NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE

INFORMATION SECURITY LAB

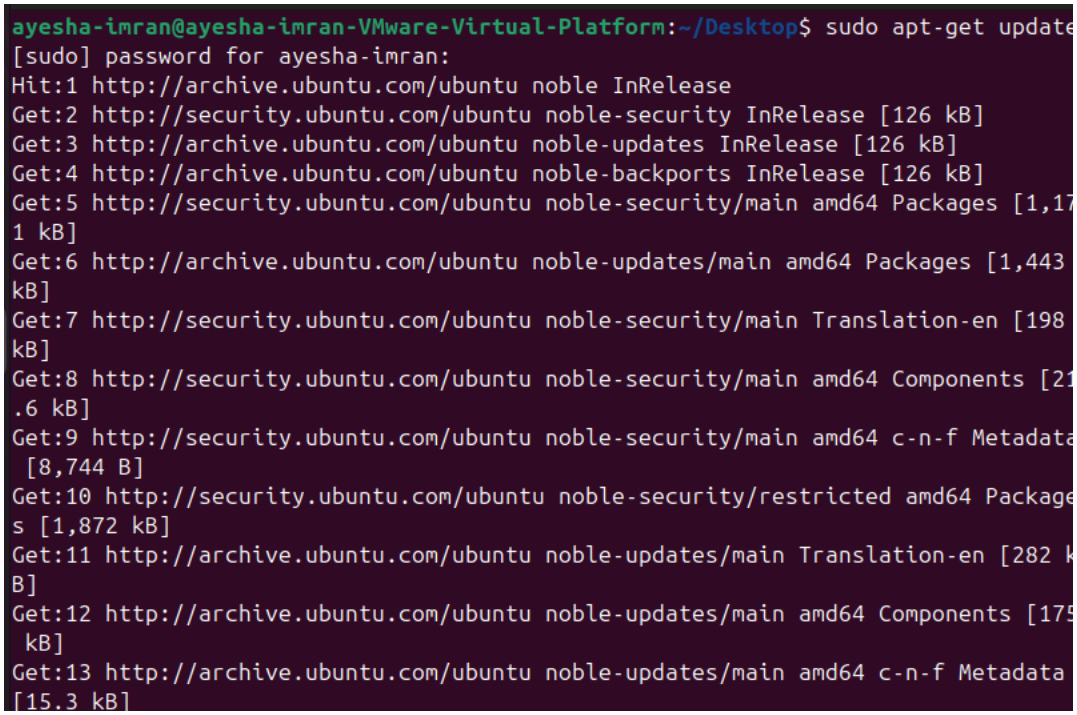
Name	Ayesha Imran
Class	CS-A
Lab	02
Course	Information Security
Date	29-September-25
Submitted To	Lec. Attiya Ashraf

IN LAB TASKS

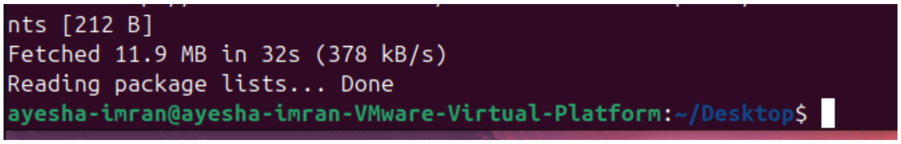
Experiment Steps

1. Update packages

o Update the package list using command: sudo apt update



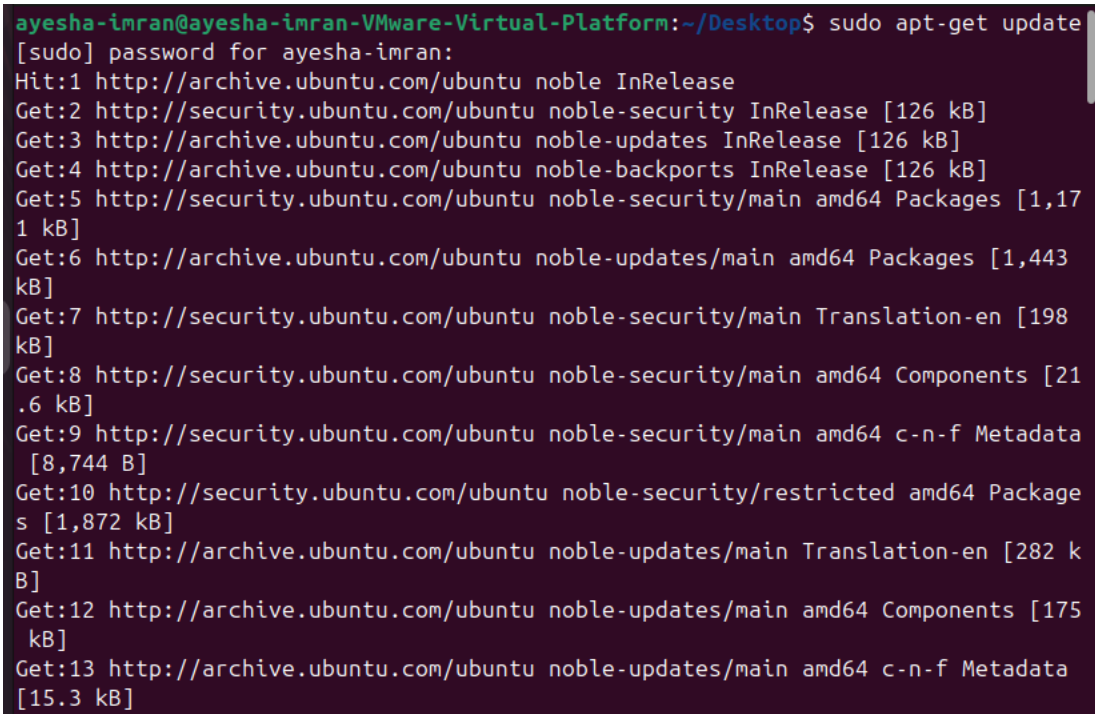
```
ayesha-imran@ayesha-imran-VMware-Virtual-Platform:~/Desktop$ sudo apt-get update
[sudo] password for ayesha-imran:
Hit:1 http://archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:3 http://archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:4 http://archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:5 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [1,17
1 kB]
Get:6 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [1,443
kB]
Get:7 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [198
kB]
Get:8 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [21
.6 kB]
Get:9 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata
 [8,744 B]
Get:10 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Package
s [1,872 kB]
Get:11 http://archive.ubuntu.com/ubuntu noble-updates/main Translation-en [282 k
B]
Get:12 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [175
 kB]
Get:13 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata
[15.3 kB]
```



```
nts [212 B]
Fetched 11.9 MB in 32s (378 kB/s)
Reading package lists... Done
ayesha-imran@ayesha-imran-VMware-Virtual-Platform:~/Desktop$
```

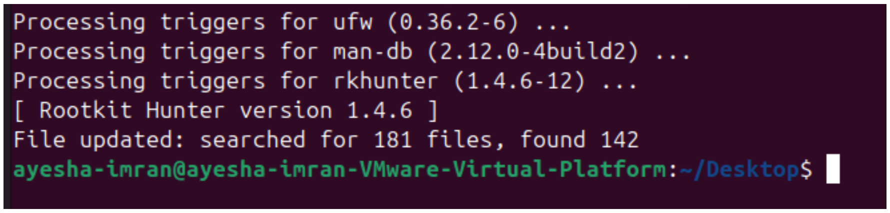
2. Install Rootkit Hunter

o Install rkhunter using the command below: sudo apt install rkhunter



```
ayesha-imran@ayesha-imran-VMware-Virtual-Platform:~/Desktop$ sudo apt-get update
[sudo] password for ayesha-imran:
Hit:1 http://archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:3 http://archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:4 http://archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:5 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [1,17
1 kB]
Get:6 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [1,443
kB]
Get:7 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [198
kB]
Get:8 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [21
.6 kB]
Get:9 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata
 [8,744 B]
Get:10 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Package
s [1,872 kB]
Get:11 http://archive.ubuntu.com/ubuntu noble-updates/main Translation-en [282 k
B]
Get:12 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [175
 kB]
Get:13 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata
[15.3 kB]
```

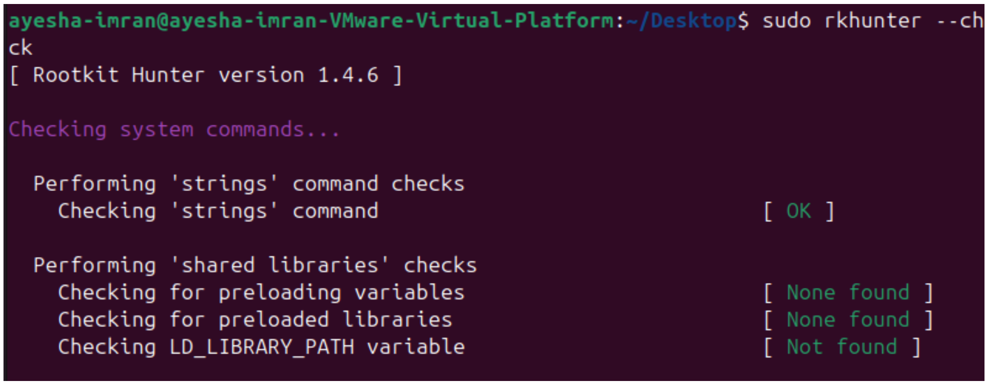
3. Postfix Configuration:



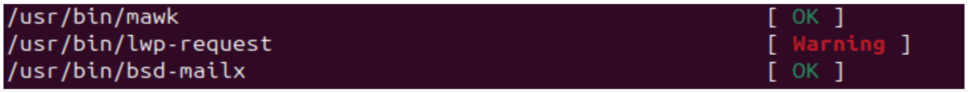
```
Processing triggers for ufw (0.36.2-6) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for rkhunter (1.4.6-12) ...
[ Rootkit Hunter version 1.4.6 ]
File updated: searched for 181 files, found 142
ayesha-imran@ayesha-imran-VMware-Virtual-Platform:~/Desktop$
```

5. Run a Rootkit Scan

o After updating, run a full system scan using: sudo rkhunter –check



```
ayesha-imran@ayesha-imran-VMware-Virtual-Platform:~/Desktop$ sudo rkhunter --ch
ck
[ 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 ]
```

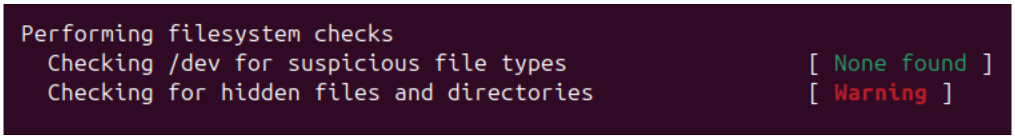


```
/usr/bin/mawk                                              [ OK ]
/usr/bin/lwp-request                                       [ Warning ]
/usr/bin/bsd-mailx                                         [ OK ]
```

Warning Explaination:

- `/usr/bin/mawk` → OK, nothing suspicious.
- `/usr/bin/lwp-request` **[Warning]**
  - This is part of the **libwww-perl** package, a normal Perl library tool for making HTTP requests.
  - RKHunter flags it because some malware uses it for downloading malicious files.
  - If you installed it yourself (e.g., as part of a web tool or script), it's probably safe.
- `/usr/bin/bsd-mailx` → OK, legitimate mail utility.

Meaning: Most likely a **false positive**. You can verify by checking its package source:

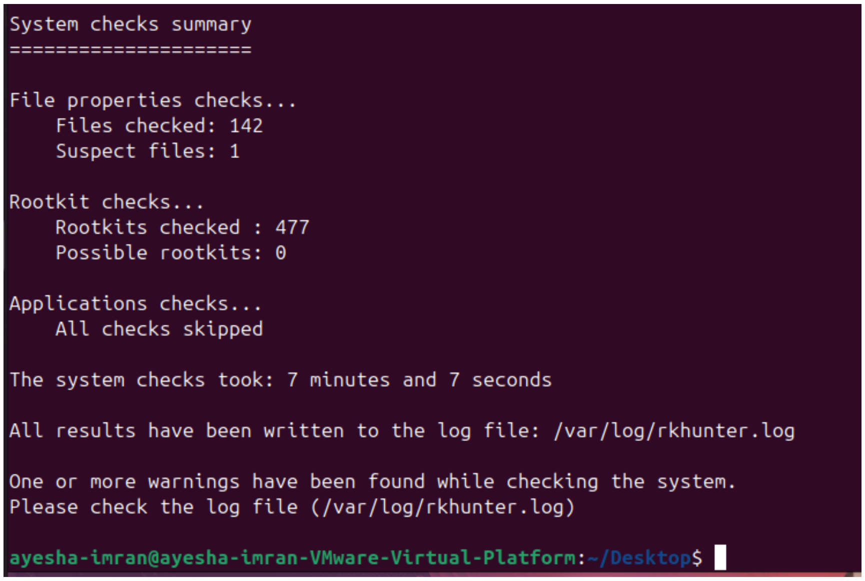


```
Performing filesystem checks
  Checking /dev for suspicious file types                  [ None found ]
  Checking for hidden files and directories                [ Warning ]
```

Warning Explaination:

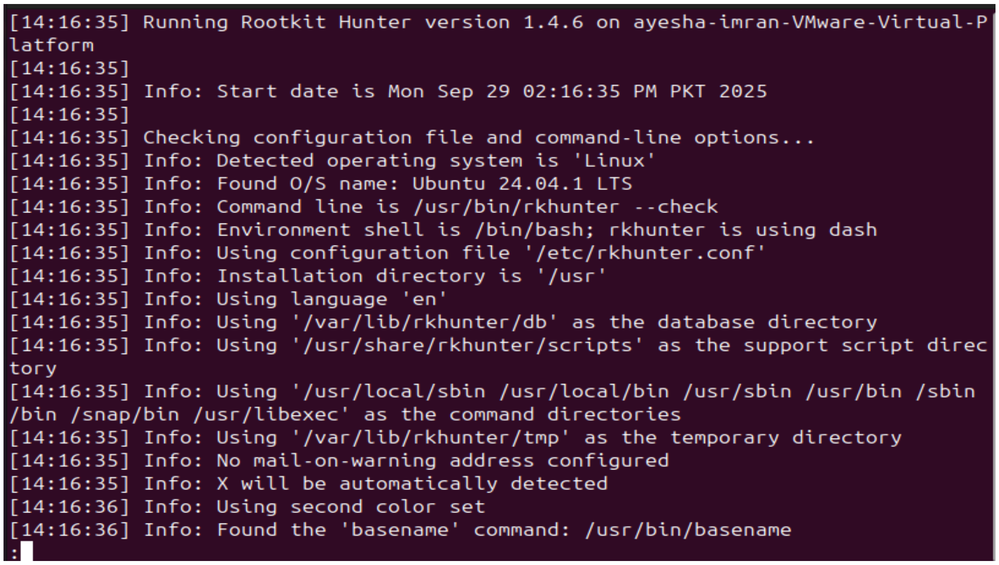
Hidden files and directories [Warning]

- RKHunter often flags hidden files (starting with a dot `.`) or directories.
- Many of these are completely normal (e.g., `.Xauthority`, `.ICE-unix`, `.ssh`, `.cache`).
- The warning simply means: *"I found hidden files — please review them to be sure they're legitimate."*

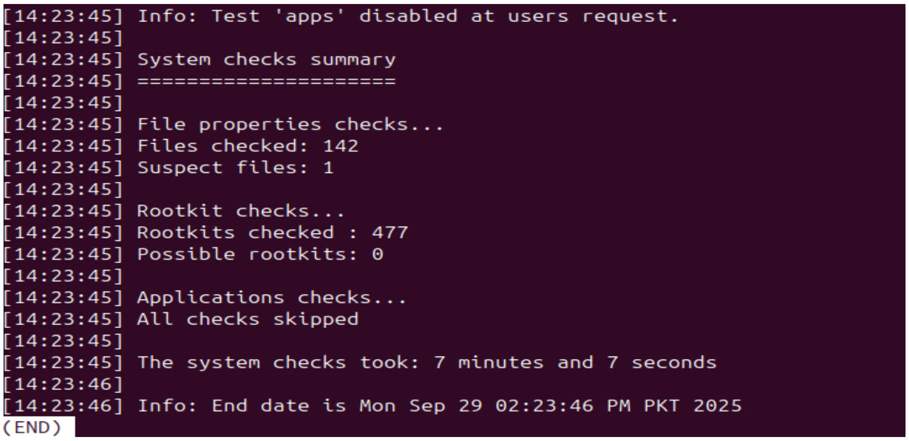


```
System checks summary
=====================

File properties checks...
    Files checked: 142
    Suspect files: 1

Rootkit checks...
    Rootkits checked : 477
    Possible rootkits: 0

Applications checks...
    All checks skipped

The system checks took: 7 minutes and 7 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)

ayesha-imran@ayesha-imran-VMware-Virtual-Platform:~/Desktop$
```

6. Review the Scan Results: sudo less/var/log/rkhunter.log



```
[14:16:35] Running Rootkit Hunter version 1.4.6 on ayesha-imran-VMware-Virtual-P
latform
[14:16:35]
[14:16:35] Info: Start date is Mon Sep 29 02:16:35 PM PKT 2025
[14:16:35]
[14:16:35] Checking configuration file and command-line options...
[14:16:35] Info: Detected operating system is 'Linux'
[14:16:35] Info: Found O/S name: Ubuntu 24.04.1 LTS
[14:16:35] Info: Command line is /usr/bin/rkhunter --check
[14:16:35] Info: Environment shell is /bin/bash; rkhunter is using dash
[14:16:35] Info: Using configuration file '/etc/rkhunter.conf'
[14:16:35] Info: Installation directory is '/usr'
[14:16:35] Info: Using language 'en'
[14:16:35] Info: Using '/var/lib/rkhunter/db' as the database directory
[14:16:35] Info: Using '/usr/share/rkhunter/scripts' as the support script direc
tory
[14:16:35] Info: Using '/usr/local/sbin /usr/local/bin /usr/sbin /usr/bin /sbin
/bin /snap/bin /usr/libexec' as the command directories
[14:16:35] Info: Using '/var/lib/rkhunter/tmp' as the temporary directory
[14:16:35] Info: No mail-on-warning address configured
[14:16:35] Info: X will be automatically detected
[14:16:36] Info: Using second color set
[14:16:36] Info: Found the 'basename' command: /usr/bin/basename
:
```



```
[14:23:45] Info: Test 'apps' disabled at users request.
[14:23:45]
[14:23:45] System checks summary
[14:23:45] =====================
[14:23:45]
[14:23:45] File properties checks...
[14:23:45] Files checked: 142
[14:23:45] Suspect files: 1
[14:23:45]
[14:23:45] Rootkit checks...
[14:23:45] Rootkits checked : 477
[14:23:45] Possible rootkits: 0
[14:23:45]
[14:23:45] Applications checks...
[14:23:45] All checks skipped
[14:23:45]
[14:23:45] The system checks took: 7 minutes and 7 seconds
[14:23:46]
[14:23:46] Info: End date is Mon Sep 29 02:23:46 PM PKT 2025
(END)
```

1. What are the most common types of rootkits detected by RKHunter?

Most Common Types of Rootkits Detected by RKHunter

RKHunter (Rootkit Hunter) is designed to scan for known patterns of rootkits, backdoors, and local exploits. Some of the most common rootkit families it detects include:

- **Linux Kernel Modules (LKM) Rootkits** – These modify or replace parts of the Linux kernel to hide processes, files, or network connections.
- **Application-Level Rootkits** – Malicious replacements of common binaries (e.g., `ls`, `ps`, `top`) to conceal malicious activity.
- **File-Based Rootkits** – Hidden or suspicious files in system directories, often with unusual permissions or names.

- **Network Rootkits** – Rootkits that intercept or manipulate network traffic to avoid detection.
- **Trojaned Commands and Backdoors** – Altered versions of commands like `ifconfig`, `netstat`, or `ssh` that provide unauthorized access.

2. How can we distinguish between legitimate software and rootkits?

Distinguishing Between Legitimate Software and Rootkits
It can be difficult to separate false positives from real threats. Key approaches include:

- **Checksum Verification** – Comparing file checksums against trusted databases (e.g., package manager records) to confirm integrity.
- **File Locations** – Rootkits often place files in unusual or hidden directories (e.g., `/dev/.something`, `/tmp/...`).
- **Unusual Behavior** – Legitimate software should not hide processes, modify system calls, or intercept kernel modules.
- **Digital Signatures & Repositories** – Packages installed from official repositories with valid signatures are far more likely to be safe.
- **Cross-check with Other Tools** – Using `chkrootkit`, `Lynis`, or package managers (e.g., `rpm -V` or `debsums`) to confirm authenticity.

3. What steps would you take if RKHunter detected a potential rootkit on a production server?

Steps if RKHunter Detected a Potential Rootkit on a Production Server
If a potential rootkit is detected, the response must be cautious and systematic:

1. **Do Not Ignore the Alert** – Even if it looks like a false positive, treat it as suspicious until verified.
2. **Confirm Findings** – Cross-check with other rootkit detection tools (`chkrootkit`, `Lynis`) and verify file integrity with package managers.
3. **Isolate the Server** – Disconnect the affected machine from the network to prevent data exfiltration or lateral movement.
4. **Avoid Tampering with Evidence** – Do not delete suspicious files immediately; preserve logs and artifacts for investigation.
5. **Check Backups** – Ensure recent clean backups are available.
6. **Plan Recovery** – In many cases, the safest solution is to rebuild the server from trusted installation media rather than attempting to “clean” the rootkit.
7. **Apply Patches and Harden Security** – Update all software, close unnecessary ports, enforce strong authentication, and enable intrusion detection/prevention systems.
8. **Monitor Closely** – After restoration, keep monitoring system logs, file integrity, and network traffic for anomalies.