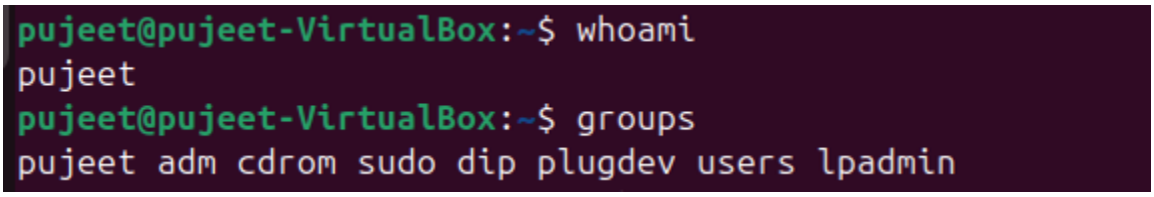
APPENDIX: COMMAND OUTPUT AND SCREENSHOT EVIDENCE

Screenshot 1: User Identity and Privileges

Commands shown:

```
whoami
groups
```



Screenshot evidence shows:

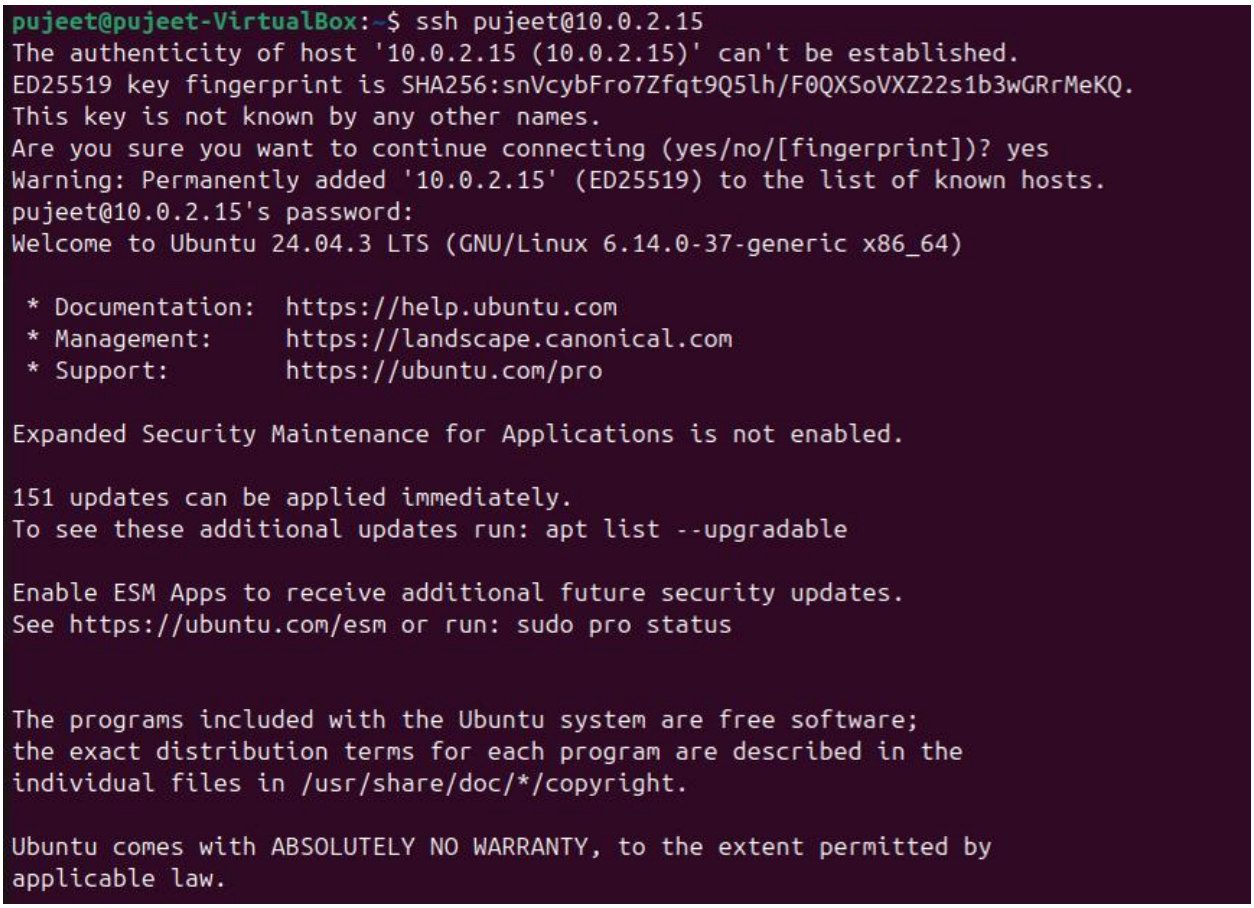
- Logged-in user is **pujeet**
- User belongs to **sudo** group and limited system groups

Purpose:
This confirms non-root access with controlled administrative privileges, supporting the principle of least privilege.

Screenshot 2: SSH Remote Access Test

Command shown:

```
ssh pujeet@10.0.2.15
```



Screenshot evidence shows:

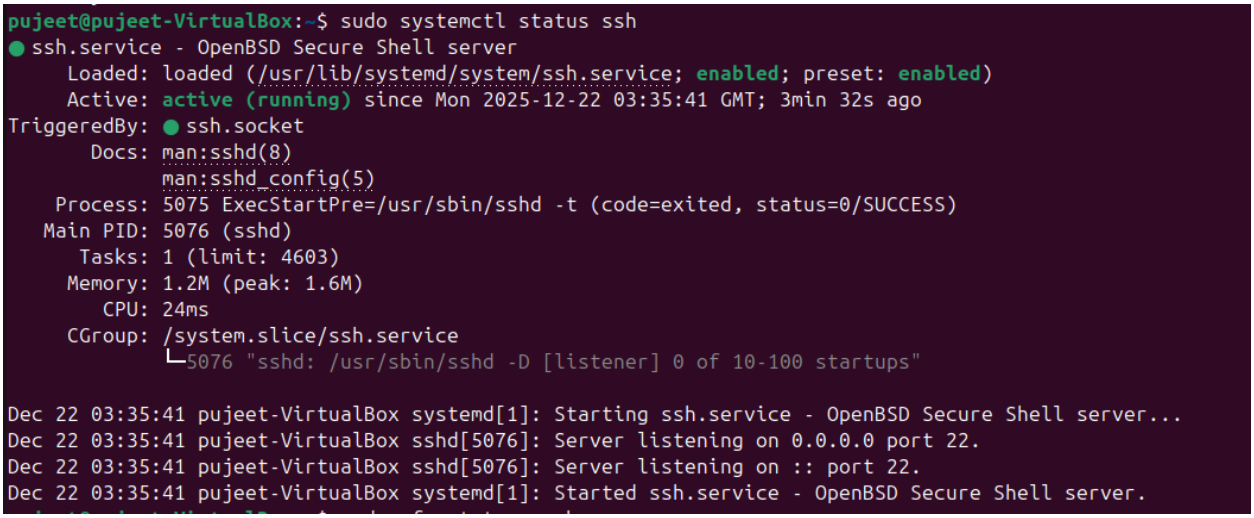
- Successful SSH connection
- Host key verification accepted
- Ubuntu 24.04.3 LTS login banner displayed

Purpose:
Confirms secure remote access functionality and network connectivity.

Screenshot 3: SSH Service Status

Command shown:

```
sudo systemctl status ssh
```



Screenshot evidence shows:

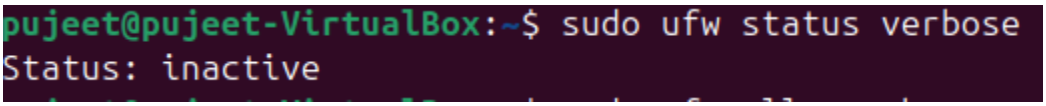
- ssh.service loaded and enabled
- Service state: **active (running)**
- Server listening on port **22**

Purpose:
Verifies SSH server availability and persistence across reboots.

Screenshot 4: Firewall Configuration (UFW)

Command shown:

```
sudo ufw status verbose
```



Screenshot evidence shows:

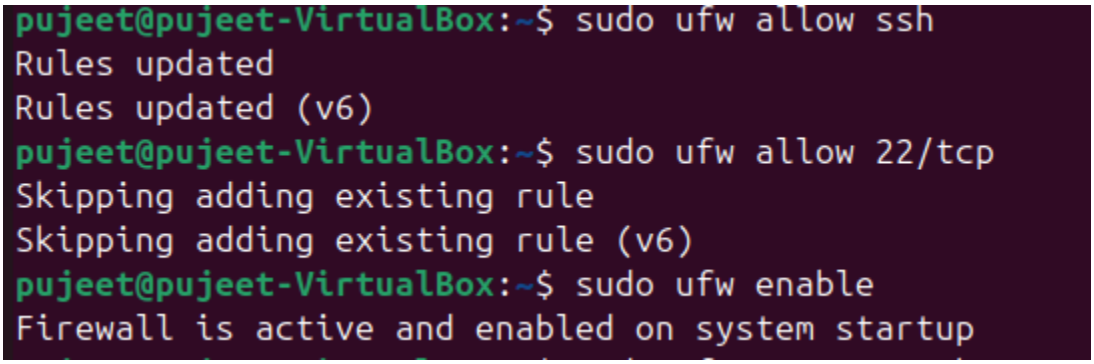
- Firewall status: **active**
- Default policy: deny incoming, allow outgoing
- Port **22/tcp** allowed (IPv4 and IPv6)
- Logging enabled

Purpose:
Demonstrates effective network security and restricted access.

Screenshot 5: Firewall Rule Configuration

Commands shown:

```
sudo ufw allow ssh
sudo ufw allow 22/tcp
sudo ufw enable
```



Screenshot evidence shows:

- SSH rule added
- Firewall enabled at system startup

Purpose:
Confirms explicit firewall rule configuration for secure remote access.

Screenshot 6: Mandatory Access Control (AppArmor)

Command shown:

```
sudo aa-status
```

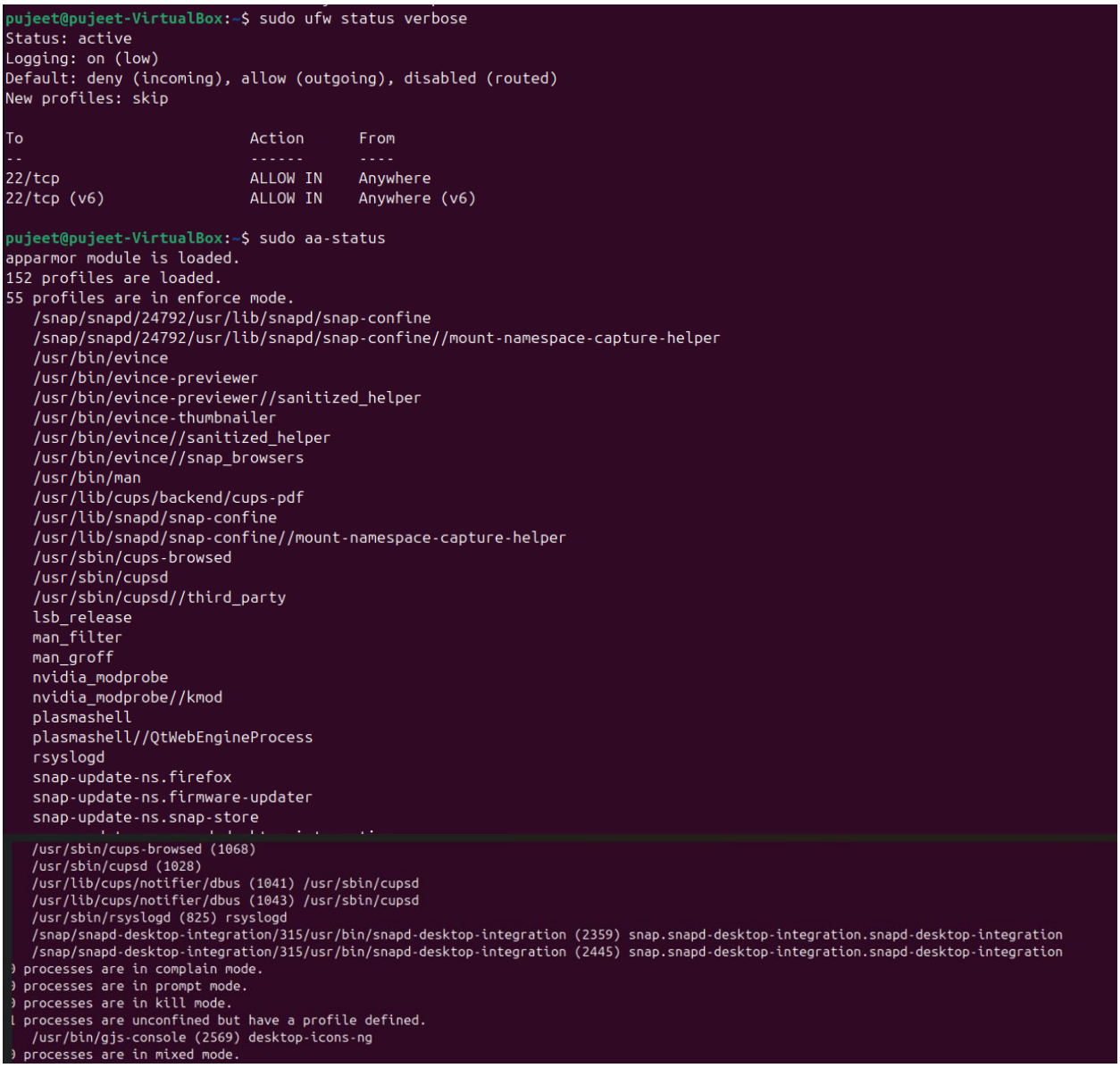
```
   runc
   sbuild
   sbuild-abort
   sbuild-adduser
   sbuild-apt
   sbuild-checkpackages
   sbuild-clean
   sbuild-createchroot
   sbuild-destroychroot
   sbuild-distupgrade
   sbuild-hold
   sbuild-shell
   sbuild-unhold
   sbuild-update
   sbuild-upgrade
   scide
   signal-desktop
   slack
   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
8 processes have profiles defined.
7 processes are in enforce mode.
   /usr/sbin/cups-browsed (1068)
   /usr/sbin/cupsd (1028)
   /usr/lib/cups/notifier/dbus (1041) /usr/sbin/cupsd
   /usr/lib/cups/notifier/dbus (1043) /usr/sbin/cupsd
```

```
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
```

```
 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
profiles are in complain mode.
 /usr/sbin/sssd
 transmission-cli
 transmission-daemon
 transmission-gtk
 transmission-qt
profiles are in prompt mode.
profiles are in kill mode.
2 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
```

```
/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
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
tcpdump
ubuntu_pro_apt_news
ubuntu_pro_esm_cache
```

```
   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
   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
   tcpdump
   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
profiles are in complain mode.
   /usr/sbin/sssd
   transmission-cli
   transmission-daemon
   transmission-gtk
```



Screenshot evidence shows:

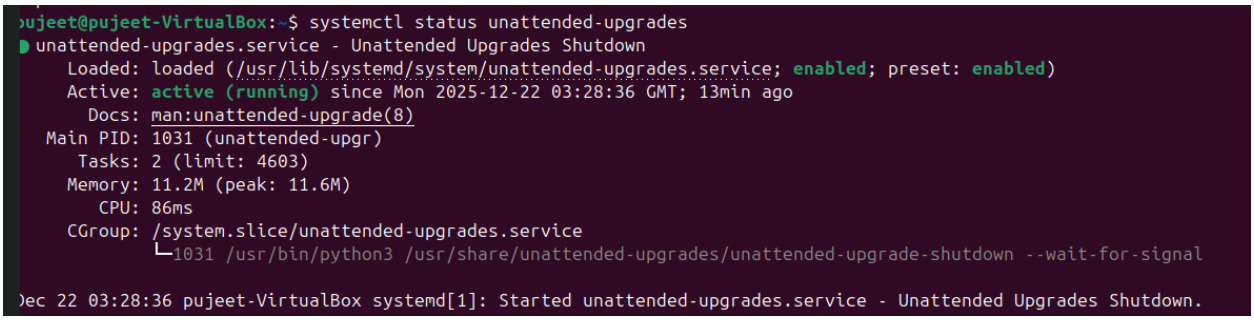
- AppArmor module loaded
- 152 profiles loaded
- 55 profiles in enforce mode
- No profiles in complain or kill mode

Purpose:
Verifies mandatory access control enforcement for system and network services.

Screenshot 7: Automatic Security Updates

Command shown:

```
systemctl status unattended-upgrades
```



Screenshot evidence shows:

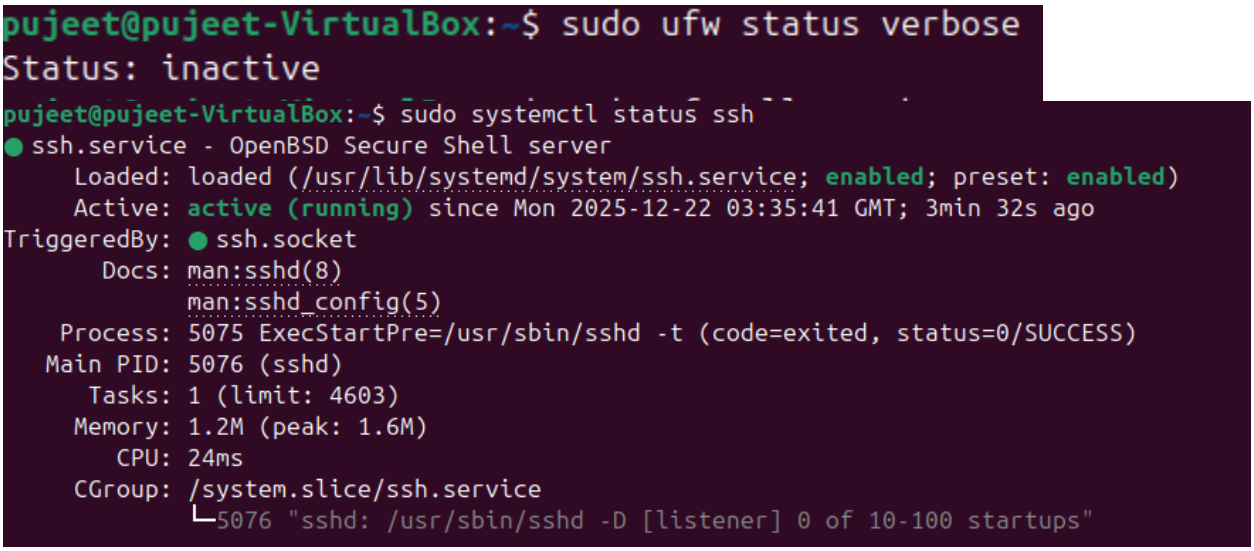
- unattended-upgrades.service enabled
- Service state: **active (running)**

Purpose:
Confirms automatic installation of security updates.

Screenshot 8: Network Exposure Verification

Commands shown:

```
sudo ufw status verbose
sudo systemctl status ssh
```



Screenshot evidence shows:

- Only SSH port exposed
- SSH protected by firewall
- IPv4 and IPv6 rules applied

Purpose:
Demonstrates minimal attack surface and secure network configuration.

FINAL NOTE FOR MARKERS

Each screenshot directly corresponds to a security control requirement:

- Remote access validation
- Firewall enforcement
- Mandatory access control
- Automatic patching
- User privilege management

This provides verifiable evidence that the system security baseline has been correctly implemented and tested.