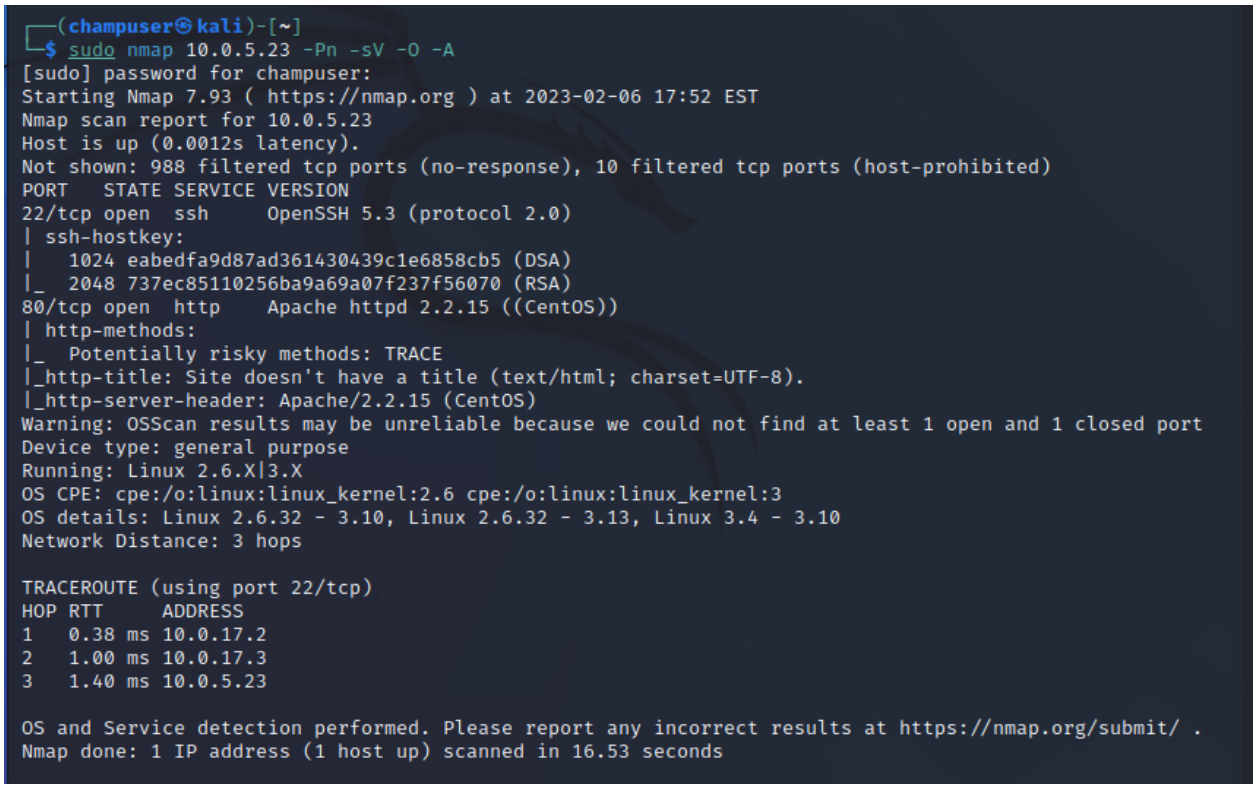
David Thomsen
Max Gallagher

Deliverable 1. Provide a screenshot of your team's version detection scan(s).

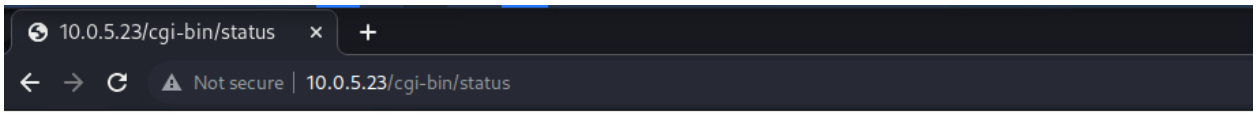


```
┌──(champuser㉿kali)-[~]
└─$ sudo nmap 10.0.5.23 -Pn -sV -O -A
[sudo] password for champuser:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-06 17:52 EST
Nmap scan report for 10.0.5.23
Host is up (0.0012s latency).
Not shown: 988 filtered tcp ports (no-response), 10 filtered tcp ports (host-prohibited)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|   1024 eabedfa9d87ad361430439c1e6858cb5 (DSA)
|_  2048 737ec85110256ba9a69a07f237f56070 (RSA)
80/tcp open  http    Apache httpd 2.2.15 ((CentOS))
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-server-header: Apache/2.2.15 (CentOS)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10, Linux 2.6.32 - 3.13, Linux 3.4 - 3.10
Network Distance: 3 hops

TRACEROUTE (using port 22/tcp)
HOP RTT     ADDRESS
1   0.38 ms 10.0.17.2
2   1.00 ms 10.0.17.3
3   1.40 ms 10.0.5.23

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.53 seconds
```

Deliverable 2. Examine any applications that are publicly accessible. What did you find?




hostname:cupcake uptime: 17:57:16 up 32 days, 9:36, 0 users, load average: 0.00, 0.00, 0.00

```
┌──(champuser㉿kali)-[~]
└─$ wget http://10.0.5.23
--2023-02-06 17:56:53--  http://10.0.5.23/
Connecting to 10.0.5.23:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 53 [text/html]
Saving to: 'index.html'

index.html                  100%[=========================>]      53  --.-KB/s    in 0s

2023-02-06 17:56:53 (1.92 MB/s) - 'index.html' saved [53/53]
```

```
┌──(champuser㉿kali)-[~]
└─$ cat index.html
<a href="../cgi-bin/status">Server Status Report</a>
```

Deliverable 3. You should have the versions of at least two applications. Go ahead and hit the internet and see if your group can find:

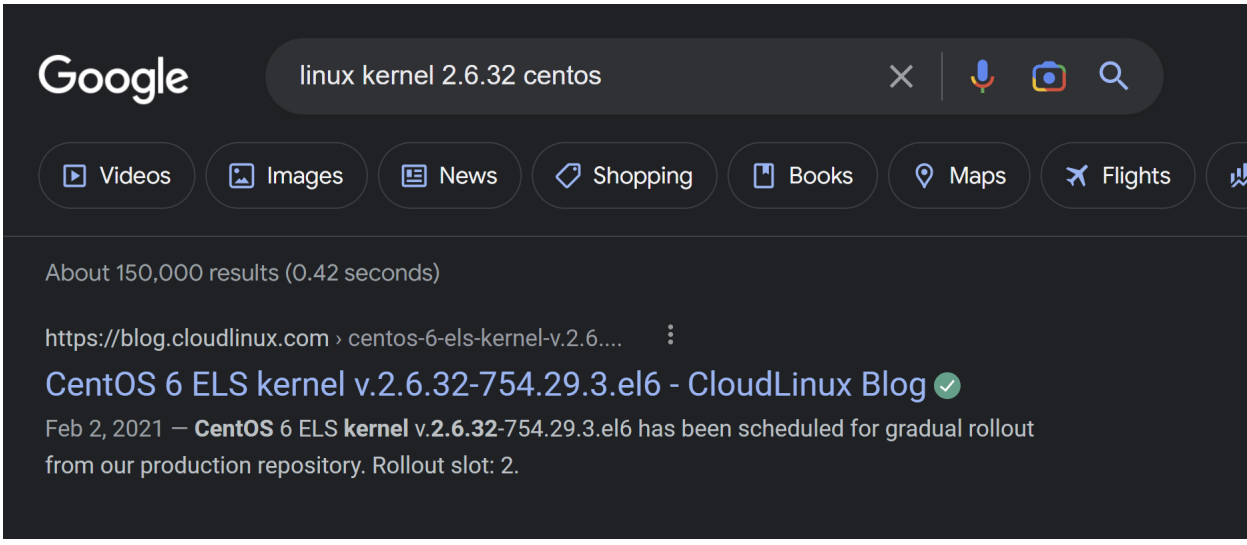
1. The operating system (this is easy)

```
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10, Linux 2.6.32 - 3.13, Linux 3.10, Linux 3.4 - 3.
10
```

2. release (a bit harder).
    a. Centos 6~
    b.

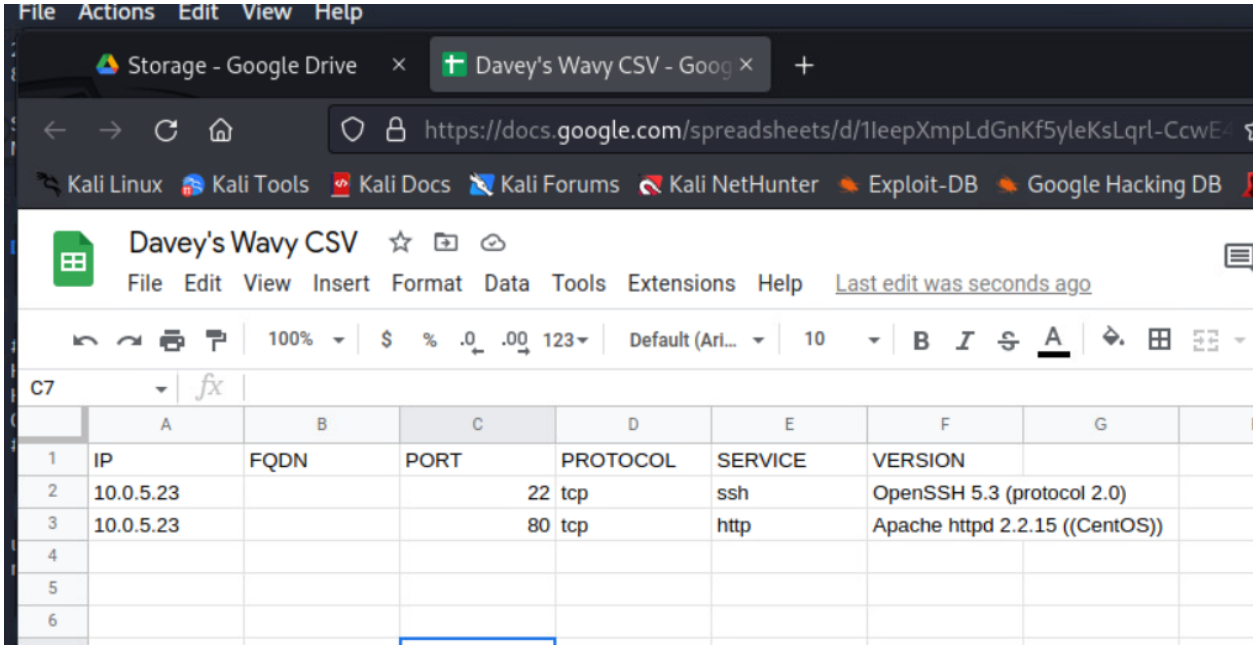
```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|   1024 eabedfa9d87ad361430439c1e6858cb5 (DSA)
|_  2048 737ec85110256ba9a69a07f237f56070 (RSA)
80/tcp open  http    Apache httpd 2.2.15 ((CentOS))
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Site doesn't have a title (text/html;
|_http-server-header: Apache/2.2.15 (CentOS)
Warning: OSScan results may be unreliable because we
pen and 1 closed port
```

    c.
    d.

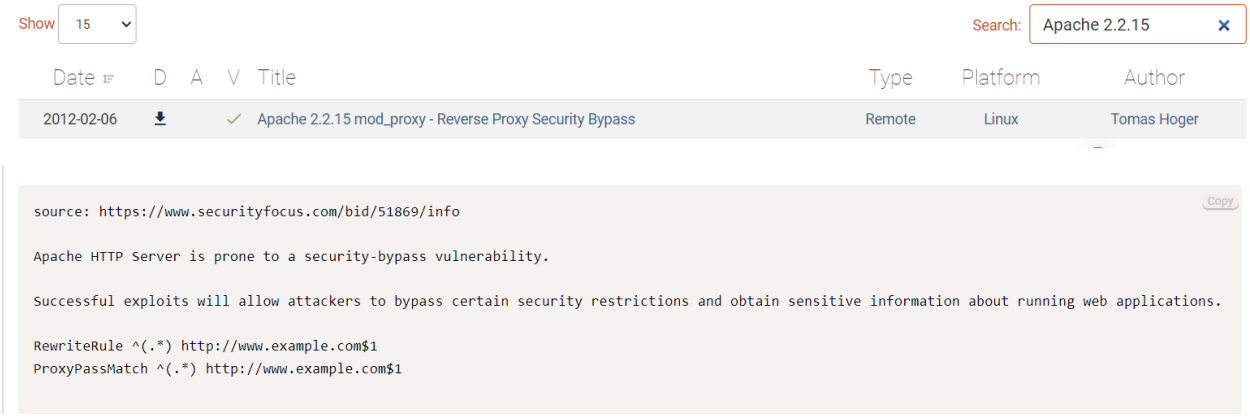


3. What did you find and how did you find it? Be prepared to share your findings with the rest of the class.
    a. (**Shared in class**)

Deliverable 4. Provide a screenshot similar to the one below that shows your exported google sheet of nmap scan data against cupcake. Note, the scan in the demo did not show version detection. See if you can figure out how to do that. You will have at least two ports.



Deliverable 5. What potential remote vulnerabilities did your team find?




**https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/version_id-459994/Apache-Http-Server-2.2.15.html**

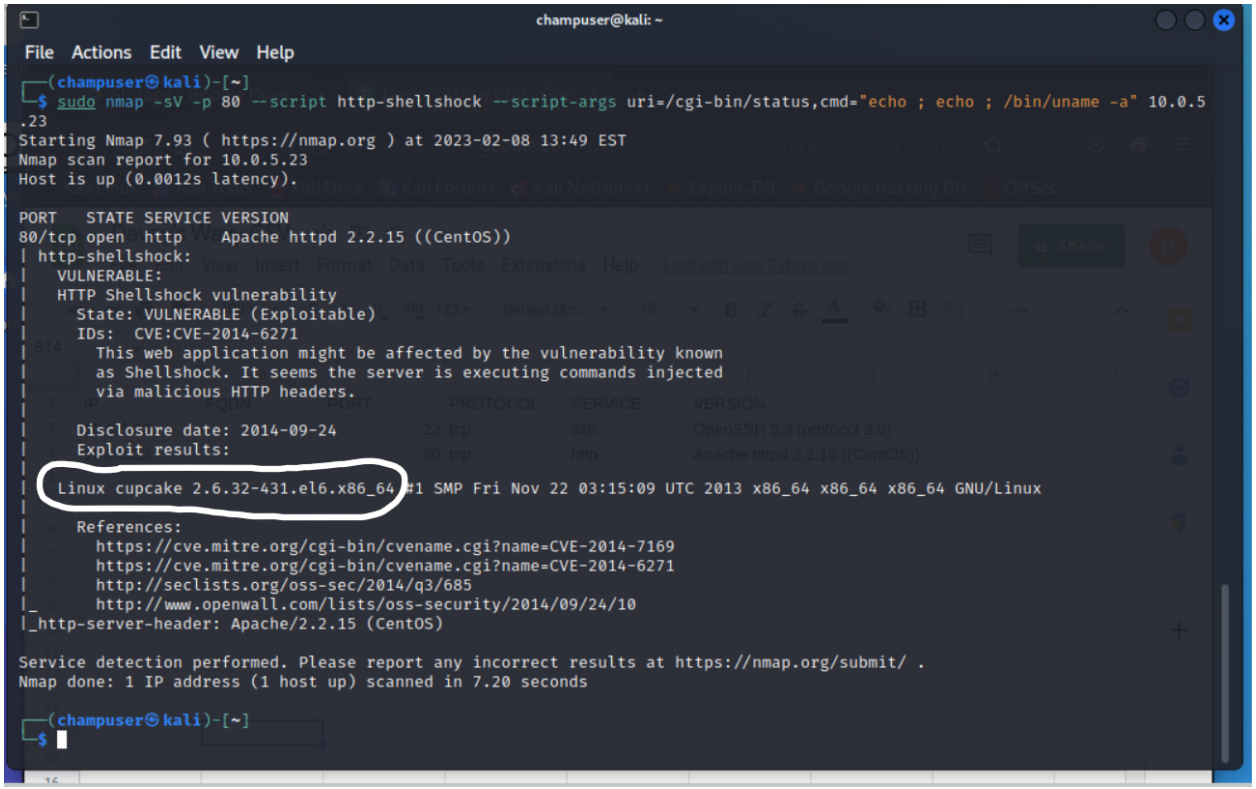
**https://www.cvedetails.com/vulnerability-list/vendor_id-97/product_id-585/version_id-462753/Openbsd-Openssh-5.3.html**

- **The First link as well as the screenshot attached are exploits that relate to the Apache 2.2.15 vulnerabilities. There were multiple different vulnerabilities that were found and the link rates them based on how much potential impact they can have on a system. This is similar to OpenSSH 5.3 where there is a list of known exploits that are all ranked based on how much damage can be done to the PC being exploited.**
- **The first screenshot shows an exploit with Apache 2.2.15 that allows the person using the exploit to bypass security on files within the directory of the apache web server.**

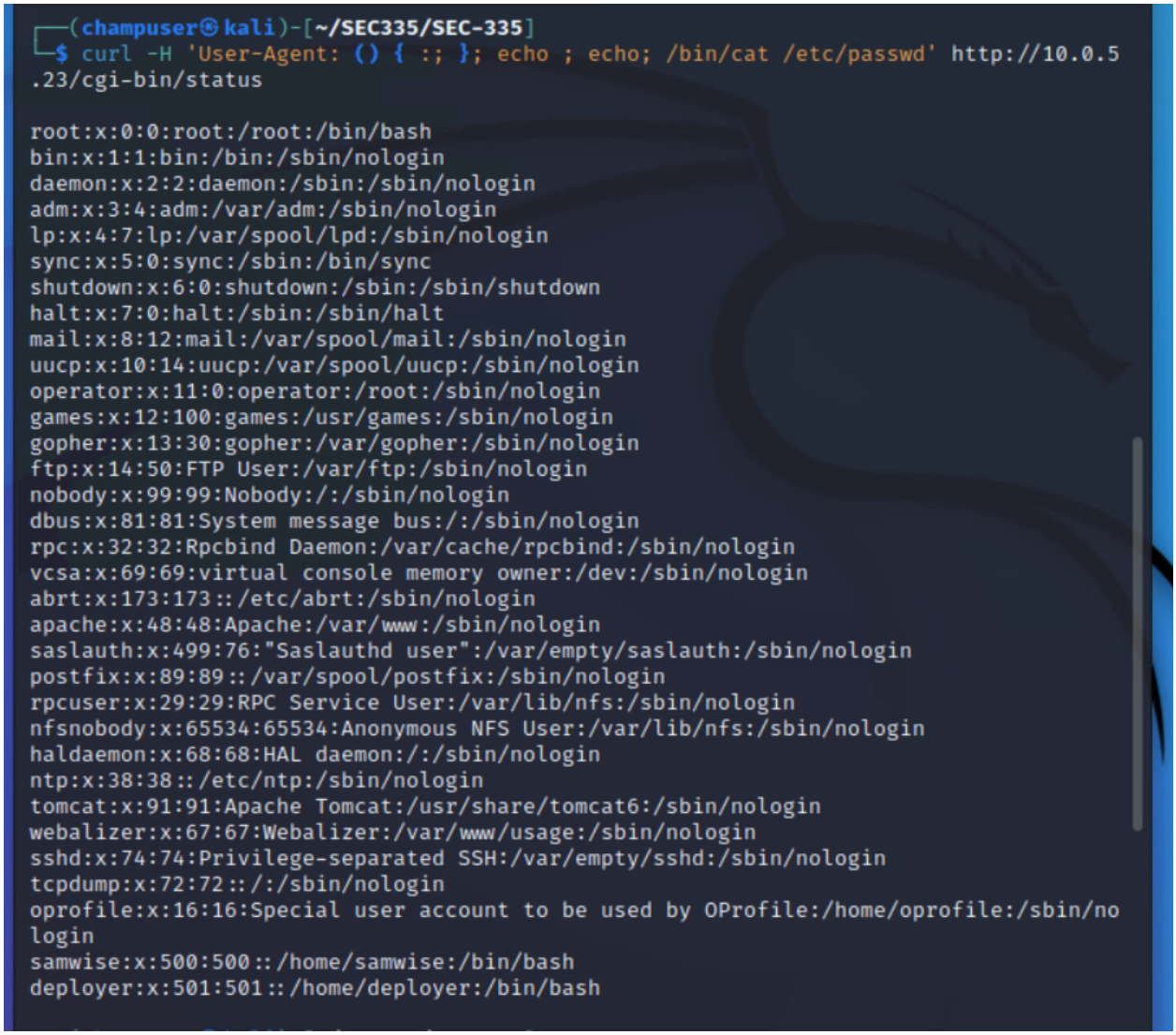
---

David Thomsen

Deliverable 6. Using the following screenshot as a point of departure. Determine what the target's running kernel version (you would use the uname command for this). Provide a screenshot that shows the major and minor release of the kernel.

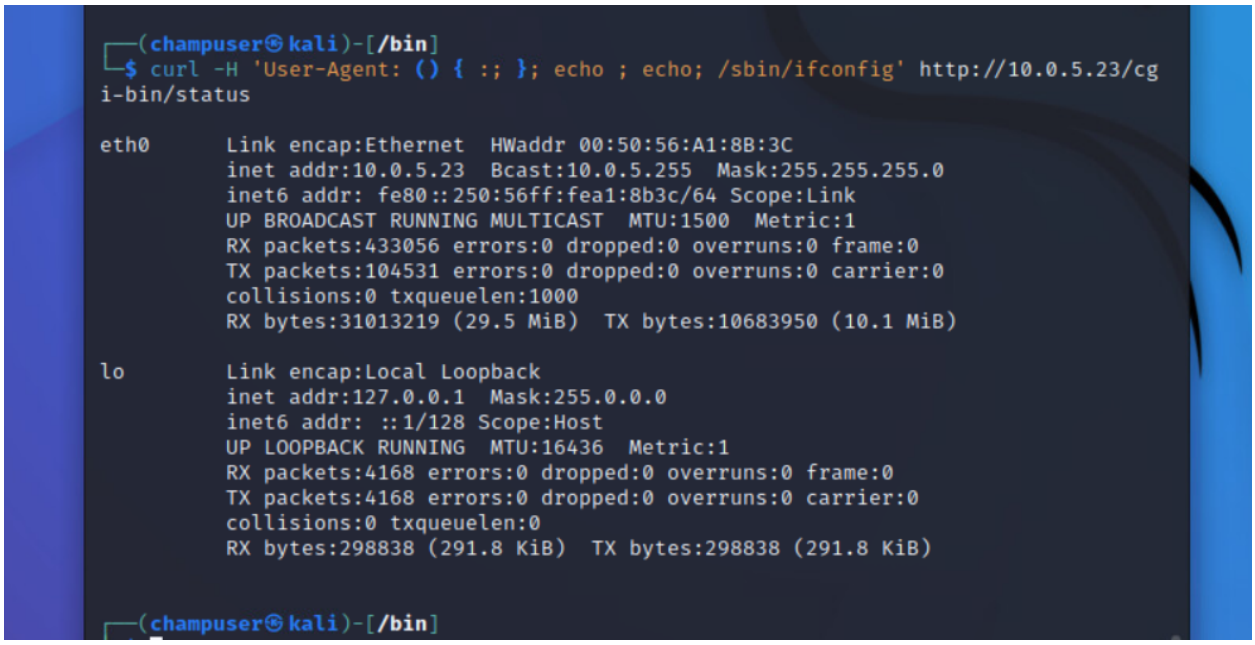


Deliverable 7. The following technique exposes the OS release. Show similar screenshots that show:

- the contents of /etc/passwd
- 

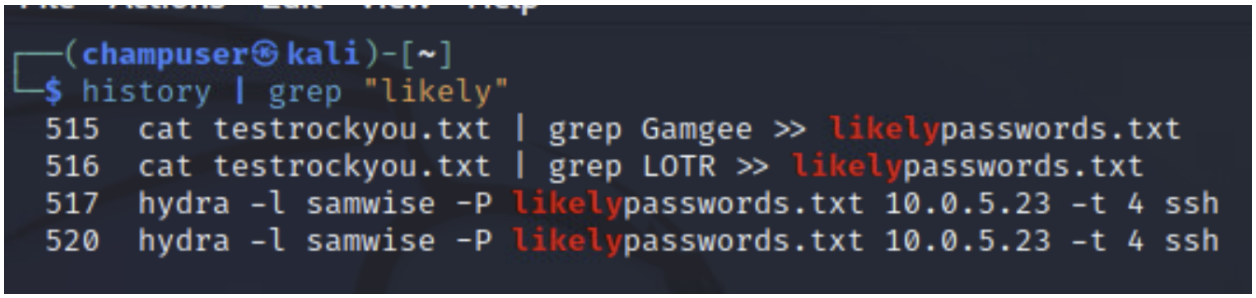
- the code behind the status cgi

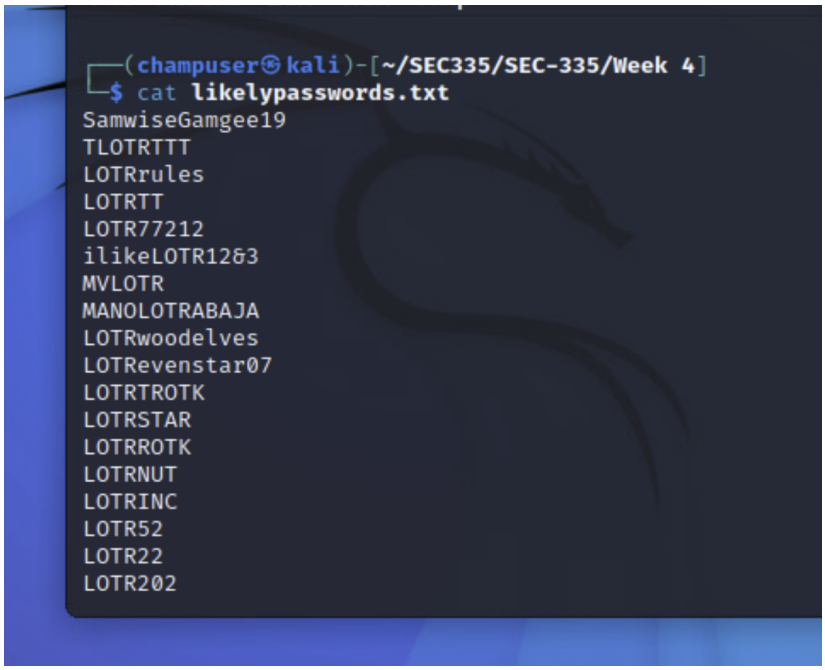
- 

- the results of running ifconfig
- 

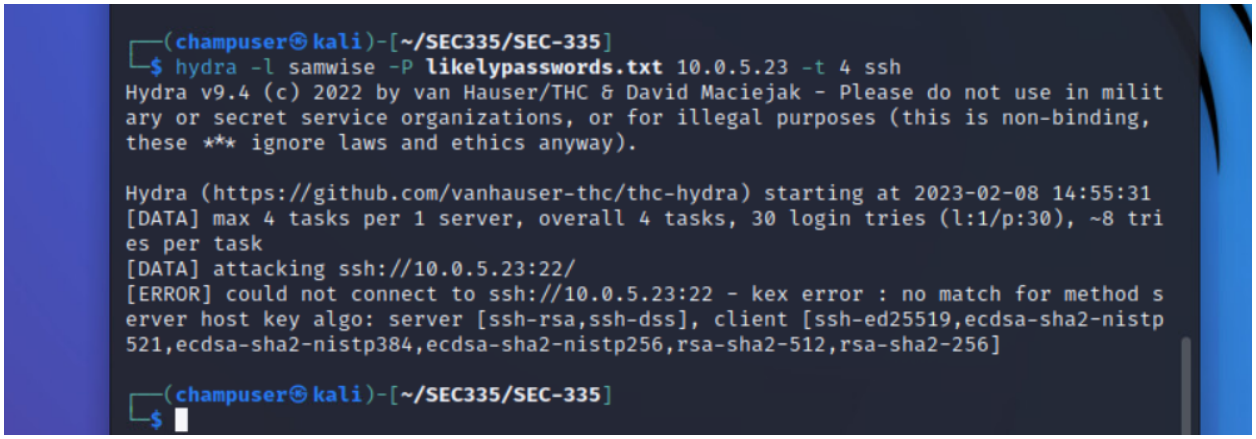
- https://askubuntu.com/questions/120628/ifconfig-command-ifconfig-is-available-in-sbin-ifconfig

Deliverable 8. Armed with the contents of /etc/passwd, let's see if we can build a list of likely passwords for the target account. You should end up with 28 passwords in your list. Provide a screenshot that shows how you generated the list as well as the list contents

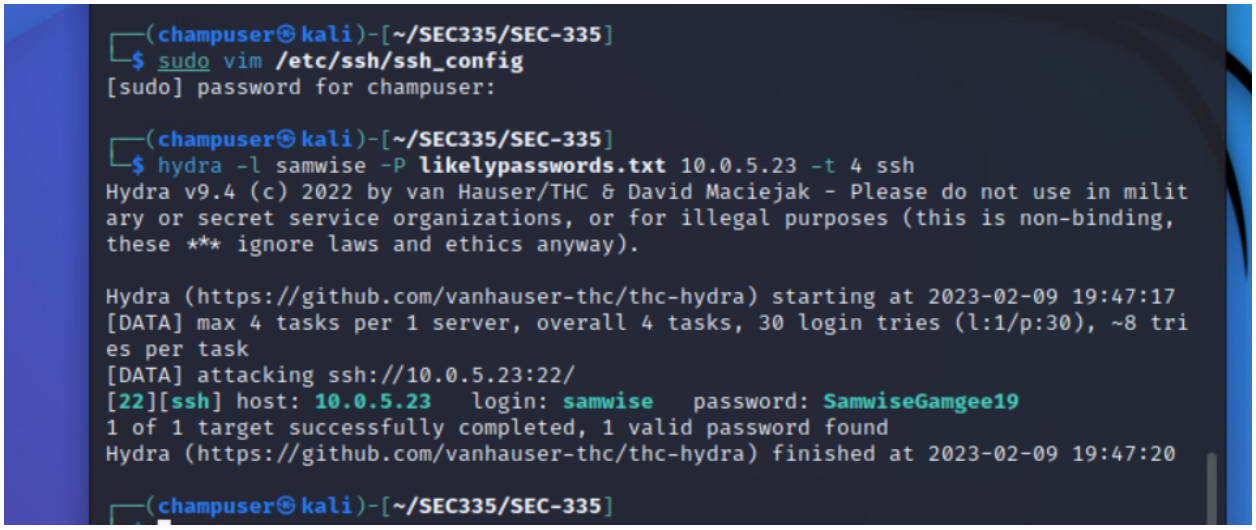


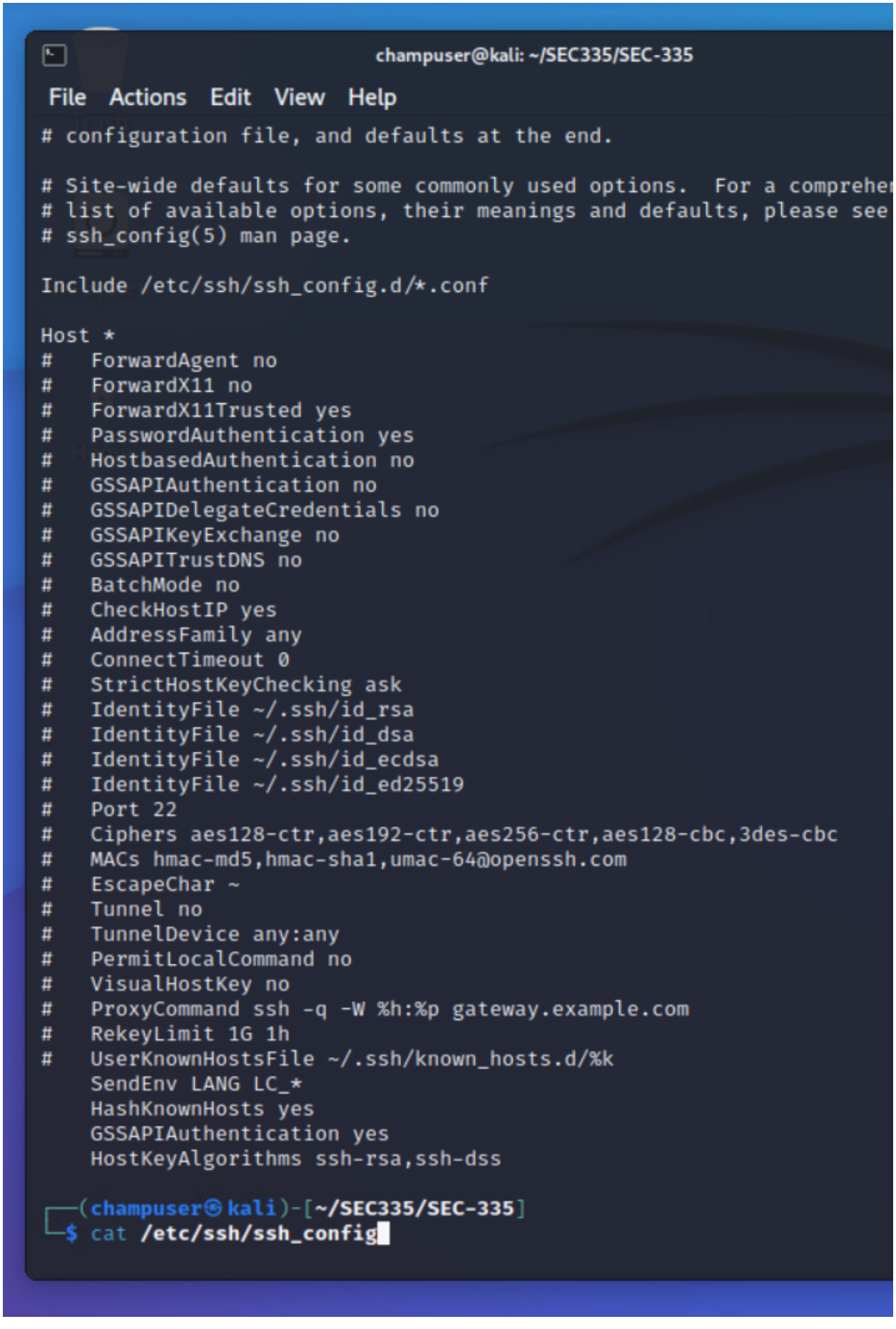



Deliverable 9. Show a screenshot of your hydra session as well as a ssh login session using the targeted account. Also dump the contents of user-flag.txt using cat or more.

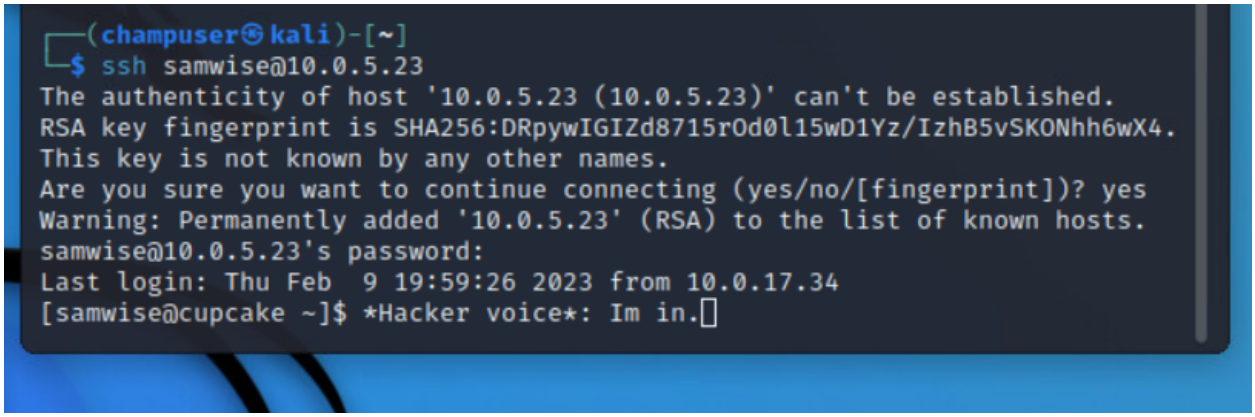


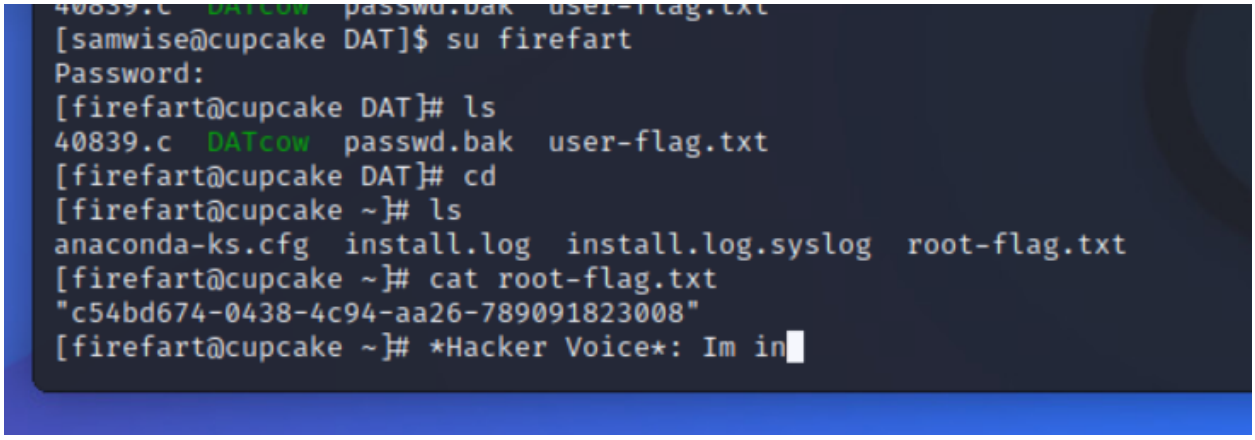

- Error due to the server being down. Same command shown working below with an additional fix (on Git under *Troubles Encountered*)



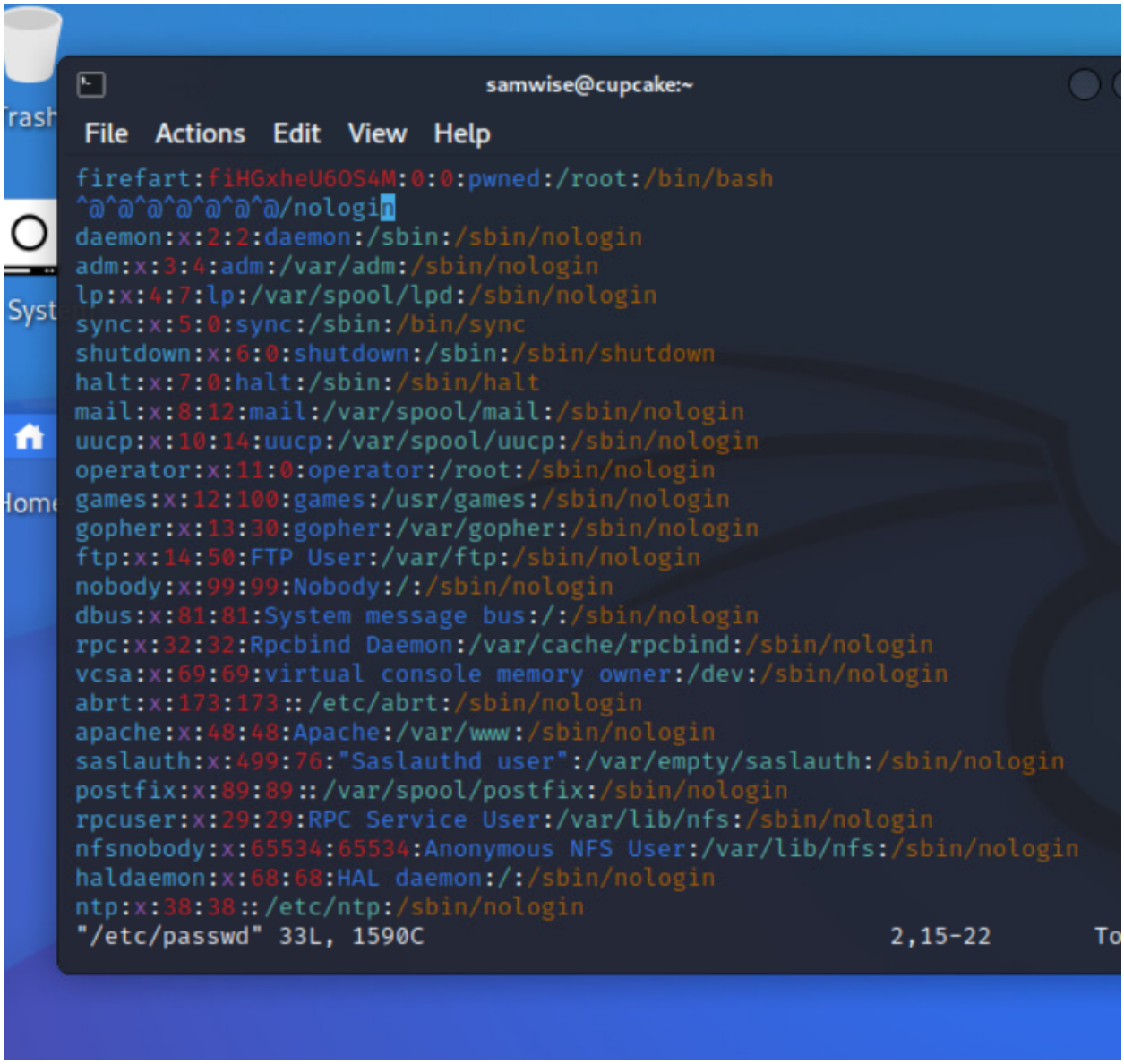

champuser@kali: ~/SEC335/SEC-335
File Actions Edit View Help
# configuration file, and defaults at the end.
# Site-wide defaults for some commonly used options. For a compreher
# list of available options, their meanings and defaults, please see
# ssh_config(5) man page.
Include /etc/ssh/ssh_config.d/*.conf
Host *
# ForwardAgent no
# ForwardX11 no
# ForwardX11Trusted yes
# PasswordAuthentication yes
# HostbasedAuthentication no
# GSSAPIAuthentication no
# GSSAPIDelegateCredentials no
# GSSAPIKeyExchange no
# GSSAPITrustDNS no
# BatchMode no
# CheckHostIP yes
# AddressFamily any
# ConnectTimeout 0
# StrictHostKeyChecking ask
# IdentityFile ~/.ssh/id_rsa
# IdentityFile ~/.ssh/id_dsa
# IdentityFile ~/.ssh/id_ecdsa
# IdentityFile ~/.ssh/id_ed25519
# Port 22
# Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc
# MACs hmac-md5,hmac-sha1,umac-64@openssh.com
# EscapeChar ~
# Tunnel no
# TunnelDevice any:any
# PermitLocalCommand no
# VisualHostKey no
# ProxyCommand ssh -q -W %h:%p gateway.example.com
# RekeyLimit 1G 1h
# UserKnownHostsFile ~/.ssh/known_hosts.d/%k
SendEnv LANG LC_*
HashKnownHosts yes
GSSAPIAuthentication yes
HostKeyAlgorithms ssh-rsa,ssh-dss
(champuser㉿kali)-[~/SEC335/SEC-335]
$ cat /etc/ssh/ssh_config

Deliverable 9. Show a screenshot of your hydra session as well as a ssh login session using the targeted account. Also dump the contents of user-flag.txt using cat or more.




-


samwise@cupcake:~
File Actions Edit View Help
firefart:fiHGxheU6OS4M:0:0:pwned:/root:/bin/bash
^@^@^@^@^@^@^@/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/cache/rpcbind:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
saslauth:x:499:76:"Saslauthd user":/var/empty/saslauth:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
"/etc/passwd" 33L, 1590C
2,15-22
To

Deliverable 10. Provide a screenshot that shows the results of the id command as well as the contents of root-flag.txt similar to the one below.