OSYS3030: PROJECT 1

Hardening Security for Virtual Machines

SHERWIN LACONSAY
W0467725
10/21/2024

Contents

Objective:

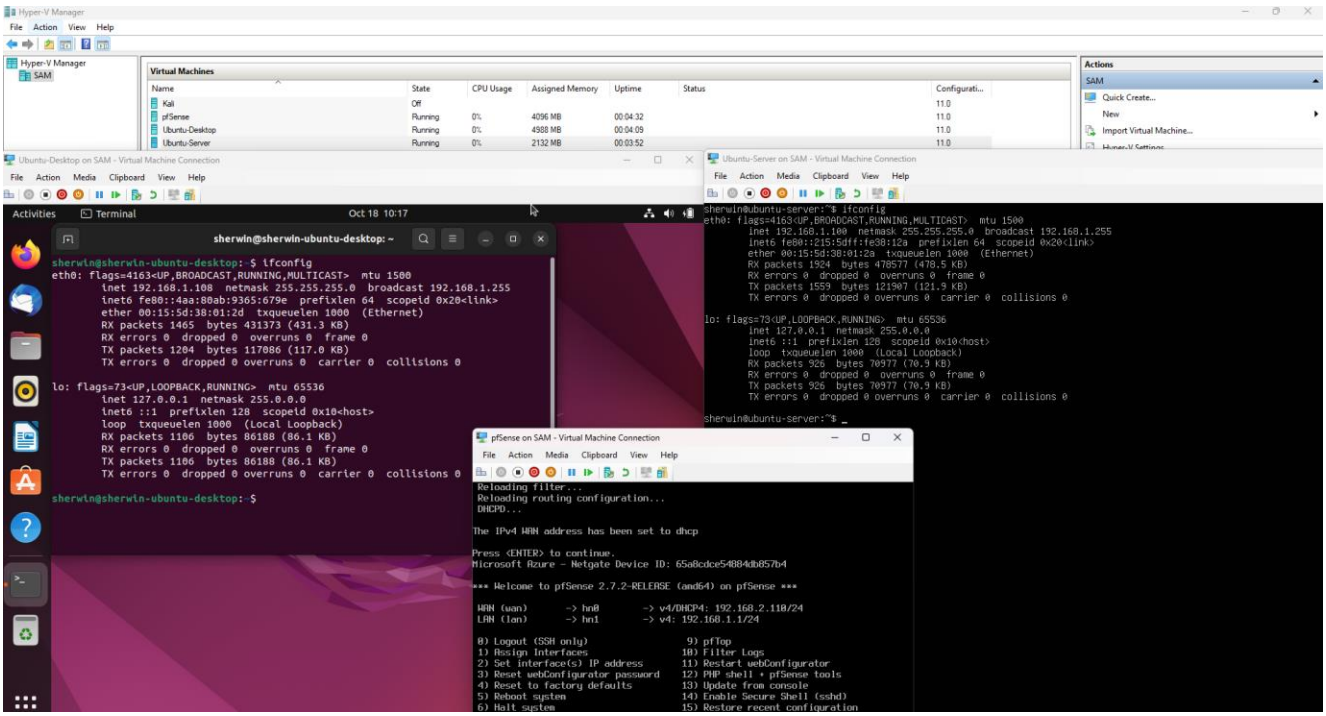
To implement and document security best practices for hardening virtual machines running Ubuntu Desktop, Ubuntu Server, and a PFsense router. Utilize all available tools to assist in this task. Ensure to create checkpoints and back up your VMs before starting.

Tasks and Evaluation:

1. **Update and Patch Management (1 point)**
2. **User Account Management (1 point)**
3. **Network Security (1 point)**
4. **Service Hardening (1 point)**
5. **File System Security (1 point)**
6. **System Monitoring and Logging (1 point)**
7. **Backup and Recovery (1 point)**
8. **Security Policies and Documentation (1 point)**
9. **Overall Execution and Quality (2 points)**
10. Submissions:
    1. Please document and take screenshots for each process. Submit to Bright space when complete and i will arrange a time to go over your project together.

VM Setup

Note: I am accessing the Ubuntu server through SSH for easier script copy-pasting.

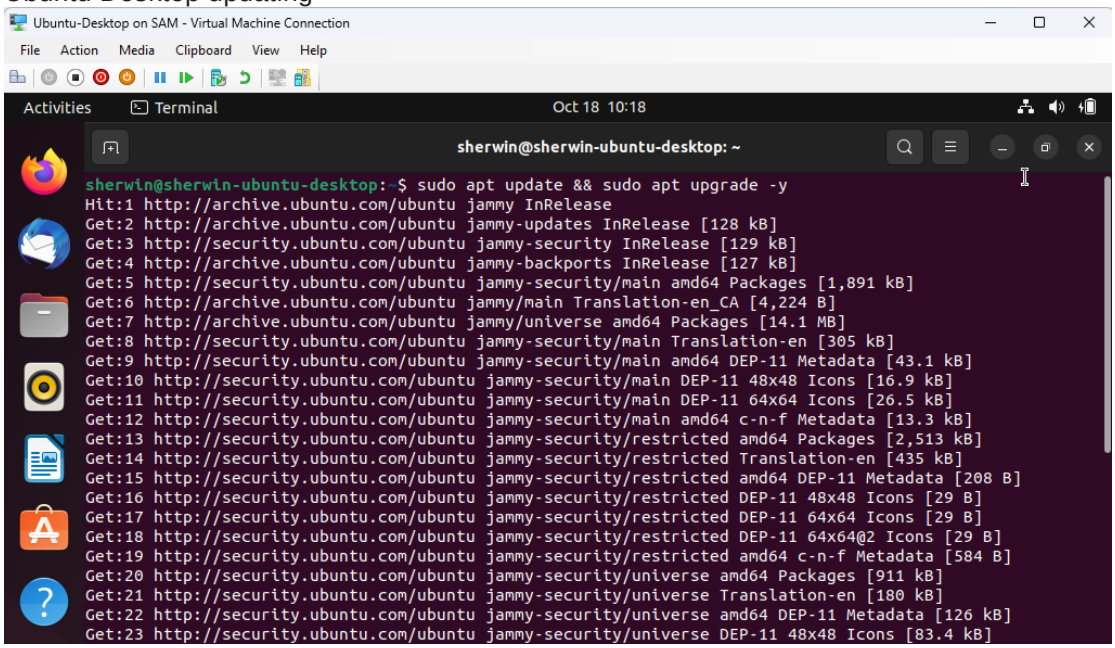


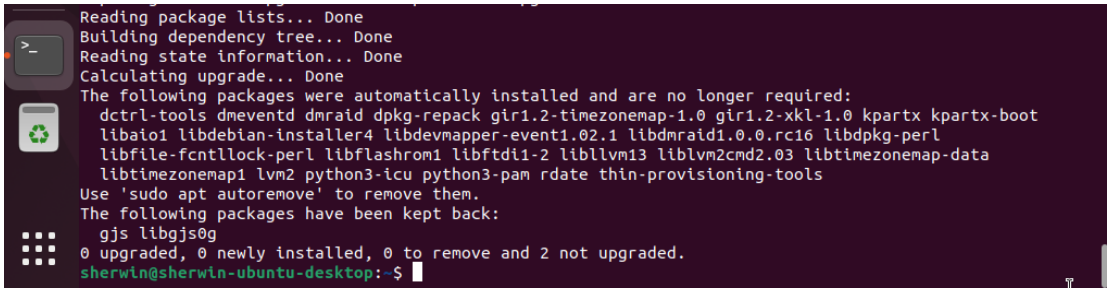
Proof of Work Done

1. Update and Patch Management

- Ensure all VMs are running the latest updates and security patches.
- Document the update process and any issues encountered.

Ubuntu Desktop updating



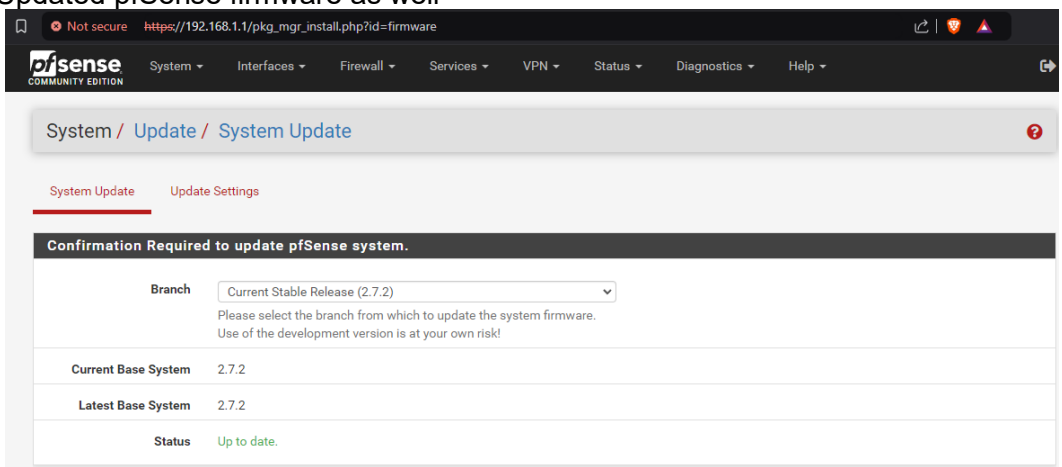


Ubuntu Server updating

```
sherwin@ubuntu-server: ~
sherwin@ubuntu-server:~$ sudo apt update && sudo apt upgrade -y
[sudo] password for sherwin:
Get:1 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Hit:2 http://ca.archive.ubuntu.com/ubuntu noble InRelease
Get:3 http://ca.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [7,224 B]
Get:5 http://ca.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:6 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [212 B]
Get:7 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [51.9 kB]
Get:8 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [212 B]
Get:9 http://ca.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [597 kB]
Get:10 http://ca.archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [114 kB]
Get:11 http://ca.archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [10.2 kB]
Get:12 http://ca.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [212 B]
Get:13 http://ca.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [705 kB]
Get:14 http://ca.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [305 kB]
Get:15 http://ca.archive.ubuntu.com/ubuntu noble-updates/universe amd64 c-n-f Metadata [19.8 kB]
Get:16 http://ca.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [940 B]
Get:17 http://ca.archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [208 B]
Get:18 http://ca.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [216 B]
Get:19 http://ca.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [21.2 kB]
Get:20 http://ca.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 B]
Fetched 2,212 kB in 1s (2,110 kB/s)
```

```
update-initramfs: Generating /boot/initrd.img-6.8.0-47-generic
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
sherwin@ubuntu-server:~$
```

Updated pfSense firmware as well



2. User Account Management

1. **Create two user accounts** on both the server and desktop Ubuntu systems.
    1. Match user name and passwords for server and desktop

Added new users (Walter and Jesse) in Ubuntu Desktop

```
sherwin@sherwin-ubuntu-desktop: ~
sherwin@sherwin-ubuntu-desktop:~$ sudo adduser walter && sudo adduser jesse
Adding user `walter' ...
Adding new group `walter' (1001) ...
Adding new user `walter' (1001) with group `walter' ...
The home directory `/home/walter' already exists. Not copying from `/etc/skel'.
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for walter
Enter the new value, or press ENTER for the default
        Full Name []: Walter White
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
Adding user `jesse' ...
Adding new group `jesse' (1002) ...
Adding new user `jesse' (1002) with group `jesse' ...
The home directory `/home/jesse' already exists. Not copying from `/etc/skel'.
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for jesse
Enter the new value, or press ENTER for the default
        Full Name []: Jesse Pinkman
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
sherwin@sherwin-ubuntu-desktop:~$
```

```
sherwin@sherwin-ubuntu-desktop: ~
sherwin@sherwin-ubuntu-desktop:~$ sudo cat /etc/shadow | tail -2
walter:$y$j9T$pbe1JnEWBWYqWv/1NppK00$avnblYlgDCoxlF1tRwRNRow4THtqI2D4hE1IJVTcIA2:20014:0:99999:7:::
jesse:$y$j9T$5vMoLOZeA131K3yJ67ad9.$VsofcnNCrGd/prl4hSXcMIY1Ayfw.yFHvEEhY/RfFJ6:20014:0:99999:7:::
sherwin@sherwin-ubuntu-desktop:~$
```

Added the same new users (Walter and Jesse) in Ubuntu Server

```
sherwin@ubuntu-server: ~
sherwin@ubuntu-server:~$ sudo adduser walter && sudo adduser jesse
[sudo] password for sherwin:
info: Adding user `walter' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `walter' (1001) ...
info: Adding new user `walter' (1001) with group `walter (1001)' ...
info: Creating home directory `/home/walter' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for walter
Enter the new value, or press ENTER for the default
        Full Name []: Walter White
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
info: Adding new user `walter' to supplemental / extra groups `users' ...
info: Adding user `walter' to group `users' ...
info: Adding user `jesse' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `jesse' (1002) ...
info: Adding new user `jesse' (1002) with group `jesse (1002)' ...
info: Creating home directory `/home/jesse' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for jesse
Enter the new value, or press ENTER for the default
        Full Name []: Jesse Pinkman
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
info: Adding new user `jesse' to supplemental / extra groups `users' ...
info: Adding user `jesse' to group `users' ...
sherwin@ubuntu-server:~$
```

```
sherwin@ubuntu-server:~$ cat /etc/shadow | tail -2
cat: /etc/shadow: Permission denied
sherwin@ubuntu-server:~$ sudo !!
sudo cat /etc/shadow | tail -2
walter:$y$j9T$UF4GRofp1NO5Cfm1VgfrX.$llQUfyD9mIuoHdKOkQzeqQHpwxNUy52hFUgDFWb3A65:20014:0:99999:7:::
jesse:$y$j9T$T3e0qgA.NOpri6ZrjpBAY/$0qeIWFuPl7kXtgtZZQvQeg46BGY3MHjP2ECZXm8cuz5:20014:0:99999:7:::
sherwin@ubuntu-server:~$
```

2. **Create strong, unique passwords** for all user accounts.

Ubuntu Desktop users passwords update

```
sherwin@sherwin-ubuntu-desktop: ~
sherwin@sherwin-ubuntu-desktop:~$ sudo passwd walter
New password:
Retype new password:
passwd: password updated successfully
sherwin@sherwin-ubuntu-desktop:~$ sudo passwd jesse
New password:
Retype new password:
passwd: password updated successfully
sherwin@sherwin-ubuntu-desktop:~$
```

Ubuntu Desktop users passwords update

```
sherwin@ubuntu-server: ~
sherwin@ubuntu-server:~$ sudo passwd walter
New password:
Retype new password:
passwd: password updated successfully
sherwin@ubuntu-server:~$ sudo passwd jesse
New password:
Retype new password:
passwd: password updated successfully
sherwin@ubuntu-server:~$
```

3. (optional) Implement multi-factor authentication (MFA) where possible.

Ubuntu Desktop MFA configuration

To enable the MFA, libpam-google-authenticator should be installed in the VM and a google authenticator app should be installed to my phone.

```
sherwin@sherwin-ubuntu-desktop: ~
sherwin@sherwin-ubuntu-desktop:~$ sudo apt install libpam-google-authenticator
[sudo] password for sherwin:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

I paired my machine to my google authenticator installed in my phone by scanning the QR below.

```
sherwin@sherwin-ubuntu-desktop: ~
sherwin@sherwin-ubuntu-desktop:~$ google-authenticator

Do you want authentication tokens to be time-based (y/n) y
Warning: pasting the following URL into your browser exposes the OTP secret to Google:
  https://www.google.com/chart?chs=200x200&chld=M|0&cht=qr&chl=otpauth://totp/sherwin@sherwin-ubuntu-desktop%3Fsecret%3DZCAJ
```

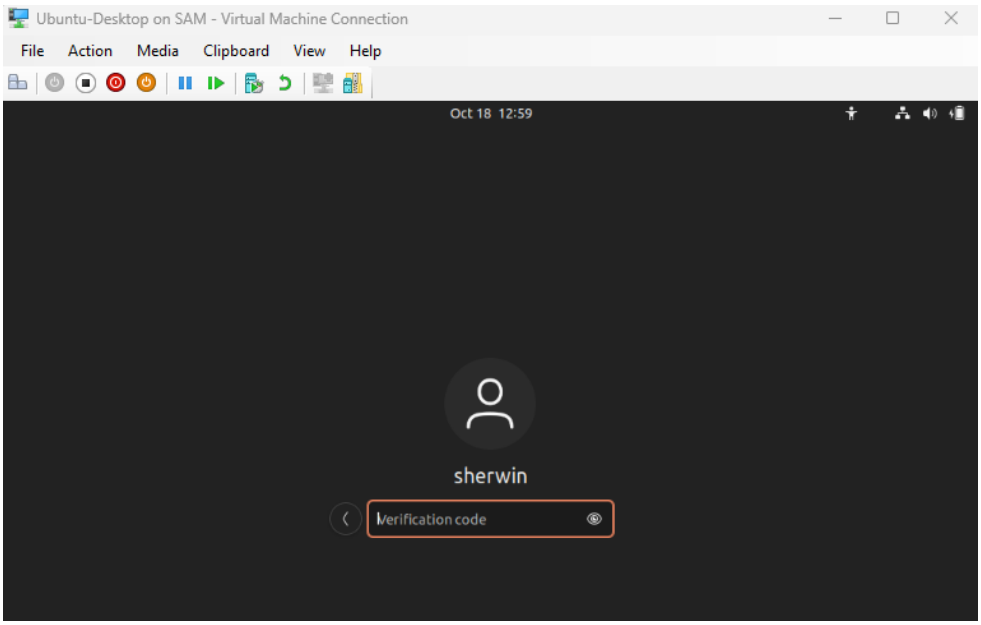
I took note of the emergency scratch codes and answer the following checks.

```
Do you want me to update your "/home/sherwin/.google_authenticator" file? (y/n) y

Do you want to disallow multiple uses of the same authentication
token? This restricts you to one login about every 30s, but it increases
your chances to notice or even prevent man-in-the-middle attacks (y/n) y

By default, a new token is generated every 30 seconds by the mobile app.
In order to compensate for possible time-skew between the client and the server,
we allow an extra token before and after the current time. This allows for a
time skew of up to 30 seconds between authentication server and client. If you
experience problems with poor time synchronization, you can increase the window
from its default size of 3 permitted codes (one previous code, the current
code, the next code) to 17 permitted codes (the 8 previous codes, the current
code, and the 8 next codes). This will permit for a time skew of up to 4 minutes
between client and server.
Do you want to do so? (y/n) n

If the computer that you are logging into isn't hardened against brute-force
login attempts, you can enable rate-limiting for the authentication module.
By default, this limits attackers to no more than 3 login attempts every 30s.
Do you want to enable rate-limiting? (y/n) y
sherwin@sherwin-ubuntu-desktop:~$
```

For the MFA to work, I've added the PAM google authenticator module to the common-auth config file.

```
sherwin@sherwin-ubuntu-desktop: ~
sherwin@sherwin-ubuntu-desktop:~$ sudo nano /etc/pam.d/common-auth
sherwin@sherwin-ubuntu-desktop:~$ sudo cat /etc/pam.d/common-auth | tail -10
# here's the fallback if no module succeeds
auth    requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
auth    required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
auth    optional                        pam_cap.so
# end of pam-auth-update config
auth    required                        pam_google_authenticator.so nullok
sherwin@sherwin-ubuntu-desktop:~$
```

Below is the verification code prompt when I am trying to login to my Ubuntu Desktop.



Below is also a prompt for verification code when issuing sudo.

```
sherwin@sherwin-ubuntu-desktop: ~
sherwin@sherwin-ubuntu-desktop:~$ sudo -l
[sudo] password for sherwin:
Verification code:
Matching Defaults entries for sherwin on sherwin-ubuntu-desktop:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User sherwin may run the following commands on sherwin-ubuntu-desktop:
    (ALL : ALL) ALL
sherwin@sherwin-ubuntu-desktop:~$
```

Ubuntu Server MFA configuration

To enable the MFA, I also installed libpam-google-authenticator in this VM and pair it to my phone's google authenticator and answer the pre-checks.

```
sherwin@ubuntu-server: ~
sherwin@ubuntu-server:~$ sudo apt install libpam-google-authenticator
[sudo] password for sherwin:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

```
sherwin@ubuntu-server: ~
sherwin@ubuntu-server:~$ google-authenticator

Do you want authentication tokens to be time-based (y/n) y
Warning: pasting the following URL into your browser exposes the OTP secret to Google:
  https://www.google.com/chart?chs=200x200&chld=M|0&cht=qr&chl=otpauth://totp/sherwin@ubuntu-server%3Fsecret%3DMNL4PMXB2CZUF4
```

```
Do you want me to update your "/home/sherwin/.google_authenticator" file? (y/n) y

Do you want to disallow multiple uses of the same authentication
token? This restricts you to one login about every 30s, but it increases
your chances to notice or even prevent man-in-the-middle attacks (y/n) y

By default, a new token is generated every 30 seconds by the mobile app.
In order to compensate for possible time-skew between the client and the server,
we allow an extra token before and after the current time. This allows for a
time skew of up to 30 seconds between authentication server and client. If you
experience problems with poor time synchronization, you can increase the window
from its default size of 3 permitted codes (one previous code, the current
code, the next code) to 17 permitted codes (the 8 previous codes, the current
code, and the 8 next codes). This will permit for a time skew of up to 4 minutes
between client and server.
Do you want to do so? (y/n) n

If the computer that you are logging into isn't hardened against brute-force
login attempts, you can enable rate-limiting for the authentication module.
By default, this limits attackers to no more than 3 login attempts every 30s.
Do you want to enable rate-limiting? (y/n) y
sherwin@ubuntu-server:~$
```

I then added this line to common-auth config to be able to use the google authenticator module.

```
sherwin@ubuntu-server: ~

sherwin@ubuntu-server:~$ sudo nano /etc/pam.d/common-auth
sherwin@ubuntu-server:~$ cat /etc/pam.d/common-auth | tail -10
# here's the fallback if no module succeeds
auth    requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
auth    required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
auth    optional                        pam_cap.so
# end of pam-auth-update config
auth    required                        pam_google_authenticator.so nullok
sherwin@ubuntu-server:~$
```

I tested it by logging in to the device and executing sudo commands.

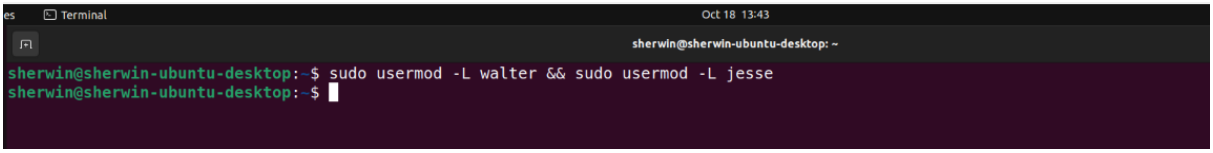
```
Ubuntu-Server on SAM - Virtual Machine Connection
File  Action  Media  Clipboard  View  Help

Ubuntu 24.04.1 LTS ubuntu-server tty1

ubuntu-server login: sherwin
Password:
Verification code:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-47-generic x86_64)

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

 System information as of Fri Oct 18 04:16:55 PM UTC 2024

  System load:  0.01               Processes:             144
  Usage of /:   17.5% of 28.37GB   Users logged in:       1
  Memory usage: 38%                IPv4 address for eth0: 192.168.1.100
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


sherwin@ubuntu-server:~$
```

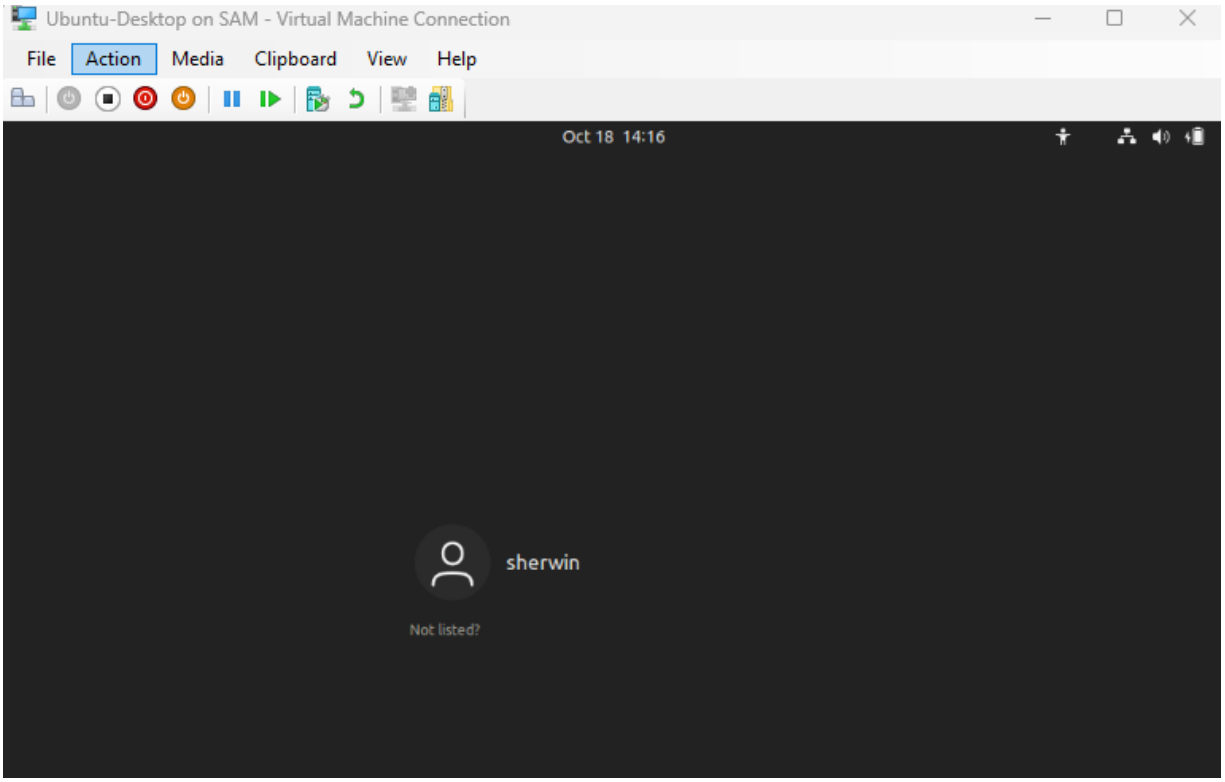
```
Ubuntu-Server on SAM - Virtual Machine Connection
File  Action  Media  Clipboard  View  Help

sherwin@ubuntu-server:~$ sudo -l
[sudo] password for sherwin:
Verification code:
Matching Defaults entries for sherwin on ubuntu-server:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User sherwin may run the following commands on ubuntu-server:
    (ALL : ALL) ALL
sherwin@ubuntu-server:~$
```

4. Remove or disable unnecessary user accounts.

   I disabled the two accounts that I created in Part 2 since these accounts are no use as of the moment. I keep the default accounts since these are pre-installed and serves its own purposes to run the OS.

   Ubuntu Dekstop. Disabling walter and jesse's account from logging in.





   Although these are effective methods for hardening, those accounts remain accessible if a valid sudoers account is used to switch to them, which is referred to as lateral movement.

```
sherwin@sherwin-ubuntu-desktop:~$ sudo su walter
walter@sherwin-ubuntu-desktop:/home/sherwin$ exit
exit
sherwin@sherwin-ubuntu-desktop:~$ sudo su jesse
jesse@sherwin-ubuntu-desktop:/home/sherwin$
```

   To address this, disabling their shell is a possible solution

```
sherwin@sherwin-ubuntu-desktop: ~
sherwin@sherwin-ubuntu-desktop:~$ sudo usermod -s /usr/bin/nologin walter
[sudo] password for sherwin:
sherwin@sherwin-ubuntu-desktop:~$ sudo su walter
su: failed to execute /usr/bin/nologin: No such file or directory
sherwin@sherwin-ubuntu-desktop:~$ sudo usermod -s /usr/bin/nologin jesse
sherwin@sherwin-ubuntu-desktop:~$ sudo su jesse
su: failed to execute /usr/bin/nologin: No such file or directory
sherwin@sherwin-ubuntu-desktop:~$
```

Ubuntu Server. Disabling walter and jesse's account from logging in.

```
sherwin@ubuntu-server: ~
sherwin@ubuntu-server:~$ sudo usermod -L walter && sudo usermod -L jesse
sherwin@ubuntu-server:~$
```

```
Ubuntu-Server on SAM - Virtual Machine Connection
File  Action  Media  Clipboard  View  Help

Ubuntu 24.04.1 LTS ubuntu-server tty1

ubuntu-server login: walter
Password:

Login incorrect
ubuntu-server login: jesse
Password:

Login incorrect
ubuntu-server login:
```

Same goes with Ubuntu Server, I've also disabled their shells to avoid lateral movement.

```
sherwin@ubuntu-server: ~
sherwin@ubuntu-server:~$ sudo usermod -s /usr/bin/nologin walter
usermod: Warning: missing or non-executable shell '/usr/bin/nologin'
sherwin@ubuntu-server:~$ sudo usermod -s /usr/bin/nologin jesse
usermod: Warning: missing or non-executable shell '/usr/bin/nologin'
sherwin@ubuntu-server:~$ sudo su walter
su: failed to execute /usr/bin/nologin: No such file or directory
sherwin@ubuntu-server:~$ sudo su jesse
su: failed to execute /usr/bin/nologin: No such file or directory
sherwin@ubuntu-server:~$
```

5. Do not modify your main account.
   My main account remains untouched for both VMs.
   Ubuntu Desktop

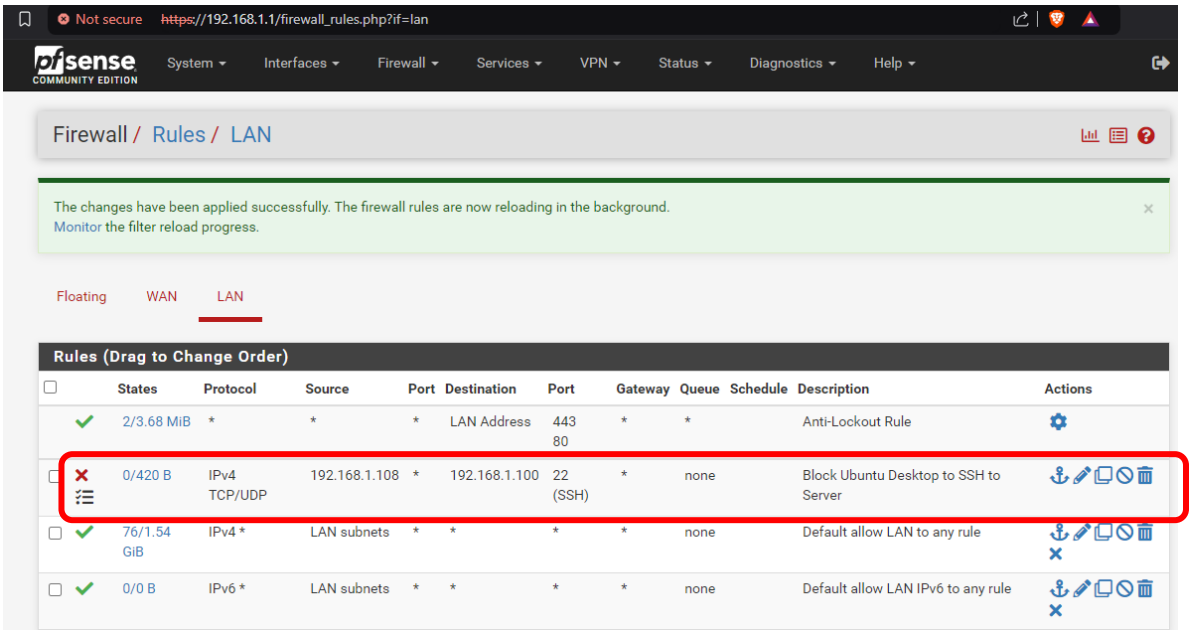
```
sherwin@sherwin-ubuntu-desktop: ~
sherwin@sherwin-ubuntu-desktop:~$ cat /etc/passwd | grep sherwin
sherwin:x:1000:1000:sherwin,,,:/home/sherwin:/bin/bash
sherwin@sherwin-ubuntu-desktop:~$ echo $SHELL
/bin/bash
sherwin@sherwin-ubuntu-desktop:~$
```

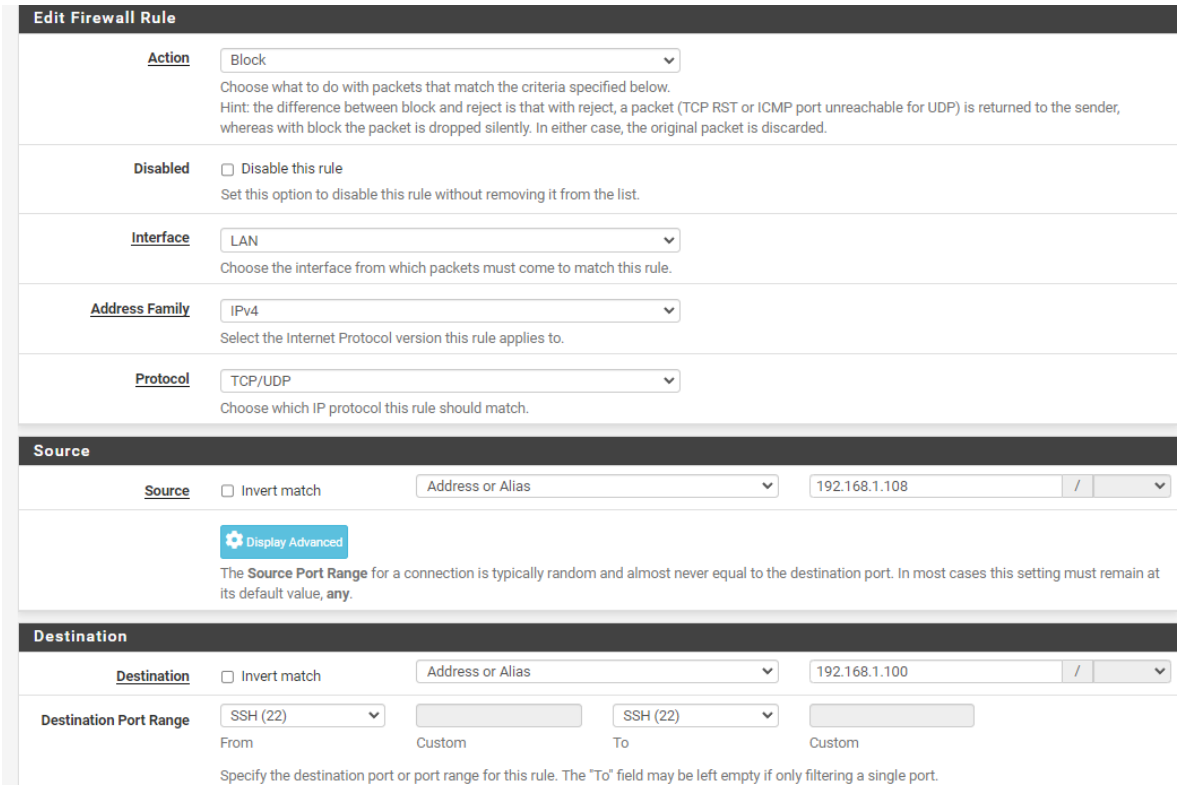
Ubuntu Server

```
sherwin@ubuntu-server: ~
sherwin@ubuntu-server:~$ cat /etc/passwd | grep sherwin
sherwin:x:1000:1000:sherwin:/home/sherwin:/bin/bash
sherwin@ubuntu-server:~$ echo $SHELL
/bin/bash
sherwin@ubuntu-server:~$
```

3. Network Security

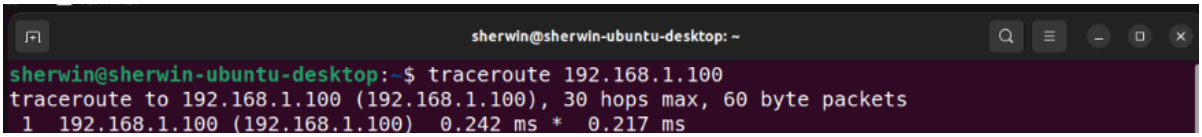
- Configure firewalls and access control lists (ACLs) on the PFsense router. (as long as you show were you create ACL it doesn't need an actual function).
- Document firewall rules and network configurations.





Issue encountered

I've noticed that my Ubuntu Desktop and Server are forming a direct connection instead of routing their traffic to the pfSense firewall. Hence, ssh is still passing thru despite of the firewall rule in place.



To solve this, I've added a default route to my ubuntu desktop to force it to route its traffic to the pfsense before it hits the Ubuntu Server. Now the SSH blocking rule is working in the LAN interfaces.

```
sherwin@sherwin-ubuntu-desktop:~$ sudo ip route add 192.168.1.0/24 via 192.168.1.1
sherwin@sherwin-ubuntu-desktop:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.1.1     0.0.0.0         UG    100    0        0 eth0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 eth0
192.168.1.0     192.168.1.1     255.255.255.0   UG    0      0        0 eth0
192.168.1.0     0.0.0.0         255.255.255.0   U     100    0        0 eth0
sherwin@sherwin-ubuntu-desktop:~$ traceroute 192.168.1.100
traceroute to 192.168.1.100 (192.168.1.100), 30 hops max, 60 byte packets
 1  pfSense.home.arpa (192.168.1.1)  0.457 ms  0.440 ms  0.432 ms
 2  * * *
 3  * 192.168.1.100 (192.168.1.100)  0.427 ms *
sherwin@sherwin-ubuntu-desktop:~$ ssh sherwin@192.168.1.100
ssh: connect to host 192.168.1.100 port 22: Connection timed out
sherwin@sherwin-ubuntu-desktop:~$
```

4. Service Hardening

- Disable unnecessary services and applications on each VM.
- Ensure only necessary ports are open and properly secured.
- Document the services that were disabled and the reasons for doing so.

Ubuntu Desktop

I first need to determine which services are not useful in my current VM's operation.

```
sherwin@sherwin-ubuntu-desktop:~$ systemctl list-unit-files --type=service
UNIT FILE                                   STATE           VENDOR PRESET
accounts-daemon.service                     enabled         enabled
acpid.service                               disabled        enabled
alsa-restore.service                        static          -
alsa-state.service                          static          -
alsa-utils.service                          masked          enabled
anacron.service                             enabled         enabled
apparmor.service                            enabled         enabled
apport-autoreport.service                   static          -
apport-forward@.service                     static          -
apport.service                              generated       -
apt-daily-upgrade.service                   static          -
apt-daily.service                           static          -
apt-news.service                            static          -
autovt@.service                             alias           -
```

I throw the list to AI to have an idea on what services are not mandatory in my current VM setup. I disabled these services for the following reasons:

- avahi-daemon.service – I don't want this machine to be discoverable by unknown entities
- bluetooth.service – I don't need bluetooth from these machines
- cups.service, cups-browsed.service – since I don't need any printing services and there is a latest CVE involving CUPS protocol.
- ModemManager.service – since I won't be connecting it to any dongles
- NetworkManager-wait-online.service – I also disabled this since it is delaying the boot process and this VM is not hosting any file shares or website.

Disabling the services:

```
sherwin@sherwin-ubuntu-desktop: ~
sherwin@sherwin-ubuntu-desktop:~$ cat appstodisable
avahi-daemon.service bluetooth.service cups.service cups-browsed.service ModemManager.service NetworkManager-wait-online.service
sherwin@sherwin-ubuntu-desktop:~$ sudo systemctl stop avahi-daemon.service bluetooth.service cups.service cups-browsed.service ModemManager.service Netwo
rkManager-wait-online.service
[sudo] password for sherwin:
Job for avahi-daemon.service canceled.
sherwin@sherwin-ubuntu-desktop:~$ sudo systemctl disable avahi-daemon.service bluetooth.service cups.service cups-browsed.service ModemManager.service Ne
tworkManager-wait-online.service
Synchronizing state of avahi-daemon.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable avahi-daemon
Synchronizing state of bluetooth.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable bluetooth
Synchronizing state of cups.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable cups
```

After I restarted my Ubuntu Desktop, I checked for the status of the services that I disabled and all of them are now inactive.

```
sherwin@sherwin-ubuntu-desktop: ~
sherwin@sherwin-ubuntu-desktop:~$ sudo systemctl status avahi-daemon.service bluetooth.service cups.service cups-browsed.service ModemManager.service Net
workManager-wait-online.service
○ avahi-daemon.service - Avahi mDNS/DNS-SD Stack
     Loaded: loaded (/lib/systemd/system/avahi-daemon.service; disabled; vendor preset: enabled)
     Active: inactive (dead)
TriggeredBy: ○ avahi-daemon.socket

○ bluetooth.service - Bluetooth service
     Loaded: loaded (/lib/systemd/system/bluetooth.service; disabled; vendor preset: enabled)
     Active: inactive (dead)
       Docs: man:bluetoothd(8)

○ cups.service - CUPS Scheduler
     Loaded: loaded (/lib/systemd/system/cups.service; disabled; vendor preset: enabled)
     Active: inactive (dead)
TriggeredBy: ○ cups.socket
       Docs: man:cupsd(8)

○ cups-browsed.service - Make remote CUPS printers available locally
     Loaded: loaded (/lib/systemd/system/cups-browsed.service; disabled; vendor preset: enabled)
     Active: inactive (dead)

○ ModemManager.service - Modem Manager
     Loaded: loaded (/lib/systemd/system/ModemManager.service; disabled; vendor preset: enabled)
     Active: inactive (dead)

○ NetworkManager-wait-online.service - Network Manager Wait Online
     Loaded: loaded (/lib/systemd/system/NetworkManager-wait-online.service; disabled; vendor preset: enabled)
     Active: inactive (dead)
       Docs: man:nm-online(1)
sherwin@sherwin-ubuntu-desktop:~$
```

Blocking traffic to the ports that I don't need for my Ubuntu desktop.
I first determine which ports are open in this machine. From the result below, only port 22 is open to other machines in my network. The rest are only open locally. I then confirm this using nmap scan from my windows machine.

```
sherwin@sherwin-ubuntu-desktop:~$ netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 ::1:3350                :::*                    LISTEN
udp        0      0 127.0.0.53:53           0.0.0.0:*
udp6       0      0 fe80::4aa:80ab:9365:546 :::*
```

```
sherwin@ubuntu-server: ~   Windows PowerShell   Windows PowerShell
PS D:\Downloads> nmap -sC -sV 192.168.1.108
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-19 13:32 Atlantic Summer Time
Nmap scan report for 192.168.1.108
Host is up (0.00s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
MAC Address: 00:15:5D:38:01:2D (Microsoft)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.09 seconds
PS D:\Downloads>
```

I blocked the access to port 22 to strengthen my machine's security. I use Ubuntu's built-in firewall to block this port. SSH is essential for my setup, but since port 22 is commonly used, it may be at risk from automated attacks. While this approach isn't completely foolproof, it adds an extra layer of difficulty for attackers.

```
sherwin@sherwin-ubuntu-desktop: ~
sherwin@sherwin-ubuntu-desktop:~$ sudo ufw deny 22
Rule added
Rule added (v6)
sherwin@sherwin-ubuntu-desktop:~$ sudo systemctl restart ufw
sherwin@sherwin-ubuntu-desktop:~$
```

```
sherwin@ubuntu-server: ~   Windows PowerShell   Windows PowerShell
PS D:\Downloads> ssh sherwin@192.168.1.108
ssh: connect to host 192.168.1.108 port 22: Connection timed out
PS D:\Downloads> nmap -sC -sV 192.168.1.108
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-19 13:44 Atlantic Summer Time
Nmap scan report for 192.168.1.108
Host is up (0.00s latency).
All 1000 scanned ports on 192.168.1.108 are filtered
MAC Address: 00:15:5D:38:01:2D (Microsoft)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.16 seconds
PS D:\Downloads>
```

Ubuntu Server

I did the same process for my server but unlike in my Ubuntu Desktop, Ubuntu Server have less unnecessary services.

```
sherwin@ubuntu-server: ~   Windows PowerShell
sherwin@ubuntu-server:~$ systemctl list-unit-files --type=service
UNIT FILE                                STATE           PRESET
apache-htcacheclean.service              disabled        enabled
apache-htcacheclean@.service             disabled        enabled
apache2.service                          enabled         enabled
apache2@.service                         disabled        enabled
apparmor.service                         enabled         enabled
apport-autoreport.service                static          -
apport-coredump-hook@.service            static          -
apport-forward@.service                  static          -
apport.service                           enabled         enabled
apt-daily-upgrade.service                static          -
apt-daily.service                        static          -
apt-news.service                         static          -
```

I throw the list to AI to determine the purpose of each services. I disabled these services for the following reasons:

- console-getty.service – since the server is running headless by default and can be managed thru SSH.
- unattended-upgrades.service – since I want my updates to be manually controlled instead of over-the-air (e.g. recent Crowdstrike fiasco)
- cloud-init.service – since this server is running only in my local network.
- rsync.service – this file transfer is unsecure since it doesn't encrypt the data during transfer so I will disable it and use a more secure one like FileZilla.

```
sherwin@ubuntu-server: ~        Windows PowerShell

sherwin@ubuntu-server:~$ sudo systemctl stop console-getty.service unattended-upgrades.service cloud-init.service rsync.service
[sudo] password for sherwin:
sherwin@ubuntu-server:~$ sudo systemctl disable console-getty.service unattended-upgrades.service cloud-init.service rsync.service
Synchronizing state of unattended-upgrades.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install disable unattended-upgrades
Synchronizing state of rsync.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install disable rsync
Removed "/etc/systemd/system/multi-user.target.wants/unattended-upgrades.service".
Removed "/etc/systemd/system/cloud-init.target.wants/cloud-init.service".
sherwin@ubuntu-server:~$
```

After the reboot, those services are now inactive.

```
sherwin@ubuntu-server: ~        Windows PowerShell

sherwin@ubuntu-server:~$ sudo systemctl status console-getty.service unattended-upgrades.service cloud-init.service rsync.service
[sudo] password for sherwin:
○ console-getty.service - Console Getty
     Loaded: loaded (/usr/lib/systemd/system/console-getty.service; disabled; preset: disabled)
     Active: inactive (dead)
       Docs: man:agetty(8)
             man:systemd-getty-generator(8)

○ unattended-upgrades.service - Unattended Upgrades Shutdown
     Loaded: loaded (/usr/lib/systemd/system/unattended-upgrades.service; disabled; preset: enabled)
     Active: inactive (dead)
       Docs: man:unattended-upgrade(8)

○ cloud-init.service - Cloud-init: Network Stage
     Loaded: loaded (/usr/lib/systemd/system/cloud-init.service; disabled; preset: enabled)
     Active: inactive (dead)

○ rsync.service - fast remote file copy program daemon
     Loaded: loaded (/usr/lib/systemd/system/rsync.service; disabled; preset: enabled)
     Active: inactive (dead)
       Docs: man:rsync(1)
             man:rsyncd.conf(5)
```

Disabling the ports that I don’t need for my Ubuntu Server.
After checking my open ports and scanning my server using nmap on my windows machine, I found out that ports 22 and 80 (used by Apache) are open to other devices in my network. Although I am using port 80 for apache, I can switch to 443 which is a more secure protocol.

```
sherwin@ubuntu-server: ~        Windows PowerShell

sherwin@ubuntu-server:~$ netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:33060         0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.54:53           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
udp        0      0 127.0.0.54:53           0.0.0.0:*
udp        0      0 127.0.0.53:53           0.0.0.0:*
udp6       0      0 fe80::215:5dff:fe38:546 :::*
sherwin@ubuntu-server:~$
```

```
sherwin@ubuntu-server: ~        Windows PowerShell

PS D:\Downloads> nmap -sC -sV 192.168.1.100
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-19 14:10 Atlantic Summer Time
Nmap scan report for 192.168.1.100
Host is up (0.00s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-generator: WordPress 6.6.2
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: wordpress
MAC Address: 00:15:5D:38:01:2A (Microsoft)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.93 seconds
PS D:\Downloads>
```

Blocking access to the ports 22 and 80.

```
sherwin@ubuntu-server: ~        Windows PowerShell
sherwin@ubuntu-server:~$ sudo ufw deny 22
Rules updated
Rules updated (v6)
sherwin@ubuntu-server:~$ sudo ufw deny 80
Rules updated
Rules updated (v6)
sherwin@ubuntu-server:~$ sudo systemctl restart ufw
sherwin@ubuntu-server:~$
```

```
Windows PowerShell        Windows PowerShell
PS D:\Downloads> nmap -sC -sV 192.168.1.100
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-19 14:22 Atlantic Summer Time
Nmap scan report for 192.168.1.100
Host is up (0.00s latency).
All 1000 scanned ports on 192.168.1.100 are filtered
MAC Address: 00:15:5D:38:01:2A (Microsoft)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.17 seconds
PS D:\Downloads>
```

Trying to SSH and accessing WordPress via http after blocking the ports.

```
Windows PowerShell        Windows PowerShell
PS C:\Users\sherw> ssh sherwin@192.168.1.100
ssh: connect to host 192.168.1.100 port 22: Connection timed out
PS C:\Users\sherw> curl http://192.168.1.100/wp-login.php
curl : Unable to connect to the remote server
At line:1 char:1
+ curl http://192.168.1.100/wp-login.php
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (System.Net.HttpWebRequest:HttpWebRequest) [Invoke-WebRequest], WebException
    + FullyQualifiedErrorId : WebCmdletWebResponseException,Microsoft.PowerShell.Commands.InvokeWebRequestCommand

PS C:\Users\sherw>
```

5. File System Security

- Implement file permissions and ownership settings to restrict access.
- Document the file system security measures taken.

Ubuntu Desktop

Changing directory permissions from its default permission of 775. I changed it to 700 which means that the only the user who owns the directory has the read, write, and execute permissions.

```
sherwin@sherwin-ubuntu-desktop: ~
sherwin@sherwin-ubuntu-desktop:~$ ls -ld infections/
drwxrwxr-x 3 sherwin sherwin 4096 Oct 19 15:16 infections/
sherwin@sherwin-ubuntu-desktop:~$ sudo chmod 700 infections/affected/
sherwin@sherwin-ubuntu-desktop:~$ ls -ld infections/affected/
drwx------ 2 sherwin sherwin 4096 Oct 19 15:16 infections/affected/
sherwin@sherwin-ubuntu-desktop:~$
```

Changing the file permissions from its default of 664. I changed it to 600 which means that only the user who owns the file has the permissions of read and write.

```
sherwin@sherwin-ubuntu-desktop: ~
sherwin@sherwin-ubuntu-desktop:~$ ls -ld infections/virus.txt
-rw-rw-r-- 1 sherwin sherwin 0 Oct 19 15:16 infections/virus.txt
sherwin@sherwin-ubuntu-desktop:~$ chmod 600 infections/virus.txt
sherwin@sherwin-ubuntu-desktop:~$ ls -ld infections/virus.txt
-rw------- 1 sherwin sherwin 0 Oct 19 15:16 infections/virus.txt
sherwin@sherwin-ubuntu-desktop:~$
```

Changing the file ownership to root user and group. Upon changing the owner to root, my main user unable to read the file. I have to switch to root user to be able to see the file contents.

```
root@sherwin-ubuntu-desktop: /home/sherwin
sherwin@sherwin-ubuntu-desktop:~$ sudo chown root:root infections/virus.txt
[sudo] password for sherwin:
sherwin@sherwin-ubuntu-desktop:~$ ls -ld infections/virus.txt
-rw------- 1 root root 9 Oct 19 15:52 infections/virus.txt
sherwin@sherwin-ubuntu-desktop:~$ cat infections/virus.txt
cat: infections/virus.txt: Permission denied
sherwin@sherwin-ubuntu-desktop:~$ sudo su root
root@sherwin-ubuntu-desktop:/home/sherwin# cat infections/virus.txt
covid-19
root@sherwin-ubuntu-desktop:/home/sherwin#
```

I encrypted a sample file using gpg and deleted the source file for security purposes.

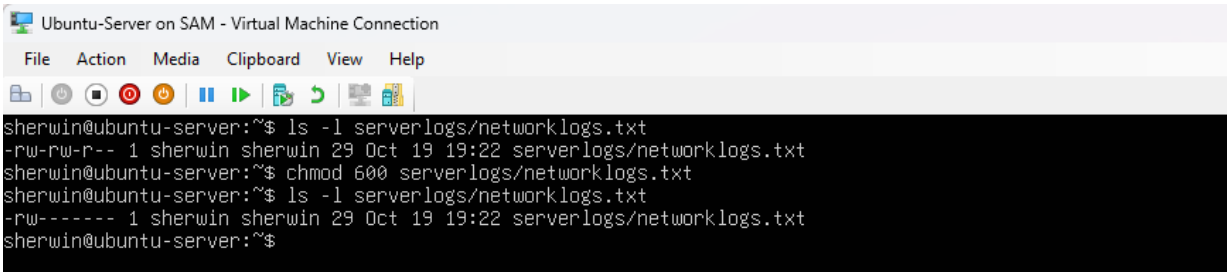
```
sherwin@sherwin-ubuntu-desktop: ~
sherwin@sherwin-ubuntu-desktop:~$ cat infections/affected_locations.txt
Philippines
sherwin@sherwin-ubuntu-desktop:~$ gpg -c infections/affected_locations.txt
File 'infections/affected_locations.txt.gpg' exists. Overwrite? (y/N) y
sherwin@sherwin-ubuntu-desktop:~$ ls -l infections/
total 16
drwx------ 2 sherwin sherwin 4096 Oct 19 15:16 affected
-rw-rw-r-- 1 sherwin sherwin   12 Oct 19 15:57 affected_locations.txt
-rw-rw-r-- 1 sherwin sherwin  104 Oct 19 16:00 affected_locations.txt.gpg
-rw------- 1 root    root       9 Oct 19 15:52 virus.txt
sherwin@sherwin-ubuntu-desktop:~$ rm infections/affected_locations.txt
sherwin@sherwin-ubuntu-desktop:~$ ls -l infections/
total 12
drwx------ 2 sherwin sherwin 4096 Oct 19 15:16 affected
-rw-rw-r-- 1 sherwin sherwin  104 Oct 19 16:00 affected_locations.txt.gpg
-rw------- 1 root    root       9 Oct 19 15:52 virus.txt
sherwin@sherwin-ubuntu-desktop:~$ cat infections/affected_locations.txt.gpg
[illegible]
sherwin@sherwin-ubuntu-desktop:~$
```

Ubuntu Server

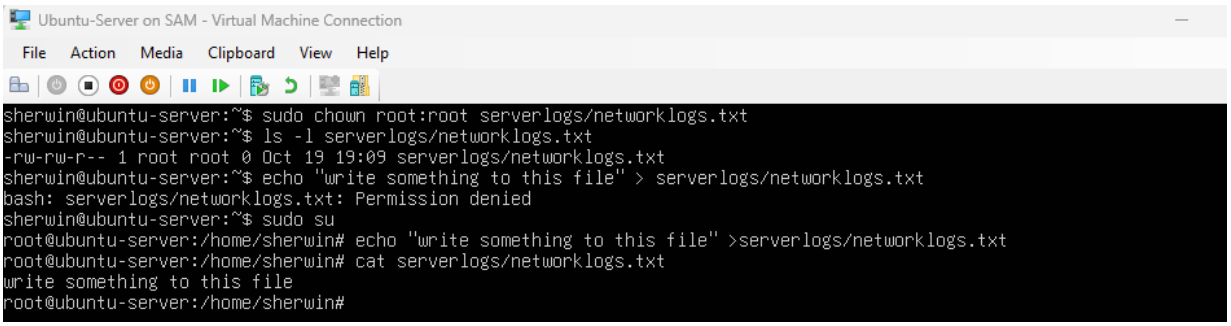
Same steps are taken in my server. I changed the directory permissions from 775 to 700 or read, write, and execute permissions only to the directory owner.

```
Ubuntu-Server on SAM - Virtual Machine Connection
File  Action  Media  Clipboard  View  Help
sherwin@ubuntu-server:~$ ls -ld serverlogs/
drwxrwxr-x 2 sherwin sherwin 4096 Oct 19 19:09 serverlogs/
sherwin@ubuntu-server:~$ sudo chmod 700 serverlogs
[sudo] password for sherwin:
sherwin@ubuntu-server:~$ ls -ld serverlogs/
drwx------ 2 sherwin sherwin 4096 Oct 19 19:09 serverlogs/
sherwin@ubuntu-server:~$ _
```

I changed the directory permissions from 664 to 600 or read, write permissions only to the file owner.



Changing the file ownership to root user and group. Upon changing the owner to root, my main user unable to write in the file. I have to switch to root user to be able to write and read the file contents.

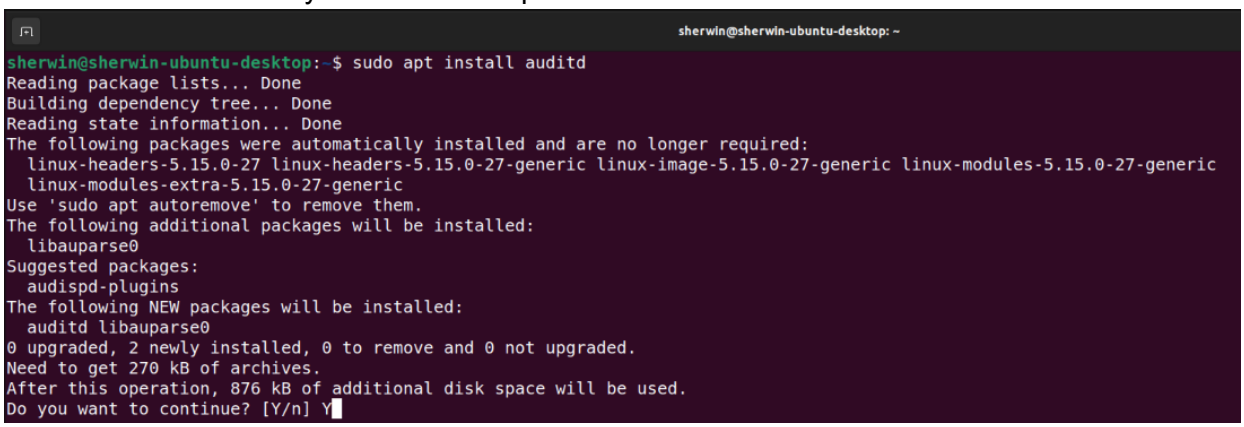


6. System Monitoring and Logging

- Set up system monitoring and logging tools (e.g., auditd, syslog).
- Configure alerts for suspicious activities.
- Document the monitoring setup and any alerts generated during the lab.

Ubuntu Desktop

I installed auditd into my Ubuntu Desktop.



I then edit the auditd.conf to increase the size of the log file to 10 MB and the number of logs to 20.

```
sherwin@sherwin-ubuntu-desktop: ~
sherwin@sherwin-ubuntu-desktop:~$ sudo nano /etc/audit/auditd.conf
sherwin@sherwin-ubuntu-desktop:~$ sudo cat /etc/audit/auditd.conf | head -20
#
# This file controls the configuration of the audit daemon
#

local_events = yes
write_logs = yes
log_file = /var/log/audit/audit.log
log_group = adm
log_format = ENRICHED
flush = INCREMENTAL_ASYNC
freq = 50
max_log_file = 10
num_logs = 20
priority_boost = 4
name_format = NONE
##name = mydomain
max_log_file_action = ROTATE
space_left = 75
space_left_action = SYSLOG
verify_email = yes
sherwin@sherwin-ubuntu-desktop:~$
```

I then created a rule that will create a log when someone is accessing the file that is owned by the root.

```
sherwin@sherwin-ubuntu-desktop: ~
sherwin@sherwin-ubuntu-desktop:~$ sudo auditctl -w ~/passwords.txt -p r -k file_read
sherwin@sherwin-ubuntu-desktop:~$ sudo auditctl -l
-w /home/sherwin/passwords.txt -p r -k file_read
sherwin@sherwin-ubuntu-desktop:~$ ls -l passwords.txt
-r-------- 1 root root 30 Oct 19 21:31 passwords.txt
sherwin@sherwin-ubuntu-desktop:~$
```

I added this lines in my rsyslog.conf to be able to use imfile module. These lines will let the rsyslog service to read the logs from auditd. I also made sure that rsyslog service is running.

```
sherwin@sherwin-ubuntu-desktop: ~
sherwin@sherwin-ubuntu-desktop:~$ sudo nano /etc/rsyslog.conf
sherwin@sherwin-ubuntu-desktop:~$ cat /etc/rsyslog.conf | tail -10

# Define the input for audit logs
input(type="imfile"
      File="/var/log/audit/audit.log"
      Tag="auditd"
      Severity="info"
      Facility="local1")

# Forward auditd logs to a specific log file
local1.* /var/log/audit_alerts.log
sherwin@sherwin-ubuntu-desktop:~$ sudo systemctl restart rsyslog
sherwin@sherwin-ubuntu-desktop:~$
```

I then tested my alerts if it is being received by rsyslog. I checked the log in inside audit_alerts.log file that I set in rsyslog.conf. I used lnav application to read the logs easier. The bottom lines of the audit_alerts.log are composed of syscall=257 (which means opening a file) and the path of which file is the unauthorized user is trying to open.

```
sherwin@sherwin-ubuntu-desktop: ~
sherwin@sherwin-ubuntu-desktop:~$ date && cat passwords.txt
Sat 19 Oct 2024 10:06:36 PM ADT
cat: passwords.txt: Permission denied
sherwin@sherwin-ubuntu-desktop:~$
```

```
Oct 19 22:03:458:31rwin-ubuntu-desktop auditd type=SYSCALL msg=audit(1729386225.185:510): arch=c000003e syscall=257 success=no exit=-13 a0=ffffff9c a1=7ffd9618e7c0
var/log/audit_alerts.log|Oct 19 22:05:19 sherwin-ubuntu-desktop auditd type=CWD msg=audit(1729386319.839:518): cwd="/home/sherwin"
var/log/audit_alerts.log|Oct 19 22:05:19 sherwin-ubuntu-desktop auditd type=PATH msg=audit(1729386319.839:518): item=0 name="passwords.txt" inode=1039835 dev=08:01
var/log/audit_alerts.log|Oct 19 22:05:19 sherwin-ubuntu-desktop auditd type=PROCTITLE msg=audit(1729386319.839:518): proctitle=636174007061737377 6F7264732E747874
var/log/audit_alerts.log|Oct 19 22:05:44 sherwin-ubuntu-desktop auditd type=BPF msg=audit(1729386344.867:519): prog-id=145 op=LOAD
var/log/audit_alerts.log|Oct 19 22:05:44 sherwin-ubuntu-desktop auditd type=BPF msg=audit(1729386344.871:520): prog-id=146 op=LOAD
var/log/audit_alerts.log|Oct 19 22:05:44 sherwin-ubuntu-desktop auditd type=BPF msg=audit(1729386344.871:521): prog-id=147 op=LOAD
var/log/audit_alerts.log|Oct 19 22:05:44 sherwin-ubuntu-desktop auditd type=SERVICE_START msg=audit(1729386344.959:522): pid=1 uid=0 auid=4294967295 ses=4294967295
var/log/audit_alerts.log|Oct 19 22:05:57 sherwin-ubuntu-desktop auditd type=SYSCALL msg=audit(1729386357.323:523): arch=c000003e syscall=257 success=no exit=-13 a0=
var/log/audit_alerts.log|Oct 19 22:05:57 sherwin-ubuntu-desktop auditd type=CWD msg=audit(1729386357.323:523): cwd="/home/sherwin"
var/log/audit_alerts.log|Oct 19 22:05:57 sherwin-ubuntu-desktop auditd type=PATH msg=audit(1729386357.323:523): item=0 name="passwords.txt" inode=1039835 dev=08:01
var/log/audit_alerts.log|Oct 19 22:05:57 sherwin-ubuntu-desktop auditd type=PROCTITLE msg=audit(1729386357.323:523): proctitle=636174007061737377 6F7264732E747874
var/log/audit_alerts.log|Oct 19 22:06:14 sherwin-ubuntu-desktop auditd type=SERVICE_STOP msg=audit(1729386374.996:524): pid=1 uid=0 auid=4294967295 ses=4294967295 s
var/log/audit_alerts.log|Oct 19 22:06:15 sherwin-ubuntu-desktop auditd type=BPF msg=audit(1729386375.016:525): prog-id=147 op=UNLOAD
var/log/audit_alerts.log|Oct 19 22:06:15 sherwin-ubuntu-desktop auditd type=BPF msg=audit(1729386375.016:526): prog-id=146 op=UNLOAD
var/log/audit_alerts.log|Oct 19 22:06:15 sherwin-ubuntu-desktop auditd type=BPF msg=audit(1729386375.016:527): prog-id=145 op=UNLOAD
var/log/audit_alerts.log|Oct 19 22:06:28 sherwin-ubuntu-desktop auditd type=SYSCALL msg=audit(1729386388.420:528): arch=c000003e syscall=257 success=no exit=-13 a0=
var/log/audit_alerts.log|Oct 19 22:06:28 sherwin-ubuntu-desktop auditd type=CWD msg=audit(1729386388.420:528): cwd="/home/sherwin"
var/log/audit_alerts.log|Oct 19 22:06:28 sherwin-ubuntu-desktop auditd type=PATH msg=audit(1729386388.420:528): item=0 name="passwords.txt" inode=1039835 dev=08:01
var/log/audit_alerts.log|Oct 19 22:06:28 sherwin-ubuntu-desktop auditd type=PROCTITLE msg=audit(1729386388.420:528): proctitle=636174007061737377 6F7264732E747874
var/log/audit_alerts.log|Oct 19 22:06:36 sherwin-ubuntu-desktop auditd type=SYSCALL msg=audit(1729386396.100:529): arch=c000003e syscall=257 success=no exit=-13 a0=
var/log/audit_alerts.log|Oct 19 22:06:36 sherwin-ubuntu-desktop auditd type=CWD msg=audit(1729386396.100:529): cwd="/home/sherwin"
var/log/audit_alerts.log|Oct 19 22:06:36 sherwin-ubuntu-desktop auditd type=PATH msg=audit(1729386396.100:529): item=0 name="passwords.txt" inode=1039835 dev=08:01
var/log/audit_alerts.log|Oct 19 22:06:36 sherwin-ubuntu-desktop auditd type=PROCTITLE msg=audit(1729386396.100:529): proctitle=636174007061737377 6F7264732E747874
```

I also created a simple bash script that will alert my terminal that an authorized user is trying to access the passwords.txt. The script will read the last 5 lines of the audit_alerts.log and if the keywords (syscall=257, success=no, passwords.txt) are in the lines, it will trigger an alert in my terminal. I set it into a background service so I can still use my terminal in case there are no alerts.

```
sherwin@sherwin-ubuntu-desktop: ~
sherwin@sherwin-ubuntu-desktop:~$ cat fileread_alert.sh
#!/bin/bash

# Continuous monitoring loop
while true; do
    # Check for the specific log entry in the audit alert log
    if tail -5 /var/log/audit_alerts.log | grep -q "syscall=257" &&  tail -5 /var/log/audit_alerts.log | grep -q "success=no" &&  tail -5 /var/log
alerts.log | grep -q "passwords.txt"; then
        # Notify users that an Nmap scan has been detected
        echo "File access detected in passwords.txt on $(date)"
    fi
    # Sleep for a short time to avoid excessive CPU usage
    sleep 5
done



sherwin@sherwin-ubuntu-desktop:~$ sudo chmod +x fileread_alert.sh
sherwin@sherwin-ubuntu-desktop:~$ ./fileread_alert.sh &
[1] 5463
sherwin@sherwin-ubuntu-desktop:~$ date && cat passwords.txt
Sat 19 Oct 2024 10:21:25 PM ADT
cat: passwords.txt: Permission denied
sherwin@sherwin-ubuntu-desktop:~$ File access detected in passwords.txt on Sat 19 Oct 2024 10:21:28 PM ADT
File access detected in passwords.txt on Sat 19 Oct 2024 10:21:33 PM ADT
File access detected in passwords.txt on Sat 19 Oct 2024 10:21:38 PM ADT
```

Ubuntu Server

```
sherwin@ubuntu-server: ~
sherwin@ubuntu-server:~$ sudo nano /etc/audit/auditd.conf
sherwin@ubuntu-server:~$ sudo cat /etc/audit/auditd.conf | head -20
#
# This file controls the configuration of the audit daemon
#

local_events = yes
write_logs = yes
log_file = /var/log/audit/audit.log
log_group = adm
log_format = ENRICHED
flush = INCREMENTAL_ASYNC
freq = 50
max_log_file = 10
num_logs = 20
priority_boost = 4
name_format = NONE
##name = mydomain
max_log_file_action = ROTATE
space_left = 75
space_left_action = SYSLOG
verify_email = yes
sherwin@ubuntu-server:~$
```

Make sure auditd service is running

```
sherwin@ubuntu-server:~$ sudo systemctl status auditd.service
● auditd.service - Security Auditing Service
     Loaded: loaded (/usr/lib/systemd/system/auditd.service; enabled; preset: enabled)
     Active: active (running) since Sat 2024-10-19 20:18:24 UTC; 3min 59s ago
       Docs: man:auditd(8)
             https://github.com/linux-audit/audit-documentation
    Process: 2993 ExecStart=/sbin/auditd (code=exited, status=0/SUCCESS)
    Process: 3001 ExecStartPost=/sbin/augenrules --load (code=exited, status=0/SUCCESS)
   Main PID: 2998 (auditd)
      Tasks: 2 (limit: 4613)
     Memory: 484.0K (peak: 2.5M)
        CPU: 27ms
     CGroup: /system.slice/auditd.service
             └─2998 /sbin/auditd
```

I've added a rule to detect if someone is trying to scan my Ubuntu Server

```
sherwin@ubuntu-server: ~    Windows PowerShell
sherwin@ubuntu-server:~$ sudo auditctl -a always,exit -F arch=b64 -S socket -k nmap_detect
sherwin@ubuntu-server:~$ sudo auditctl -l
-a always,exit -F arch=b64 -S socket -F key=nmap_detect
```

Now I did an nmap scan from my Windows machine

```
sherwin@ubuntu-server: ~    Windows PowerShell
PS C:\Users\sherw> nmap -sC -sV 192.168.1.100
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-19 17:37 Atlantic Summer Time
Nmap scan report for 192.168.1.100
Host is up (0.00s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-generator: WordPress 6.6.2
|_http-server-header: Apache/2.4.58 (Ubuntu)
```

I then checked the audit logs in my Ubuntu Server. We can see from the image below that it was triggered by a system call of 44 which means “sendto” and 41 which means “socketcall” or someone performed a socket-related operations which in this case was nmap. We can then check the key which is pointing to the rules that I set for detecting nmap scans.

```
sherwin@ubuntu-server: ~        Windows PowerShell
sherwin@ubuntu-server:~$ sudo ausearch -k nmap_detect
----
time->Sat Oct 19 17:37:06 2024
type=PROCTITLE msg=audit(1729370226.466:299): proctitle=617564697463746C002D6100616C776179732C65786974002D46006172636800623634002D5300736F636B6574002D6
B006E6D61705F646574656374
type=SYSCALL msg=audit(1729370226.466:299): arch=c000003e syscall=44 success=yes exit=1068 a0=4 a1=7ffcecc51a10 a2=42c a3=0 items=0 ppid=3444 pid=3445
auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts2 ses=4 comm="auditctl" exe="/usr/sbin/auditctl" subj=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(1729370226.466:299): auid=1000 ses=4 subj=unconfined op=add_rule key="nmap_detect" list=4 res=1
----
time->Sat Oct 19 17:37:06 2024
type=PROCTITLE msg=audit(1729370226.467:300): proctitle=7375646F006175646697463746C002D6100616C776179732C65786974002D4600617263683D623634002D5300736F636
B6574002D6B006E6D61705F646574656374
type=SYSCALL msg=audit(1729370226.467:300): arch=c000003e syscall=41 success=yes exit=3 a0=10 a1=3 a2=9 a3=5d122ca74d60 items=0 ppid=1732 pid=3443 auid
=1000 uid=1000 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0 ses=4 comm="sudo" exe="/usr/bin/sudo" subj=unconfined key="nmap_detect"
```

To fetch the logs from auditd to syslog, I then input the following configs to rsyslog.conf

```
sherwin@ubuntu-server: ~        Windows PowerShell
sherwin@ubuntu-server:~$ sudo nano /etc/rsyslog.conf
sherwin@ubuntu-server:~$ cat /etc/rsyslog.conf | tail -20
#
$WorkDirectory /var/spool/rsyslog

#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf

# Load imfile module for reading log files
module(load="imfile")

# Define the input for audit logs
input(type="imfile"
      File="/var/log/audit/audit.log"
      Tag="auditd"
      Severity="info"
      Facility="local1")

# Forward auditd logs to a specific log file
local1.*    /var/log/audit_alerts.log
sherwin@ubuntu-server:~$ sudo systemctl restart rsyslog.service
sherwin@ubuntu-server:~$
```

Then I perform the nmap scan again in my Windows machine and check if the logs are registered in the directory that I set in rsyslog.conf

```
sherwin@ubuntu-server: ~        Windows PowerShell
PS C:\Users\sherw> nmap -sC -sV 192.168.1.100
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-19 19:23 Atlantic Summer Time
Nmap scan report for 192.168.1.100
Host is up (0.00036s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-generator: WordPress 6.6.2
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: wordpress
MAC Address: 00:15:5D:38:01:2A (Microsoft)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.56 seconds
PS C:\Users\sherw>
```

Checking from the log file that I set in the rsyslog.conf, there is a logs from syscall=41 at the same time my nmap scan starts.

```
sherwin@ubuntu-server:~$ cat /var/log/audit_alerts.log | tail -100 | grep "syscall=41"
2024-10-19T19:23:33.645944-03:00 ubuntu-server auditd type=SYSCALL msg=audit(1729376613.644:478): arch=c000003e syscall=41 success=y
=socket AUID="unset" UID="www-data" GID="www-data" EUID="www-data" SUID="www-data" FSUID="www-data" EGID="www-data" SGID="www-data"
2024-10-19T19:23:33.646982-03:00 ubuntu-server auditd type=SYSCALL msg=audit(1729376613.645:479): arch=c000003e syscall=41 success=y
=socket AUID="unset" UID="www-data" GID="www-data" EUID="www-data" SUID="www-data" FSUID="www-data" EGID="www-data" SGID="www-data"
2024-10-19T19:23:33.696650-03:00 ubuntu-server auditd type=SYSCALL msg=audit(1729376613.695:480): arch=c000003e syscall=41 success=y
=socket AUID="unset" UID="www-data" GID="www-data" EUID="www-data" SUID="www-data" FSUID="www-data" EGID="www-data" SGID="www-data"
2024-10-19T19:23:33.750318-03:00 ubuntu-server auditd type=SYSCALL msg=audit(1729376613.749:481): arch=c000003e syscall=41 success=y
```

To create an alert, I created this simple bash script that reads the last two lines of audit_alerts.log. If it detected syscall=41 it will alert in my terminal. I then run it in the background.

```
sherwin@ubuntu-server: ~    sherwin@ubuntu-server:LC    Windows PowerShell

sherwin@ubuntu-server:~$ sudo cat nmap_alert.sh
#!/bin/bash

# Continuous monitoring loop
while true; do
    # Check for the specific log entry in the audit alert log
    if tail -2 /var/log/audit_alerts.log | grep -q "syscall=41"; then
        # Notify users that an Nmap scan has been detected
        echo "Nmap scan detected on $(date)" | wall
    fi
    # Sleep for a short time to avoid excessive CPU usage
    sleep 5
done
sherwin@ubuntu-server:~$ chmod +x nmap_alert.sh
sherwin@ubuntu-server:~$ ./nmap_alert.sh &
[1] 7015
sherwin@ubuntu-server:~$
```

I tested it by doing an nmap scan again in my windows machine and the alerts are reflected in my ubuntu server's terminal.

```
PS C:\Users\sherw> nmap -sC -sV 192.168.1.100
Starting Nmap 7.80 ( https://nmap.org ) at 2024-10-19 21:08 Atlantic Summer Time
Nmap scan report for 192.168.1.100
Host is up (0.00s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-generator: WordPress 6.6.2
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: wordpress
MAC Address: 00:15:5D:38:01:2A (Microsoft)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.06 seconds
PS C:\Users\sherw>
```

```
sherwin@ubuntu-server: ~    sherwin@ubuntu-server:LC    Windows PowerShell

sherwin@ubuntu-server:~$ sudo nano nmap_alert.sh
sherwin@ubuntu-server:~$ ./nmap_alert.sh &
[1] 6637

Broadcast message from sherwin@ubuntu-server (pts/1) (Sat Oct 19 21:08:23 2024)

Nmap scan detected on Sat Oct 19 09:08:23 PM ADT 2024


Broadcast message from sherwin@ubuntu-server (pts/1) (Sat Oct 19 21:08:28 2024)

Nmap scan detected on Sat Oct 19 09:08:28 PM ADT 2024
```

7. Backup and Recovery

- Implement regular backup procedures for each VM.
- Test the recovery process to ensure backups are functional.
- Document the backup and recovery procedures.

pfSense checkpoint creation and restoration

Virtual Machines

Name	State	CPU Usage	Assigned Memory	Uptime
Kali	Off			
pfSense	Running	0%	4096 MB	1.12:46:28
Ubuntu-Desktop	Running	0%	5000 MB	09:33:33
Ubuntu-Server	Running	0%	2060 MB	01:18:22

Checkpoints

pfSense - (10/19/24 - 10:56:45 PM)
Now

Virtual Machines

Name	State	CPU Usage	Assigned Memory	Uptime	Status
Kali	Off				
pfSense	Running	0%	4096 MB	00:00:00	Restoring - Succeeded
Ubuntu-Desktop	Running	0%	5000 MB	09:35:19	
Ubuntu-Server	Running	0%	2060 MB	01:20:08	

Checkpoints

pfSense - (10/19/24 - 10:56:45 PM)
Now

Ubuntu Desktop checkpoint creation and restoration

Virtual Machines

Name	State	CPU Usage	Assigned Memory	Uptime
Kali	Off			
pfSense	Running	0%	4096 MB	1.12:46:47
Ubuntu-Desktop	Running	0%	5000 MB	09:33:55
Ubuntu-Server	Running	0%	2060 MB	01:18:42

Checkpoints

Ubuntu-Desktop - (10/19/24 - 10:56:50 PM)
Now

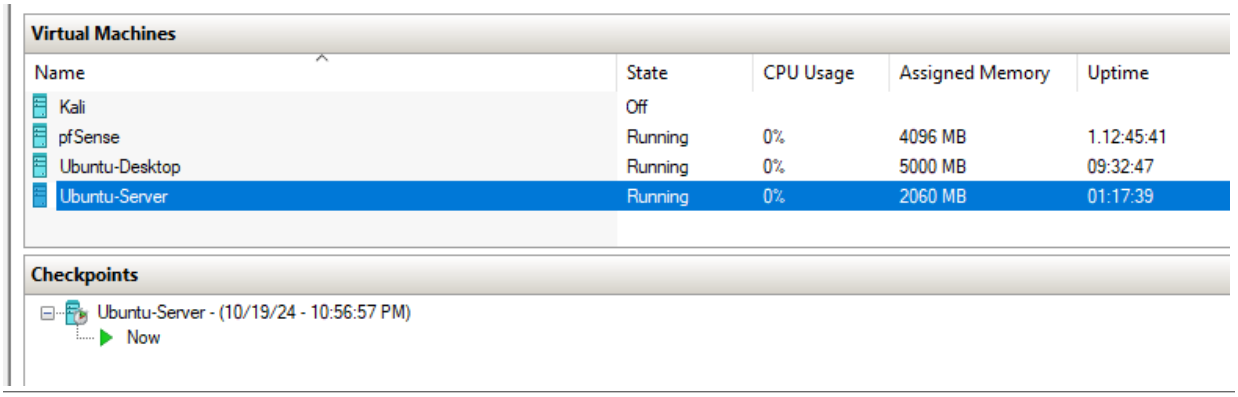
Virtual Machines

Name	State	CPU Usage	Assigned Memory	Uptime	Status
Kali	Off				
pfSense	Running	0%	4096 MB	00:01:38	
Ubuntu-Desktop	Running	0%	5000 MB	00:00:00	Restoring - Succeeded
Ubuntu-Server	Running	0%	2060 MB	01:21:47	

Checkpoints

Ubuntu-Desktop - (10/19/24 - 10:56:50 PM)
Now

Ubuntu Server checkpoint creation and restoration

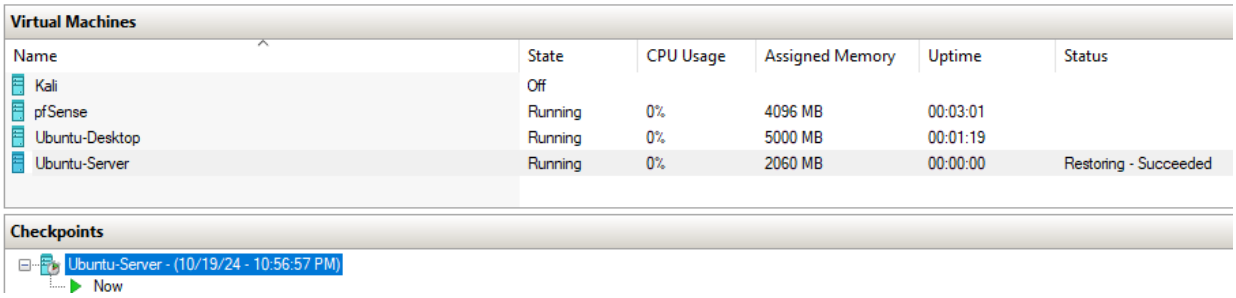


Virtual Machines

Name	State	CPU Usage	Assigned Memory	Uptime
Kali	Off			
pfSense	Running	0%	4096 MB	1.12:45:41
Ubuntu-Desktop	Running	0%	5000 MB	09:32:47
Ubuntu-Server	Running	0%	2060 MB	01:17:39

Checkpoints

Ubuntu-Server - (10/19/24 - 10:56:57 PM)
Now



Virtual Machines

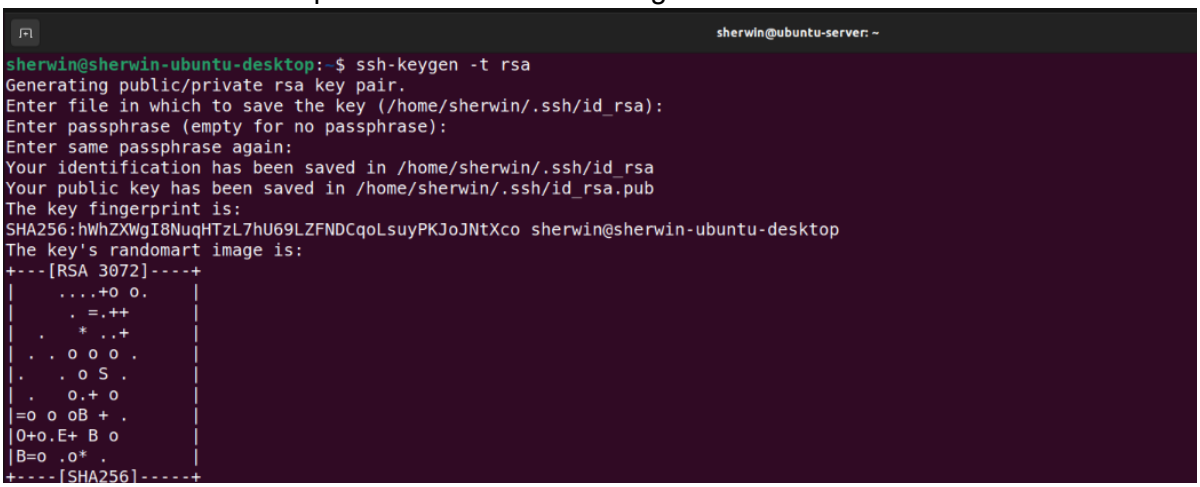
Name	State	CPU Usage	Assigned Memory	Uptime	Status
Kali	Off				
pfSense	Running	0%	4096 MB	00:03:01	
Ubuntu-Desktop	Running	0%	5000 MB	00:01:19	
Ubuntu-Server	Running	0%	2060 MB	00:00:00	Restoring - Succeeded

Checkpoints

Ubuntu-Server - (10/19/24 - 10:56:57 PM)
Now

Aside from VM checkpoints, I've also create a cron job. It is like a scheduled task that will run based on the set schedule. This is just a simple copying of a zip file from Ubuntu Desktop to Ubuntu Server thru SSH.

I first created a public key and copy it to the Ubuntu server, this will allow me to automate the task without the need of ssh password when connecting to Ubuntu Server via SSH.



sherwin@ubuntu-server: ~

```
sherwin@sherwin-ubuntu-desktop:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/sherwin/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/sherwin/.ssh/id_rsa
Your public key has been saved in /home/sherwin/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:hWhZXWgI8NuqHTzL7hU69LZFNDCqoLsuyPKJoJNtXco sherwin@sherwin-ubuntu-desktop
The key's randomart image is:
+---[RSA 3072]----+
|     ....+o o.    |
|      . =.++      |
|  .    * ..+      |
| . . o o o .      |
|.   . o S .       |
| .   o.+ o        |
|=o o oB + .       |
|O+o.E+ B o        |
|B=o .o* .         |
+----[SHA256]-----+
```

```
sherwin@sherwin-ubuntu-desktop:~$ ssh-copy-id sherwin@192.168.1.100
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/sherwin/.ssh/id_rsa.pub"
The authenticity of host '192.168.1.100 (192.168.1.100)' can't be established.
ED25519 key fingerprint is SHA256:7w182bQ4kgDiv/Oj5zy5+DieLbck/6nm6t169ds/q4E.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
sherwin@192.168.1.100's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'sherwin@192.168.1.100'"
and check to make sure that only the key(s) you wanted were added.

sherwin@sherwin-ubuntu-desktop:~$ ssh sherwin@192.168.1.100
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-47-generic x86_64)
```

Once the SSH connection has setup, I then create the cron job and give it a schedule of 10:53 pm everyday (for testing purposes). The job will copy the file.zip from my home directory to the backups folder of my Ubuntu Server.

```
sherwin@ubuntu-server: ~
sherwin@ubuntu-server:~$ crontab -e
crontab: installing new crontab
sherwin@ubuntu-server:~$ crontab -l | tail -10
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
53 22 * * * scp /home/sherwin/file.zip sherwin@192.168.1.100:/home/sherwin/backups/
sherwin@ubuntu-server:~$ sudo systemctl status cron
● cron.service - Regular background program processing daemon
     Loaded: loaded (/usr/lib/systemd/system/cron.service; enabled; preset: enabled)
     Active: active (running) since Sat 2024-10-19 19:16:26 ADT; 3h 36min ago
       Docs: man:cron(8)
   Main PID: 856 (cron)
      Tasks: 1 (limit: 4613)
     Memory: 460.0K (peak: 3.6M)
        CPU: 299ms
     CGroup: /system.slice/cron.service
             └─856 /usr/sbin/cron -f -P

Oct 19 22:45:01 ubuntu-server CRON[11680]: pam_unix(cron:session): session closed for user root
Oct 19 22:47:01 ubuntu-server cron[856]: (sherwin) RELOAD (crontabs/sherwin)
Oct 19 22:48:01 ubuntu-server CRON[11733]: pam_unix(cron:session): session opened for user sherwin(uid=1000) by sherwin(uid=0)
Oct 19 22:48:01 ubuntu-server CRON[11734]: (sherwin) CMD (scp /home/sherwin/file.zip sherwin@192.168.1.100:/home/sherwin/backups/)
Oct 19 22:48:01 ubuntu-server CRON[11733]: (CRON) info (No MTA installed, discarding output)
Oct 19 22:48:01 ubuntu-server CRON[11733]: pam_unix(cron:session): session closed for user sherwin
Oct 19 22:53:01 ubuntu-server cron[856]: (sherwin) RELOAD (crontabs/sherwin)
Oct 19 22:53:01 ubuntu-server CRON[12035]: pam_unix(cron:session): session opened for user sherwin(uid=1000) by sherwin(uid=0)
Oct 19 22:53:01 ubuntu-server CRON[12036]: (sherwin) CMD (scp /home/sherwin/file.zip sherwin@192.168.1.100:/home/sherwin/backups/)
Oct 19 22:53:01 ubuntu-server CRON[12035]: pam_unix(cron:session): session closed for user sherwin
sherwin@ubuntu-server:~$
```

Below will show that the file.zip was copied to Ubuntu Server after the execution of the cron job in my Ubuntu Desktop.

```
sherwin@ubuntu-server: ~/ba
sherwin@ubuntu-server:~/backups$ date && ls -la
Sat Oct 19 10:53:14 PM ADT 2024
total 8
drwxrwxr-x 2 sherwin sherwin 4096 Oct 19 22:53 .
drwxr-x--- 8 sherwin sherwin 4096 Oct 19 22:49 ..
-rw-rw-r-- 1 sherwin sherwin    0 Oct 19 22:53 file.zip
sherwin@ubuntu-server:~/backups$
```

8. Security Policies and Documentation

- Create and enforce security policies for each VM.
- Document all security measures taken and provide a final report.

To ensure that only a strong password should be given, I've added quality checks in common-password file to set the minimum password requirements. Though this only works if the user is not a sudoer.

Ubuntu Desktop password quality config.

```
sherwin@sherwin-ubuntu-desktop:~$ cat /etc/pam.d/common-password | tail -20
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password        requisite                       pam_pwquality.so minlen=10 minclass=3 usercheck=1 retry=1
password        [success=2 default=ignore]      pam_unix.so obscure use_authtok try_first_pass yescrypt
password        sufficient                      pam_sss.so use_authtok
#
# here's the fallback if no module succeeds
password        requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password        required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
password        optional        pam_gnome_keyring.so
# end of pam-auth-update config
sherwin@sherwin-ubuntu-desktop:~$
```

```
jesse@sherwin-ubuntu-desktop: /home/sherwin
jesse@sherwin-ubuntu-desktop:/home/sherwin$ passwd
Changing password for jesse.
Current password:
New password:
BAD PASSWORD: The password is shorter than 10 characters
passwd: Authentication token manipulation error
passwd: password unchanged
jesse@sherwin-ubuntu-desktop:/home/sherwin$ passwd
Changing password for jesse.
Current password:
New password:
BAD PASSWORD: The password contains less than 3 character classes
passwd: Authentication token manipulation error
passwd: password unchanged
jesse@sherwin-ubuntu-desktop:/home/sherwin$
```

In Ubuntu Server, I installed the libpam-pwquality library first before I able to configure the password quality.

```
sherwin@ubuntu-server:/etc/security$ sudo apt install libpam-pwquality
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  cracklib-runtime libcrack2 libpwquality-common libpwquality1 wamerican
The following NEW packages will be installed:
  cracklib-runtime libcrack2 libpam-pwquality libpwquality-common libpwquality1 wamerican
0 upgraded, 6 newly installed, 0 to remove and 2 not upgraded.
Need to get 446 kB of archives.
After this operation, 1,932 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ca.archive.ubuntu.com/ubuntu noble/main amd64 libcrack2 amd64 2.9.6-5.1build2 [29.0 kB]
Get:2 http://ca.archive.ubuntu.com/ubuntu noble/main amd64 cracklib-runtime amd64 2.9.6-5.1build2 [147
 kB]
```

```
sherwin@ubuntu-server: /etc,    sherwin@sherwin-ubuntu-des
  GNU nano 7.2                                                    common-password *
# /etc/pam.d/common-password - password-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords.  The default is pam_unix.

# Explanation of pam_unix options:
# The "yescrypt" option enables
#hashed passwords using the yescrypt algorithm, introduced in Debian
#11.  Without this option, the default is Unix crypt.  Prior releases
#used the option "sha512"; if a shadow password hash will be shared
#between Debian 11 and older releases replace "yescrypt" with "sha512"
#for compatibility .  The "obscure" option replaces the old
#`OBSCURE_CHECKS_ENAB' option in login.defs.  See the pam_unix manpage
#for other options.

# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password        requisite                       pam_pwquality.so minlen=10 minclass=3 usercheck=1 retry=1
password        [success=1 default=ignore]      pam_unix.so obscure use_authtok try_first_pass yescrypt
# here's the fallback if no module succeeds
password        requisite                       pam_deny.so
```

Trying out if the new password minimum requirements applied.

```
walter@ubuntu-server: ~    sherwin@sherwin-ubuntu-des
walter@ubuntu-server:~$ passwd
Changing password for walter.
Current password:
New password:
BAD PASSWORD: The password is shorter than 10 characters
passwd: Authentication token manipulation error
passwd: password unchanged
walter@ubuntu-server:~$ passwd
Changing password for walter.
Current password:
New password:
BAD PASSWORD: The password contains less than 3 character classes
passwd: Authentication token manipulation error
passwd: password unchanged
```

Final Report

1. **Update and Patch Management**
   - Updated the Ubuntu Desktop and Ubuntu Server with the latest image available using sudo apt update and upgrade.
   - Updated pfSense firmware with the latest version.

2. **User Account Management**
   - Used strong and unique passwords for all of the accounts.
   - Implemented MFA using google authenticator which is paired to the user's mobile phone.
   - Disabled unnecessary user login and their shells to avoid lateral movements.
   - Implemented a more secure password requirements for new users (minimum length, minimum number of character class, etc.

3. **Network Security**
   - Implemented a Firewall Rule in the pfSense GUI (blocked unauthorized IP addresses from using a specific protocol when connecting to the Ubuntu Server)

4. **Service Hardening**
   - Disabled unnecessary services and applications in Ubuntu Desktop and Server.
   - Disabled common ports like 80 and 22. Changed these to more uncommon ports instead.

5. **File System Security**
   - Configured the correct permissions and ownership for certain files. Making sure that only authorized users and groups are able to perform specific tasks on those files.
   - Implemented encryption in a certain files that only authorized users have access to the decryption keys.

6. **System Monitoring and Logging**
   - Setup a monitoring rules and logs against nmap scan and unauthorized file access using auditd and syslog
   - Created a bash scripts that will alert authorized users for any nmap scan and unauthorized file access.

7. **Backup and Recovery**
   - Created a checkpoints for each VMs (Ubuntu Desktop, Ubuntu Server, and pfSense) and making sure that everything can be restored in case of disaster.
   - Implmented a scheduled backup solution using cron jobs. The cron job will automatically copy important files to the Ubuntu Server thru SSH when a schedule time has reached.

References

https://manpages.ubuntu.com/manpages/mantic/man8/pam_pwquality.8.html
https://www.youtube.com/watch?v=wrx2cm3qDNI
https://www.esds.co.in/kb/how-to-clean-up-ubuntu-server/
https://sematext.com/glossary/auditd/

I used AI to aid me with some tasks since I can’t get the exact answers from Google / Ubuntu forums

-END-