LOVELY PROFESSIONAL UNIVERSITY

INT301

Ca3

Shaik Mohammed Nishad

11902388

kE058

Q) As a network administrator, briefly what techniques, tools, and methodologies would follow to perform testing on linux

a) Network devices security

b) Physical security

Introduction:-

Objectives

The objective of the report is to provide network administrators with an overview of the techniques, tools, and methodologies that can be used to test and enhance the security of network devices and physical environment on Linux systems. The report aims to help network administrators identify potential vulnerabilities and mitigate security threats through the use of various tools and techniques such as vulnerability scanning, network traffic analysis, access controls and authentication, regular updates and patches, security audits and risk assessments, access control systems, CCTV cameras, system hardening and configuration management, encryption, and regular security audits. By following the techniques, tools, and methodologies outlined in the report, network administrators can ensure that their Linux-based network devices and physical environment are secure and protected against potential security threats.

Description

As a network administrator, when performing testing on Kali Linux for network devices security and physical security, various techniques, tools, and methodologies can be utilized to assess the robustness and resilience of the network infrastructure against potential threats.

Scope

The scope of a project for a network administrator to perform testing on Kali Linux for network devices security and physical security typically involves conducting thorough assessments and evaluations to identify potential vulnerabilities, weaknesses, and risks in the network infrastructure. This may include the following techniques, tools, and methodologies:

a) Network Devices Security:

Vulnerability Scanning: Using tools like OpenVAS, Nikto, or Nessus to scan network devices for known vulnerabilities, misconfigurations, and weaknesses, and generating reports to prioritize and address the identified issues.

Penetration Testing: Employing tools like Metasploit or Nmap to simulate attacks and attempt to exploit vulnerabilities in network devices, mimicking real-world scenarios to identify potential entry points for unauthorized access.

Traffic Analysis: Analyzing network traffic using tools like Wireshark or tcpdump to detect any suspicious or malicious activity, such as network attacks, unauthorized access attempts, or data breaches, and investigating and mitigating any identified anomalies.

Configuration Auditing: Reviewing and auditing the configuration settings of network devices to ensure they adhere to security best practices, such as disabling unnecessary services, implementing proper authentication methods, and encrypting communications, and making necessary configuration changes.

b) Physical Security:

Physical Access Testing: Conducting tests to evaluate the effectiveness of physical security measures, such as attempting to gain unauthorized access to network devices physically, bypassing security controls, or tampering with equipment, and implementing necessary measures to address identified vulnerabilities.

Social Engineering Testing: Utilizing social engineering techniques to assess the vulnerabilities of physical security measures, such as attempting to impersonate employees, tailgating, or manipulating employees to gain unauthorized access, and implementing awareness and training programs to mitigate social engineering attacks.

Video Surveillance Analysis: Reviewing video surveillance footage to detect any security breaches or suspicious activities related to physical security, such as unauthorized access, tampering, or suspicious behavior, and taking necessary actions to address any identified security incidents.

Security Audits: Performing regular inspections and assessments of physical security measures, such as locks, alarms, access control systems, and CCTV cameras, to ensure they are functioning properly and providing adequate protection, and making necessary upgrades or improvements as needed.

Target system description

As a target system I am using my own kali linux virtual machine so

Analysis Report

a) <u>Network Devices Security</u>:

To ensure the security of network devices, several techniques, tools, and methodologies can be utilized, including:

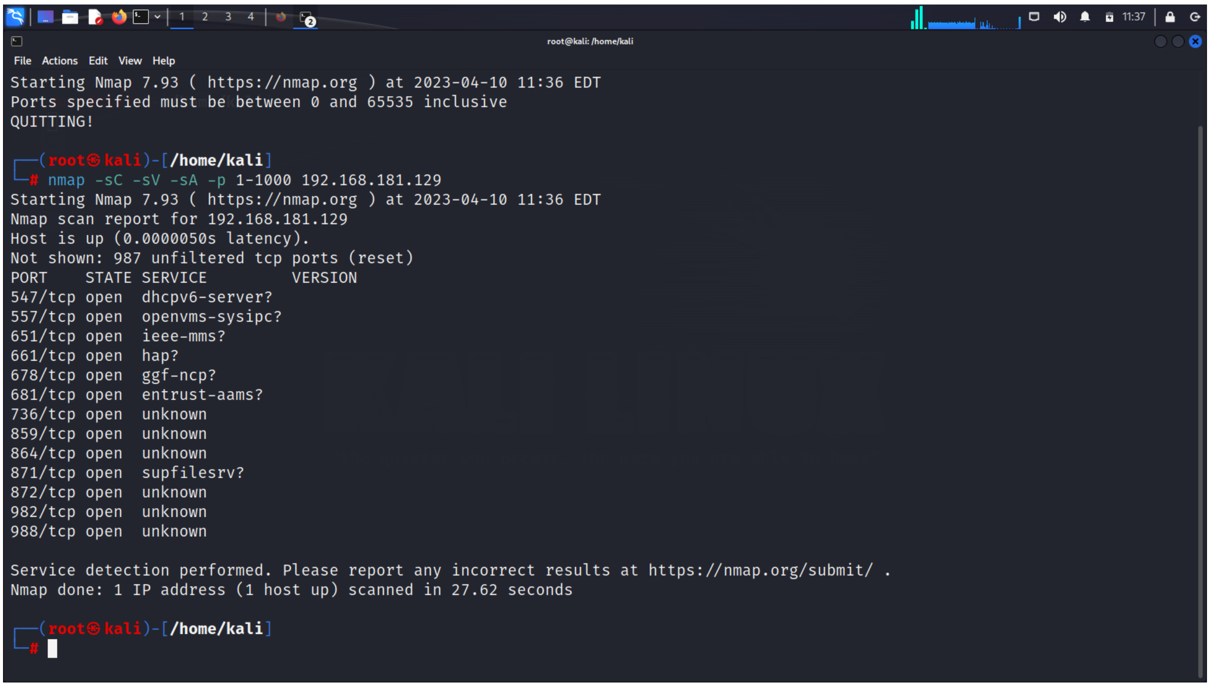
1. **<u>Vulnerability Scanning and Penetration Testing:</u>**

Vulnerability scanning and penetration testing are essential techniques to identify potential security vulnerabilities in network devices. Tools like Nmap and Metasploit can be used to perform these tests.

Example Code:

To perform a vulnerability scan using Nmap, the following command can be used:

nmap -sV -p 1-10000 <target IP address>



```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-10 11:36 EDT
Ports specified must be between 0 and 65535 inclusive
QUITTING!

┌──(root㉿kali)-[/home/kali]
└─# nmap -sC -sV -sA -p 1-1000 192.168.181.129
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-10 11:36 EDT
Nmap scan report for 192.168.181.129
Host is up (0.0000050s latency).
Not shown: 987 unfiltered tcp ports (reset)
PORT    STATE SERVICE         VERSION
547/tcp open  dhcpv6-server?
557/tcp open  openvms-sysipc?
651/tcp open  ieee-mms?
661/tcp open  hap?
678/tcp open  ggf-ncp?
681/tcp open  entrust-aams?
736/tcp open  unknown
859/tcp open  unknown
864/tcp open  unknown
871/tcp open  supfilesrv?
872/tcp open  unknown
982/tcp open  unknown
988/tcp open  unknown

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.62 seconds

┌──(root㉿kali)-[/home/kali]
└─# 
```

this command will scan the target IP address, identify open ports, and detect running services.

To perform a penetration test using Metasploit, the following command can be used:

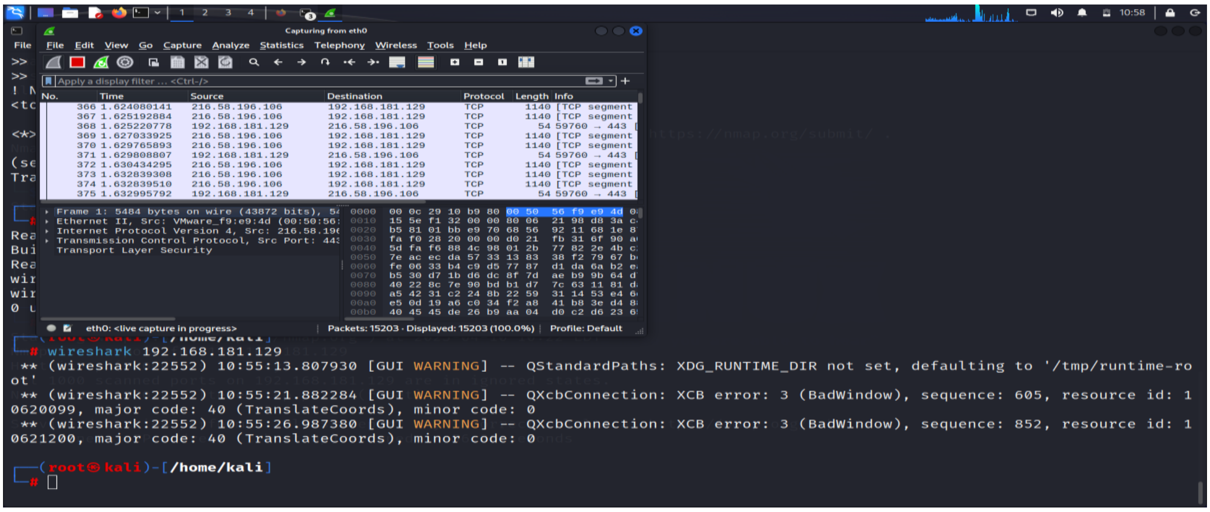
2. **Network Traffic Analysis**:
   Network traffic analysis tools like Wireshark can be used to monitor network traffic and detect any suspicious activity.

Example Code:

To capture network traffic using Wireshark, the following command can be used:

Wireshark

command will launch Wireshark and allow you to capture and analyze network traffic for any suspicious activity.



Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

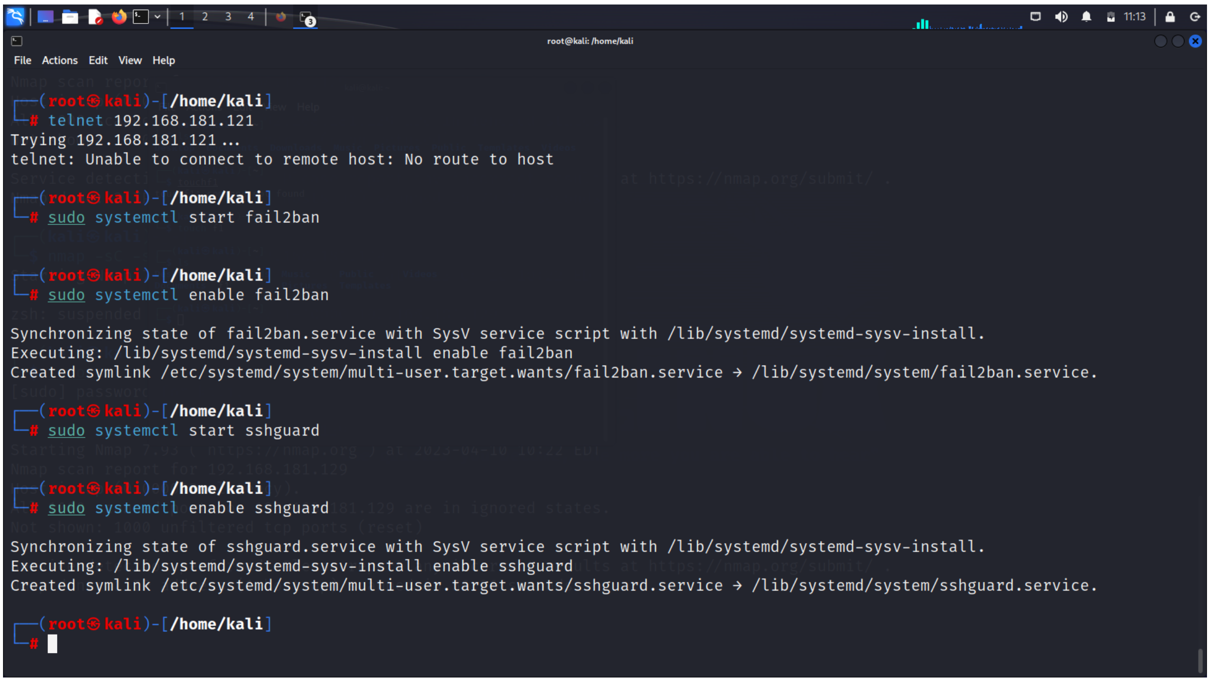
```
No.  Time          Source            Destination       Protocol  Length  Info
 366 1.624080141   216.58.196.106    192.168.181.129   TCP       1140 [TCP segment
 367 1.625192884   216.58.196.106    192.168.181.129   TCP       1140 [TCP segment
 368 1.625220778   192.168.181.129   216.58.196.106    TCP         54 59760 → 443 [
 369 1.627033925   216.58.196.106    192.168.181.129   TCP       1140 [TCP segment
 370 1.629765893   216.58.196.106    192.168.181.129   TCP       1140 [TCP segment
 371 1.629808807   192.168.181.129   216.58.196.106    TCP         54 59760 → 443 [
 372 1.630434295   216.58.196.106    192.168.181.129   TCP       1140 [TCP segment
 373 1.632839308   216.58.196.106    192.168.181.129   TCP       1140 [TCP segment
 374 1.632839510   216.58.196.106    192.168.181.129   TCP       1140 [TCP segment
 375 1.632995792   192.168.181.129   216.58.196.106    TCP         54 59760 → 443 [

▸ Frame 1: 5484 bytes on wire (43872 bits), 54
▸ Ethernet II, Src: VMware_f9:e9:4d (00:50:56:
▸ Internet Protocol Version 4, Src: 216.58.19€
▸ Transmission Control Protocol, Src Port: 443
  Transport Layer Security

0000  00 0c 29 10 b9 80 00 50  56 f9 e9 4d 0
0010  15 5e f1 32 00 00 80 06  21 98 d8 3a c
0020  b5 81 01 bb e9 70 68 56  92 11 68 1e 8
0030  fa f0 28 20 00 00 d0 21  fb 31 6f 90 a
0040  5d fa f6 88 4c 98 01 2b  77 82 2e 4b c
0050  7e ac ec da 57 33 13 83  38 f2 79 67 b
0060  fe 06 33 b4 c9 d5 77 87  d1 da 6a b2 e
0070  b5 30 d7 1b d6 dc 8f 7d  ae b9 9b 64 d
0080  40 22 8c 7e 90 bd b1 d7  7c 63 11 81 d
0090  a5 42 31 c2 24 8b 22 59  31 14 53 e4 6
00a0  e5 0d 19 a6 c0 34 f2 a8  41 b8 3e d4 8
00b0  40 45 45 de 26 b9 aa 04  d0 c2 d6 23 6

eth0: <live capture in progress>   Packets: 15203 · Displayed: 15203 (100.0%)   Profile: Default
```

```
└─# wireshark 192.168.181.129
 ** (wireshark:22552) 10:55:13.807930 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-ro
ot'
 ** (wireshark:22552) 10:55:21.882284 [GUI WARNING] -- QXcbConnection: XCB error: 3 (BadWindow), sequence: 605, resource id: 1
0620099, major code: 40 (TranslateCoords), minor code: 0
 ** (wireshark:22552) 10:55:26.987380 [GUI WARNING] -- QXcbConnection: XCB error: 3 (BadWindow), sequence: 852, resource id: 1
0621200, major code: 40 (TranslateCoords), minor code: 0

┌──(root㉿kali)-[/home/kali]
└─# 
```

3. **Access Controls and Authentication**:
Access controls and authentication mechanisms can be implemented to secure network devices. This includes using strong passwords, multi-factor authentication, and implementing role-based access controls.

Example Code:

To implement access controls and authentication mechanisms, the following commands can be used:



```
┌──(root㉿kali)-[/home/kali]
└─# telnet 192.168.181.121
Trying 192.168.181.121 ...
telnet: Unable to connect to remote host: No route to host

┌──(root㉿kali)-[/home/kali]
└─# sudo systemctl start fail2ban

┌──(root㉿kali)-[/home/kali]
└─# sudo systemctl enable fail2ban
Synchronizing state of fail2ban.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable fail2ban
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /lib/systemd/system/fail2ban.service.

┌──(root㉿kali)-[/home/kali]
└─# sudo systemctl start sshguard

┌──(root㉿kali)-[/home/kali]
└─# sudo systemctl enable sshguard
Synchronizing state of sshguard.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable sshguard
Created symlink /etc/systemd/system/multi-user.target.wants/sshguard.service → /lib/systemd/system/sshguard.service.

┌──(root㉿kali)-[/home/kali]
└─# █
```

1. Configure Fail2Ban: Fail2Ban is a log-parsing application that can automatically block IP addresses that show signs of malicious activity, such as repeated failed login attempts. After installation, you can configure Fail2Ban by editing its configuration file located at **/etc/fail2ban/jail.conf** or **/etc/fail2ban/jail.d/** directory. You can specify the services you want to protect, set parameters such as the ban time, and customize the action to be taken when an IP is banned (e.g., adding it to the firewall blacklist).

2. Start and enable Fail2Ban: After configuring Fail2Ban, you can start and enable it as a service so that it runs automatically on system boot. You can use the following commands:

```
sudo apt-get install fail2bansudo apt-get install sshguard
```

Configure Sshguard: sshguard is a similar tool to Fail2Ban that protects against brute-force attacks specifically targeting SSH (Secure Shell) service. After installation, you can configure sshguard by editing its configuration file located at /etc/sshguard/sshguard.conf. You can specify various parameters such as the ban time, the log file to monitor, and the action to be taken when an ip is banned.

Start and enable sshguard: After configuring sshguard, you can start and enable it as a service using the following commands:

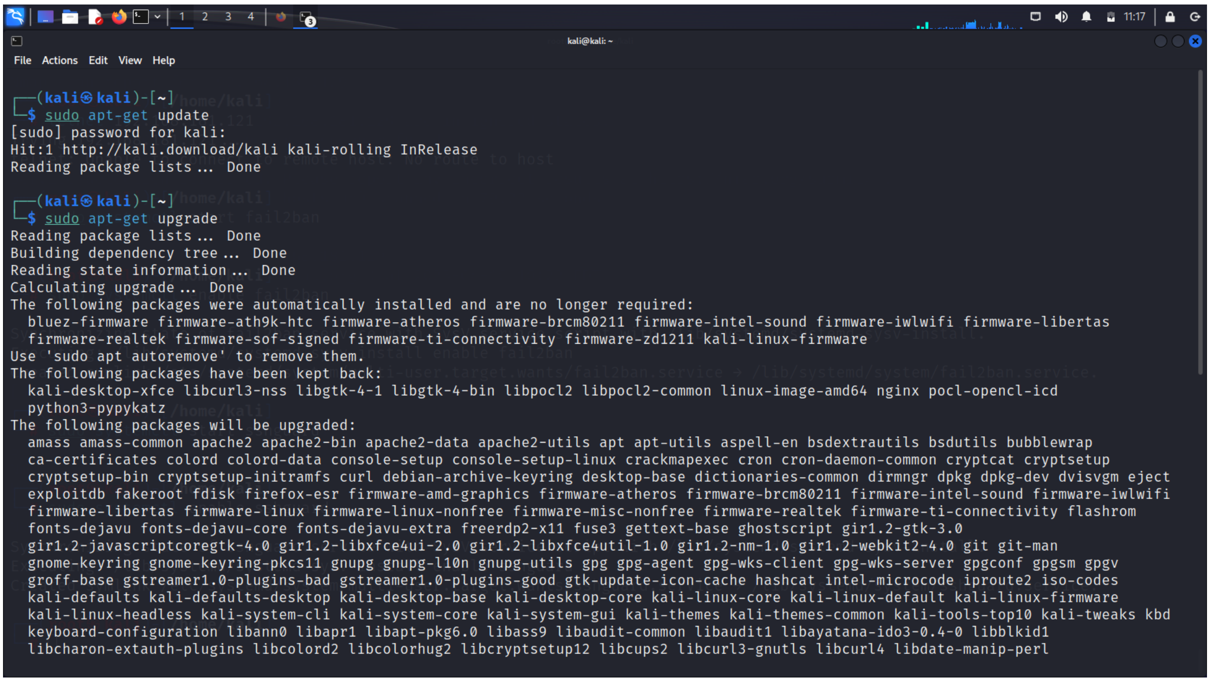
These commands will install fail2ban and sshguard, which are tools that can be used to implement access controls and authentication mechanisms.

4. **<u>Regular Updates and Patches</u>**:
   Regular updates and patches must be applied to network devices to address known vulnerabilities and security issues.

Example Code:

To update and patch network devices, the following command can be used:

```
sudo apt-get updatesudo apt-get upgrade
```



```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get update
[sudo] password for kali:
Hit:1 http://kali.download/kali kali-rolling InRelease
Reading package lists ... Done

┌──(kali㉿kali)-[~]
└─$ sudo apt-get upgrade
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
Calculating upgrade ... Done
The following packages were automatically installed and are no longer required:
  bluez-firmware firmware-ath9k-htc firmware-atheros firmware-brcm80211 firmware-intel-sound firmware-iwlwifi firmware-libertas
  firmware-realtek firmware-sof-signed firmware-ti-connectivity firmware-zd1211 kali-linux-firmware
Use 'sudo apt autoremove' to remove them.
The following packages have been kept back:
  kali-desktop-xfce libcurl3-nss libgtk-4-1 libgtk-4-bin libpocl2 libpocl2-common linux-image-amd64 nginx pocl-opencl-icd
  python3-pypykatz
The following packages will be upgraded:
  amass amass-common apache2 apache2-bin apache2-data apache2-utils apt apt-utils aspell-en bsdextrautils bsdutils bubblewrap
  ca-certificates colord colord-data console-setup console-setup-linux crackmapexec cron cron-daemon-common cryptcat cryptsetup
  cryptsetup-bin cryptsetup-initramfs curl debian-archive-keyring desktop-base dictionaries-common dirmngr dpkg dpkg-dev dvisvgm eject
  exploitdb fakeroot fdisk firefox-esr firmware-amd-graphics firmware-atheros firmware-brcm80211 firmware-intel-sound firmware-iwlwifi
  firmware-libertas firmware-linux firmware-linux-nonfree firmware-misc-nonfree firmware-realtek firmware-ti-connectivity flashrom
  fonts-dejavu fonts-dejavu-core fonts-dejavu-extra freerdp2-x11 fuse3 gettext-base ghostscript gir1.2-gtk-3.0
  gir1.2-javascriptcoregtk-4.0 gir1.2-libxfce4ui-2.0 gir1.2-libxfce4util-1.0 gir1.2-nm-1.0 gir1.2-webkit2-4.0 git git-man
  gnome-keyring gnome-keyring-pkcs11 gnupg gnupg-l10n gnupg-utils gpg gpg-agent gpg-wks-client gpg-wks-server gpgconf gpgsm gpgv
  groff-base gstreamer1.0-plugins-bad gstreamer1.0-plugins-good gtk-update-icon-cache hashcat intel-microcode iproute2 iso-codes
  kali-defaults kali-defaults-desktop kali-desktop-base kali-desktop-core kali-linux-core kali-linux-default kali-linux-firmware
  kali-linux-headless kali-system-cli kali-system-core kali-system-gui kali-themes kali-themes-common kali-tools-top10 kali-tweaks kbd
  keyboard-configuration libann0 libapr1 libapt-pkg6.0 libass9 libaudit-common libaudit1 libayatana-ido3-0.4-0 libblkid1
  libcharon-extauth-plugins libcolord2 libcolorhug2 libcryptsetup12 libcups2 libcurl3-gnutls libcurl4 libdate-manip-perl
```

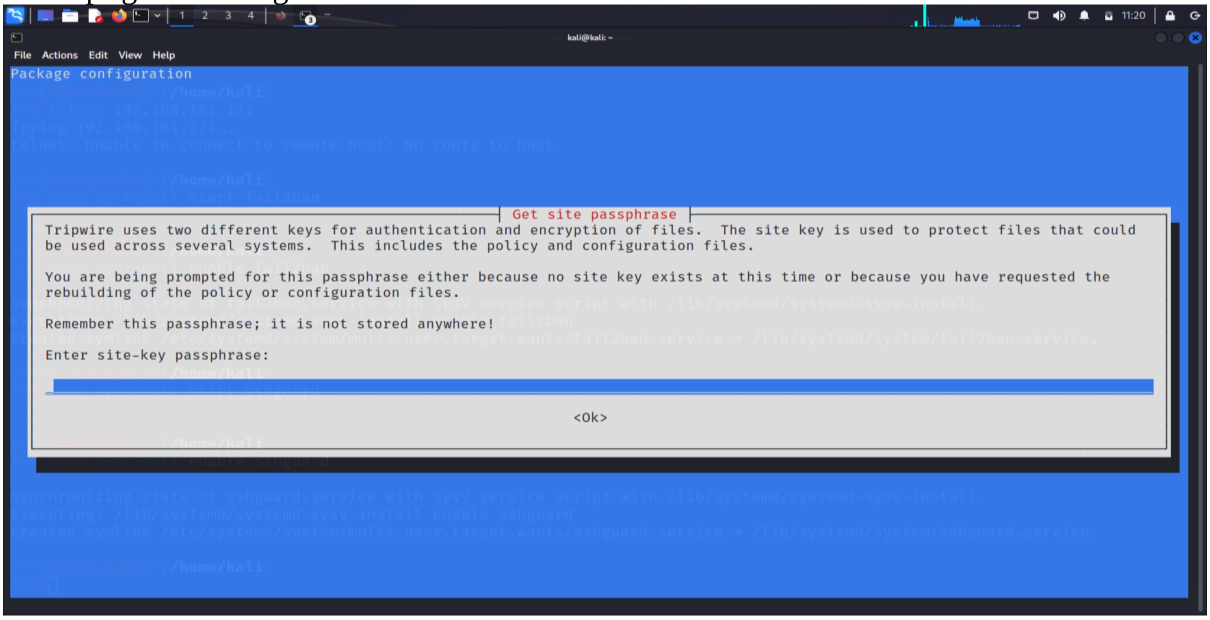
These commands will update and upgrade the software and firmware of network devices to ensure that they are secure.

5. **Security Audits and Risk Assessments**:
   Regular security audits and risk assessments must be conducted to identify and mitigate potential security threats.

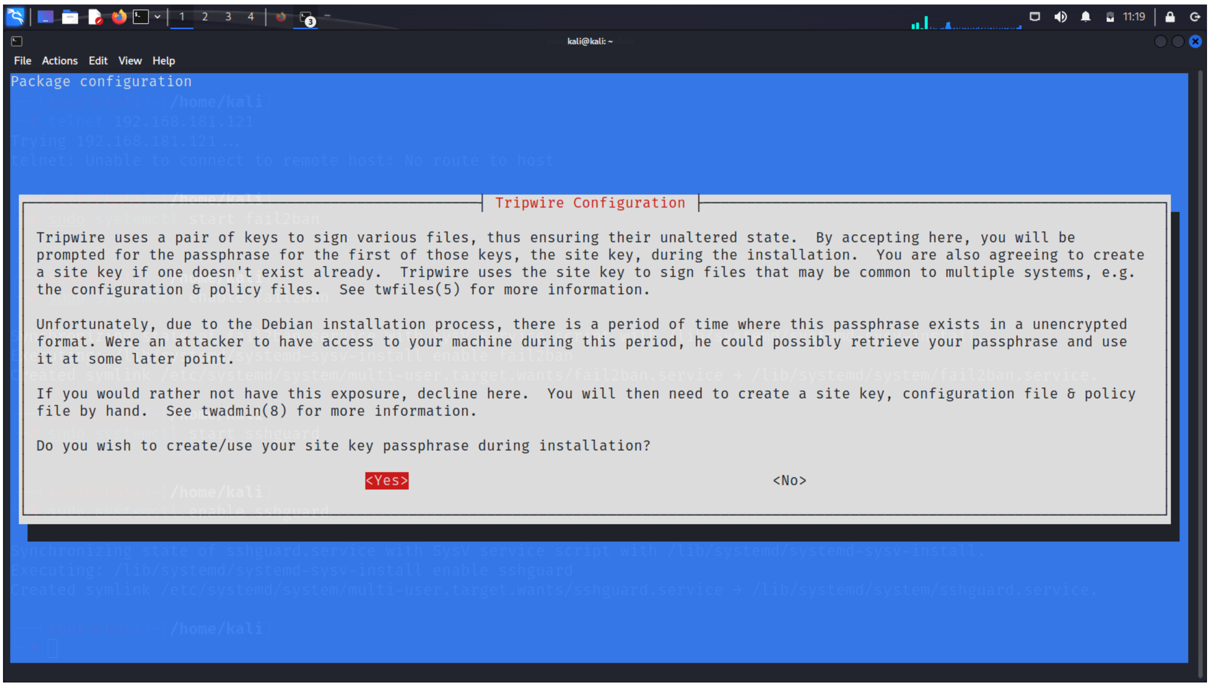
Example Code:

To conduct a security audit, the following command can be used:

sudo apt-get install tiger



```
Package configuration

Get site passphrase

Tripwire uses two different keys for authentication and encryption of files.  The site key is used to protect files that could
be used across several systems.  This includes the policy and configuration files.

You are being prompted for this passphrase either because no site key exists at this time or because you have requested the
rebuilding of the policy or configuration files.

Remember this passphrase; it is not stored anywhere!

Enter site-key passphrase:
```



```
Package configuration

Tripwire Configuration

Tripwire uses a pair of keys to sign various files, thus ensuring their unaltered state.  By accepting here, you will be
prompted for the passphrase for the first of those keys, the site key, during the installation.  You are also agreeing to create
a site key if one doesn't exist already.  Tripwire uses the site key to sign files that may be common to multiple systems, e.g.
the configuration & policy files.  See twfiles(5) for more information.

Unfortunately, due to the Debian installation process, there is a period of time where this passphrase exists in a unencrypted
format. Were an attacker to have access to your machine during this period, he could possibly retrieve your passphrase and use
it at some later point.

If you would rather not have this exposure, decline here.  You will then need to create a site key, configuration file & policy
file by hand.  See twadmin(8) for more information.

Do you wish to create/use your site key passphrase during installation?
```

is command will install tiger, a tool that can be used to perform security audits and identify potential security threats.

b) Physical Security:

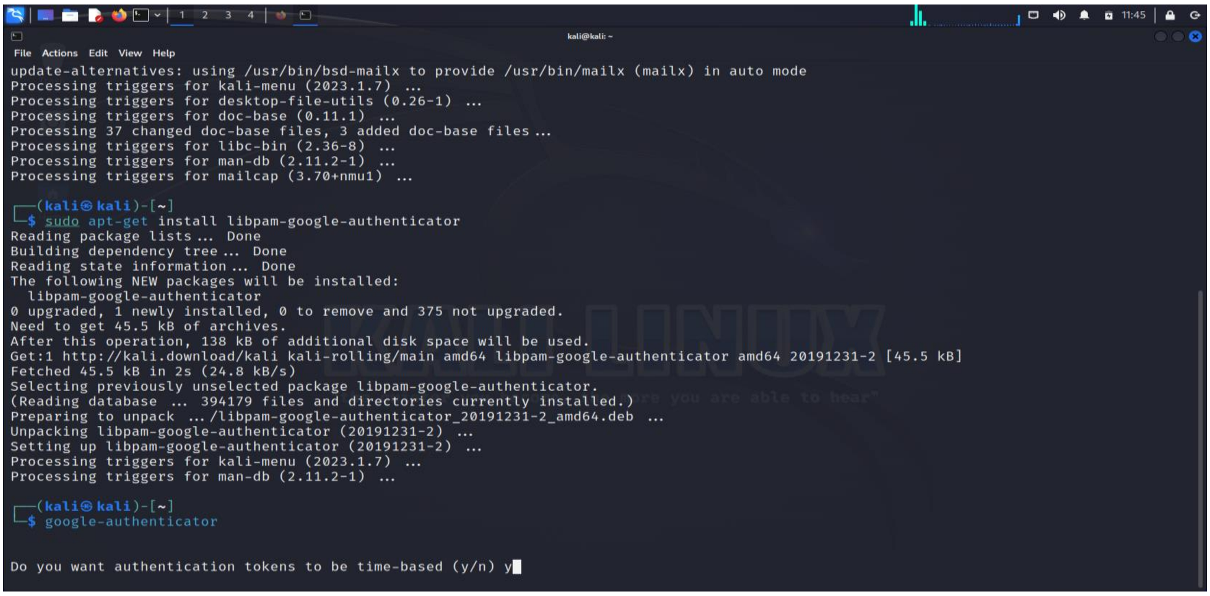
Physical security is equally important as network devices security. To ensure the physical security of network devices, several techniques, tools, and methodologies can be utilized, including:

1. Access Control Systems:
   Access control systems can be implemented to restrict physical access to network devices.

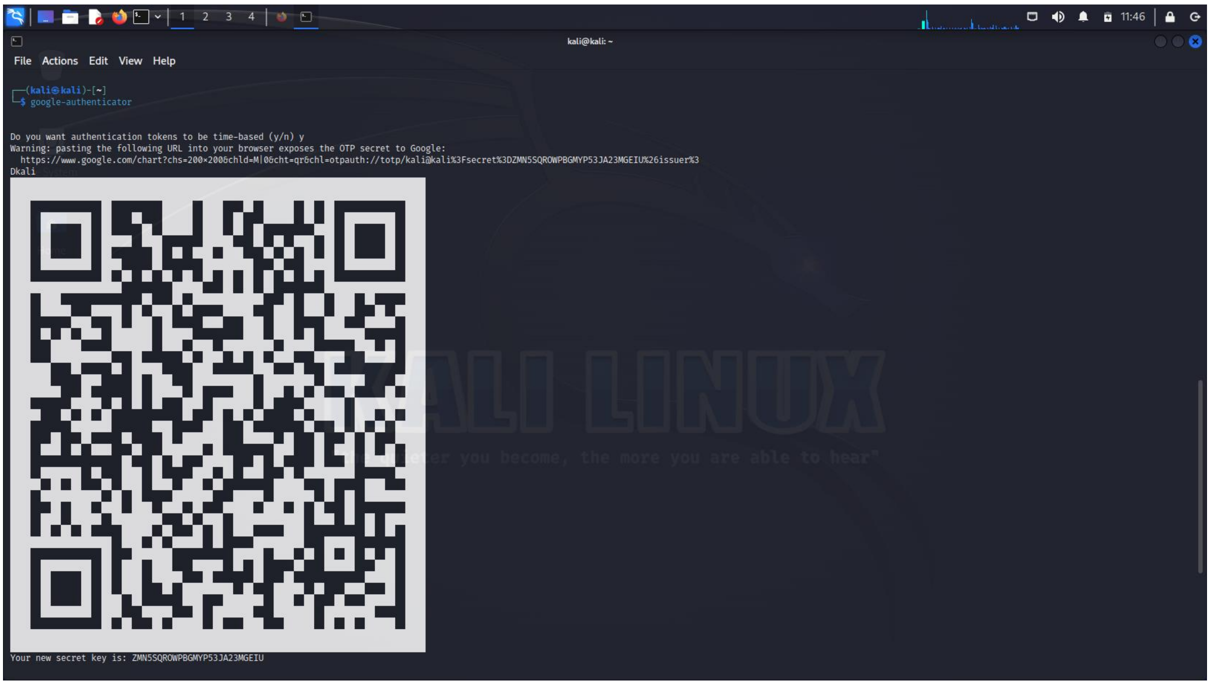
Example Code:

To implement an access control system, the following command can be used:

sudo apt-get install libpam-google-authenticator



```
update-alternatives: using /usr/bin/bsd-mailx to provide /usr/bin/mailx (mailx) in auto mode
Processing triggers for kali-menu (2023.1.7) ...
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for doc-base (0.11.1) ...
Processing 37 changed doc-base files, 3 added doc-base files ...
Processing triggers for libc-bin (2.36-8) ...
Processing triggers for man-db (2.11.2-1) ...
Processing triggers for mailcap (3.70+nmu1) ...

┌──(kali㉿kali)-[~]
└─$ sudo apt-get install libpam-google-authenticator
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  libpam-google-authenticator
0 upgraded, 1 newly installed, 0 to remove and 375 not upgraded.
Need to get 45.5 kB of archives.
After this operation, 138 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 libpam-google-authenticator amd64 20191231-2 [45.5 kB]
Fetched 45.5 kB in 2s (24.8 kB/s)
Selecting previously unselected package libpam-google-authenticator.
(Reading database ... 394179 files and directories currently installed.)
Preparing to unpack .../libpam-google-authenticator_20191231-2_amd64.deb ...
Unpacking libpam-google-authenticator (20191231-2) ...
Setting up libpam-google-authenticator (20191231-2) ...
Processing triggers for kali-menu (2023.1.7) ...
Processing triggers for man-db (2.11.2-1) ...

┌──(kali㉿kali)-[~]
└─$ google-authenticator


Do you want authentication tokens to be time-based (y/n) y
```



```
┌──(kali㉿kali)-[~]
└─$ google-authenticator


Do you want authentication tokens to be time-based (y/n) y
Warning: pasting the following URL into your browser exposes the OTP secret to Google:
  https://www.google.com/chart?chs=200x200&chld=M|0&cht=qr&chl=otpauth://totp/kali@kali%3Fsecret%3DZMN5SQROWPBGMYP53JA23MGEIU%26issuer%3
Dkali
```

```
Your new secret key is: ZMN5SQROWPBGMYP53JA23MGEIU
```

sudo nano /etc/pam.d/sshd

auth required pam_google_authenticator.so
sudo service ssh restart

This command will install the Google Authenticator PAM module, which can be used to implement multi-factor authentication for physical access to network devices.

2. CCTV cameras:
   CCTV cameras can be used to monitor physical access to network devices.

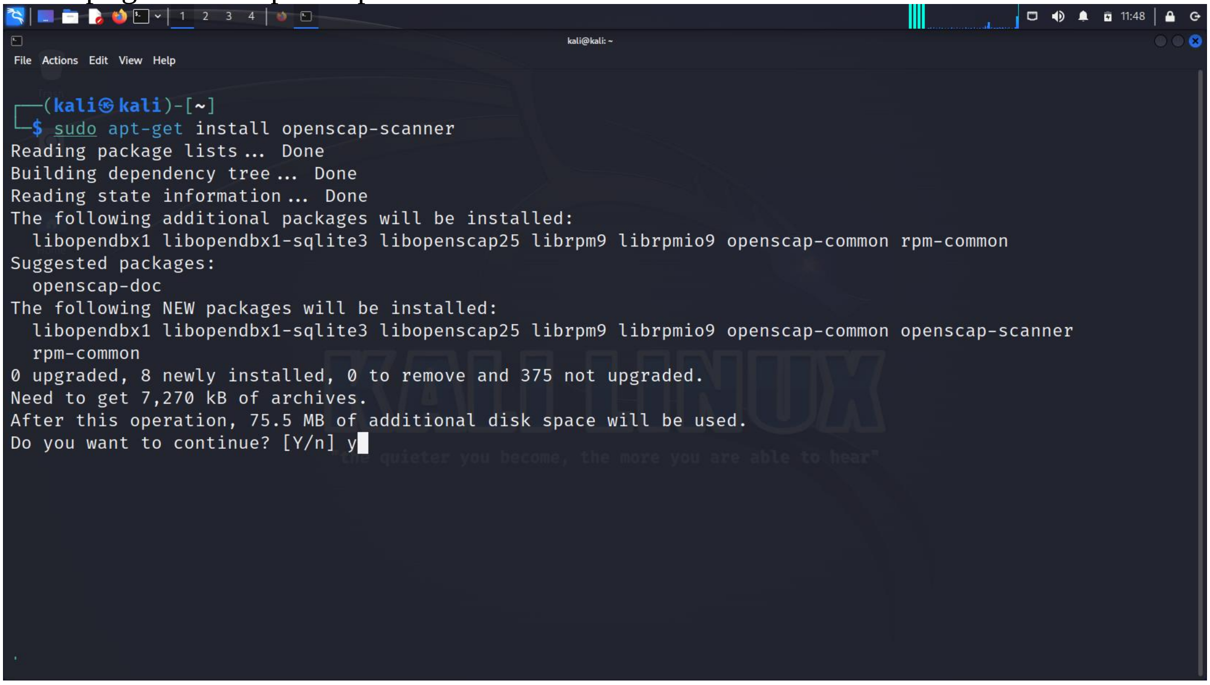
   We can use cctv as physical security so it can help us to so it can help the mediator

3. System Hardening and Configuration Management:
   System hardening and configuration management tools like OpenSCAP and Lynis can be used to ensure that network devices are properly configured and secure.

Example Code:

To perform system hardening and configuration management using OpenSCAP, the following command can be used:

sudo apt-get install openscap-scanner



```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install openscap-scanner
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libopendbx1 libopendbx1-sqlite3 libopenscap25 librpm9 librpmio9 openscap-common rpm-common
Suggested packages:
  openscap-doc
The following NEW packages will be installed:
  libopendbx1 libopendbx1-sqlite3 libopenscap25 librpm9 librpmio9 openscap-common openscap-scanner
  rpm-common
0 upgraded, 8 newly installed, 0 to remove and 375 not upgraded.
Need to get 7,270 kB of archives.
After this operation, 75.5 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

command on a Linux system, you can use it to perform security compliance scanning and assessment of the system against predefined security policies. OpenSCAP (Security Content Automation Protocol) is a standard for automating the assessment, measurement, and enforcement of security baselines on systems.

oscap scanner <path/to/security_policy.xml>

Review the generated report to identify any security issues that need to be addressed on the system.

Take appropriate actions to remediate the identified security issues. This may involve modifying system configurations, applying patches or updates, or implementing other security measures as needed.
Optionally, you can schedule periodic scans using OpenSCAP Scanner to continuously monitor the system's compliance with the defined security policy and take corrective actions as needed.

This command will install the OpenSCAP scanner, which can be used to perform system hardening and configuration management on network devices.

4. Encryption:
   Encryption mechanisms must be implemented to protect sensitive data stored on network devices.

Example Code:

To implement encryption, the following command can be used:

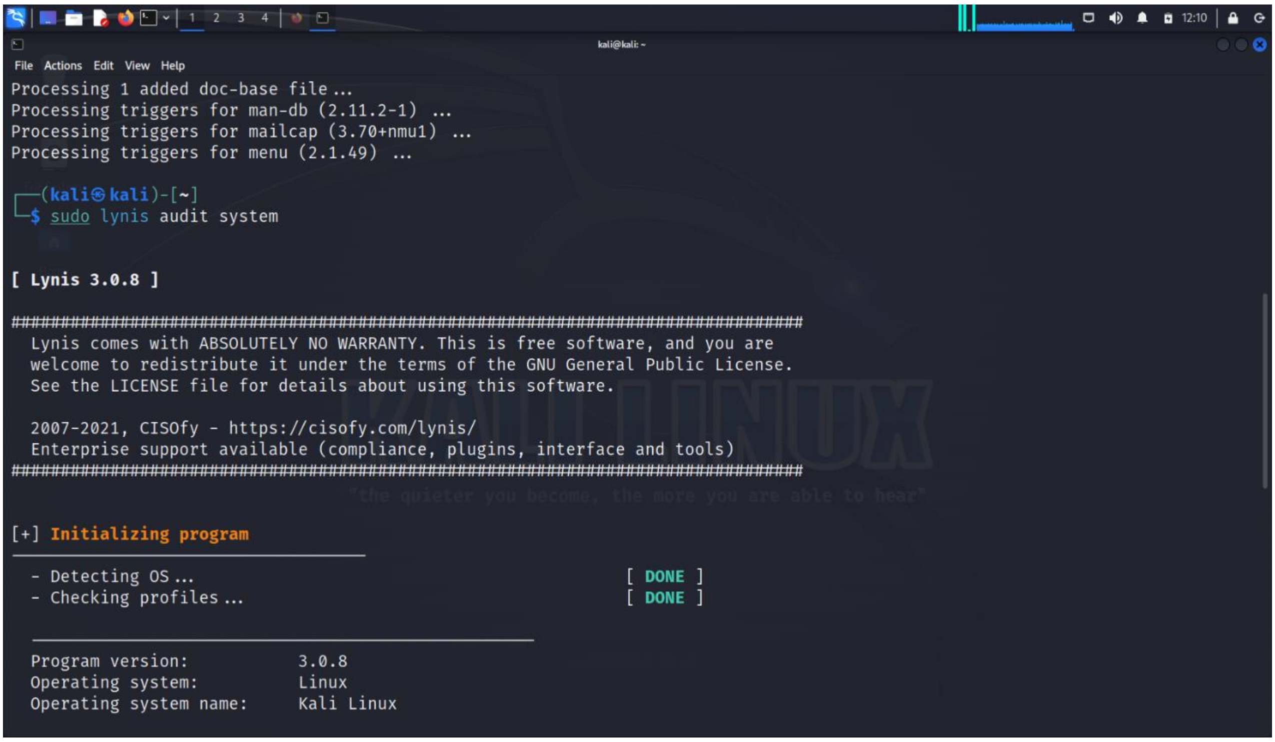
sudo apt-get install truecrypt
hat TrueCrypt is a deprecated encryption software and is no longer actively maintained or recommended for use. It is recommended to use alternative encryption tools that are actively maintained and have undergone security audits.

This command will install TrueCrypt, a tool that can be used to encrypt data stored on network devices.

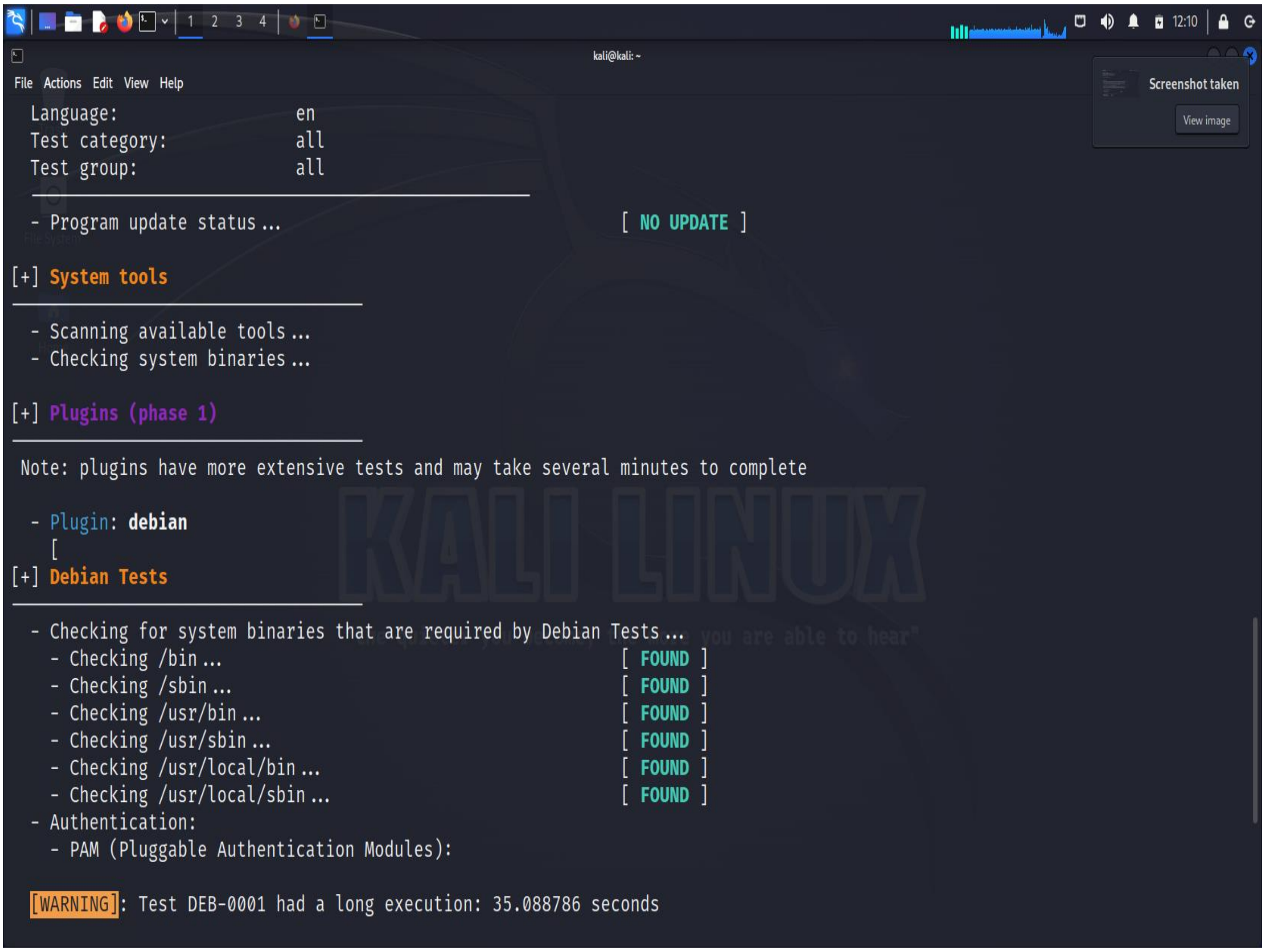
5. Regular Security Audits:
   Regular security audits must be conducted to ensure that physical security measures are effective in mitigating threats.

Configuration assessment with lynis : use lynis to assess the configuration settings of linux systems .for example

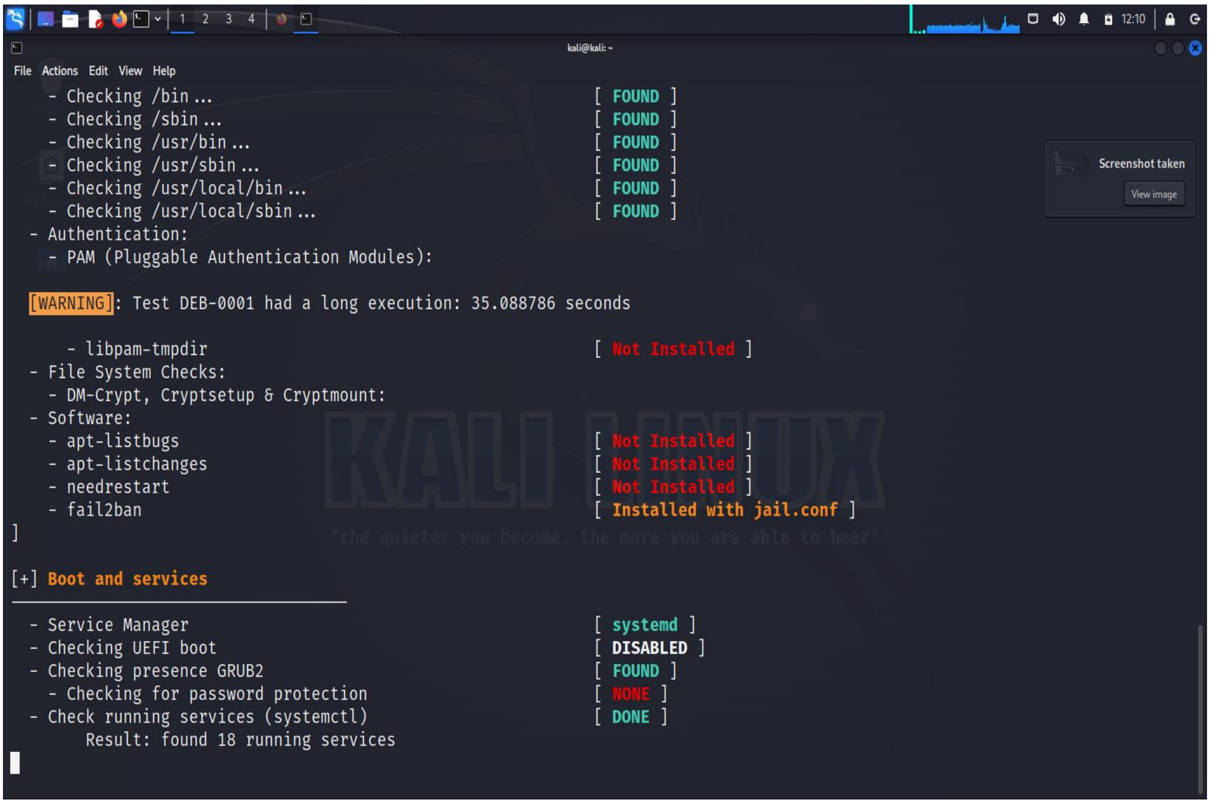
This command installs lynis and performs a system audit providing a report with finding and recommendations for improving security settings



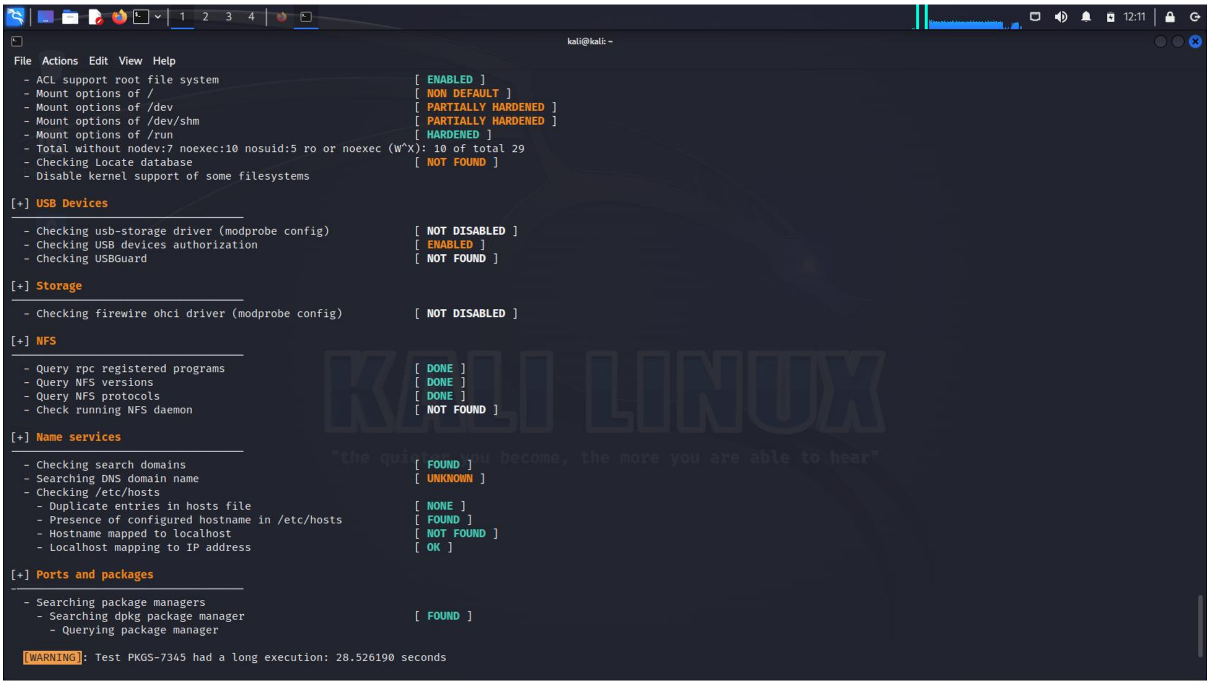
```
Processing 1 added doc-base file ...
Processing triggers for man-db (2.11.2-1) ...
Processing triggers for mailcap (3.70+nmu1) ...
Processing triggers for menu (2.1.49) ...

┌──(kali㉿kali)-[~]
└─$ sudo lynis audit system

[ Lynis 3.0.8 ]

################################################################################
  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 ]
  - Checking profiles ...                                     [ DONE ]

  ───────────────────────────────────────────────────
  Program version:           3.0.8
  Operating system:          Linux
  Operating system name:     Kali Linux
```



```
  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 /sbin ...                               [ FOUND ]
    - Checking /usr/bin ...                            [ FOUND ]
    - Checking /usr/sbin ...                           [ FOUND ]
    - Checking /usr/local/bin ...                      [ FOUND ]
    - Checking /usr/local/sbin ...                     [ FOUND ]
  - Authentication:
    - PAM (Pluggable Authentication Modules):

  [WARNING]: Test DEB-0001 had a long execution: 35.088786 seconds
```



```
    - Checking /bin ...                                [ FOUND ]
    - Checking /sbin ...                               [ FOUND ]
    - Checking /usr/bin ...                            [ FOUND ]
    - Checking /usr/sbin ...                           [ FOUND ]
    - Checking /usr/local/bin ...                      [ FOUND ]
    - Checking /usr/local/sbin ...                     [ FOUND ]
  - Authentication:
    - PAM (Pluggable Authentication Modules):

  [WARNING]: Test DEB-0001 had a long execution: 35.088786 seconds

      - libpam-tmpdir                                  [ Not Installed ]
  - File System Checks:
    - DM-Crypt, Cryptsetup & Cryptmount:
  - Software:
    - apt-listbugs                                     [ Not Installed ]
    - apt-listchanges                                  [ Not Installed ]
    - needrestart                                      [ Not Installed ]
    - fail2ban                                         [ Installed with jail.conf ]
]

[+] Boot and services
────────────────────────────
  - Service Manager                                    [ systemd ]
  - Checking UEFI boot                                 [ DISABLED ]
  - Checking presence GRUB2                            [ FOUND ]
    - Checking for password protection                 [ NONE ]
  - Check running services (systemctl)                 [ DONE ]
        Result: found 18 running services
```



```
  - ACL support root file system                              [ ENABLED ]
  - Mount options of /                                        [ NON DEFAULT ]
  - Mount options of /dev                                     [ PARTIALLY HARDENED ]
  - Mount options of /dev/shm                                 [ PARTIALLY HARDENED ]
  - Mount options of /run                                     [ HARDENED ]
  - Total without nodev:7 noexec:10 nosuid:5 ro or noexec (W^X): 10 of total 29
  - Checking Locate database                                  [ NOT FOUND ]
  - Disable kernel support of some filesystems

[+] 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)           [ NOT DISABLED ]

[+] NFS
------------------------------------
  - Query rpc registered programs                             [ DONE ]
  - Query NFS versions                                        [ DONE ]
  - Query NFS protocols                                       [ DONE ]
  - Check running NFS daemon                                  [ NOT FOUND ]

[+] Name services
------------------------------------
  - Checking search domains                                   [ FOUND ]
  - Searching DNS domain name                                 [ UNKNOWN ]
  - Checking /etc/hosts
    - Duplicate entries in hosts file                         [ NONE ]
    - Presence of configured hostname in /etc/hosts           [ 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

  [WARNING]: Test PKGS-7345 had a long execution: 28.526190 seconds
```

Reference

https://youtu.be/ifbwTt3_oCg

https://youtu.be/b-k4pgyU1kg

https://www.linuxtopia.org/online_books/linux_administrators_security_guide/13_Linux_Network_Security.html

https://www.secur/physical-security-for-linux-systems/