2. Windows and Linux Systems (Hardening Policies)

Prepared by: Ross Moravec / A00322717

The company operates a mixed environment with both Windows and Linux servers. These systems handle critical functions like:

o Windows VM: Running internal applications for customer management and financial analytics, it must be part of the company's Active Directory for centralized authentication and policy enforcement.

o Linux VM: Hosting secure web applications and providing development environments for blockchain and financial analytics tools. The Linux system must support secure SSH access and be hardened against threats.

Introduction

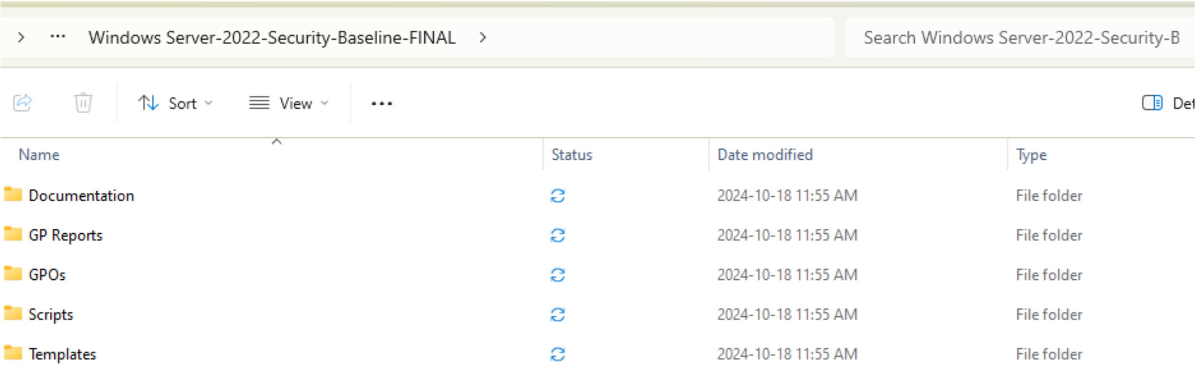
Note: Unlike the '1. Firewall Setup' document, this document maintains screenshots next to the corresponding commands and configuration steps. This format is intended to provide immediate visual context, especially for PowerShell commands and other configurations, to make it easier to follow along.

This document outlines the hardening policies for Windows and Linux systems within TechSecure Solutions' corporate environment. System hardening is crucial for minimizing vulnerabilities and securing the infrastructure against threats. The strategies in this document include setting secure configurations, applying relevant policies, and ensuring both Windows and Linux systems are adequately protected.

Windows Hardening - Script Scanning and Real-Time Monitoring

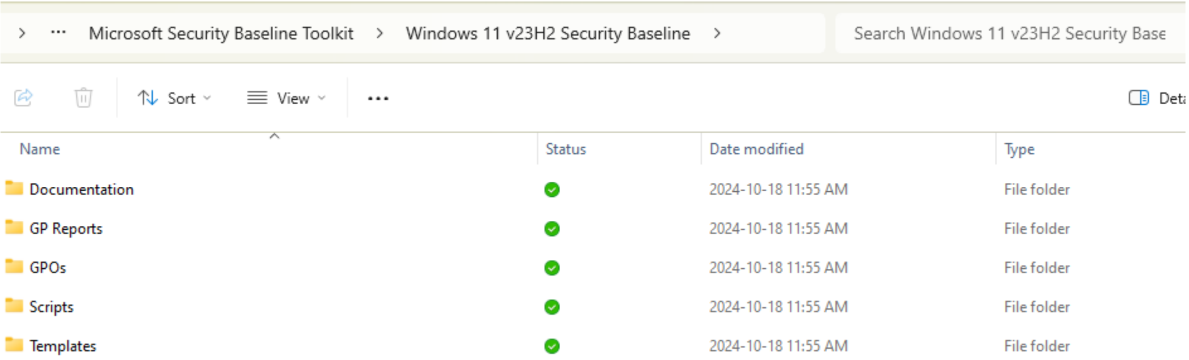
Enabling script scanning and real-time monitoring is essential in protecting the system against various forms of malware, especially script-based attacks. By enforcing these configurations, you ensure that Windows Defender actively monitors scripts executed on the system, minimizing the risk of malicious scripts going undetected. Furthermore, real-time monitoring enables continuous scanning of files and processes, which allows immediate detection and mitigation of potential security threats.

Microsoft Security Baseline Toolkit: The **Microsoft Security Baseline Toolkit** was chosen as the primary tool for hardening Windows systems because it provides a comprehensive, pre-configured set of security settings recommended by Microsoft. These settings are based on industry best practices and are tailored to reduce vulnerabilities in Windows environments. The toolkit simplifies the implementation of security policies by offering PowerShell scripts and GPO templates that can be easily applied across multiple systems. It ensures that critical areas, such as password policies, account lockout policies, malware protection, and network security configurations, are configured according to recommended security standards. By leveraging this toolkit, the system can be hardened effectively while maintaining compatibility with enterprise environments.


Windows Server-2022-Security-Baseline-FINAL
Search Windows Server-2022-Security-B
Sort
View
Det

Name	Status	Date modified	Type
Documentation	🔄	2024-10-18 11:55 AM	File folder
GP Reports	🔄	2024-10-18 11:55 AM	File folder
GPOs	🔄	2024-10-18 11:55 AM	File folder
Scripts	🔄	2024-10-18 11:55 AM	File folder
Templates	🔄	2024-10-18 11:55 AM	File folder

1.Windows Server-2022-Security-Baseline-FINAL was used to harden the Srv-TechSecure virtual machine.


Microsoft Security Baseline Toolkit
Windows 11 v23H2 Security Baseline
Search Windows 11 v23H2 Security Base
Sort
View
Deta

Name	Status	Date modified	Type
Documentation	✓	2024-10-18 11:55 AM	File folder
GP Reports	✓	2024-10-18 11:55 AM	File folder
GPOs	✓	2024-10-18 11:55 AM	File folder
Scripts	✓	2024-10-18 11:55 AM	File folder
Templates	✓	2024-10-18 11:55 AM	File folder

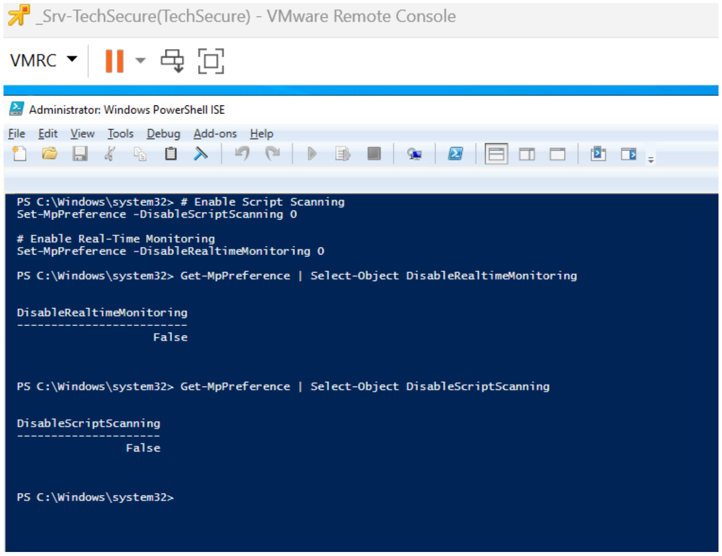
2. Microsoft Security Baseline Toolkit - Windows 11 v23H2 Security Baseline was used to harden the Win11-TechSecure virtual machine.

Pre-Snapshot and Post-Snapshot Explanations:

- **Pre-Snapshot**: Before executing the PowerShell script, a snapshot was taken to ensure the system could be restored to its original state in case of any issues.
- **Post-Snapshot**: After executing the PowerShell script and verifying the changes, another snapshot was taken to preserve the hardened system state.

PowerShell commands used to apply and verify the changes:

```
# Enable Script Scanning

Set-MpPreference -DisableScriptScanning 0

# Enable Real-Time Monitoring

Set-MpPreference -DisableRealtimeMonitoring 0

# Check Real-Time Monitoring Status

Get-MpPreference | Select-Object DisableRealtimeMonitoring

# Check Script Scanning Status

Get-MpPreference | Select-Object DisableScriptScanning
```



_Srv-TechSecure(TechSecure) - VMware Remote Console
VMRC
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help

```
PS C:\Windows\system32> # Enable Script Scanning
Set-MpPreference -DisableScriptScanning 0

# Enable Real-Time Monitoring
Set-MpPreference -DisableRealtimeMonitoring 0

PS C:\Windows\system32> Get-MpPreference | Select-Object DisableRealtimeMonitoring


DisableRealtimeMonitoring
-------------------------
                    False



PS C:\Windows\system32> Get-MpPreference | Select-Object DisableScriptScanning


DisableScriptScanning
---------------------
                False



PS C:\Windows\system32>
```

3. Enabling Script Scanning and Real-Time Monitoring - PowerShell commands were used to enable script scanning and real-time monitoring in the Srv-TechSecure system, enhancing protection against malicious scripts and unauthorized changes.

The printing restrictions script addresses the PrintNightmare vulnerability by restricting printer driver installations to administrators only.

PrintNightmare Vulnerability: The PrintNightmare vulnerability (CVE-2021-34527) exposes Windows systems to remote code execution attacks, allowing attackers to install malicious printer drivers. Restricting printer driver installations to administrators only helps mitigate this vulnerability by ensuring that only trusted drivers are installed on the system. This policy is enforced using a registry key that limits driver installations to administrative accounts.

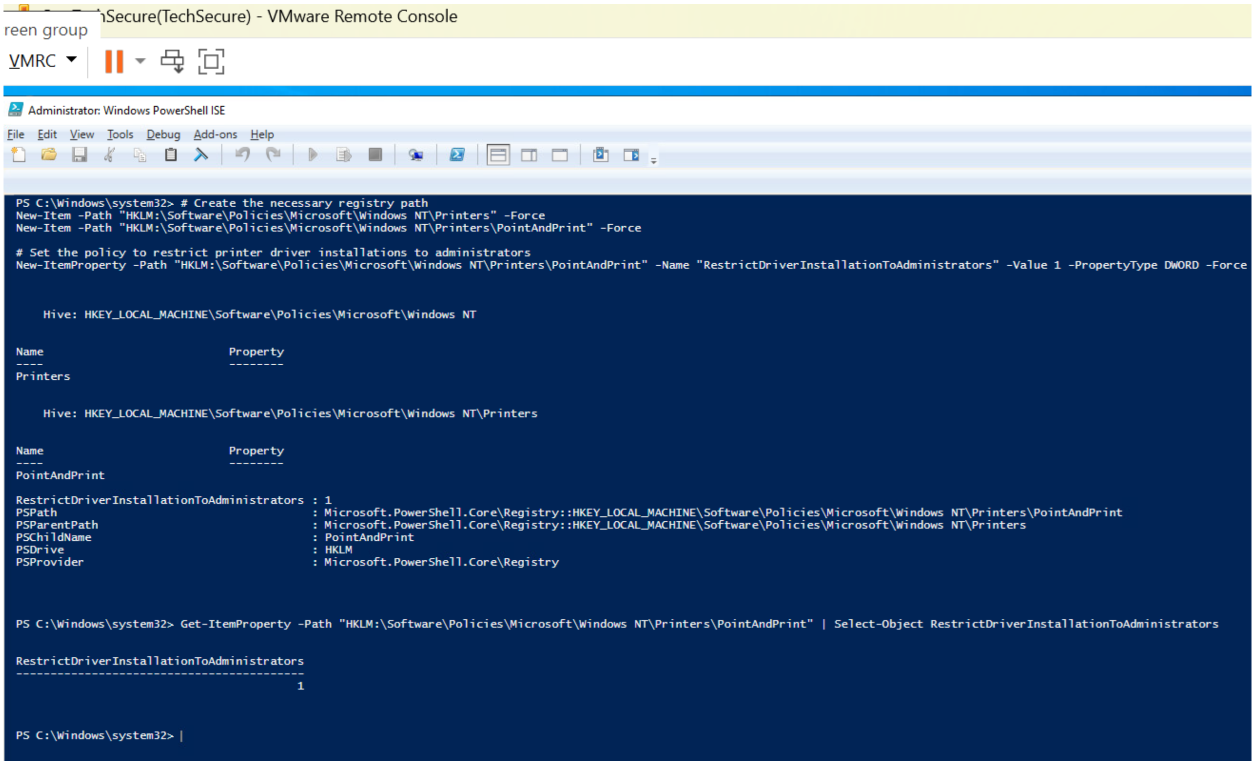
Using the following script to restrict printer driver installations:

```
# Create the necessary registry path

New-Item -Path "HKLM:\Software\Policies\Microsoft\Windows NT\Printers" -Force

New-Item -Path "HKLM:\Software\Policies\Microsoft\Windows NT\Printers\PointAndPrint" -Force


# Set the policy to restrict printer driver installations to administrators
```

New-ItemProperty -Path "HKLM:\Software\Policies\Microsoft\Windows NT\Printers\PointAndPrint" -Name "RestrictDriverInstallationToAdministrators" -Value 1 -PropertyType DWORD -Force

Running the following script to verify that the registry key has been applied:

Get-ItemProperty -Path "HKLM:\Software\Policies\Microsoft\Windows NT\Printers\PointAndPrint" | Select-Object RestrictDriverInstallationToAdministrators


hSecure(TechSecure) - VMware Remote Console
reen group
VMRC
Administrator: Windows PowerShell ISE
File
Edit
View
Tools
Debug
Add-ons
Help

```
PS C:\Windows\system32> # Create the necessary registry path
New-Item -Path "HKLM:\Software\Policies\Microsoft\Windows NT\Printers" -Force
New-Item -Path "HKLM:\Software\Policies\Microsoft\Windows NT\Printers\PointAndPrint" -Force

# Set the policy to restrict printer driver installations to administrators
New-ItemProperty -Path "HKLM:\Software\Policies\Microsoft\Windows NT\Printers\PointAndPrint" -Name "RestrictDriverInstallationToAdministrators" -Value 1 -PropertyType DWORD -Force


    Hive: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT


Name                           Property
----                           --------
Printers


    Hive: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Printers


Name                           Property
----                           --------
PointAndPrint

RestrictDriverInstallationToAdministrators : 1
PSPath                                     : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Printers\PointAndPrint
PSParentPath                               : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Printers
PSChildName                                : PointAndPrint
PSDrive                                    : HKLM
PSProvider                                 : Microsoft.PowerShell.Core\Registry



PS C:\Windows\system32> Get-ItemProperty -Path "HKLM:\Software\Policies\Microsoft\Windows NT\Printers\PointAndPrint" | Select-Object RestrictDriverInstallationToAdministrators


RestrictDriverInstallationToAdministrators
------------------------------------------
                                         1


PS C:\Windows\system32> |
```

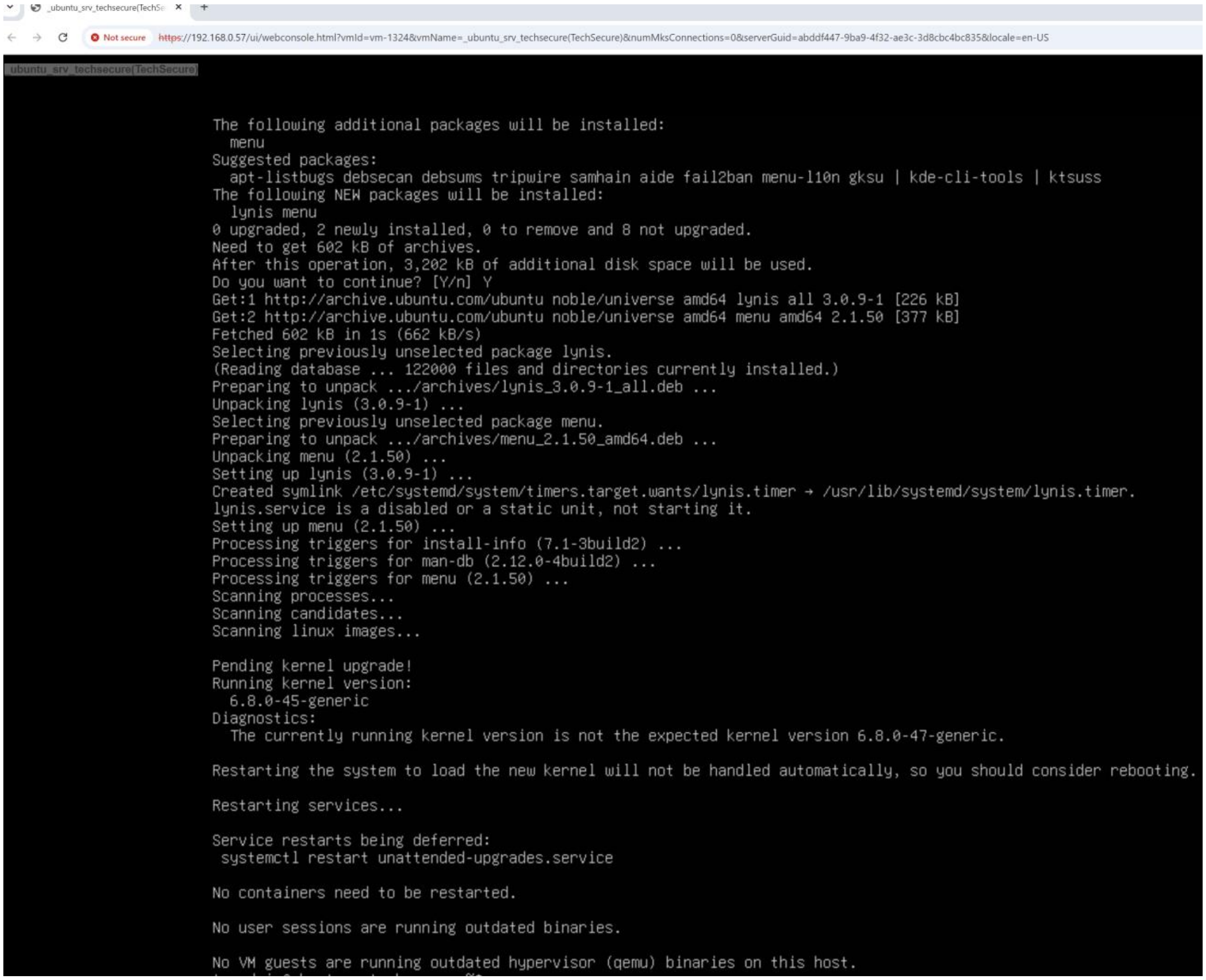
4. Restricting Printer Driver Installations - PowerShell commands were used to create registry keys to restrict printer driver installations to administrators only, mitigating the PrintNightmare vulnerability on the Srv-TechSecure system.

Conclusion: These security hardening steps—enabling script scanning, real-time monitoring, and restricting printer driver installations—help protect the system from potential vulnerabilities such as malware execution and unauthorized software installations. Regular auditing and monitoring should be continued to ensure the system remains secure over time.

2.2 Linux hardening

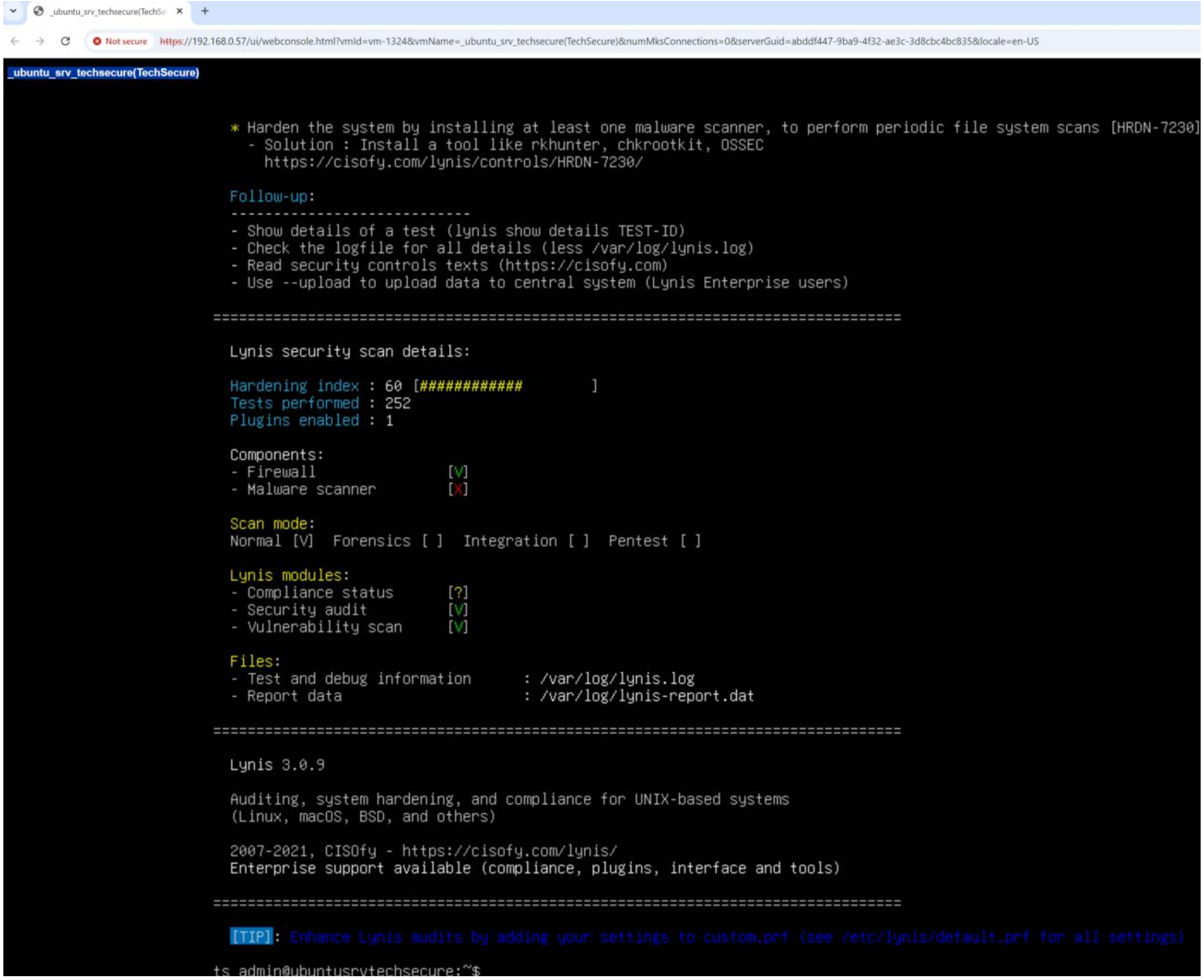
Linux Hardening - Disabling Root SSH Access

The decision to turn off root login for SSH in the Linux environment serves as a vital security measure. Allowing root access over SSH creates a high-value target for attackers. Once compromised, the root account gives unlimited control over the system. Disabling root SSH access adds an extra layer of protection, requiring users to log in with a less privileged account and then escalate privileges if necessary. This mitigates the risk of unauthorized users gaining unrestricted control over the server.


_ubuntu_srv_techsecure(TechSe
Not secure
https://192.168.0.57/ui/webconsole.html?vmId=vm-1324&vmName=_ubuntu_srv_techsecure(TechSecure)&numMksConnections=0&serverGuid=abddf447-9ba9-4f32-ae3c-3d8cbc4bc835&locale=en-US
_ubuntu_srv_techsecure(TechSecure)

```
The following additional packages will be installed:
  menu
Suggested packages:
  apt-listbugs debsecan debsums tripwire samhain aide fail2ban 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 8 not upgraded.
Need to get 602 kB of archives.
After this operation, 3,202 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://archive.ubuntu.com/ubuntu noble/universe amd64 lynis all 3.0.9-1 [226 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble/universe amd64 menu amd64 2.1.50 [377 kB]
Fetched 602 kB in 1s (662 kB/s)
Selecting previously unselected package lynis.
(Reading database ... 122000 files and directories currently installed.)
Preparing to unpack .../archives/lynis_3.0.9-1_all.deb ...
Unpacking lynis (3.0.9-1) ...
Selecting previously unselected package menu.
Preparing to unpack .../archives/menu_2.1.50_amd64.deb ...
Unpacking menu (2.1.50) ...
Setting up lynis (3.0.9-1) ...
Created symlink /etc/systemd/system/timers.target.wants/lynis.timer → /usr/lib/systemd/system/lynis.timer.
lynis.service is a disabled or a static unit, not starting it.
Setting up menu (2.1.50) ...
Processing triggers for install-info (7.1-3build2) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for menu (2.1.50) ...
Scanning processes...
Scanning candidates...
Scanning linux images...

Pending kernel upgrade!
Running kernel version:
  6.8.0-45-generic
Diagnostics:
  The currently running kernel version is not the expected kernel version 6.8.0-47-generic.

Restarting the system to load the new kernel will not be handled automatically, so you should consider rebooting.

Restarting services...

Service restarts being deferred:
 systemctl restart unattended-upgrades.service

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
```

5. Lynis Installation and System Check - Lynis was installed on the Ubuntu server for system auditing, followed by a system check indicating a pending kernel upgrade. A system restart is recommended to apply the new kernel version.


_ubuntu_srv_techsecure(TechSe
Not secure
https://192.168.0.57/ui/webconsole.html?vmId=vm-1324&vmName=_ubuntu_srv_techsecure(TechSecure)&numMksConnections=0&serverGuid=abddf447-9ba9-4f32-ae3c-3d8cbc4bc835&locale=en-US
_ubuntu_srv_techsecure(TechSecure)

```
  * Harden the system by installing at least one malware scanner, to perform periodic file system scans [HRDN-7230]
    - Solution : Install a tool like rkhunter, chkrootkit, OSSEC
      https://cisofy.com/lynis/controls/HRDN-7230/

  Follow-up:
  ----------------------------
  - Show details of a test (lynis show details TEST-ID)
  - Check the logfile for all details (less /var/log/lynis.log)
  - Read security controls texts (https://cisofy.com)
  - Use --upload to upload data to central system (Lynis Enterprise users)

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

  Lynis security scan details:

  Hardening index : 60 [############        ]
  Tests performed : 252
  Plugins enabled : 1

  Components:
  - Firewall               [V]
  - Malware scanner        [X]

  Scan mode:
  Normal [V]  Forensics [ ]  Integration [ ]  Pentest [ ]

  Lynis modules:
  - Compliance status      [?]
  - Security audit         [V]
  - Vulnerability scan     [V]

  Files:
  - Test and debug information      : /var/log/lynis.log
  - Report data                     : /var/log/lynis-report.dat

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

  Lynis 3.0.9

  Auditing, system hardening, and compliance for UNIX-based systems
  (Linux, macOS, BSD, and others)

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

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

  [TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)

ts_admin@ubuntusrvtechsecure:~$
```

6. Lynis Security Scan Report - A Lynis security scan was performed, resulting in a hardening index score of 60 out of 100. Recommendations were provided to enhance system security, including the installation of a malware scanner to improve the overall hardening score.

- **Hardening Index**: 60 (out of 100), which indicates that there's room for improvement in hardening your system.
- **Tests Performed**: 252
- **Plugins Enabled**: 1 (Firewall is configured, but no malware scanner is installed)

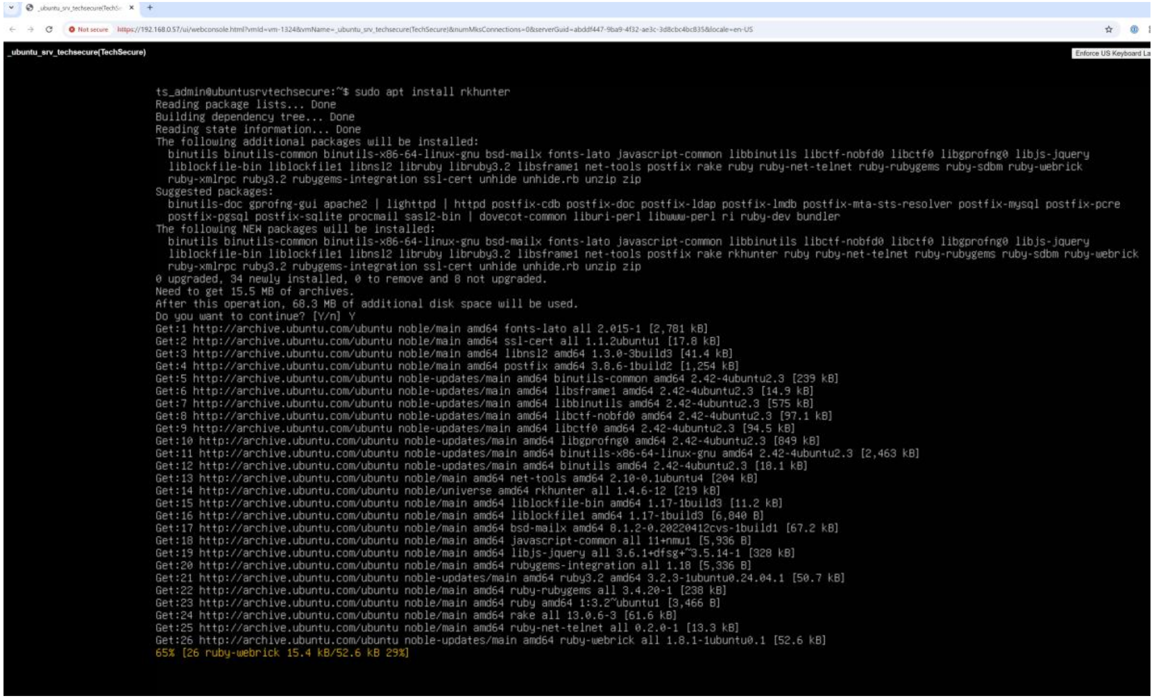
Recommendations:

- Install a malware scanner such as **rkhunter**, **chkrootkit**, or **OSSEC** for periodic file system scans. The next steps involve deploying additional recommended tools and conducting regular audits to enhance the overall hardening score and ensure continuous improvement.

Hardening Index Improvement: The current hardening index score of 60 out of 100 indicates that there is significant room for improvement in securing the system. To address the recommendations, the next steps include implementing a malware scanner, such as rkhunter or chkrootkit, to regularly audit the file system for anomalies. Additionally, further measures like applying stricter SSH policies and reviewing system configurations could enhance the overall security posture.

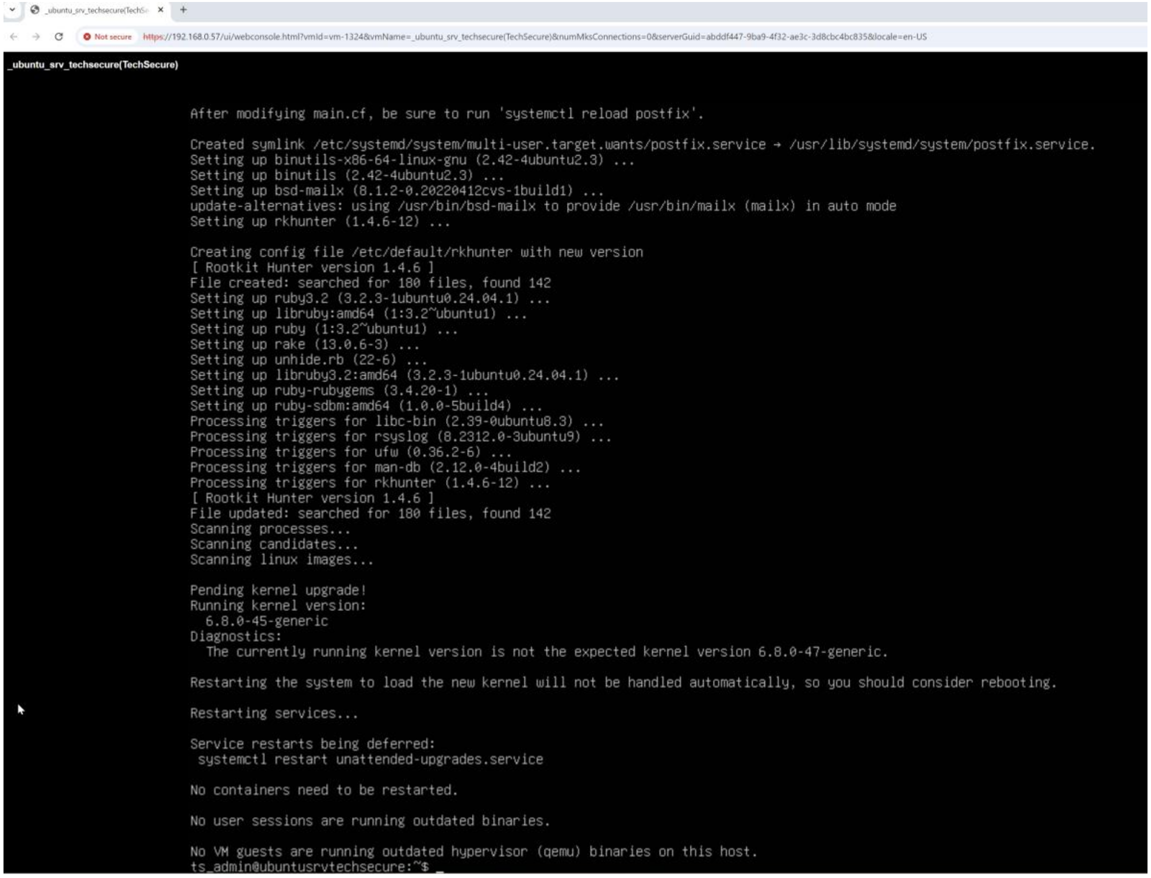
Installing **rkhunter** (Rootkit Hunter) to scan for rootkits and malware on the system:

sudo apt install rkhunter


_ubuntu_srv_techsecure(TechSe
Not secure
https://192.168.0.57/ui/webconsole.html?vmId=vm-1324&vmName=_ubuntu_srv_techsecure(TechSecure)&numMksConnections=0&serverGuid=abddf447-9ba9-4f32-ae3c-3d8cbc4bc835&locale=en-US
_ubuntu_srv_techsecure(TechSecure)
Enforce US Keyboard La

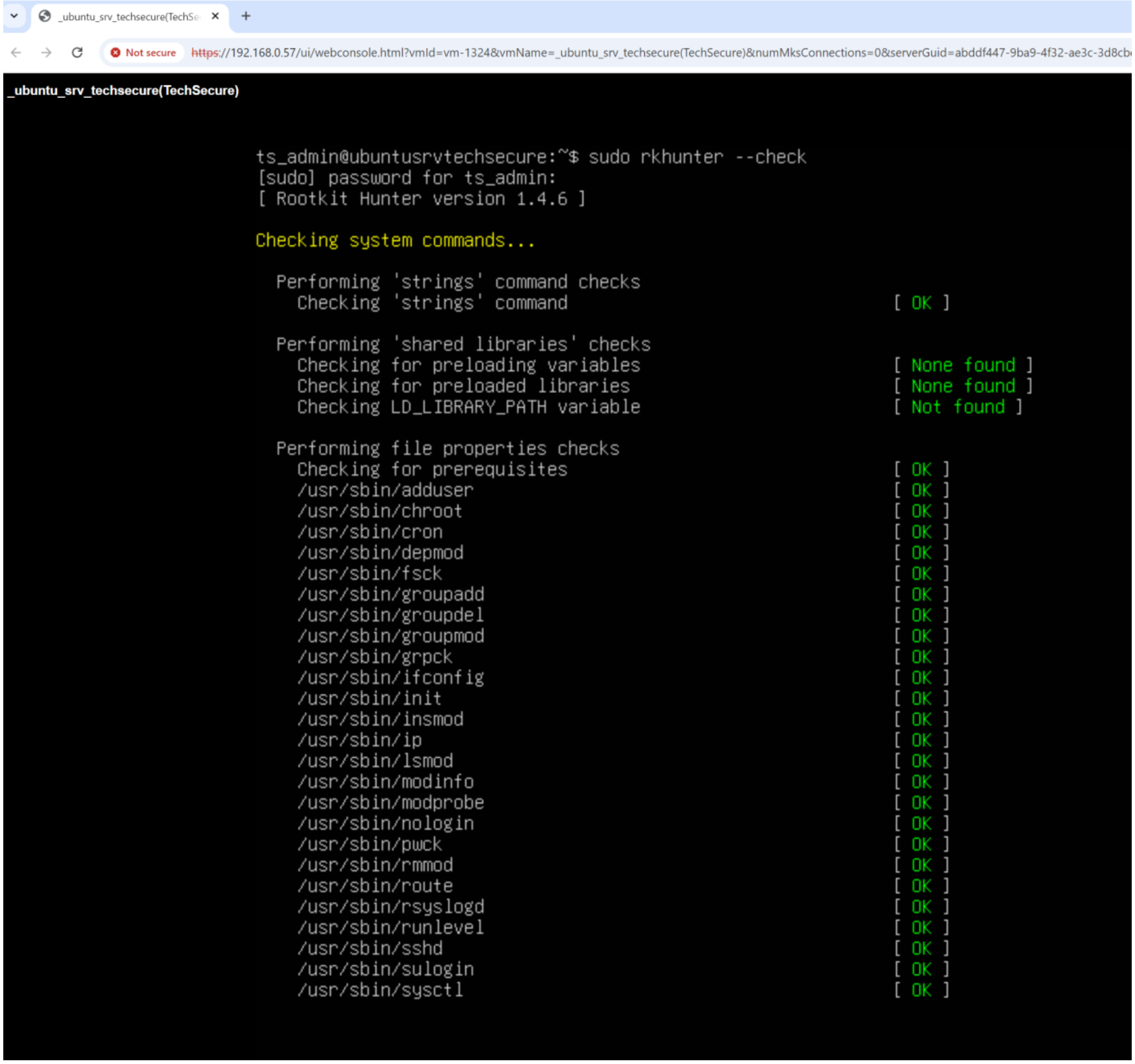
```
ts_admin@ubuntusrvtechsecure:~$ sudo apt install rkhunter
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu bsd-mailx fonts-lato javascript-common libbinutils libctf-nobfd0 libctf0 libgprofng0 libjs-jquery
  liblockfile-bin liblockfile1 libnsl2 libruby libruby3.2 libsframe1 net-tools postfix rake ruby ruby-net-telnet ruby-rubygems ruby-sdbm ruby-webrick
  ruby-xmlrpc ruby3.2 rubygems-integration ssl-cert unhide unhide.rb unzip zip
Suggested packages:
  binutils-doc gprofng-gui apache2 | lighttpd | httpd postfix-cdb postfix-doc postfix-ldap postfix-lmdb postfix-mta-sts-resolver postfix-mysql postfix-pcre
  postfix-pgsql postfix-sqlite procmail sasl2-bin | dovecot-common liburi-perl libwww-perl ri ruby-dev bundler
The following NEW packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu bsd-mailx fonts-lato javascript-common libbinutils libctf-nobfd0 libctf0 libgprofng0 libjs-jquery
  liblockfile-bin liblockfile1 libnsl2 libruby libruby3.2 libsframe1 net-tools postfix rake rkhunter ruby ruby-net-telnet ruby-rubygems ruby-sdbm ruby-webrick
  ruby-xmlrpc ruby3.2 rubygems-integration ssl-cert unhide unhide.rb unzip zip
0 upgraded, 34 newly installed, 0 to remove and 8 not upgraded.
Need to get 15.5 MB of archives.
After this operation, 68.3 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://archive.ubuntu.com/ubuntu noble/main amd64 fonts-lato all 2.015-1 [2,781 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble/main amd64 ssl-cert all 1.1.2ubuntu1 [17.8 kB]
Get:3 http://archive.ubuntu.com/ubuntu noble/main amd64 libnsl2 amd64 1.3.0-3build3 [41.4 kB]
Get:4 http://archive.ubuntu.com/ubuntu noble/main amd64 postfix amd64 3.8.6-1build2 [1,254 kB]
Get:5 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 binutils-common amd64 2.42-4ubuntu2.3 [239 kB]
Get:6 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libsframe1 amd64 2.42-4ubuntu2.3 [14.9 kB]
Get:7 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libbinutils amd64 2.42-4ubuntu2.3 [575 kB]
Get:8 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libctf-nobfd0 amd64 2.42-4ubuntu2.3 [97.1 kB]
Get:9 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libctf0 amd64 2.42-4ubuntu2.3 [94.5 kB]
Get:10 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libgprofng0 amd64 2.42-4ubuntu2.3 [849 kB]
Get:11 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 binutils-x86-64-linux-gnu amd64 2.42-4ubuntu2.3 [2,463 kB]
Get:12 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 binutils amd64 2.42-4ubuntu2.3 [18.1 kB]
Get:13 http://archive.ubuntu.com/ubuntu noble/main amd64 net-tools amd64 2.10-0.1ubuntu4 [204 kB]
Get:14 http://archive.ubuntu.com/ubuntu noble/universe amd64 rkhunter all 1.4.6-12 [219 kB]
Get:15 http://archive.ubuntu.com/ubuntu noble/main amd64 liblockfile-bin amd64 1.17-1build3 [11.2 kB]
Get:16 http://archive.ubuntu.com/ubuntu noble/main amd64 liblockfile1 amd64 1.17-1build3 [6,840 B]
Get:17 http://archive.ubuntu.com/ubuntu noble/main amd64 bsd-mailx amd64 8.1.2-0.20220412cvs-1build1 [67.2 kB]
Get:18 http://archive.ubuntu.com/ubuntu noble/main amd64 javascript-common all 11+nmu1 [5,936 B]
Get:19 http://archive.ubuntu.com/ubuntu noble/main amd64 libjs-jquery all 3.6.1+dfsg+~3.5.14-1 [328 kB]
Get:20 http://archive.ubuntu.com/ubuntu noble/main amd64 rubygems-integration all 1.18 [5,336 B]
Get:21 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 ruby3.2 amd64 3.2.3-1ubuntu0.24.04.1 [50.7 kB]
Get:22 http://archive.ubuntu.com/ubuntu noble/main amd64 ruby-rubygems all 3.4.20-1 [238 kB]
Get:23 http://archive.ubuntu.com/ubuntu noble/main amd64 ruby amd64 1:3.2~ubuntu1 [3,466 B]
Get:24 http://archive.ubuntu.com/ubuntu noble/main amd64 rake all 13.0.6-3 [61.6 kB]
Get:25 http://archive.ubuntu.com/ubuntu noble/main amd64 ruby-net-telnet all 0.2.0-1 [13.3 kB]
Get:26 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 ruby-webrick all 1.8.1-1ubuntu0.1 [52.6 kB]
65% [26 ruby-webrick 15.4 kB/52.6 kB 29%]
```

7. Installing Rootkit Hunter (rkhunter) - The rkhunter tool was installed on the ubuntu_srv_techsecure system to scan for rootkits and enhance malware detection capabilities, addressing recommendations from the Lynis security scan.


_ubuntu_srv_techsecure(TechSe
Not secure
https://192.168.0.57/ui/webconsole.html?vmId=vm-1324&vmName=_ubuntu_srv_techsecure(TechSecure)&numMksConnections=0&serverGuid=abddf447-9ba9-4f32-ae3c-3d8cbc4bc835&locale=en-US
_ubuntu_srv_techsecure(TechSecure)

```
After modifying main.cf, be sure to run 'systemctl reload postfix'.

Created symlink /etc/systemd/system/multi-user.target.wants/postfix.service → /usr/lib/systemd/system/postfix.service.
Setting up binutils-x86-64-linux-gnu (2.42-4ubuntu2.3) ...
Setting up binutils (2.42-4ubuntu2.3) ...
Setting up bsd-mailx (8.1.2-0.20220412cvs-1build1) ...
update-alternatives: using /usr/bin/bsd-mailx to provide /usr/bin/mailx (mailx) in auto mode
Setting up rkhunter (1.4.6-12) ...

Creating config file /etc/default/rkhunter with new version
[ Rootkit Hunter version 1.4.6 ]
File created: searched for 180 files, found 142
Setting up ruby3.2 (3.2.3-1ubuntu0.24.04.1) ...
Setting up libruby:amd64 (1:3.2~ubuntu1) ...
Setting up ruby (1:3.2~ubuntu1) ...
Setting up rake (13.0.6-3) ...
Setting up unhide.rb (22-6) ...
Setting up libruby3.2:amd64 (3.2.3-1ubuntu0.24.04.1) ...
Setting up ruby-rubygems (3.4.20-1) ...
Setting up ruby-sdbm:amd64 (1.0.0-5build4) ...
Processing triggers for libc-bin (2.39-0ubuntu8.3) ...
Processing triggers for rsyslog (8.2312.0-3ubuntu9) ...
Processing triggers for ufw (0.36.2-6) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for rkhunter (1.4.6-12) ...
[ Rootkit Hunter version 1.4.6 ]
File updated: searched for 180 files, found 142
Scanning processes...
Scanning candidates...
Scanning linux images...

Pending kernel upgrade!
Running kernel version:
  6.8.0-45-generic
Diagnostics:
  The currently running kernel version is not the expected kernel version 6.8.0-47-generic.

Restarting the system to load the new kernel will not be handled automatically, so you should consider rebooting.

Restarting services...

Service restarts being deferred:
 systemctl restart unattended-upgrades.service

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ts_admin@ubuntusrvtechsecure:~$ _
```

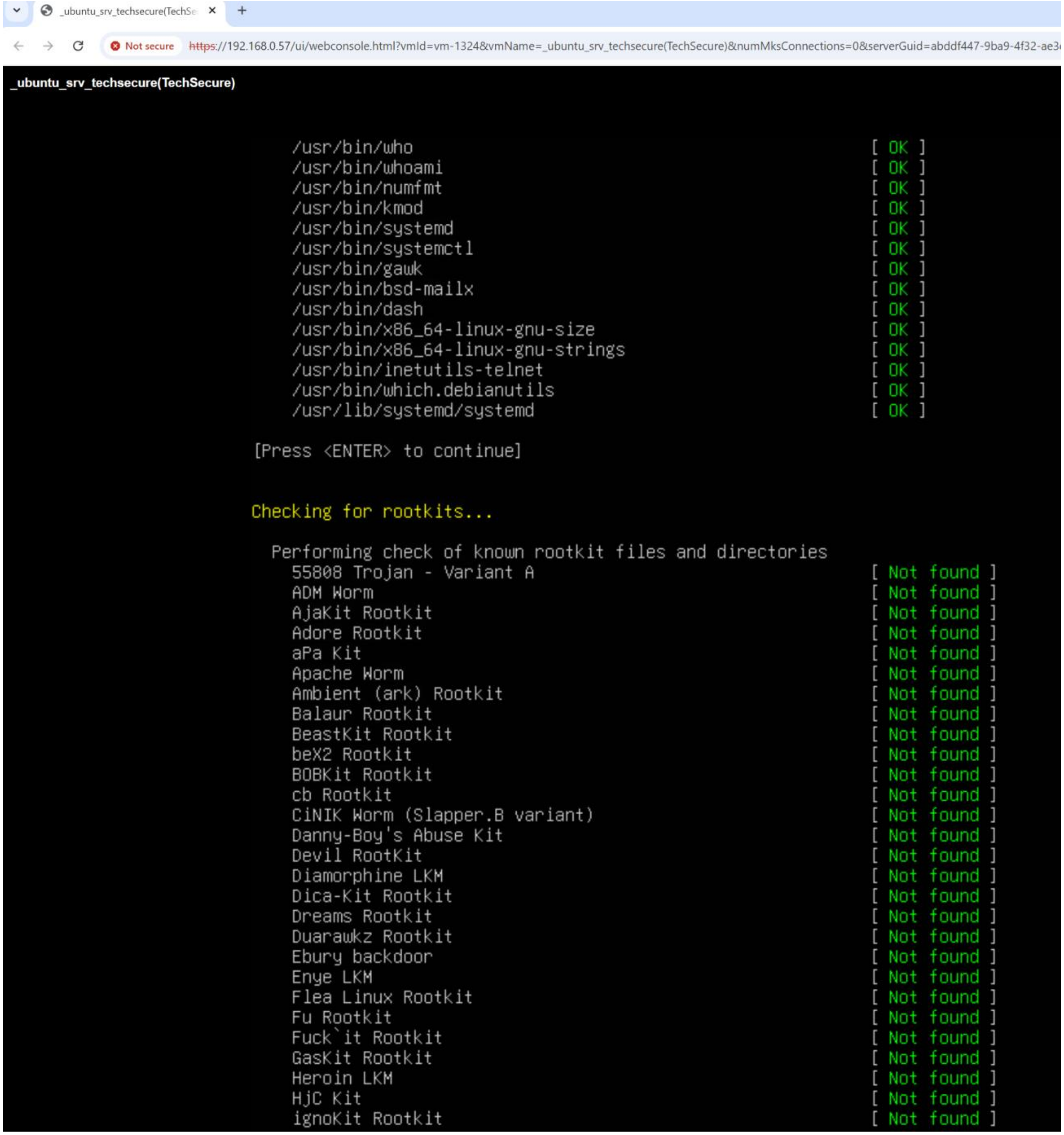
8. Rootkit Hunter Setup Verification - The rkhunter tool was successfully set up and configured on the ubuntu_srv_techsecure system. The configuration confirmed that files were searched and scanned, supporting enhanced security by regularly checking for rootkits.



_ubuntu_srv_techsecure(TechSe
Not secure
https://192.168.0.57/ui/webconsole.html?vmId=vm-1324&vmName=_ubuntu_srv_techsecure(TechSecure)&numMksConnections=0&serverGuid=abddf447-9ba9-4f32-ae3c-3d8cb
_ubuntu_srv_techsecure(TechSecure)

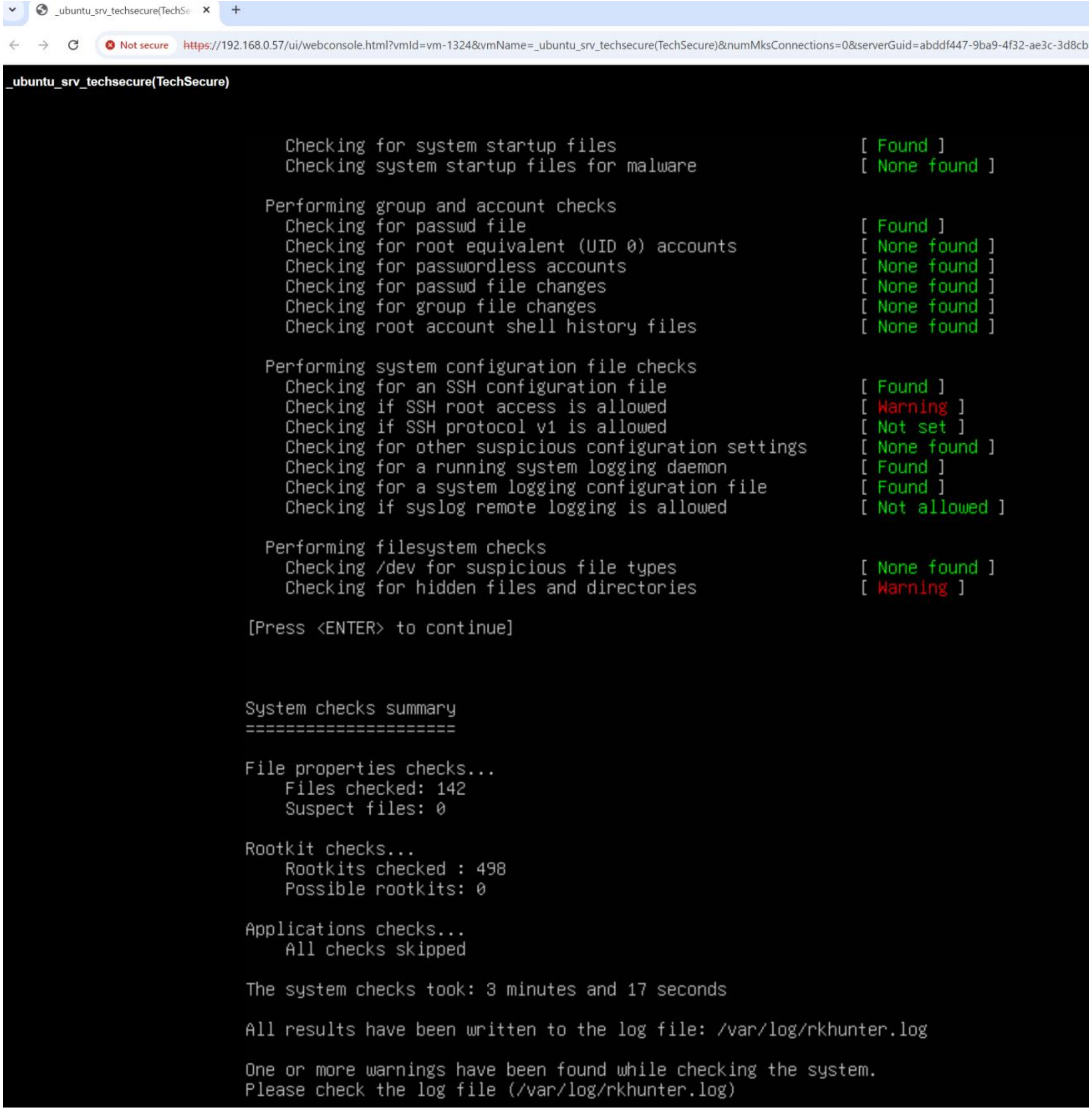
```
ts_admin@ubuntusrvtechsecure:~$ sudo rkhunter --check
[sudo] password for ts_admin:
[ Rootkit Hunter version 1.4.6 ]

Checking system commands...

  Performing 'strings' command checks
    Checking 'strings' command                              [ OK ]

  Performing 'shared libraries' checks
    Checking for preloading variables                       [ None found ]
    Checking for preloaded libraries                        [ None found ]
    Checking LD_LIBRARY_PATH variable                       [ Not found ]

  Performing file properties checks
    Checking for prerequisites                              [ OK ]
    /usr/sbin/adduser                                       [ OK ]
    /usr/sbin/chroot                                        [ OK ]
    /usr/sbin/cron                                          [ OK ]
    /usr/sbin/depmod                                        [ OK ]
    /usr/sbin/fsck                                          [ OK ]
    /usr/sbin/groupadd                                      [ OK ]
    /usr/sbin/groupdel                                      [ OK ]
    /usr/sbin/groupmod                                      [ OK ]
    /usr/sbin/grpck                                         [ OK ]
    /usr/sbin/ifconfig                                      [ OK ]
    /usr/sbin/init                                          [ OK ]
    /usr/sbin/insmod                                        [ OK ]
    /usr/sbin/ip                                            [ OK ]
    /usr/sbin/lsmod                                         [ OK ]
    /usr/sbin/modinfo                                       [ OK ]
    /usr/sbin/modprobe                                      [ OK ]
    /usr/sbin/nologin                                       [ OK ]
    /usr/sbin/pwck                                          [ OK ]
    /usr/sbin/rmmod                                         [ OK ]
    /usr/sbin/route                                         [ OK ]
    /usr/sbin/rsyslogd                                      [ OK ]
    /usr/sbin/runlevel                                      [ OK ]
    /usr/sbin/sshd                                          [ OK ]
    /usr/sbin/sulogin                                       [ OK ]
    /usr/sbin/sysctl                                        [ OK ]
```

9. Running Rootkit Hunter Check - The rkhunter tool was executed on the ubuntu_srv_techsecure system to perform checks on system commands, shared libraries, and file properties, ensuring that no malicious modifications or rootkits are present.


_ubuntu_srv_techsecure(TechSe ×
Not secure
https://192.168.0.57/ui/webconsole.html?vmId=vm-1324&vmName=_ubuntu_srv_techsecure(TechSecure)&numMksConnections=0&serverGuid=abddf447-9ba9-4f32-ae3
_ubuntu_srv_techsecure(TechSecure)

```
      /usr/bin/who                                             [ OK ]
      /usr/bin/whoami                                          [ OK ]
      /usr/bin/numfmt                                          [ OK ]
      /usr/bin/kmod                                            [ OK ]
      /usr/bin/systemd                                         [ OK ]
      /usr/bin/systemctl                                       [ OK ]
      /usr/bin/gawk                                            [ OK ]
      /usr/bin/bsd-mailx                                       [ OK ]
      /usr/bin/dash                                            [ OK ]
      /usr/bin/x86_64-linux-gnu-size                           [ OK ]
      /usr/bin/x86_64-linux-gnu-strings                        [ OK ]
      /usr/bin/inetutils-telnet                                [ OK ]
      /usr/bin/which.debianutils                               [ OK ]
      /usr/lib/systemd/systemd                                 [ OK ]

  [Press <ENTER> to continue]


  Checking for rootkits...

    Performing check of known rootkit files and directories
      55808 Trojan - Variant A                                 [ Not found ]
      ADM Worm                                                 [ Not found ]
      AjaKit Rootkit                                           [ Not found ]
      Adore Rootkit                                            [ Not found ]
      aPa Kit                                                  [ Not found ]
      Apache Worm                                              [ Not found ]
      Ambient (ark) Rootkit                                    [ Not found ]
      Balaur Rootkit                                           [ Not found ]
      BeastKit Rootkit                                         [ Not found ]
      beX2 Rootkit                                             [ Not found ]
      BOBKit Rootkit                                           [ Not found ]
      cb Rootkit                                               [ Not found ]
      CiNIK Worm (Slapper.B variant)                           [ Not found ]
      Danny-Boy's Abuse Kit                                    [ Not found ]
      Devil RootKit                                            [ Not found ]
      Diamorphine LKM                                          [ Not found ]
      Dica-Kit Rootkit                                         [ Not found ]
      Dreams Rootkit                                           [ Not found ]
      Duarawkz Rootkit                                         [ Not found ]
      Ebury backdoor                                           [ Not found ]
      Enye LKM                                                 [ Not found ]
      Flea Linux Rootkit                                       [ Not found ]
      Fu Rootkit                                               [ Not found ]
      Fuck`it Rootkit                                          [ Not found ]
      GasKit Rootkit                                           [ Not found ]
      Heroin LKM                                               [ Not found ]
      HjC Kit                                                  [ Not found ]
      ignoKit Rootkit                                          [ Not found ]
```

10. Rootkit Hunter Scan for Known Rootkits - The rkhunter tool was used on the ubuntu_srv_techsecure system to check for known rootkits and trojans, confirming that no malicious rootkits were found.


_ubuntu_srv_techsecure(TechSe
Not secure
https://192.168.0.57/ui/webconsole.html?vmId=vm-1324&vmName=_ubuntu_srv_techsecure(TechSecure)&numMksConnections=0&serverGuid=abddf447-9ba9-4f32-ae3c-3d8cb
_ubuntu_srv_techsecure(TechSecure)

```
    Checking for system startup files                           [ Found ]
    Checking system startup files for malware                   [ None found ]

  Performing group and account checks
    Checking for passwd file                                    [ Found ]
    Checking for root equivalent (UID 0) accounts               [ None found ]
    Checking for passwordless accounts                          [ None found ]
    Checking for passwd file changes                            [ None found ]
    Checking for group file changes                             [ None found ]
    Checking root account shell history files                   [ None found ]

  Performing system configuration file checks
    Checking for an SSH configuration file                      [ Found ]
    Checking if SSH root access is allowed                      [ Warning ]
    Checking if SSH protocol v1 is allowed                      [ Not set ]
    Checking for other suspicious configuration settings        [ None found ]
    Checking for a running system logging daemon                [ Found ]
    Checking for a system logging configuration file            [ Found ]
    Checking if syslog remote logging is allowed                [ Not allowed ]

  Performing filesystem checks
    Checking /dev for suspicious file types                     [ None found ]
    Checking for hidden files and directories                   [ Warning ]

[Press <ENTER> to continue]



System checks summary
=====================

File properties checks...
    Files checked: 142
    Suspect files: 0

Rootkit checks...
    Rootkits checked : 498
    Possible rootkits: 0

Applications checks...
    All checks skipped

The system checks took: 3 minutes and 17 seconds

All results have been written to the log file: /var/log/rkhunter.log

One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)
```

11. Rootkit Hunter Scan Results Summary - The rkhunter tool was used to conduct a detailed scan on the ubuntu_srv_techsecure system, verifying system configuration files, startup files, and group and account checks, with a few warnings found regarding SSH and hidden files.

the **rkhunter scan** completed successfully, with the following results:

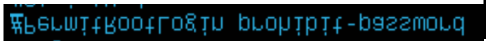
Key Findings:

- **System startup files**: No malware found.
- **Group and account checks**: No issues found.
- **System configuration checks**:
    - **SSH configuration file** found, but there are warnings:
        - **SSH root access**: Warning (potential security risk if enabled).
        - **SSH Protocol v1**: Not set (recommend ensuring Protocol v1 is disabled, as it's outdated).
        - **Syslog remote logging**: Not allowed (this is typically okay unless you need remote logging).
- **Filesystem checks**: No suspicious file types, but a warning about hidden files and directories (might require investigation).

Disabling Root Login via SSH:

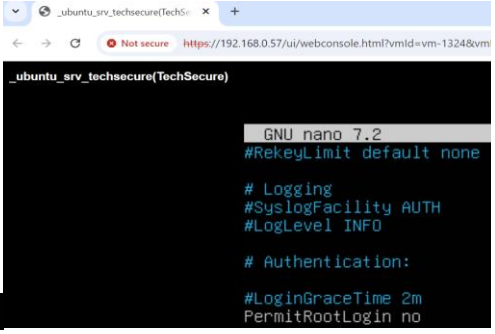
Disabling root login via SSH helps reduce the attack surface available to malicious users. Even though administrators can still escalate privileges using sudo, starting from a non-root account forces attackers to compromise a regular user account before attempting privilege escalation. Additionally, by not allowing root access directly, you can enforce stricter access control policies, which can further be audited and logged. This helps system administrators maintain better control over who accesses the system and what operations are being performed.

Original:



```
#PermitRootLogin prohibit-password
```

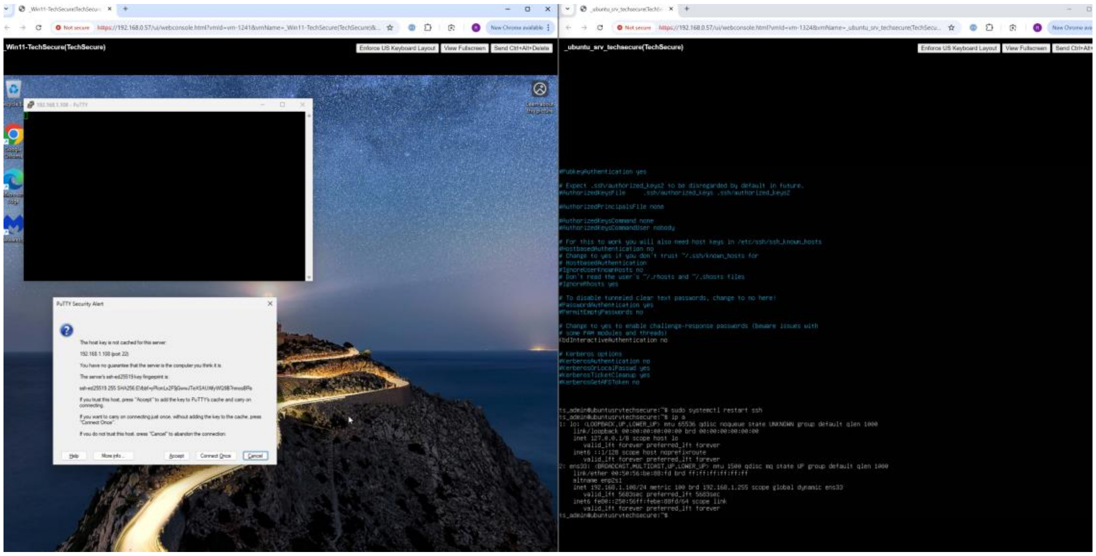
Modified:



_ubuntu_srv_techsecure(TechSe
Not secure
https://192.168.0.57/ui/webconsole.html?vmId=vm-1324&vmI
_ubuntu_srv_techsecure(TechSecure)

```
  GNU nano 7.2
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
```

12. Disabling Root Login via SSH illustrates the modification of the SSH configuration file (/etc/ssh/sshd_config) on the ubuntu_srv_techsecure system.



_Win11-TechSecure(TechSecure)
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
_ubuntu_srv_techsecure(TechSecure)
192.168.1.108 - PuTTY

PuTTY Security Alert

The host key is not cached for this server:

192.168.1.108 (port 22)

You have no guarantee that the server is the computer you think it is.

The server's ssh-ed25519 key fingerprint is:

ssh-ed25519 255 SHA256:[illegible]

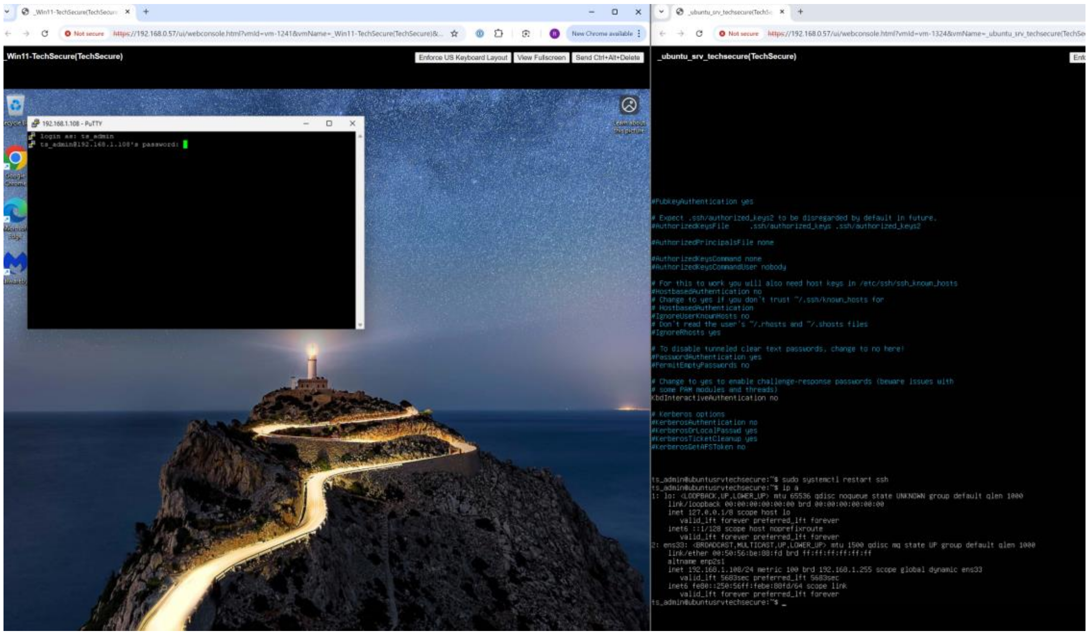
If you trust this host, press "Accept" to add the key to PuTTY's cache and carry on connecting.

If you want to carry on connecting just once, without adding the key to the cache, press "Connect Once".

If you do not trust this host, press "Cancel" to abandon the connection.

```
#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
KbdInteractiveAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no


ts_admin@ubuntusrvtechsecure:~$ sudo systemctl restart ssh
ts_admin@ubuntusrvtechsecure:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:be:80:fd brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.1.108/24 metric 100 brd 192.168.1.255 scope global dynamic ens33
       valid_lft 5683sec preferred_lft 5683sec
    inet6 fe80::250:56ff:febe:80fd/64 scope link
       valid_lft forever preferred_lft forever
ts_admin@ubuntusrvtechsecure:~$
```

13. SSH Connection Verification - Using PuTTY to verify SSH access from Win11-TechSecure to ubuntu_srv_techsecure: The snapshot shows the PuTTY Security Alert during an SSH connection attempt, highlighting the importance of verifying host key authenticity to ensure secure connections between systems. On the right, configurations on the ubuntu_srv_techsecure system are being updated to support the secure connection.

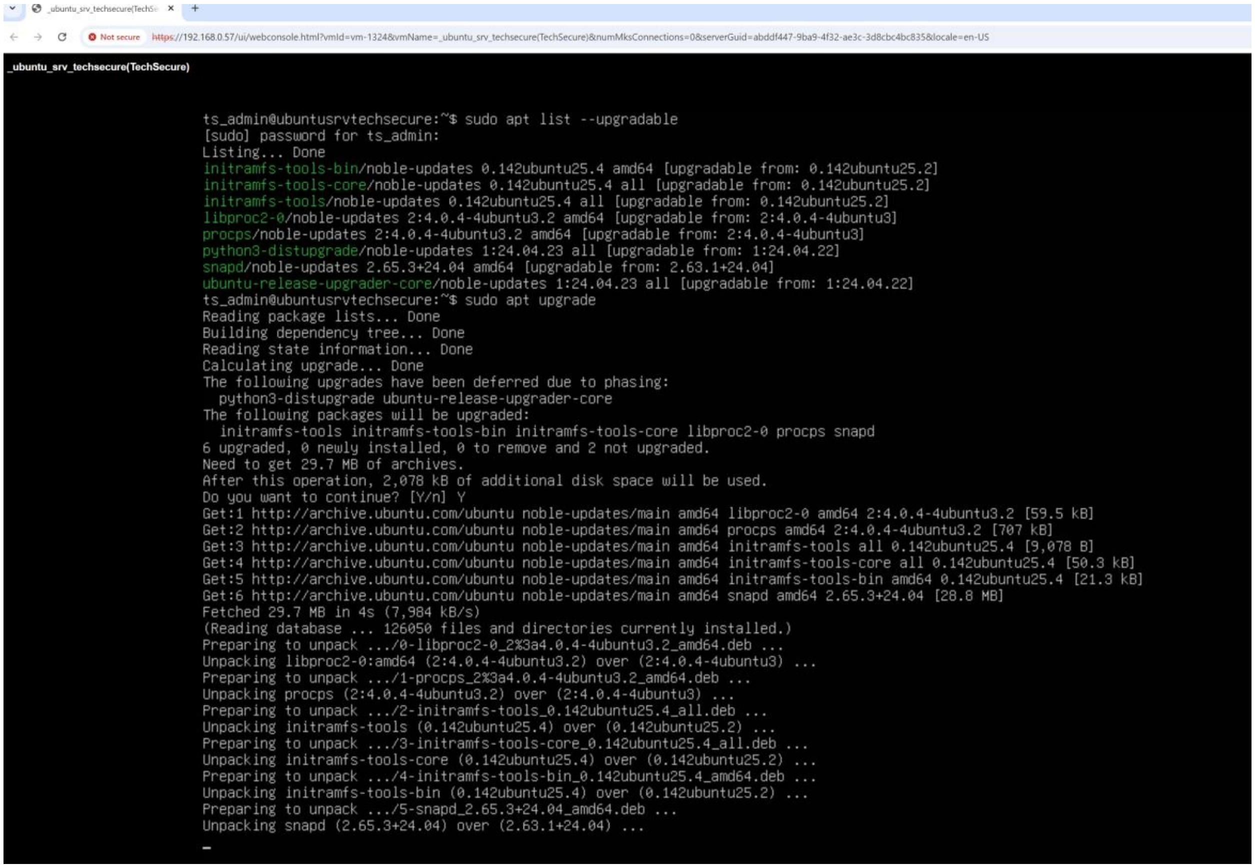


_Win11-TechSecure(TechSecure)
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
_ubuntu_srv_techsecure(TechSecure)
192.168.1.108 - PuTTY

```
login as: ts_admin
ts_admin@192.168.1.108's password:
```

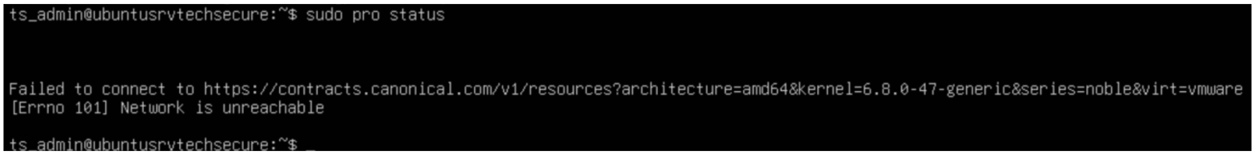
```
#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
KbdInteractiveAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no


ts_admin@ubuntusrvtechsecure:~$ sudo systemctl restart ssh
ts_admin@ubuntusrvtechsecure:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:be:80:fd brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.1.108/24 metric 100 brd 192.168.1.255 scope global dynamic ens33
       valid_lft 5683sec preferred_lft 5683sec
    inet6 fe80::250:56ff:febe:80fd/64 scope link
       valid_lft forever preferred_lft forever
ts_admin@ubuntusrvtechsecure:~$ _
```

14. SSH Login Prompt - Initiating Secure Access to ubuntu_srv_techsecure: This snapshot illustrates the login process via PuTTY from the Win11-TechSecure machine to the ubuntu_srv_techsecure system, prompting for the ts_admin credentials, indicating the beginning of a secure SSH session.


_ubuntu_srv_techsecure(TechSe
Not secure
https://192.168.0.57/ui/webconsole.html?vmId=vm-1324&vmName=_ubuntu_srv_techsecure(TechSecure)&numMksConnections=0&serverGuid=abddf447-9ba9-4f32-ae3c-3d8cbc4bc835&locale=en-US
_ubuntu_srv_techsecure(TechSecure)

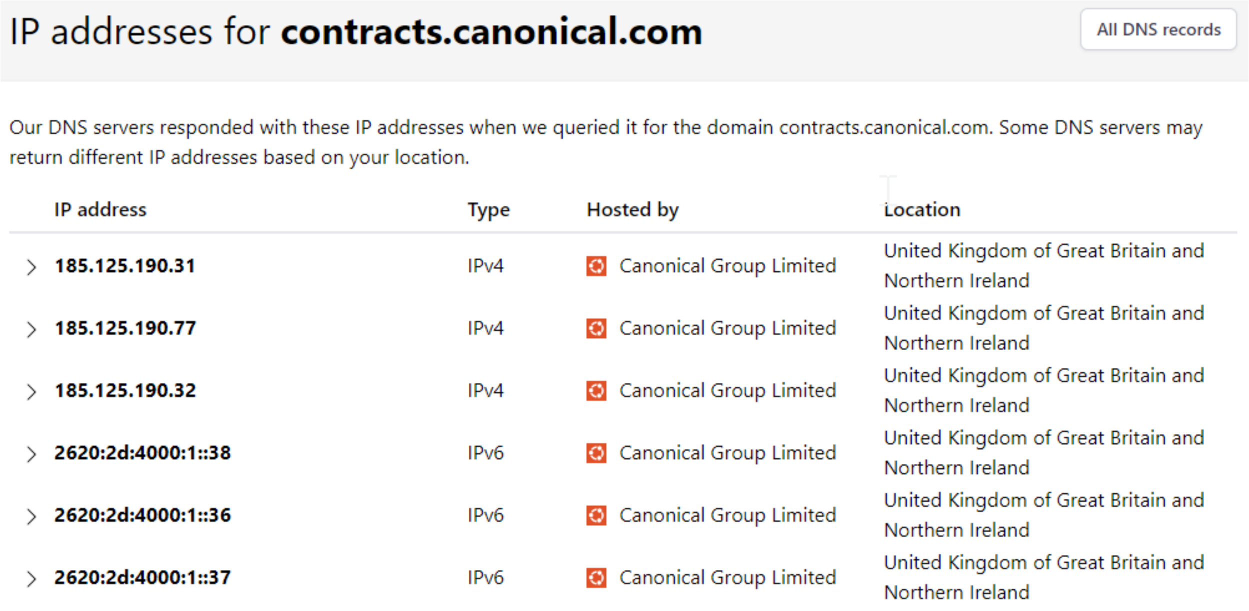
```
ts_admin@ubuntusrvtechsecure:~$ sudo apt list --upgradable
[sudo] password for ts_admin:
Listing... Done
initramfs-tools-bin/noble-updates 0.142ubuntu25.4 amd64 [upgradable from: 0.142ubuntu25.2]
initramfs-tools-core/noble-updates 0.142ubuntu25.4 all [upgradable from: 0.142ubuntu25.2]
initramfs-tools/noble-updates 0.142ubuntu25.4 all [upgradable from: 0.142ubuntu25.2]
libproc2-0/noble-updates 2:4.0.4-4ubuntu3.2 amd64 [upgradable from: 2:4.0.4-4ubuntu3]
procps/noble-updates 2:4.0.4-4ubuntu3.2 amd64 [upgradable from: 2:4.0.4-4ubuntu3]
python3-distupgrade/noble-updates 1:24.04.23 all [upgradable from: 1:24.04.22]
snapd/noble-updates 2.65.3+24.04 amd64 [upgradable from: 2.63.1+24.04]
ubuntu-release-upgrader-core/noble-updates 1:24.04.23 all [upgradable from: 1:24.04.22]
ts_admin@ubuntusrvtechsecure:~$ sudo apt upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following upgrades have been deferred due to phasing:
  python3-distupgrade ubuntu-release-upgrader-core
The following packages will be upgraded:
  initramfs-tools initramfs-tools-bin initramfs-tools-core libproc2-0 procps snapd
6 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
Need to get 29.7 MB of archives.
After this operation, 2,078 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libproc2-0 amd64 2:4.0.4-4ubuntu3.2 [59.5 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 procps amd64 2:4.0.4-4ubuntu3.2 [707 kB]
Get:3 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 initramfs-tools all 0.142ubuntu25.4 [9,078 B]
Get:4 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 initramfs-tools-core all 0.142ubuntu25.4 [50.3 kB]
Get:5 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 initramfs-tools-bin amd64 0.142ubuntu25.4 [21.3 kB]
Get:6 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 snapd amd64 2.65.3+24.04 [28.8 MB]
Fetched 29.7 MB in 4s (7,984 kB/s)
(Reading database ... 126050 files and directories currently installed.)
Preparing to unpack .../0-libproc2-0_2%3a4.0.4-4ubuntu3.2_amd64.deb ...
Unpacking libproc2-0:amd64 (2:4.0.4-4ubuntu3.2) over (2:4.0.4-4ubuntu3) ...
Preparing to unpack .../1-procps_2%3a4.0.4-4ubuntu3.2_amd64.deb ...
Unpacking procps (2:4.0.4-4ubuntu3.2) over (2:4.0.4-4ubuntu3) ...
Preparing to unpack .../2-initramfs-tools_0.142ubuntu25.4_all.deb ...
Unpacking initramfs-tools (0.142ubuntu25.4) over (0.142ubuntu25.2) ...
Preparing to unpack .../3-initramfs-tools-core_0.142ubuntu25.4_all.deb ...
Unpacking initramfs-tools-core (0.142ubuntu25.4) over (0.142ubuntu25.2) ...
Preparing to unpack .../4-initramfs-tools-bin_0.142ubuntu25.4_amd64.deb ...
Unpacking initramfs-tools-bin (0.142ubuntu25.4) over (0.142ubuntu25.2) ...
Preparing to unpack .../5-snapd_2.65.3+24.04_amd64.deb ...
Unpacking snapd (2.65.3+24.04) over (2.63.1+24.04) ...
_
```

15. Upgrading Packages on ubuntu_srv_techsecure - The snapshot shows the process of upgrading available packages on the ubuntu_srv_techsecure system using sudo apt upgrade, ensuring the system is kept up-to-date with the latest security patches and improvements.



```
ts_admin@ubuntusrvtechsecure:~$ sudo pro status


Failed to connect to https://contracts.canonical.com/v1/resources?architecture=amd64&kernel=6.8.0-47-generic&series=noble&virt=vmware
[Errno 101] Network is unreachable

ts_admin@ubuntusrvtechsecure:~$ _
```

16. Geolocation Blocking in Effect - The snapshot indicates that geolocation blocking on the firewall is active, as a network connection attempt to Canonical resources failed due to the U.K. IP addresses being blocked, making the network unreachable.

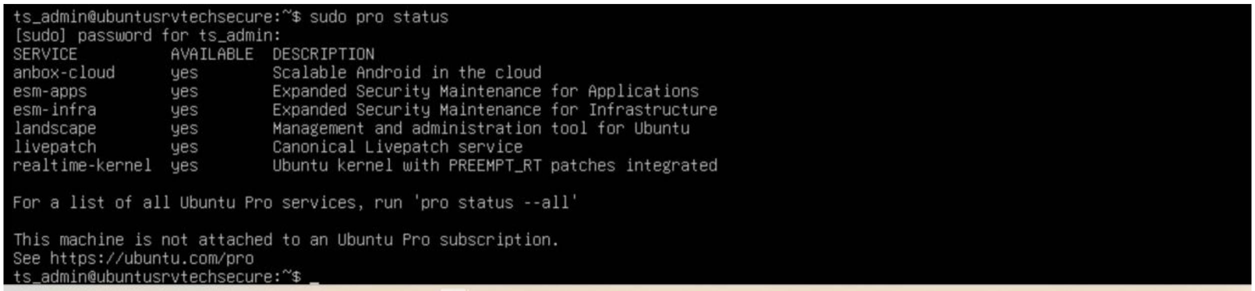


IP addresses for **contracts.canonical.com**

Our DNS servers responded with these IP addresses when we queried it for the domain contracts.canonical.com. Some DNS servers may return different IP addresses based on your location.

IP address	Type	Hosted by	Location
185.125.190.31	IPv4	Canonical Group Limited	United Kingdom of Great Britain and Northern Ireland
185.125.190.77	IPv4	Canonical Group Limited	United Kingdom of Great Britain and Northern Ireland
185.125.190.32	IPv4	Canonical Group Limited	United Kingdom of Great Britain and Northern Ireland
2620:2d:4000:1::38	IPv6	Canonical Group Limited	United Kingdom of Great Britain and Northern Ireland
2620:2d:4000:1::36	IPv6	Canonical Group Limited	United Kingdom of Great Britain and Northern Ireland
2620:2d:4000:1::37	IPv6	Canonical Group Limited	United Kingdom of Great Britain and Northern Ireland

17. Canonical IP Addresses Location - The DNS query results show that the IP addresses for contracts.canonical.com are located in the United Kingdom, confirming that the connection was blocked due to geolocation firewall rules targeting U.K. IP addresses.



```
ts_admin@ubuntusrvtechsecure:~$ sudo pro status
[sudo] password for ts_admin:
SERVICE          AVAILABLE  DESCRIPTION
anbox-cloud      yes        Scalable Android in the cloud
esm-apps         yes        Expanded Security Maintenance for Applications
esm-infra        yes        Expanded Security Maintenance for Infrastructure
landscape        yes        Management and administration tool for Ubuntu
livepatch        yes        Canonical Livepatch service
realtime-kernel  yes        Ubuntu kernel with PREEMPT_RT patches integrated

For a list of all Ubuntu Pro services, run 'pro status --all'

This machine is not attached to an Ubuntu Pro subscription.
See https://ubuntu.com/pro
ts_admin@ubuntusrvtechsecure:~$ _
```

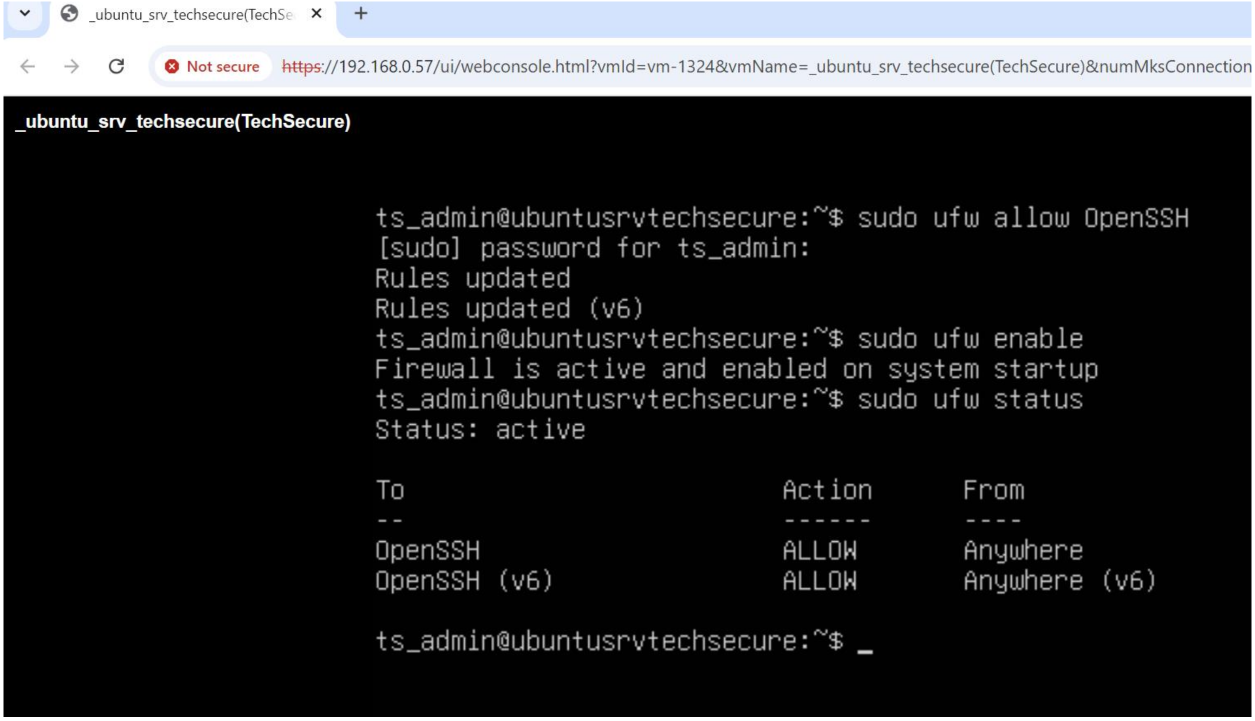
18. Access to Canonical Restored - After disabling the geolocation blocking on the firewall, access to Canonical services has been restored, as indicated by the successful execution of `sudo pro status`.

The Ubuntu Pro subscription might be one of the options for hardening a Linux machine in the Fintech sector.

Firewall Configuration (UFW):

The project mentions the need for secure SSH access and hardening. Configuring a firewall using **ufw** would enhance security by restricting unnecessary incoming traffic, thus reducing potential attack surfaces. Allowing only SSH traffic fits the requirement to ensure secure access while also protecting the server from unwanted connections.

Implementing **ufw** to allow **OpenSSH** traffic, ensuring that only essential services are exposed:


_ubuntu_srv_techsecure(TechSe
Not secure
~~https~~://192.168.0.57/ui/webconsole.html?vmId=vm-1324&vmName=_ubuntu_srv_techsecure(TechSecure)&numMksConnection
_ubuntu_srv_techsecure(TechSecure)

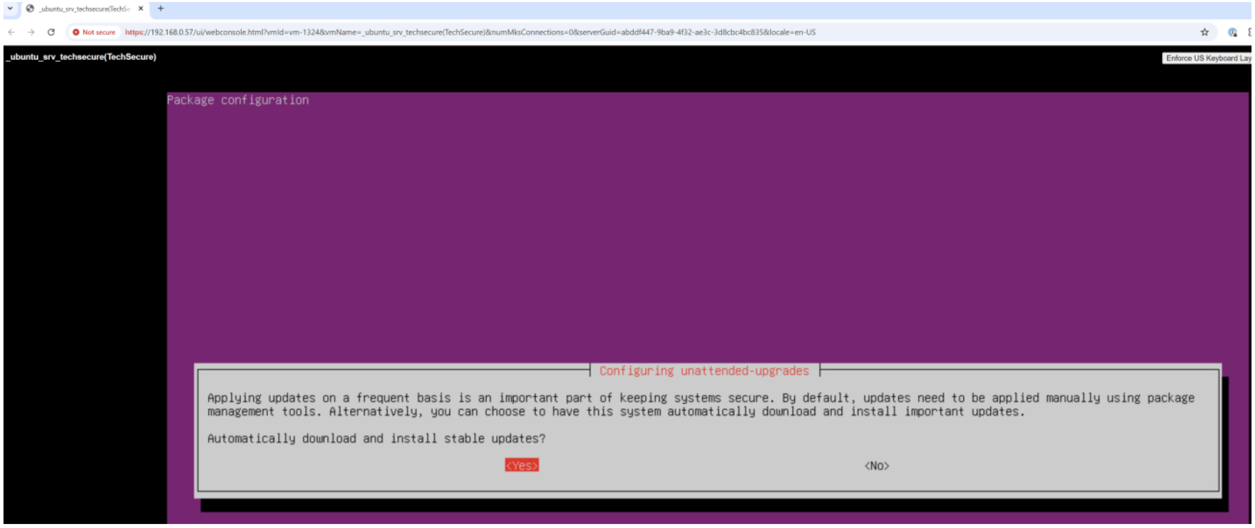
```
ts_admin@ubuntusrvtechsecure:~$ sudo ufw allow OpenSSH
[sudo] password for ts_admin:
Rules updated
Rules updated (v6)
ts_admin@ubuntusrvtechsecure:~$ sudo ufw enable
Firewall is active and enabled on system startup
ts_admin@ubuntusrvtechsecure:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
OpenSSH                    ALLOW       Anywhere
OpenSSH (v6)               ALLOW       Anywhere (v6)

ts_admin@ubuntusrvtechsecure:~$ _
```

19. Configuring UFW to Allow OpenSSH - Implemented Uncomplicated Firewall (UFW) rules to allow OpenSSH traffic, ensuring that only necessary services are exposed on the ubuntu_srv_techsecure system, which helps reduce the attack surface.

Automatic Security Updates:

Since the Linux server hosts secure web applications and development environments, keeping it updated with security patches is crucial. Automatic updates will help ensure that vulnerabilities are patched regularly, without manual intervention, aligning well with the hardening requirements.

Enabling **unattended-upgrades** is a practical way to automatically install security updates, minimizing potential attack vectors from unpatched software:

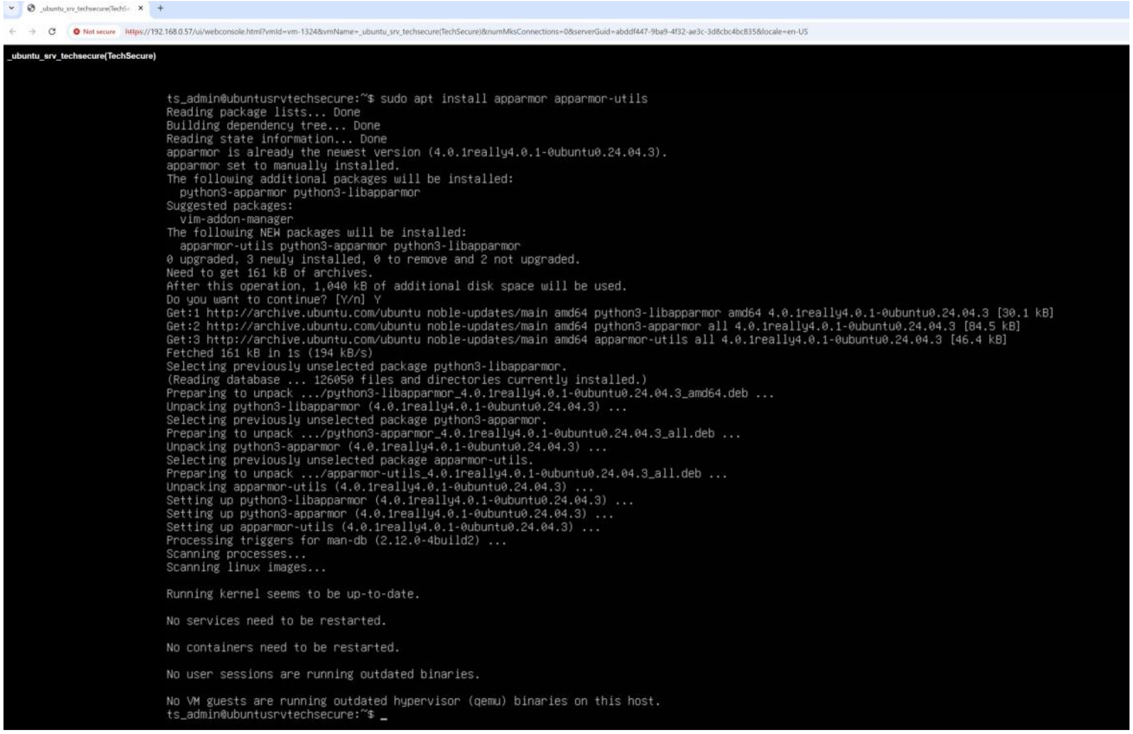

_ubuntu_srv_techsecure(TechSe
Not secure
https://192.168.0.57/ui/webconsole.html?vmId=vm-1324&vmName=_ubuntu_srv_techsecure(TechSecure)&numMksConnections=0&serverGuid=abddf447-9ba9-4f32-ae3c-3d8cbc4bc835&locale=en-US
_ubuntu_srv_techsecure(TechSecure)
Enforce US Keyboard Lay

```
Package configuration

┤ Configuring unattended-upgrades ├

Applying updates on a frequent basis is an important part of keeping systems secure. By default, updates need to be applied manually using package
management tools. Alternatively, you can choose to have this system automatically download and install important updates.

Automatically download and install stable updates?

                    <Yes>                                              <No>
```

20 Configuring Unattended Upgrades - Enabled unattended-upgrades on the ubuntu_srv_techsecure system to ensure that security updates are automatically installed, minimizing the risk posed by vulnerabilities in unpatched software.

AppArmor:

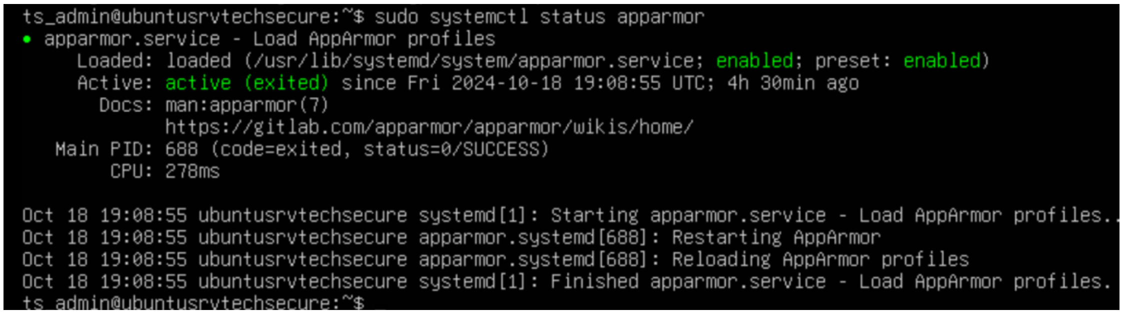
AppArmor helps enforce security policies at the application level, which is especially useful for isolating the web applications and tools running on the server. This aligns with the requirement to harden the system against threats by limiting the potential damage an exploited application can cause. Using AppArmor to define security profiles for the applications running on the server would add an additional layer of defence, particularly for web applications that may be exposed to the internet.



_ubuntu_srv_techsecure(TechS…
Not secure
https://192.168.0.57/ui/webconsole.html?vmId=vm-1324&vmName=_ubuntu_srv_techsecure(TechSecure)&numMksConnections=0&serverGuid=abddf447-9ba9-4f32-ae3c-3d8cbc4bc835&locale=en-US
_ubuntu_srv_techsecure(TechSecure)

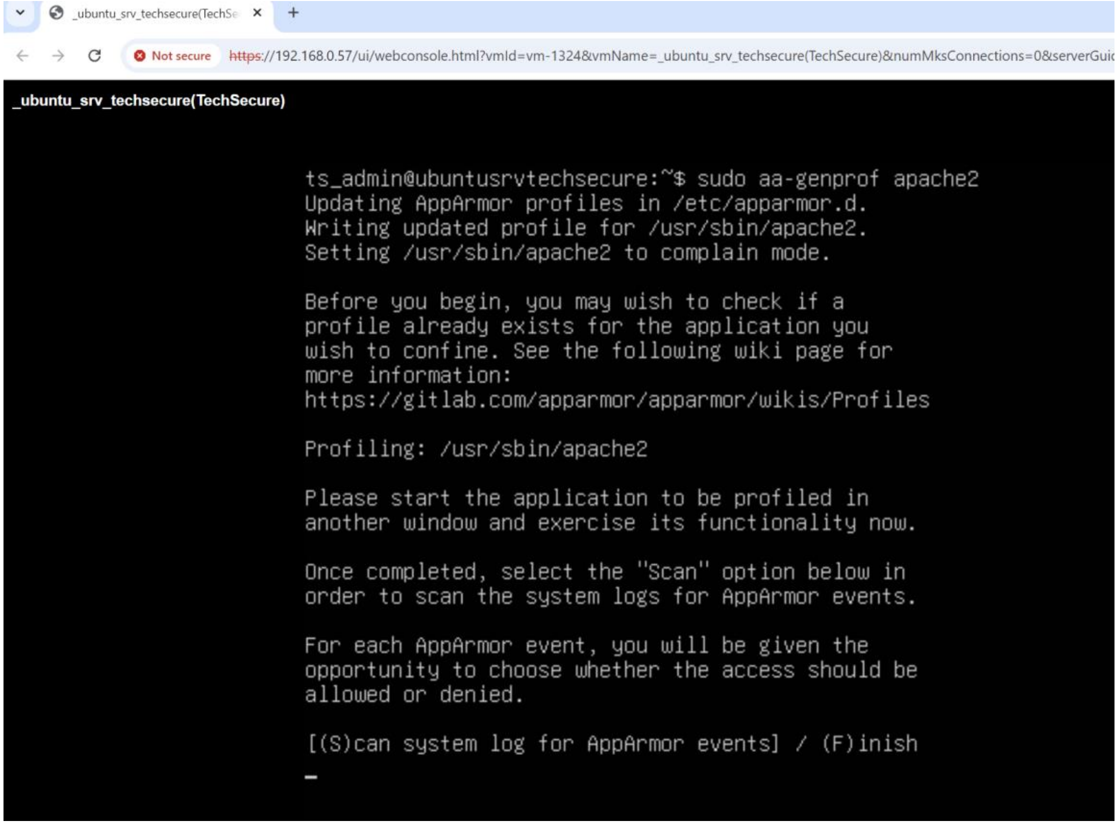
```
ts_admin@ubuntusrvtechsecure:~$ sudo apt install apparmor apparmor-utils
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
apparmor is already the newest version (4.0.1really4.0.1-0ubuntu0.24.04.3).
apparmor set to manually installed.
The following additional packages will be installed:
  python3-apparmor python3-libapparmor
Suggested packages:
  vim-addon-manager
The following NEW packages will be installed:
  apparmor-utils python3-apparmor python3-libapparmor
0 upgraded, 3 newly installed, 0 to remove and 2 not upgraded.
Need to get 161 kB of archives.
After this operation, 1,040 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 python3-libapparmor amd64 4.0.1really4.0.1-0ubuntu0.24.04.3 [30.1 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 python3-apparmor all 4.0.1really4.0.1-0ubuntu0.24.04.3 [84.5 kB]
Get:3 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 apparmor-utils all 4.0.1really4.0.1-0ubuntu0.24.04.3 [46.4 kB]
Fetched 161 kB in 1s (194 kB/s)
Selecting previously unselected package python3-libapparmor.
(Reading database ... 126050 files and directories currently installed.)
Preparing to unpack .../python3-libapparmor_4.0.1really4.0.1-0ubuntu0.24.04.3_amd64.deb ...
Unpacking python3-libapparmor (4.0.1really4.0.1-0ubuntu0.24.04.3) ...
Selecting previously unselected package python3-apparmor.
Preparing to unpack .../python3-apparmor_4.0.1really4.0.1-0ubuntu0.24.04.3_all.deb ...
Unpacking python3-apparmor (4.0.1really4.0.1-0ubuntu0.24.04.3) ...
Selecting previously unselected package apparmor-utils.
Preparing to unpack .../apparmor-utils_4.0.1really4.0.1-0ubuntu0.24.04.3_all.deb ...
Unpacking apparmor-utils (4.0.1really4.0.1-0ubuntu0.24.04.3) ...
Setting up python3-libapparmor (4.0.1really4.0.1-0ubuntu0.24.04.3) ...
Setting up python3-apparmor (4.0.1really4.0.1-0ubuntu0.24.04.3) ...
Setting up apparmor-utils (4.0.1really4.0.1-0ubuntu0.24.04.3) ...
Processing triggers for man-db (2.12.0-4build2) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ts_admin@ubuntusrvtechsecure:~$ _
```

21. Installing AppArmor - Installed AppArmor and related utilities on the `ubuntu_srv_techsecure` system to provide enhanced security by enforcing application-level policies and restricting program capabilities.



```
ts_admin@ubuntusrvtechsecure:~$ sudo systemctl status apparmor
● apparmor.service - Load AppArmor profiles
     Loaded: loaded (/usr/lib/systemd/system/apparmor.service; enabled; preset: enabled)
     Active: active (exited) since Fri 2024-10-18 19:08:55 UTC; 4h 30min ago
       Docs: man:apparmor(7)
             https://gitlab.com/apparmor/apparmor/wikis/home/
   Main PID: 688 (code=exited, status=0/SUCCESS)
        CPU: 278ms

Oct 18 19:08:55 ubuntusrvtechsecure systemd[1]: Starting apparmor.service - Load AppArmor profiles..
Oct 18 19:08:55 ubuntusrvtechsecure apparmor.systemd[688]: Restarting AppArmor
Oct 18 19:08:55 ubuntusrvtechsecure apparmor.systemd[688]: Reloading AppArmor profiles
Oct 18 19:08:55 ubuntusrvtechsecure systemd[1]: Finished apparmor.service - Load AppArmor profiles.
ts_admin@ubuntusrvtechsecure:~$
```

22. Verifying AppArmor Status - Verified that AppArmor service is active and running on the ubuntu_srv_techsecure system, ensuring that security profiles are properly loaded and enforced.


_ubuntu_srv_techsecure(TechSe
Not secure
https://192.168.0.57/ui/webconsole.html?vmId=vm-1324&vmName=_ubuntu_srv_techsecure(TechSecure)&numMksConnections=0&serverGuic
_ubuntu_srv_techsecure(TechSecure)

```
ts_admin@ubuntusrvtechsecure:~$ sudo aa-genprof apache2
Updating AppArmor profiles in /etc/apparmor.d.
Writing updated profile for /usr/sbin/apache2.
Setting /usr/sbin/apache2 to complain mode.

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/apache2

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
_
```

23. Generating AppArmor Profile for Apache2 - Used aa-genprof to create and update an AppArmor profile for Apache2 on the ubuntu_srv_techsecure system, setting the application to "complain" mode for easier profiling and adjustment of permissions.

Final Conclusion: The hardening policies implemented for both Windows and Linux systems serve as a foundation for improving system security. By enabling script scanning, real-time monitoring, and limiting root access, the systems are more resilient to various cyber threats. However, security is an ongoing process, and it is crucial to continuously monitor, audit, and update these settings as new vulnerabilities and attack vectors are discovered. Combining proactive hardening steps with vigilant monitoring ensures that both Windows and Linux environments are safeguarded against potential risks, providing a robust defense for organizational systems.

Moving forward, the plan includes deploying additional security tools, such as intrusion detection systems and advanced firewall configurations, to further harden the systems. Regular audits and updates will also be prioritized to ensure that emerging threats are addressed promptly. By incrementally enhancing system security, the organization can improve the hardening index and provide a more resilient defense against cyber threats.