St. Francis Institute of Technology, Mumbai-400 103

Department of Information Technology

A.Y. 2023-2024

Class: SE-ITA/B, Semester: IV

Subject: **UNIX LAB**

Experiment – 6A: Study of security tools and best practices in Linux (Ubuntu) operating system

1. **Aim:** To Study security tools and best practices in Linux (Ubuntu) operating system
2. **Objectives:** After study of this experiment, the student will be able to
   - Understand what UNIX operating system is.
   - Identify the variants of various security tools in UNIX operating system.
3. **Outcomes:** After study of this experiment, the student will be able to
   - Understand different security tools used in UNIX operating system. (L402.4)
4. **Prerequisite:** None.
5. **Requirements:** Personal Computer, Ubuntu 20.04 operating system, LibreOffice, Internet Connection.

6. Laboratory Exercise

A. Procedure

Introduction to security tools and best practices in Linux (Ubuntu) operating system

Explore following tools : Snort, Nmap, Wireshark, CalmAV, OpenVAS, Nikto etc

For above listed tools Elaborate on points such as

- Name of Tools
- features,
- user interface
- advantages,
- limitations (if any).
- screenshot of installation any one tool listed above

B. Result/Observation

Attach printout of above case study

7. Post-Experiments Exercise

A. Extended Theory:

Nil.

B. Questions:

1. Compare and contrast Wireshark , Nmap and Snort

C. Conclusion:

1. Write what was performed in the experiment.
2. Mention a few applications of what was studied.
3. Write the significance of the topic studied in the experiment.

D. References:

1. Sumitabha Das, UNIX Concepts and Applications, 3rd Ed., Tata McGraw Hill.

Name: Vishal Rajesh Mahajan Exp: 6A
Class: SE IT A 3 Roll No: 63

Introduction:

In today's world of heightened cybersecurity concerns, understanding and implementing robust security measures are crucial, especially within the Linux (Ubuntu) operating system. This comprehensive case study delves into several prominent security tools, examining their features, user interfaces, advantages, limitations, and providing insights into their installation processes. The tools under review include Snort, Nmap, Wireshark, ClamAV, OpenVAS, and Nikto.

Snort

1. **Features**: Snort is an Intrusion Detection and Prevention System (IDPS) known for its real-time traffic analysis and packet logging capabilities. Its highly configurable and adaptable command-line interface sets it apart.
2. **User Interface**: Designed primarily for command-line use, it caters to security professionals familiar with manual configurations.
3. **Advantages**: Being open-source, Snort benefits from continuous community-driven updates and is renowned for its rules-based detection system.
4. **Limitations**: However, Snort's limited protocol support may hinder its effectiveness in certain network environments.

Wireshark

1. Features: Wireshark functions as a network protocol analyzer, enabling deep inspection of various protocols.
2. User Interface: Its user-friendly Graphical User Interface (GUI) makes it accessible to a wide range of users.
3. Advantages: Wireshark's extensive protocol support allows for in-depth analysis of network traffic.
4. Limitations: Nevertheless, Wireshark's resource-intensive nature can impact performance, particularly during extensive network monitoring.

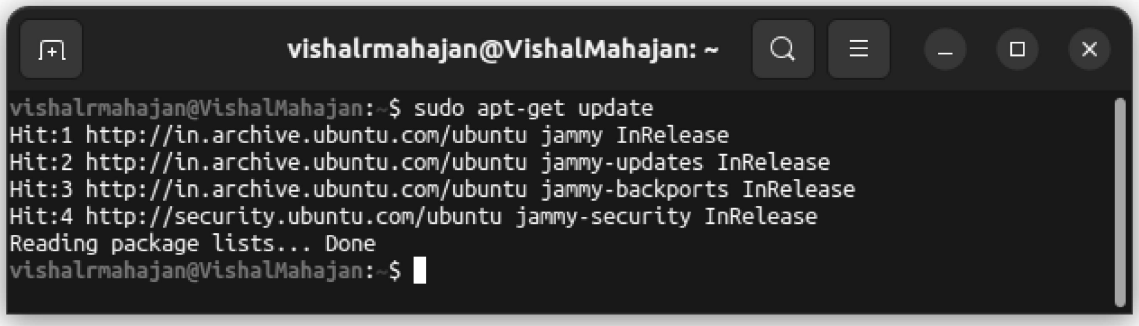
Name: Vishal Rajesh Mahajan Exp: 6A
Class: SE IT A 3 Roll No: 63

ClamAV

1. **Features**: ClamAV operates as an antivirus engine with a command-line scanner, known for its efficiency through the command line.
2. **User Interface**: Its primary command-line interface offers flexibility in usage.
3. **Advantages**: ClamAV's open-source nature ensures continuous updates to its virus database.
4. **Limitations**: However, its focus on malware detection limits its capabilities compared to more comprehensive commercial alternatives.

Nmap

1. **Features**: Nmap is renowned for its capabilities in network scanning, host discovery, and version detection, featuring a powerful scripting engine.
2. **User Interface**: With a command-line interface, Nmap provides extensive options for network exploration, requiring a certain level of expertise.
3. **Advantages**: Its scanning versatility and scripting capabilities make Nmap a potent tool.
4. **Limitations**: However, utilizing Nmap optimally requires specialized knowledge.

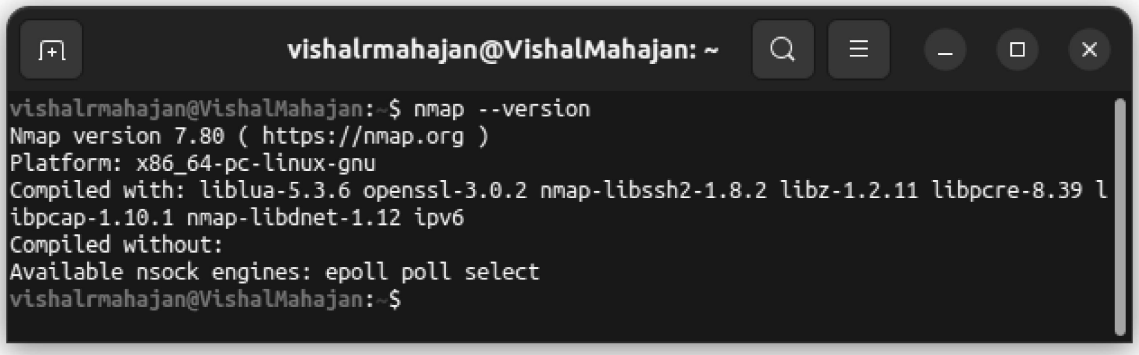


Name: Vishal Rajesh Mahajan Exp: 6A

Class: SE IT A 3 Roll No: 63

Name: Vishal Rajesh Mahajan Exp: 6A

Class: SE IT A 3 Roll No: 63



OpenVAS

1. **Features**: OpenVAS serves as a web-based vulnerability scanner and security management framework, known for its comprehensive vulnerability assessment capabilities.
2. **User Interface**: Its web-based interface enhances user accessibility, offering an intuitive platform.
3. **Advantages**: OpenVAS excels in thorough vulnerability assessments.
4. **Limitations**: However, it can be resource-intensive, especially during large-scale scans, necessitating careful implementation considerations.
5.

Nikto

1. **Features**: Nikto is a command-line web server vulnerability scanner offering fast and comprehensive scans.
2. **User Interface**: Its command-line interface provides detailed information on web server vulnerabilities.
3. **Advantages**: Nikto's speed and comprehensive scans make it valuable for web server security.
4. **Limitations**: However, it is limited to known vulnerabilities, potentially missing zero-day exploits.

Name: Vishal Rajesh Mahajan
Class: SE IT A 3
Exp: 6A
Roll No: 63

Conclusion:

In the constantly evolving realm of cybersecurity, knowledge and implementation of security tools are critical. By integrating tools like Snort, Nmap, Wireshark, ClamAV, OpenVAS, and Nikto, organizations and individuals can establish a robust defense against potential cyber threats in the Linux (Ubuntu) operating system. Regular updates, continuous monitoring, and a holistic security strategy are essential in maintaining the integrity and security of Linux-based systems in today's dynamic cybersecurity landscape. The comprehensive understanding of these tools and their effective implementation play a pivotal role in safeguarding digital assets and information.

St. Francis Institute of Technology, Mumbai-400 103

Department of Information Technology

A.Y. 2023-2024

Class: SE-ITA/B, Semester: IV

Subject: **UNIX LAB**

Experiment – 6B: Study of various Text Editors.

1. **Aim:** To study various text editors in UNIX Operating System**.**
2. **Objectives:** After study of this experiment, the student will be able to
   - Understand what UNIX operating system is.
   - Identify the variants of UNIX operating system.
3. **Outcomes:** After study of this experiment, the student will be able to
   - Understand text editors in UNIX operating system. (L402.4)
4. **Prerequisite:** None.
5. **Requirements:** Personal Computer, Ubuntu 20.04 operating system, LibreOffice, Internet Connection.

6. Laboratory Exercise

A. Procedure

Prepare a case study for following editor:

vi, nano, pico, emacs, bluefish, brackets,atom, sublime,vim,gedit.

Elaborate on points such as

- modes,
- features,
- commands,
- user interface ,
- installation (if any),
- advantages,
- limitations (if any).
- screenshot of editor screen

B. Result/Observation

Attach printout of above case study

7. Post-Experiments Exercise

A. Extended Theory:

Nil.

B. Questions:

1. Compare and contrast vi and vim editor
2. Describe the commands used in vi text editor.
3. Explain the control commands of Nano Text Editor.

C. Conclusion:

1. Write what was performed in the experiment.
2. Mention a few applications of what was studied.
3. Write the significance of the topic studied in the experiment.

D. References:

1. https://www.cs.colostate.edu/helpdocs/vi.html .
2. https://www.tutorialspoint.com/how-to-use-nano-text-editor
3. Sumitabha Das, UNIX Concepts and Applications, 3rd Ed., Tata McGraw Hill.

Name: Vishal Rajesh Mahajan Exp: 6B
Class: SE IT A 3 Roll No: 63

Introduction:
This study explores ten key text editors native to the Linux environment, examining their features, modes, commands, and user interfaces. Through thorough analysis and accompanying screenshots, it aims to provide insights for users to optimize their text editing experience on Linux.

1. **vi**
    a. Modes: Normal, Insert, Command-line.
    b. Features: Efficient text manipulation, syntax highlighting.
    c. Commands: Varied commands for navigation, editing, and saving.
    d. UI: Terminal-based, minimalist.
    e. Installation: Pre-installed on most Linux distributions.
    f. Advantages: Lightweight, universally available.
    g. Limitations: Steep learning curve for beginners.

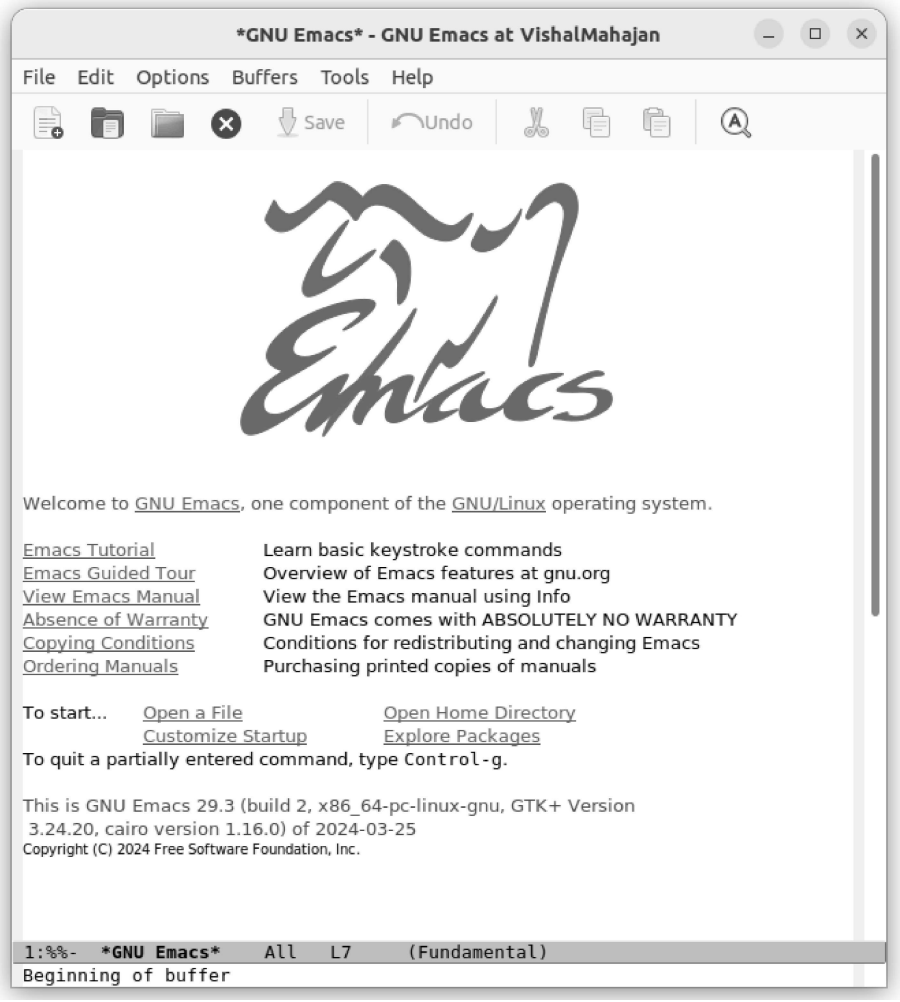
2. **pico**
    a. Modes: Single-mode.
    b. Features: Simple text editing, navigation.
    c. Commands: Displayed on the screen.
    d. UI: Terminal-based, user-friendly.
    e. Installation: Part of Pine email client, may need installation.
    f. Advantages: Easy for beginners.
    g. Limitations: Limited features.

Name: Vishal Rajesh Mahajan Exp: 6B

Class: SE IT A 3 Roll No: 63

3. emacs

a. Modes: Multiple modes for various tasks.
b. Features: Powerful text editing, extensibility.
c. Commands: Extensive, highly customizable.
d. UI: GUI and terminal versions.
e. Installation: Requires installation on most systems.
f. Advantages: Highly customizable, feature-rich.
g. Limitations: Steeper learning curve.

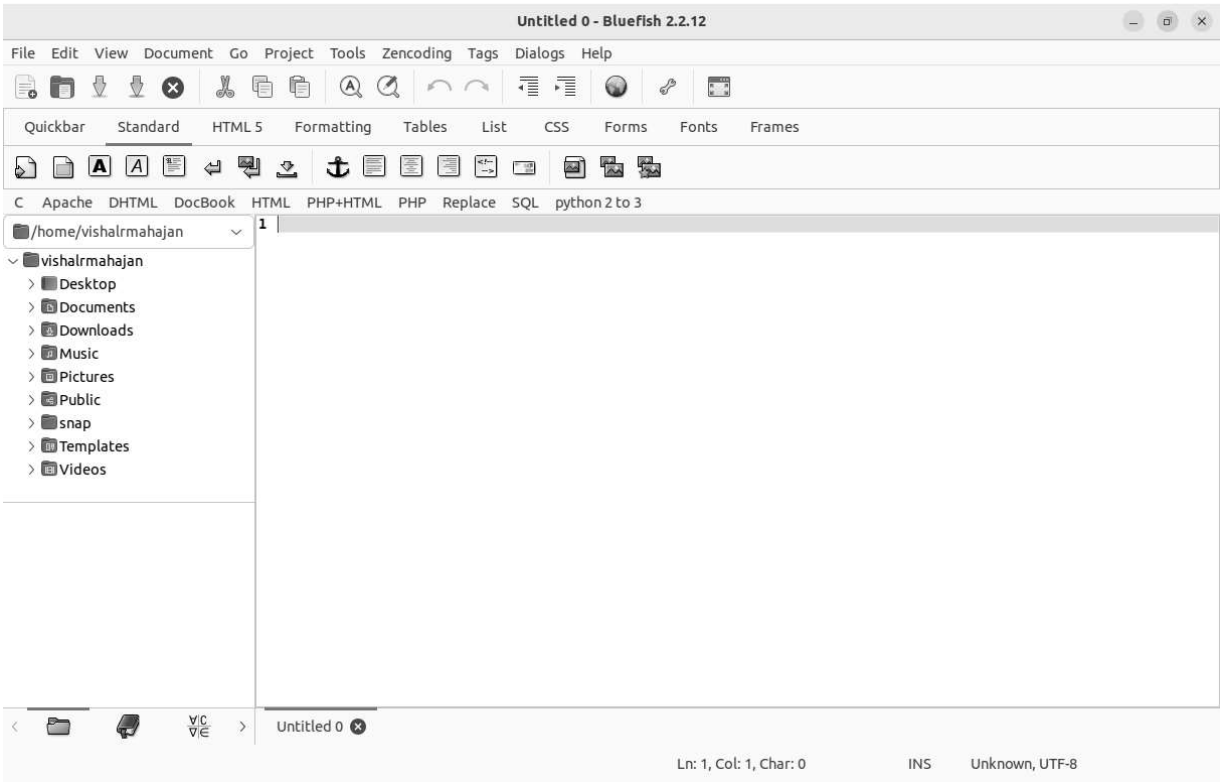


Name: Vishal Rajesh Mahajan Exp: 6B

Class: SE IT A 3 Roll No: 63

4. bluefish

a. Modes: WYSIWYG mode for web development.
b. Features: Web development support, syntax highlighting.
c. Commands: GUI-based, menu-driven.
d. UI: Graphical, designed for web development.
e. Installation: Requires installation, available in package managers.
f. Advantages: Specialized for web development.
g. Limitations: May be overwhelming for basic text editing.



5. **brackets**
    a. Modes: WYSIWYG mode, Live Preview.
    b. Features: Web development tools, visual CSS editing.
    c. Commands: GUI-based, menu-driven.
    d. UI: Graphical, modern design.
    e. Installation: Requires installation, available for Linux.
    f. Advantages: Real-time preview, visual editing.
    g. Limitations: Focused on web development.

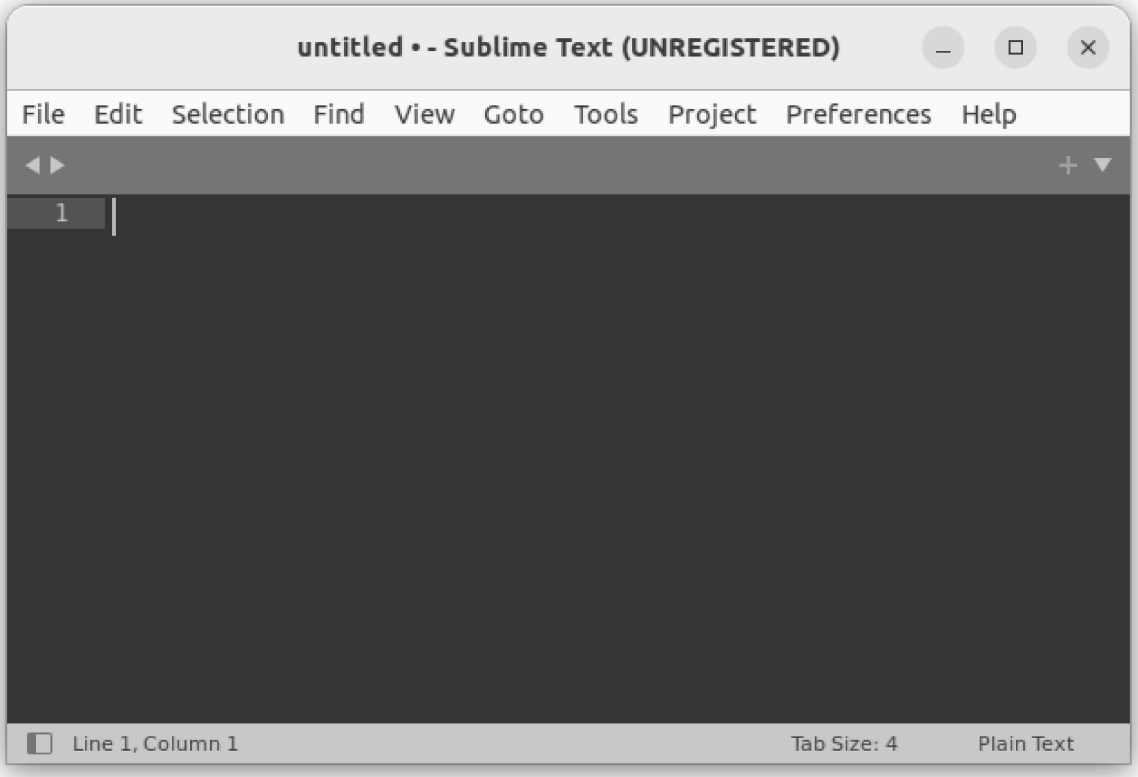
6. **atom**
    a. Modes: Extensible, supports plugins.
    b. Features: Cross-platform, integrated package manager.
    c. Commands: GUI-based, customizable.
    d. UI: Modern graphical interface.
    e. Installation: Requires installation, available for Linux.
    f. Advantages: Highly customizable, extensive plugin ecosystem.
    g. Limitations: May be resource-intensive.

7. **sublime**

Name: Vishal Rajesh Mahajan Exp: 6B

Class: SE IT A 3 Roll No: 63

a. Modes: Single mode, powerful features.
b. Features: Advanced text editing, customizable.
c. Commands: GUI-based, keyboard shortcuts.
d. UI: Sleek graphical interface.
e. Installation: Requires installation, available for Linux.
f. Advantages: Fast and feature-rich.
g. Limitations: Proprietary software, occasional reminders.

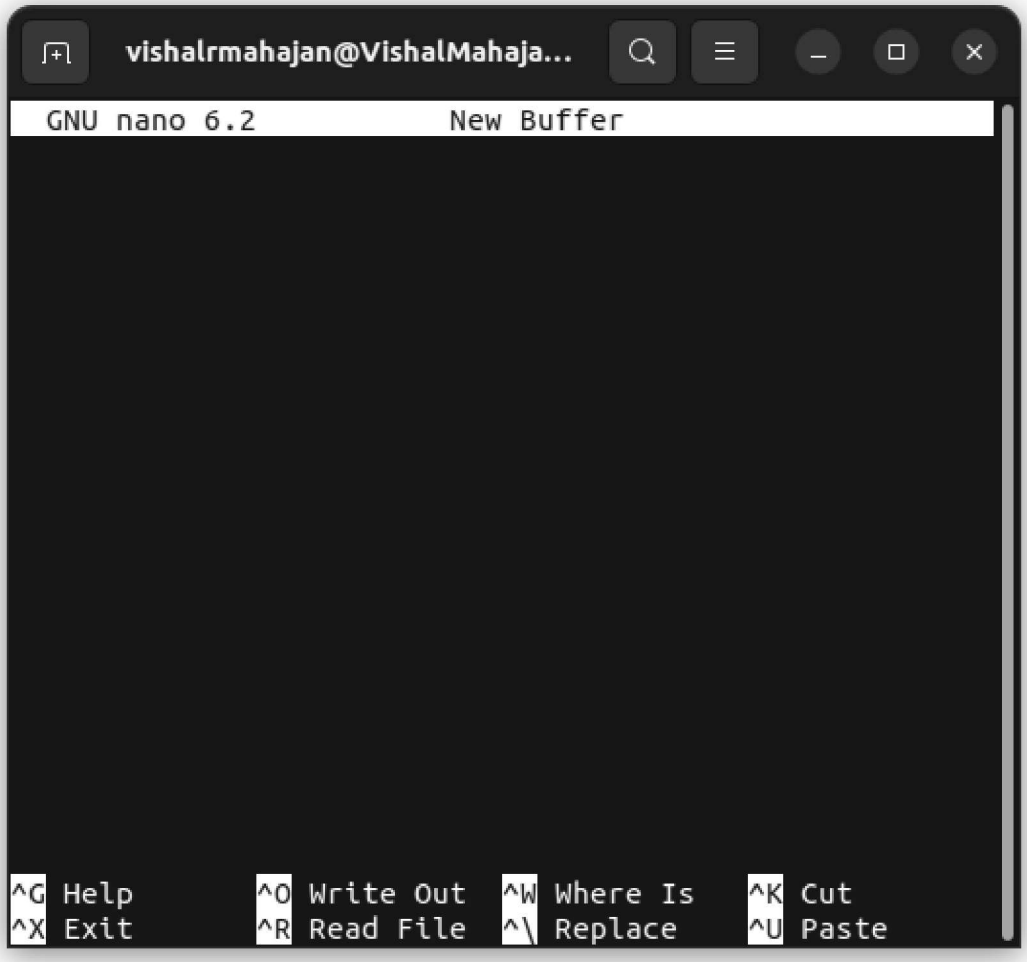


Name: Vishal Rajesh Mahajan
Class: SE IT A 3

Exp: 6B
Roll No: 63

8. nano

a. Modes: Simple interface, no distinct modes.
b. Features: Basic text editing, easy navigation.
c. Commands: Displayed at the bottom, user-friendly.
d. UI: Terminal-based, straightforward.
e. Installation: Pre-installed or easily installable.
f. Advantages: Beginner-friendly, intuitive.
g. Limitations: Lacks advanced features.

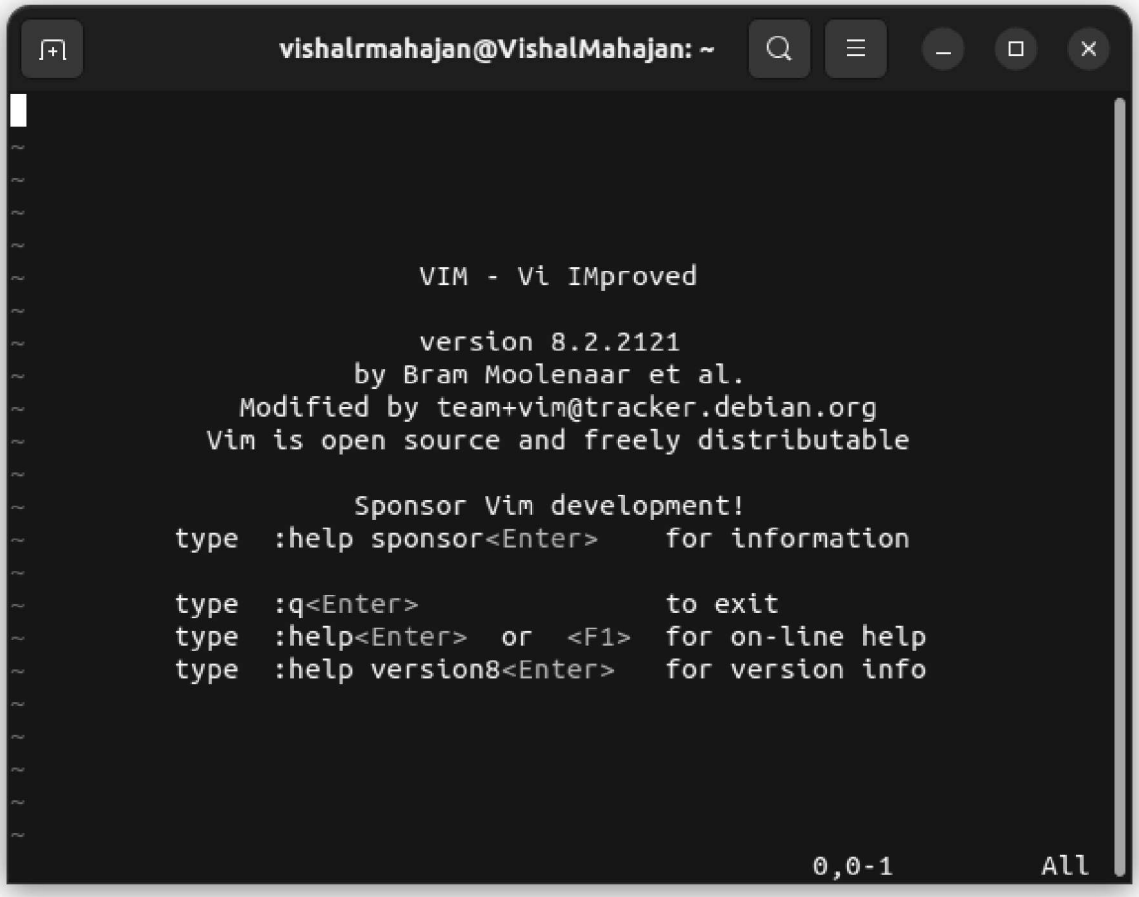


Name: Vishal Rajesh Mahajan Exp: 6B

Class: SE IT A 3 Roll No: 63

9. vim

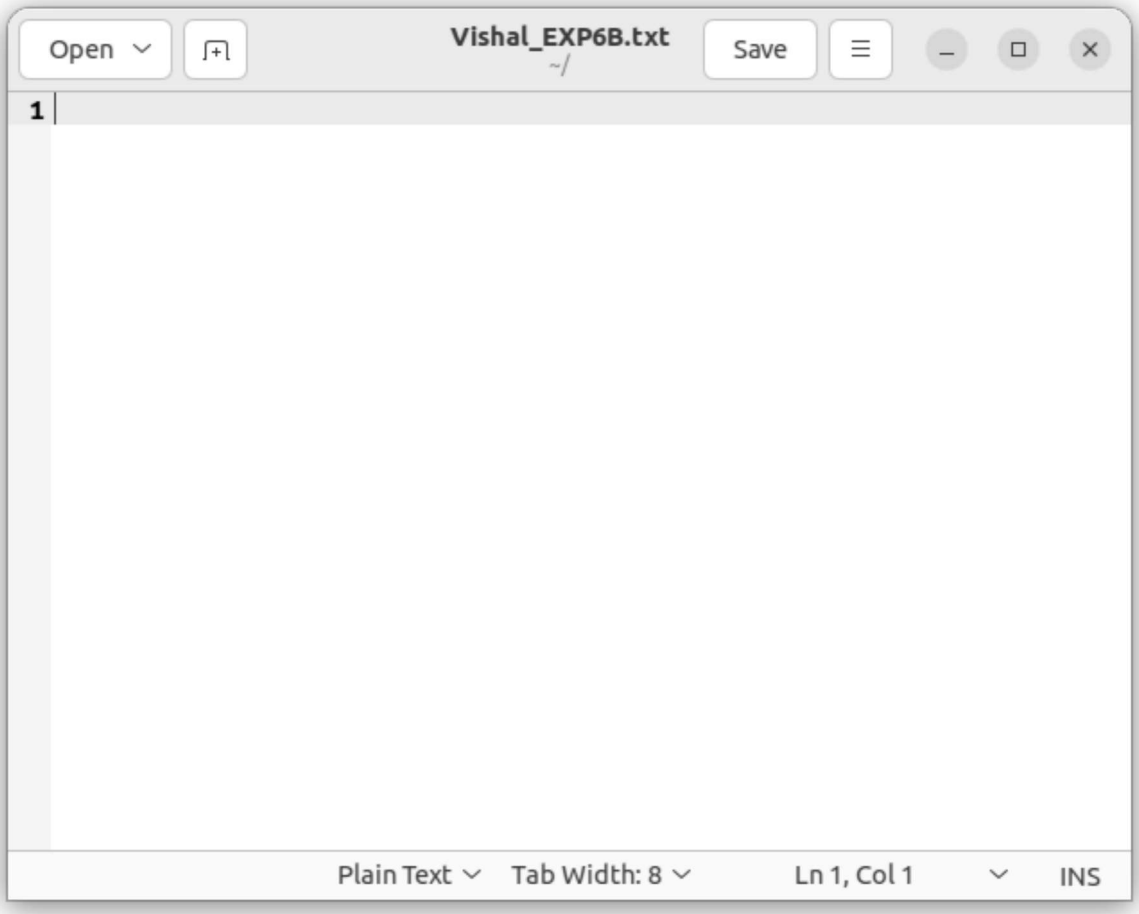
a. Modes: Normal, Insert, Visual.
b. Features: Efficient text manipulation, extensible.
c. Commands: Extensive, customizable.
d. UI: Terminal-based, powerful.
e. Installation: Pre-installed on most Linux distributions.
f. Advantages: Powerful and efficient.
g. Limitations: Learning curve for beginners.



Name: Vishal Rajesh Mahajan Exp: 6B
Class: SE IT A 3 Roll No: 63

10.gedit

a. Modes: Single mode, simplicity.
b. Features: Basic text editing, syntax highlighting.
c. Commands: GUI-based, menu-driven.
d. UI: Graphical interface, simple design.
e. Installation: Pre-installed on GNOME-based Linux systems.
f. Advantages: Lightweight, easy to use.
g. Limitations: Lacks advanced features for power users.



Name: Vishal Rajesh Mahajan
Class: SE IT A 3

Exp: 6B
Roll No: 63

Conclusion:

This detailed examination of Linux text editors showcases their diverse features, catering to a range of user preferences. Understanding their strengths and limitations aids users in selecting the most suitable editor based on their needs and proficiency.