INFOTACT
SOLUTIONS

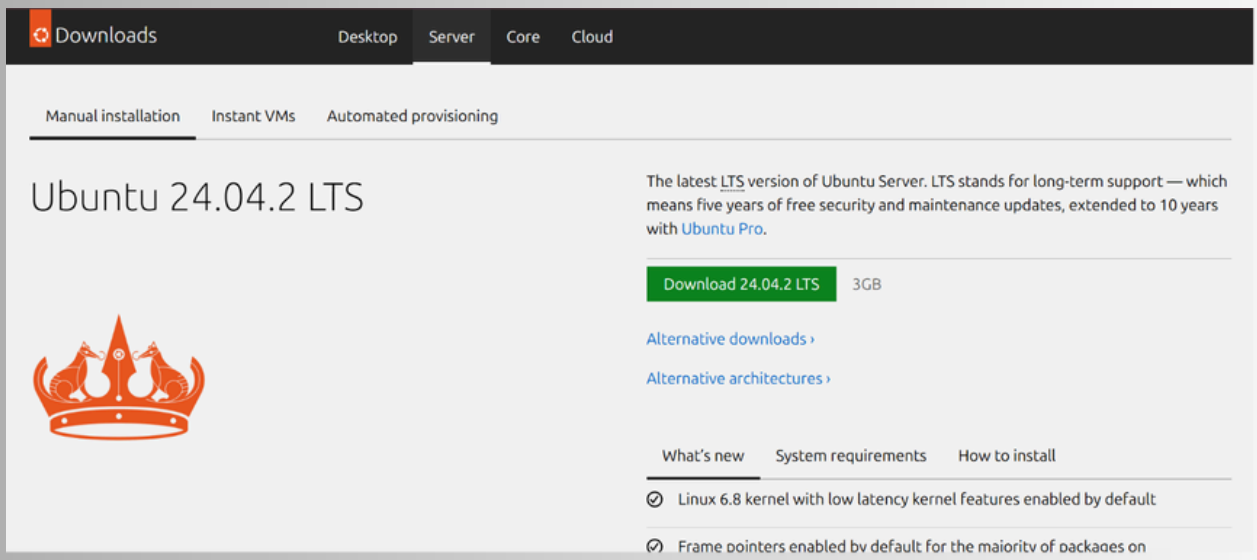
🔐 Project 3: Secure Linux Server Setup & Hardening

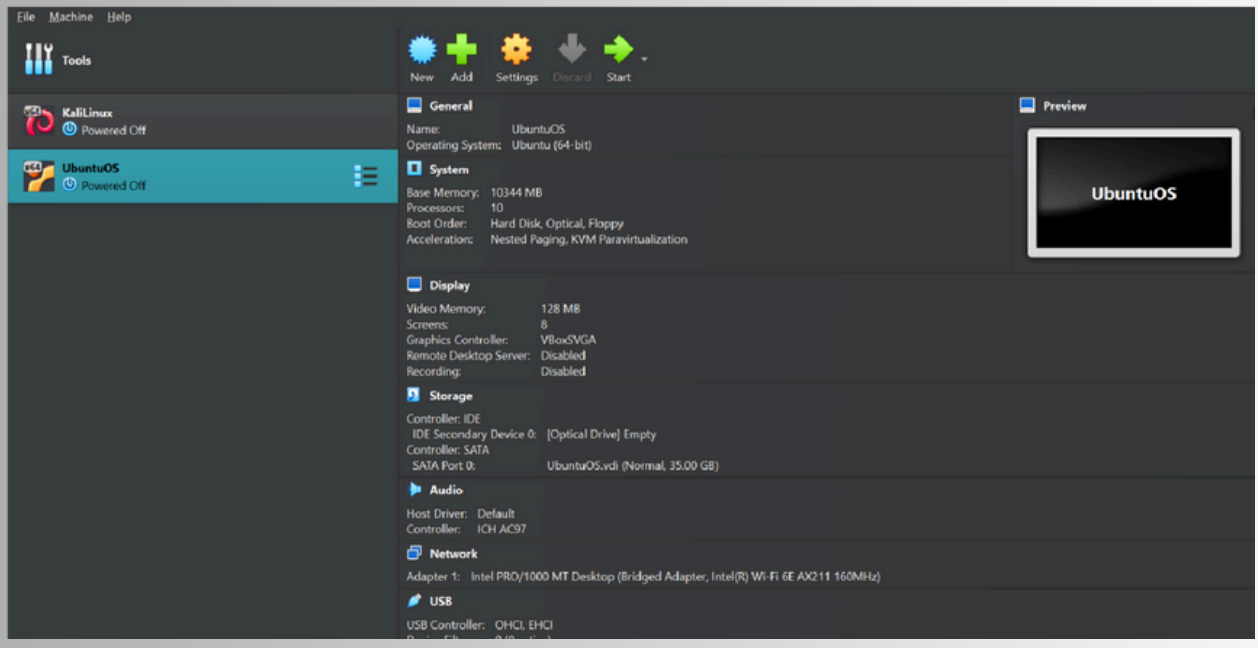
✅ Initial Server Deployment & Basic Hardening

🔹 Step 1: Set up the Linux Server

Using Local (VirtualBox)

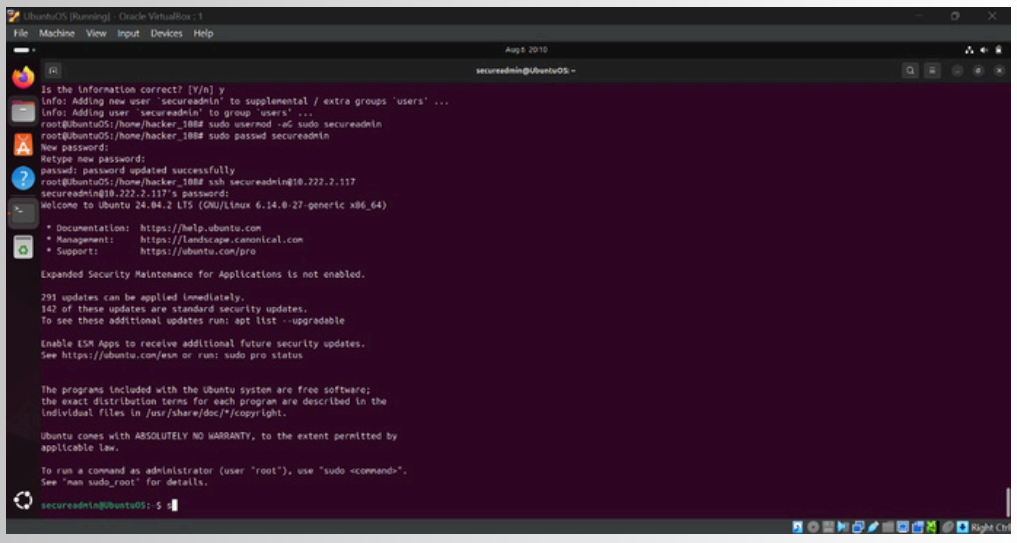
- Download **Ubuntu Server 24.04.2 LTS ISO**
- Installing in VirtualBox





INFOTACT
SOLUTIONS

Photo for the Step 2:→



Step 2: Secure SSH

```
sshroot@your_server_ip
adduser secureadmin
usermod -aG sudo secureadmin
```

Enable key-based login:

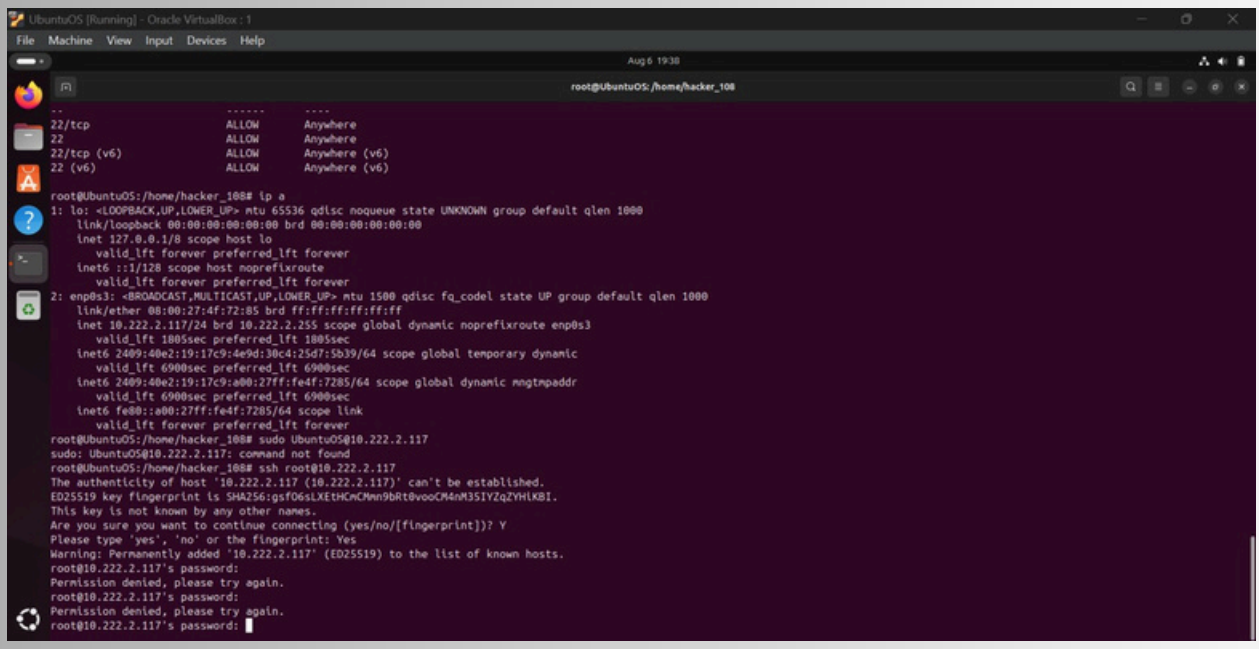
```
ssh-keygen -t rsa
ssh-copy-id secureadmin@your_server_ip
```

Edit SSH configuration:

```
sudo nano /etc/ssh/sshd_config
# Changes:
PermitRootLogin no
PasswordAuthentication no
```

Restart SSH service:

```
sudo systemctl restart ssh
```



```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

secureadmin@UbuntuOS:~$ sudo ufw allow OpenSSH
[sudo] password for secureadmin:
Rule added
Rule added (v6)
secureadmin@UbuntuOS:~$ sudo ufw allow 80
Rule added
Rule added (v6)
secureadmin@UbuntuOS:~$ sudo ufw allow 443
Rule added
Rule added (v6)
secureadmin@UbuntuOS:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
secureadmin@UbuntuOS:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW IN    Anywhere
22                         ALLOW IN    Anywhere
22/tcp (OpenSSH)           ALLOW IN    Anywhere
80                         ALLOW IN    Anywhere
443                        ALLOW IN    Anywhere
22/tcp (v6)                ALLOW IN    Anywhere (v6)
22 (v6)                    ALLOW IN    Anywhere (v6)
22/tcp (OpenSSH (v6))      ALLOW IN    Anywhere (v6)
80 (v6)                    ALLOW IN    Anywhere (v6)
443 (v6)                   ALLOW IN    Anywhere (v6)

secureadmin@UbuntuOS:~$
```

🔹 Step 3: Set Up UFW Firewall

```
sudo apt install ufw
sudo ufw allow OpenSSH
sudo ufw allow 80
sudo ufw allow 443
sudo ufw enable
sudo ufw status
```

✅ Intrusion Protection & System Auditing

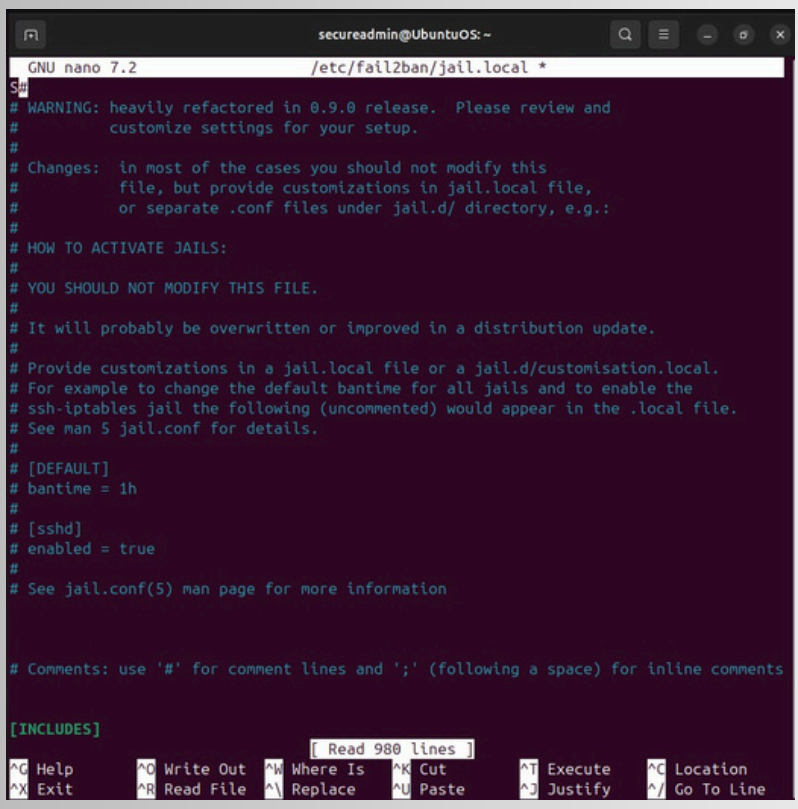
🔹 Step 4: Install & Configure `fail2ban`

```
sudo apt installfail2ban
sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
sudo nano /etc/fail2ban/jail.local
# In [sshd] section:
enabled = true
maxretry = 5
bantime = 3600
sudo systemctl restart fail2ban
```

```
Building dependency tree... Done
Reading state information... Done
296 packages can be upgraded. Run 'apt list --upgradable' to see them.
secureadmin@UbuntuOS:~$ sudo apt install fail2ban -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  python3-pkg-resources python3-pyasyncore python3-pyinotify python3-setuptools
  whois
Suggested packages:
  mailx monit sqlite3 python-pyinotify-doc python-setuptools-doc
The following NEW packages will be installed:
  fail2ban python3-pyasyncore python3-pyinotify python3-setuptools whois
The following packages will be upgraded:
  python3-pkg-resources
1 upgraded, 5 newly installed, 0 to remove and 295 not upgraded.
Need to get 1,060 kB of archives.
After this operation, 4,858 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu noble-updates/main amd64 python3-pkg-resour
ces all 68.1.2-2ubuntu1.2 [168 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu noble-updates/main amd64 python3-setuptools
 all 68.1.2-2ubuntu1.2 [397 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu noble/main amd64 python3-pyasyncore all 1.0
.2-2 [10.1 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu noble-updates/universe amd64 fail2ban all 1
.0.2-3ubuntu0.1 [409 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu noble/main amd64 python3-pyinotify all 0.9.
6-2ubuntu1 [25.0 kB]
Get:6 http://in.archive.ubuntu.com/ubuntu noble/main amd64 whois amd64 5.5.22 [51.7 k
B]
Fetched 1,060 kB in 2s (438 kB/s)
(Reading database ... 152836 files and directories currently installed.)
Preparing to unpack .../0-python3-pkg-resources_68.1.2-2ubuntu1.2_all.deb ...
Unpacking python3-pkg-resources (68.1.2-2ubuntu1.2) over (68.1.2-2ubuntu1.1) ...
Selecting previously unselected package python3-setuptools.
Preparing to unpack .../1-python3-setuptools_68.1.2-2ubuntu1.2_all.deb ...
```

```
secureadmin@UbuntuOS:~$ sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
secureadmin@UbuntuOS:~$ sudo nano /etc/fail2ban/jail.local
secureadmin@UbuntuOS:~$ sudo systemctl enable fail2ban
Synchronizing state of fail2ban.service with SysV service script with /usr/lib/system
d/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable fail2ban
secureadmin@UbuntuOS:~$ sudo systemctl start fail2ban
secureadmin@UbuntuOS:~$ sudo fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:   sshd
secureadmin@UbuntuOS:~$ 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:
secureadmin@UbuntuOS:~$
```

```
secureadmin@UbuntuOS:~$ sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
secureadmin@UbuntuOS:~$ sudo nano /etc/fail2ban/jail.local
secureadmin@UbuntuOS:~$
```



INFOTACT
SOLUTIONS

Step 5: Install & Configure auditd

```
sudo aptinstall auditd
sudo systemctl start auditd
sudo systemctl enable auditd
sudo ausearch -x sshd
```

```
secureadmin@UbuntuOS:~$ sudo apt install auditd audispd-plugins -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libauparse0t64
The following NEW packages will be installed:
  audispd-plugins auditd libauparse0t64
0 upgraded, 3 newly installed, 0 to remove and 295 not upgraded.
Need to get 312 kB of archives.
After this operation, 1,024 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu noble-updates/main amd64 libauparse0t64 amd
64 1:3.1.2-2.1build1.1 [58.9 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu noble-updates/main amd64 auditd amd64 1:3.1
.2-2.1build1.1 [215 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu noble-updates/universe amd64 audispd-plugin
s amd64 1:3.1.2-2.1build1.1 [38.8 kB]
Fetched 312 kB in 2s (126 kB/s)
Selecting previously unselected package libauparse0t64:amd64.
(Reading database ... 153533 files and directories currently installed.)
Preparing to unpack .../libauparse0t64_1%3a3.1.2-2.1build1.1_amd64.deb ...
Adding 'diversion of /lib/x86_64-linux-gnu/libauparse.so.0 to /lib/x86_64-linux-gnu/l
ibauparse.so.0.usr-is-merged by libauparse0t64'
Adding 'diversion of /lib/x86_64-linux-gnu/libauparse.so.0.0.0 to /lib/x86_64-linux-g
nu/libauparse.so.0.0.0.usr-is-merged by libauparse0t64'
Unpacking libauparse0t64:amd64 (1:3.1.2-2.1build1.1) ...
Selecting previously unselected package auditd.
Preparing to unpack .../auditd_1%3a3.1.2-2.1build1.1_amd64.deb ...
Unpacking auditd (1:3.1.2-2.1build1.1) ...
Selecting previously unselected package audispd-plugins.
Preparing to unpack .../audispd-plugins_1%3a3.1.2-2.1build1.1_amd64.deb ...
Unpacking audispd-plugins (1:3.1.2-2.1build1.1) ...
Setting up libauparse0t64:amd64 (1:3.1.2-2.1build1.1) ...
Setting up auditd (1:3.1.2-2.1build1.1) ...
```

```
secureadmin@UbuntuOS:~$ sudo aureport -au

Authentication Report
============================================
# date time acct host term exe success event
============================================
<no events of interest were found>
```

```
Synchronizing state of auditd.service with SysV service script with /usr/lib/systemd/
systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable auditd
secureadmin@UbuntuOS:~$ sudo systemctl start auditd
secureadmin@UbuntuOS:~$ sudo ausearch -x sshd
<no matches>
secureadmin@UbuntuOS:~$ sudo aureport

Summary Report
======================
Range of time in logs: 08/06/2025 20:21:33.234 - 08/06/2025 20:26:50.643
Selected time for report: 08/06/2025 20:21:33 - 08/06/2025 20:26:50.643
Number of changes in configuration: 3
Number of changes to accounts, groups, or roles: 0
Number of logins: 0
Number of failed logins: 0
Number of authentications: 0
Number of failed authentications: 0
Number of users: 4
Number of terminals: 5
Number of host names: 1
Number of executables: 5
Number of commands: 3
Number of files: 0
Number of AVC's: 0
Number of MAC events: 0
Number of failed syscalls: 0
Number of anomaly events: 0
Number of responses to anomaly events: 0
Number of crypto events: 0
Number of integrity events: 0
Number of virt events: 0
Number of keys: 0
Number of process IDs: 11
Number of events: 154

secureadmin@UbuntuOS:~$
```

INFOTACT
SOLUTIONS

Step 6: Run CIS Benchmark with Lynis

```
sudo apt install lynis
sudo lynis audit system
```

```
secureadmin@UbuntuOS:~$ sudo apt install lynis -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  menu
Suggested packages:
  apt-listbugs debsecan debsums tripwire samhain aide menu-l10n gksu
  | kde-cli-tools | ktsuss
The following NEW packages will be installed:
  lynis menu
0 upgraded, 2 newly installed, 0 to remove and 295 not upgraded.
Need to get 602 kB of archives.
After this operation, 3,202 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 lynis all 3.0.9-1 [226
 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 menu amd64 2.1.50 [377
 kB]
Fetched 602 kB in 4s (146 kB/s)
Selecting previously unselected package lynis.
(Reading database ... 153643 files and directories currently installed.)
Preparing to unpack .../archives/lynis_3.0.9-1_all.deb ...
Unpacking lynis (3.0.9-1) ...

Progress: [ 22%] [#############.....................................................]
```

```
secureadmin@UbuntuOS:~$ sudo lynis audit system

[ Lynis 3.0.9 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2021, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
  - Detecting OS...                                           [ DONE ]
```

- Run scans via https://localhost:8834/

INFOTACT
SOLUTIONS

✅ Vulnerability Scanning & Fixing Issues

🔹 Step 7: Run Vulnerability Scans

```
sudo lynis audit system
```

```
secureadmin@UbuntuOS:~$ sudo apt install lynis -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  menu
Suggested packages:
  apt-listbugs debsecan debsums tripwire samhain aide menu-l10n gksu
  | kde-cli-tools | ktsuss
The following NEW packages will be installed:
  lynis menu
0 upgraded, 2 newly installed, 0 to remove and 295 not upgraded.
Need to get 602 kB of archives.
After this operation, 3,202 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 lynis all 3.0.9-1 [226
 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 menu amd64 2.1.50 [377
 kB]
Fetched 602 kB in 4s (146 kB/s)
Selecting previously unselected package lynis.
(Reading database ... 153643 files and directories currently installed.)
Preparing to unpack .../archives/lynis_3.0.9-1_all.deb ...
Unpacking lynis (3.0.9-1) ...

Progress: [ 22%] [##############.....................................................]
```

```
secureadmin@UbuntuOS:~$ sudo lynis audit system

[ Lynis 3.0.9 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2021, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
  - Detecting OS...                                           [ DONE ]
```

```
  2007-2021, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
  - Detecting OS...                                           [ DONE ]
  - Checking profiles...                                      [ DONE ]

  ---------------------------------------------------
  Program version:           3.0.9
  Operating system:          Linux
  Operating system name:     Ubuntu
  Operating system version:  24.04
  Kernel version:            6.14.0
  Hardware platform:         x86_64
  Hostname:                  UbuntuOS
  ---------------------------------------------------
  Profiles:                  /etc/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
  Plugin directory:          /etc/lynis/plugins
  ---------------------------------------------------
  Auditor:                   [Not Specified]
  Language:                  en
  Test category:             all
  Test group:                all
  ---------------------------------------------------
  - Program update status...                                  [ NO UPDATE ]

[+] System tools
------------------------------------
  - Scanning available tools...
  - Checking system binaries...
```

```
  Program version:           3.0.9
  Operating system:          Linux
  Operating system name:     Ubuntu
  Operating system version:  24.04
  Kernel version:            6.14.0
  Hardware platform:         x86_64
  Hostname:                  UbuntuOS
  ------------------------------------------------
  Profiles:                  /etc/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
  Plugin directory:          /etc/lynis/plugins
  ------------------------------------------------
  Auditor:                   [Not Specified]
  Language:                  en
  Test category:             all
  Test group:                all
  ------------------------------------------------
  - Program update status...                                [ NO UPDATE ]

[+] System tools
------------------------------------
  - Scanning available tools...
  - Checking system binaries...

[+] Plugins (phase 1)
------------------------------------
 Note: plugins have more extensive tests and may take several minutes to complete

  - Plugin: debian
    [
[+] Debian Tests
------------------------------------
  - Checking for system binaries that are required by Debian Tests...
    - Checking /bin...                                      [ FOUND ]
```

```
  - Checking mount points
    - Checking /home mount point                              [ SUGGESTION ]
    - Checking /tmp mount point                               [ SUGGESTION ]
    - Checking /var mount point                               [ SUGGESTION ]
  - Query swap partitions (fstab)                             [ NONE ]
  - Testing swap partitions                                   [ OK ]
  - Testing /proc mount (hidepid)                             [ SUGGESTION ]
  - Checking for old files in /tmp                            [ OK ]
  - Checking /tmp sticky bit                                  [ OK ]
  - Checking /var/tmp sticky bit                              [ OK ]
  - ACL support root file system                              [ ENABLED ]
  - Mount options of /                                        [ OK ]
  - Mount options of /dev                                     [ PARTIALLY HARDENED ]
  - Mount options of /dev/shm                                 [ PARTIALLY HARDENED ]
  - Mount options of /run                                     [ HARDENED ]
  - Total without nodev:5 noexec:20 nosuid:12 ro or noexec (W^X): 11 of total 36
  - Disable kernel support of some filesystems
S
[+] USB Devices
-----------------------------------
  - Checking usb-storage driver (modprobe config)             [ NOT DISABLED ]
  - Checking USB devices authorization                        [ ENABLED ]
  - Checking USBGuard                                         [ NOT FOUND ]

[+] Storage
-----------------------------------
  - Checking firewire ohci driver (modprobe config)           [ DISABLED ]

[+] NFS
-----------------------------------
  - Check running NFS daemon                                  [ NOT FOUND ]

[+] Name services
-----------------------------------
  - Checking search domains                                   [ FOUND ]
  - Checking /etc/resolv.conf options                         [ FOUND ]
```

```
- Running 'systemd-analyze security'
      - ModemManager.service:                                [ MEDIUM ]
      - NetworkManager.service:                              [ EXPOSED ]
      - accounts-daemon.service:                             [ MEDIUM ]
      - alsa-state.service:                                  [ UNSAFE ]
      - anacron.service:                                     [ UNSAFE ]
      - auditd.service:                                      [ EXPOSED ]
      - avahi-daemon.service:                                [ UNSAFE ]
      - colord.service:                                      [ PROTECTED ]
      - cron.service:                                        [ UNSAFE ]
      - cups-browsed.service:                                [ UNSAFE ]
      - cups.service:                                        [ UNSAFE ]
      - dbus.service:                                        [ UNSAFE ]
      - dmesg.service:                                       [ UNSAFE ]
      - emergency.service:                                   [ UNSAFE ]
      - fail2ban.service:                                    [ UNSAFE ]
      - fwupd.service:                                       [ EXPOSED ]
      - gdm.service:                                         [ UNSAFE ]
      - getty@tty1.service:                                  [ UNSAFE ]
      - gnome-remote-desktop.service:                        [ UNSAFE ]
      - kerneloops.service:                                  [ UNSAFE ]
      - lynis.service:                                       [ UNSAFE ]
      - networkd-dispatcher.service:                         [ UNSAFE ]
      - packagekit.service:                                  [ UNSAFE ]
      - plymouth-start.service:                              [ UNSAFE ]
      - polkit.service:                                      [ PROTECTED ]
      - power-profiles-daemon.service:                       [ MEDIUM ]
      - rc-local.service:                                    [ UNSAFE ]
      - rescue.service:                                      [ UNSAFE ]
      - rsyslog.service:                                     [ MEDIUM ]
      - rtkit-daemon.service:                                [ MEDIUM ]
      - snapd.service:                                       [ UNSAFE ]
      - ssh.service:                                         [ UNSAFE ]
      - sssd-autofs.service:                                 [ UNSAFE ]
      - sssd-nss.service:                                    [ UNSAFE ]
      - sssd-pac.service:                                    [ UNSAFE ]
      - sssd-pam.service:                                    [ UNSAFE ]
```

```
  - Mount options of /dev                                        [ PARTIALLY HARDENED ]
  - Mount options of /dev/shm                                    [ PARTIALLY HARDENED ]
  - Mount options of /run                                        [ HARDENED ]
  - Total without nodev:5 noexec:20 nosuid:12 ro or noexec (W^X): 11 of total 36
  - Disable kernel support of some filesystems
S
[+] USB Devices
------------------------------------
  - Checking usb-storage driver (modprobe config)                [ NOT DISABLED ]
  - Checking USB devices authorization                           [ ENABLED ]
  - Checking USBGuard                                            [ NOT FOUND ]

[+] Storage
------------------------------------
  - Checking firewire ohci driver (modprobe config)              [ DISABLED ]

[+] NFS
------------------------------------
  - Check running NFS daemon                                     [ NOT FOUND ]

[+] Name services
------------------------------------
  - Checking search domains                                      [ FOUND ]
  - Checking /etc/resolv.conf options                            [ FOUND ]
  - Searching DNS domain name                                    [ UNKNOWN ]
  - Checking /etc/hosts
    - Duplicate entries in hosts file                            [ NONE ]
    - Presence of configured hostname in /etc/hosts              [ NOT FOUND ]
    - Hostname mapped to localhost                               [ NOT FOUND ]
    - Localhost mapping to IP address                            [ OK ]

[+] Ports and packages
------------------------------------
  - Searching package managers
    - Searching dpkg package manager                             [ FOUND ]
      - Querying package manager
```

INFOTACT
SOLUTIONS

```
  - Installed rsh server package                          [ OK ]
  - Installed telnet client package                       [ OK ]
  - Installed telnet server package                       [ NOT FOUND ]
  - Checking NIS client installation                      [ OK ]
  - Checking NIS server installation                      [ OK ]
  - Checking TFTP client installation                     [ OK ]
  - Checking TFTP server installation                     [ OK ]

[+] Banners and identification
-----------------------------------
  - /etc/issue                                            [ FOUND ]
    - /etc/issue contents                                 [ WEAK ]
  - /etc/issue.net                                        [ FOUND ]
    - /etc/issue.net contents                             [ WEAK ]

[+] Scheduled tasks
-----------------------------------
  - Checking crontab and cronjob files                    [ DONE ]

[+] Accounting
-----------------------------------
  - Checking accounting information                       [ NOT FOUND ]
  - Checking sysstat accounting data                      [ DISABLED ]
  - Checking auditd                                       [ ENABLED ]
    - Checking audit rules                                [ SUGGESTION ]
    - Checking audit configuration file                   [ OK ]
    - Checking auditd log file                            [ FOUND ]

[+] Time and Synchronization
-----------------------------------
  - NTP daemon found: systemd (timesyncd)                 [ FOUND ]
  - Checking for a running NTP daemon or client           [ OK ]
  - Last time synchronization                             [ 1212s ]

[+] Cryptography
-----------------------------------
```

```
    - OpenSSH option: AllowUsers                              [ NOT FOUND ]
    - OpenSSH option: AllowGroups                             [ NOT FOUND ]

[+] SNMP Support
------------------------------------
  - Checking running SNMP daemon                              [ NOT FOUND ]

[+] Databases
------------------------------------
    No database engines found

[+] LDAP Services
------------------------------------
  - Checking OpenLDAP instance                                [ NOT FOUND ]

[+] PHP
------------------------------------
  - Checking PHP                                              [ NOT FOUND ]

[+] Squid Support
------------------------------------
  - Checking running Squid daemon                             [ NOT FOUND ]

[+] Logging and files
------------------------------------
  - Checking for a running log daemon                         [ OK ]
    - Checking Syslog-NG status                               [ NOT FOUND ]
    - Checking systemd journal status                         [ FOUND ]
    - Checking Metalog status                                 [ NOT FOUND ]
    - Checking RSyslog status                                 [ FOUND ]
    - Checking RFC 3195 daemon status                         [ NOT FOUND ]
    - Checking minilogd instances                             [ NOT FOUND ]
  - Checking logrotate presence                               [ OK ]
  - Checking remote logging                                   [ NOT ENABLED ]
  - Checking log directories (static list)                    [ DONE ]
  - Checking open log files                                   [ DONE ]
  - Checking deleted files in use                             [ FILES FOUND ]
```

```
    - Checking for unused rules                                [ FOUND ]
  - Checking host based firewall                               [ ACTIVE ]

[+] Software: webserver
------------------------------------
  - Checking Apache                                            [ NOT FOUND ]
  - Checking nginx                                             [ NOT FOUND ]

[+] SSH Support
------------------------------------
  - Checking running SSH daemon                                [ FOUND ]
    - Searching SSH configuration                              [ FOUND ]
    - OpenSSH option: AllowTcpForwarding                       [ SUGGESTION ]
    - OpenSSH option: ClientAliveCountMax                      [ SUGGESTION ]
    - OpenSSH option: ClientAliveInterval                      [ OK ]
    - OpenSSH option: FingerprintHash                          [ OK ]
    - OpenSSH option: GatewayPorts                             [ OK ]
    - OpenSSH option: IgnoreRhosts                             [ OK ]
    - OpenSSH option: LoginGraceTime                           [ OK ]
    - OpenSSH option: LogLevel                                 [ SUGGESTION ]
    - OpenSSH option: MaxAuthTries                             [ SUGGESTION ]
    - OpenSSH option: MaxSessions                              [ SUGGESTION ]
    - OpenSSH option: PermitRootLogin                          [ SUGGESTION ]
    - OpenSSH option: PermitUserEnvironment                    [ OK ]
    - OpenSSH option: PermitTunnel                             [ OK ]
    - OpenSSH option: Port                                     [ SUGGESTION ]
    - OpenSSH option: PrintLastLog                             [ OK ]
    - OpenSSH option: StrictModes                              [ OK ]
    - OpenSSH option: TCPKeepAlive                             [ SUGGESTION ]
    - OpenSSH option: UseDNS                                   [ OK ]
    - OpenSSH option: X11Forwarding                            [ SUGGESTION ]
    - OpenSSH option: AllowAgentForwarding                     [ SUGGESTION ]
    - OpenSSH option: AllowUsers                               [ NOT FOUND ]
    - OpenSSH option: AllowGroups                              [ NOT FOUND ]

[+] SNMP Support
```


```
2025-08-06 20:34:42,671 fail2ban                [52932]: ERROR   Init of command line
 failed
    - Checking Fail2ban jails                                   [ DISABLED ]
  - Checking for IDS/IPS tooling                                [ FOUND ]

[+] Software: Malware
------------------------------------
pgrep: pattern that searches for process name longer than 15 characters will result i
n zero matches
Try `pgrep -f' option to match against the complete command line.
  - Malware software components                                 [ NOT FOUND ]

[+] File Permissions
------------------------------------
  - Starting file permissions check
    File: /boot/grub/grub.cfg                                   [ OK ]
    File: /etc/crontab                                          [ SUGGESTION ]
    File: /etc/group                                            [ OK ]
    File: /etc/group-                                           [ OK ]
    File: /etc/hosts.allow                                      [ OK ]
    File: /etc/hosts.deny                                       [ OK ]
    File: /etc/issue                                            [ OK ]
    File: /etc/issue.net                                        [ OK ]
    File: /etc/passwd                                           [ OK ]
    File: /etc/passwd-                                          [ OK ]
    File: /etc/ssh/sshd_config                                  [ SUGGESTION ]
    Directory: /root/.ssh                                       [ OK ]
    Directory: /etc/cron.d                                      [ SUGGESTION ]
    Directory: /etc/cron.daily                                  [ SUGGESTION ]
    Directory: /etc/cron.hourly                                 [ SUGGESTION ]
    Directory: /etc/cron.weekly                                 [ SUGGESTION ]
    Directory: /etc/cron.monthly                                [ SUGGESTION ]

[+] Home directories
------------------------------------
  - Permissions of home directories                             [ OK ]
```

INFOTACT
SOLUTIONS

```
[+] Home directories
------------------------------------
  - Permissions of home directories                    [ OK ]
  - Ownership of home directories                      [ OK ]
  - Checking shell history files                       [ OK ]

[+] Kernel Hardening
------------------------------------
  - Comparing sysctl key pairs with scan profile
    - dev.tty.ldisc_autoload (exp: 0)                  [ DIFFERENT ]
    - fs.protected_fifos (exp: 2)                      [ DIFFERENT ]
    - fs.protected_hardlinks (exp: 1)                  [ OK ]
    - fs.protected_regular (exp: 2)                    [ OK ]
    - fs.protected_symlinks (exp: 1)                   [ OK ]
    - fs.suid_dumpable (exp: 0)                        [ DIFFERENT ]
    - kernel.core_uses_pid (exp: 1)                    [ DIFFERENT ]
    - kernel.ctrl-alt-del (exp: 0)                     [ OK ]
    - kernel.dmesg_restrict (exp: 1)                   [ OK ]
    - kernel.kptr_restrict (exp: 2)                    [ DIFFERENT ]
```

```
    - net.ipv4.conf.all.rp_filter (exp: 1)                    [ DIFFERENT ]
    - net.ipv4.conf.all.send_redirects (exp: 0)               [ DIFFERENT ]
    - net.ipv4.conf.default.accept_redirects (exp: 0)         [ OK ]
    - net.ipv4.conf.default.accept_source_route (exp: 0)      [ DIFFERENT ]
    - net.ipv4.conf.default.log_martians (exp: 1)             [ DIFFERENT ]
    - net.ipv4.icmp_echo_ignore_broadcasts (exp: 1)           [ OK ]
    - net.ipv4.icmp_ignore_bogus_error_responses (exp: 1)     [ OK ]
    - net.ipv4.tcp_syncookies (exp: 1)                        [ OK ]
    - net.ipv4.tcp_timestamps (exp: 0 1)                      [ OK ]
    - net.ipv6.conf.all.accept_redirects (exp: 0)             [ OK ]
    - net.ipv6.conf.all.accept_source_route (exp: 0)          [ OK ]
    - net.ipv6.conf.default.accept_redirects (exp: 0)         [ OK ]
    - net.ipv6.conf.default.accept_source_route (exp: 0)      [ OK ]

[+] Hardening
------------------------------------

  [WARNING]: Test KRNL-6000 had a long execution: 19.184489 seconds

    - Installed compiler(s)                                   [ NOT FOUND ]
    - Installed malware scanner                               [ NOT FOUND ]
    - Non-native binary formats                               [ FOUND ]

[+] Custom tests
------------------------------------
  - Running custom tests...                                   [ NONE ]

[+] Plugins (phase 2)
------------------------------------

================================================================================

  -[ Lynis 3.0.9 Results ]-

  Warnings (2):
  ----------------------------
```

INFOTACT
SOLUTIONS

```
      https://cisofy.com/lynis/controls/TOOL-5104/

  Suggestions (51):
  ----------------------------
  * This release is more than 4 months old. Check the website or GitHub to see if the
re is an update available. [LYNIS]
      https://cisofy.com/lynis/controls/LYNIS/

  * Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [DEB-0280]
      https://cisofy.com/lynis/controls/DEB-0280/

  * Install apt-listbugs to display a list of critical bugs prior to each APT install
ation. [DEB-0810]
      https://cisofy.com/lynis/controls/DEB-0810/

  * Install apt-listchanges to display any significant changes prior to any upgrade v
ia APT. [DEB-0811]
      https://cisofy.com/lynis/controls/DEB-0811/

  * Install needrestart, alternatively to debian-goodies, so that you can run needres
tart after upgrades to determine which daemons are using old versions of libraries an
d need restarting. [DEB-0831]
      https://cisofy.com/lynis/controls/DEB-0831/

  * Set a password on GRUB boot loader to prevent altering boot configuration (e.g. b
oot in single user mode without password) [BOOT-5122]
      https://cisofy.com/lynis/controls/BOOT-5122/

  * Consider hardening system services [BOOT-5264]
    - Details  : Run '/usr/bin/systemd-analyze security SERVICE' for each service
      https://cisofy.com/lynis/controls/BOOT-5264/

  * If not required, consider explicit disabling of core dump in /etc/security/limits
.conf file [KRNL-5820]
      https://cisofy.com/lynis/controls/KRNL-5820/
```

```
  * Consider hardening system services [BOOT-5264]
    - Details  : Run '/usr/bin/systemd-analyze security SERVICE' for each service
      https://cisofy.com/lynis/controls/BOOT-5264/

  * If not required, consider explicit disabling of core dump in /etc/security/limits
.conf file [KRNL-5820]
      https://cisofy.com/lynis/controls/KRNL-5820/

  * Check PAM configuration, add rounds if applicable and expire passwords to encrypt
 with new values [AUTH-9229]
      https://cisofy.com/lynis/controls/AUTH-9229/

  * Configure password hashing rounds in /etc/login.defs [AUTH-9230]
      https://cisofy.com/lynis/controls/AUTH-9230/

  * When possible set expire dates for all password protected accounts [AUTH-9282]
      https://cisofy.com/lynis/controls/AUTH-9282/

  * Configure minimum password age in /etc/login.defs [AUTH-9286]
      https://cisofy.com/lynis/controls/AUTH-9286/

  * Configure maximum password age in /etc/login.defs [AUTH-9286]
      https://cisofy.com/lynis/controls/AUTH-9286/

  * Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]
      https://cisofy.com/lynis/controls/AUTH-9328/

  * To decrease the impact of a full /home file system, place /home on a separate par
tition [FILE-6310]
      https://cisofy.com/lynis/controls/FILE-6310/

  * To decrease the impact of a full /tmp file system, place /tmp on a separate parti
tion [FILE-6310]
      https://cisofy.com/lynis/controls/FILE-6310/

  * To decrease the impact of a full /var file system, place /var on a separate parti
```

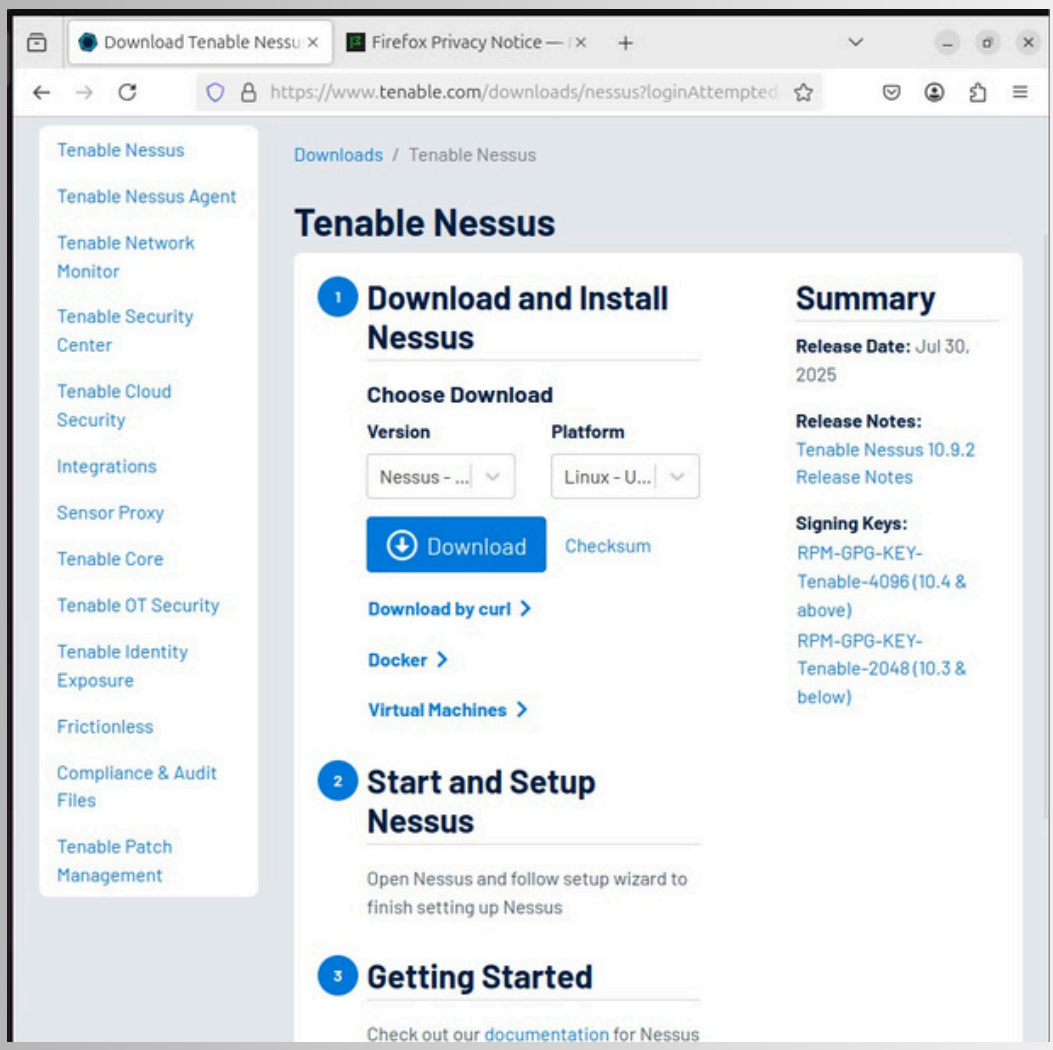
```
    - Details  : PermitRootLogin (set YES to (FORCED-COMMANDS-ONLY|NO|PROHIBIT-PASSWO
RD|WITHOUT-PASSWORD))
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : Port (set 22 to )
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : TCPKeepAlive (set YES to NO)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : X11Forwarding (set YES to NO)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : AllowAgentForwarding (set YES to NO)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Enable logging to an external logging host for archiving purposes and additional
protection [LOGG-2154]
      https://cisofy.com/lynis/controls/LOGG-2154/

  * Check what deleted files are still in use and why. [LOGG-2190]
      https://cisofy.com/lynis/controls/LOGG-2190/

  * Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]
      https://cisofy.com/lynis/controls/BANN-7126/

  * Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]
      https://cisofy.com/lynis/controls/BANN-7130/

  * Enable process accounting [ACCT-9622]
      https://cisofy.com/lynis/controls/ACCT-9622/

  * Enable sysstat to collect accounting (disabled) [ACCT-9626]
```

✅ ***Finding:*** **Outdated packages, default SSH config, and unnecessary services like Apache were flagged.**

Optional (GUI Tools):

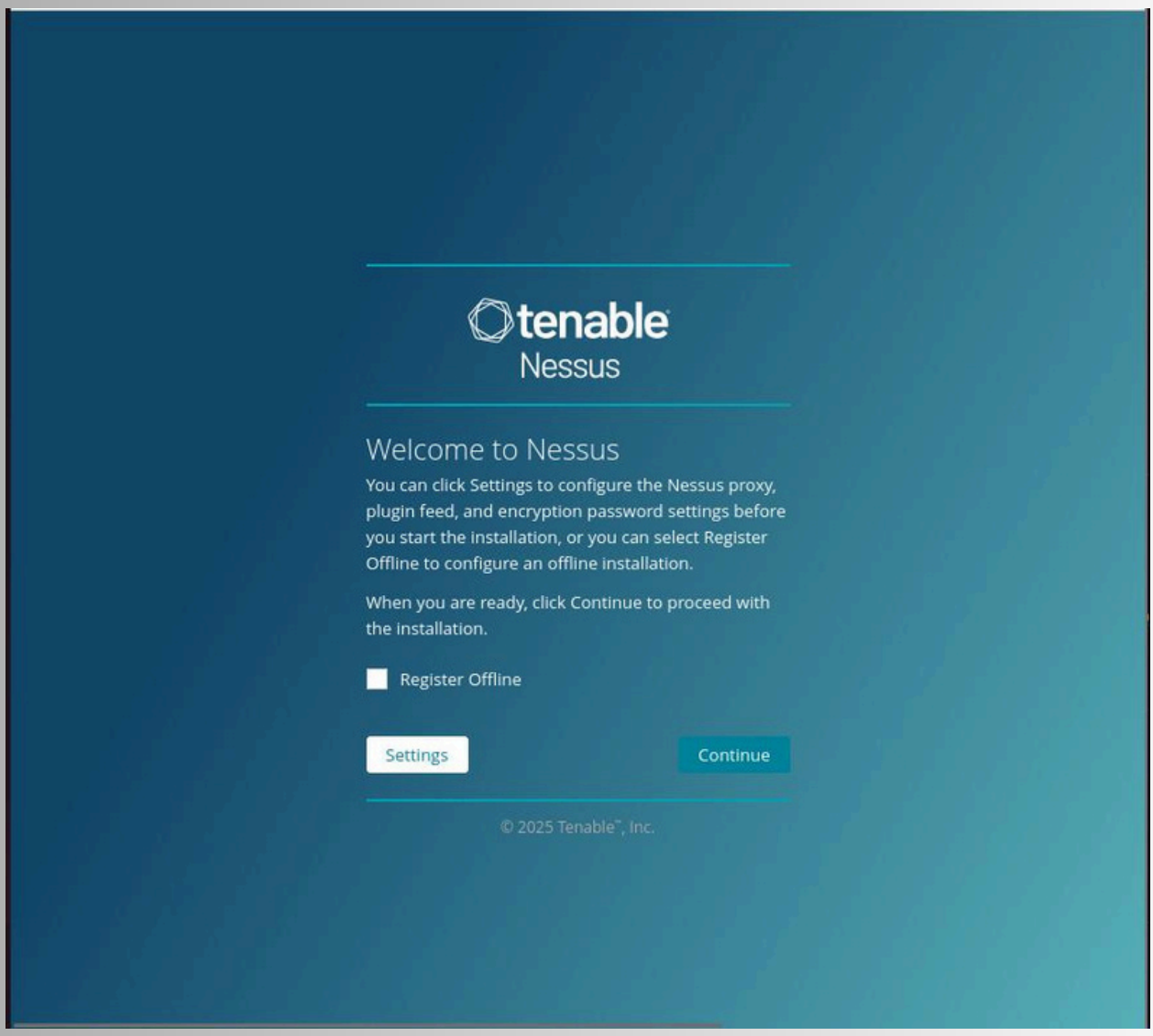
- Install Nessus Essentials

```
secureadmin@UbuntuOS:~$ wget https://downloads.nessus.org/nessus3dl.php?file=nessus-1
0.6.2-ubuntu1110_amd64deb&licence_accept=yes
[1] 58496
secureadmin@UbuntuOS:~$
Redirecting output to 'wget-log'.
sudo dpkg -i nessus-*.deb
[sudo] password for secureadmin:
dpkg: error: cannot access archive 'nessus-*.deb': No such file or directory
[1]+  Done                    wget https://downloads.nessus.org/nessus3dl.php?file=ne
ssus-10.6.2-ubuntu1110_amd64deb
secureadmin@UbuntuOS:~$
```

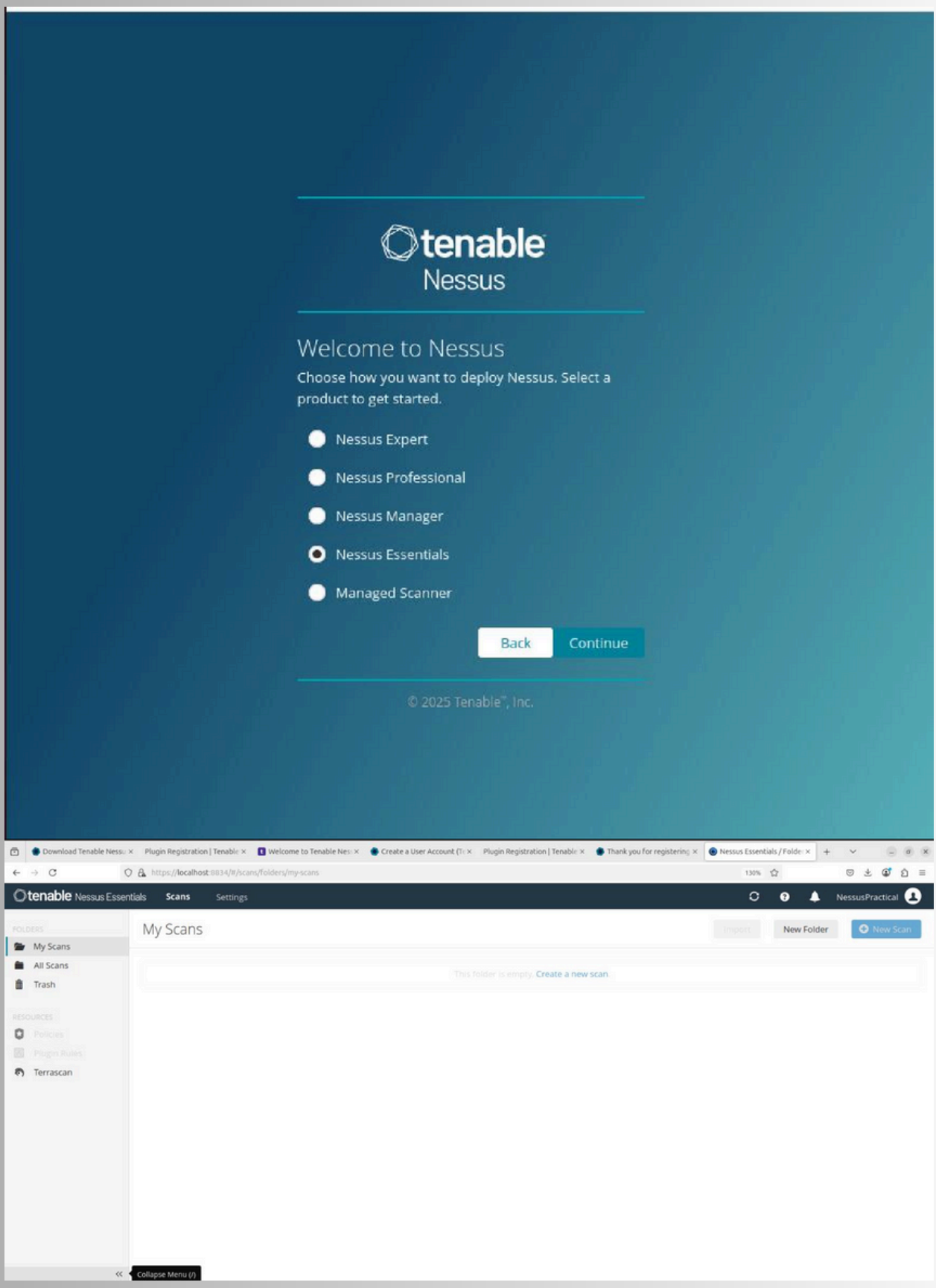


```
(Reading database ... 153942 files and directories currently installed.)
Preparing to unpack Nessus-10.9.2-ubuntu1604_amd64.deb ...
Unpacking nessus (10.9.2) ...
Setting up nessus (10.9.2) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components...
```

INFOTACT
SOLUTIONS



INFOTACT
SOLUTIONS



INFOTACT
SOLUTIONS

```
secureadmin@UbuntuOS:~$ sudo systemctl start nessusd
secureadmin@UbuntuOS:~$ sudo systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/usr/lib/systemd/system/nessusd.service; enabled; preset: enabl>
     Active: active (running) since Wed 2025-08-06 21:22:21 UTC; 10s ago
   Main PID: 62180 (nessus-service)
      Tasks: 13 (limit: 11959)
     Memory: 45.5M (peak: 49.1M)
        CPU: 7.987s
     CGroup: /system.slice/nessusd.service
             ├─62180 /opt/nessus/sbin/nessus-service -q
             └─62182 nessusd -q

Aug 06 21:22:21 UbuntuOS systemd[1]: Started nessusd.service - The Nessus Vulnerabil>
Aug 06 21:22:21 UbuntuOS nessus-service[62180]: nessus-service [62180][INFO] : Nessu>
lines 1-13/13 (END)
```

Small Sample Report of Vulnerability Scanning By Nessus on host https://127.0.0.1

```
timestamp,plugins_failed_to_compile_count,plugins_description_db_corrupted,plugins_co-
de_db_corrupted,kbytes_received,kbytes_sent,dns_reverse_failures,dns_failures,avg_dns_
lookup_time,num_dns_lookups,avg_rdns_lookup_time,num_rdns_lookups,nessus_cpu,cpu_load_
avg,nessus_log_disk_free,nessus_log_disk_total,nessus_data_disk_free,nessus_data_disk_
total,temp_disk_free,temp_disk_total,num_tcp_sessions,nessus_vmem,nessus_mem,sys_ram_
used,sys_ram,sys_cores,num_hosts,num_scans
1754515429,0,0,0,0,0,0,2,7405,3,0,0,0,1,27047,34970,27047,34970,27047,34970,0,264,89,,
10045,10,0,0
1754515459,0,0,0,0,0,0,0,0,0,0,0,0,0,27047,34970,27047,34970,27047,34970,0,268,89,,100
45,10,0,0
1754515489,0,0,0,11,1494,0,0,0,0,0,0,3,3,27045,34970,27045,34970,27045,34970,0,281,88,
,10045,10,0,0
1754515519,0,0,0,1,1,0,0,0,0,0,0,0,2,27045,34970,27045,34970,27045,34970,0,281,88,,100
45,10,0,0
1754515549,0,0,0,1,37,0,0,0,0,0,0,0,2,27045,34970,27045,34970,27045,34970,0,281,88,,10
045,10,0,0
1754515579,0,0,0,0,0,0,0,0,0,0,0,0,0,2,27045,34970,27045,34970,27045,34970,0,281,88,,100
45,10,0,0
1754515609,0,0,0,0,0,0,0,0,0,0,0,0,0,4,27045,34970,27045,34970,27045,34970,0,281,88,,100
45,10,0,0
1754515639,0,0,0,0,0,0,0,0,0,0,0,0,0,3,27045,34970,27045,34970,27045,34970,0,281,88,,100
45,10,0,0
1754515669,0,0,0,0,0,0,0,0,0,0,0,0,0,2,27045,34970,27045,34970,27045,34970,0,281,88,,100
45,10,0,0
1754515699,0,0,0,0,0,0,0,0,0,0,0,0,0,1,27045,34970,27045,34970,27045,34970,0,281,88,,100
45,10,0,0
1754515729,0,0,0,0,0,0,0,0,0,0,0,0,0,1,27045,34970,27045,34970,27045,34970,0,281,88,,100
45,10,0,0
1754515759,0,0,0,0,0,0,0,0,0,0,0,0,0,0,27045,34970,27045,34970,27045,34970,0,281,88,,100
45,10,0,0
```

INFOTACT
SOLUTIONS

🔹 Step 8: Fix Issues Found

Theory: Fixing reported issues helps maintain system integrity and protects against exploitation.

Commands:-

```
sudo aptupdate && sudo aptupgrade    -y
sudo systemctl stop apache2
sudo systemctl disable apache2
```

```
secureadmin@UbuntuOS:~$ sudo su
[sudo] password for secureadmin:
root@UbuntuOS:/home/secureadmin# sudo apt update && sudo apt update upgrade -y
Ign:1 http://in.archive.ubuntu.com/ubuntu noble InRelease
Ign:2 http://security.ubuntu.com/ubuntu noble-security InRelease
Ign:3 http://in.archive.ubuntu.com/ubuntu noble-updates InRelease
Ign:4 http://in.archive.ubuntu.com/ubuntu noble-backports InRelease
Ign:2 http://security.ubuntu.com/ubuntu noble-security InRelease
Ign:1 http://in.archive.ubuntu.com/ubuntu noble InRelease
Ign:3 http://in.archive.ubuntu.com/ubuntu noble-updates InRelease
Ign:4 http://in.archive.ubuntu.com/ubuntu noble-backports InRelease
Ign:1 http://in.archive.ubuntu.com/ubuntu noble InRelease
Ign:2 http://security.ubuntu.com/ubuntu noble-security InRelease
Ign:3 http://in.archive.ubuntu.com/ubuntu noble-updates InRelease
Ign:4 http://in.archive.ubuntu.com/ubuntu noble-backports InRelease
Err:2 http://security.ubuntu.com/ubuntu noble-security InRelease
  Temporary failure resolving 'security.ubuntu.com'
Err:1 http://in.archive.ubuntu.com/ubuntu noble InRelease
  Temporary failure resolving 'in.archive.ubuntu.com'
Err:3 http://in.archive.ubuntu.com/ubuntu noble-updates InRelease
  Temporary failure resolving 'in.archive.ubuntu.com'
Err:4 http://in.archive.ubuntu.com/ubuntu noble-backports InRelease
  Temporary failure resolving 'in.archive.ubuntu.com'
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
295 packages can be upgraded. Run 'apt list --upgradable' to see them.
W: Failed to fetch http://in.archive.ubuntu.com/ubuntu/dists/noble/InRelease  Tempora
ry failure resolving 'in.archive.ubuntu.com'
W: Failed to fetch http://in.archive.ubuntu.com/ubuntu/dists/noble-updates/InRelease
 Temporary failure resolving 'in.archive.ubuntu.com'
W: Failed to fetch http://in.archive.ubuntu.com/ubuntu/dists/noble-backports/InReleas
e  Temporary failure resolving 'in.archive.ubuntu.com'
W: Failed to fetch http://security.ubuntu.com/ubuntu/dists/noble-security/InRelease
Temporary failure resolving 'security.ubuntu.com'
W: Some index files failed to download. They have been ignored, or old ones used inst
ead.
```

INFOTACT
SOLUTIONS

```
root@UbuntuOS:/home/secureadmin# sudo apt update
Get:1 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Hit:2 http://in.archive.ubuntu.com/ubuntu noble InRelease
Get:3 http://in.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [21.6 kB
]
Get:5 http://in.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:6 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [2
08 B]
Get:7 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [52.
3 kB]
Get:8 http://in.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [1,313 kB
]
Get:9 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [2
12 B]
Get:10 http://in.archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [164 k
B]
Get:11 http://in.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components
[212 B]
Get:12 http://in.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [1,1
20 kB]
Get:13 http://in.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [3
77 kB]
Get:14 http://in.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components
[940 B]
Get:15 http://in.archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [7,1
16 B]
Get:16 http://in.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Component
s [216 B]
Get:17 http://in.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components
[28.4 kB]
Get:18 http://in.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Component
s [212 B]
Fetched 3,464 kB in 18s (192 kB/s)
```

```
root@UbuntuOS:/home/secureadmin# sudo systemctl stop apache2
root@UbuntuOS:/home/secureadmin# sudo systemctl disable apache2
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd
/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install disable apache2
Removed "/etc/systemd/system/multi-user.target.wants/apache2.service".
root@UbuntuOS:/home/secureadmin#
```

sudo apt purge apache2 -y

```
root@UbuntuOS:/home/secureadmin# sudo apt purge apache2 -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  apache2-bin apache2-data apache2-utils libapr1t64 libaprutil1-dbd-sqlite3
  libaprutil1-ldap libaprutil1t64
Use 'sudo apt autoremove' to remove them.
The following packages will be REMOVED:
  apache2*
0 upgraded, 0 newly installed, 1 to remove and 295 not upgraded.
After this operation, 465 kB disk space will be freed.
(Reading database ... 154692 files and directories currently installed.)
Removing apache2 (2.4.58-1ubuntu8.7) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for ufw (0.36.2-6) ...
Rules updated for profile 'OpenSSH'
Firewall reloaded
(Reading database ... 154642 files and directories currently installed.)
Purging configuration files for apache2 (2.4.58-1ubuntu8.7) ...
Processing triggers for ufw (0.36.2-6) ...
Rules updated for profile 'OpenSSH'
Firewall reloaded
```

sudo apt autoremove -y

```
root@UbuntuOS:/home/secureadmin# sudo apt autoremove -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be REMOVED:
  apache2-bin apache2-data apache2-utils libapr1t64 libaprutil1-dbd-sqlite3
  libaprutil1-ldap libaprutil1t64
0 upgraded, 0 newly installed, 7 to remove and 295 not upgraded.
After this operation, 6,986 kB disk space will be freed.
(Reading database ... 154474 files and directories currently installed.)
Removing apache2-bin (2.4.58-1ubuntu8.7) ...
Removing apache2-data (2.4.58-1ubuntu8.7) ...
Removing apache2-utils (2.4.58-1ubuntu8.7) ...
Removing libaprutil1-dbd-sqlite3:amd64 (1.6.3-1.1ubuntu7) ...
Removing libaprutil1-ldap:amd64 (1.6.3-1.1ubuntu7) ...
Removing libaprutil1t64:amd64 (1.6.3-1.1ubuntu7) ...
Removing libapr1t64:amd64 (1.7.2-3.1ubuntu0.1) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.5) ...
root@UbuntuOS:/home/secureadmin#
```

INFOTACT
SOLUTIONS

✅ Conclusion

In this project, we successfully explored and implemented the foundational techniques of server security hardening, using a virtualized environment on Ubuntu Server within VirtualBox. This setup reflects real-world systems where server security is a critical necessity for enterprise and personal infrastructure.

We implemented a step-by-step approach including secure user authentication,

firewall

configurations, service auditing, and vulnerability scanning with Nessus . Through this, we understood the importance of minimizing attack surfaces, ensuring only

necessary

services run, and validating configurations via automated scans.

🔐 Purpose of Secure Server Setup

A

secureLinuxserver ensures:

- Confidentiality of system and user data
- Integrity of software and services
- Availability through reduced attack exposure
- Compliance with industry standards (e.g., CIS benchmarks)

📡 Future Research Directions

- Integration with SIEM tools (e.g., Splunk, Wazuh)
- Use of container security for Docker/Kubernetes environments
- Advanced techniques like SELinux, AppArmor, and systemcall monitoring
- Automated Ansible scripts for server hardening at scale
  Studying zero-trust architecture with endpoint verification

---

🔗 Important Links

- VirtualBox Download:
  https://www.virtualbox.org
- Ubuntu Server ISO (٢٠.٠٤ or ٢٢.٠٤):
  https://ubuntu.com/download/server
- Nessus Essentials (free):
  https://www.tenable.com/products/nessus/nessus-essentials

💻 Important Commands Used

Command	Purpose
`sudo apt update && sudo apt upgrade -y`	Update system
`sudo adduser secureadmin`	Add new secure user
`sudo usermod -aG sudo secureadmin`	Grant sudo rights
`sudo ufw enable`	Enable UFW firewall
`sudo ufw allow ssh`	Allow SSH through firewall
`sudo systemctl restart ssh`	Restart SSH daemon
`sudo apt install fail2ban`	Prevent brute force attacks
`sudo apt install apache2`	Install Apache (optional for testing)
`sudo apt purge apache2 -y`	Remove Apache if unnecessary
`sudo apt autoremove -y`	Clean unused dependencies
`sudo dpkg -i Nessus*.deb`	Install Nessus from .deb
`/opt/nessus/sbin/nessuscli fetch --challenge`	Start offline Nessus registration
`/opt/nessus/sbin/nessusd`	Start Nessus service manually
`sudo systemctl status nessusd.service`	Check Nessus service status
`https://localhost:8834`	Web interface to run scans

INFOTACT
SOLUTIONS

Thank you !