

Week 5 Journal: Security Automation & Remote Monitoring

Introduction

This week focused on securing my Ubuntu server and setting up remote monitoring from my Linux Mint workstation. I configured AppArmor, automatic updates, fail2ban, and created two scripts: security-baseline.sh and monitor-server.sh. Below is my Week 5 journal detailing everything I did.

1. AppArmor Access Control

I verified AppArmor was running using `sudo aa-status`. Since Ubuntu did not include a default profile for sshd, I created my own AppArmor profile file and loaded it using apparmor_parser. I switched it to complain mode later so SSH could run normally.

```
abdulazeer@Ubuntu:~$ sudo aa-status
apparmor module is loaded.
155 profiles are loaded.
58 profiles are in enforce mode.
  /snap/snapd/25202/usr/lib/snapd/snap-confine
  /snap/snapd/25202/usr/lib/snapd/snap-confine//mount-namespace-capture-helper
  /snap/snapd/25577/usr/lib/snapd/snap-confine
  /snap/snapd/25577/usr/lib/snapd/snap-confine//mount-namespace-capture-helper
  /usr/bin/evince
  /usr/bin/evince-previewer
  /usr/bin/evince-previewer//sanitized_helper
  /usr/bin/evince-thumbnailer
  /usr/bin/evince//sanitized_helper
  /usr/bin/evince//snap_browsers
  /usr/bin/man
  /usr/lib/cups/backend/cups-pdf
  /usr/lib/snapd/snap-confine
  /usr/lib/snapd/snap-confine//mount-namespace-capture-helper
  /usr/sbin/cups-browsed
  /usr/sbin/cupsd
  /usr/sbin/cupsd//third_party
  lsb_release
  man_filter
  man_groff
  nvidia_modprobe
  nvidia_modprobe//kmod
  plasmashell
  plasmashell//QtWebEngineProcess
  rsyslogd
  snap-update-ns.firefox
  snap-update-ns.firmware-updater
  snap-update-ns.snap-store
  snap-update-ns.snapd-desktop-integration
```



```
wpc0m
7 processes have profiles defined.
6 processes are in enforce mode.
  /usr/sbin/cups-browsed (1184)
  /usr/sbin/cupsd (1124)
  /usr/lib/cups/notifier/dbus (1159) /usr/sbin/cupsd
  /usr/sbin/rsyslogd (862) rsyslogd
  /snap/snapd-desktop-integration/315/usr/bin/snapd-desktop-integration (2493) snap.snapd-desktop-integration.snapd-desktop-integration
  /snap/snapd-desktop-integration/315/usr/bin/snapd-desktop-integration (2614) snap.snapd-desktop-integration.snapd-desktop-integration
0 processes are in complain mode.
0 processes are in prompt mode.
0 processes are in kill mode.
1 processes are unconfined but have a profile defined.
  /usr/bin/gjs-console (2571) desktop-icons-ng
0 processes are in mixed mode.
abdulazeez@Ubuntu:~$
```

2. Automatic Security Updates

I installed and enabled unattended-upgrades to automate security patching. I checked the configuration using `cat /etc/apt/apt.conf.d/20auto-upgrades`, which confirmed automatic updates were enabled.

```
abdulazeez@Ubuntu:~$ sudo apt install unattended-upgrades -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
unattended-upgrades is already the newest version (2.9.1+nmu4ubuntu1).
The following package was automatically installed and is no longer required:
  liblvm19
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 121 not upgraded.
abdulazeez@Ubuntu:~$ sudo dpkg-reconfigure --priority=low unattended-upgrades
abdulazeez@Ubuntu:~$ cat /etc/apt/apt.conf.d/20auto-upgrades
APT::Periodic::Update-Package-Lists "1";
APT::Periodic::Unattended-Upgrade "1";
abdulazeez@Ubuntu:~$
```

3. Fail2ban – SSH Protection

I installed fail2ban and configured the SSH jail in `/etc/fail2ban/jail.local`. After restarting the service, I confirmed the jail was active using `fail2ban-client status sshd`.

4. security-baseline.sh Script

I wrote a script that prints a full security baseline report including firewall status, AppArmor, SSH config, fail2ban, and automatic update settings.

```
-- Banned IP list:  
abdulazeez@Ubuntu:~$ cd ~  
abdulazeez@Ubuntu:~$ nano monitor-server.sh  
abdulazeez@Ubuntu:~$ chmod +x ~/monitor-server.sh  
abdulazeez@Ubuntu:~$ ./monitor-server.sh  
REMOTE SERVER MONITORING  
  
kex_exchange_identification: read: Connection reset by peer  
Connection reset by 192.168.56.101 port 22  
kex_exchange_identification: read: Connection reset by peer  
Connection reset by 192.168.56.101 port 22  
Connection closed by 192.168.56.101 port 22  
Connection closed by 192.168.56.101 port 22  
kex_exchange_identification: read: Connection reset by peer  
Connection reset by 192.168.56.101 port 22  
abdulazeez@Ubuntu:~$
```

5. monitor-server.sh – Remote Monitoring

On Linux Mint, I created a monitoring script that connects to Ubuntu through SSH and prints hostname, uptime, memory usage, disk usage, and network connections.

```

Connection to 192.168.56.101 closed.
azeez@azeez-VirtualBox:~/monitor-server.sh
REMOTE SERVER MONITORING

Ubuntu
19:16:24 up 5:23, 3 users, load average: 0.10, 0.07, 0.02
           total        used        free      shared  buff/cache   available
Mem:       3.8Gi       1.1Gi     243Mi       36Mi       2.8Gi       2.7Gi
Swap:          0B          0B          0B

Filesystem  Size  Used Avail Use% Mounted on
tmpfs       392M  1.7M  391M   1% /run
/dev/sda2    46G  8.3G   35G  20% /
tmpfs       2.0G     0  2.0G   0% /dev/shm
tmpfs       5.0M  8.0K  5.0M   1% /run/lock
tmpfs       392M 140K  392M   1% /run/user/1000
/dev/sr0     6.0G  6.0G     0 100% /media/abdulazeez/Ubuntu 24.04.3 LTS amd64

Netid State      Recv-Q Send-Q          Local Address:Port      Peer Address:Port Process
udp  ESTAB      0      0          10.0.3.15:45204    172.28.28.4:53
udp  ESTAB      0      0          127.0.0.1:43179    127.0.0.53:53
udp  ESTAB      0      0          10.0.3.15:45255    172.28.28.4:53
udp  ESTAB      0      0          10.0.3.15:57579    172.28.28.4:53
udp  ESTAB      0      0          10.0.3.15:49463    172.28.28.4:53
udp  ESTAB      0      0          10.0.3.15:39232    172.28.28.4:53
udp  ESTAB      0      0          10.0.3.15:35139    172.28.28.4:53
udp  ESTAB      0      0          10.0.3.15:39291    172.28.28.4:53
udp  ESTAB      0      0          10.0.3.15:39401    172.28.28.4:53
udp  ESTAB      0      0          10.0.3.15:47617    172.28.28.4:53
udp  ESTAB      0      0          10.0.3.15:35481    172.28.28.4:53
udp  ESTAB      0      0          10.0.3.15:60080    172.28.28.4:53
udp  ESTAB      0      0          127.0.0.1:43794    127.0.0.53:53
udp  ESTAB      0      0          10.0.3.15:44216    172.28.28.4:53
udp  ESTAB      0      0          10.0.3.15:34097    172.28.28.4:53
udp  ESTAB      0      0          10.0.3.15:42569    172.28.28.4:53
udp  ESTAB      0      0          10.0.3.15:52897    172.28.28.4:53
udp  ESTAB      0      0          10.0.3.15:34670    172.28.28.4:53
udp  ESTAB      0      0          10.0.3.15:44928    172.28.28.4:53
udp  ESTAB      0      0          10.0.3.15:51235    172.28.28.4:53
udp  ESTAB      0      0  192.168.56.101%enp0s3:68  192.168.56.100:67
udp  ESTAB      0      0          10.0.3.15%enp0s8:68  10.0.3.2:67
tcp  ESTAB      0      0          192.168.56.101:22  192.168.56.102:36814
tcp  SYN-SENT   0      1          10.0.3.15:37846    172.28.28.1:53

azeez@azeez-VirtualBox:~$
```

Reflection

This week was challenging, especially dealing with AppArmor profiles and SSH issues, but I learned a lot about real server security. Setting up fail2ban and automatic updates improved my understanding of how to protect Linux systems. The monitoring script also helped me understand remote server management better.