Week 5 – Advanced Security and Monitoring Infrastructure

Introduction

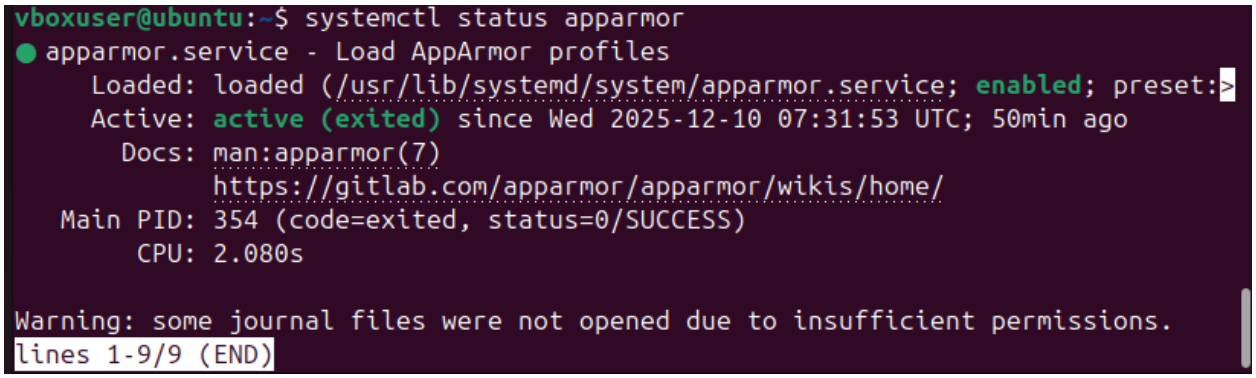
In Week 5, advanced security controls and monitoring mechanisms were implemented on the Ubuntu server. This included mandatory access control, automatic security updates and monitoring scripts. All configurations were applied remotely via SSH from the Fedora workstation.

1. Mandatory Access Control (AppArmor)

AppArmor Status Check

```
Systemctl status apparmor
```

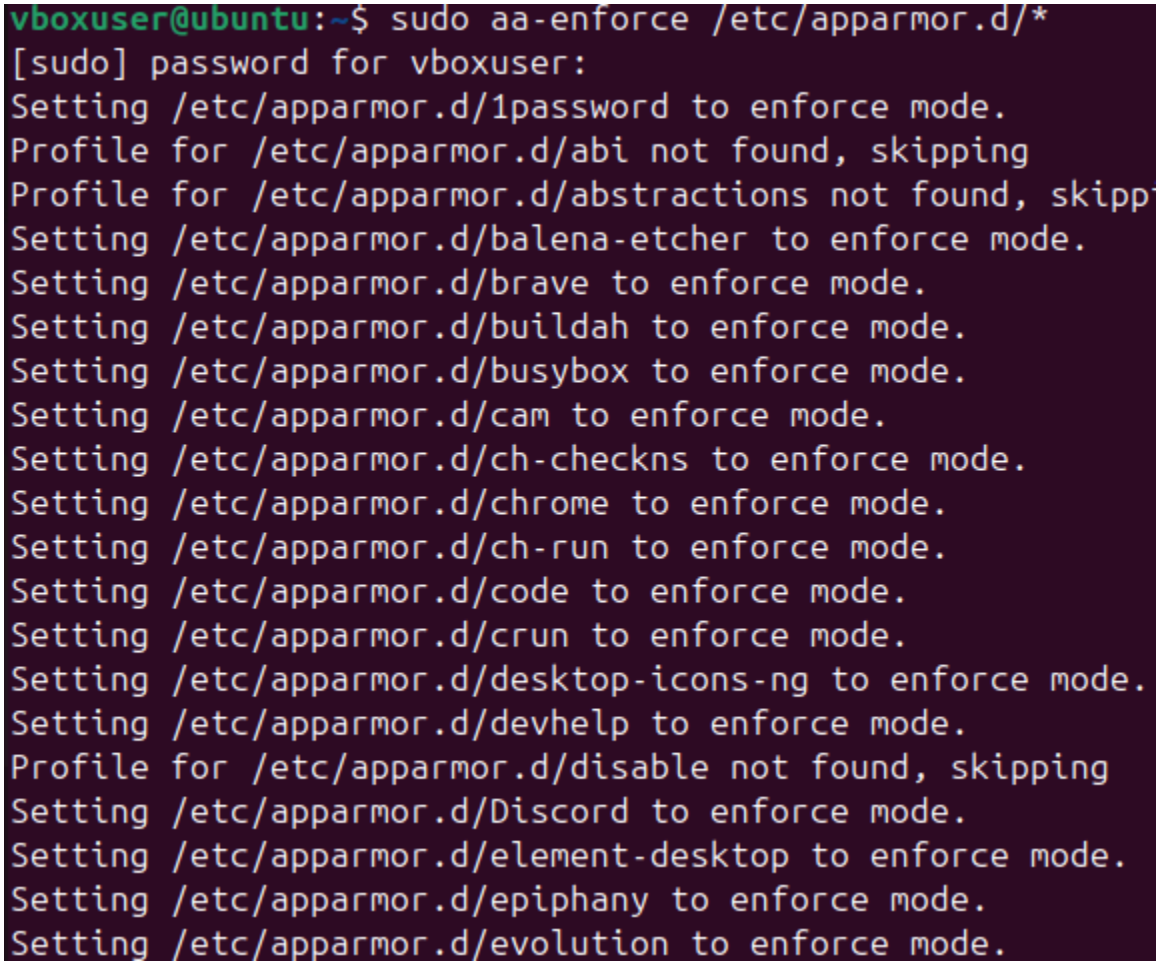
Displays whether AppArmor is enabled, shows which profiles are loaded and enforced, and confirms that mandatory access control is actively protecting system services.



Enforcing AppArmor Profiles

```
sudo aa-enforce /etc/apparmor.d/*
```

Forces all AppArmor profiles into enforce mode, prevents applications from accessing unauthorised files or resources, and reduces the impact of compromised services.

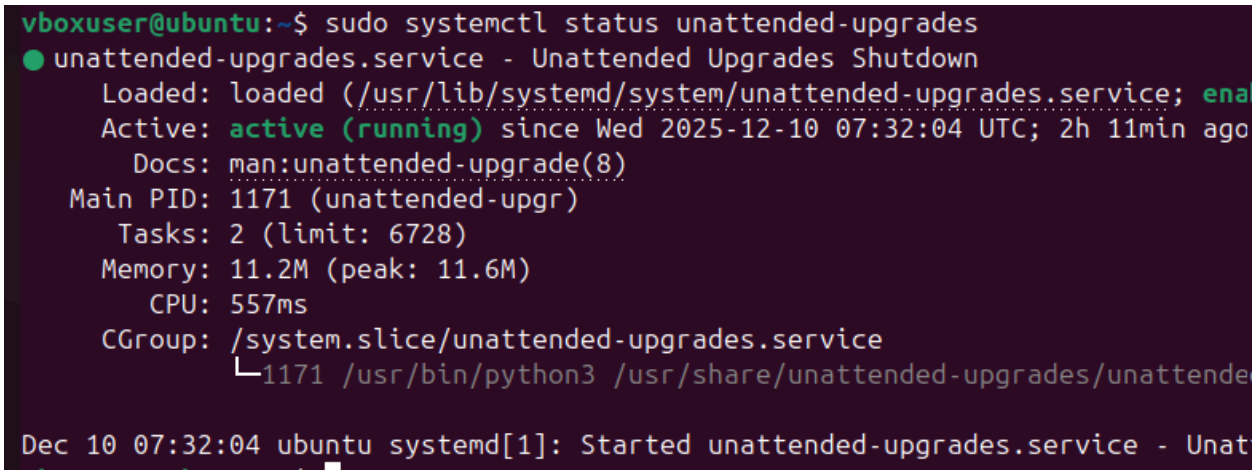


2. Automatic Security Updates

Installing Unattended Upgrades

```
sudo apt install unattended-upgrades -y
```

Automatically applies security patches to reduce vulnerability risks and keep the system updated.



Enabling Automatic Updates

`sudo dpkg-reconfigure unattended-upgrades`

Configures the system to automatically check for and install security updates.

3. Intrusion Detection with Fail2Ban

Installing Fail2Ban

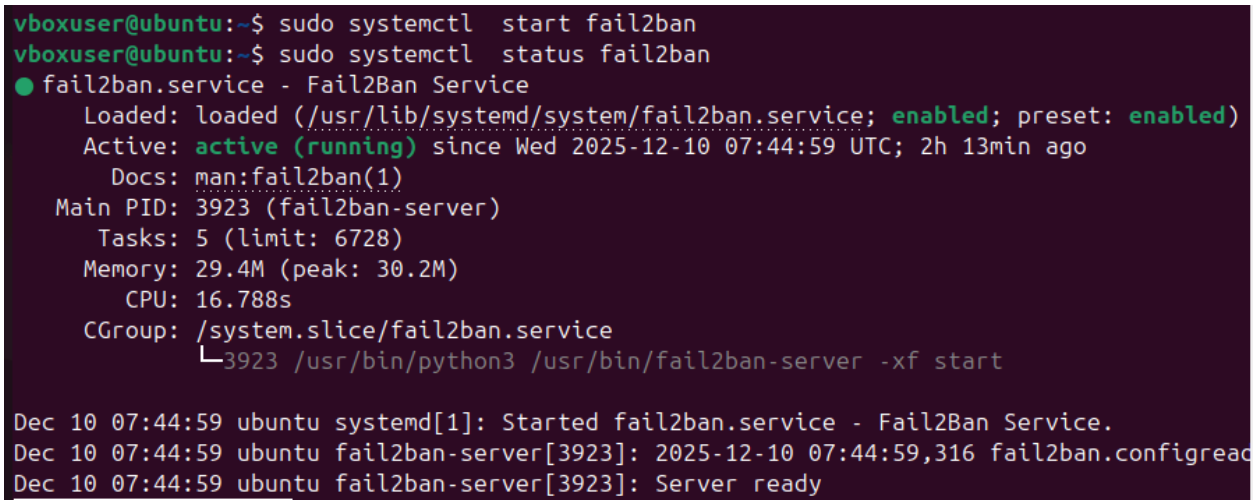
`sudo apt install fail2ban -y`

`Installs an intrusion prevention system that monitors logs and blocks IPs after repeated failed logins.`

Checking Fail2Ban Status

`sudo systemctl status fail2ban`

Deploys an intrusion prevention system to monitor logs and automatically block suspicious IPs.



4. Security Baseline Verification Script

Script: `security-baseline.sh`

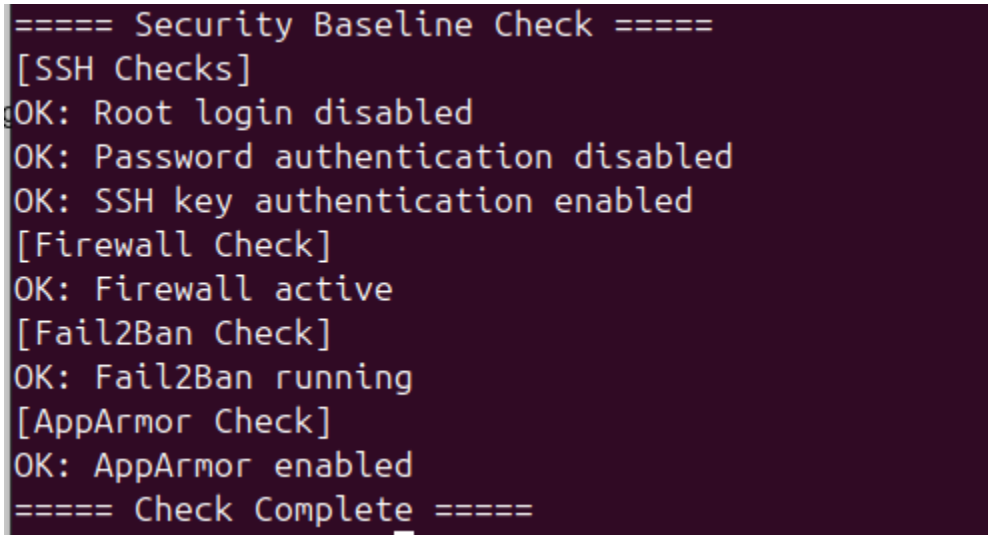
This script verifies that all critical security controls from Weeks 4 and 5 are enabled.

```
#!/bin/bash
# Security baseline verification script

echo "=== SSH Configuration ==="
sshd -T | grep -E "passwordauthentication|permitrootlogin"
```

```
echo "=== Firewall Status ==="
ufw status verbose

echo "=== AppArmor Status ==="
aa-status

echo "=== Fail2Ban Status ==="
systemctl is-active fail2ban

echo "=== Automatic Updates ==="
systemctl is-active unattended-upgrades
```

What this script does:

- Confirms SSH password authentication is disabled
- Checks firewall rules are active
- Verifies AppArmor enforcement
- Ensures Fail2Ban and automatic updates are running
- Provides quick security validation after changes



5. Remote Monitoring Script (Workstation)

Script: `monitor-server.sh`

This script runs on the **Fedora workstation** and collects live performance data from the Ubuntu server via SSH.

```
#!/bin/bash
# Remote server monitoring script

SERVER="192.168.56.101"

ssh $SERVER << EOF
echo "=== CPU Load ==="
uptime

echo "=== Memory Usage ==="
free -h

echo "=== Disk Usage ==="
df -h

echo "=== Network Interfaces ==="
ip addr
EOF
```

What this script does:

- Connects securely to the server via SSH
- Collects CPU, memory, disk, and network information
- Allows monitoring without logging into the server console
- Supports performance testing in later weeks

```
===== SERVER MONITOR =====
Hostname: ubuntu
Date: Fri Dec 12 09:53:03 AM UTC 2025
---- Uptime ----
 09:53:03 up 11 min,  3 users,  load average: 0.15, 0.56, 0.57
---- CPU Usage ----
%Cpu(s):  0.0 us,  2.0 sy,  0.0 ni, 95.9 id,  0.0 wa,  0.0 hi,  2.0 si,  0.0 st
---- Memory ----
               total        used        free      shared  buff/cache   available
Mem:           9.1Gi       1.6Gi       6.2Gi        46Mi       1.5Gi       7.5Gi
Swap:             0B          0B          0B
---- Disk ----
Filesystem      Size  Used Avail Use% Mounted on
tmpfs           937M  1.6M  935M   1% /run
/dev/sda2        25G  8.5G   15G  37% /
tmpfs           4.6G     0  4.6G   0% /dev/shm
tmpfs           5.0M  8.0K  5.0M   1% /run/lock
tmpfs           937M  120K  936M   1% /run/user/1000
tmpfs           937M   80K  937M   1% /run/user/1001
---- Network ----
lo               UNKNOWN        127.0.0.1/8 ::1/128
enp0s3           UP             192.168.50.10/24 192.168.56.101/24 fe80::a00:27ff:feb9:10d4/64
enp0s8           UP             10.0.3.15/24 fd17:625c:f037:3:7b63:8b7:c16d:347/64 fd17:625c:f037:3:d68d:646:6a1:6a49/64 fe80::4d9c:173:e4ba:6fd5/64
---- Top 5 Processes ----
    PID    PPID CMD                         %MEM %CPU
   4797    4788 ps -eo pid,ppid,cmd,%mem,%c  0.0  300
   2728    2106 /snap/firefox/7477/usr/lib/  5.3 13.0
   2106    1852 /usr/bin/gnome-shell         4.1 11.2
   4788    4787 bash                         0.0  9.5
   4743    1221 sshd: adminuser [priv]       0.1  8.6
===== END =====
```