Assessment Week 5

Phase 5: Advanced Security and Monitoring Infrastructure

Student Name: Purnawashi Mallah
Username: purnawashi
Server OS: Ubuntu Server 24.04 LTS
Environment: Oracle VirtualBox (NAT Networking)

1. Access Control Implementation using AppArmor

Ubuntu Server 24.04 uses **AppArmor** as its mandatory access control (MAC) framework. AppArmor restricts applications by enforcing security profiles that define allowed system resources.

The AppArmor service was verified using the following command:

```
sudo aa-status
```

The output confirmed that AppArmor was enabled and enforcing profiles, including the SSH daemon profile. This ensures that even if a service is compromised, its access to the system is limited according to predefined rules.

Justification:
AppArmor provides an additional security layer beyond standard UNIX permissions. Enforcing profiles for critical services such as SSH reduces the risk of privilege escalation and system compromise.

2. Automatic Security Updates Configuration

To ensure the system remains protected against known vulnerabilities, automatic security updates were configured using `unattended-upgrades`.

Installation was performed using:

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

Automatic updates were enabled by running:

```
sudo dpkg-reconfigure --priority=low unattended-upgrades
```

The configuration file `/etc/apt/apt.conf.d/20auto-upgrades` was checked to confirm that periodic package list updates and unattended upgrades were enabled.

Justification:
Automatic security updates reduce the window of exposure to vulnerabilities by applying critical patches without requiring manual intervention.

3. Fail2Ban Intrusion Detection Configuration

Fail2Ban was implemented to protect the server from brute-force authentication attacks, particularly targeting SSH.

Fail2Ban installation:

```
sudo apt install fail2ban -y
```

Service activation:

```
sudo systemctl enable fail2ban
sudo systemctl start fail2ban
```

Status verification:

```
sudo fail2ban-client status
sudo fail2ban-client status sshd
```

Fail2Ban monitors authentication logs and automatically bans IP addresses that generate repeated failed login attempts.

Justification:
Fail2Ban enhances server security by actively preventing brute-force login attempts and reducing attack surface.

4. Security Baseline Verification Script

A security baseline verification script named `security-baseline.sh` was created to validate all security controls implemented in Weeks 4 and 5.

Script Purpose

The script verifies:

- SSH service status
- Firewall rules
- AppArmor enforcement
- Fail2Ban operation
- Automatic update configuration

Script Execution

The script is executed directly on the server via SSH and produces a consolidated security status report.

Justification:
Automating security checks ensures consistency and simplifies future audits by providing a repeatable verification mechanism.

5. Remote Monitoring Script

A remote monitoring script named `monitor-server.sh` was created and executed from the workstation. The script connects to the Ubuntu server using SSH and collects key performance metrics, including:

- Hostname
- System uptime
- CPU usage
- Memory usage
- Disk usage

Justification:
Remote monitoring allows administrators to assess system performance without direct console access. This approach aligns with real-world server management practices.

6. SSH-Based Administrative Compliance

All configurations and scripts implemented during Week 5 were executed **via SSH**, in compliance with the administrative constraint specified in the assessment. This demonstrates secure remote server administration practices.

7. Summary of Week 5 Outcomes

The following advanced security and monitoring controls were successfully implemented:

- Mandatory access control using AppArmor
- Automatic security patching via unattended upgrades
- Intrusion detection using Fail2Ban
- Security baseline verification through scripting
- Remote performance monitoring using SSH

These measures significantly strengthen the server’s security posture and provide a foundation for performance evaluation and auditing in subsequent weeks.