📘 Phase 5: Advanced Security and Monitoring Infrastructure (Week 5)

5.1 Phase Objective

The objective of Phase 5 was to enhance the system's security posture beyond baseline hardening by implementing **mandatory access control**, **automatic security updates**, **intrusion detection**, and **automated verification and monitoring scripts**. These controls aim to improve system resilience, reduce attack surface, and provide continuous visibility into security and performance.

All configurations and validations were performed **remotely via SSH**, maintaining compliance with the headless server administration requirement.

5.2 Mandatory Access Control – AppArmor

AppArmor was used to enforce **mandatory access control (MAC)**, restricting application behaviour even in the event of compromise.

AppArmor Status Verification

```
sudo aa-status
```

```
pujeet@pujeet-VirtualBox:~$ sudo aa-status
[sudo] password for pujeet:
apparmor module is loaded.
182 profiles are loaded.
83 profiles are in enforce mode.
   /snap/snapd/24792/usr/lib/snapd/snap-confine
   /snap/snapd/24792/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/bin/pidgin
   /usr/bin/pidgin//sanitized_helper
   /usr/bin/totem
   /usr/bin/totem-audio-preview
   /usr/bin/totem-video-thumbnailer
   /usr/bin/totem//sanitized_helper
   /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
   apt-cacher-ng
   avahi-daemon
   dnsmasq
   dnsmasq//libvirt_leaseshelper
   identd
   klogd
   lsb_release
   man_filter
   man_groff
   mdnsd
   nmbd
   nscd
   nvidia_modprobe
   nvidia_modprobe//kmod
   php-fpm
   ping
   plasmashell
   plasmashell//QtWebEngineProcess
   rsyslogd
```

```
samba-bgqd
samba-dcerpcd
samba-rpcd
samba-rpcd-classic
samba-rpcd-spoolss
smbd
smbldap-useradd
smbldap-useradd///etc/init.d/nscd
snap-update-ns.firefox
snap-update-ns.firmware-updater
snap-update-ns.snap-store
snap-update-ns.snapd-desktop-integration
snap.firefox.firefox
snap.firefox.geckodriver
snap.firefox.hook.configure
snap.firefox.hook.disconnect-plug-host-hunspell
snap.firefox.hook.install
snap.firefox.hook.post-refresh
snap.firmware-updater.firmware-notifier
snap.firmware-updater.firmware-updater
snap.firmware-updater.firmware-updater-app
snap.firmware-updater.hook.configure
snap.snap-store.hook.configure
snap.snap-store.show-updates
snap.snap-store.snap-store
snap.snapd-desktop-integration.hook.configure
snap.snapd-desktop-integration.snapd-desktop-integration
syslog-ng
syslogd
tcpdump
traceroute
ubuntu_pro_apt_news
ubuntu_pro_esm_cache
ubuntu_pro_esm_cache//apt_methods
ubuntu_pro_esm_cache//apt_methods_gpgv
ubuntu_pro_esm_cache//cloud_id
ubuntu_pro_esm_cache//dpkg
ubuntu_pro_esm_cache//ps
ubuntu_pro_esm_cache//ubuntu_distro_info
ubuntu_pro_esm_cache_systemctl
ubuntu_pro_esm_cache_systemd_detect_virt
unix-chkpwd
unprivileged_userns
```

```
7 profiles are in complain mode.
   /usr/bin/irssi
   /usr/sbin/nginx
   /usr/sbin/sssd
   transmission-cli
   transmission-daemon
   transmission-gtk
   transmission-qt
0 profiles are in prompt mode.
0 profiles are in kill mode.
92 profiles are in unconfined mode.
   1password
   Discord
   MongoDB Compass
   QtWebEngineProcess
   balena-etcher
   brave
   buildah
   busybox
   cam
   ch-checkns
   ch-run
   chrome
   crun
   desktop-icons-ng
   devhelp
   element-desktop
   epiphany
   evolution
   firefox
   flatpak
   foliate
   geary
   github-desktop
   goldendict
   ipa_verify
   kchmviewer
   keybase
   lc-compliance
   libcamerify
   linux-sandbox
```

```
loupe
lxc-attach
lxc-create
lxc-destroy
lxc-execute
lxc-stop
lxc-unshare
lxc-usernsexec
mmdebstrap
msedge
nautilus
notepadqq
obsidian
opam
opera
pageedit
podman
polypane
privacybrowser
qcam
qmapshack
qutebrowser
rootlesskit
rpm
rssguard
runc
sbuild
sbuild-abort
sbuild-adduser
sbuild-apt
sbuild-checkpackages
sbuild-clean
sbuild-createchroot
sbuild-destroychroot
sbuild-distupgrade
sbuild-hold
sbuild-shell
sbuild-unhold
sbuild-update
sbuild-upgrade
scide
```

```
   signal-desktop
   slack
   slirp4netns
   steam
   stress-ng
   surfshark
   systemd-coredump
   thunderbird
   toybox
   trinity
   tup
   tuxedo-control-center
   userbindmount
   uwsgi-core
   vdens
   virtiofsd
   vivaldi-bin
   vpnns
   vscode
   wike
   wpcom
24 processes have profiles defined.
19 processes are in enforce mode.
   /usr/sbin/cups-browsed (1282)
   /usr/sbin/cupsd (1239)
   /usr/sbin/avahi-daemon (772) avahi-daemon
   /usr/sbin/avahi-daemon (928) avahi-daemon
   /usr/sbin/rsyslogd (910) rsyslogd
   /snap/firefox/7559/usr/lib/firefox/firefox (3390) snap.firefox.firefox
   /snap/firefox/7559/usr/lib/firefox/crashhelper (3455) snap.firefox.firefox
   /snap/firefox/7559/usr/lib/firefox/firefox (3532) snap.firefox.firefox
   /snap/firefox/7559/usr/lib/firefox/firefox (3537) snap.firefox.firefox
   /snap/firefox/7559/usr/lib/firefox/firefox (3571) snap.firefox.firefox
   /snap/firefox/7559/usr/lib/firefox/firefox (3582) snap.firefox.firefox
   /snap/firefox/7559/usr/lib/firefox/firefox (3785) snap.firefox.firefox
   /snap/firefox/7559/usr/lib/firefox/firefox (4156) snap.firefox.firefox
   /snap/firefox/7559/usr/lib/firefox/firefox (4162) snap.firefox.firefox
   /snap/firefox/7559/usr/lib/firefox/firefox (4177) snap.firefox.firefox
   /snap/firefox/7559/usr/lib/firefox/firefox (4188) snap.firefox.firefox
   /snap/firefox/7559/usr/lib/firefox/firefox (4386) snap.firefox.firefox
   /snap/snapd-desktop-integration/315/usr/bin/snapd-desktop-integration (2544) snap.snapd-
desktop-integration.snapd-desktop-integration
   /snap/snapd-desktop-integration/315/usr/bin/snapd-desktop-integration (2600) snap.snapd-
desktop-integration.snapd-desktop-integration
4 processes are in complain mode.
```

```
4 processes are in complain mode.
   /usr/sbin/nginx (1297)
   /usr/sbin/nginx (1298)
   /usr/sbin/nginx (1299)
   /usr/sbin/nginx (1300)
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 (3218) desktop-icons-ng
0 processes are in mixed mode.
pujeet@pujeet-VirtualBox:~$
```

The output confirmed that AppArmor was loaded and that multiple profiles were running in **enforce mode**, including nginx.

Figure 5.1 – AppArmor status showing enforced profiles

AppArmor Profiling of nginx

The nginx web server was profiled using:

```
sudo aa-genprof nginx
```

```
pujeet@pujeet-VirtualBox:~$ sudo aa-genprof nginx
Updating AppArmor profiles in /etc/apparmor.d.

Before you begin, you may wish to check if a
profile already exists for the application you
wish to confine. See the following wiki page for
more information:
https://gitlab.com/apparmor/apparmor/wikis/Profiles

Profiling: /usr/sbin/nginx

Please start the application to be profiled in
another window and exercise its functionality now.

Once completed, select the "Scan" option below in
order to scan the system logs for AppArmor events.

For each AppArmor event, you will be given the
opportunity to choose whether the access should be
allowed or denied.

[(S)can system log for AppArmor events] / (F)inish
```

During profiling:

- nginx activity was monitored
- Required permissions were learned
- A confined profile was generated and saved

This ensures nginx operates within a restricted security context.

📸 **Figure 5.2 – AppArmor profiling of nginx using aa-genprof**

Service Validation

After profiling, nginx service availability was verified:

```
systemctl status nginx --no-pager
```

```
pujeet@pujeet-VirtualBox:~$ systemctl status nginx --no-pager
● nginx.service - A high performance web server and a reverse proxy server
     Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-12-28 22:14:19 GMT; 49min ago
       Docs: man:nginx(8)
    Process: 1284 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code
=exited, status=0/SUCCESS)
    Process: 1293 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited,
status=0/SUCCESS)
   Main PID: 1297 (nginx)
      Tasks: 4 (limit: 4601)
     Memory: 4.3M (peak: 4.5M)
        CPU: 65ms
     CGroup: /system.slice/nginx.service
             ├─1297 "nginx: master process /usr/sbin/nginx -g daemon on; master_process on…
             ├─1298 "nginx: worker process"
             ├─1299 "nginx: worker process"
             └─1300 "nginx: worker process"

Dec 28 22:14:19 pujeet-VirtualBox systemd[1]: Starting nginx.service - A high performa…r...
Dec 28 22:14:19 pujeet-VirtualBox systemd[1]: Started nginx.service - A high performan…ver.
Hint: Some lines were ellipsized, use -l to show in full.
pujeet@pujeet-VirtualBox:~$
```

The service remained active, confirming AppArmor confinement did not disrupt functionality.

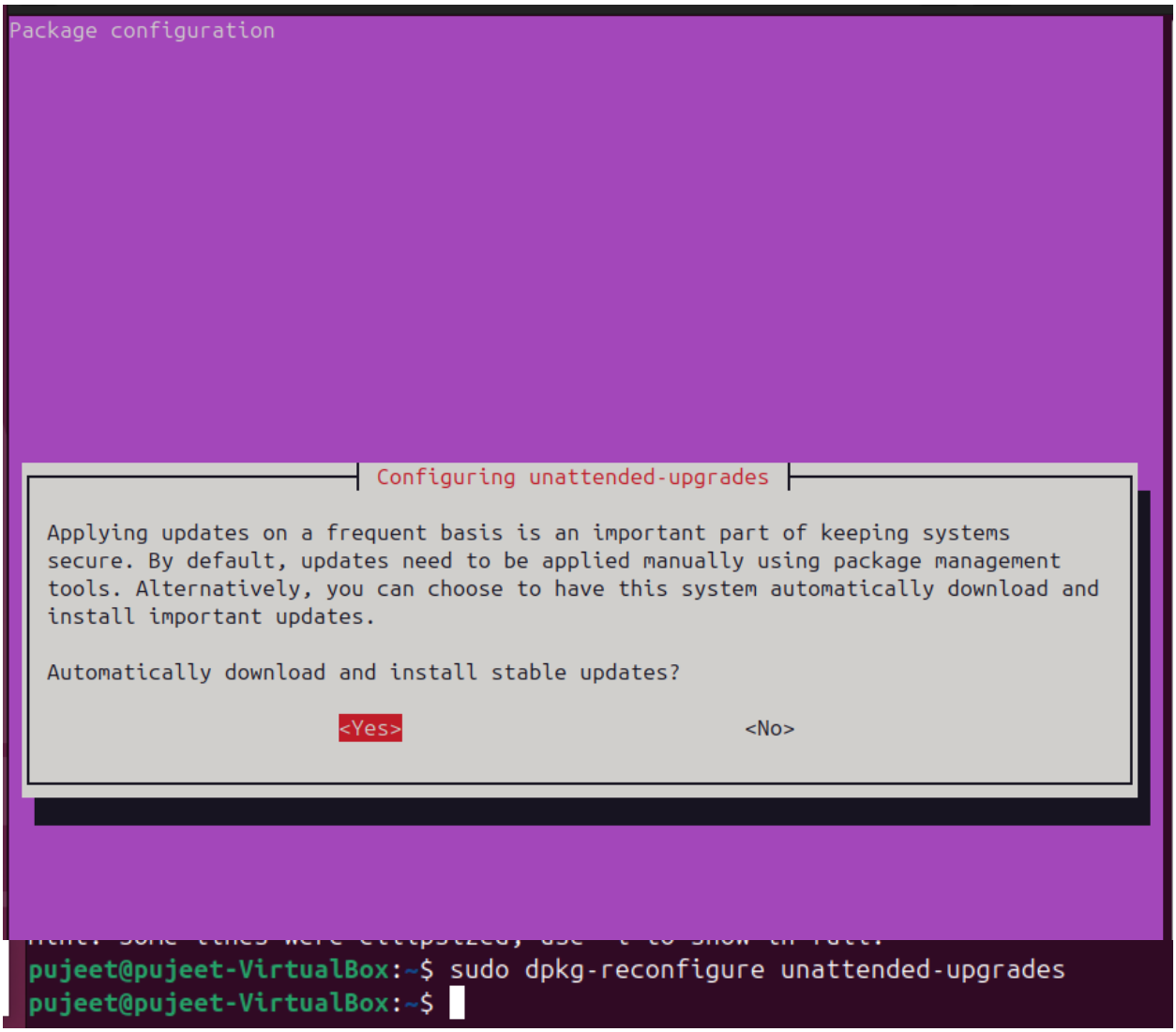
📸 **Figure 5.3 – nginx service running under AppArmor confinement**

5.3 Automatic Security Updates (Unattended Upgrades)

Automatic security updates were enabled to ensure timely patching of known vulnerabilities.

Configuration

```
sudo dpkg-reconfigure unattended-upgrades
```



Automatic updates were enabled by selecting **Yes**.

Figure 5.4 – Enabling unattended security upgrades

Service Verification

```
systemctl status unattended-upgrades --no-pager
```

```
pujeet@pujeet-VirtualBox:~$ systemctl status unattended-upgrades --no-pager
● unattended-upgrades.service - Unattended Upgrades Shutdown
     Loaded: loaded (/usr/lib/systemd/system/unattended-upgrades.service; enabled; preset:
enabled)
     Active: active (running) since Sun 2025-12-28 22:14:18 GMT; 51min ago
       Docs: man:unattended-upgrade(8)
   Main PID: 1249 (unattended-upgr)
      Tasks: 2 (limit: 4601)
     Memory: 11.0M (peak: 11.4M)
        CPU: 119ms
     CGroup: /system.slice/unattended-upgrades.service
             └─1249 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shu…

Dec 28 22:14:18 pujeet-VirtualBox systemd[1]: Started unattended-upgrades.service - Un…own.
Hint: Some lines were ellipsized, use -l to show in full.
```

The service was confirmed to be active and running.

📸 **Figure 5.5 – unattended-upgrades service running**

Configuration File Validation

```
cat /etc/apt/apt.conf.d/20auto-upgrades
```

```
pujeet@pujeet-VirtualBox:~$ cat /etc/apt/apt.conf.d/20auto-upgrades
APT::Periodic::Update-Package-Lists "1";
APT::Periodic::Unattended-Upgrade "1";
```

The output confirmed that both automatic update checks and unattended upgrades were enabled.

📸 **Figure 5.6 – Automatic update configuration (20auto-upgrades)**

5.4 Intrusion Detection – Fail2Ban

Fail2Ban was implemented to protect the system against brute-force attacks by monitoring authentication logs and dynamically banning offending IP addresses.

Service Status

```
sudo systemctl status fail2ban --no-pager
```

```
pujeet@pujeet-VirtualBox:~$ sudo systemctl status fail2ban --no-pager
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-12-28 22:14:18 GMT; 54min ago
       Docs: man:fail2ban(1)
   Main PID: 1240 (fail2ban-server)
      Tasks: 5 (limit: 4601)
     Memory: 30.5M (peak: 31.0M)
        CPU: 4.786s
     CGroup: /system.slice/fail2ban.service
             └─1240 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Dec 28 22:14:18 pujeet-VirtualBox systemd[1]: Started fail2ban.service - Fail2Ban Service.
Dec 28 22:14:18 pujeet-VirtualBox fail2ban-server[1240]: 2025-12-28 22:14:18,957 fail2b…to'
Dec 28 22:14:19 pujeet-VirtualBox fail2ban-server[1240]: Server ready
Hint: Some lines were ellipsized, use -l to show in full.
```

📸 **Figure 5.7 – Fail2Ban service running**

Jail Verification

```
sudo fail2ban-client status
```

The output confirmed that the SSH jail was active.

📸 **Figure 5.8 – Fail2Ban active jails**

SSH Jail Details

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

```
pujeet@pujeet-VirtualBox:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
```

The SSH jail was actively monitoring authentication attempts with no banned IPs during normal operation.

Figure 5.9 – Fail2Ban SSH jail status

5.5 Security Baseline Verification Script

A custom script (`security-baseline.sh`) was executed to automatically verify that all security controls from Phases 4 and 5 were correctly enforced.

```
./security-baseline.sh
```

```
pujeet@pujeet-VirtualBox:~$ ./security-baseline.sh
Security Baseline Verification - Sun Dec 28 11:10:49 PM GMT 2025
Hostname: pujeet-VirtualBox
User: pujeet

============================================================
1) SSH Hardening (Phase 4)
============================================================
[PASS] PermitRootLogin is set to 'no'
[PASS] PasswordAuthentication is set to 'no'
[PASS] SSH service is active

============================================================
2) Firewall (UFW) (Phase 4)
============================================================
[PASS] UFW firewall is active

[INFO] Current UFW rules:
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22/tcp                     ALLOW IN    Anywhere
[ 2] 22/tcp                     ALLOW IN    192.168.56.1
[ 3] 22/tcp (v6)                ALLOW IN    Anywhere (v6)

[FAIL] SSH appears restricted to workstation IP (192.168.56.1)

============================================================
3) Mandatory Access Control - AppArmor (Phase 5)
============================================================
[PASS] AppArmor service is active
[PASS] nginx is confined (enforced) by AppArmor (or system has enforced profiles)

[INFO] AppArmor status summary:
apparmor module is loaded.
182 profiles are loaded.
83 profiles are in enforce mode.
   /snap/snapd/24792/usr/lib/snapd/snap-confine
   /snap/snapd/24792/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-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/bin/pidgin
   /usr/bin/pidgin//sanitized_helper
   /usr/bin/totem
   /usr/bin/totem-audio-preview
   /usr/bin/totem-video-thumbnailer
   /usr/bin/totem//sanitized_helper
   /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
   apt-cacher-ng
   avahi-daemon
   dnsmasq
   dnsmasq//libvirt_leaseshelper
   identd
   klogd
   lsb_release
   man_filter
   man_groff
   mdnsd
   nmbd
   nscd
   nvidia_modprobe
   nvidia_modprobe//kmod
   php-fpm
   ping
   plasmashell
   plasmashell//QtWebEngineProcess
   rsyslogd
   samba-bgqd
   samba-dcerpcd
   samba-rpcd
   samba-rpcd-classic
   samba-rpcd-spoolss
```

```
samba-rpcd-classic
samba-rpcd-spoolss
smbd
smbldap-useradd
smbldap-useradd///etc/init.d/nscd
snap-update-ns.firefox
snap-update-ns.firmware-updater
snap-update-ns.snap-store
snap-update-ns.snapd-desktop-integration
snap.firefox.firefox
snap.firefox.geckodriver
snap.firefox.hook.configure
snap.firefox.hook.disconnect-plug-host-hunspell
snap.firefox.hook.install
snap.firefox.hook.post-refresh
snap.firmware-updater.firmware-notifier
snap.firmware-updater.firmware-updater
snap.firmware-updater.firmware-updater-app
snap.firmware-updater.hook.configure
snap.snap-store.hook.configure
snap.snap-store.show-updates
snap.snap-store.snap-store
snap.snapd-desktop-integration.hook.configure
snap.snapd-desktop-integration.snapd-desktop-integration
syslog-ng
syslogd
tcpdump
traceroute
ubuntu_pro_apt_news
ubuntu_pro_esm_cache
ubuntu_pro_esm_cache//apt_methods
ubuntu_pro_esm_cache//apt_methods_gpgv
ubuntu_pro_esm_cache//cloud_id
ubuntu_pro_esm_cache//dpkg
ubuntu_pro_esm_cache//ps
ubuntu_pro_esm_cache//ubuntu_distro_info
ubuntu_pro_esm_cache_systemctl
ubuntu_pro_esm_cache_systemd_detect_virt
unix-chkpwd
unprivileged_userns
```

```
7 profiles are in complain mode.
   /usr/bin/irssi
   /usr/sbin/nginx
   /usr/sbin/sssd
   transmission-cli
   transmission-daemon
   transmission-gtk
   transmission-qt
0 profiles are in prompt mode.
0 profiles are in kill mode.
92 profiles are in unconfined mode.
   1password
   Discord
   MongoDB Compass
   QtWebEngineProcess
   balena-etcher
   brave
   buildah
   busybox
   cam
   ch-checkns
   ch-run
   chrome
   crun
   desktop-icons-ng
   devhelp
   element-desktop
   epiphany
   evolution
   firefox
   flatpak
   foliate
   geary
   github-desktop
   goldendict
   ipa_verify
   kchmviewer
   keybase
   lc-compliance
   libcamerify
   linux-sandbox
   loupe
```

```
linux-sandbox
loupe
lxc-attach
lxc-create
lxc-destroy
lxc-execute
lxc-stop
lxc-unshare
lxc-usernsexec
mmdebstrap
msedge
nautilus
notepadqq
obsidian
opam
opera
pageedit
podman
polypane
privacybrowser
qcam
qmapshack
qutebrowser
rootlesskit
rpm
rssguard
runc
sbuild
sbuild-abort
sbuild-adduser
sbuild-apt
sbuild-checkpackages
sbuild-clean
sbuild-createchroot
sbuild-destroychroot
sbuild-distupgrade
sbuild-hold
sbuild-shell
sbuild-unhold
sbuild-update
sbuild-upgrade
scide
```

```
   scide
   signal-desktop
   slack
   slirp4netns
   steam
   stress-ng
   surfshark
   systemd-coredump
   thunderbird
   toybox
   trinity
   tup
   tuxedo-control-center
   userbindmount
   uwsgi-core
   vdens
   virtiofsd
   vivaldi-bin
   vpnns
   vscode
   wike
   wpcom
24 processes have profiles defined.
19 processes are in enforce mode.
   /usr/sbin/cups-browsed (1282)
   /usr/sbin/cupsd (1239)
   /usr/sbin/avahi-daemon (772) avahi-daemon
   /usr/sbin/avahi-daemon (928) avahi-daemon
   /usr/sbin/rsyslogd (910) rsyslogd
   /snap/firefox/7559/usr/lib/firefox/firefox (3390) snap.firefox.firefox
   /snap/firefox/7559/usr/lib/firefox/crashhelper (3455) snap.firefox.firefox
   /snap/firefox/7559/usr/lib/firefox/firefox (3532) snap.firefox.firefox
   /snap/firefox/7559/usr/lib/firefox/firefox (3537) snap.firefox.firefox
   /snap/firefox/7559/usr/lib/firefox/firefox (3571) snap.firefox.firefox
   /snap/firefox/7559/usr/lib/firefox/firefox (3582) snap.firefox.firefox
   /snap/firefox/7559/usr/lib/firefox/firefox (3785) snap.firefox.firefox
   /snap/firefox/7559/usr/lib/firefox/firefox (4156) snap.firefox.firefox
   /snap/firefox/7559/usr/lib/firefox/firefox (4162) snap.firefox.firefox
   /snap/firefox/7559/usr/lib/firefox/firefox (4177) snap.firefox.firefox
   /snap/firefox/7559/usr/lib/firefox/firefox (4188) snap.firefox.firefox
   /snap/firefox/7559/usr/lib/firefox/firefox (4386) snap.firefox.firefox
```

```
   /snap/firefox/7559/usr/lib/firefox/firefox (3582) snap.firefox.firefox
   /snap/firefox/7559/usr/lib/firefox/firefox (3785) snap.firefox.firefox
   /snap/firefox/7559/usr/lib/firefox/firefox (4156) snap.firefox.firefox
   /snap/firefox/7559/usr/lib/firefox/firefox (4162) snap.firefox.firefox
   /snap/firefox/7559/usr/lib/firefox/firefox (4177) snap.firefox.firefox
   /snap/firefox/7559/usr/lib/firefox/firefox (4188) snap.firefox.firefox
   /snap/firefox/7559/usr/lib/firefox/firefox (4386) snap.firefox.firefox
   /snap/snapd-desktop-integration/315/usr/bin/snapd-desktop-integration (2544) snap.snapd-
desktop-integration.snapd-desktop-integration
   /snap/snapd-desktop-integration/315/usr/bin/snapd-desktop-integration (2600) snap.snapd-
desktop-integration.snapd-desktop-integration
4 processes are in complain mode.
   /usr/sbin/nginx (1297)
   /usr/sbin/nginx (1298)
   /usr/sbin/nginx (1299)
   /usr/sbin/nginx (1300)
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 (3218) desktop-icons-ng
0 processes are in mixed mode.

============================================================
4) Automatic Security Updates (Phase 5)
============================================================
[PASS] unattended-upgrades service is active
[PASS] Auto update package lists enabled (20auto-upgrades)
[PASS] Unattended upgrades enabled (20auto-upgrades)

[INFO] /etc/apt/apt.conf.d/20auto-upgrades:
APT::Periodic::Update-Package-Lists "1";
APT::Periodic::Unattended-Upgrade "1";

============================================================
5) Intrusion Detection - Fail2Ban (Phase 5)
============================================================
[PASS] Fail2Ban service is active
[PASS] Fail2Ban sshd jail is available

[INFO] Fail2Ban status:
Status
```

```
0 processes are in kill mode.
1 processes are unconfined but have a profile defined.
   /usr/bin/gjs-console (3218) desktop-icons-ng
0 processes are in mixed mode.

============================================================
4) Automatic Security Updates (Phase 5)
============================================================
[PASS] unattended-upgrades service is active
[PASS] Auto update package lists enabled (20auto-upgrades)
[PASS] Unattended upgrades enabled (20auto-upgrades)

[INFO] /etc/apt/apt.conf.d/20auto-upgrades:
APT::Periodic::Update-Package-Lists "1";
APT::Periodic::Unattended-Upgrade "1";

============================================================
5) Intrusion Detection - Fail2Ban (Phase 5)
============================================================
[PASS] Fail2Ban service is active
[PASS] Fail2Ban sshd jail is available

[INFO] Fail2Ban status:
Status
|- Number of jail:      1
`- Jail list:   sshd

[INFO] Fail2Ban sshd jail status:
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:

============================================================
6) Service Status Check (Support Evidence)
============================================================
[PASS] nginx service is active

===== BASELINE CHECK COMPLETE =====
pujeet@pujeet-VirtualBox:~$
```

The script confirmed:

- SSH hardening enforced
- Firewall enabled
- AppArmor active
- Automatic updates enabled
- Fail2Ban running
- nginx service active

📸 **Figure 5.10 – Automated security baseline verification script output**

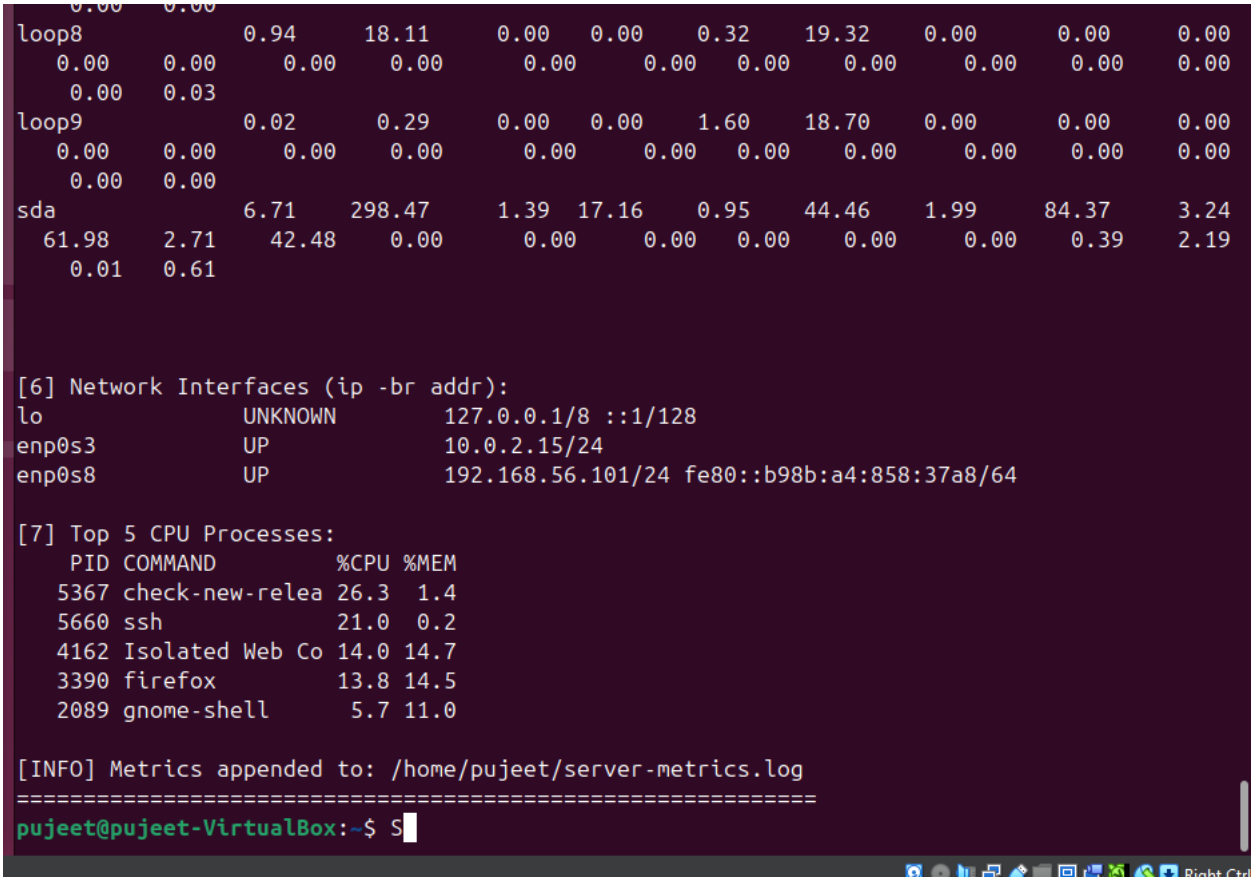
5.6 Remote Monitoring Script

A monitoring script (`monitor-server.sh`) was executed remotely via SSH to collect live system performance metrics.

```
./monitor-server.sh
```

```
pujeet@pujeet-VirtualBox:~$ ./monitor-server.sh
============================================================
REMOTE MONITOR SNAPSHOT: Sun Dec 28 11:14:28 PM GMT 2025
Target: pujeet@192.168.56.101
============================================================

[1] Uptime + Load:
 23:14:28 up  1:00,  2 users,  load average: 1.11, 0.82, 0.57

[2] CPU Usage (top snapshot):
%Cpu(s): 24.1 us, 17.2 sy,  0.0 ni, 55.2 id,  3.4 wa,  0.0 hi,  0.0 si,  0.0 st

[3] Memory Usage (free -h):
               total        used        free      shared  buff/cache   available
Mem:           3.8Gi       1.9Gi       454Mi        65Mi       1.6Gi       2.0Gi
Swap:          3.8Gi          0B       3.8Gi

[4] Disk Usage (df -h):
Filesystem      Size  Used Avail Use% Mounted on
tmpfs           392M  1.6M  391M   1% /run
/dev/sda3        22G   11G  9.4G  54% /
tmpfs           2.0G     0  2.0G   0% /dev/shm
tmpfs           5.0M  8.0K  5.0M   1% /run/lock
tmpfs           392M  124K  392M   1% /run/user/1000
```

```
[5] Disk I/O (iostat, if available):
Linux 6.14.0-37-generic (pujeet-VirtualBox)     12/28/2025      _x86_64_        (3 CPU)

Device            r/s     rkB/s   rrqm/s  %rrqm r_await rareq-sz     w/s     wkB/s   wrqm/s
  %wrqm w_await wareq-sz     d/s     dkB/s   drqm/s  %drqm d_await dareq-sz     f/s f_await
  aqu-sz  %util
loop0            0.00      0.00     0.00   0.00    0.07     1.21    0.00      0.00     0.00
   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00    0.00
    0.00   0.00
loop1            0.11      1.39     0.00   0.00    0.40    12.44    0.00      0.00     0.00
   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00    0.00
    0.00   0.00
loop10           0.02      0.48     0.00   0.00    0.91    19.27    0.00      0.00     0.00
   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00    0.00
    0.00   0.00
loop11           0.01      0.10     0.00   0.00    0.89     8.04    0.00      0.00     0.00
   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00    0.00
    0.00   0.00
loop12           0.01      0.09     0.00   0.00    0.69     9.49    0.00      0.00     0.00
   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00    0.00
    0.00   0.00
loop13           0.00      0.00     0.00   0.00    0.00     1.27    0.00      0.00     0.00
   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00    0.00
    0.00   0.00
loop2            0.01      0.10     0.00   0.00    1.14     8.09    0.00      0.00     0.00
   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00    0.00
    0.00   0.00
loop3            0.43     22.78     0.00   0.00    0.86    53.03    0.00      0.00     0.00
   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00    0.00
    0.00   0.04
loop4            0.01      0.30     0.00   0.00    1.44    20.07    0.00      0.00     0.00
   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00    0.00
    0.00   0.00
loop5            0.02      0.30     0.00   0.00    1.25    19.32    0.00      0.00     0.00
   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00    0.00
    0.00   0.00
loop6            0.01      0.10     0.00   0.00    0.81     8.09    0.00      0.00     0.00
   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00    0.00
    0.00   0.00
loop7            0.78      3.41     0.00   0.00    0.07     4.37    0.00      0.00     0.00
   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00    0.00
    0.00   0.00
loop8            0.94     18.11     0.00   0.00    0.32    19.32    0.00      0.00     0.00
   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00    0.00
    0.00   0.03
```



Metrics collected included CPU usage, memory usage, disk utilisation, network interfaces, and top resource-consuming processes.

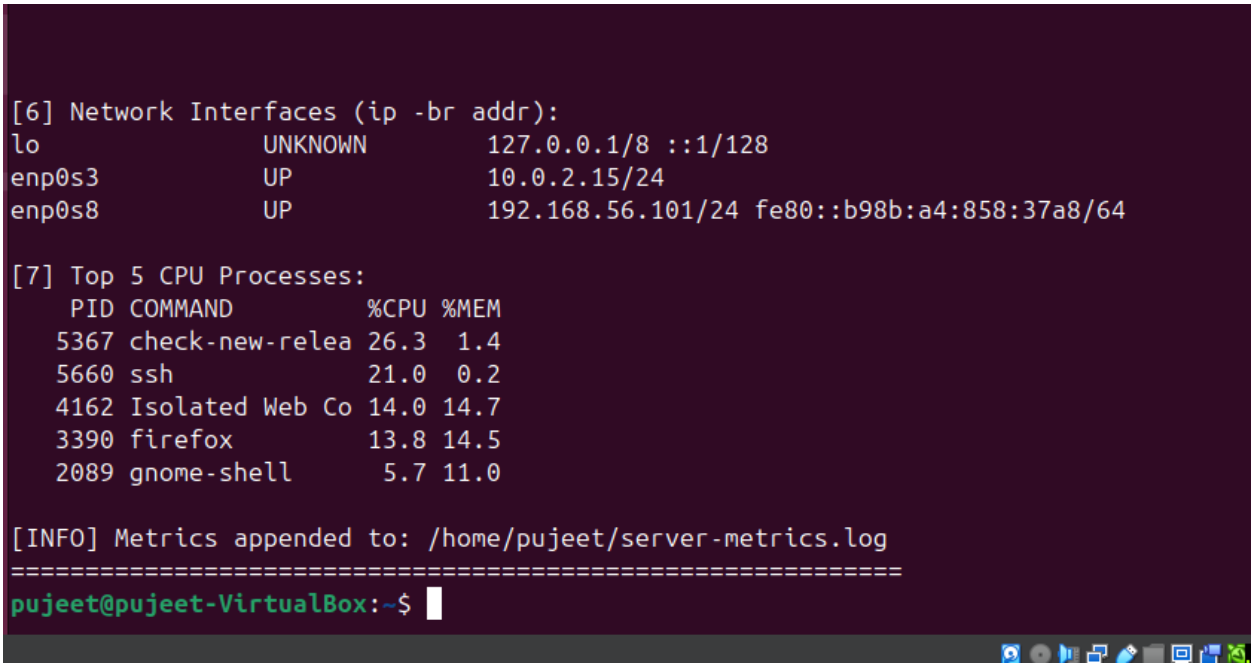
📸 **Figure 5.11 – Live server monitoring via SSH**

Persistent Metrics Logging

Logged metrics were verified using:

```
tail -n 30 ~/server-metrics.log
```

```
pujeet@pujeet-VirtualBox:~$ tail -n 30 ~/server-metrics.log
loop11           0.01      0.10     0.00   0.00    0.89     8.04    0.00      0.00     0.00
   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00    0.00
    0.00   0.00
loop12           0.01      0.09     0.00   0.00    0.69     9.49    0.00      0.00     0.00
   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00    0.00
    0.00   0.00
loop13           0.00      0.00     0.00   0.00    0.00     1.27    0.00      0.00     0.00
   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00    0.00
    0.00   0.00
loop2            0.01      0.10     0.00   0.00    1.14     8.09    0.00      0.00     0.00
   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00    0.00
    0.00   0.00
loop3            0.43     22.78     0.00   0.00    0.86    53.03    0.00      0.00     0.00
   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00    0.00
    0.00   0.04
loop4            0.01      0.30     0.00   0.00    1.44    20.07    0.00      0.00     0.00
   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00    0.00
    0.00   0.00
loop5            0.02      0.30     0.00   0.00    1.25    19.32    0.00      0.00     0.00
   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00    0.00
    0.00   0.00
loop6            0.01      0.10     0.00   0.00    0.81     8.09    0.00      0.00     0.00
   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00    0.00
    0.00   0.00
loop7            0.78      3.41     0.00   0.00    0.07     4.37    0.00      0.00     0.00
   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00    0.00
    0.00   0.00
loop8            0.94     18.11     0.00   0.00    0.32    19.32    0.00      0.00     0.00
   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00    0.00
    0.00   0.03
loop9            0.02      0.29     0.00   0.00    1.60    18.70    0.00      0.00     0.00
   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00    0.00
    0.00   0.00
sda              6.71    298.47     1.39  17.16    0.95    44.46    1.99     84.37     3.24
  61.98    2.71    42.48    0.00      0.00     0.00   0.00    0.00     0.00    0.39    2.19
    0.01   0.61
```



This confirms that performance data is persistently recorded for later analysis.

Figure 5.12 – Persistent server metrics log

5.7 Reflection

The implementation of AppArmor, unattended upgrades, and Fail2Ban significantly strengthened the system's defence-in-depth strategy. While these controls introduce additional configuration complexity, the use of automated verification and monitoring scripts reduces operational overhead and improves reliability.

This phase demonstrates professional Linux server security practices commonly used in enterprise and cloud environments, balancing **security, automation, and manageability**.