Guardian Toolkit - Phase 1 Summary

UFW (Uncomplicated Firewall) - Installed

- UFW firewall installed using apt.
- Default incoming set to deny, outgoing to allow.
- UFW service enabled and running at startup.
- Confirmed rules via `sudo ufw status verbose`.

fail2ban - Installed

- fail2ban installed and service enabled.
- Tested using `sudo systemctl status fail2ban`.
- Lynis audit flagged config as 'UNSAFE' will harden later.
- Used for SSH brute-force protection.

arp-scan - Installed

- arp-scan installed via apt.
- Used to scan local network for connected devices.
- Example: `sudo arp-scan --interface=eth0 --localnet`.
- Useful for detecting unknown or rogue devices.

clamav + clamtk - Installed

- clamav antivirus installed and updated with freshclam.
- clamtk (GUI) installed for ease of use.
- ClamTK GUI launched successfully and configured.
- Confirmed scan options and quarantine setup.

lynis - Installed

- Lynis installed via apt.
- Performed a full audit with `sudo lynis audit system`.
- Output showed UNSAFE flags for services.
- Next step: Address UNSAFE flags and harden system.

nmap - Installed

- Installed nmap for port scanning.
- Tested with basic scans like `nmap localhost`.
- Ready for remote and internal scanning scenarios.
- Important tool for auditing open ports on LAN.

Guardian service - Added

- Custom 'guardian.service' added for persistent monitoring.
- Flagged as UNSAFE by Lynis will be reviewed in Phase 2.
- Designed to run lightweight network scans and alerts.
- Planned for future automation and notifications.