**Project 3: Secure Linux Server Setup & Hardening**

**Analyst:** Ramjith M  
**Date:** 6 July 2025  
**Target System:** Ubuntu Server 20.04.6 LTS  
**Host:** baseubuntu (192.168.29.43)  
**Environment:** VirtualBox VM

**1. Project Overview**

This project involved securing a freshly deployed Ubuntu 20.04 server using the **CIS Benchmark v3.0.0** for Ubuntu 20.04 LTS.  
I cross-referenced the configuration manually using the **CIS PDF** and validated results with automated tools like **OpenVAS**, and **Nmap**.

The goal was to:

* Harden SSH access
* Enforce PAM and password policies
* Configure auditing, logging, and firewall
* Apply kernel and service-level hardening
* Validate with vulnerability scanning

**2. Tools & Environment**

| **Category** | **Tools Used** |
| --- | --- |
| Virtualization | VirtualBox 7.x |
| Operating System | Ubuntu Server 20.04.6 LTS |
| Hardening Guide | CIS Benchmark for Ubuntu 20.04 LTS v3.0.0 |
| Configuration Tools | nano, systemctl, chage, modprobe |
| Security Tools | auditd, fail2ban, AppArmor, rkhunter, chkrootkit |
| Assessment Tools | OpenVAS, Nmap |

**3. Step-by-Step Hardening Summary**

**SSH Hardening (CIS 5.2.x)**

* PermitRootLogin no, PasswordAuthentication no
* Port 54321, MaxAuthTries 2, X11Forwarding no
* ClientAliveInterval 300, ClientAliveCountMax 0
* MACs hmac-sha2-512,hmac-sha2-256
* Verified using sshd -t && systemctl restart sshd

**PAM & Password Policy (CIS 5.4.1)**

* /etc/pam.d/common-password

password requisite pam\_pwquality.so retry=3 minlen=14 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1

* Set password expiry:  
  chage -M 90 -m 7 -W 7 server

**UFW Firewall (CIS 3.4.x)**

sudo ufw default deny incoming

sudo ufw default allow outgoing

sudo ufw allow OpenSSH

sudo ufw enable

**Audit Logging (CIS 4.1.x)**

Rules added to /etc/audit/rules.d/hardening.rules:

-w /etc/passwd -p wa -k passwd\_changes

-w /etc/shadow -p wa -k shadow\_changes

-w /etc/group -p wa -k group\_changes

Reloaded with sudo augenrules --load

**Automatic Updates (CIS 1.9.2)**

* Enabled unattended-upgrades
* Verified via:

cat /etc/apt/apt.conf.d/50unattended-upgrades

**File System & Kernel Hardening**

* /etc/modprobe.d/CIS.conf to disable: cramfs, squashfs, udf, etc.
* /etc/sysctl.conf tuned:

net.ipv4.tcp\_timestamps = 0

fs.suid\_dumpable = 0

kernel.core\_uses\_pid = 1

kernel.kptr\_restrict = 2

kernel.dmesg\_restrict = 1

net.ipv4.conf.all.rp\_filter = 1

net.ipv4.conf.all.send\_redirects = 0

net.ipv4.conf.default.accept\_source\_route = 0

net.ipv4.conf.default.log\_martians = 1

**Bootloader Protection (CIS 1.7.x)**

sudo chmod 400 /boot/grub/grub.cfg

sudo chown root:root /boot/grub/grub.cfg

**Disabled Unused Services (CIS 2.1.x)**

sudo systemctl disable --now ModemManager.service

sudo systemctl disable --now multipathd.service

**4. CIS Compliance Checklist**

| **CIS Control** | **Description** | **Status** | **Command/Location** |
| --- | --- | --- | --- |
| 5.2.3 | Disable root SSH login | Success | sshd\_config |
| 5.3.1 | Set password expiration | Success | chage |
| 3.4.x | Configure firewall (UFW) | Success | ufw |
| 4.1.x | Enable auditd | Success | auditctl, rules.d |
| 5.4.1 | PAM password policy | Success | common-password |
| 1.1.x | Disable unused filesystems | Success | modprobe.d |
| 1.9.2 | Automatic security updates | Success | unattended-upgrades |
| 1.7.x | Secure GRUB bootloader | Success | chmod/chown |
| 2.1.x | Remove unnecessary services | Success | systemctl disable |
| 5.2.4–5.2.6 | SSH timeout + retry limits | Success | sshd\_config |
| 5.2.10 | Disable SSH X11 forwarding | Success | sshd\_config |

**5. Vulnerability Scanning Summary**

**Nmap (Stealth & Version Scan)**

Only port 54321 open (SSH)

Port 22 filtered (stealth mode)

OS guessed as Linux 5.X

**OpenVAS**

High: 0 | Medium: 0 | Low: 0

Findings (post-filter): 0

Initial: 24 (filtered info/debug results)

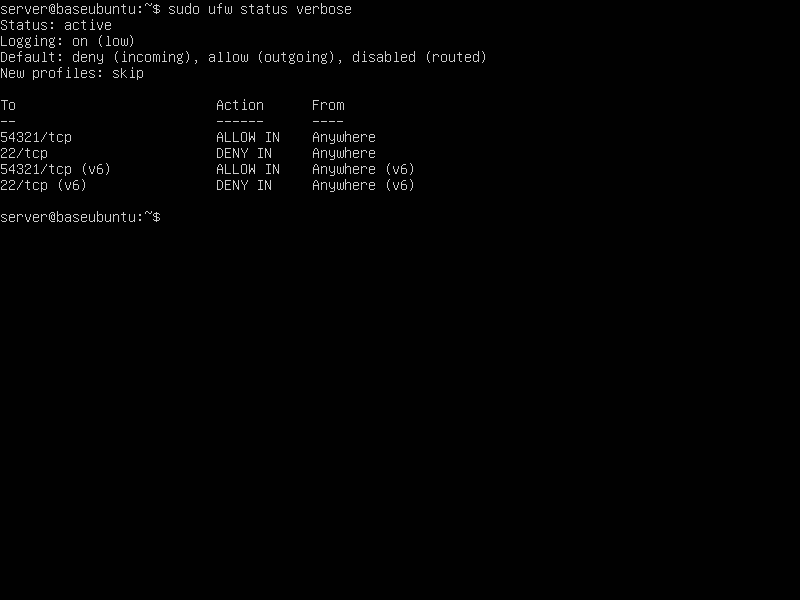
**6. Legal Login Banners**

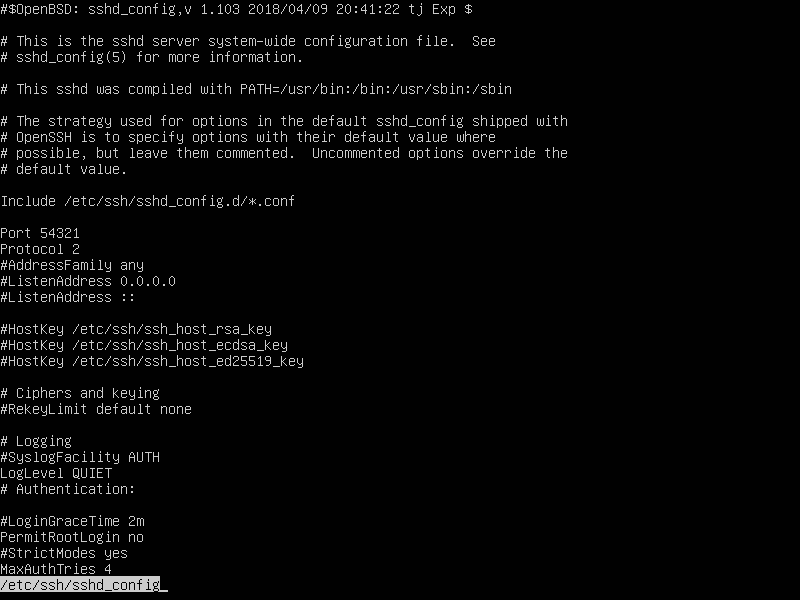
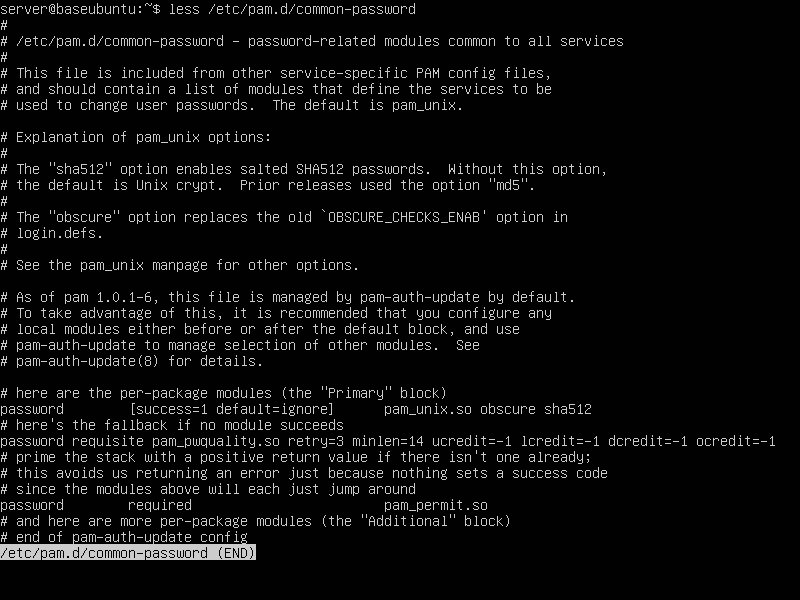
/etc/issue:

"Unauthorized access is prohibited. Activity may be monitored and reported."

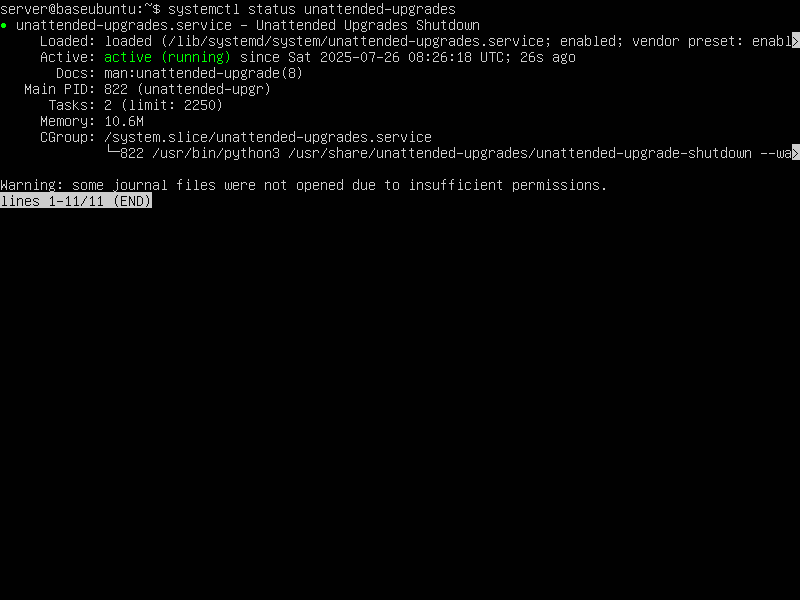
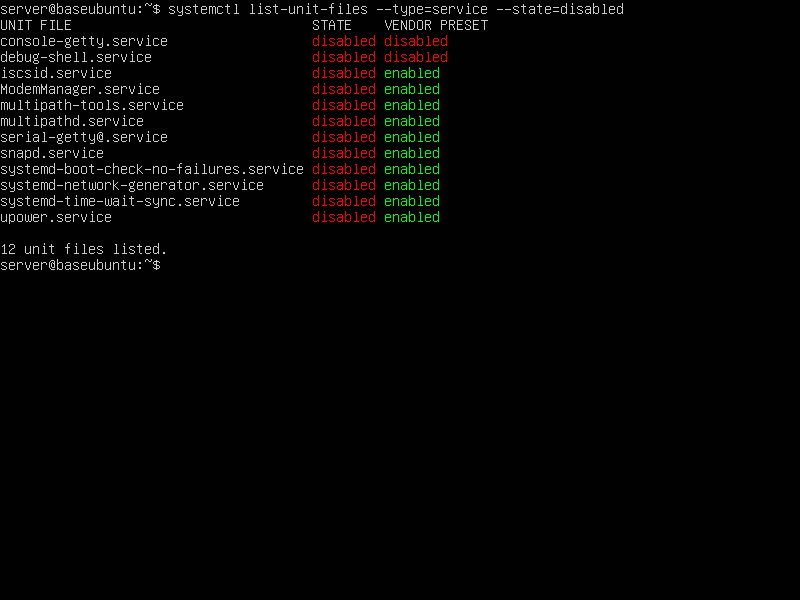
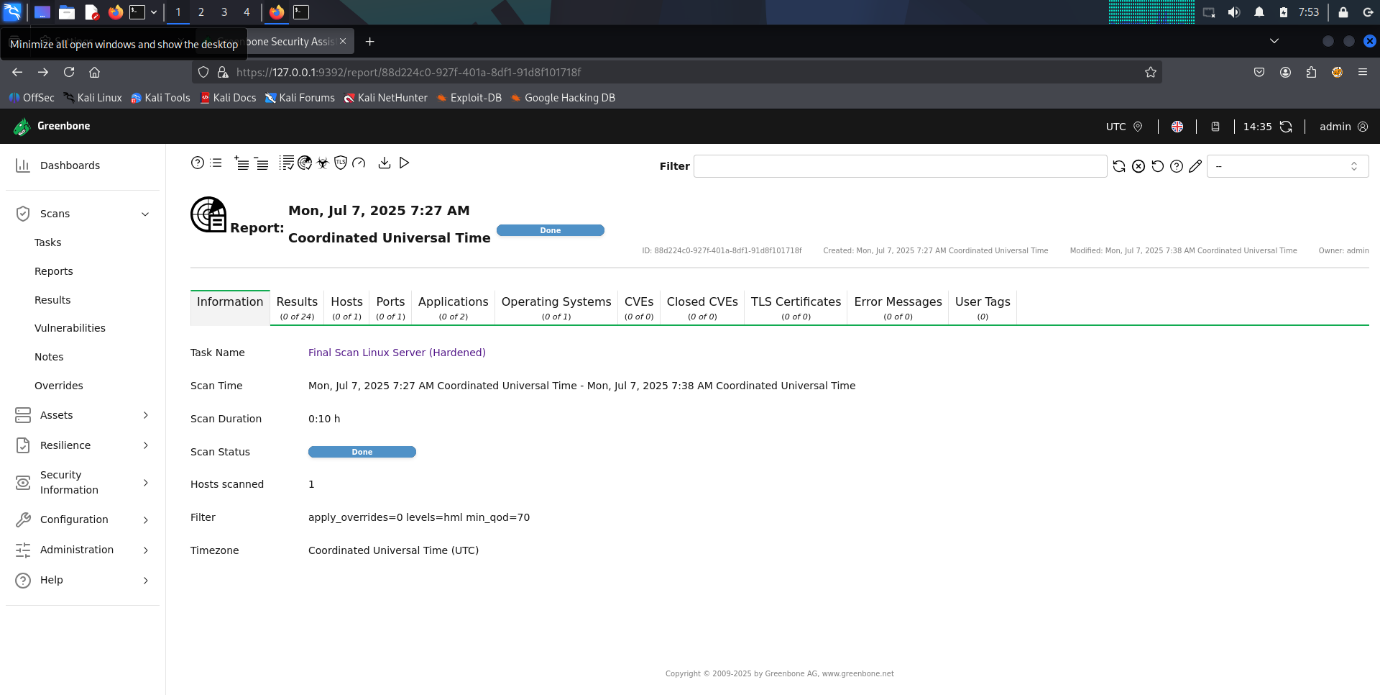
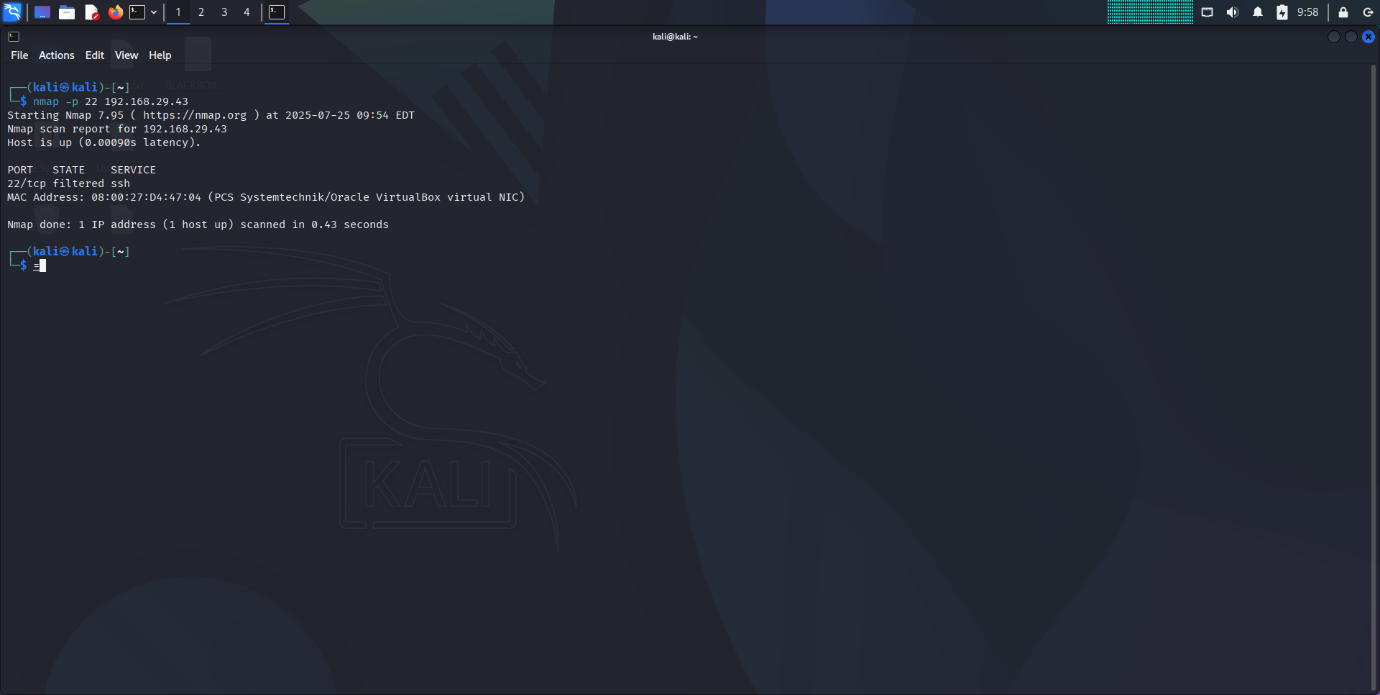
/etc/issue.net:  
"Unauthorized access is prohibited. Activity may be monitored and reported."

**7. Screenshots**

* ufw status verbose   
  Shows active firewall rules  
    
  

* less /etc/ssh/sshd\_config   
  Shows Hardened SSH settings  
    
  
* ls -l /etc/passwd /etc/shadow   
  Shows Permission verification  
    
  
* less /etc/pam.d/common-password   
  Shows Enforced PAM policy  
    
  
* auditctl -l   
  Shows Audit rules loaded



* systemctl status unattended-upgrades  
  Shows status of unattended upgrades  
    
  
* modprobe -n -v cramfs   
  Shows Disabled filesystems check  
    
  
* systemctl list-unit-files --type=service --state=disabled   
  Shows disabled services  
    
  
* ls -l /boot/grub/grub.cfg   
  Shows GRUB protection check  
    
  
* OpenVAS Summary UI   
    
  
* Nmap Output terminal   
    
  

**8. Conclusion**

The Ubuntu 20.04 server has been **systematically hardened** using a combination of **manual CIS benchmark checks**, **vulnerability scans** from **OpenVAS** and **Nmap**.

The result is a **secure, production-ready baseline** for any environment requiring hardened Linux infrastructure.  
This project can be presented as a **security case study** for audits, interviews, or future deployments.