2024

Penetration Test Report

INTRODUCTION

This report is written based on the penetrating test result under Virtual Machine environment where Ubuntu 22.04 is installed. This VAPT is performed during internship.This report is follow CIS benchmark security standards and mitigation techniques. Ubuntu 22.04 LTS is a popular open-source operating system used by individuals and organnizations worldwide. As with any operating system, it is essential to evaluate its security features and configurations to ensure the protection of sensitive data and prevent potential threat.

This report presents the findings of security assessment counducted on ubuntu 22.04 LTS. The assessment focused on system configurations, and software updates, providing recommendations for enhancing the security of operating system.

Table of Contents

1. Executive Summary

This penetration testing report provides an overview of the security audit conducted on the Ubuntu 22.04 LTS system. The assessment aimed to identify and exploit potential vulnerabilities to determine the system's security against malicious attacks.

1.1. Scope of Work

The test was designed to do following steps within a virtual environment.

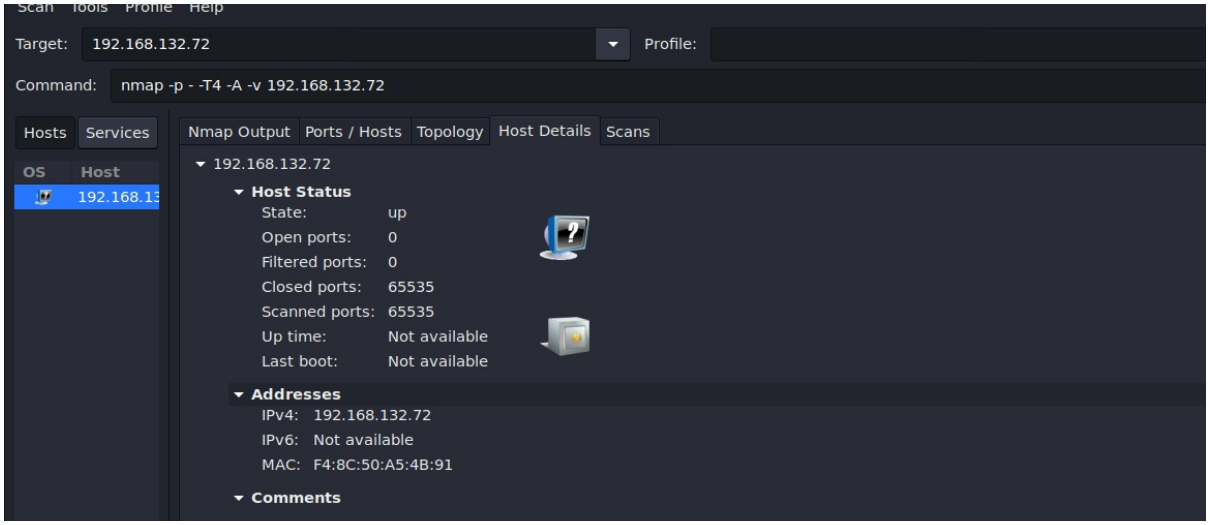
- Scanning target network
- Getting detail information about the operating system
- Perform audit on operating system according to CIS benchmark standards.

1.2. OBJECTIVES

The objective of this test is to determine vulnerabilities in Ubuntu 22.04 LTS operating system. The test provides the security misconfiguration in operating system and to audit the operating system according to CIS benchmark Ubuntu 22.04 LTS. The purpose of the CIS benchmark for ubuntu 22.04 is to provide a set of security best practices and guidelines for securing systems running the ubuntu 22.04 operating system.

2.Gathering information

Gathering information is the first step of our penetration test, so we use nmap command to scan the target network 192.168.132.72 . We couldn't find the detail of the open ports -nmap -sV -p - -A -v 192.168.132.72 where 1 is the start port number and 65535 is the last port number.



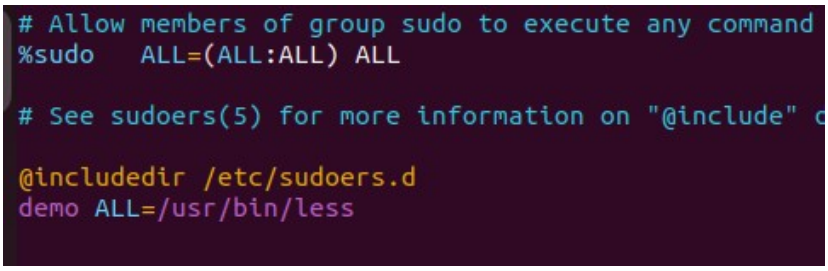
- Ubuntu 22.04 LTS contain GNOME 42 which offers smoother visuals, animations, and workspace transitions. **Linux Kernel 5.15:** This kernel comes with a stable base and a bunch of features including newer NTFS3 drivers, in-kernel SMB file service, Ext4 improvements, and better support for newer hardware including alder lake and apple M1.

3. Vulnerability check and get access to the target system

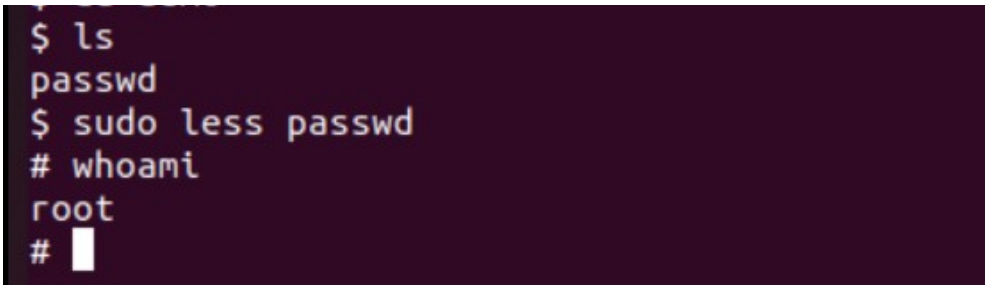
3.1 Privileged escalation with less vulnerability:

We have found less command vulnerability on target ubuntu 22.04 LTS operating system. Less command is a Linux utility that can be used to read the contents of a text file at a time. It has faster access. Found that if local user has given less command access in sudoers file it will give access of root. we Below are steps for exploitation of :

- Create new user demo.
- Give sudo access of less command only.
- Give the command that will copy passwd file- cp /etc/passwd /home/demo



- Switch user to demo and give command – sudo less passwd. And shell out the less command as !/bin/sh and press enter.
- Here we got the root access –



- Risk Factor : Critical

- Reference : https://ubuntu.com/security/notices/USN-6664-1

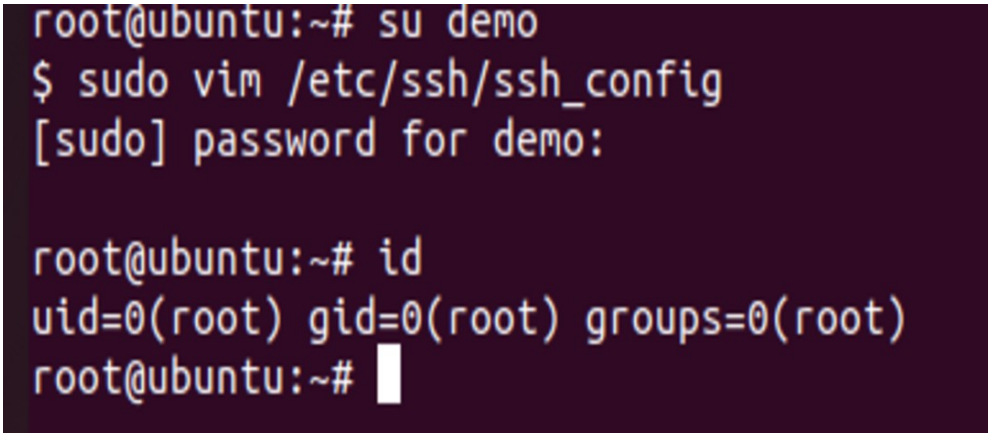
- Remediation : Affected package : less_590-1ubuntu0.22.04.1
  Fixed package : less_590-1ubuntu0.22.04.2

3.2 Privileged escalation with vim vulnerability :

We have found vim vulnerability on target ubuntu 22.04 LTS operating system. It is a highly configurable text editor built to enable efficient text editing. Found that if local user has given vim and ssh_config file access in sudoers file it will give access of root. we Below are steps for exploitation of :

- We came to know that vim vulnerability with ssh_config file
- We have assigned sudo access to user demo – demo ALL(ALL:ALL)

  /usr/bin/vim , /etc/ssh/ssh_config.
- switch user to demo. And open ssh_config file using vim editor.
- Give command in vim :shell and you will get root access.



- Risk Factor : Medium
- Reference : https://ubuntu.com/security/notices/USN-6698-1
- Remediation : Update the affected package

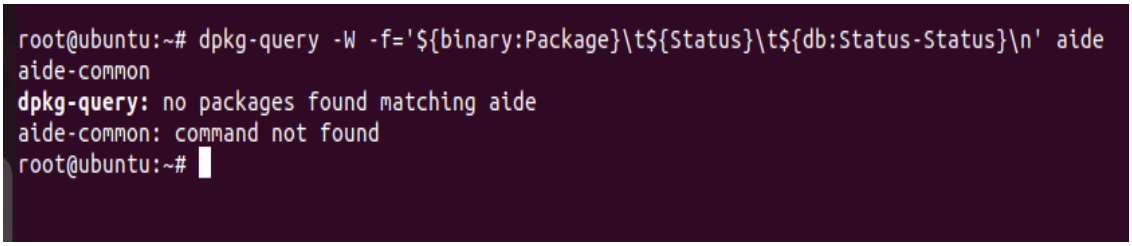
4. System audit according to CIS benchmark

In this section we are going to conduct system audit according to CIS benchmark Ubuntu 22.04 LTS. The CIS Benchmarks are **c**ommunity-developed secure configuration recommendations for hardening organizations' technologies against cyber attacks. Here we compare the configurations and settings of the target system in the inventory to the recommended benchmarks.

1. AIDE is not installed :

AIDE (Advanced Intrusion Detection Environment) takes a snapshot of filesystem state including modification times, permissions,and file hashes which can then be used to compare against the current state of the filesystem to detect modifications to the system.

By monitoring the filesystem state compromised files can be detected to prevent exposure of accidental or malicious misconfigurations.

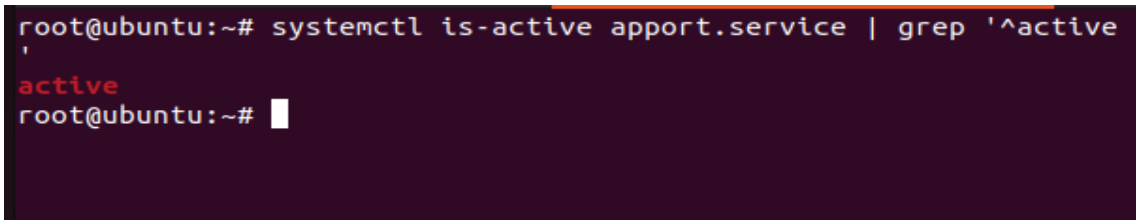


- Remediation : Install AIDE using package manager or run the command :

 # apt install aide aide-common

2. Apport Error Reporting Service is active :

The Apport Error Reporting Service automatically generates crash reports for debugging. Apport collects potentially sensitive data, such as core dumps, stack traces, and log files. They can contain passwords, credit card numbers, serial numbers,and other private material.

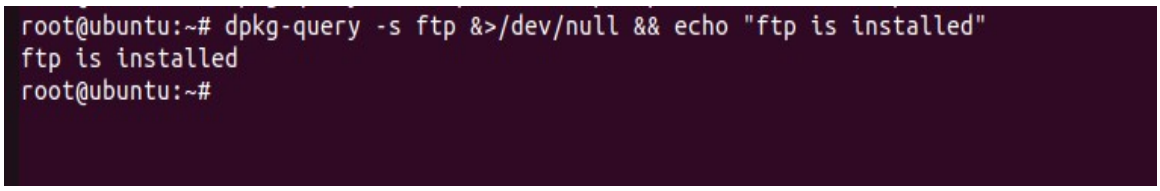


- Remediation : Run the following command to stop and disable apport service.

systemctl stop apport.service
systemctl --now disable apport.service

3. FTP server is installed :

The File Transfer Protocol (FTP) provides networked computers with the ability to transfer files. FTP does not protect the confidentiality of data or authentication credentials. It is recommended SFTP (simple file transfer protocol) be used if file transfer is required.

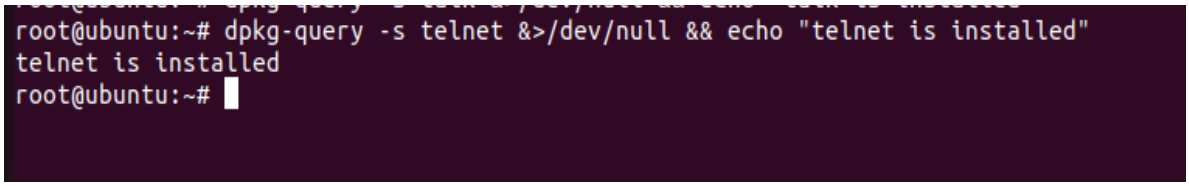


- Remediation : Run the following command to remove vsftpd:

apt purge vsftpd

4. Telnet is installed :

The telnet package contains the telnet client, which allows users to start connections to other systems via the telnet protocol. The telnet protocol is insecure and unencrypted. The use of an unencrypted transmission medium could allow an unauthorized user to steal credentials.

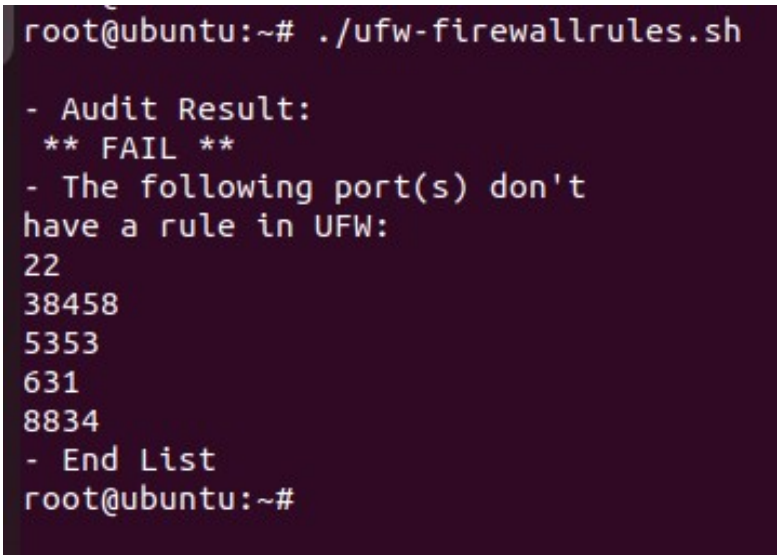


- Remediation : - Use ssh package which provides an encrypted session and stronger security for connections.

  - Uninstall telnet - # apt purge telnet

5. ufw firewall rules not exist for all open ports :

Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic. Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.

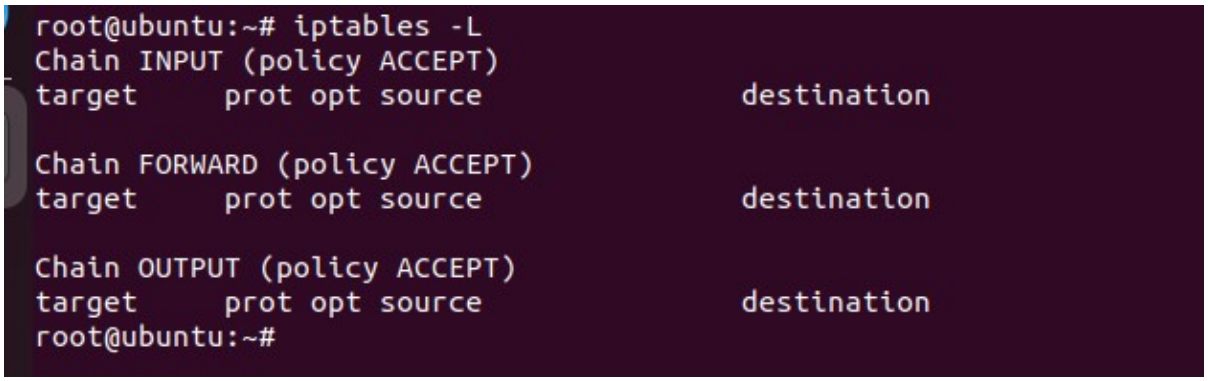


- Remediation : For each port identified in the audit which does not have a firewall rule, add rule for accepting or denying inbound connections:

  Example: # ufw allow in <port>/<tcp or udp protocol>

6. iptables are not flushed with nftables :

It is possible to mix iptables and nftables. However, this increases complexity and also the chance to introduce errors. For simplicity flush out all iptables rules, and ensure it is not loaded. nftables is a replacement for iptables.

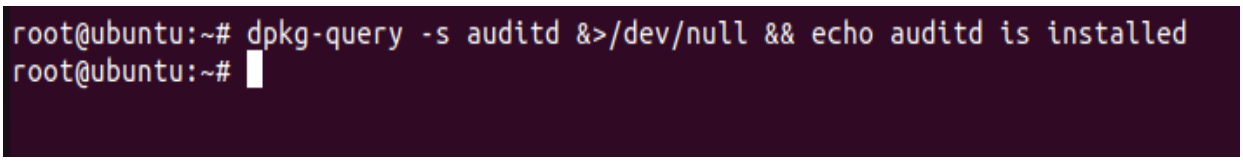


- *Remediation: Run the following commands to flush iptables:*

  # iptables -F

7. auditd is not installed :

auditd is the userspace component to the Linux Auditing System. It's responsible for writing audit records to the disk.The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.

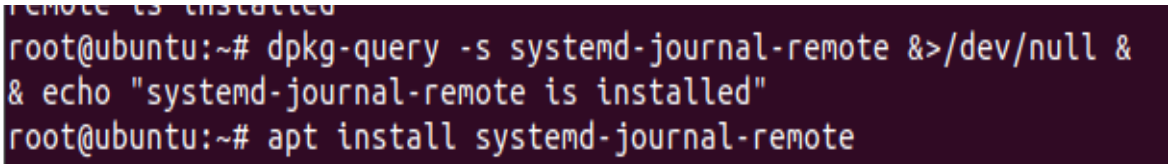


- Remediation : Run the following command to Install auditd

  # apt install auditd audispd-plugins

8. systemd-journal-remote is not installed :

systemd-journal-remote supports the ability to send log events it gathers to a remote log host or to receive messages from remote hosts. Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.

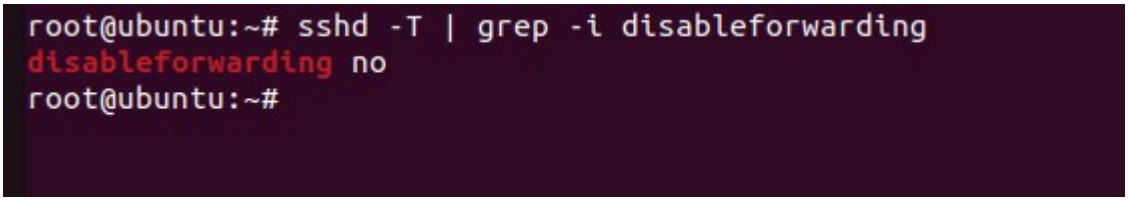


- Remediation : Run the following command to install systemd-journal-remote:

  # apt install systemd-journal-remote

9. sshd DisableForwarding is not enabled :

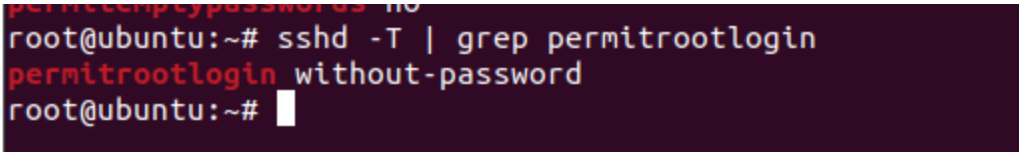
The DisableForwarding parameter disables all forwarding features, including X11, ssh-agent(1), TCP and StreamLocal.There is a small risk that the remote X11 servers of users who are logged in via SSH with X11 forwarding could be compromised by other users on the X11 server.anyone with root privilege on the the intermediate server can make free use of ssh-agent to authenticate them to other servers Leaving port forwarding enabled can expose the organization to security risks and backdoors.



- Remediation : Edit the /etc/ssh/sshd_config file to set the **DisableForwarding parameter to yes**

10. sshd PermitRootLogin is enabled :

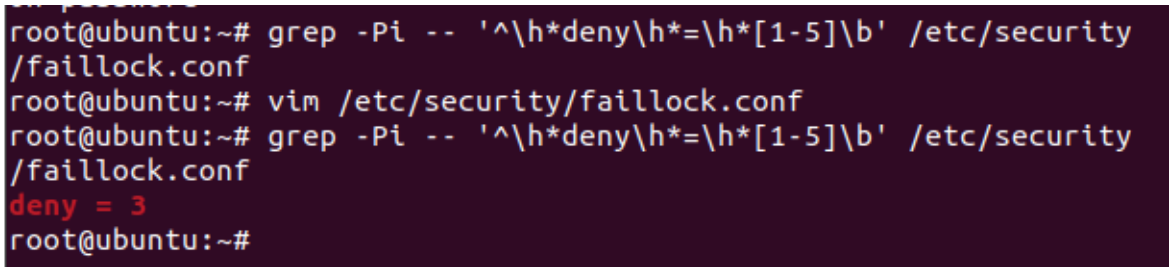
The PermitRootLogin parameter specifies if the root user can log in using SSH. Disallowing root logins over SSH requires system admins to authenticate using their own individual account, then escalating to root. This limits opportunity for non repudiation and provides a clear audit trail in the event of a security incident.



- Remediation : Edit the /etc/ssh/sshd_config file to set the **PermitRootLogin parameter to no**

11. Password failed attempts lockout is not configured :

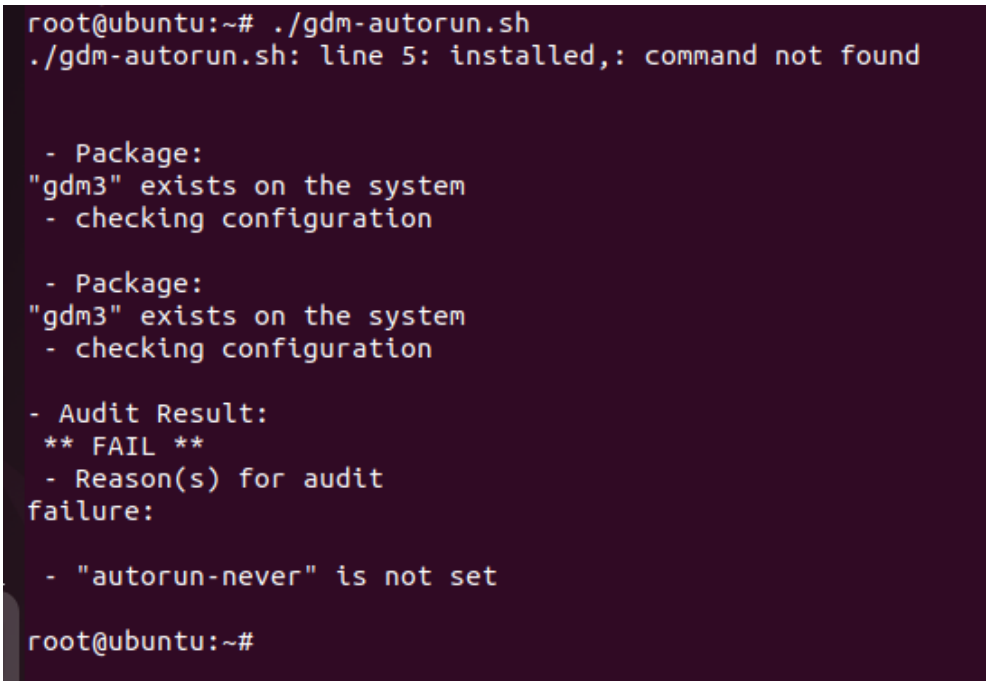
The deny=<n> option will deny access if the number of consecutive authentication failures for this user during the recent interval exceeds . Locking out user IDs after n unsuccessful consecutive login attempts mitigates brute force password attacks against your systems. We can run the following command to verify that Number of failed logon attempts before the account is locked is no greater than 5 and meets local site policy here i have set 3 attempts.:



- Remediation : Create or edit the following line in /etc/security/faillock.conf setting the deny option to 5 or less.

12. GDM autorun-never is disabled :

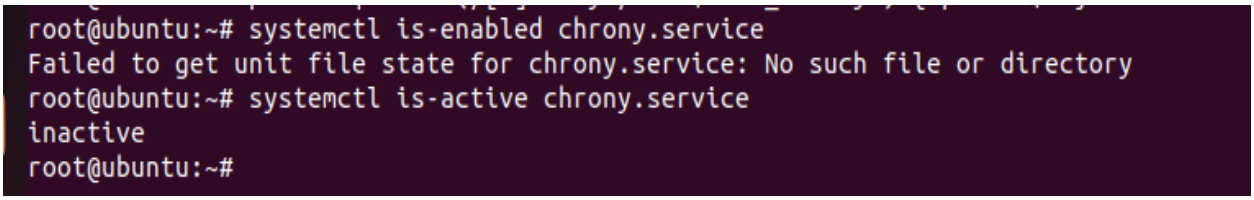
The autorun-never setting allows the GNOME Desktop Display Manager to disable autorun through GDM. Malware on removable media may taking advantage of Autorun features when the media is inserted into a system and execute.



- Remediation : set autorun-never to true for GDM users:

13. chrony service is disabled and not running :

chrony is a daemon for synchronizing the system clock across the network chrony needs to be enabled and running in order to synchronize the system to a timeserver. Time synchronization is important to support time sensitive security mechanisms and to ensure log files have consistent time records across the enterprise to aid in forensic investigations.



- Remediation : IF - chrony is in use on the system, run the following commands:
  - Run the following command to unmask chrony.service:

    # systemctl unmask chrony.service
  - Run the following command to enable and start chrony.service:

    # systemctl --now enable chrony.service
  - If another time synchronization service is in use on the system, run the following

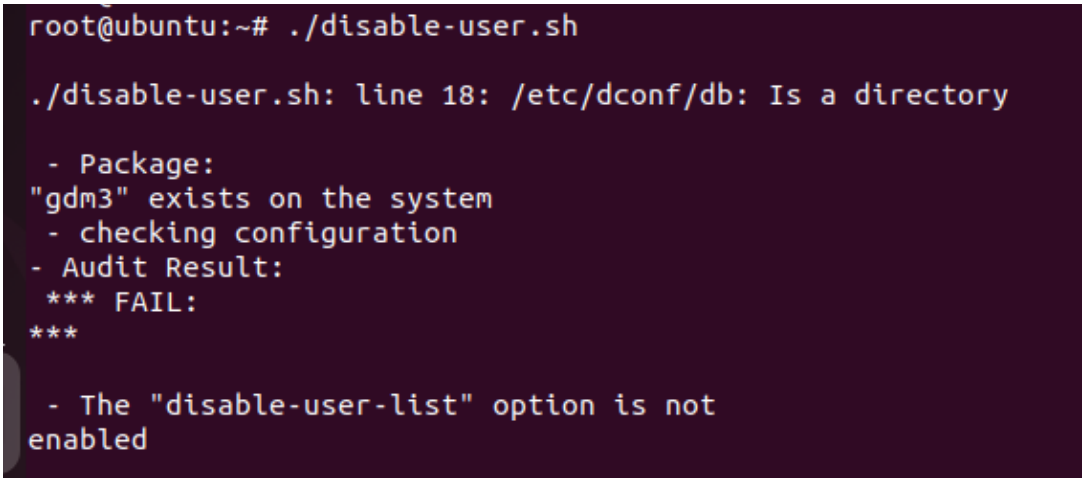
  command to remove chrony:

    # apt purge chrony

    # apt autoremove chrony

14. GDM disable-user-list option is not enabled :

E Display Manager which handles graphical login for GNOME based systems. The disable-user-list option controls if a list of users is displayed on the login screen Displaying the user list eliminates half of the Userid/Password equation that an unauthorized person would need to log on.



Remediation : If - GDM is installed: enable the disable-user-list option.

5. Conclusion:

The Vulnerability Assessment and Penetration Testing (VAPT) conducted on the operating system, guided by the CIS benchmark, has provided a comprehensive evaluation of the security posture. The audit identified critical vulnerabilities and misconfigurations that could potentially be exploited, posing a significant risk to the system's integrity, confidentiality, and availability

All activities were conducted under the written permission. All activities are conducted to simulate an unauthorized access from outside. Through gives the customer the following result of: The target system is cracked through finding vulnerabilities

Conducted the penetration test based on the CIS benchmark Ubuntu 22.04 LTS and using some executable files with having root privilege during their execution. The test result shows that those poor practices led the hacker into the system.