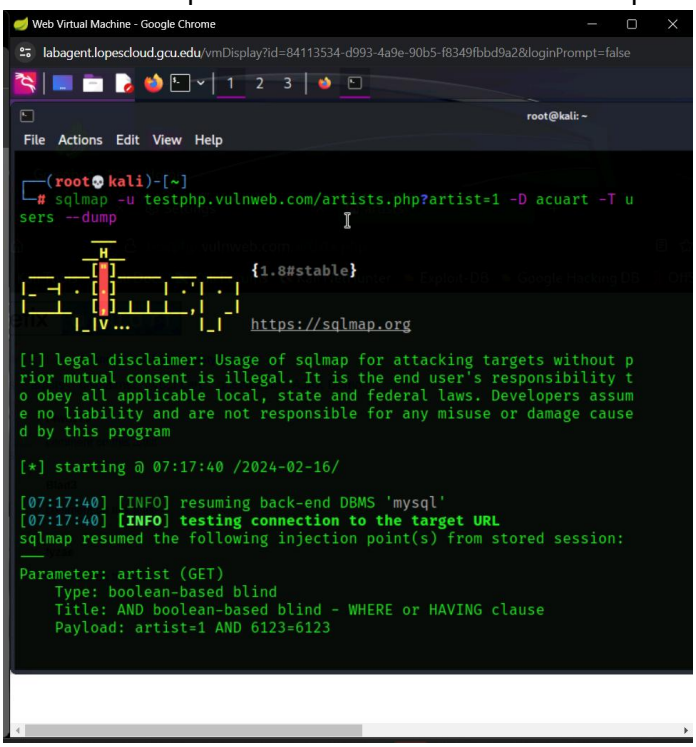
To enter the users column you enter the same url and code from previous and add -T for table and users then –columns to list all the info within the table for users.

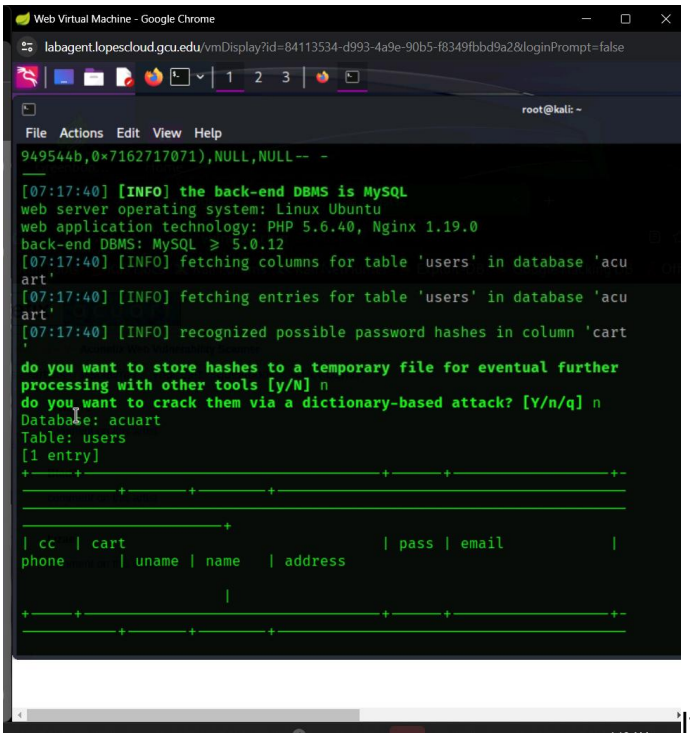


Which presented us with the following information:

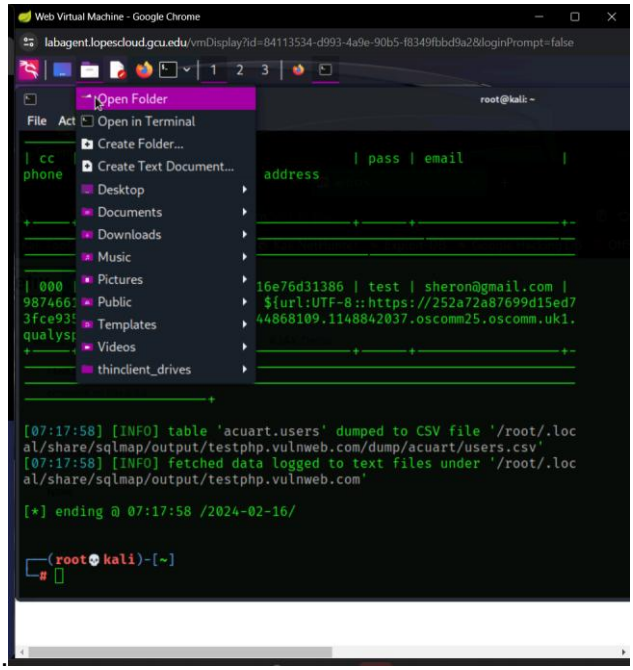


To download the information from users enter the same first part of the url and code with –dump which will save it to the computer.

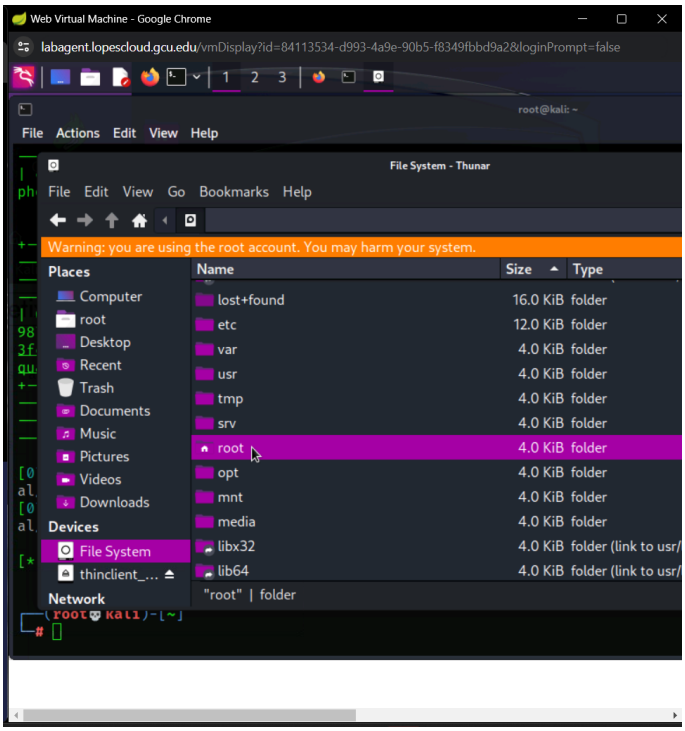


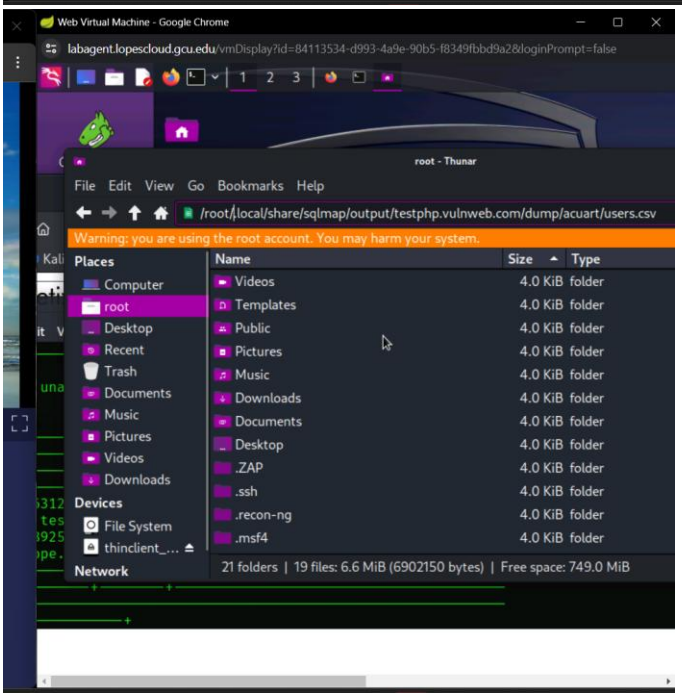


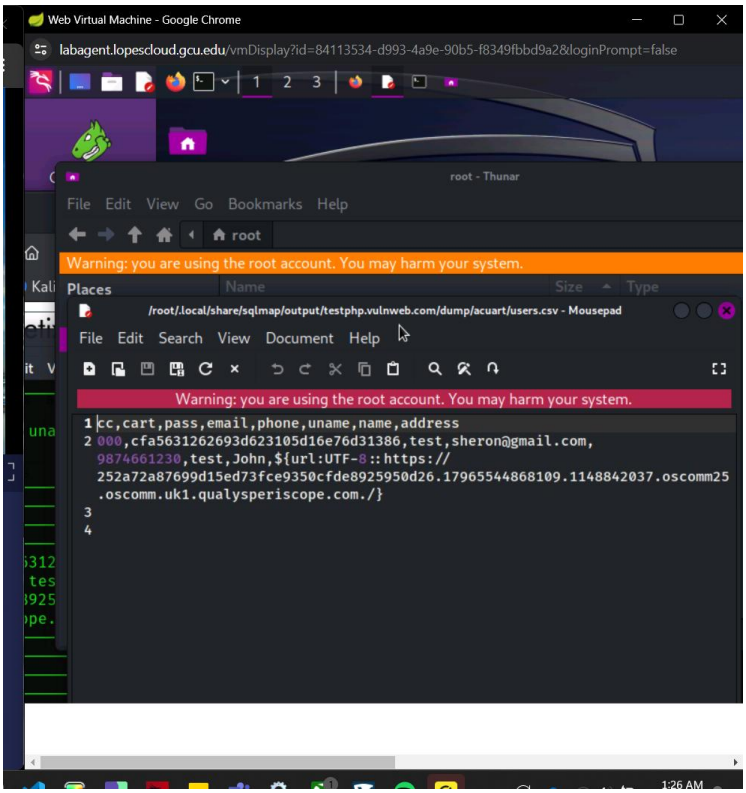
It presents the exact file folder path which you can follow manually or open up file folder….



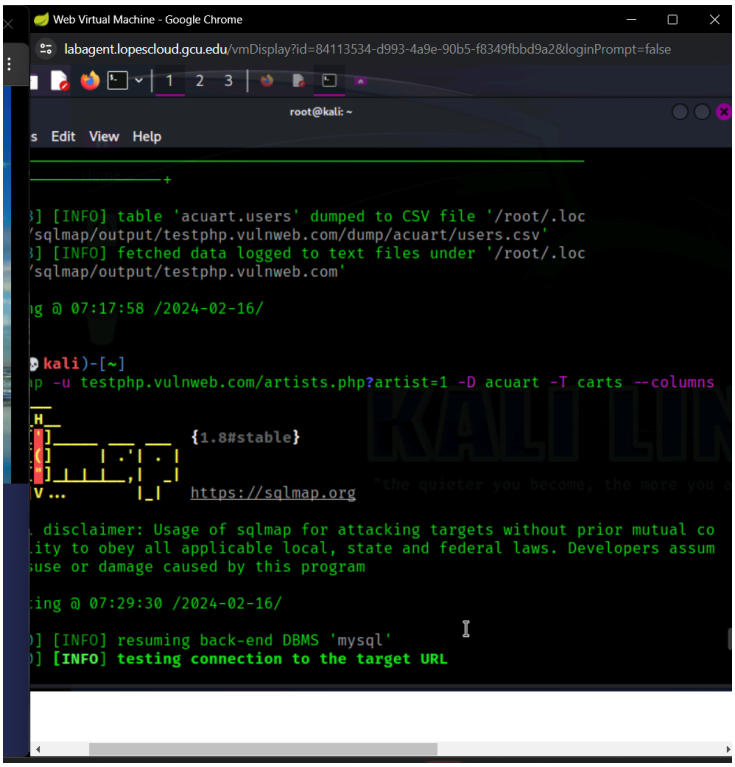
Go to the root folder and copy the file path directly.

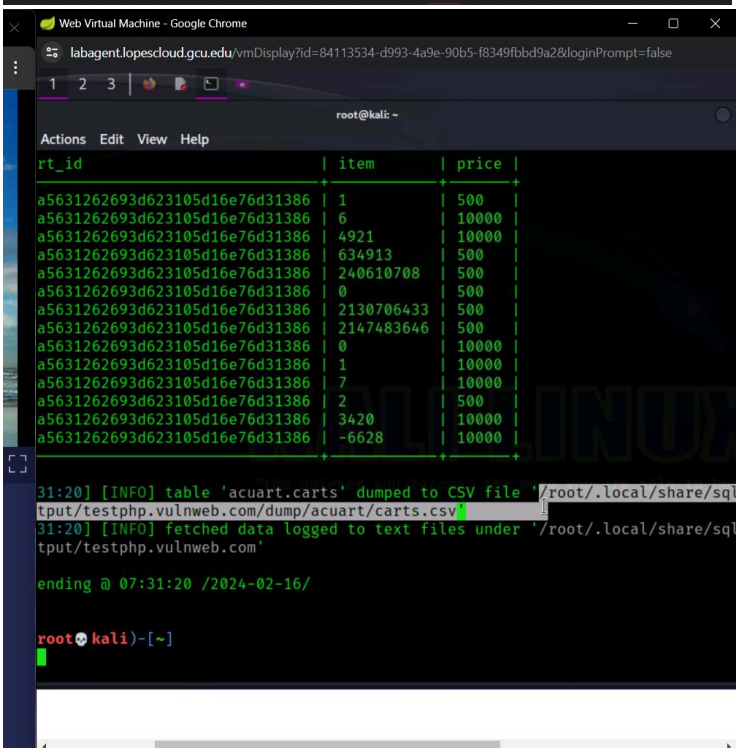


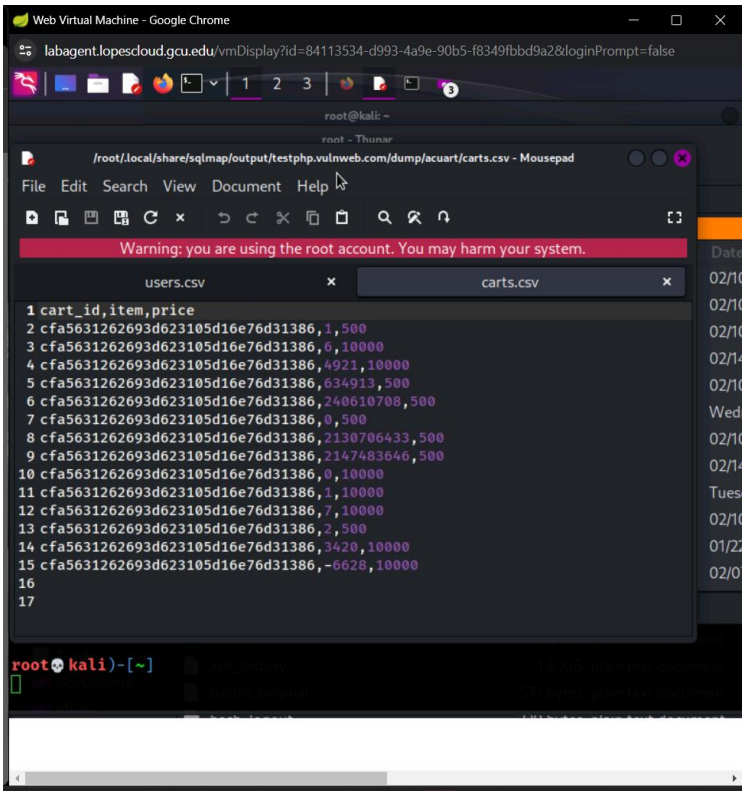




I repeated the same process again for the cart tables and to download that information to the computer.







Recommendations

This section will contain your recommendation(s) to repair/mitigate the discovered vulnerabilities.

Scope

This section provides the details of the test to be performed.

Details

This section will contain the step-by-step details of the test that was performed. Document commands that were used and their output. Screenshots can be included here. Make sure that if the customer follows these steps, they will be able replicate your results.

- Complete the "Details" section for each major phase of the test.
- Use of headings and numbering is required

Appendix

This section is used to document extensive results; for example, Nmap scans or results of vulnerability scans.

Resources

While APA format is not required for the body of this assignment, solid academic writing is expected, and documentation of sources should be presented using APA formatting guidelines, which can be found in the APA Style Guide, located in the Student Success Center.