Sri Lanka Institute of Information Technology

Database and OS security of the HR system of a company

IE3062- Data and Operating Systems Security

Cyber Security - Year 3, Semester 2

Submitted by:

Student Registration number	Student Name
IT21110184	Peiris B.L.H.D
IT21051548	A.R.W.M.V. Hasaranga
IT21049354	Athauda A.M.I.R.B.
IT21085376	J.P.A.S. Pathmendre

26 Oct 2023

Date of Submission

Contents

Task 01 - OS Security

Distribution	**Pros**	**Cons**
Red Hat Enterprise Linux (RHEL)	• **Stable and Secure**: Known for its stability and security, making it a preferred choice for enterprise environments. • **Support and Certification**: Provides extensive professional support and a wide range of certified hardware and software. • **Ecosystem and Community**: Boasts a large ecosystem and community, offering a wealth of resources and third-party applications.	• **Cost**: Comes with a subscription cost, which might be prohibitive for small businesses or individual users. • **Less Cutting-Edge**: Tends to prioritize stability over the latest features, which might not suit users looking for the newest software. • **Complexity**: Can be complex to set up and manage, especially for those new to Linux.
OpenSUSE	• **YaST**: Features the powerful YaST administration tool that simplifies many complex tasks. • **Tumbleweed and Leap**: Offers both a rolling release version (Tumbleweed) and a regular release version (Leap).	• **Less Popular**: Not as widely adopted as some other distributions, potentially leading to fewer community resources. • **Software Availability:** Some proprietary software might not be readily available or might require additional configuration.

	• **Community and Documentation**: Has a strong community and extensive documentation.	• **Hardware Compatibility:** Some users have reported issues with hardware compatibility, particularly with newer hardware.
CentOS	• **Free**: Completely free to use. • **Enterprise-Grade**: Provides an enterprise-grade platform without the associated costs. • **Compatibility with RHEL**: Highly compatible with RHEL, facilitating easy transitions between the two.	• **End of Life**: CentOS Linux 8 reached its end of life in 2021, with users encouraged to move to CentOS Stream. • **Slower Updates**: May have slower updates compared to distributions with faster release cycles. • **Community Support**: While there is a community, the level of support might not be as extensive as with other distributions.
Ubuntu Server	• **User Accessibility:** Renowned for its straightforward installation process and intuitive user interface. • **Comprehensive Software Options:**	• **Controversial Package Management:** The shift towards using Snap packages has received mixed reactions from the user base.

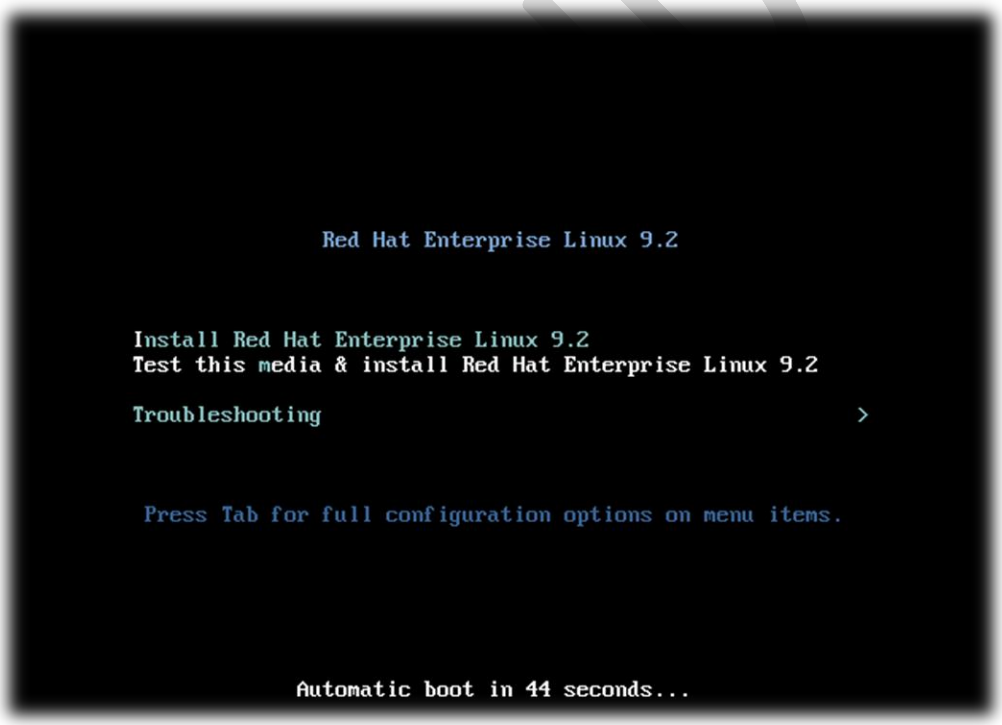
	Hosts a vast array of applications and services available for installation. • **Robust Community and Resources:** Supported by a large and active user community, along with plentiful documentation.	• **Rapid Release Cycles:** While it ensures access to the latest features, the fast-paced updates can sometimes introduce instability. • **Concerns Over Commercial Influence:** Some users express unease regarding the influence of Canonical, the parent company, and its commercial interests.
Debian	• **Stability**: Renowned for its stability, especially the Debian Stable branch. • **Free Software**: Committed to providing free software, appealing to open-source enthusiasts. • **Extensive Repositories**: Offers a vast array of software packages in its repositories.	• **Older Packages**: Focus on stability means software packages can be outdated. • **Less User-Friendly**: Can be less user-friendly, especially for those new to Linux. • **Slower Release Cycle**: Has a slower release cycle, potentially leading to longer waits for the latest software and features.

Choose Distribution – Red Hat.

Red Hat Enterprise Linux's robust security posture, extensive certifications against industry standards, emphasis on reliability, and long-term support make it an ideal choice when hardening a database server for an enterprise scenario. RHEL incorporates advanced security technologies like SELinux and sophisticated security modules out-of-the-box providing a hardened base to build upon. Rigorous testing and compliance with standards like FISMA, PCI-DSS, and HIPAA lend assurance that RHEL can securely run sensitive databases. Major releases receive up to 10 years of support, ensuring ample time to implement and fine-tune security properly. The Red Hat ecosystem smoothly facilitates integrating Oracle, automation tools, and enterprise infrastructure. While licensing costs and the learning curve are downsides, RHEL's specialized security capabilities make it a sensible choice when emulating real-world conditions for hardening a database server assignment.

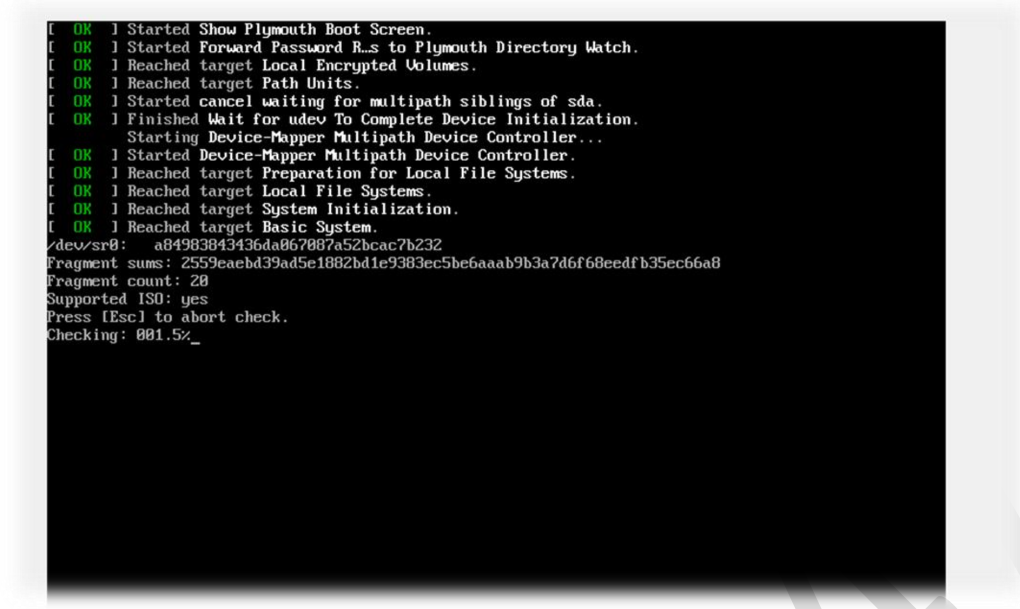
Installation of the Distribution.

Step 01: Booting the VM.



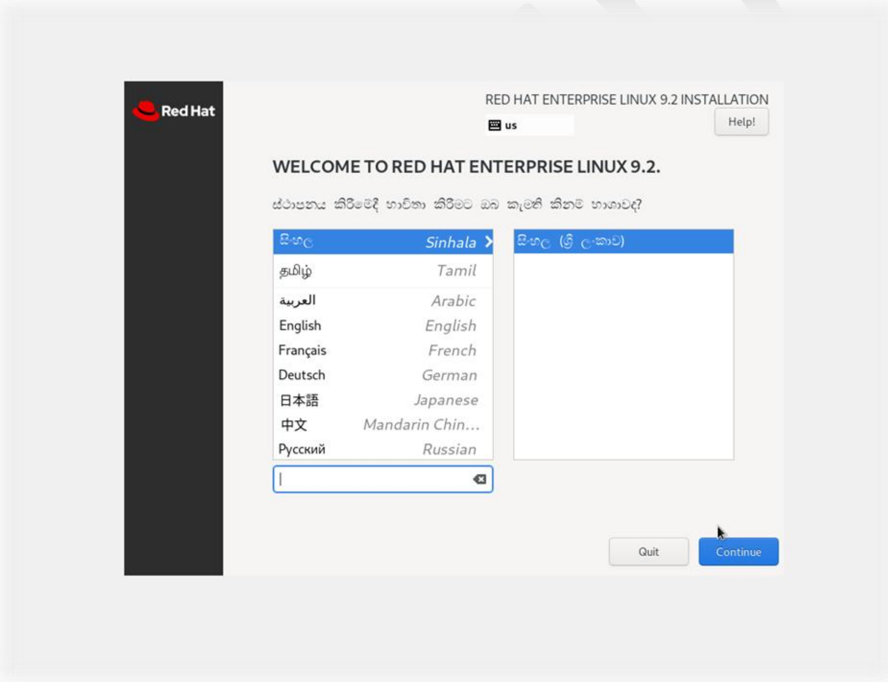
```
                    Red Hat Enterprise Linux 9.2

          Install Red Hat Enterprise Linux 9.2
          Test this media & install Red Hat Enterprise Linux 9.2

          Troubleshooting                                      >

           Press Tab for full configuration options on menu items.

                        Automatic boot in 44 seconds...
```

Step 02: After the VM boot, it will begin to install Red Hat.



```
[  OK  ] Started Show Plymouth Boot Screen.
[  OK  ] Started Forward Password R…s to Plymouth Directory Watch.
[  OK  ] Reached target Local Encrypted Volumes.
[  OK  ] Reached target Path Units.
[  OK  ] Started cancel waiting for multipath siblings of sda.
[  OK  ] Finished Wait for udev To Complete Device Initialization.
         Starting Device-Mapper Multipath Device Controller...
[  OK  ] Started Device-Mapper Multipath Device Controller.
[  OK  ] Reached target Preparation for Local File Systems.
[  OK  ] Reached target Local File Systems.
[  OK  ] Reached target System Initialization.
[  OK  ] Reached target Basic System.
/dev/sr0:   a84983843436da067087a52bcac7b232
Fragment sums: 2559eaebd39ad5e1882bd1e9383ec5be6aaab9b3a7d6f68eedfb35ec66a8
Fragment count: 20
Supported ISO: yes
Press [Esc] to abort check.
Checking: 001.5%_
```

Step 03: The "Start using Red Hat Enterprise Linux" button appears in blue once you click it. It will open a popup asking you to choose a language.



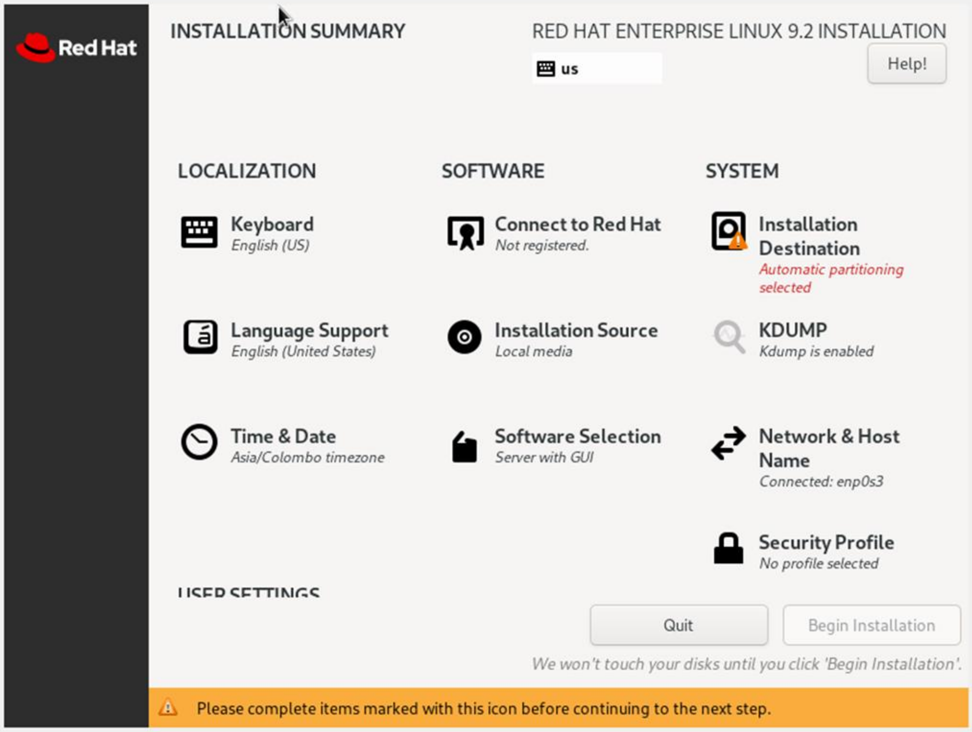
WELCOME TO RED HAT ENTERPRISE LINUX 9.2.

ස්ථාපනය කිරීමේදී භාවිතා කිරීමට ඔබ කැමති කිනම් භාෂාවද?

සිංහල	Sinhala
தமிழ்	Tamil
العربية	Arabic
English	English
Français	French
Deutsch	German
日本語	Japanese
中文	Mandarin Chin…
Русский	Russian

සිංහල (ශ්‍රී ලංකාව)

Step 4: Following that, the window seen above will prompt. (Here, log in with the credentials you made while setting up the virtual machine earlier.)



INSTALLATION SUMMARY

RED HAT ENTERPRISE LINUX 9.2 INSTALLATION

us

LOCALIZATION

- Keyboard — *English (US)*
- Language Support — *English (United States)*
- Time & Date — *Asia/Colombo timezone*

SOFTWARE

- Connect to Red Hat — *Not registered.*
- Installation Source — *Local media*
- Software Selection — *Server with GUI*

SYSTEM

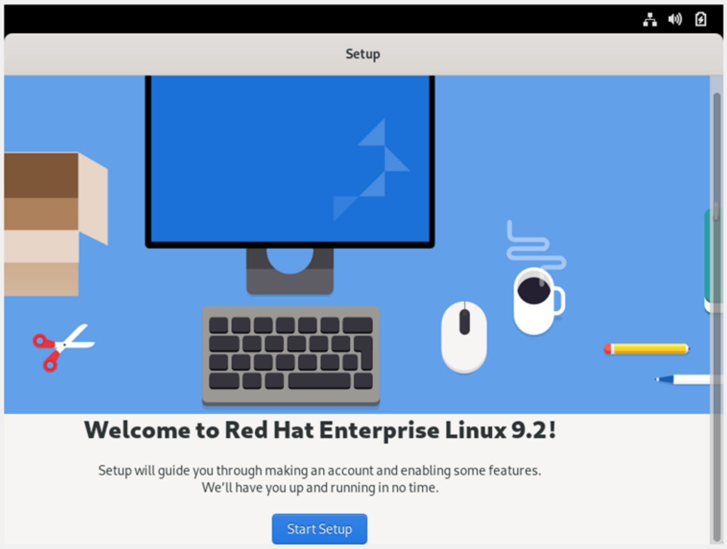
- Installation Destination — *Automatic partitioning selected*
- KDUMP — *Kdump is enabled*
- Network & Host Name — *Connected: enp0s3*
- Security Profile — *No profile selected*

USER SETTINGS

We won't touch your disks until you click 'Begin Installation'.

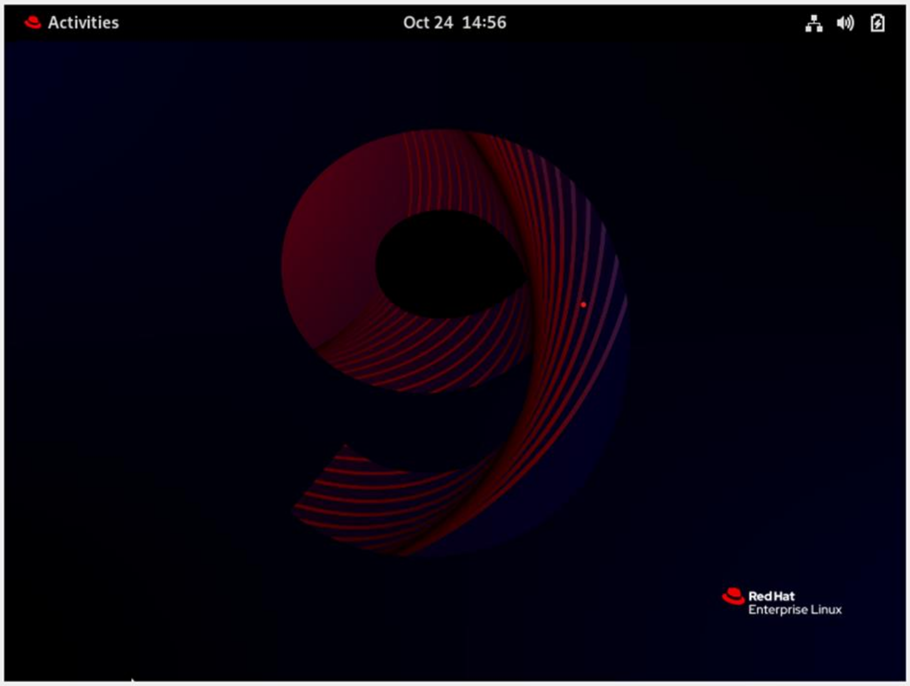
Please complete items marked with this icon before continuing to the next step.

Step 5: After setting up passwords and configurations Red Hat starts.



Welcome to Red Hat Enterprise Linux 9.2!

Setup will guide you through making an account and enabling some features.
We'll have you up and running in no time.



Security Risks Faced by the Red Hat Enterprise Linux.

Default/weak passwords - If default passwords or weak passwords are used for user accounts or services, attackers can easily guess them and gain access. Should enforce strong password policies.

Unnecessary services enabled - By default some unused network services may be running opening unnecessary ports. Should disable any unneeded services.

Outdated software - If system software is not updated, vulnerabilities in older versions could be exploited. Keeping software updated is critical.

Improper filesystem permissions - If filesystem permissions are too lax, accounts may access unauthorized files. Filesystem access should be locked down.

Lack of firewall - Without a firewall configured, all ports are exposed allowing attackers to target services. A firewall should be set up to limit access.

Insecure authentication - Using only password logins is insecure. Should use multi-factor authentication like SSH keys.

Missing security patches - Not applying the latest security errata patches leaves known vulnerabilities open for attackers. Must maintain regular patching.

No logging or auditing - With no system activity logs, malicious access could go undetected. Enabling and centralizing logs is important.

Configurations to harden the Red Hat Enterprise Linux

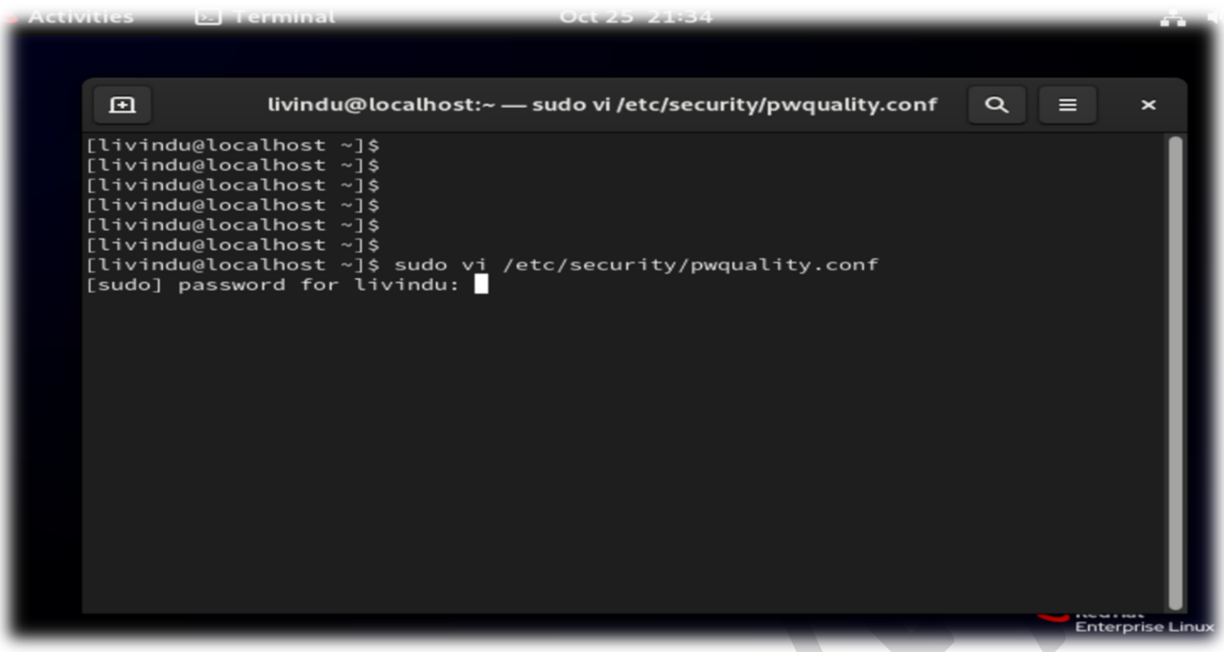
1. Enforce Strong Password Policies

Configuration: Edit the /etc/security/pwquality.conf file to set strict password policies.

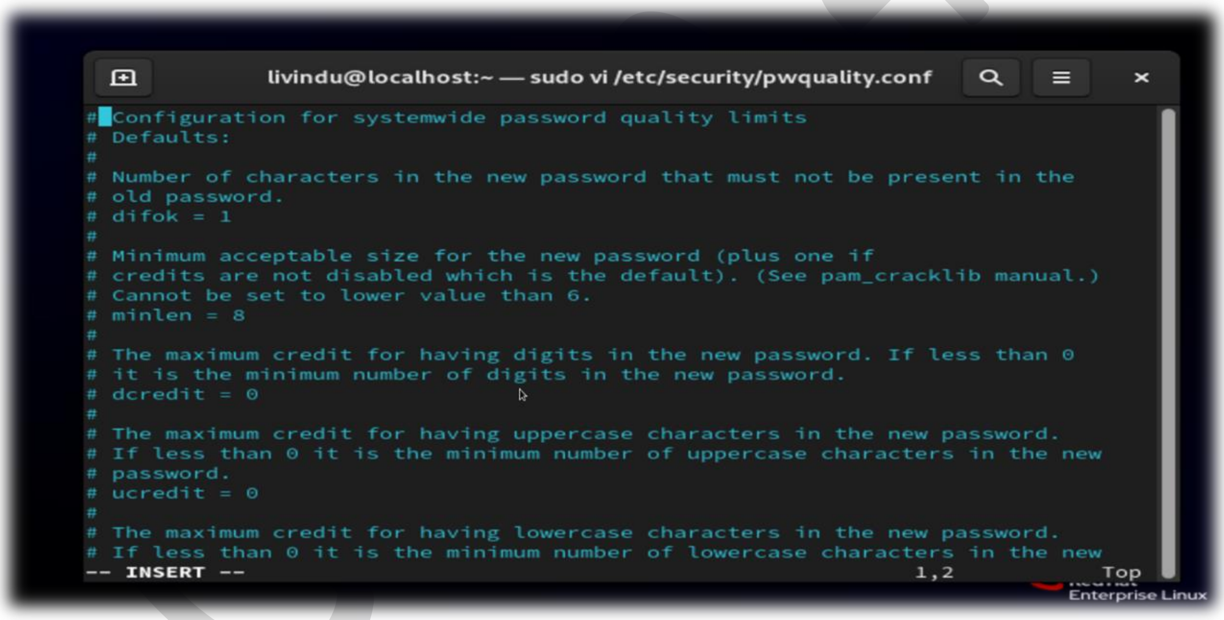
Why It Increases Security: Ensures that all user passwords are complex and difficult for attackers to guess or crack.

Protection Against: Brute force attacks, password guessing, and credential stuffing.

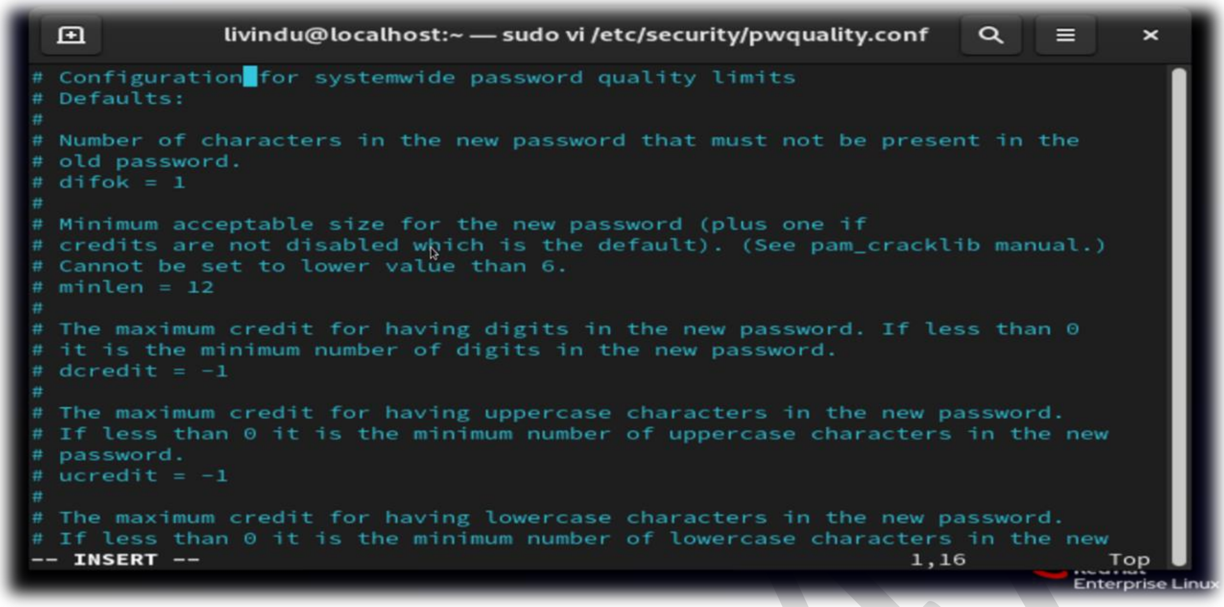
```
(Commands - echo "minlen = 12
minclass = 4
dcredit = -1
ucredit = -1
lcredit = -1
ocredit = -1" >> /etc/security/pwquality.conf)
```



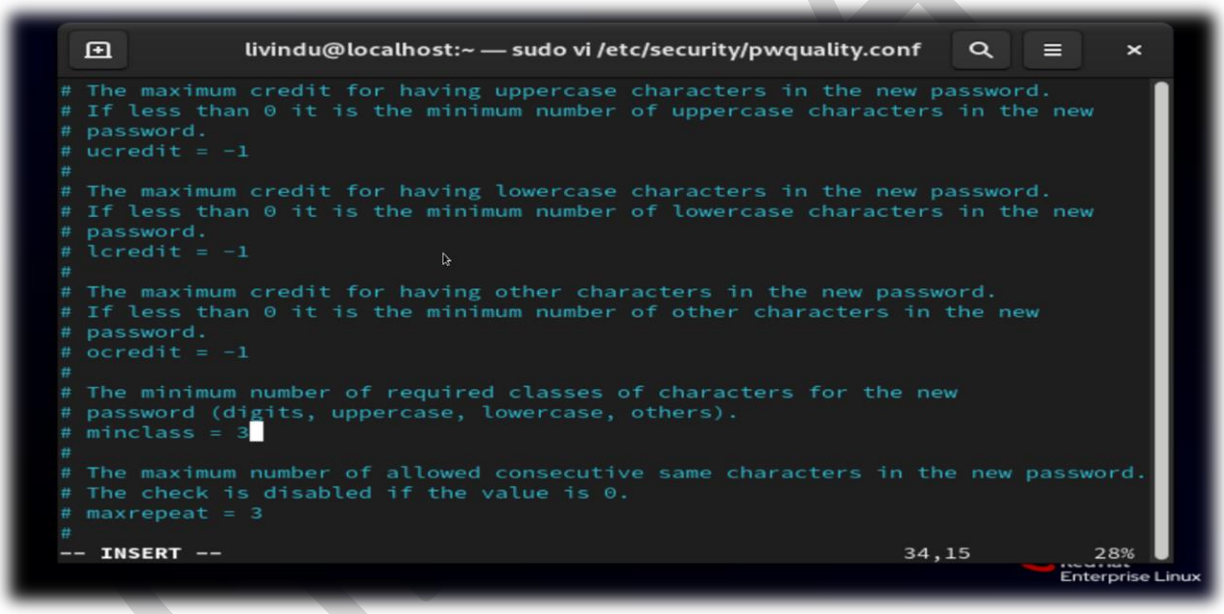
```
[livindu@localhost ~]$
[livindu@localhost ~]$
[livindu@localhost ~]$
[livindu@localhost ~]$
[livindu@localhost ~]$
[livindu@localhost ~]$
[livindu@localhost ~]$ sudo vi /etc/security/pwquality.conf
[sudo] password for livindu:
```



```
# Configuration for systemwide password quality limits
# Defaults:
#
# Number of characters in the new password that must not be present in the
# old password.
# difok = 1
#
# Minimum acceptable size for the new password (plus one if
# credits are not disabled which is the default). (See pam_cracklib manual.)
# Cannot be set to lower value than 6.
# minlen = 8
#
# The maximum credit for having digits in the new password. If less than 0
# it is the minimum number of digits in the new password.
# dcredit = 0
#
# The maximum credit for having uppercase characters in the new password.
# If less than 0 it is the minimum number of uppercase characters in the new
# password.
# ucredit = 0
#
# The maximum credit for having lowercase characters in the new password.
# If less than 0 it is the minimum number of lowercase characters in the new
-- INSERT --                                                  1,2         Top
```



```
# Configuration for systemwide password quality limits
# Defaults:
#
# Number of characters in the new password that must not be present in the
# old password.
# difok = 1
#
# Minimum acceptable size for the new password (plus one if
# credits are not disabled which is the default). (See pam_cracklib manual.)
# Cannot be set to lower value than 6.
# minlen = 12
#
# The maximum credit for having digits in the new password. If less than 0
# it is the minimum number of digits in the new password.
# dcredit = -1
#
# The maximum credit for having uppercase characters in the new password.
# If less than 0 it is the minimum number of uppercase characters in the new
# password.
# ucredit = -1
#
# The maximum credit for having lowercase characters in the new password.
# If less than 0 it is the minimum number of lowercase characters in the new
-- INSERT --                                                  1,16          Top
```



```
# The maximum credit for having uppercase characters in the new password.
# If less than 0 it is the minimum number of uppercase characters in the new
# password.
# ucredit = -1
#
# The maximum credit for having lowercase characters in the new password.
# If less than 0 it is the minimum number of lowercase characters in the new
# password.
# lcredit = -1
#
# The maximum credit for having other characters in the new password.
# If less than 0 it is the minimum number of other characters in the new
# password.
# ocredit = -1
#
# The minimum number of required classes of characters for the new
# password (digits, uppercase, lowercase, others).
# minclass = 3
#
# The maximum number of allowed consecutive same characters in the new password.
# The check is disabled if the value is 0.
# maxrepeat = 3
#
-- INSERT --                                                 34,15          28%
```

2. Disable Unnecessary Services and Ports

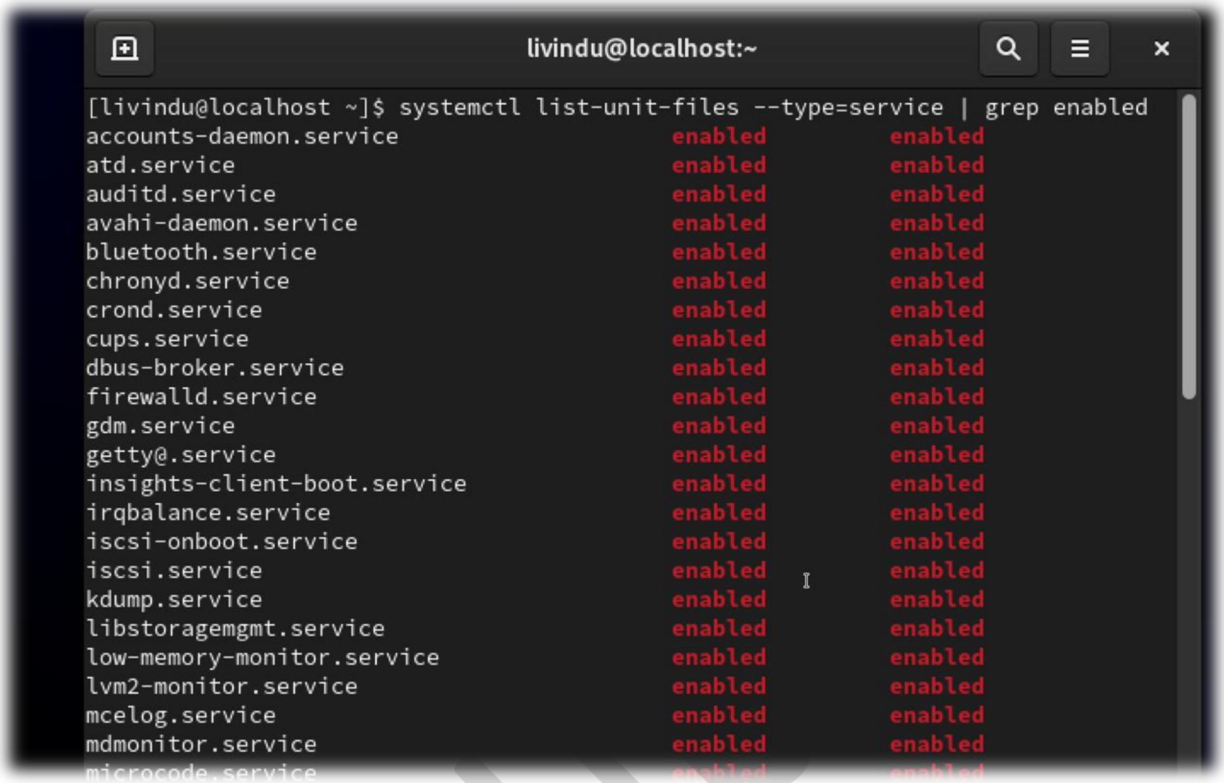
Configuration: Use Systemctl to disable and stop services that are not required.

Why It Increases Security: Reduces the attack surface by eliminating potential vulnerabilities associated with unused services.

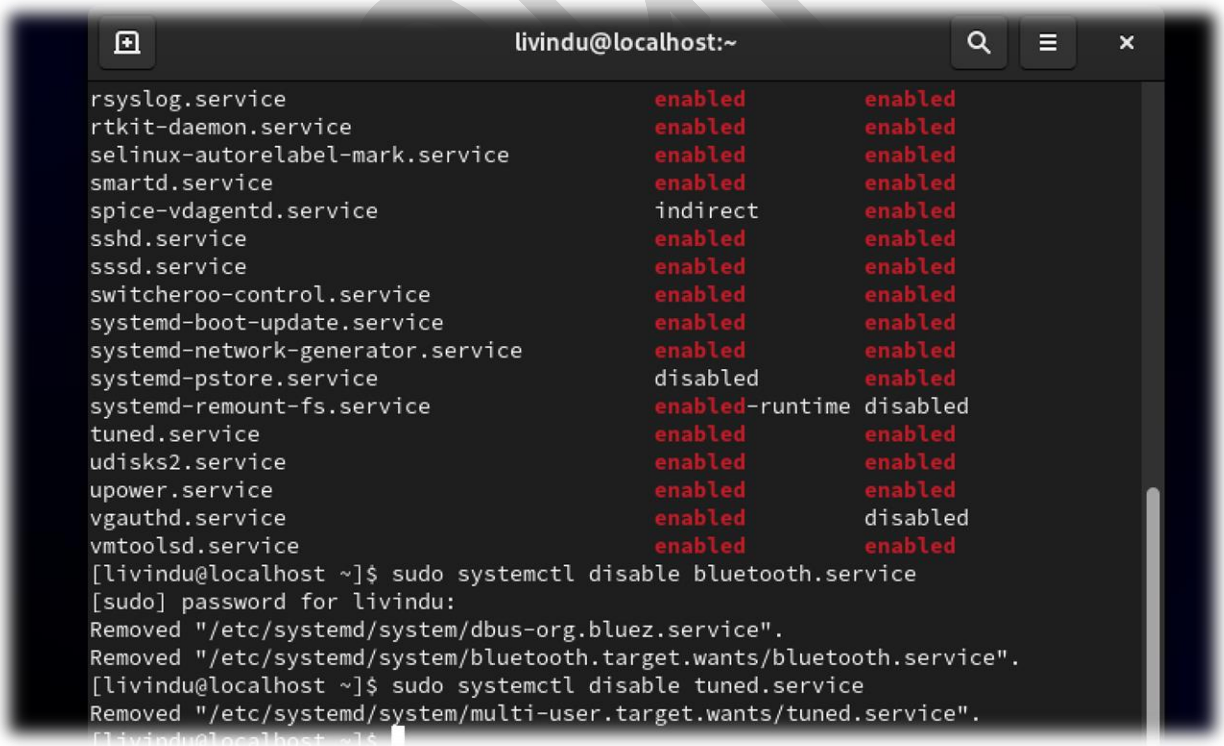
Protection Against: Unauthorized access and exploitation of services.

(***Commands*** *- systemctl disable unnecessary-service*

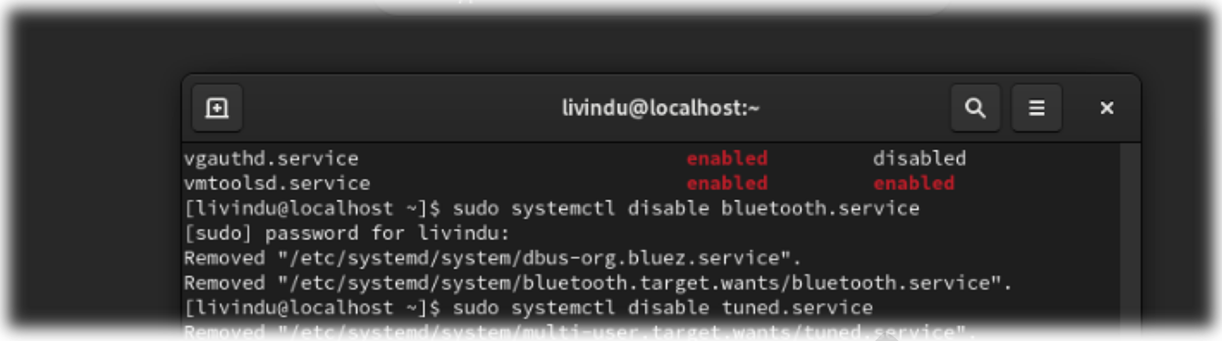
systemctl stop unnecessary-service)



```
[livindu@localhost ~]$ systemctl list-unit-files --type=service | grep enabled
accounts-daemon.service                    enabled         enabled
atd.service                                enabled         enabled
auditd.service                             enabled         enabled
avahi-daemon.service                       enabled         enabled
bluetooth.service                          enabled         enabled
chronyd.service                            enabled         enabled
crond.service                              enabled         enabled
cups.service                               enabled         enabled
dbus-broker.service                        enabled         enabled
firewalld.service                          enabled         enabled
gdm.service                                enabled         enabled
getty@.service                             enabled         enabled
insights-client-boot.service               enabled         enabled
irqbalance.service                         enabled         enabled
iscsi-onboot.service                       enabled         enabled
iscsi.service                              enabled         enabled
kdump.service                              enabled         enabled
libstoragemgmt.service                     enabled         enabled
low-memory-monitor.service                 enabled         enabled
lvm2-monitor.service                       enabled         enabled
mcelog.service                             enabled         enabled
mdmonitor.service                          enabled         enabled
microcode.service                          enabled         enabled
```



```
rsyslog.service                            enabled         enabled
rtkit-daemon.service                       enabled         enabled
selinux-autorelabel-mark.service           enabled         enabled
smartd.service                             enabled         enabled
spice-vdagentd.service                     indirect        enabled
sshd.service                               enabled         enabled
sssd.service                               enabled         enabled
switcheroo-control.service                 enabled         enabled
systemd-boot-update.service                enabled         enabled
systemd-network-generator.service          enabled         enabled
systemd-pstore.service                     disabled        enabled
systemd-remount-fs.service                 enabled-runtime disabled
tuned.service                              enabled         enabled
udisks2.service                            enabled         enabled
upower.service                             enabled         enabled
vgauthd.service                            enabled         disabled
vmtoolsd.service                           enabled         enabled
[livindu@localhost ~]$ sudo systemctl disable bluetooth.service
[sudo] password for livindu:
Removed "/etc/systemd/system/dbus-org.bluez.service".
Removed "/etc/systemd/system/bluetooth.target.wants/bluetooth.service".
[livindu@localhost ~]$ sudo systemctl disable tuned.service
Removed "/etc/systemd/system/multi-user.target.wants/tuned.service".
[livindu@localhost ~]$
```



```
vgauthd.service                                 enabled         disabled
vmtoolsd.service                                enabled         enabled
[livindu@localhost ~]$ sudo systemctl disable bluetooth.service
[sudo] password for livindu:
Removed "/etc/systemd/system/dbus-org.bluez.service".
Removed "/etc/systemd/system/bluetooth.target.wants/bluetooth.service".
[livindu@localhost ~]$ sudo systemctl disable tuned.service
Removed "/etc/systemd/system/multi-user.target.wants/tuned.service".
```

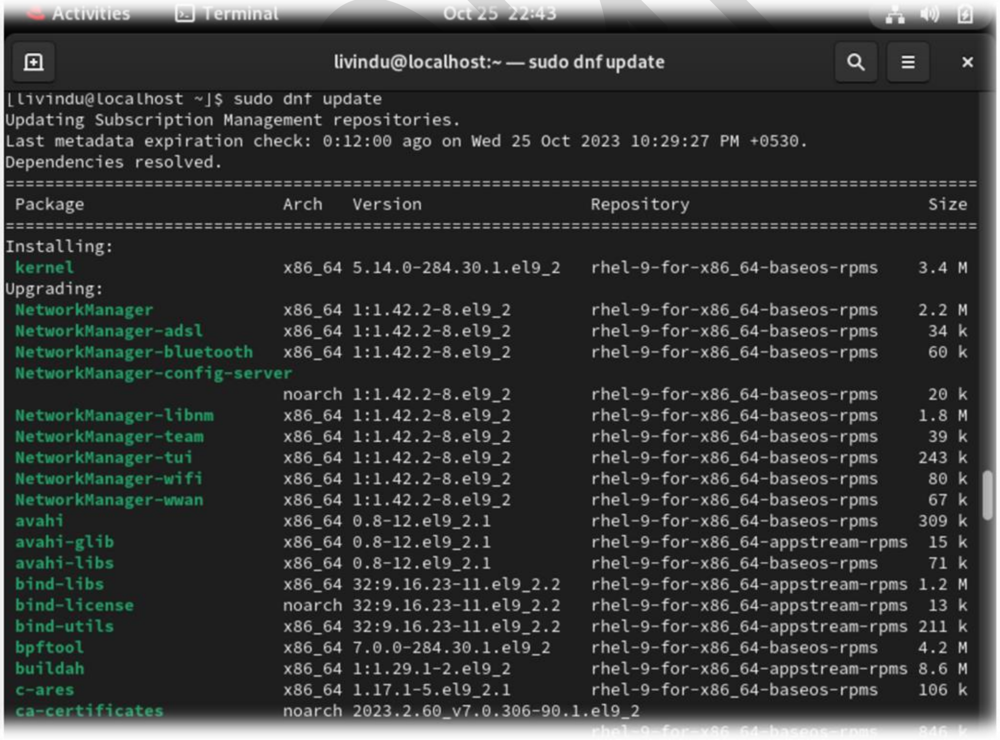
3. Keep System and Software Up to Date

Configuration: Regularly apply updates and patches using yum or dnf.

Why It Increases Security: Ensures that the system is protected from vulnerabilities found in older versions of software.

Protection Against: Exploitation of known vulnerabilities and zero-day attacks.

*(**Commands** - dnf update)*



```
[livindu@localhost ~]$ sudo dnf update
Updating Subscription Management repositories.
Last metadata expiration check: 0:12:00 ago on Wed 25 Oct 2023 10:29:27 PM +0530.
Dependencies resolved.
================================================================================================
 Package                     Arch   Version                     Repository                  Size
================================================================================================
Installing:
 kernel                      x86_64 5.14.0-284.30.1.el9_2       rhel-9-for-x86_64-baseos-rpms    3.4 M
Upgrading:
 NetworkManager              x86_64 1:1.42.2-8.el9_2            rhel-9-for-x86_64-baseos-rpms    2.2 M
 NetworkManager-adsl         x86_64 1:1.42.2-8.el9_2            rhel-9-for-x86_64-baseos-rpms     34 k
 NetworkManager-bluetooth    x86_64 1:1.42.2-8.el9_2            rhel-9-for-x86_64-baseos-rpms     60 k
 NetworkManager-config-server
                             noarch 1:1.42.2-8.el9_2            rhel-9-for-x86_64-baseos-rpms     20 k
 NetworkManager-libnm        x86_64 1:1.42.2-8.el9_2            rhel-9-for-x86_64-baseos-rpms    1.8 M
 NetworkManager-team         x86_64 1:1.42.2-8.el9_2            rhel-9-for-x86_64-baseos-rpms     39 k
 NetworkManager-tui          x86_64 1:1.42.2-8.el9_2            rhel-9-for-x86_64-baseos-rpms    243 k
 NetworkManager-wifi         x86_64 1:1.42.2-8.el9_2            rhel-9-for-x86_64-baseos-rpms     80 k
 NetworkManager-wwan         x86_64 1:1.42.2-8.el9_2            rhel-9-for-x86_64-baseos-rpms     67 k
 avahi                       x86_64 0.8-12.el9_2.1              rhel-9-for-x86_64-baseos-rpms    309 k
 avahi-glib                  x86_64 0.8-12.el9_2.1              rhel-9-for-x86_64-appstream-rpms  15 k
 avahi-libs                  x86_64 0.8-12.el9_2.1              rhel-9-for-x86_64-baseos-rpms     71 k
 bind-libs                   x86_64 32:9.16.23-11.el9_2.2       rhel-9-for-x86_64-appstream-rpms 1.2 M
 bind-license                noarch 32:9.16.23-11.el9_2.2       rhel-9-for-x86_64-appstream-rpms  13 k
 bind-utils                  x86_64 32:9.16.23-11.el9_2.2       rhel-9-for-x86_64-appstream-rpms 211 k
 bpftool                     x86_64 7.0.0-284.30.1.el9_2        rhel-9-for-x86_64-baseos-rpms    4.2 M
 buildah                     x86_64 1:1.29.1-2.el9_2            rhel-9-for-x86_64-appstream-rpms 8.6 M
 c-ares                      x86_64 1.17.1-5.el9_2.1            rhel-9-for-x86_64-baseos-rpms    106 k
 ca-certificates             noarch 2023.2.60_v7.0.306-90.1.el9_2
                                                                rhel-9-for-x86_64-baseos-rpms    846 k
```

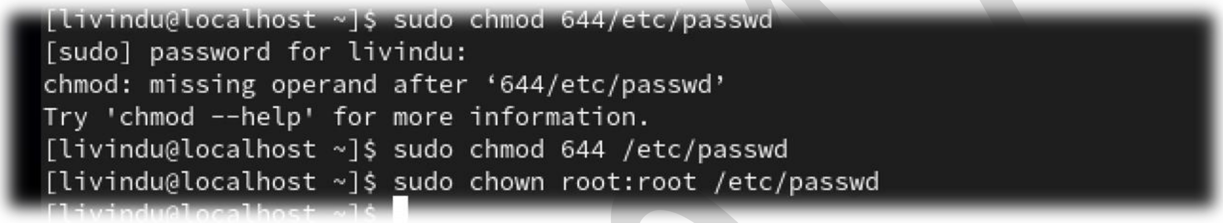
4. Configure Strict Filesystem Permissions

Configuration: Use chmod and chown to set appropriate permissions and ownership on files and directories.

Why It Increases Security: Prevents unauthorized access and modification of system files and directories.

Protection Against: Unauthorized file access, data tampering, and privilege escalation.

*(**Commands** - chmod 750 /important/directory*
chown root:root /important/file)



```
[livindu@localhost ~]$ sudo chmod 644/etc/passwd
[sudo] password for livindu:
chmod: missing operand after ‘644/etc/passwd’
Try 'chmod --help' for more information.
[livindu@localhost ~]$ sudo chmod 644 /etc/passwd
[livindu@localhost ~]$ sudo chown root:root /etc/passwd
[livindu@localhost ~]$
```

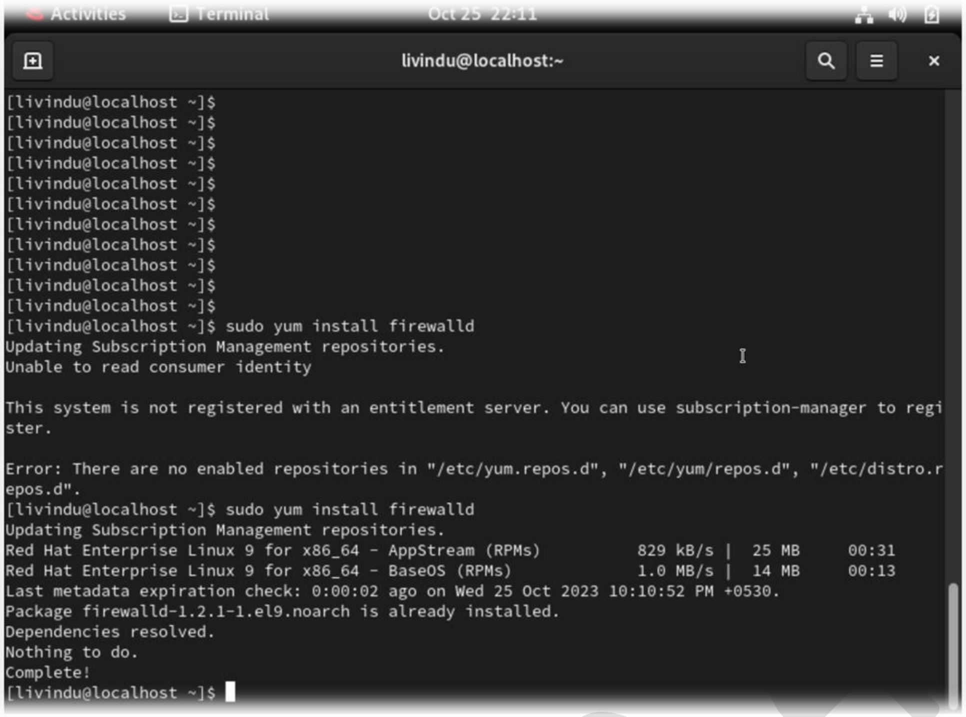
5. Implement a Firewall

Configuration: Use firewalld to configure and manage firewall settings.

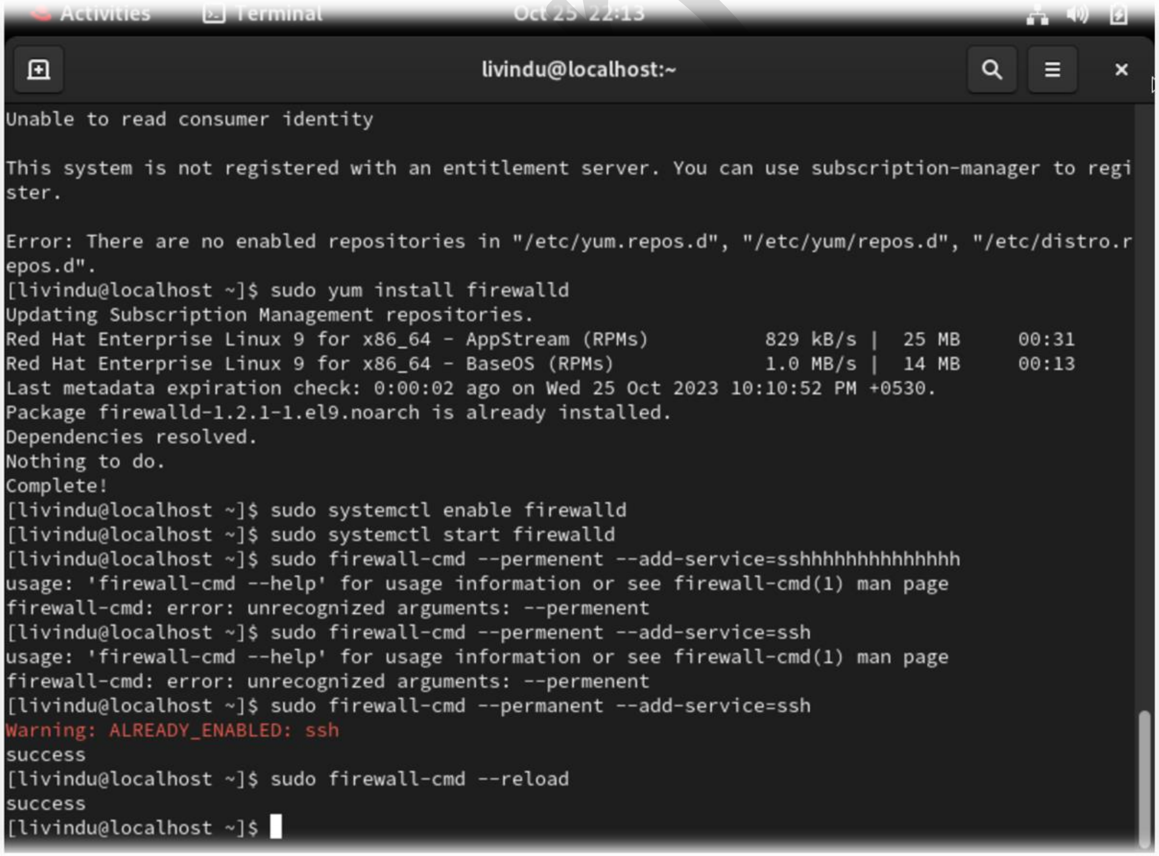
Why It Increases Security: Controls incoming and outgoing network traffic based on security policies.

Protection Against: Unauthorized network access, port scanning, and DoS attacks.

*(**Commands** - firewall-cmd --permanent --add-service=http*
firewall-cmd –reload)



```
[livindu@localhost ~]$
[livindu@localhost ~]$
[livindu@localhost ~]$
[livindu@localhost ~]$
[livindu@localhost ~]$
[livindu@localhost ~]$
[livindu@localhost ~]$
[livindu@localhost ~]$
[livindu@localhost ~]$
[livindu@localhost ~]$
[livindu@localhost ~]$
[livindu@localhost ~]$ sudo yum install firewalld
Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can use subscription-manager to regi
ster.

Error: There are no enabled repositories in "/etc/yum.repos.d", "/etc/yum/repos.d", "/etc/distro.r
epos.d".
[livindu@localhost ~]$ sudo yum install firewalld
Updating Subscription Management repositories.
Red Hat Enterprise Linux 9 for x86_64 - AppStream (RPMs)          829 kB/s |  25 MB     00:31
Red Hat Enterprise Linux 9 for x86_64 - BaseOS (RPMs)             1.0 MB/s |  14 MB     00:13
Last metadata expiration check: 0:00:02 ago on Wed 25 Oct 2023 10:10:52 PM +0530.
Package firewalld-1.2.1-1.el9.noarch is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[livindu@localhost ~]$
```



```
Unable to read consumer identity

This system is not registered with an entitlement server. You can use subscription-manager to regi
ster.

Error: There are no enabled repositories in "/etc/yum.repos.d", "/etc/yum/repos.d", "/etc/distro.r
epos.d".
[livindu@localhost ~]$ sudo yum install firewalld
Updating Subscription Management repositories.
Red Hat Enterprise Linux 9 for x86_64 - AppStream (RPMs)          829 kB/s |  25 MB     00:31
Red Hat Enterprise Linux 9 for x86_64 - BaseOS (RPMs)             1.0 MB/s |  14 MB     00:13
Last metadata expiration check: 0:00:02 ago on Wed 25 Oct 2023 10:10:52 PM +0530.
Package firewalld-1.2.1-1.el9.noarch is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[livindu@localhost ~]$ sudo systemctl enable firewalld
[livindu@localhost ~]$ sudo systemctl start firewalld
[livindu@localhost ~]$ sudo firewall-cmd --permenent --add-service=sshhhhhhhhhhhhhh
usage: 'firewall-cmd --help' for usage information or see firewall-cmd(1) man page
firewall-cmd: error: unrecognized arguments: --permenent
[livindu@localhost ~]$ sudo firewall-cmd --permenent --add-service=ssh
usage: 'firewall-cmd --help' for usage information or see firewall-cmd(1) man page
firewall-cmd: error: unrecognized arguments: --permenent
[livindu@localhost ~]$ sudo firewall-cmd --permanent --add-service=ssh
Warning: ALREADY_ENABLED: ssh
success
[livindu@localhost ~]$ sudo firewall-cmd --reload
success
[livindu@localhost ~]$
```

6. Use SSH Keys for Authentication

Configuration: Disable password authentication for SSH and use key-based authentication instead.

Why It Increases Security: Adds an additional layer of security for remote access.

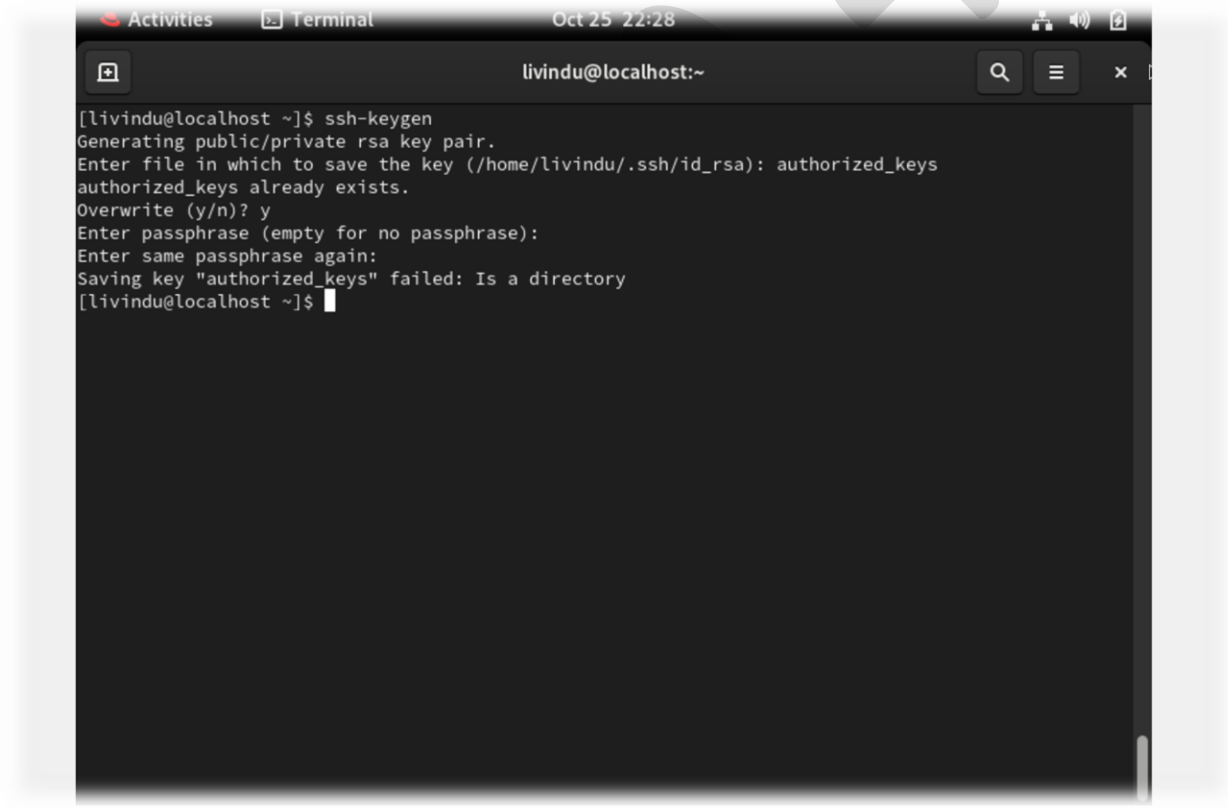
Protection Against: Brute force attacks on SSH passwords and unauthorized remote access.

*(**Commands** - Edit /etc/ssh/sshd_config and set:*

PasswordAuthentication no
PubkeyAuthentication yes

Then restart SSH service:

systemctl restart sshd)



```
[livindu@localhost ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/livindu/.ssh/id_rsa): authorized_keys
authorized_keys already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Saving key "authorized_keys" failed: Is a directory
[livindu@localhost ~]$
```

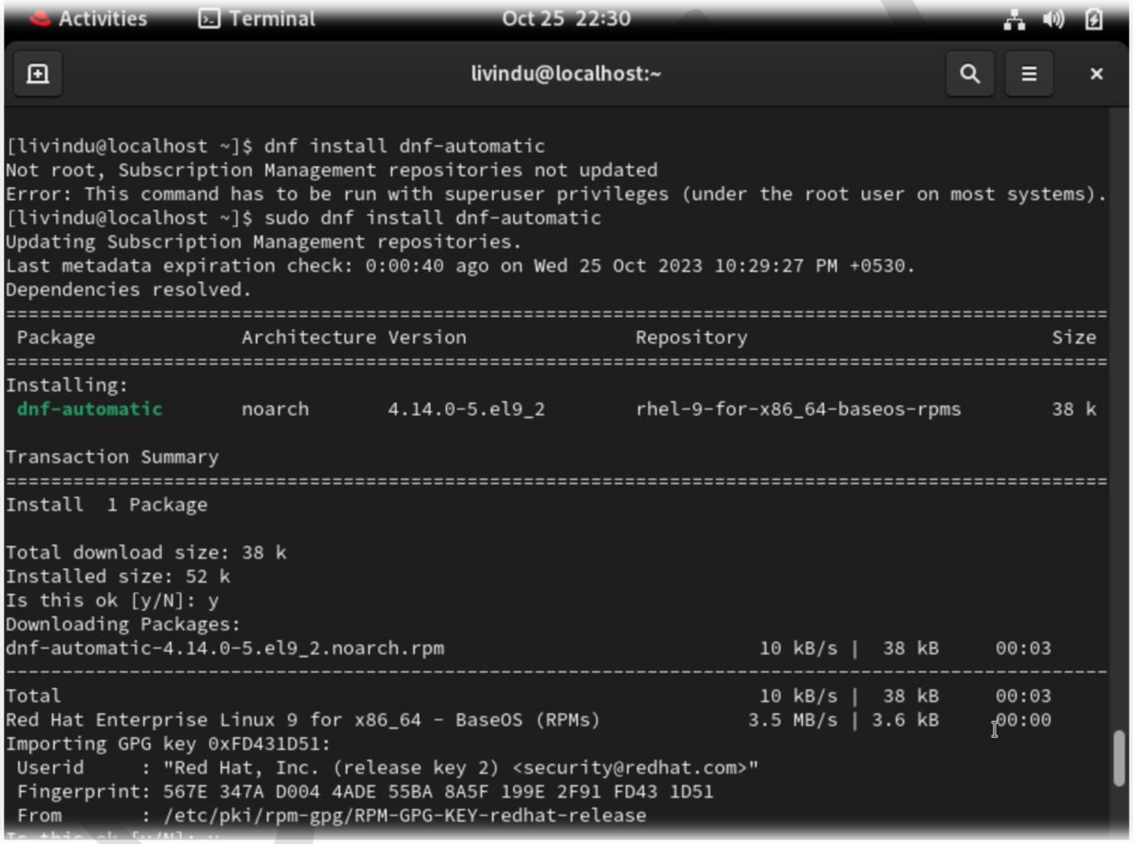
7. Regularly Apply Security Patches

Configuration: Enable automatic security updates using yum-cron or dnf-automatic.

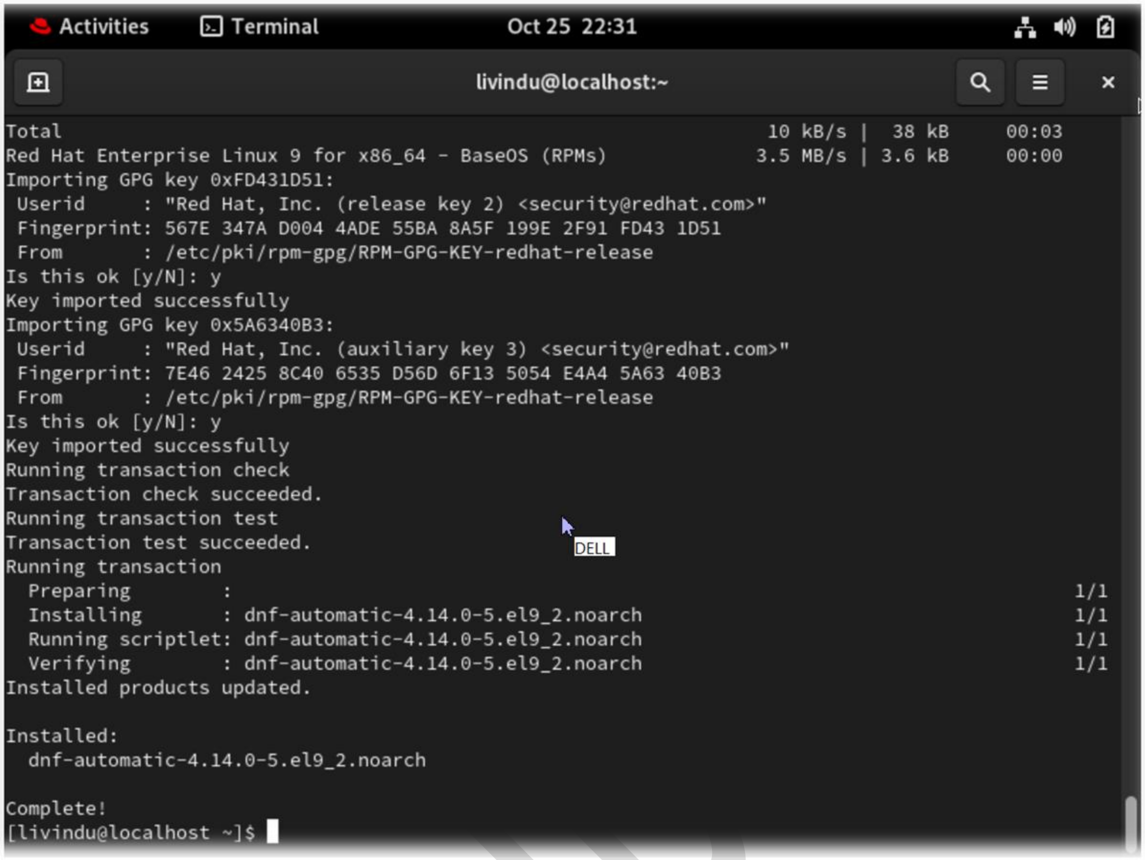
Why It Increases Security: Ensures that the system is promptly updated to protect against known vulnerabilities.

Protection Against: Exploitation of known vulnerabilities.

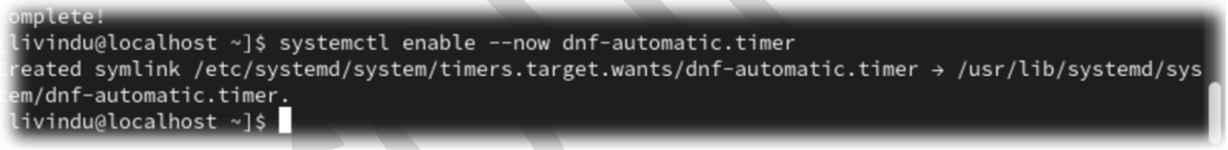
*(**Commands** - dnf install dnf-automatic*
systemctl enable --now dnf-automatic.timer)



```
[livindu@localhost ~]$ dnf install dnf-automatic
Not root, Subscription Management repositories not updated
Error: This command has to be run with superuser privileges (under the root user on most systems).
[livindu@localhost ~]$ sudo dnf install dnf-automatic
Updating Subscription Management repositories.
Last metadata expiration check: 0:00:40 ago on Wed 25 Oct 2023 10:29:27 PM +0530.
Dependencies resolved.
===================================================================================================
 Package               Architecture Version              Repository                           Size
===================================================================================================
Installing:
 dnf-automatic         noarch       4.14.0-5.el9_2       rhel-9-for-x86_64-baseos-rpms        38 k

Transaction Summary
===================================================================================================
Install  1 Package

Total download size: 38 k
Installed size: 52 k
Is this ok [y/N]: y
Downloading Packages:
dnf-automatic-4.14.0-5.el9_2.noarch.rpm                              10 kB/s |  38 kB     00:03
---------------------------------------------------------------------------------------------------
Total                                                                10 kB/s |  38 kB     00:03
Red Hat Enterprise Linux 9 for x86_64 - BaseOS (RPMs)               3.5 MB/s | 3.6 kB     00:00
Importing GPG key 0xFD431D51:
 Userid     : "Red Hat, Inc. (release key 2) <security@redhat.com>"
 Fingerprint: 567E 347A D004 4ADE 55BA 8A5F 199E 2F91 FD43 1D51
 From       : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Is this ok [y/N]: y
```



```
Total                                                    10 kB/s |  38 kB     00:03
Red Hat Enterprise Linux 9 for x86_64 - BaseOS (RPMs)   3.5 MB/s | 3.6 kB     00:00
Importing GPG key 0xFD431D51:
 Userid     : "Red Hat, Inc. (release key 2) <security@redhat.com>"
 Fingerprint: 567E 347A D004 4ADE 55BA 8A5F 199E 2F91 FD43 1D51
 From       : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Is this ok [y/N]: y
Key imported successfully
Importing GPG key 0x5A6340B3:
 Userid     : "Red Hat, Inc. (auxiliary key 3) <security@redhat.com>"
 Fingerprint: 7E46 2425 8C40 6535 D56D 6F13 5054 E4A4 5A63 40B3
 From       : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Is this ok [y/N]: y
Key imported successfully
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                           1/1
  Installing       : dnf-automatic-4.14.0-5.el9_2.noarch                       1/1
  Running scriptlet: dnf-automatic-4.14.0-5.el9_2.noarch                       1/1
  Verifying        : dnf-automatic-4.14.0-5.el9_2.noarch                       1/1
Installed products updated.

Installed:
  dnf-automatic-4.14.0-5.el9_2.noarch

Complete!
[livindu@localhost ~]$
```



```
omplete!
livindu@localhost ~]$ systemctl enable --now dnf-automatic.timer
reated symlink /etc/systemd/system/timers.target.wants/dnf-automatic.timer → /usr/lib/systemd/sys
em/dnf-automatic.timer.
livindu@localhost ~]$
```

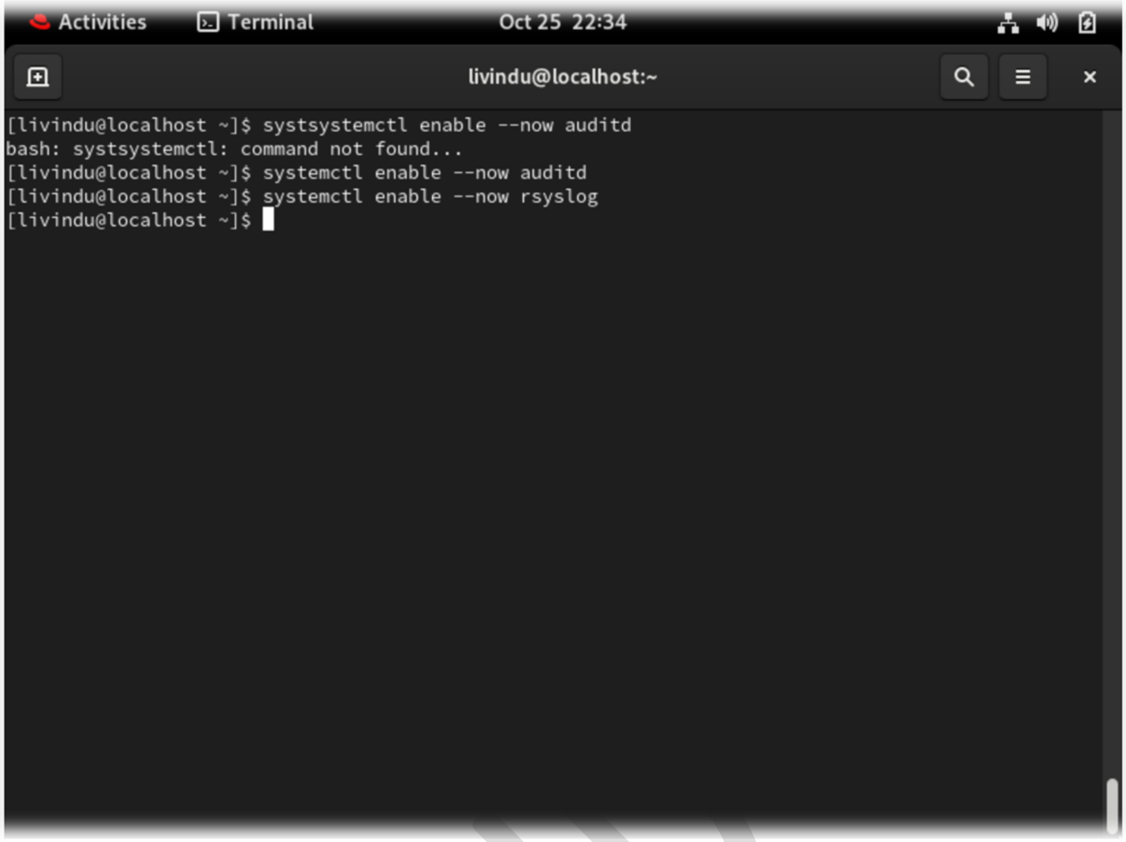
8. Enable, Configure Auditing and Logging

Configuration: Use audited for auditing and make sure that rsyslog is configured for system logging.

Why It Increases Security: Allows for monitoring of system activity and potential security incidents.

Protection Against: Undetected malicious activity and unauthorized access.

*(**Commands** - systemctl enable --now auditd*
systemctl enable --now rsyslog)



```
[livindu@localhost ~]$ systsystemctl enable --now auditd
bash: systsystemctl: command not found...
[livindu@localhost ~]$ systemctl enable --now auditd
[livindu@localhost ~]$ systemctl enable --now rsyslog
[livindu@localhost ~]$ 
```

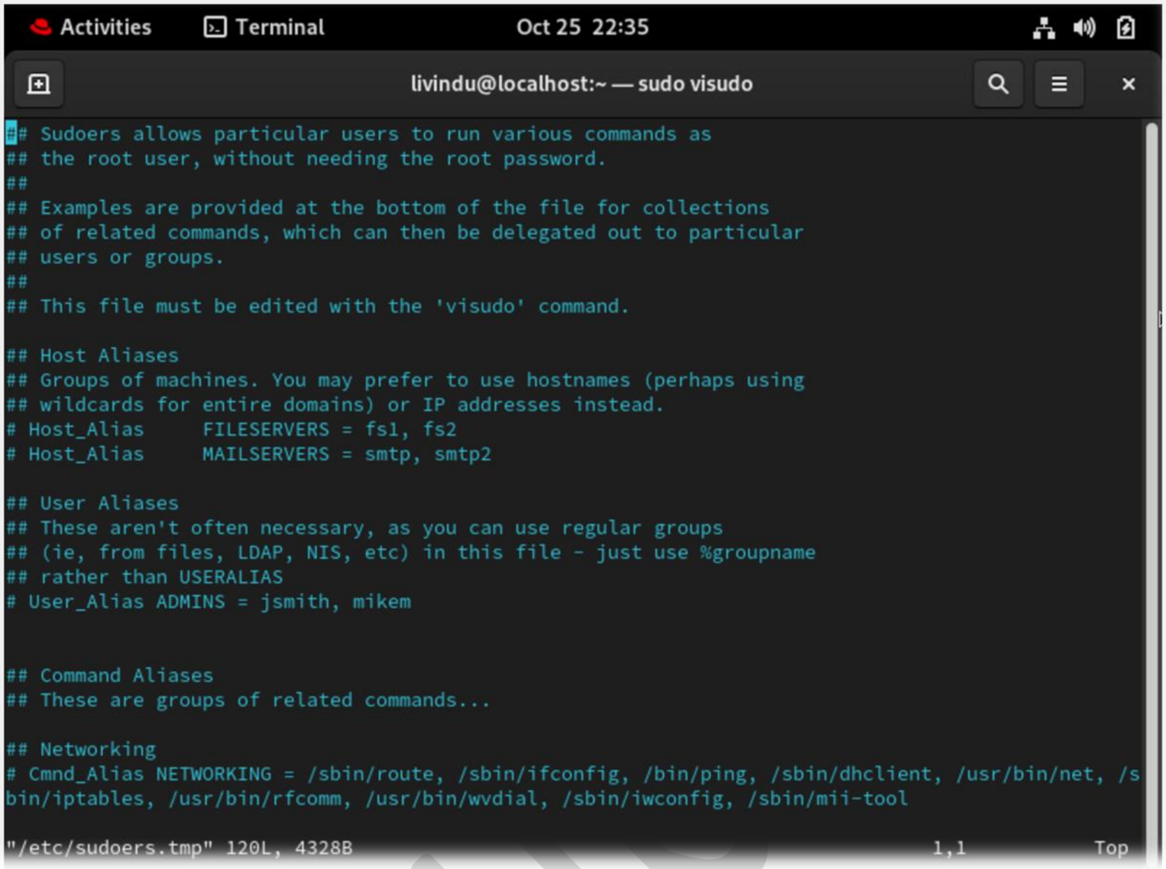
9. Limit User Privileges

Configuration: Assign users only the minimum required privileges and use sudo for administrative tasks.

Why It Increases Security: Prevents unauthorized access and limits the potential damage from compromised accounts.

Protection Against: Privilege escalation and unauthorized system changes.

*(**Commands -** Edit /etc/sudoers or use visudo to add necessary user privileges.)*



```
## Sudoers allows particular users to run various commands as
## the root user, without needing the root password.
##
## Examples are provided at the bottom of the file for collections
## of related commands, which can then be delegated out to particular
## users or groups.
##
## This file must be edited with the 'visudo' command.

## Host Aliases
## Groups of machines. You may prefer to use hostnames (perhaps using
## wildcards for entire domains) or IP addresses instead.
# Host_Alias     FILESERVERS = fs1, fs2
# Host_Alias     MAILSERVERS = smtp, smtp2

## User Aliases
## These aren't often necessary, as you can use regular groups
## (ie, from files, LDAP, NIS, etc) in this file - just use %groupname
## rather than USERALIAS
# User_Alias ADMINS = jsmith, mikem


## Command Aliases
## These are groups of related commands...

## Networking
# Cmnd_Alias NETWORKING = /sbin/route, /sbin/ifconfig, /bin/ping, /sbin/dhclient, /usr/bin/net, /s
bin/iptables, /usr/bin/rfcomm, /usr/bin/wvdial, /sbin/iwconfig, /sbin/mii-tool

"/etc/sudoers.tmp" 120L, 4328B                                              1,1          Top
```

10. Secure SSH Settings

Configuration: Edit the /etc/ssh/sshd_config file to disable root login, permit only protocol 2, and other security enhancements.

Why It Increases Security: Ensures secure and encrypted communications for remote administration.

Protection Against: MIMA attacks, eavesdropping, and unauthorized remote access attacks.

***(Commands** - Edit /etc/ssh/sshd_config to include:*

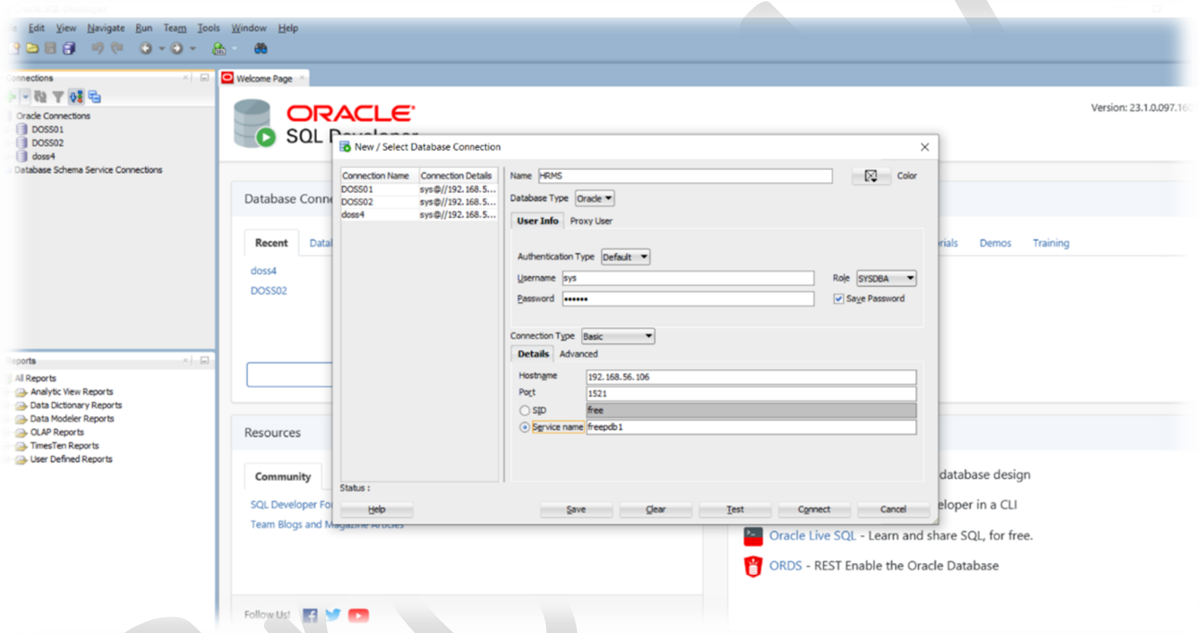
PermitRootLogin no
Protocol 2
X11Forwarding no

Then restart SSH service:

systemctl restart sshd)

Task 02 -Database Security

Oracle DB and SQL Developer Configs.



New / Select Database Connection

Connection Name	Connection Details
DOSS01	sys@//192.168.5...
DOSS02	sys@//192.168.5...
doss4	sys@//192.168.5...

Name: HRMS

Database Type: Oracle

User Info | Proxy User

Authentication Type: Default

Username: sys

Role: SYSDBA

Password: ••••••

☑ Save Password

Connection Type: Basic

Details | Advanced

Hostname: 192.168.56.106

Port: 1521

○ SID: free

● Service name: freepdb1

Status :

Configurations to Harden the DB Developer.

1. Update System Packages

Why: Ensuring that all packages are up to date is crucial as it patches known vulnerabilities in the system.

Protection Against: Various types of vulnerabilities and exploits present in outdated packages.

Command:

```
sudo dnf update -y
```

2. Configure Firewall

Why: A firewall helps protect your system from unauthorized access and can filter out malicious traffic.

Protection Against: Unauthorized access and network-based attacks.

Command:

```
sudo systemctl enable firewalld
sudo systemctl start firewalld
sudo firewall-cmd --set-default-zone=public
sudo firewall-cmd --add-service={http,https,ssh} --permanent
sudo firewall-cmd –reload
```

3. Disable Root SSH Login

Why: Preventing direct root access over SSH mitigates the risk of brute force attacks.

Protection Against: Brute force and unauthorized access.

Configuration File: /etc/ssh/sshd_config

```
PermitRootLogin no
```

Then restart the SSH service:

```
sudo systemctl restart sshd
```

4. Configure SELinux

Why: SELinux provides an additional layer of access control, ensuring processes run with the minimum necessary privileges.

Protection Against: Unauthorized access and privilege escalation.

Command:

```
sudo setenforce 1
```

Make sure it's enabled on boot in /etc/selinux/config:

```
SELINUX=enforcing
```

5. Secure Boot Settings

Why: Secure Boot ensures that only signed bootloaders and kernels can be executed during system startup.

Protection Against: Boot-time attacks and rootkits.

Configuration: Ensure Secure Boot is enabled in your system's BIOS/UEFI settings.

6. Remove Unnecessary Services and Packages

Why: Reducing the attack surface by removing unnecessary packages and services.

Protection Against: Various types of attacks depending on the services/packages removed.

Command:

```
sudo dnf remove package-name
```

7. Configure Strong Password Policies

Why: Ensuring strong password policies prevents easy password cracking.

Protection Against: Brute force and dictionary attacks.

Configuration File: /etc/security/pwquality.conf

```
minlen = 14
minclass = 4
```

And in /etc/login.defs:

```
PASS_MAX_DAYS 90
PASS_MIN_DAYS 7
PASS_WARN_AGE 14
```

8. Regularly Audit and Monitor System Logs

Why: Regular auditing helps in detecting any suspicious activities early.

Protection Against: Unauthorized access, and it helps in post-incident investigations.

Tools: Auditd, rsyslog

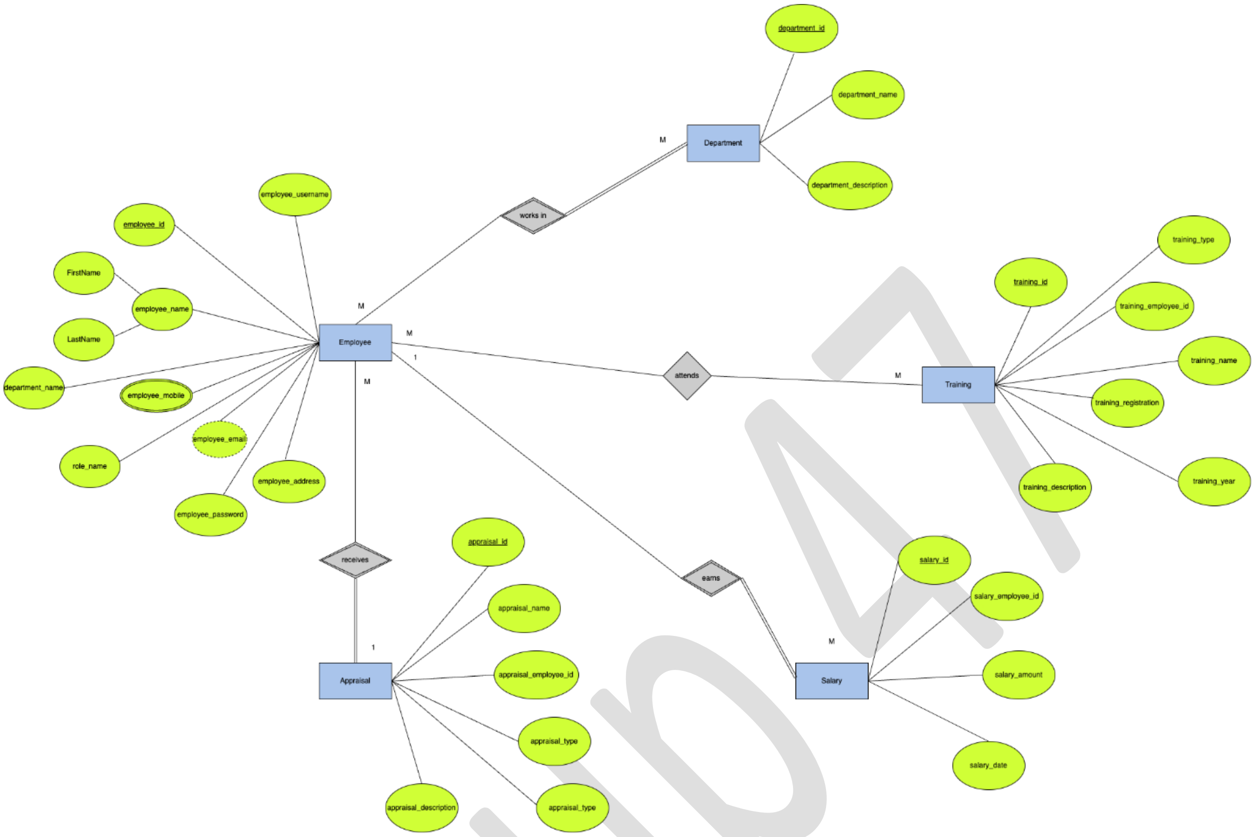
Command:

```
sudo dnf install auditd
sudo systemctl enable auditd
sudo systemctl start auditd
```

For Oracle Database Specific:

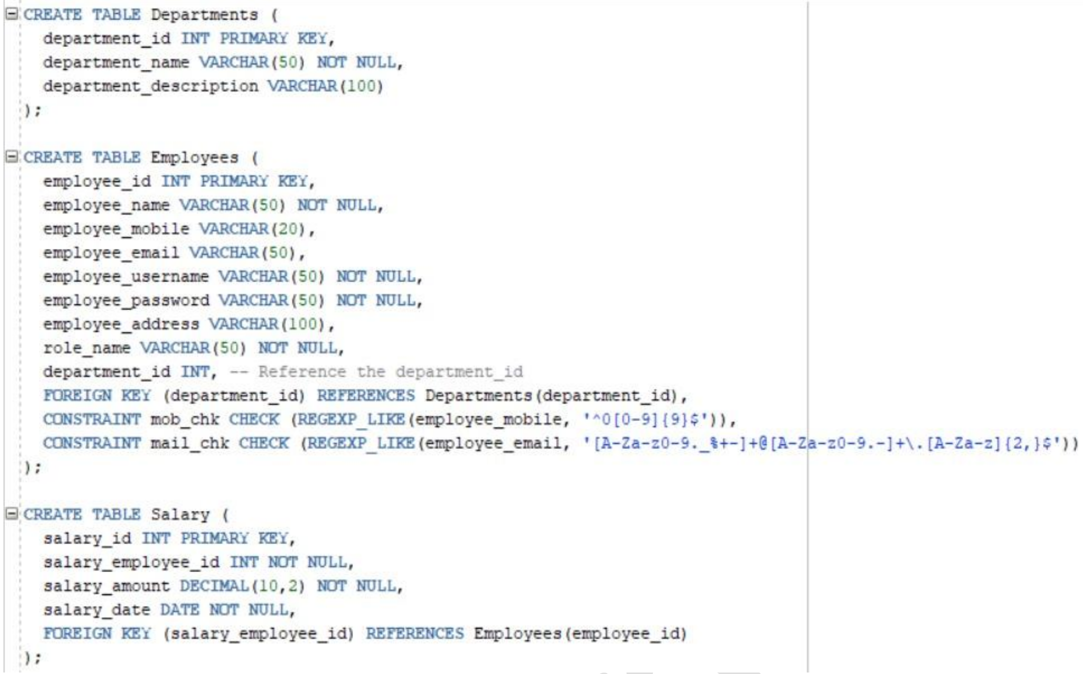
- Ensure Oracle's own user privileges are restricted.
- Regularly update Oracle software to patch any vulnerabilities.
- Limit network access to Oracle services.

Entity Relationship Diagram (ERD)

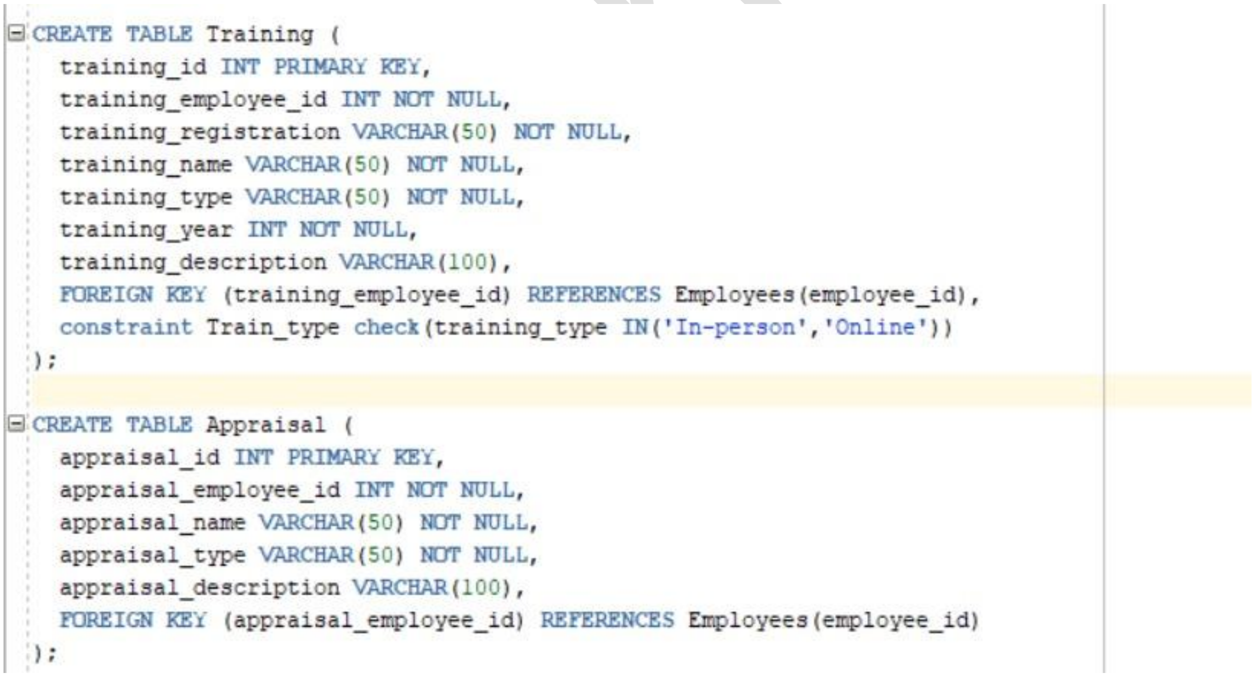


SQL Codes (Table creation and Data Inserting)

Table creation.

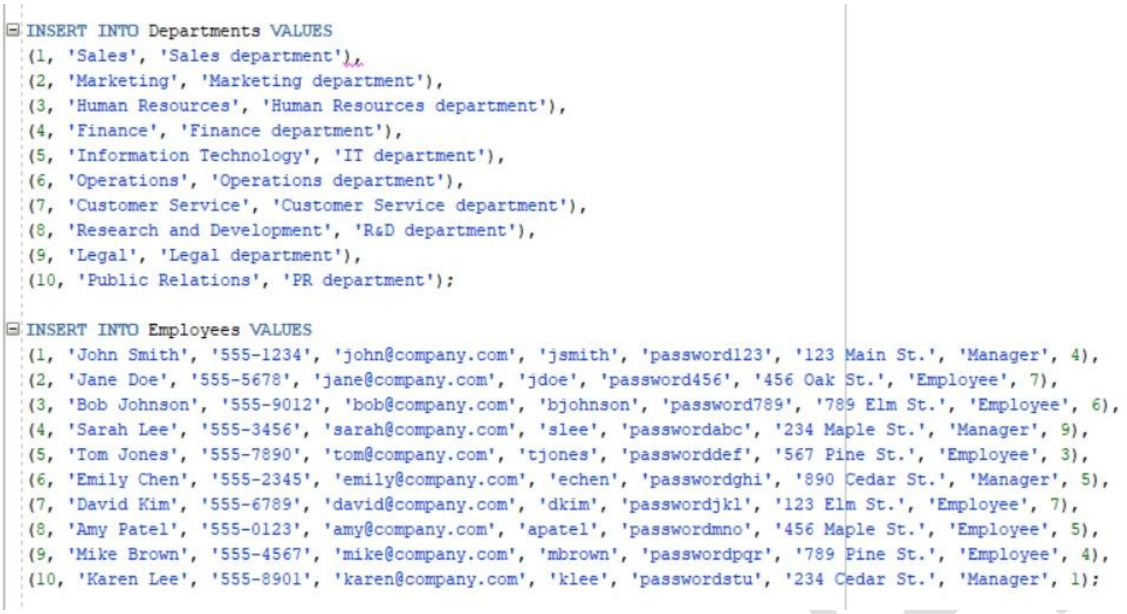


```sql
CREATE TABLE Departments (
  department_id INT PRIMARY KEY,
  department_name VARCHAR(50) NOT NULL,
  department_description VARCHAR(100)
);

CREATE TABLE Employees (
  employee_id INT PRIMARY KEY,
  employee_name VARCHAR(50) NOT NULL,
  employee_mobile VARCHAR(20),
  employee_email VARCHAR(50),
  employee_username VARCHAR(50) NOT NULL,
  employee_password VARCHAR(50) NOT NULL,
  employee_address VARCHAR(100),
  role_name VARCHAR(50) NOT NULL,
  department_id INT, -- Reference the department_id
  FOREIGN KEY (department_id) REFERENCES Departments(department_id),
  CONSTRAINT mob_chk CHECK (REGEXP_LIKE(employee_mobile, '^0[0-9]{9}$')),
  CONSTRAINT mail_chk CHECK (REGEXP_LIKE(employee_email, '[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,}$'))
);

CREATE TABLE Salary (
  salary_id INT PRIMARY KEY,
  salary_employee_id INT NOT NULL,
  salary_amount DECIMAL(10,2) NOT NULL,
  salary_date DATE NOT NULL,
  FOREIGN KEY (salary_employee_id) REFERENCES Employees(employee_id)
);
```

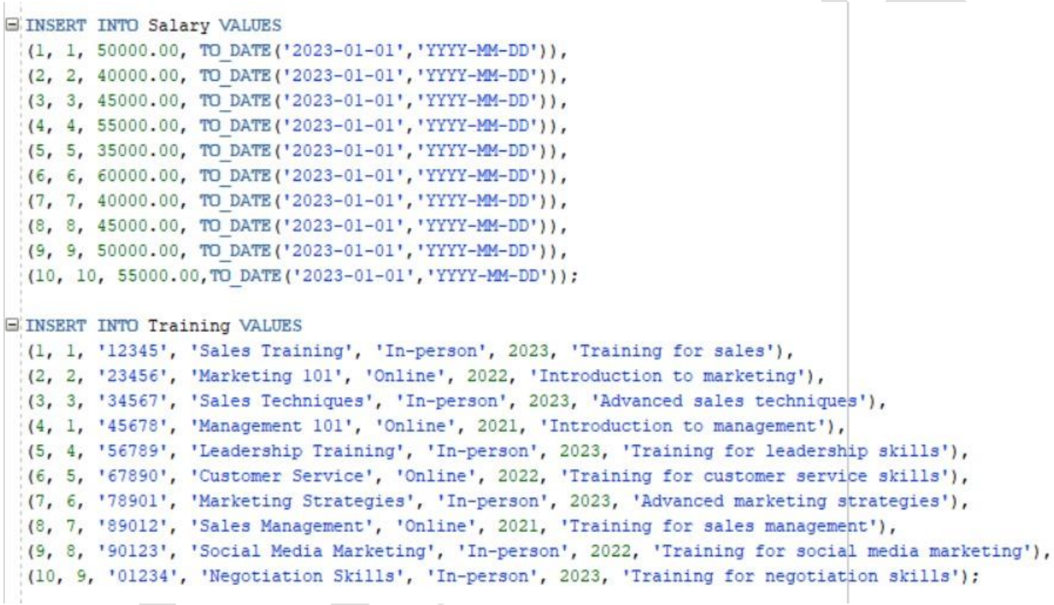


```sql
CREATE TABLE Training (
  training_id INT PRIMARY KEY,
  training_employee_id INT NOT NULL,
  training_registration VARCHAR(50) NOT NULL,
  training_name VARCHAR(50) NOT NULL,
  training_type VARCHAR(50) NOT NULL,
  training_year INT NOT NULL,
  training_description VARCHAR(100),
  FOREIGN KEY (training_employee_id) REFERENCES Employees(employee_id),
  constraint Train_type check(training_type IN('In-person','Online'))
);

CREATE TABLE Appraisal (
  appraisal_id INT PRIMARY KEY,
  appraisal_employee_id INT NOT NULL,
  appraisal_name VARCHAR(50) NOT NULL,
  appraisal_type VARCHAR(50) NOT NULL,
  appraisal_description VARCHAR(100),
  FOREIGN KEY (appraisal_employee_id) REFERENCES Employees(employee_id)
);
```

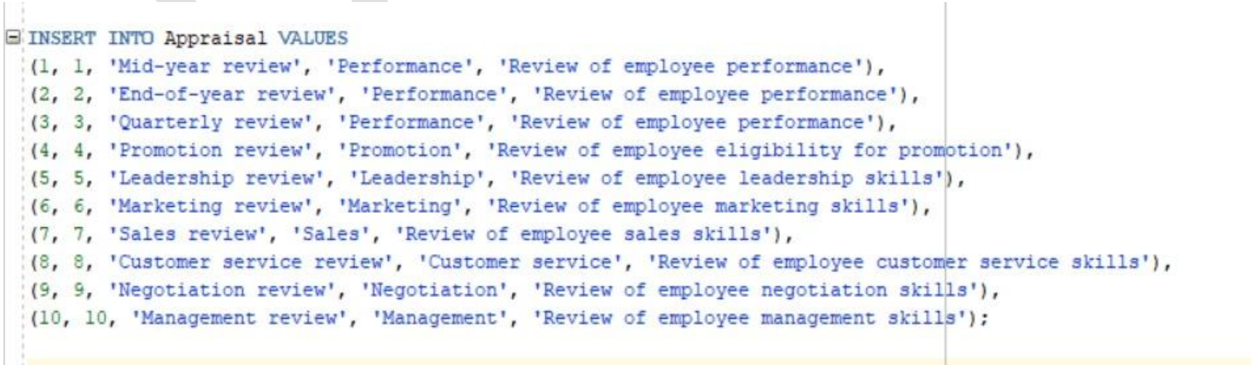
Data Inserting.



```
INSERT INTO Departments VALUES
(1, 'Sales', 'Sales department'),
(2, 'Marketing', 'Marketing department'),
(3, 'Human Resources', 'Human Resources department'),
(4, 'Finance', 'Finance department'),
(5, 'Information Technology', 'IT department'),
(6, 'Operations', 'Operations department'),
(7, 'Customer Service', 'Customer Service department'),
(8, 'Research and Development', 'R&D department'),
(9, 'Legal', 'Legal department'),
(10, 'Public Relations', 'PR department');

INSERT INTO Employees VALUES
(1, 'John Smith', '555-1234', 'john@company.com', 'jsmith', 'password123', '123 Main St.', 'Manager', 4),
(2, 'Jane Doe', '555-5678', 'jane@company.com', 'jdoe', 'password456', '456 Oak St.', 'Employee', 7),
(3, 'Bob Johnson', '555-9012', 'bob@company.com', 'bjohnson', 'password789', '789 Elm St.', 'Employee', 6),
(4, 'Sarah Lee', '555-3456', 'sarah@company.com', 'slee', 'passwordabc', '234 Maple St.', 'Manager', 9),
(5, 'Tom Jones', '555-7890', 'tom@company.com', 'tjones', 'passworddef', '567 Pine St.', 'Employee', 3),
(6, 'Emily Chen', '555-2345', 'emily@company.com', 'echen', 'passwordghi', '890 Cedar St.', 'Manager', 5),
(7, 'David Kim', '555-6789', 'david@company.com', 'dkim', 'passwordjkl', '123 Elm St.', 'Employee', 7),
(8, 'Amy Patel', '555-0123', 'amy@company.com', 'apatel', 'passwordmno', '456 Maple St.', 'Employee', 5),
(9, 'Mike Brown', '555-4567', 'mike@company.com', 'mbrown', 'passwordpqr', '789 Pine St.', 'Employee', 4),
(10, 'Karen Lee', '555-8901', 'karen@company.com', 'klee', 'passwordstu', '234 Cedar St.', 'Manager', 1);
```

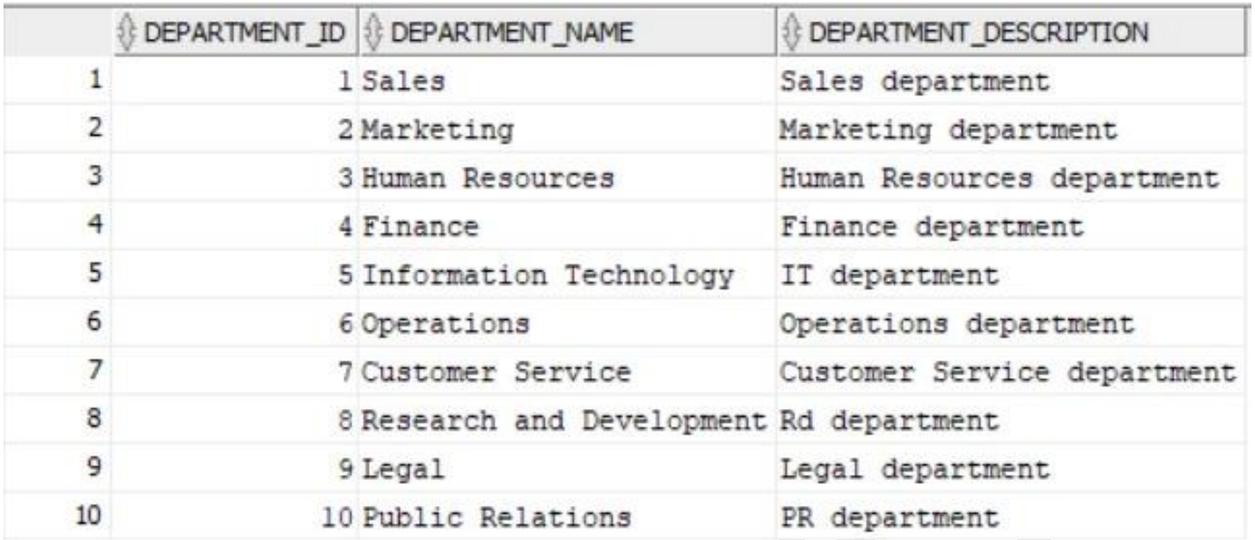


```
INSERT INTO Salary VALUES
(1, 1, 50000.00, TO_DATE('2023-01-01','YYYY-MM-DD')),
(2, 2, 40000.00, TO_DATE('2023-01-01','YYYY-MM-DD')),
(3, 3, 45000.00, TO_DATE('2023-01-01','YYYY-MM-DD')),
(4, 4, 55000.00, TO_DATE('2023-01-01','YYYY-MM-DD')),
(5, 5, 35000.00, TO_DATE('2023-01-01','YYYY-MM-DD')),
(6, 6, 60000.00, TO_DATE('2023-01-01','YYYY-MM-DD')),
(7, 7, 40000.00, TO_DATE('2023-01-01','YYYY-MM-DD')),
(8, 8, 45000.00, TO_DATE('2023-01-01','YYYY-MM-DD')),
(9, 9, 50000.00, TO_DATE('2023-01-01','YYYY-MM-DD')),
(10, 10, 55000.00,TO_DATE('2023-01-01','YYYY-MM-DD'));

INSERT INTO Training VALUES
(1, 1, '12345', 'Sales Training', 'In-person', 2023, 'Training for sales'),
(2, 2, '23456', 'Marketing 101', 'Online', 2022, 'Introduction to marketing'),
(3, 3, '34567', 'Sales Techniques', 'In-person', 2023, 'Advanced sales techniques'),
(4, 1, '45678', 'Management 101', 'Online', 2021, 'Introduction to management'),
(5, 4, '56789', 'Leadership Training', 'In-person', 2023, 'Training for leadership skills'),
(6, 5, '67890', 'Customer Service', 'Online', 2022, 'Training for customer service skills'),
(7, 6, '78901', 'Marketing Strategies', 'In-person', 2023, 'Advanced marketing strategies'),
(8, 7, '89012', 'Sales Management', 'Online', 2021, 'Training for sales management'),
(9, 8, '90123', 'Social Media Marketing', 'In-person', 2022, 'Training for social media marketing'),
(10, 9, '01234', 'Negotiation Skills', 'In-person', 2023, 'Training for negotiation skills');
```

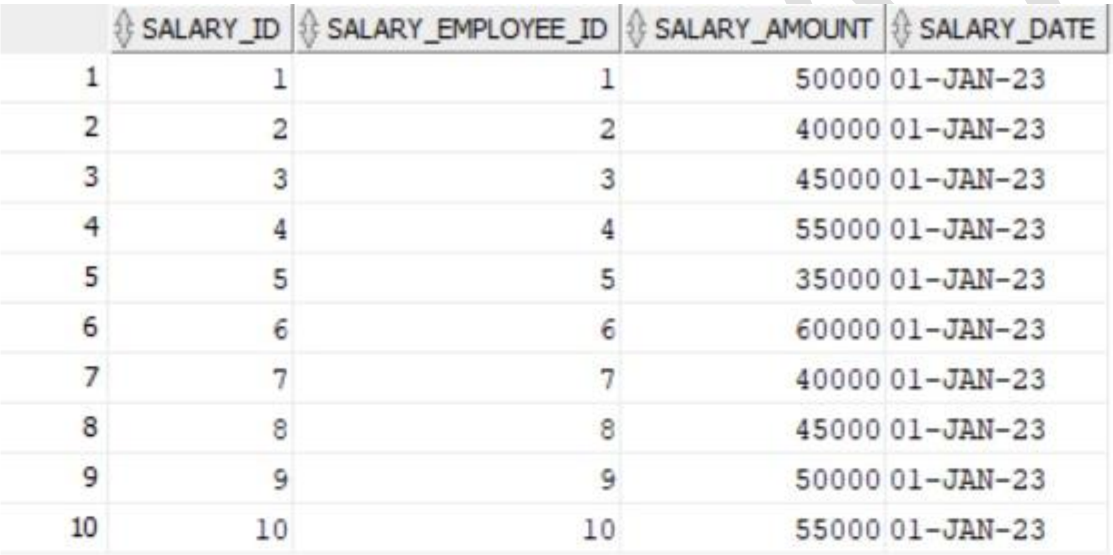


```
INSERT INTO Appraisal VALUES
(1, 1, 'Mid-year review', 'Performance', 'Review of employee performance'),
(2, 2, 'End-of-year review', 'Performance', 'Review of employee performance'),
(3, 3, 'Quarterly review', 'Performance', 'Review of employee performance'),
(4, 4, 'Promotion review', 'Promotion', 'Review of employee eligibility for promotion'),
(5, 5, 'Leadership review', 'Leadership', 'Review of employee leadership skills'),
(6, 6, 'Marketing review', 'Marketing', 'Review of employee marketing skills'),
(7, 7, 'Sales review', 'Sales', 'Review of employee sales skills'),
(8, 8, 'Customer service review', 'Customer service', 'Review of employee customer service skills'),
(9, 9, 'Negotiation review', 'Negotiation', 'Review of employee negotiation skills'),
(10, 10, 'Management review', 'Management', 'Review of employee management skills');
```

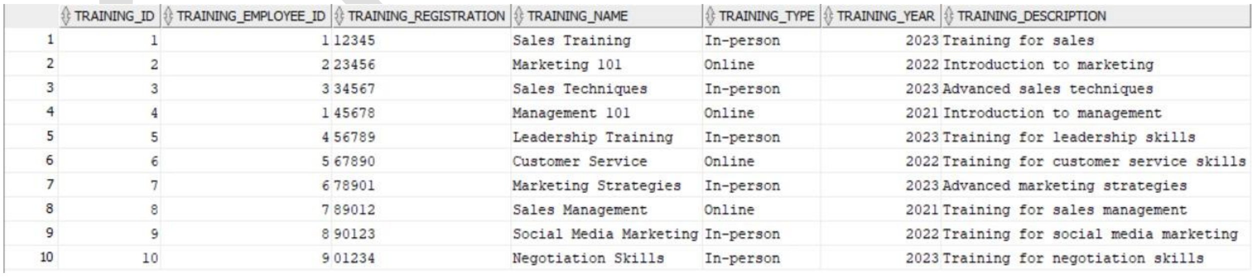
Results.



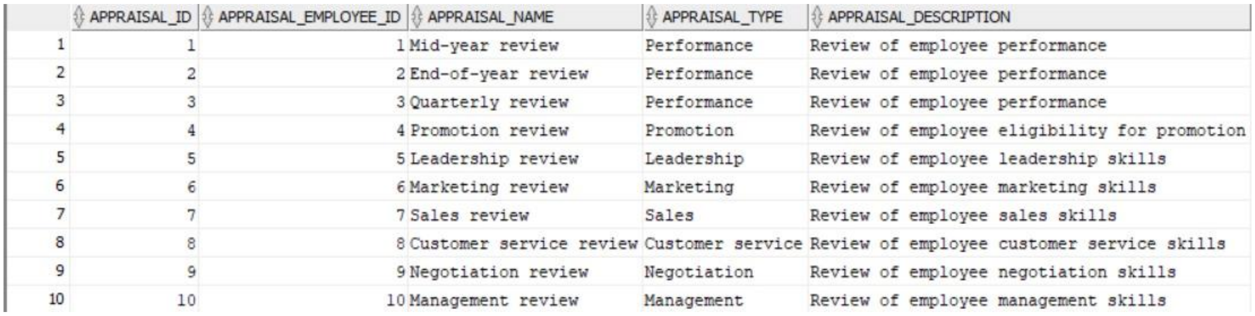
	DEPARTMENT_ID	DEPARTMENT_NAME	DEPARTMENT_DESCRIPTION
1	1	Sales	Sales department
2	2	Marketing	Marketing department
3	3	Human Resources	Human Resources department
4	4	Finance	Finance department
5	5	Information Technology	IT department
6	6	Operations	Operations department
7	7	Customer Service	Customer Service department
8	8	Research and Development	Rd department
9	9	Legal	Legal department
10	10	Public Relations	PR department



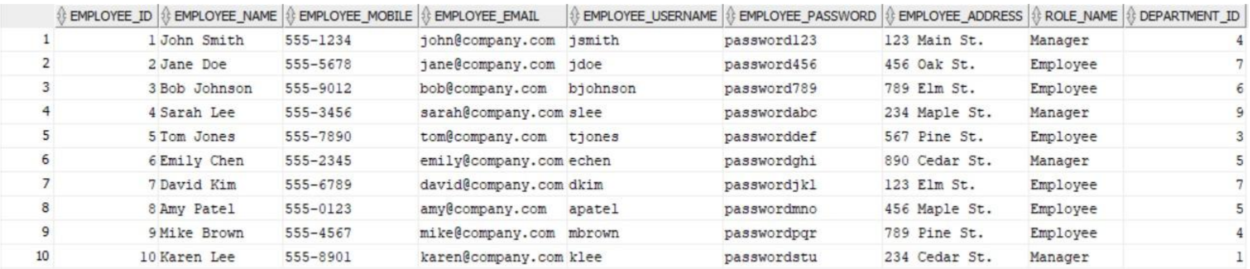
	SALARY_ID	SALARY_EMPLOYEE_ID	SALARY_AMOUNT	SALARY_DATE
1	1	1	50000	01-JAN-23
2	2	2	40000	01-JAN-23
3	3	3	45000	01-JAN-23
4	4	4	55000	01-JAN-23
5	5	5	35000	01-JAN-23
6	6	6	60000	01-JAN-23
7	7	7	40000	01-JAN-23
8	8	8	45000	01-JAN-23
9	9	9	50000	01-JAN-23
10	10	10	55000	01-JAN-23



	TRAINING_ID	TRAINING_EMPLOYEE_ID	TRAINING_REGISTRATION	TRAINING_NAME	TRAINING_TYPE	TRAINING_YEAR	TRAINING_DESCRIPTION
1	1	1	12345	Sales Training	In-person	2023	Training for sales
2	2	2	23456	Marketing 101	Online	2022	Introduction to marketing
3	3	3	34567	Sales Techniques	In-person	2023	Advanced sales techniques
4	4	1	45678	Management 101	Online	2021	Introduction to management
5	5	4	56789	Leadership Training	In-person	2023	Training for leadership skills
6	6	5	67890	Customer Service	Online	2022	Training for customer service skills
7	7	6	78901	Marketing Strategies	In-person	2023	Advanced marketing strategies
8	8	7	89012	Sales Management	Online	2021	Training for sales management
9	9	8	90123	Social Media Marketing	In-person	2022	Training for social media marketing
10	10	9	01234	Negotiation Skills	In-person	2023	Training for negotiation skills

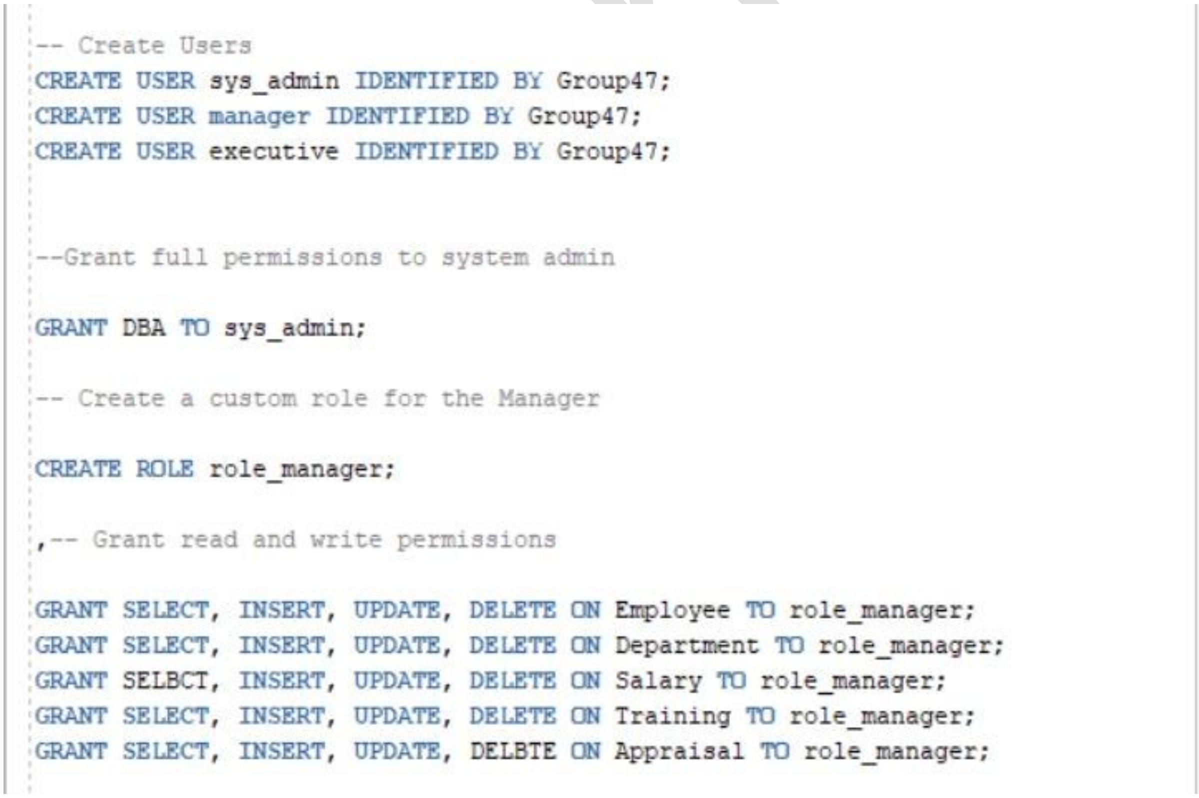


	APPRAISAL_ID	APPRAISAL_EMPLOYEE_ID	APPRAISAL_NAME	APPRAISAL_TYPE	APPRAISAL_DESCRIPTION
1	1	1	Mid-year review	Performance	Review of employee performance
2	2	2	End-of-year review	Performance	Review of employee performance
3	3	3	Quarterly review	Performance	Review of employee performance
4	4	4	Promotion review	Promotion	Review of employee eligibility for promotion
5	5	5	Leadership review	Leadership	Review of employee leadership skills
6	6	6	Marketing review	Marketing	Review of employee marketing skills
7	7	7	Sales review	Sales	Review of employee sales skills
8	8	8	Customer service review	Customer service	Review of employee customer service skills
9	9	9	Negotiation review	Negotiation	Review of employee negotiation skills
10	10	10	Management review	Management	Review of employee management skills

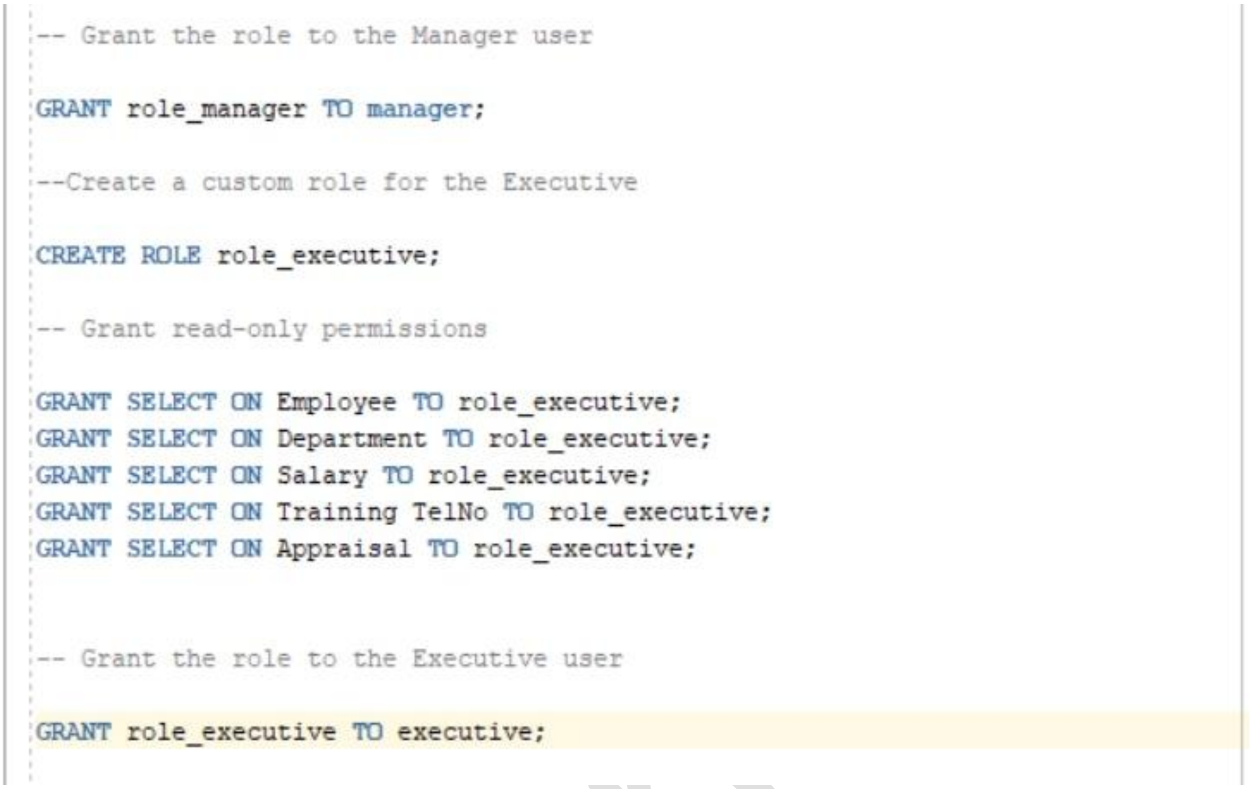


	EMPLOYEE_ID	EMPLOYEE_NAME	EMPLOYEE_MOBILE	EMPLOYEE_EMAIL	EMPLOYEE_USERNAME	EMPLOYEE_PASSWORD	EMPLOYEE_ADDRESS	ROLE_NAME	DEPARTMENT_ID
1	1	John Smith	555-1234	john@company.com	jsmith	password123	123 Main St.	Manager	4
2	2	Jane Doe	555-5678	jane@company.com	jdoe	password456	456 Oak St.	Employee	7
3	3	Bob Johnson	555-9012	bob@company.com	bjohnson	password789	789 Elm St.	Employee	6
4	4	Sarah Lee	555-3456	sarah@company.com	slee	passwordabc	234 Maple St.	Manager	9
5	5	Tom Jones	555-7890	tom@company.com	tjones	passworddef	567 Pine St.	Employee	3
6	6	Emily Chen	555-2345	emily@company.com	echen	passwordghi	890 Cedar St.	Manager	5
7	7	David Kim	555-6789	david@company.com	dkim	passwordjkl	123 Elm St.	Employee	7
8	8	Amy Patel	555-0123	amy@company.com	apatel	passwordmno	456 Maple St.	Employee	5
9	9	Mike Brown	555-4567	mike@company.com	mbrown	passwordpqr	789 Pine St.	Employee	4
10	10	Karen Lee	555-8901	karen@company.com	klee	passwordstu	234 Cedar St.	Manager	1

Creating user roles and granting permission.

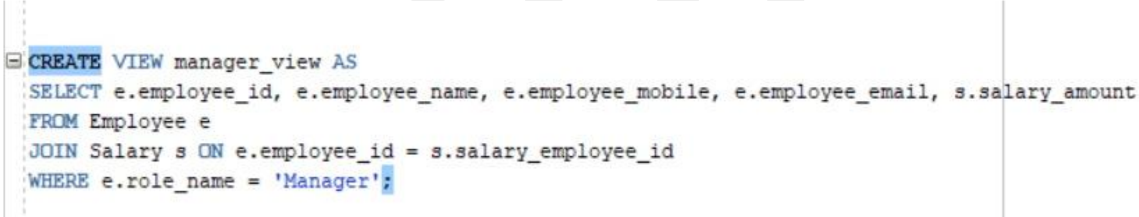


```
-- Create Users
CREATE USER sys_admin IDENTIFIED BY Group47;
CREATE USER manager IDENTIFIED BY Group47;
CREATE USER executive IDENTIFIED BY Group47;


--Grant full permissions to system admin

GRANT DBA TO sys_admin;

-- Create a custom role for the Manager

CREATE ROLE role_manager;

,-- Grant read and write permissions

GRANT SELECT, INSERT, UPDATE, DELETE ON Employee TO role_manager;
GRANT SELECT, INSERT, UPDATE, DELETE ON Department TO role_manager;
GRANT SELBCT, INSERT, UPDATE, DELETE ON Salary TO role_manager;
GRANT SELECT, INSERT, UPDATE, DELETE ON Training TO role_manager;
GRANT SELECT, INSERT, UPDATE, DELBTE ON Appraisal TO role_manager;
```



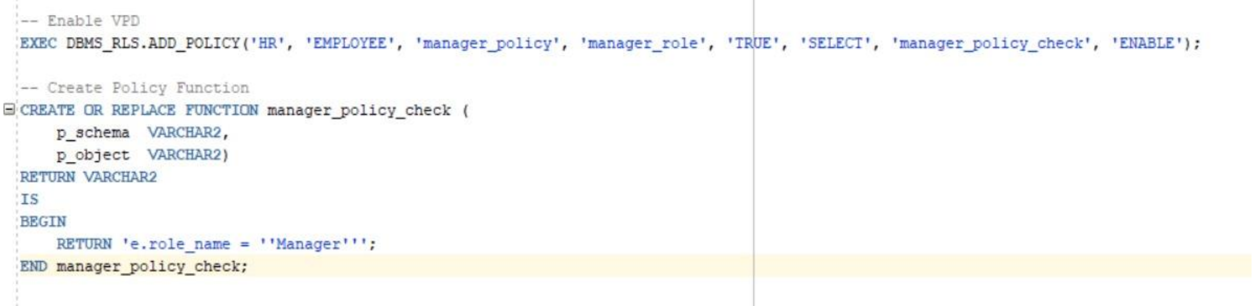
```
-- Grant the role to the Manager user

GRANT role_manager TO manager;

--Create a custom role for the Executive

CREATE ROLE role_executive;

-- Grant read-only permissions

GRANT SELECT ON Employee TO role_executive;
GRANT SELECT ON Department TO role_executive;
GRANT SELECT ON Salary TO role_executive;
GRANT SELECT ON Training TelNo TO role_executive;
GRANT SELECT ON Appraisal TO role_executive;


-- Grant the role to the Executive user

GRANT role_executive TO executive;
```

Creating a view for the Manager to View Employee details.



```
CREATE VIEW manager_view AS
SELECT e.employee_id, e.employee_name, e.employee_mobile, e.employee_email, s.salary_amount
FROM Employee e
JOIN Salary s ON e.employee_id = s.salary_employee_id
WHERE e.role_name = 'Manager';
```

Creating VPD.



```
-- Enable VPD
EXEC DBMS_RLS.ADD_POLICY('HR', 'EMPLOYEE', 'manager_policy', 'manager_role', 'TRUE', 'SELECT', 'manager_policy_check', 'ENABLE');

-- Create Policy Function
CREATE OR REPLACE FUNCTION manager_policy_check (
    p_schema  VARCHAR2,
    p_object  VARCHAR2)
RETURN VARCHAR2
IS
BEGIN
    RETURN 'e.role_name = ''Manager''';
END manager_policy_check;
```

Identifying Sensitive Information.

Sensitive information considered: "employee_mobile" and "employee_email" in the "Employee" table, containing personal contact and email information.

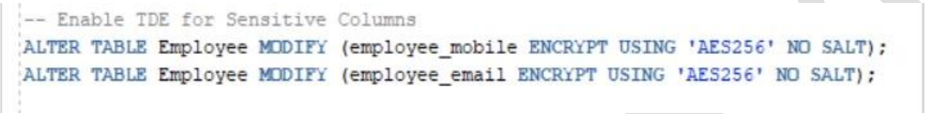
Encrypts these columns using Transparent Data Encryption (TDE) to protect data at rest.

Data Masking for Consulting Firm masks are part of email addresses for consulting firm users to maintain privacy while allowing access.

Fine-grained auditing policy Monitors and logs SELECT actions on these sensitive columns for security and accountability.

Encryption.

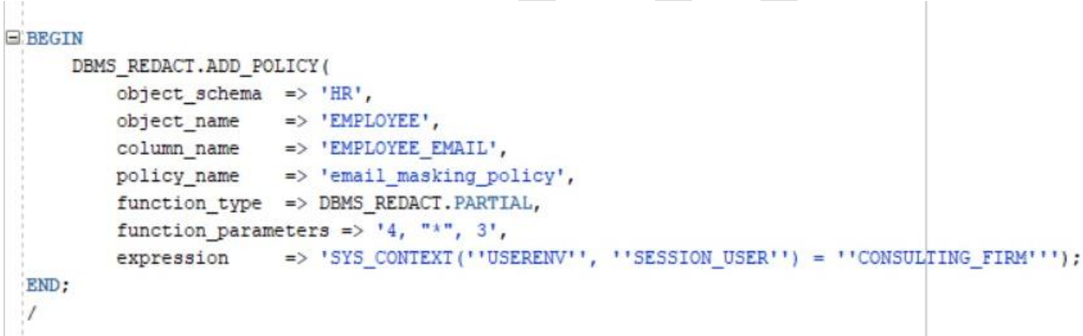
Identify the subset of data that requires higher security and encrypt it using Oracle Transparent Data Encryption (TDE). You can enable TDE for specific columns containing sensitive data.



```
-- Enable TDE for Sensitive Columns
ALTER TABLE Employee MODIFY (employee_mobile ENCRYPT USING 'AES256' NO SALT);
ALTER TABLE Employee MODIFY (employee_email ENCRYPT USING 'AES256' NO SALT);
```

Masking Data.

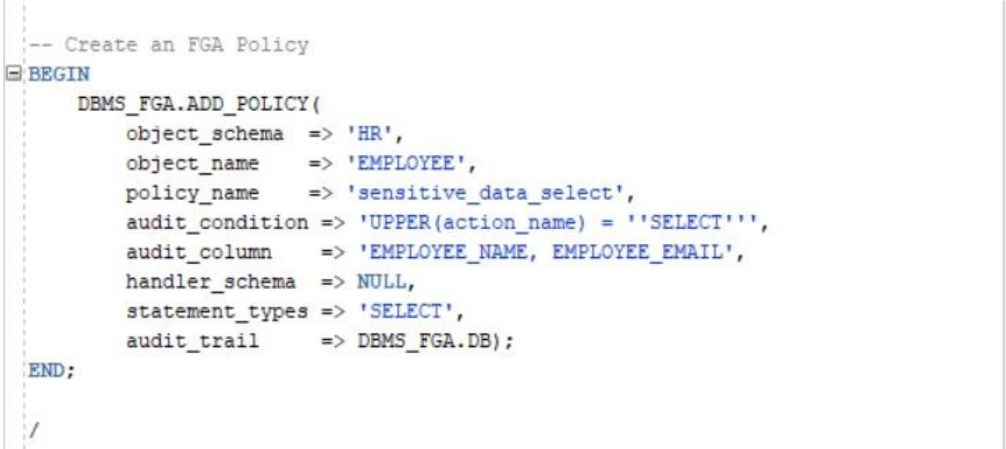
To allow access to a consulting firm while masking sensitive data, you can use data masking functions or Oracle Data Redaction.



```
BEGIN
    DBMS_REDACT.ADD_POLICY(
        object_schema  => 'HR',
        object_name    => 'EMPLOYEE',
        column_name    => 'EMPLOYEE_EMAIL',
        policy_name    => 'email_masking_policy',
        function_type  => DBMS_REDACT.PARTIAL,
        function_parameters => '4, "*", 3',
        expression     => 'SYS_CONTEXT(''USERENV'', ''SESSION_USER'') = ''CONSULTING_FIRM''');
END;
/
```

Implementing FGA policy.

To implement a suitable FGA policy, you can track specific actions on sensitive data.



```
-- Create an FGA Policy
BEGIN
    DBMS_FGA.ADD_POLICY(
        object_schema   => 'HR',
        object_name     => 'EMPLOYEE',
        policy_name     => 'sensitive_data_select',
        audit_condition => 'UPPER(action_name) = ''SELECT''',
        audit_column    => 'EMPLOYEE_NAME, EMPLOYEE_EMAIL',
        handler_schema  => NULL,
        statement_types => 'SELECT',
        audit_trail     => DBMS_FGA.DB);
END;

/
```

Task 03 -Database Security

Introduction:

The significance of big data in contemporary business operations has surged, necessitating a reevaluation of security practices distinct from those applied to conventional databases. This literature review aims to delineate the fundamental security prerequisites specific to big data, highlight their variances from traditional database security, catalog and detail five predominant security threats to big data infrastructures, and present and elaborate on a minimum of two protective strategies against each identified threat.

Fundamental Security Prerequisites for Big Data:

Big data security encompasses several key areas:

Safeguarding Sensitive Information: Ensuring that unauthorized individuals cannot access confidential data within big data systems.

Maintaining Data Integrity: Preserving the originality and consistency of data in big data systems.

Ensuring Data Accessibility: Providing reliable access to data for verified users when required.

User Identity Verification: Confirming the identities of users accessing big data systems.

Access Permission Allocation: Determining and regulating user access levels in big data systems.

Activity Logging: Keeping comprehensive logs of data interactions and user activities within big data systems.

These foundational requirements differ significantly from conventional database needs, owing to big data's typically vast and unstructured format, coupled with its demand for instantaneous processing and analytical abilities.

How does big data differ from the security requirements of traditional databases?

- Quantity, Speed, and Variety of Data:

  Big Data: Big data systems manage enormous amounts of data in a variety of forms and formats that are continuously entering the system at a fast rate (structured, semi-structured, unstructured).

  Traditional Databases: Conventional databases usually handle organized data that follows clearly specified schemas.

- Managing Access:

  Big Data: To manage the enormous volume of users and data sources to the system, access control measures must be adjusted.

  Traditional Databases: Access control in traditional databases is often more straightforward due to the limited number of users and applications.

- Authentication and Authorization:

  Big Data: Managing authentication and authorization for a large number of users and services accessing diverse data sources is challenging.

  Traditional Databases: Authentication and authorization are typically easier to manage as there are fewer users and applications.

- Data Encryption:

Big Data: Encrypting data at rest, in transit, and during processing is vital to protect data integrity in big data systems.

Traditional Databases: Data encryption is also important but may not be as extensive as in big data due to the smaller scale.

- Real-time Security Monitoring:

  Big Data: Real-time monitoring is crucial to detect and respond to security threats as data is ingested and processed continuously.

  Traditional Databases: Monitoring in traditional databases may be less real-time oriented.

- Distributed Environment:

  Big Data: Big data systems are distributed across clusters of servers, which adds complexity to security management.

  Traditional Databases: Traditional databases are often single-server or in small clusters, making security management more centralized.

- Data Transformation:

  Big Data: Transformation processes, such as ETL (Extract, Transform, Load), introduce security concerns, especially when combining data from different sources.

  Traditional Databases: Similar concerns exist in traditional databases, but they may be less complex.

- Data Lifecycle Management:

  Big Data: Managing data throughout its lifecycle, including archival and deletion, is important for compliance and data protection.

  Traditional Databases: Data lifecycle management in traditional databases is simpler due to smaller data volumes.

- Scalability:

Big Data: Security measures must be scalable to accommodate the growing data and user base.

Traditional Databases: Scalability is also important for traditional databases but is usually less extreme.

The main security requirements for big data systems differ from traditional databases due to the scale, variety, real-time nature, and complexity of big data. Security in big data environments often involves more extensive and specialized solutions to address these unique challenges.

Dominant Security Risks Facing Big Data Frameworks:

Big data systems are susceptible to various security threats, including:

Insertion of Spurious Data: Attackers may introduce false data, potentially leading to inaccurate analyses and misguided decisions.

Unauthorized Data Access: Individuals without proper authorization might access and steal confidential information.
Overwhelm Through Distributed Denial-of-Service (DDoS): Attackers could flood the system with excessive traffic, causing service disruptions.

Malicious Software Attacks: The introduction of harmful software to steal or corrupt data.

Threats from Within Harmful actions taken by authorized users, either deliberately or inadvertently, that could compromise data integrity or security.

Protective Strategies Against Security Threats:

To mitigate these threats, the following security measures are recommended:

Insertion of Spurious Data:

Rigorous Data Verification: Implement comprehensive data validation protocols to ensure only legitimate data is processed.

Data Scrutiny: Use data profiling tools to detect and remove false data.

Unauthorized Data Access:

Implementation of Access Restrictions: Apply stringent access controls to restrict data access to authorized personnel only.

Data Encryption: Utilize encryption techniques to protect sensitive data from unauthorized access.

DDoS Attacks:

Malicious Traffic Filtration: Use traffic filtering tools to block traffic from known harmful sources.

Traffic Distribution: Utilize load balancing to evenly distribute incoming traffic and prevent system overloads.

Malicious Software Attacks:

Malware Defense Mechanisms: Implement anti-malware tools to identify and eradicate harmful software.

Consistent System Updates: Maintain all systems with the most recent security enhancements and patches.