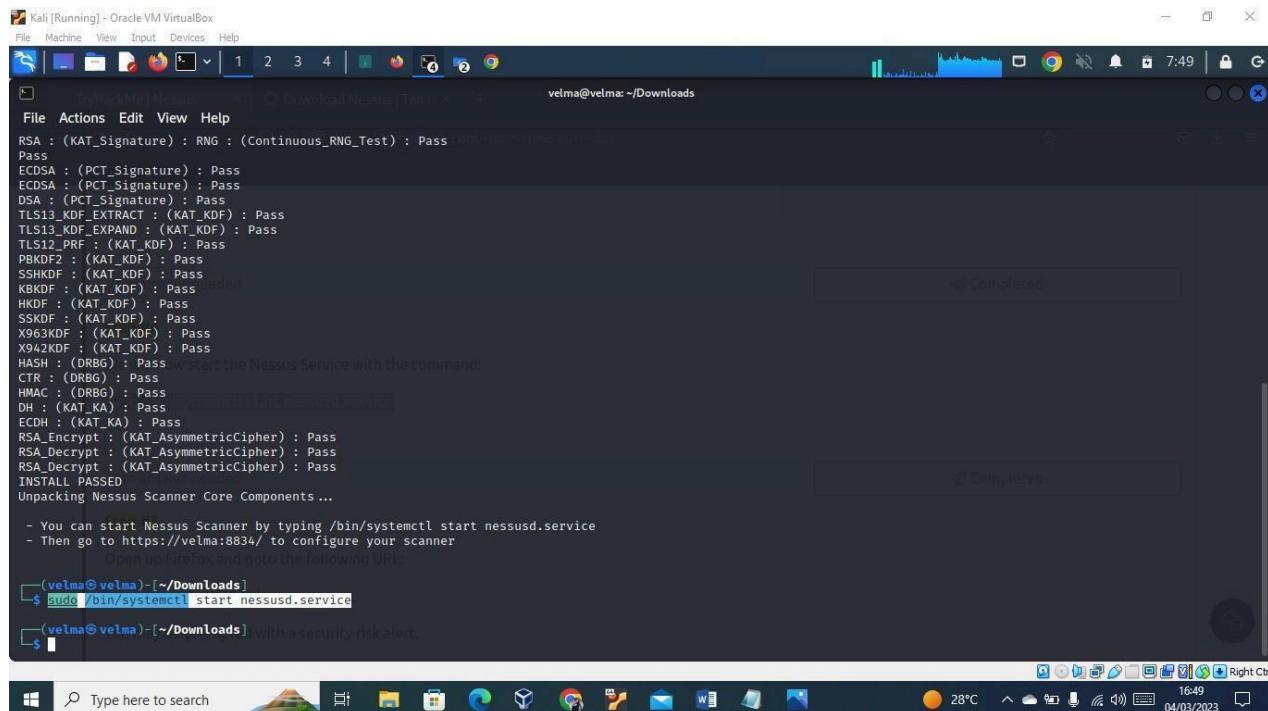


CYBER SHUJAA SECURITY ANALYST
COHORT 2 - 2024 MID EXAMINATION
PRACTICAL QUESTIONS
TIME ALLOWED: 2 HOURS
TOTAL: 30 MARKS

Instructions:

1. **Answer ALL questions**
2. The exam should **NOT be** worked on in groups or with assistance from others.
3. Use this file as your write-up reporting template as you complete each task outlined and answer the questions.
4. Rename this file with your full names and Cyber Shujaa ID.
5. Once you have completed your work, save the file and upload it for marking.
6. Before leaving the exam, ensure you have uploaded the correct file capturing all the work you have submitted for marking.
7. Ensure you compile a detailed report write-up that outlines your approach to addressing the various exam challenges. Ensure that your write up is authentic. Show screenshots of the working for all answers showing how you got your answers.
8. The screen shots should capture your full screen and display the command you ran to get the answer. Include a taskbar showing your machine taskbar and time stamp.



```

Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
velma@velma: ~/Downloads
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X9A2KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
Now start the Nessus Service with the command:
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components ...
Completed.
Completed.
Completed.

You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
Then go to https://velma:8834/ to configure your scanner
Open up Firefox and go to the following URL:
(velma@velma) ~ /Downloads
$ sudo /bin/systemctl start nessusd.service
(velma@velma) ~ /Downloads with a security risk alert.

Type here to search 28°C 16:49 Right Ctrl

```

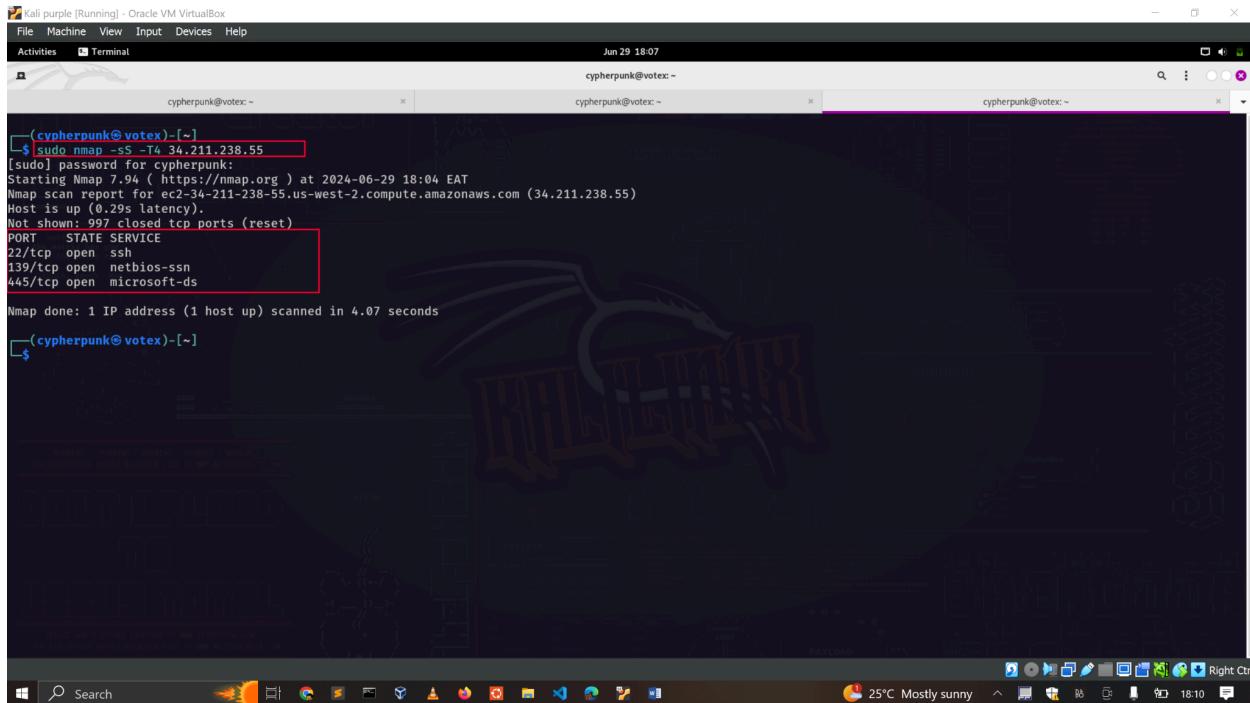
MID EXAM PRACTICAL (30 marks)

Retrieve the credentials required to log on to the provided server and answer the questions below.

QUESTIONS

- Conduct an Nmap scan on the provided Linux machine. Identify the open ports. (2 mks)

- Port 22,139,445.



```
(cyberpunk@votex)-[~]
$ sudo nmap -sS -T4 34.211.238.55
[sudo] password for cyberpunk:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-06-29 18:04 EAT
Nmap scan report for ec2-34-211-238-55.us-west-2.compute.amazonaws.com (34.211.238.55)
Host is up (0.29s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 4.07 seconds

```

- A service is running on more than one port of the system. What is the version of the service? (1 mk)

- Samba smbd 4.6.2

Kali purple [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Jun 29 18:27

```
(cyberpunk@votex)~$ nmap -sV -T4 34.211.238.55
You requested a scan type which requires root privileges.
QUITTING!
```

```
(cyberpunk@votex)~$ sudo nmap -sV -T4 34.211.238.55
[sudo] password for cyberpunk:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-06-29 18:26 EAT
Nmap scan report for ec2-34-211-238-55.us-west-2.compute.amazonaws.com (34.211.238.55)
Host is up (0.28s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 9.0p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)
139/tcp   open  netbios-ssn  Samba smbd 4.6.2
445/tcp   open  netbios-ssn  Samba smbd 4.6.2
Service Info: OS: 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 20.65 seconds
```

```
(cyberpunk@votex)~$
```

23°C Sunny 18:30 Right Ctrl

3. What is the netbios name of the server? (1 mk)

The server has no NetBios name since it is a Linux Machine. NetBios Names are assigned to Windows Computers only.

Kali purple [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Jun 29 18:25

```
(cyberpunk@votex)~$ nbtscan 34.211.238.55
Doing NBT name scan for addresses from 34.211.238.55
```

IP address	NetBIOS Name	Server	User	MAC address
34.211.238.55	<server>			00:00:00:00:00:00

```
(cyberpunk@votex)~$ nmap -A 34.211.238.55 -p 139,445
Starting Nmap 7.94 ( https://nmap.org ) at 2024-06-29 18:21 EAT
Nmap scan report for ec2-34-211-238-55.us-west-2.compute.amazonaws.com (34.211.238.55)
Host is up (0.29s latency).

PORT      STATE SERVICE      VERSION
139/tcp   open  netbios-ssn  Samba smbd 4.6.2
445/tcp   open  netbios-ssn  Samba smbd 4.6.2

Host script results:
|_nbstat: NetBIOS name: , NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb2-time:
|   date: 2024-06-29T15:24:40
|_ start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_   Message signing enabled but not required
|_clock-skew: 3m15s

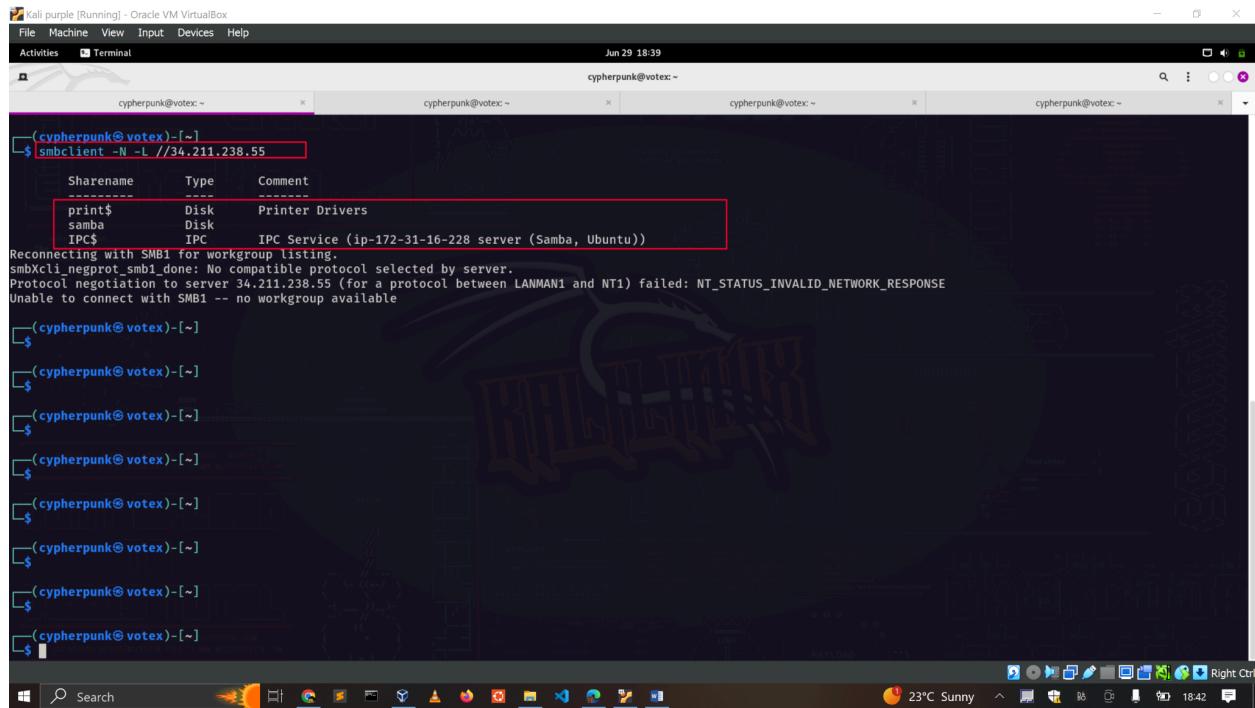
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.62 seconds
```

```
(cyberpunk@votex)~$
```

23°C Sunny 18:28 Right Ctrl

4. Using smbclient tool identify the available shares (2 mks)

- The available shares are 3, the print\$, samba and IPC\$ share.



```
(cyberpunk@votex) [~]
$ smbclient -N -L //34.211.238.55

Sharename      Type      Comment
-----        ----      -----
print$        Disk      Printer Drivers
samba         Disk      Samba Share
IPC$          IPC       IPC Service (ip-172-31-16-228 server (Samba, Ubuntu))

Reconnecting with SMB1 for workgroup listing.
smbcli_negprot_smb1 done: No compatible protocol selected by server.
Protocol negotiation to server 34.211.238.55 (for a protocol between LANMAN1 and NT1) failed: NT_STATUS_INVALID_NETWORK_RESPONSE
Unable to connect with SMB1 -- no workgroup available

(cyberpunk@votex) [~]
$ 
```

5. How many hidden shares are among the identified shares above. Name them. (2 mks)

- From the screenshot above, there are two hidden shares. The ones appended with the \$ at the end, that is, print\$ and IPC\$

Note: The screenshots are large since I took them using flameshot. I will use the above screenshot for this question to keep my report within the filesize limit.

6. What is the name of the share that is accessible? (1 mk)

- The samba share is the one accessible.

Kali purple [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Jun 29 18:41

```

smb: \> exit
(cyberpunk@votex)-[~]
$ smbclient //34.211.238.55/print
Password for [WORKGROUP/cyberpunk]:
tree connect failed: NT_STATUS_ACCESS_DENIED

(cyberpunk@votex)-[~]
$ smbclient //34.211.238.55/samba
Password for [WORKGROUP/cyberpunk]:
Try "help" to get a list of possible commands.
smb: \> ls -la
NT_STATUS_NO_SUCH_FILE listing \-la
smb: \> ls
.
D 0 Sat Jun 29 11:22:42 2024
D 0 Sat Jun 29 11:22:42 2024
0JkVXMn0.exe A 56320 Sat Jun 29 11:03:46 2024
hrvApRuZ.exe A 56320 Sat Jun 29 10:48:07 2024
cVAwCWR.exe A 56320 Sat Jun 29 11:20:58 2024
GspCKHy.exe A 56320 Sat Jun 29 02:04:32 2024
BtSBijDA.exe A 56320 Sat Jun 29 10:49:51 2024
XtStdzsk.exe A 56320 Sat Jun 29 11:22:42 2024
IdryvSTI.exe A 56320 Sat Jun 29 02:06:16 2024
XpVyaHE.exe A 56320 Sat Jun 29 07:29:57 2024
wZeUhZQ.exe A 56320 Sat Jun 29 11:05:30 2024
password_audit D 0 Fri Jun 28 23:42:42 2024
JGTFezGm.exe A 56320 Sat Jun 29 07:31:41 2024

7034376 blocks of size 1024. 4516836 blocks available
smb: \> cd password_audit\> ls
.
D 0 Fri Jun 28 23:42:42 2024
D 0 Sat Jun 29 11:22:42 2024
unzipme.tar N 10240 Fri Jun 28 23:42:42 2024

7034376 blocks of size 1024. 4516828 blocks available
smb: \password_audit\>
```

23°C Sunny 18:44 Right Ctrl

7. Access the share using null authentication, what is the folder's name discovered within the share? (2 marks)

- Foldername is **password_audit** as highlighted above

8. Download the files inside the folder and read the contents. What is the flag? (2 mks)

Kali purple [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Jun 29 18:45

```

(cyberpunk@votex)-[~]
$ smbclient //34.211.238.55/samba
Password for [WORKGROUP/cyberpunk]:
Try "help" to get a list of possible commands.
smb: \> ls -la
NT_STATUS_NO_SUCH_FILE listing \-la
smb: \> ls
.
D 0 Sat Jun 29 11:22:42 2024
D 0 Sat Jun 29 11:22:42 2024
0JkVXMn0.exe A 56320 Sat Jun 29 11:03:46 2024
hrvApRuZ.exe A 56320 Sat Jun 29 10:48:07 2024
cVAwCWR.exe A 56320 Sat Jun 29 11:20:58 2024
GspCKHy.exe A 56320 Sat Jun 29 02:04:32 2024
BtSBijDA.exe A 56320 Sat Jun 29 10:49:51 2024
XtStdzsk.exe A 56320 Sat Jun 29 11:22:42 2024
IdryvSTI.exe A 56320 Sat Jun 29 02:06:16 2024
XpVyaHE.exe A 56320 Sat Jun 29 07:29:57 2024
wZeUhZQ.exe A 56320 Sat Jun 29 11:05:30 2024
password_audit D 0 Fri Jun 28 23:42:42 2024
JGTFezGm.exe A 56320 Sat Jun 29 07:31:41 2024

7034376 blocks of size 1024. 4516836 blocks available
smb: \> cd password_audit\> ls
.
D 0 Fri Jun 28 23:42:42 2024
D 0 Sat Jun 29 11:22:42 2024
unzipme.tar N 10240 Fri Jun 28 23:42:42 2024

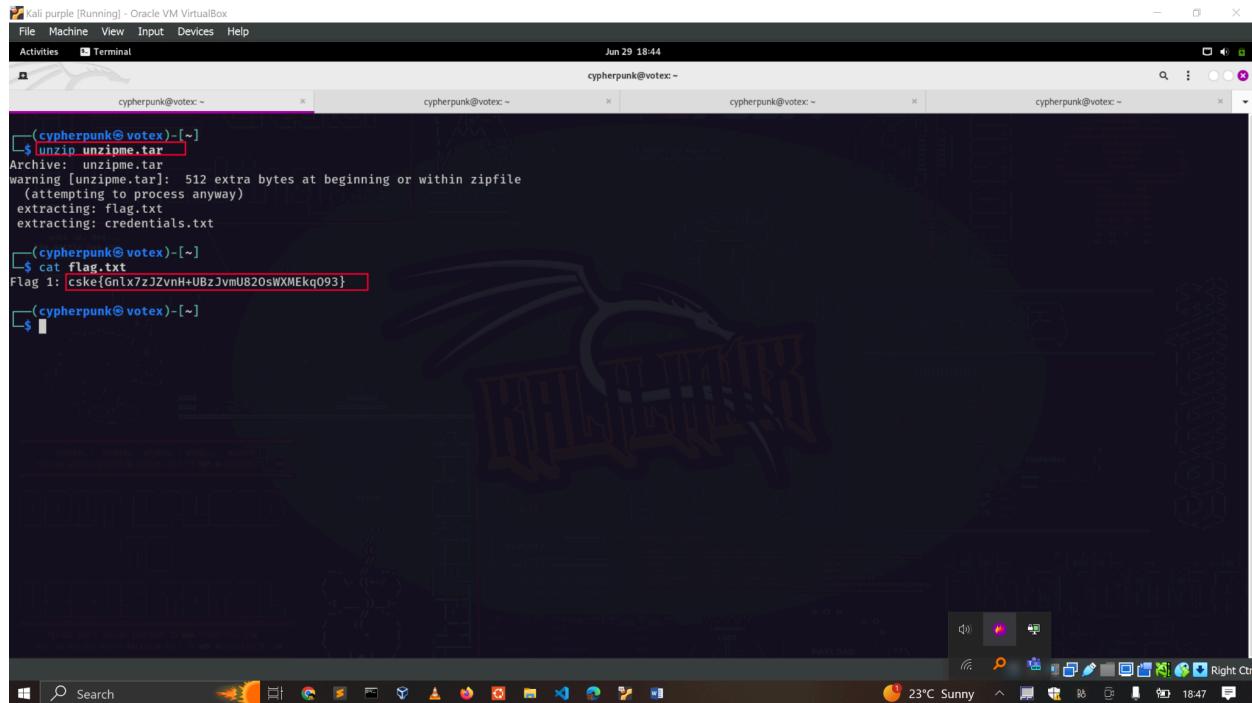
7034376 blocks of size 1024. 4516828 blocks available
smb: \password_audit\> get unzipme.tar
```

Downloaded the zip file

getting file \password_audit\unzipme.tar of size 10240 as unzipme.tar (8.3 KiloBytes/sec) (average 8.3 KiloBytes/sec)
smb: \password_audit\>
smb: \password_audit\>
smb: \password_audit\>
smb: \password_audit\>
smb: \password_audit\>

21°C Mostly clear 18:48 Right Ctrl

- After downloading the file using the get command and unzipped it, we can see the flag highlighted below.



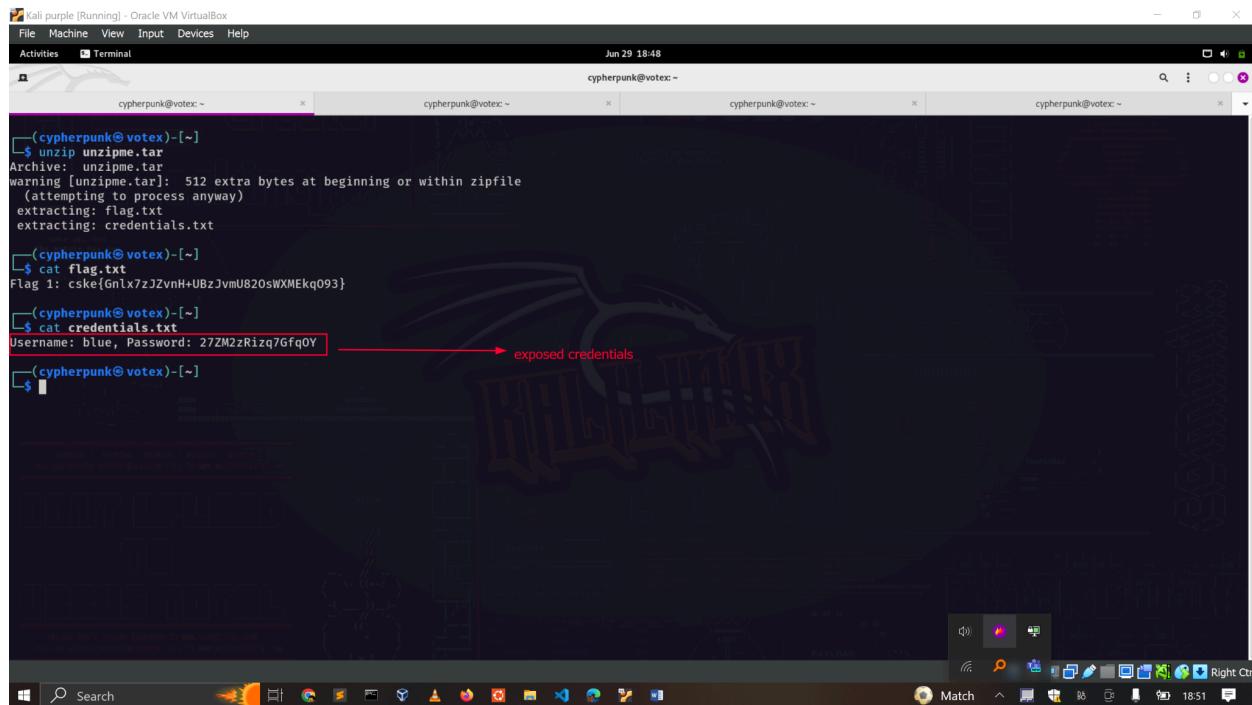
```
(cyberpunk@votex) ~]$ unzip unzipme.tar
Archive: unzipme.tar
warning [unzipme.tar]: 512 extra bytes at beginning or within zipfile
(attempting to process anyway)
extracting: flag.txt
extracting: credentials.txt

(cyberpunk@votex) ~]$ cat flag.txt
Flag 1: cske{GnIx7zJZvnH+UBzJvmU82OsWXMEkq093}

(cyberpunk@votex) ~]$
```

9. What is the exposed username and password? (1 mk)

- The exposed username and password are highlighted below.



```
(cyberpunk@votex) ~]$ unzip unzipme.tar
Archive: unzipme.tar
warning [unzipme.tar]: 512 extra bytes at beginning or within zipfile
(attempting to process anyway)
extracting: flag.txt
extracting: credentials.txt

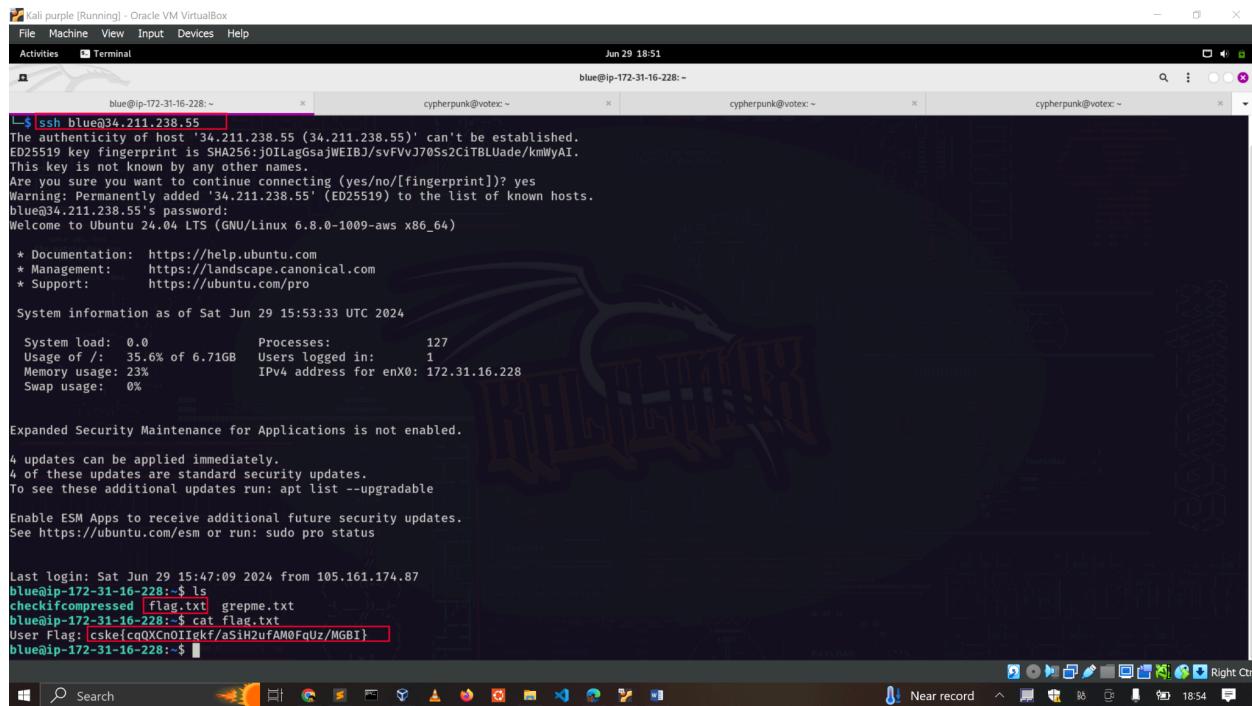
(cyberpunk@votex) ~]$ cat flag.txt
Flag 1: cske{GnIx7zJZvnH+UBzJvmU82OsWXMEkq093}

(cyberpunk@votex) ~]$ cat credentials.txt
Username: blue, Password: 27ZM2zRizq7GfqOY
→ exposed credentials

(cyberpunk@votex) ~]$
```

10. Ssh into the machine and retrieve the flag in the user's home directory. (1 mk)

- The flag is highlighted in the screenshot below.



Kali purple [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Jun 29 18:51

blue@ip-172-31-16-228: ~ cypherpunk@votex: ~ cypherpunk@votex: ~ cypherpunk@votex: ~

```
blue@ip-172-31-16-228: ~ ssh blue@34.211.238.55
The authenticity of host '34.211.238.55 (34.211.238.55)' can't be established.
ED25519 key fingerprint is SHA256:j0IlagGsajWEIB0/svFVJ70Ss2cItBLUade/kmWYAI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '34.211.238.55' (ED25519) to the list of known hosts.
blue@34.211.238.55's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1009-aws x86_64)

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

System information as of Sat Jun 29 15:53:33 UTC 2024

System load: 0.0 Processes: 127
Usage of /: 35.6% of 6.71GB Users logged in: 1
Memory usage: 23% IPv4 address for enX0: 172.31.16.228
Swap usage: 0%

Expanded Security Maintenance for Applications is not enabled.

4 updates can be applied immediately.
4 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Sat Jun 29 15:47:09 2024 from 105.161.174.87
blue@ip-172-31-16-228: ~ ls
checkifcompressed flag.txt grepme.txt
blue@ip-172-31-16-228: ~ cat flag.txt
User Flag: [cskefcQXcn0IIegf/aSiH2ufAM0FqUz/MGBI]
blue@ip-172-31-16-228: ~
```

Search Near record 18:54 Right Ctrl

11. Using grep retrieve a flag hidden in the grepme.txt within the user's home directory (2 mks)

- From the command `grep -i cake grepme.txt` we can retrieve the highlighted flag as shown below.

Kali purple [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Jun 29 18:52

blue@ip-172-31-16-228:~ cypherpunk@votex:~ cypherpunk@votex:~ cypherpunk@votex:~

```
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '34.211.238.55' (ED25519) to the list of known hosts.
blue@34.211.238.55's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-1009-aws x86_64)

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

System information as of Sat Jun 29 15:53:33 UTC 2024

 System load: 0.0 Processes: 127
 Usage of /: 35.6% of 6.71GB Users logged in: 1
 Memory usage: 23% IPv4 address for enX0: 172.31.16.228
 Swap usage: 0%

Expanded Security Maintenance for Applications is not enabled.

4 updates can be applied immediately.
4 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Sat Jun 29 15:47:09 2024 from 105.161.174.87
blue@ip-172-31-16-228:~$ ls
checkifcompressed flag.txt grepme.txt
blue@ip-172-31-16-228:~$ cat flag.txt
User Flag: cske{cqQXn0Ilgkf/aSiH2ufAM0FqUz/MGBI}
blue@ip-172-31-16-228:~$ grep -i cske grepme.txt
      one of the arguments, input will be taken from stdin. cske{you_are_a_grep_wizzard}
blue@ip-172-31-16-228:~$ 
blue@ip-172-31-16-228:~$ 
```

Search 21°C Mostly clear 18:55 Right Ctrl

12. Using any editor installed on the server, create a file with the content cybershujaa_exam, save the file, and retrieve the flag. (2 mks)

- After creating a file name **newfile.txt** the flag pops up as shown below.

Kali purple [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Jun 29 18:54

blue@ip-172-31-16-228:~ cypherpunk@votex:~ cypherpunk@votex:~ cypherpunk@votex:~

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

System information as of Sat Jun 29 15:53:33 UTC 2024

 System load: 0.0 Processes: 127
 Usage of /: 35.6% of 6.71GB Users logged in: 1
 Memory usage: 23% IPv4 address for enX0: 172.31.16.228
 Swap usage: 0%

Expanded Security Maintenance for Applications is not enabled.

4 updates can be applied immediately.
4 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

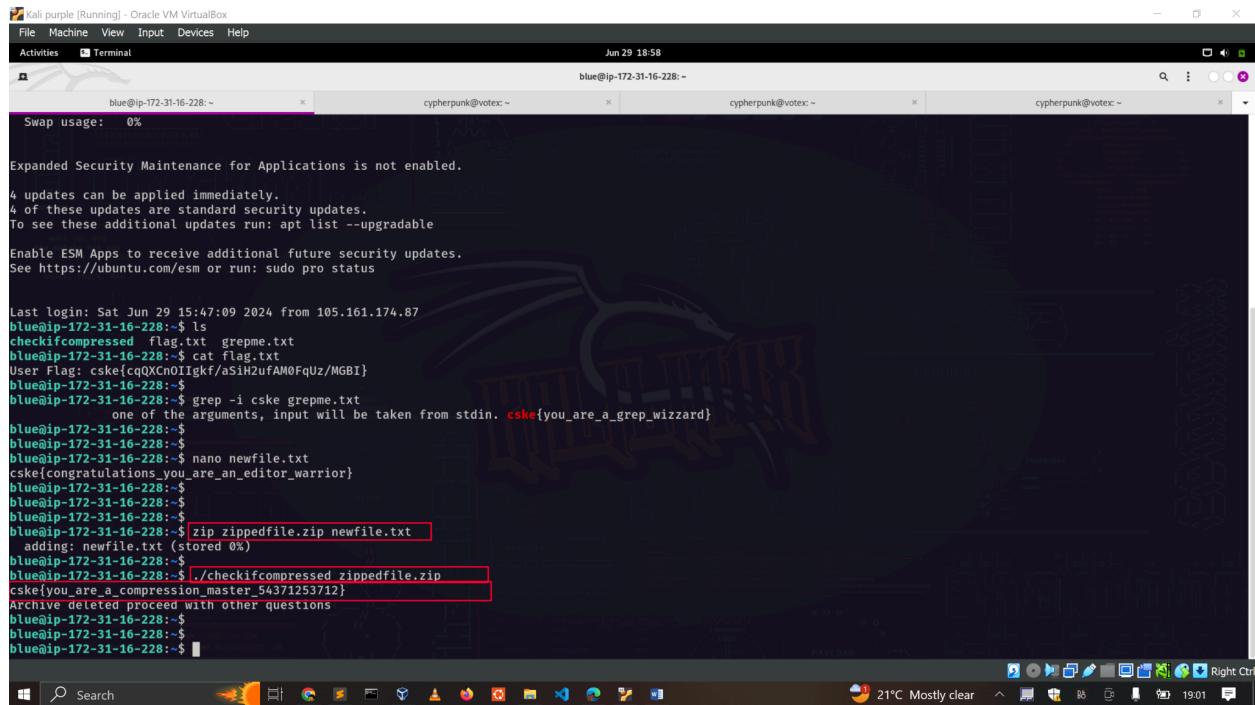
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Sat Jun 29 15:47:09 2024 from 105.161.174.87
blue@ip-172-31-16-228:~$ ls
checkifcompressed flag.txt grepme.txt
blue@ip-172-31-16-228:~$ cat flag.txt
User Flag: cske{cqQXn0Ilgkf/aSiH2ufAM0FqUz/MGBI}
blue@ip-172-31-16-228:~$ grep -i cske grepme.txt
      one of the arguments, input will be taken from stdin. cske{you_are_a_grep_wizzard}
blue@ip-172-31-16-228:~$ 
blue@ip-172-31-16-228:~$ nano newfile.txt
cske{congratulations_you_are_an_editor_warrior}
blue@ip-172-31-16-228:~$ 
blue@ip-172-31-16-228:~$ 
```

Ready for fun? Search 18:57 Right Ctrl

13. Using zip compress the file you have just created above, then run the binary in the user's home directory called "checkifcompressed" giving the name of your zip file as an argument. What is the flag? (4 mks)

- The command `zip zippedfile.zip newfile.txt` compresses our file.
- Running the binary to confirm compression reveals the flag.



```
Kali purple [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Jun 29 18:58
blue@ip-172-31-16-228:~ Swap usage: 0%
cypherpunk@votec:~ cypherpunk@votec:~ cypherpunk@votec:~

Expanded Security Maintenance for Applications is not enabled.

4 updates can be applied immediately.
4 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Sat Jun 29 15:47:09 2024 from 105.161.174.87
blue@ip-172-31-16-228:~$ ls
checkifcompressed flag.txt grepme.txt
blue@ip-172-31-16-228:~$ cat flag.txt
User Flag: cske{cuQXCnOIIgkf/asIH2ufAM0FqUz/MGBI}
blue@ip-172-31-16-228:~$ blue@ip-172-31-16-228:~$ grep -i cske grepme.txt
blue@ip-172-31-16-228:~$ one of the arguments, input will be taken from stdin. cske{you_are_a_grep_wizzard}
blue@ip-172-31-16-228:~$ blue@ip-172-31-16-228:~$ nano newfile.txt
cske{congratulations_you_are_an_editor_warrior}
blue@ip-172-31-16-228:~$ blue@ip-172-31-16-228:~$ blue@ip-172-31-16-228:~$ blue@ip-172-31-16-228:~$ blue@ip-172-31-16-228:~$ zip zippedfile.zip newfile.txt
adding: newfile.txt (stored 0%)
blue@ip-172-31-16-228:~$ blue@ip-172-31-16-228:~$ ./checkifcompressed zippedfile.zip
cske{you_are_a_compression_master_54371253712}
Archive deleted proceed with other questions
blue@ip-172-31-16-228:~$ blue@ip-172-31-16-228:~$ blue@ip-172-31-16-228:~$
```

14. A misconfiguration is on the shadow file allowing users to read its contents.

Retrieve both the password file `passwd` and the shadow file. Unshadow and crack using John. What is the root password? Use the provided wordlist. (5 mks) **HINT: use the format `--format=crypt`**

Kali purple [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Jun 29 19:30

```
(cyberpunk@votex)-[~]
$ unshadow passwd.txt shadow.txt > unshadowedhashes.txt
(cyberpunk@votex)-[~]
$ cat unshadowedhashes.txt
root:$y$j9T$Zbmn0eND1Ag9v724HaZl0$bQb1L2Met.TUeTYXims5Hnd9bNMdyzu7XwVt6r8Bh14:0:0:/root:/bin/bash

(cyberpunk@votex)-[~]
$ john --wordlist=Wordlist.txt unshadowed.txt --format=crypt
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1]:descrypt 2:md5crypt 3:unmd5 4:bcrypt 5:sha256crypt 6:sha512crypt) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Press wordlist (root)
1g 0:00:00:02 DONE (2024-06-29 19:30) 0.3597g/s 34.53p/s 34.53c/s 34.53c/s password..pimphard
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

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

Search 21°C Clear 19:33 Right Ctrl

15. Retrieve the root flag.txt from the root user's home directory. (2 mks)

Kali purple [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Terminal Jun 29 19:34

```
root@ip-172-31-16-228:~ cypherpunk@votex:~ cypherpunk@votex:~ cypherpunk@votex:~
```

```
systemd-network:x:998:998:systemd Network Management:/usr/sbin/nologin
systemd-timesyncd:x:996:996:systemd Time Synchronization:/usr/sbin/nologin
dhpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false
messagbus:x:101:101::/nonexistent:/usr/sbin/nologin
syslog:x:102:102::/nonexistent:/usr/sbin/nologin
systemd-resolve:x:991:991:systemd Resolver:/usr/sbin/nologin
uuid:x:103:103::/run/uuid:/usr/sbin/nologin
tss:x:104:104:TPM software stack,,,:/var/lib/tpm:/bin/false
sshd:x:105:65534:/run/sshd:/usr/sbin/nologin
polinate:x:106:1::/var/cache/polinate:/bin/false
tcpdump:x:107:108::/nonexistent:/usr/sbin/nologin
landscape:x:108:109::/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:990:990:Firmware update daemon:/var/lib/fwupd:/usr/sbin/nologin
polkitd:x:989:989:User for polkitd:/usr/sbin/nologin
ec2-instance-connect:x:109:65534:/nonexistent:/usr/sbin/nologin
chrony:x:110:112:chrony daemon,,,:/var/lib/chrony:/usr/sbin/nologin
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
blue:x:1001:1001:/home/blue:/bin/bash
blue@ip-172-31-16-228:~$ john -h
Command 'john' not found, but can be installed with:
snap install john-the-ripper # version roll-off fed2, or
apt install john # version 1.9.0-2
See 'snap info john-the-ripper' for additional versions.
blue@ip-172-31-16-228:~$ blue@ip-172-31-16-228:~$ blue@ip-172-31-16-228:~$ su root
Password:
root@ip-172-31-16-228:/home/blue# cd ~
root@ip-172-31-16-228:~# ls
flag.txt flag_I_am_the_flag flag_I_am_the_flag.sh flag_and_password.txt nohup.out set.zip setup snap
root@ip-172-31-16-228:~# cat flag.txt
Root Flag: cske9ytCVthOyweFhwmtfEvNTaV5J5Q+2ldj
```

Search 21°C Clear 19:37 Right Ctrl

