Guru Nanak Dev Engineering College
Ludhiana

PRACTICAL FILE

NETWORK SECURITY LABORATORY
(LMCS-133)

M.TECH.

Submitted by:- Sarvesh
C.R.N:-2450008
Branch:-CSE

Submitted to:- Dr. Amit Jain

INDEX

S.No.	Practical Name	Date	Signature
1.	Steps to ensure security of any one web browser (Mozilla Firefox/Google chrome).		
2.	Learn to install virtual box or any other equivalent software on the host OS.		
3.	Study of the features of firewall in providing network security and to set firewall security in windows.		
4.	Generating password hashes with OpenSSL.		
5.	Perform a wireless audit of an access point / router and decrypt WEP and WPA.		
6.	Setup a honey pot and monitor the Honey Pot on network.		
7.	Analysis of the security vulnerabilities of e-commerce services.		
8.	Case Study on Authentication and Encryption.		

PRACTICAL:1

AIM:-Steps to ensure security of web browser (Mozilla Firefox/Google chrome)

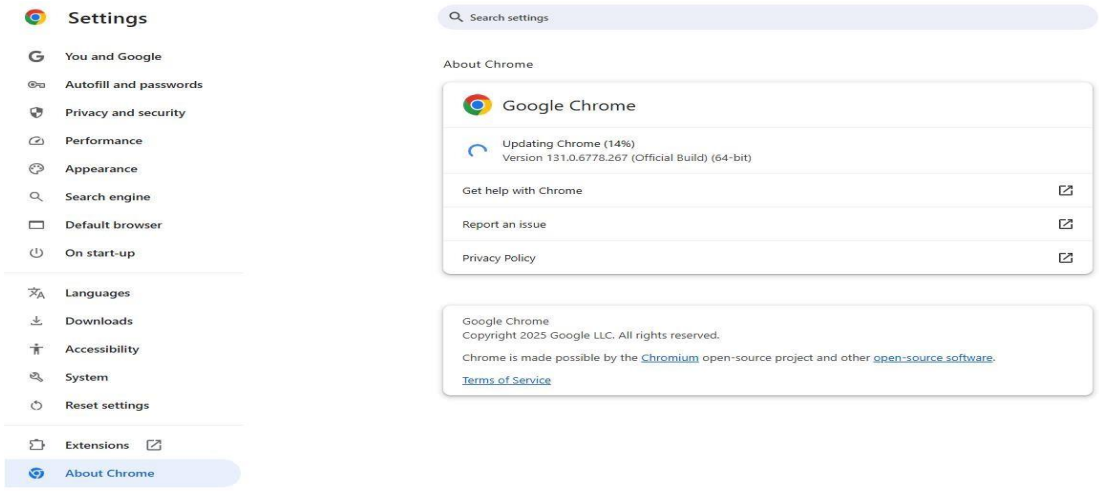
1.Steps to Secure Google Chrome:

1. Update the Browser

Keep your browser up to date for security patches and new features.

Steps:

- Open **Google Chrome**.
- Click on the **menu (three dots) → Help → About Google Chrome**.
- Chrome will automatically check for updates and install the latest version.
- Restart the browser if prompted.

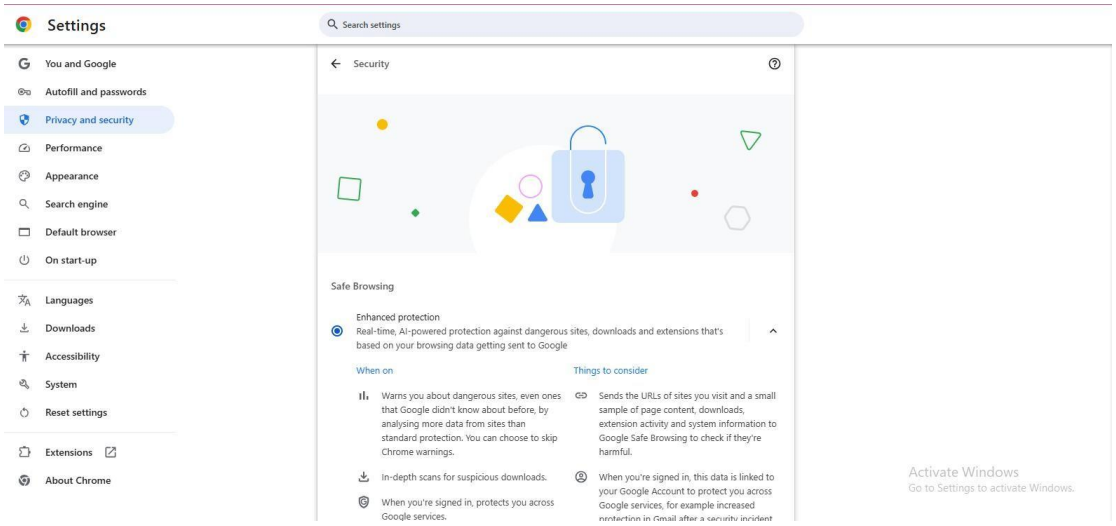


2. Enable Safe Browsing

Protect your browser from malware and phishing attacks.

Steps:

- Open **Google Chrome**.
- Go to **Settings → Privacy and Security → Security**.
- Select **Enhanced Protection** under Safe Browsing.

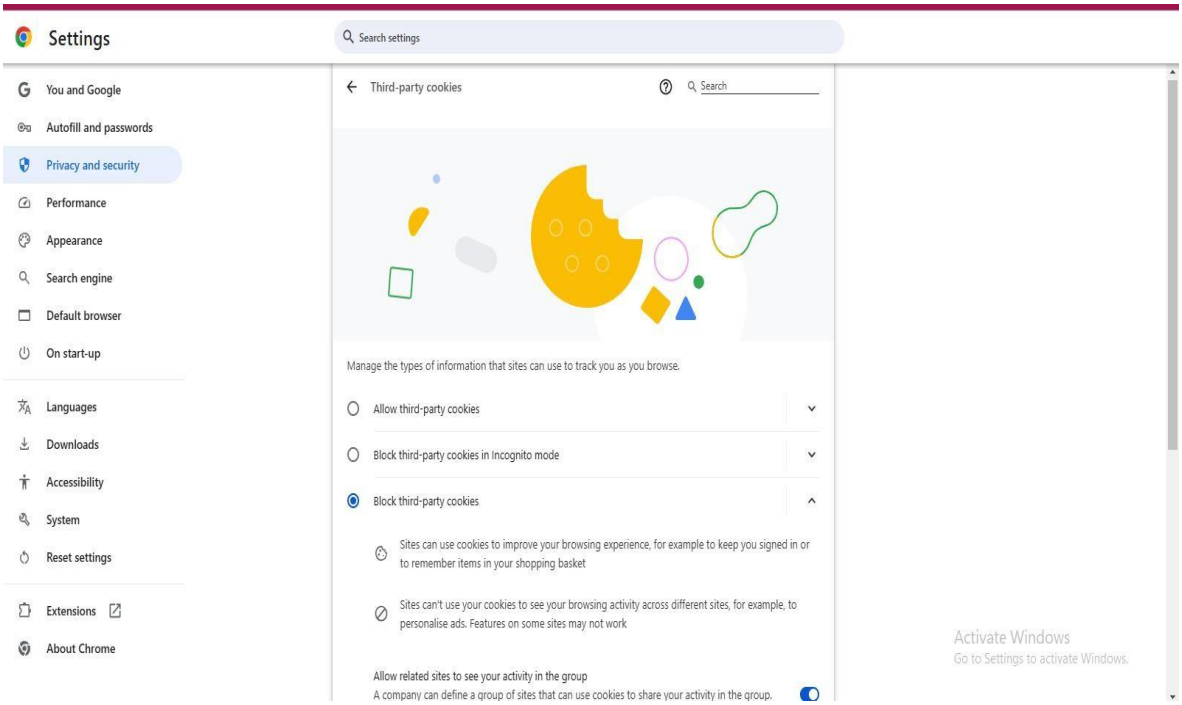


3. Disable Third-Party Cookies

Prevent websites from tracking your online activity.

Steps:

- Open **Google Chrome**.
- Go to **Settings → Privacy and Security → Cookies and Other Site Data**.
- Select **Block third-party cookies**.

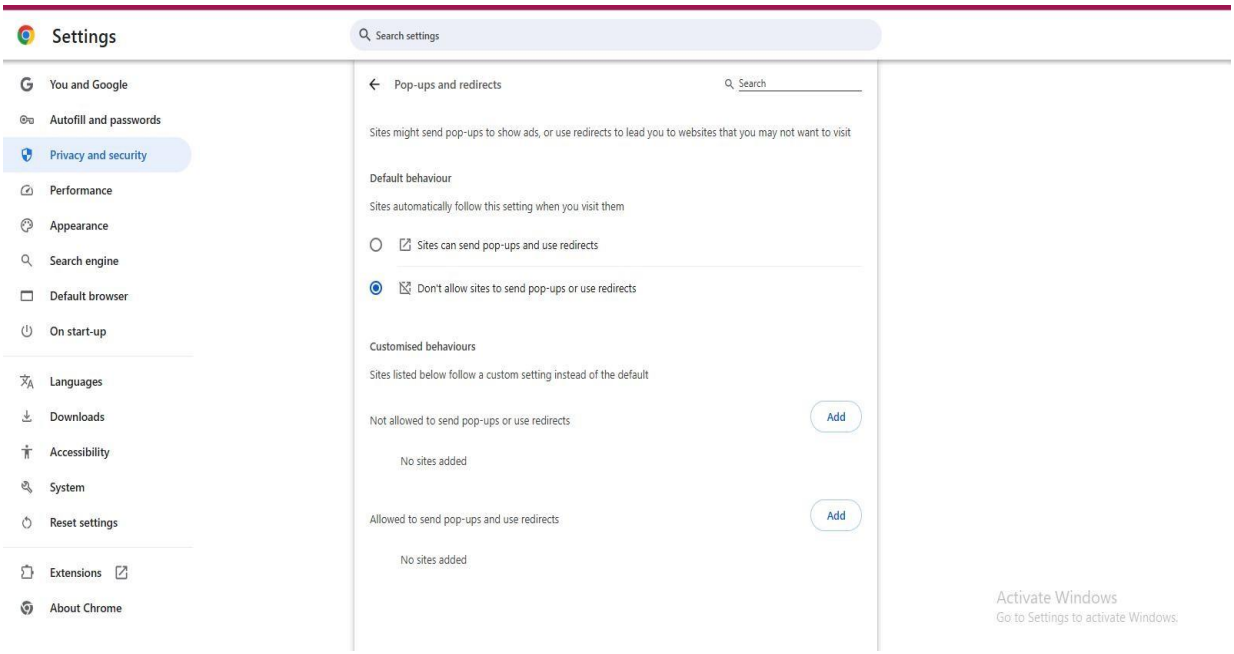


4. Block Pop-Ups

Prevent intrusive pop-ups and unwanted redirects.

Steps:

- Open **Google Chrome**.
- Go to **Settings → Privacy and Security → Site Settings → Pop-ups and redirects**.
- Select **Don't allow sites to send pop-ups or use redirects**.

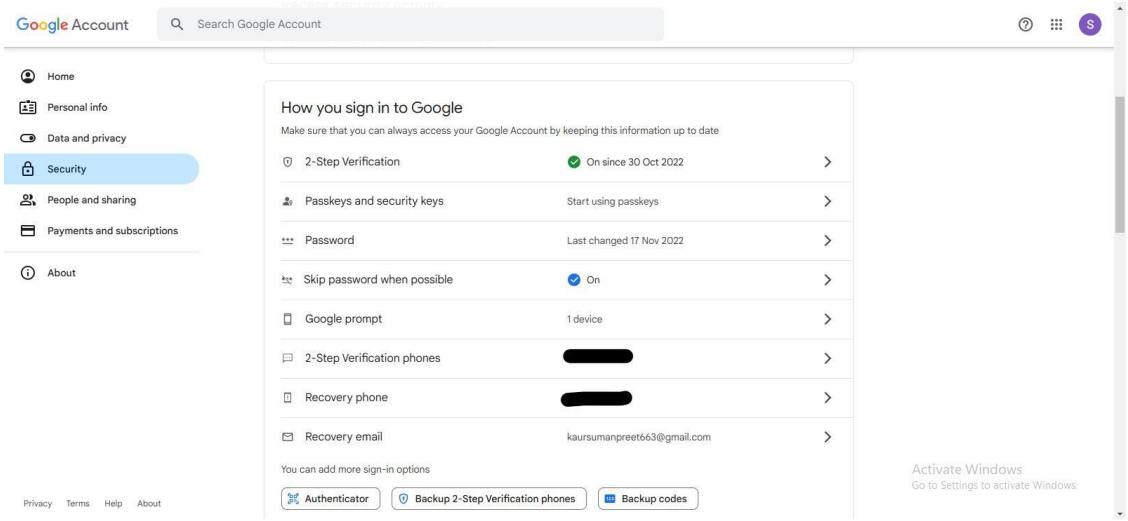


5. Enable Two-Factor Authentication (2FA)

Add an extra layer of security to your Google account.

Steps:

- Open **Google Account** and go to **Security**.
- Under **Signing in to Google**, click **2-Step Verification**.
- Follow the prompts to enable 2FA by setting up a phone number or authenticator app.

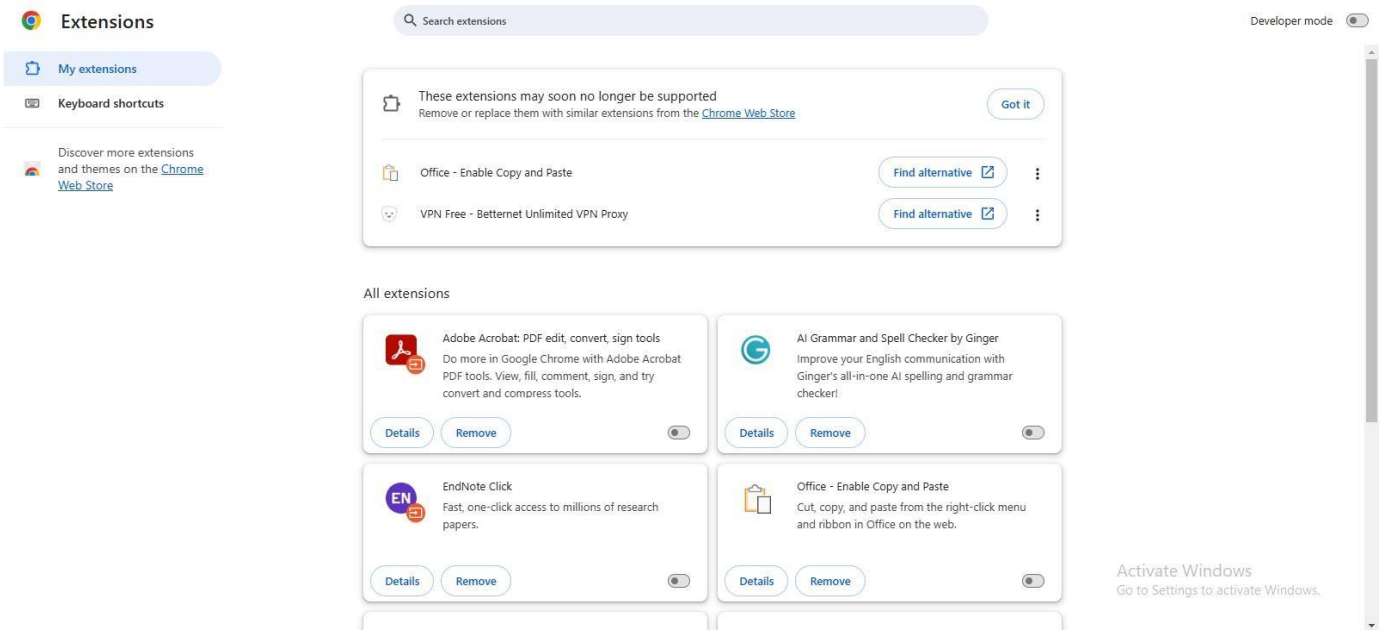


6. Check for Harmful Extensions

Ensure only trusted extensions are installed for security.

Steps:

- Open **Google Chrome** and type **chrome://extensions/** in the address bar.
- Review the list of installed extensions.
- Click **Remove** for any extension you don't recognize or trust.

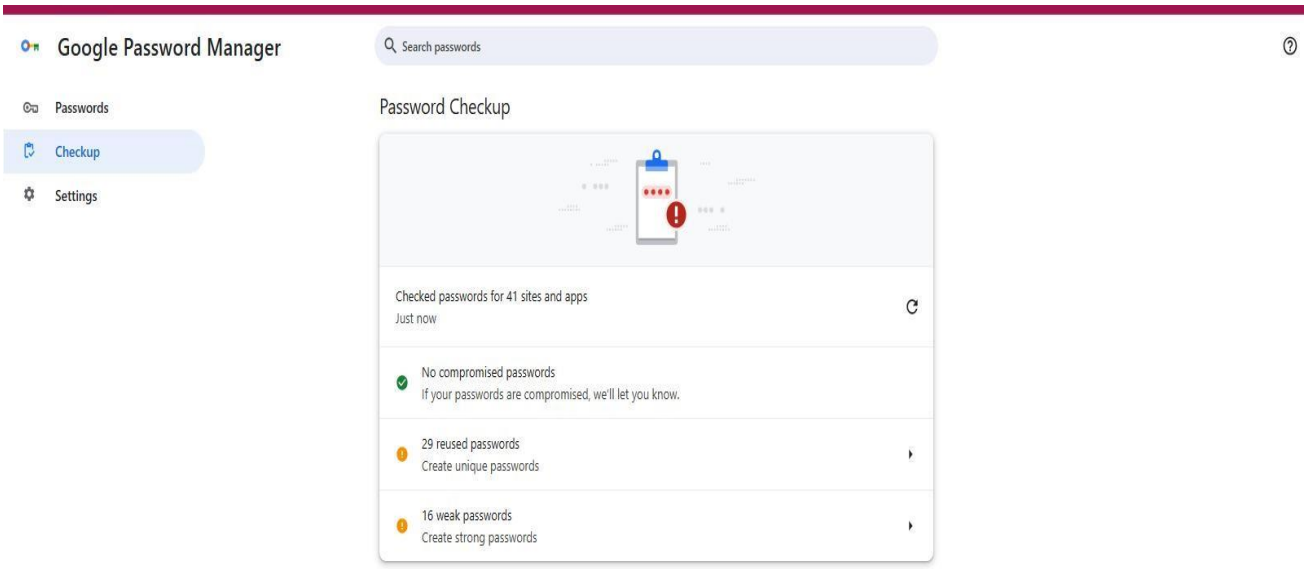


7. Use a Strong Password Manager

Securely store and manage your passwords.

Steps:

- Open **Google Chrome**.
- Go to **Settings → Autofill → Passwords**.
- Enable **Offer to save passwords** to use Chrome's built-in password manager.
- Alternatively, install a trusted password manager extension like **LastPass** or **Dashlane** from the Chrome Web Store.



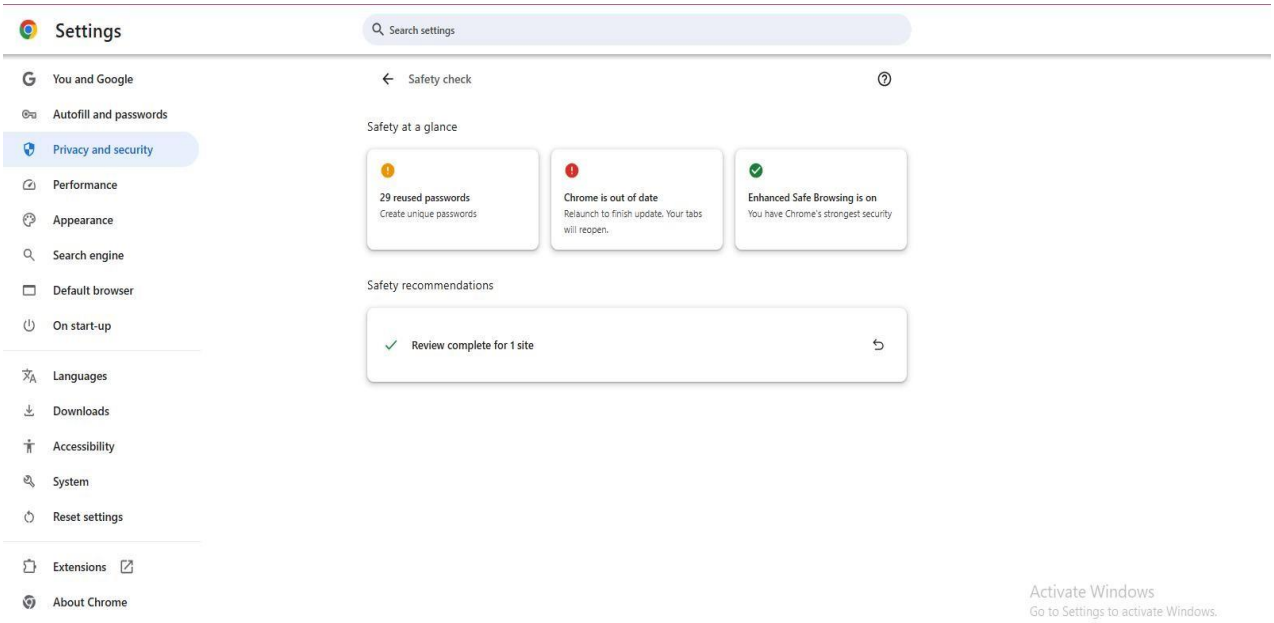
Activate Windows
Go to Settings to activate Windows.

8. Run the Safety Check Tool

Scan for security vulnerabilities and compromised data.

Steps:

- Open **Google Chrome**.
- Go to **Settings → Privacy and Security → Safety Check**.
- Click **Check now** to scan for compromised passwords, harmful extensions, and other security issues.

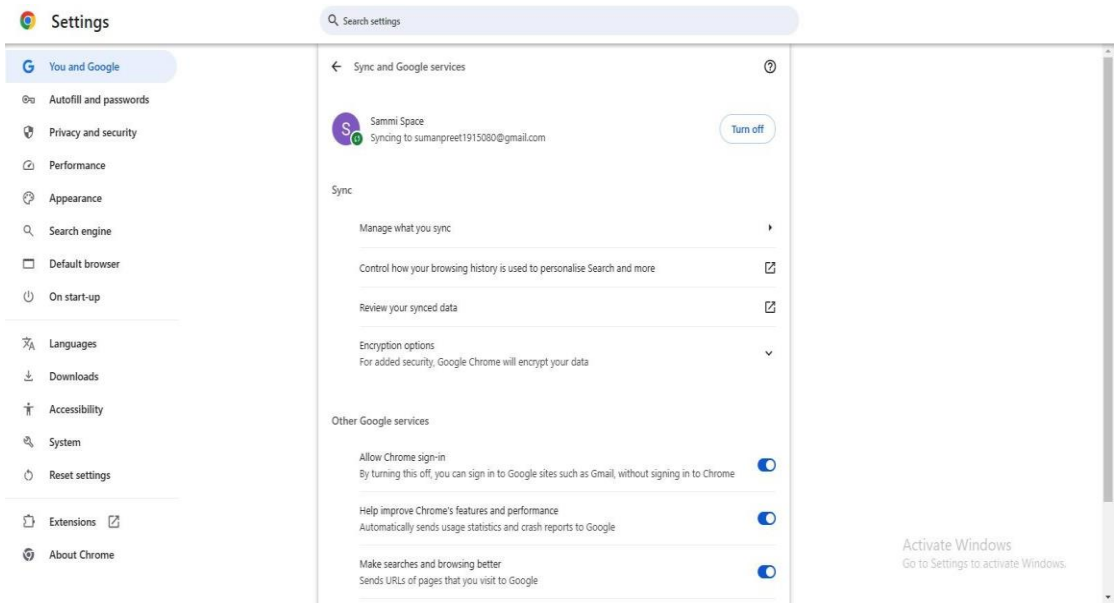


9. Avoid Saving Payment Information

Protect sensitive financial information by disabling auto-fill for payment methods.

Steps:

- Open **Google Chrome**.
- Go to **Settings → Autofill → Payment Methods**.
- Turn off **Save and fill payment methods**.

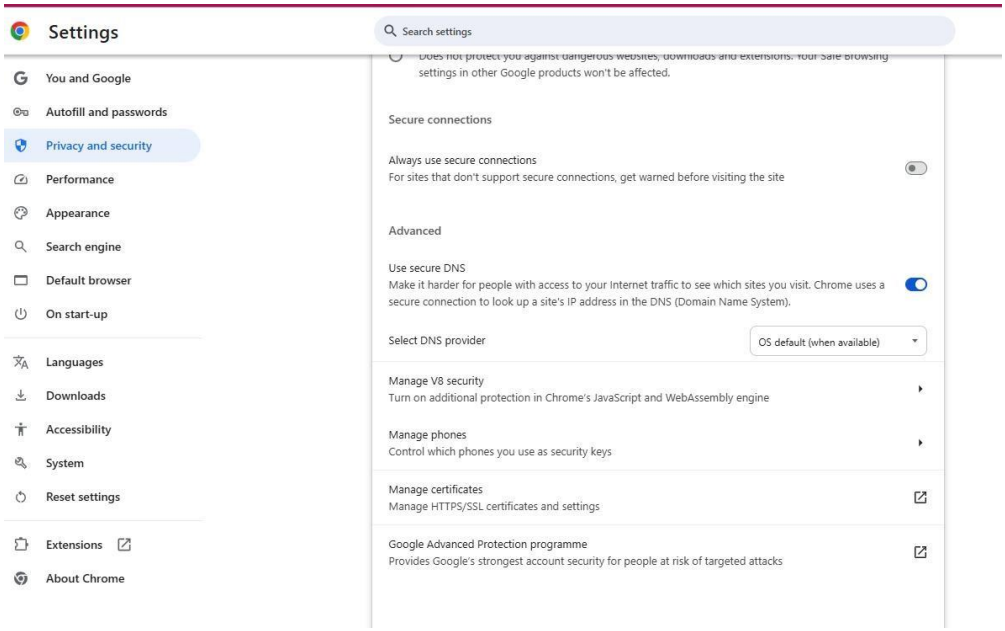


10. Use a Secure DNS Provider

Enhance your privacy by using a secure DNS provider.

Steps:

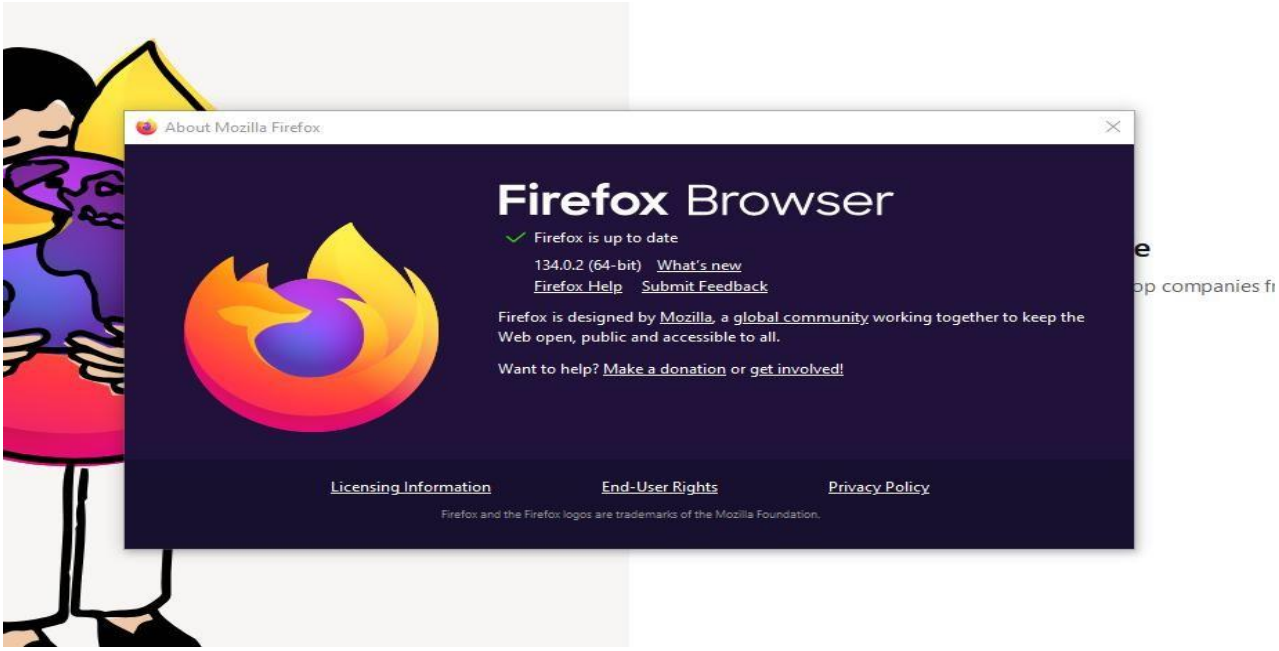
- Open Chrome and go to **Settings → Privacy and Security → Security**.
- Scroll down to **Use Secure DNS** and enable the option.
- Select **Choose a custom provider**, and pick a reliable provider like **Cloudflare (1.1.1.1)** or **NextDNS**.



2.Steps to Secure Mozilla Firefox

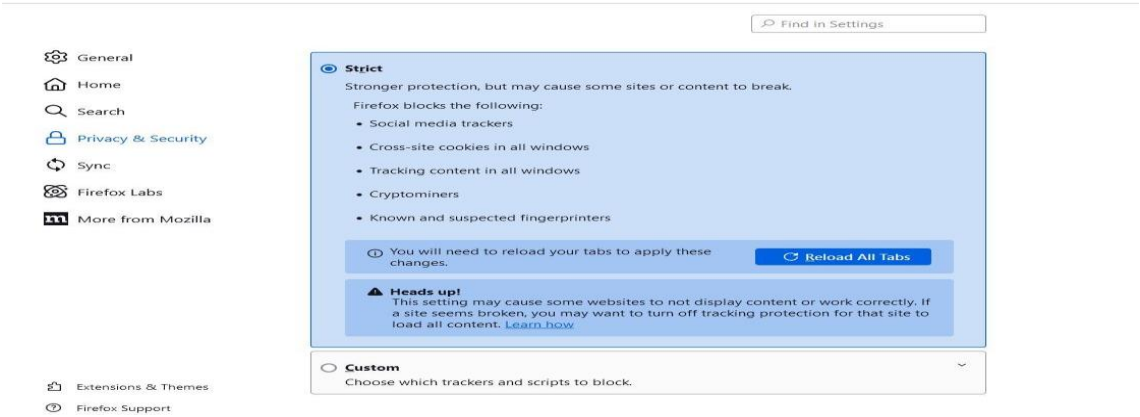
1. Update Firefox Regularly

- Ensure that Firefox is updated to the latest version, which contains important security patches.
- **Steps:**
  - Go to **Menu (three lines in the top right corner) > Help > About Firefox**.
  - Firefox will check for updates and install them automatically.



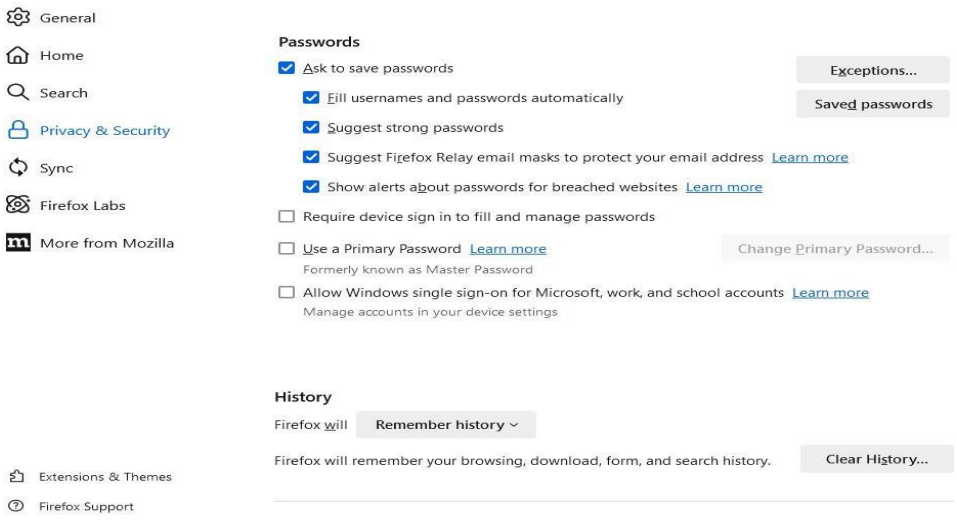
2. Enable Enhanced Tracking Protection

- Firefox includes Enhanced Tracking Protection to block trackers and scripts.
- **Steps:**
  - Go to **Settings > Privacy & Security**.
  - Under **Enhanced Tracking Protection**, select **Strict** for better security.



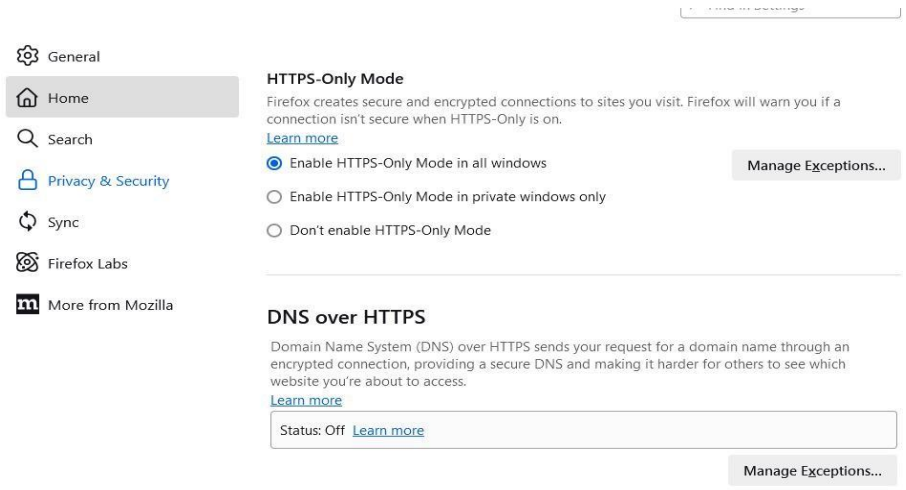
3. Use Secure Password Storage

- Firefox offers a built-in password manager called **Lockwise**.
- **Steps:**
  - Go to **Settings > Privacy & Security > Logins and Passwords**.
  - Enable **Ask to save logins and passwords for websites** and **Use a primary password** for additional security.



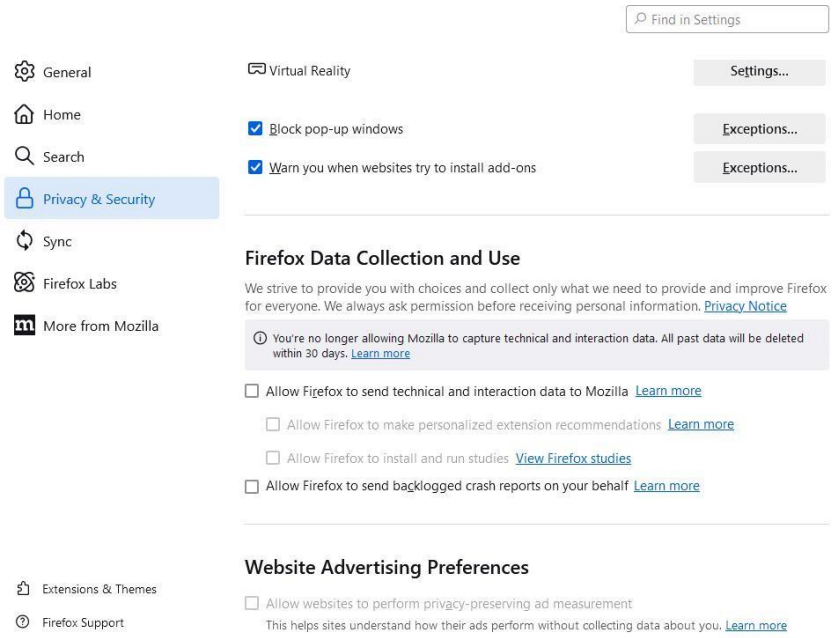
4. Enable HTTPS-Only Mode

- HTTPS encrypts your connection to websites.
- **Steps:**
  - Go to **Settings > Privacy & Security**.
  - Scroll to **HTTPS-Only Mode** and select **Enable HTTPS-Only Mode in all windows**.



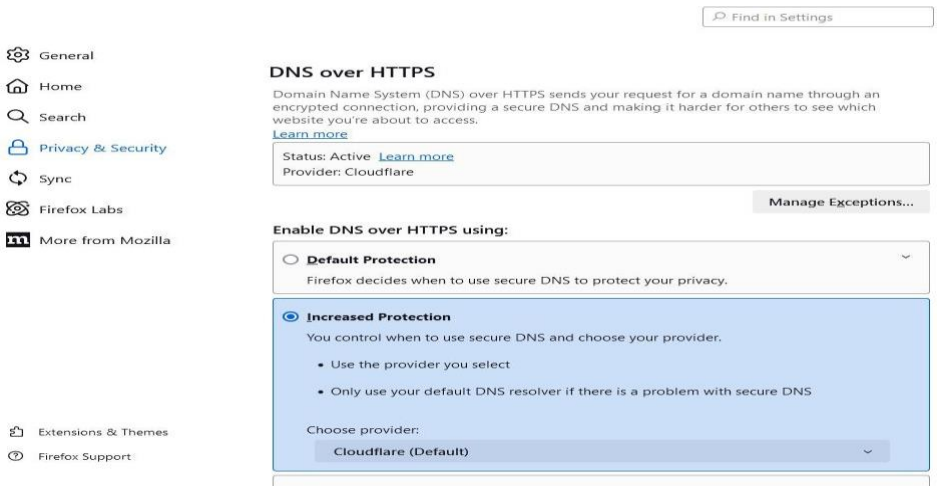
5. Disable Dangerous Features

- Disable telemetry and unwanted data sharing:
  - Go to **Settings > Privacy & Security** and uncheck all options under **Firefox Data Collection and Use**.



6. Use a Secure DNS Provider

- Enhance your privacy by using a secure DNS provider.
- **Steps:**
  - Go to **Settings > General > Network Settings**.
  - Scroll down to **Enable DNS over HTTPS**, and choose a reliable provider like Cloudflare or NextDNS.



PRACTICAL:2

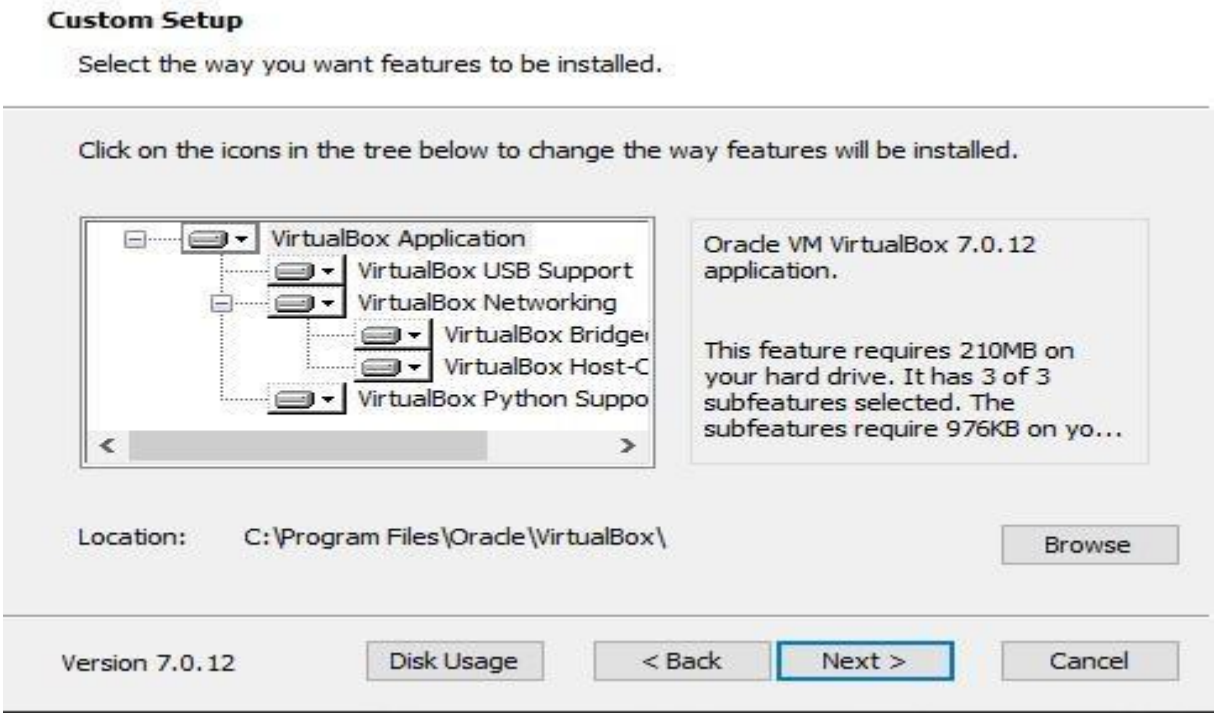
AIM:Learn to install virtual box or any other equivalent software on the host OS.

Installing VirtualBox in Windows 10

1. Open your preferred web browser then navigate to the official VirtualBox download page. Under "Windows hosts" click the link to download virtualbox for Windows 10.

2. Locate the downloaded installer file in your **Downloads** folder or wherever you saved it. Double-click the installer file to launch the VirtualBox Setup Wizard. In the welcome screen, click "Next" to proceed with the installation.

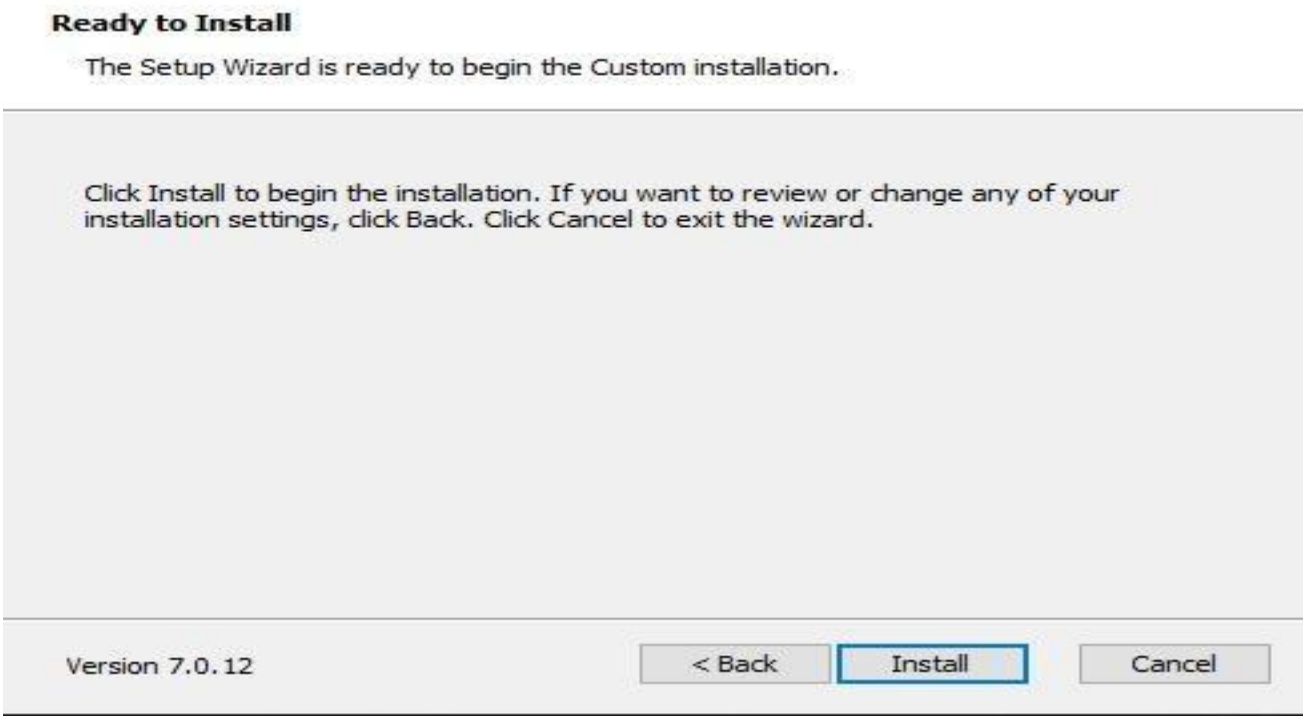
3. The next screen presents customization options for the virtual box installation which include:



- VirtualBox will be installed in the **C** directory.
- Creates a shortcut icon for VirtualBox on your desktop for easy access.
- Creates an entry for VirtualBox in your Start menu.
- Network adapter allows you to choose the adapter that VirtualBox will use.
- USB option allows you to configure USB device access for virtual machines.

4. Once reviewed the customization options click “Next” to proceed then a Warning Network interface option appears click “Yes” to proceed with the installation.

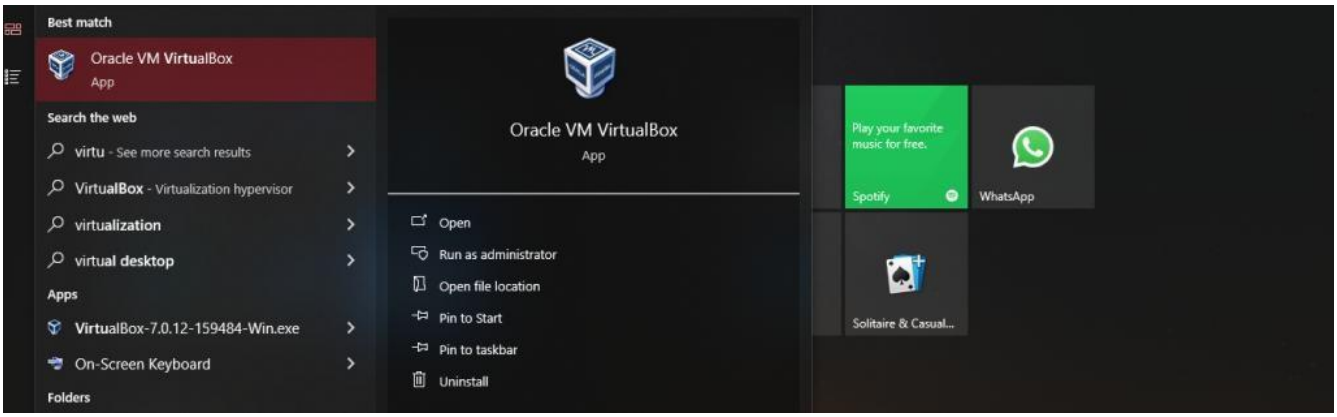
5. Ready to Install wizard appears, Click “Install” to begin the installation.



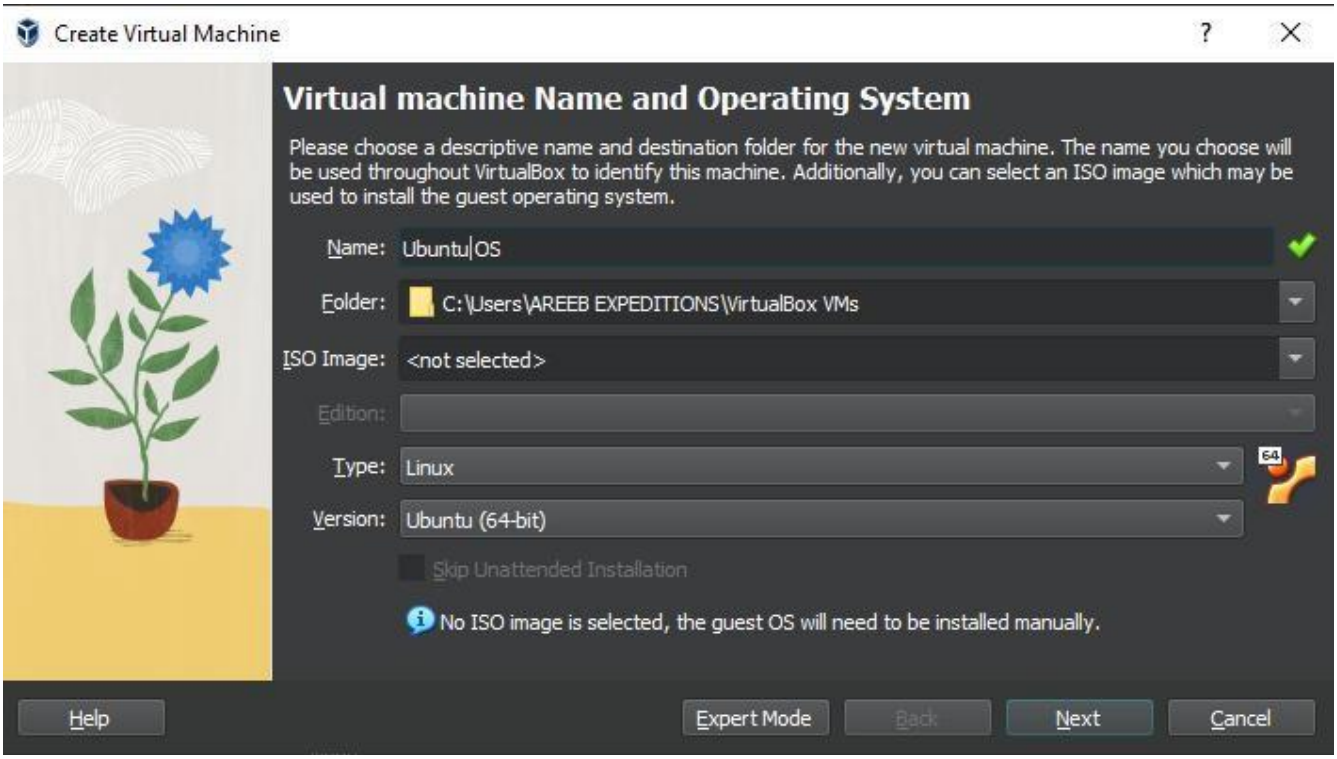
6. After the installation is complete, click “Finish” to complete the installation process.

Creating the First Virtual Machine

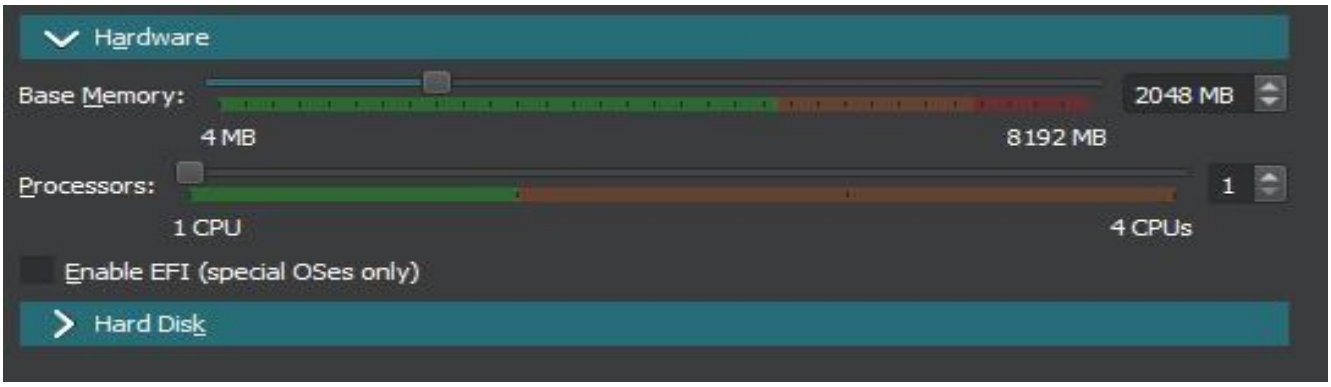
After completing the installation you can launch VirtualBox by searching for it in the Start Menu or using the desktop shortcut.



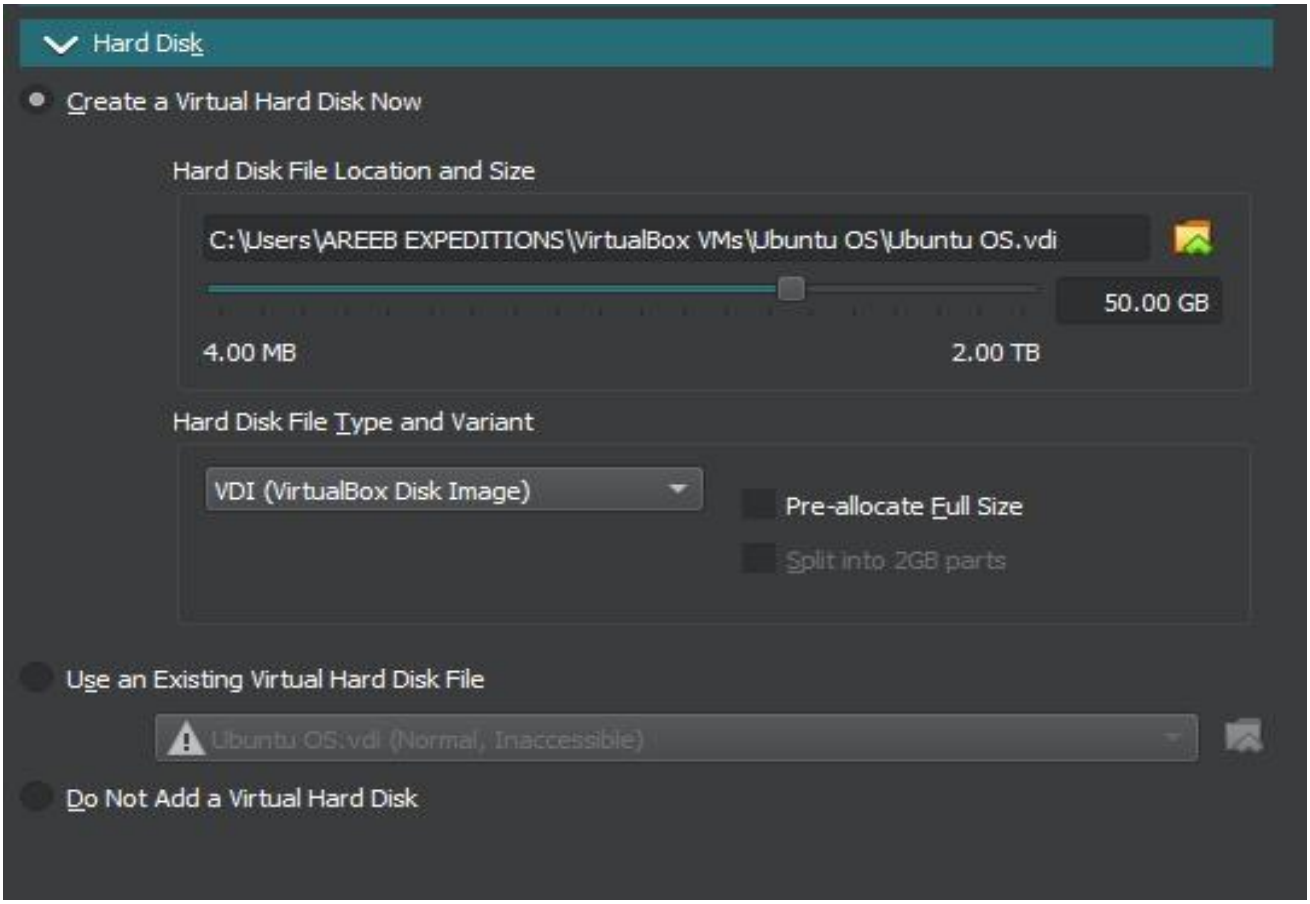
The VirtualBox Manager window will open. This is the main interface where you will manage your virtual machines. To create your first virtual machine, click the “New” button in the toolbar.



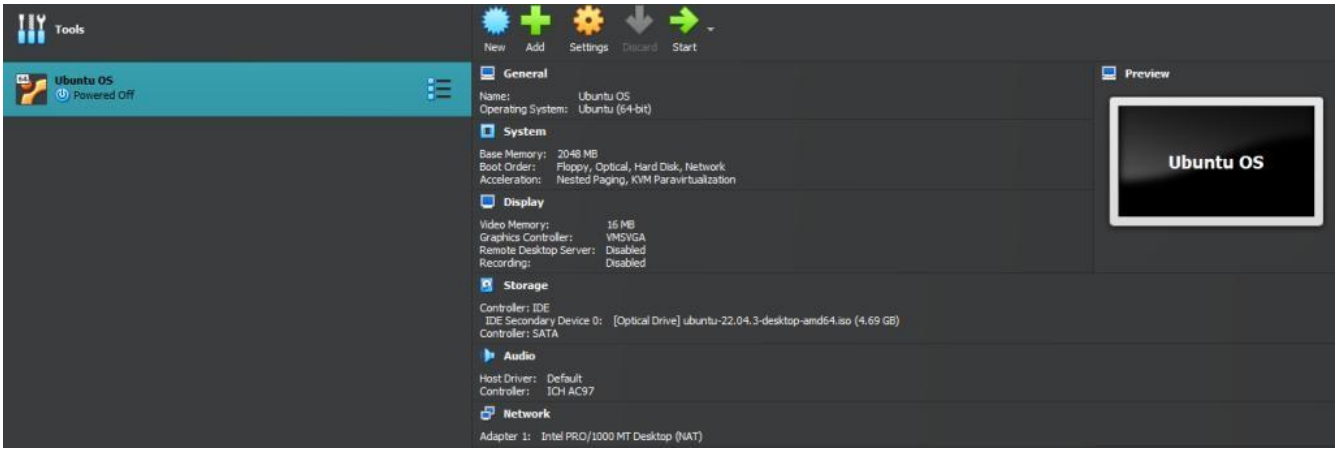
The "Create Virtual Machine" wizard will guide you through the setup process. You'll be prompted to specify various options including:



- **Name and operating system:** Choose a descriptive name for your virtual machine and select the type of operating system you plan to install.
- **RAM memory:** Allocate a sufficient amount of RAM for your virtual machine.
- **Hard disk:** Choose how you want to create the virtual hard disk. You can either create a new virtual hard disk dynamically or allocate a fixed size upfront.



After completing the setup you can see the VirtualBox interface shows the operating system installed in vbox. Click “Start” to run the operating system.



Now successfully run the Linux operating system through VirtualBox. It is important to check the system requirements for the guest operating system you plan to install within the virtual machine.

PRACTICAL. 3

Aim: Study of the features of firewall in providing network security and to set firewall security in windows.

Firewalls are essential tools for providing network security by monitoring and controlling incoming and outgoing network traffic based on predefined security rules. Here's a breakdown of the key features of firewalls in providing network security:

1. Traffic Filtering

- **Packet Filtering**: Firewalls analyze each data packet that passes through the network. They use rules to allow or block packets based on attributes such as source/destination IP addresses, port numbers, and protocols.
- **Stateful Inspection**: This type of filtering keeps track of the state of active connections (e.g., TCP handshakes). It ensures that packets are part of a valid, established session, improving security and preventing attacks like packet injection.
- **Deep Packet Inspection (DPI)**: DPI analyzes the content of the data packets, going beyond just headers, to detect malicious code, viruses, and other types of threats within the traffic.

2. Access Control

- **Access Control Lists (ACLs)**: Firewalls use ACLs to define rules for allowing or denying traffic. These rules specify which traffic is permitted or blocked based on IP addresses, port numbers, and other parameters.
- **User Authentication**: Firewalls can enforce user authentication before granting network access, ensuring that only authorized users can interact with the network.

3. Intrusion Prevention and Detection

- **Intrusion Detection Systems (IDS)**: Firewalls often incorporate IDS features to detect suspicious or malicious activities such as port scanning, denial-of-service (DoS) attacks, and unauthorized access attempts.
- **Intrusion Prevention Systems (IPS)**: Some firewalls can prevent attacks in real time by detecting and blocking suspicious traffic based on signatures of known threats.

4. Logging and Monitoring

- **Event Logging**: Firewalls generate logs of network traffic, including allowed and denied connections. These logs are invaluable for auditing network activity, troubleshooting, and detecting abnormal behavior.
- **Alerting**: Advanced firewalls can send real-time alerts about potential security threats, enabling IT staff to take immediate action.

5. VPN Support

- **Virtual Private Network (VPN) Support**: Firewalls often support VPN technology, allowing secure communication between remote clients and the internal network. This is crucial for businesses that allow employees to access resources remotely.
- **IPsec and SSL/TLS Encryption**: Firewalls with VPN capabilities can secure traffic using encryption protocols like IPsec and SSL/TLS, ensuring that the data remains private and secure while in transit.

6. Application Layer Filtering

- **Application Firewall Features**: Some firewalls operate at the application layer, where they can inspect and filter traffic specific to applications like HTTP, FTP, DNS, and more. This type of firewall is often used to block or restrict web traffic to prevent exploits like SQL injection, cross-site scripting (XSS), and malware.
- **Web Application Firewall (WAF)**: A WAF is a specialized firewall designed to protect web applications by filtering and monitoring HTTP/HTTPS traffic.

7. Network Address Translation (NAT)

- **NAT**: Firewalls often use NAT to obscure internal IP addresses from the public internet. This feature helps prevent attackers from directly targeting internal devices by translating internal IP addresses into public-facing ones, which improves security.

8. Proxy Services

- **Forward Proxy**: Firewalls can act as forward proxies to mask client requests to external servers, preventing direct connections to the internet and thereby hiding internal network structure.
- **Reverse Proxy**: A reverse proxy intercepts incoming traffic from the internet and forwards it to an internal server. This is used to protect internal servers from direct exposure to the internet and to provide load balancing.

9. Rate Limiting and Traffic Shaping

- **Rate Limiting**: Firewalls can limit the rate of incoming or outgoing traffic to prevent overloading the network and protect against certain types of DoS attacks.
- **Traffic Shaping**: Some firewalls can prioritize specific types of traffic, ensuring that critical applications, such as voice or video, receive priority over less critical traffic.

10. High Availability and Redundancy

- **Failover**: Many firewalls support high availability configurations that allow automatic failover in case of hardware or software failures. This ensures that network security remains operational even during system disruptions.
- **Clustering**: Firewalls can be clustered together to create redundant systems, providing load balancing and enhancing security by preventing a single point of failure.

11. Zero Trust Security Model

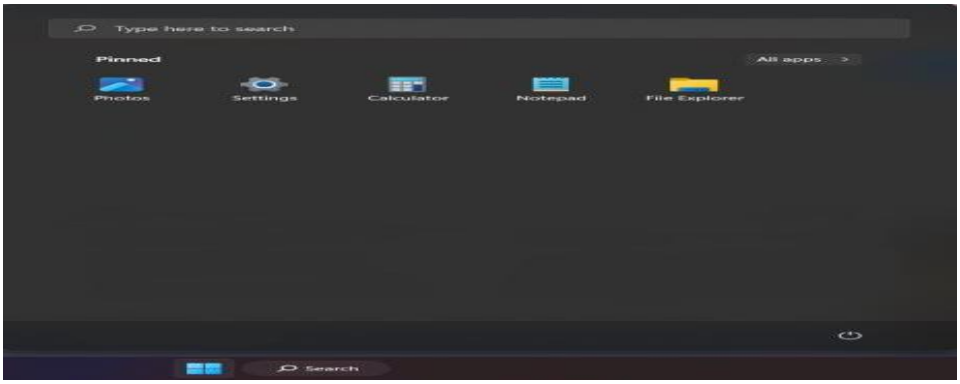
- **Zero Trust Architecture**: Some modern firewalls integrate with Zero Trust security models, where trust is never assumed, and every user or device must be authenticated and authorized before being granted access to network resources.

12. Integration with Other Security Systems

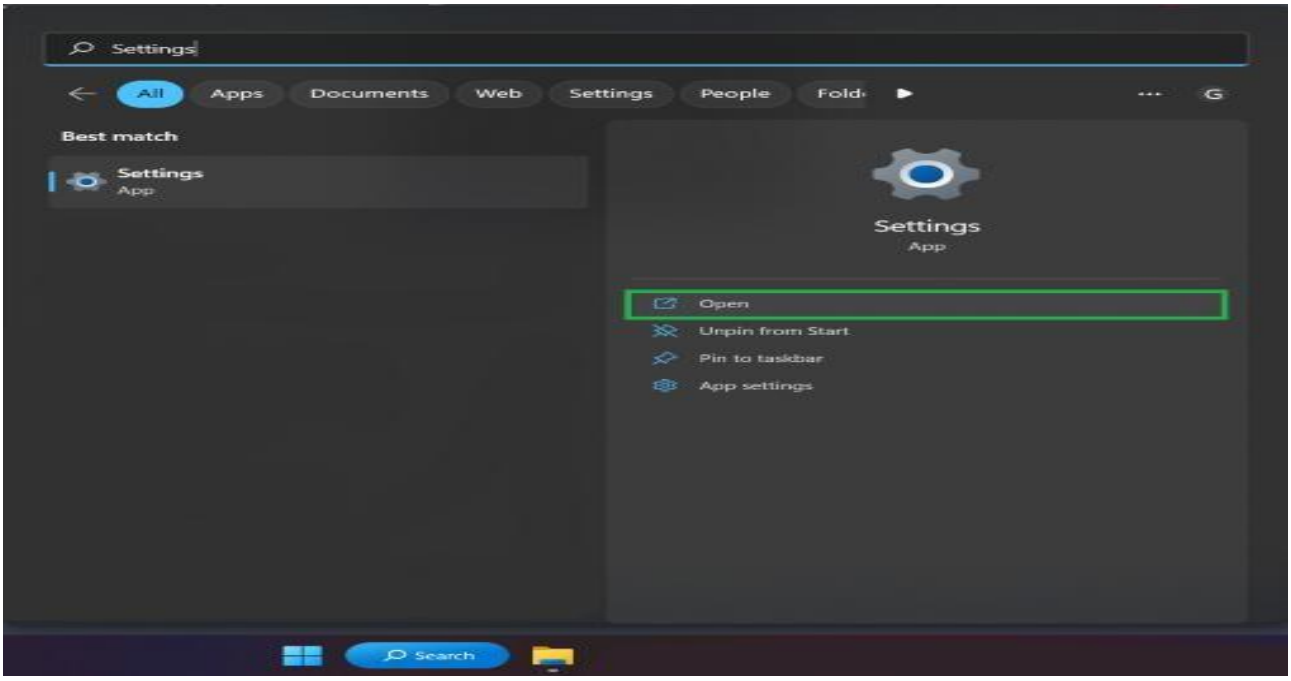
- **Security Information and Event Management (SIEM)**: Firewalls can send event data to SIEM systems for centralized analysis and correlation with other network security devices, enabling more effective threat detection and response.
- **Threat Intelligence**: Some firewalls incorporate threat intelligence feeds that provide updated information about emerging threats and vulnerabilities, helping the firewall block new attack vectors.

Configuring Firewall Defender on Windows:

Step 1: Launch **Start** from the taskbar.

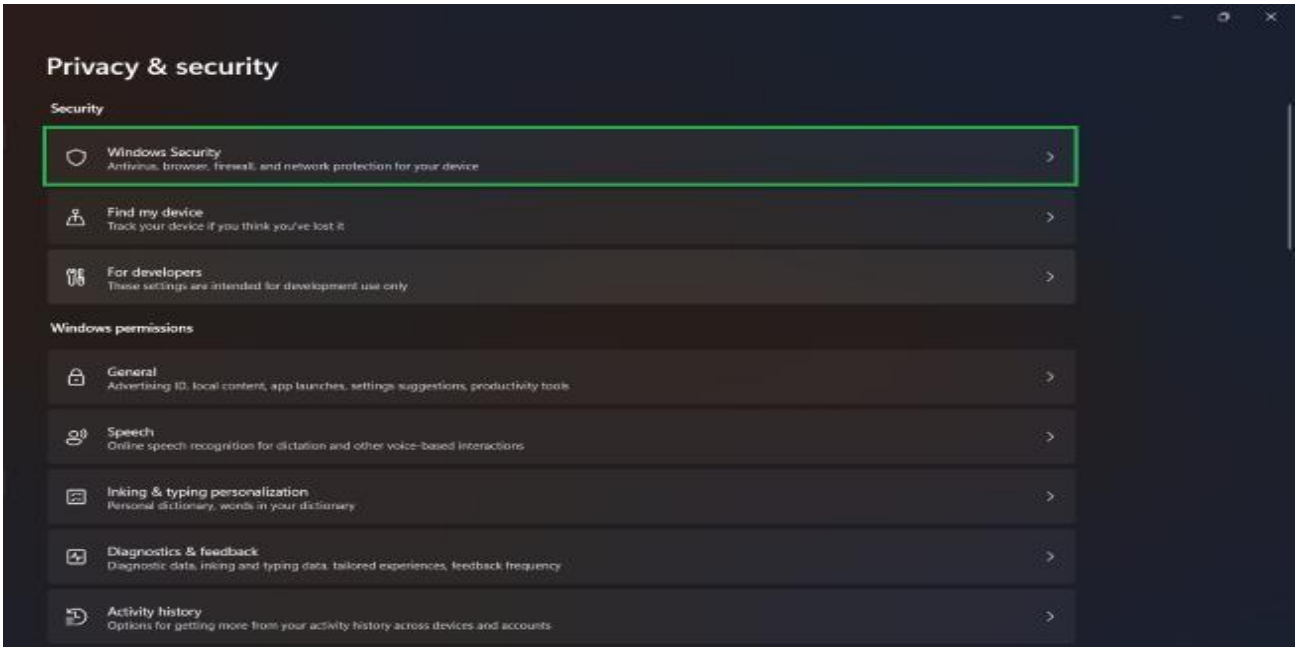


Step 2: Search **"Settings"** in the search bar if you do not find the Settings icon in Start menu.

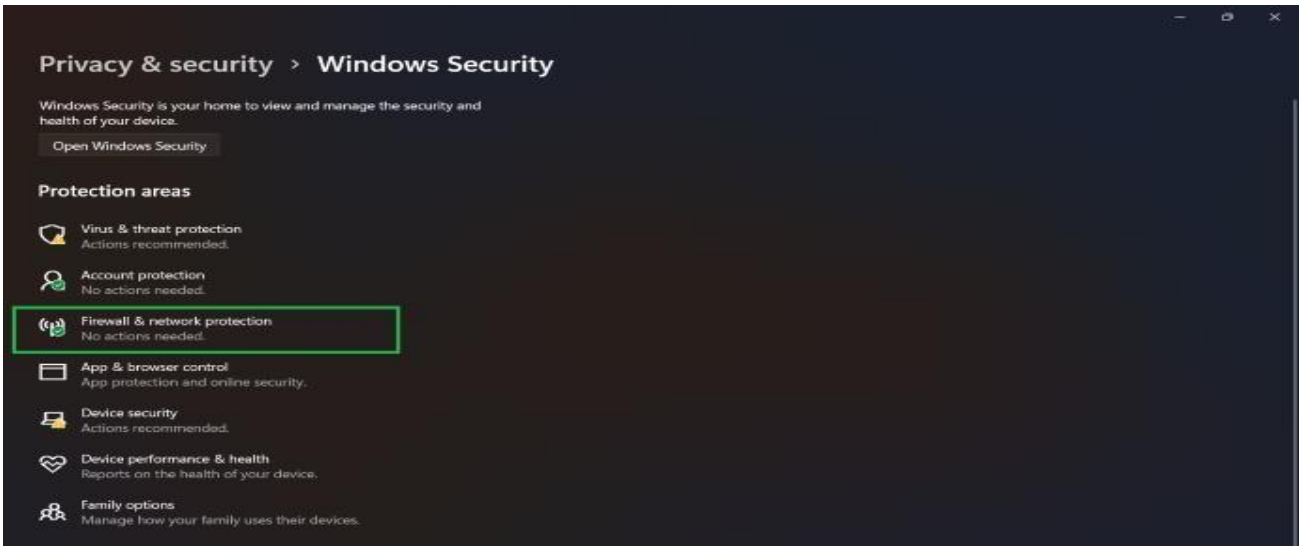


Step 3: In the left pane of Settings, click **Privacy & security**.

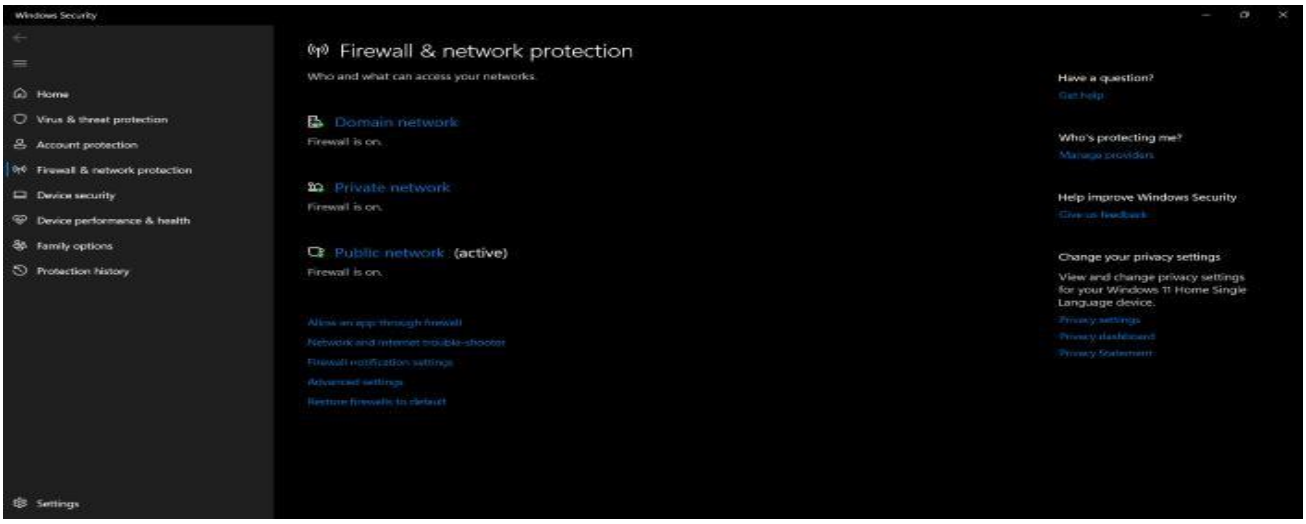
Step 4: Click **Windows Security** option in Privacy & security menu.



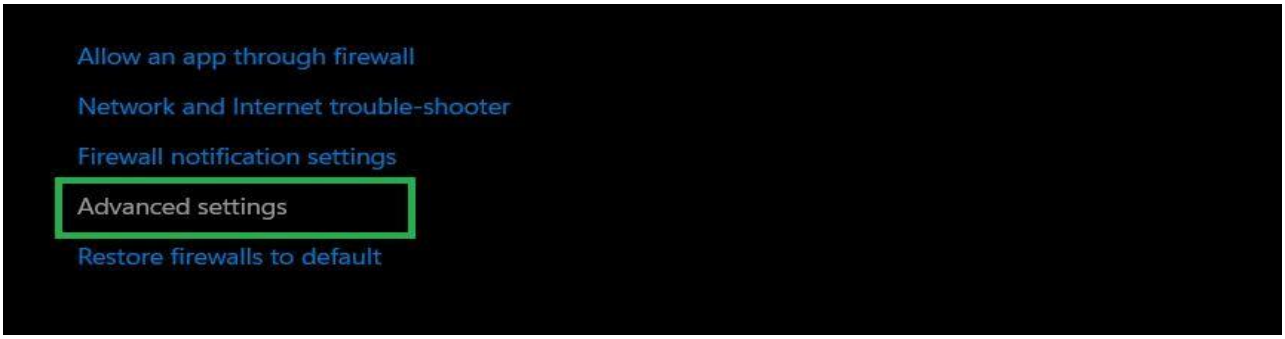
Step 5: Select **Firewall & network protection**.



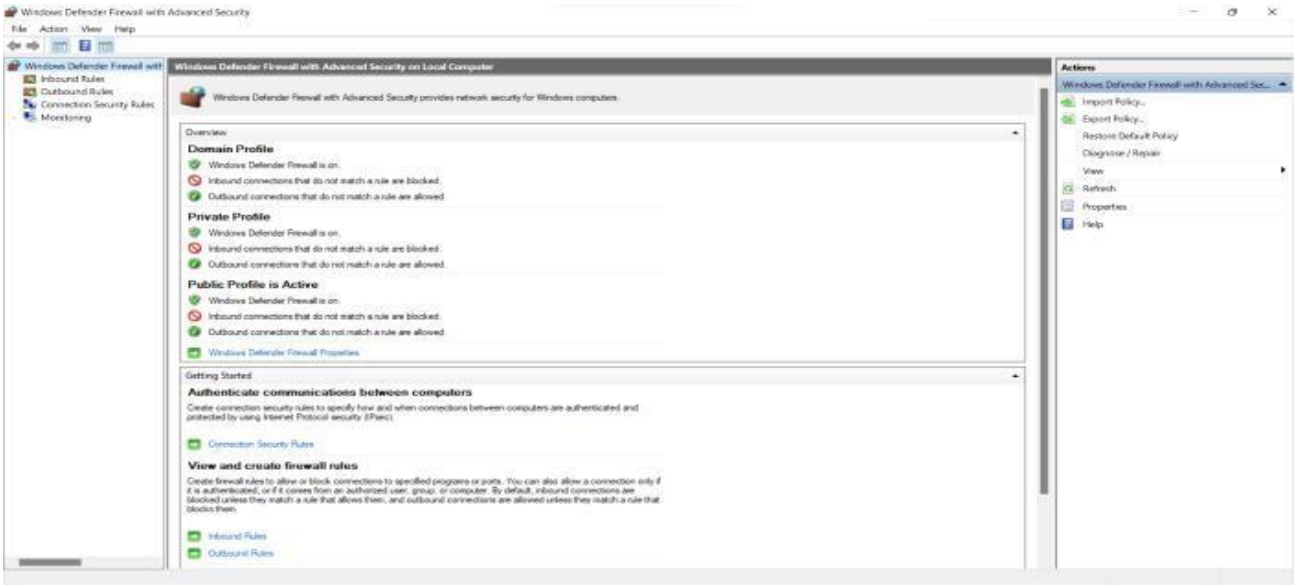
Step 6: Now **Window's Security** window will pop up window's. Here you can verify whether your Defender firewall is active or not.



Step 7: Now to configure the firewall according to your requirement, click **Advanced settings**. You will be prompted by User Account Control to give Administrative access to Windows Defender to make changes. Click **Yes** to proceed.



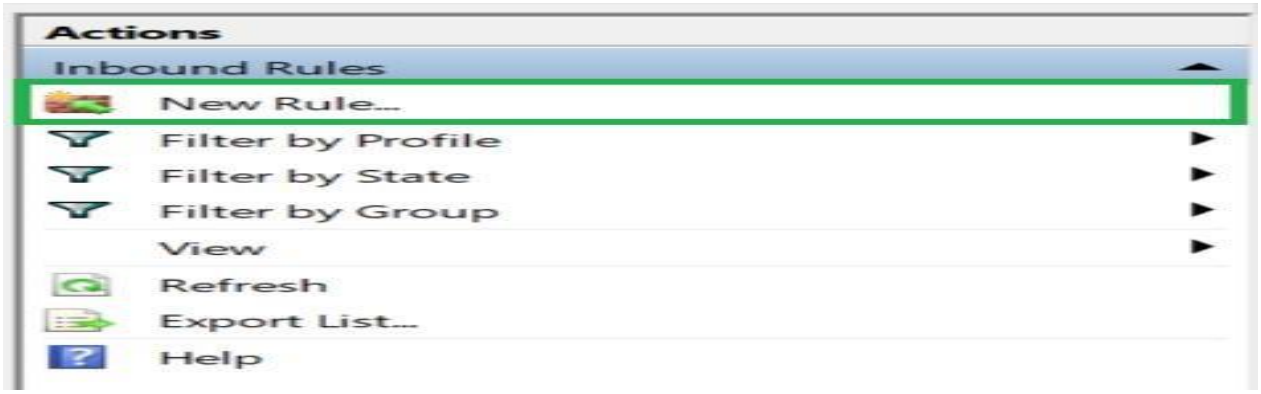
Step 8: Windows Defender Firewall with Advanced Security window will launch after giving administrative permission.



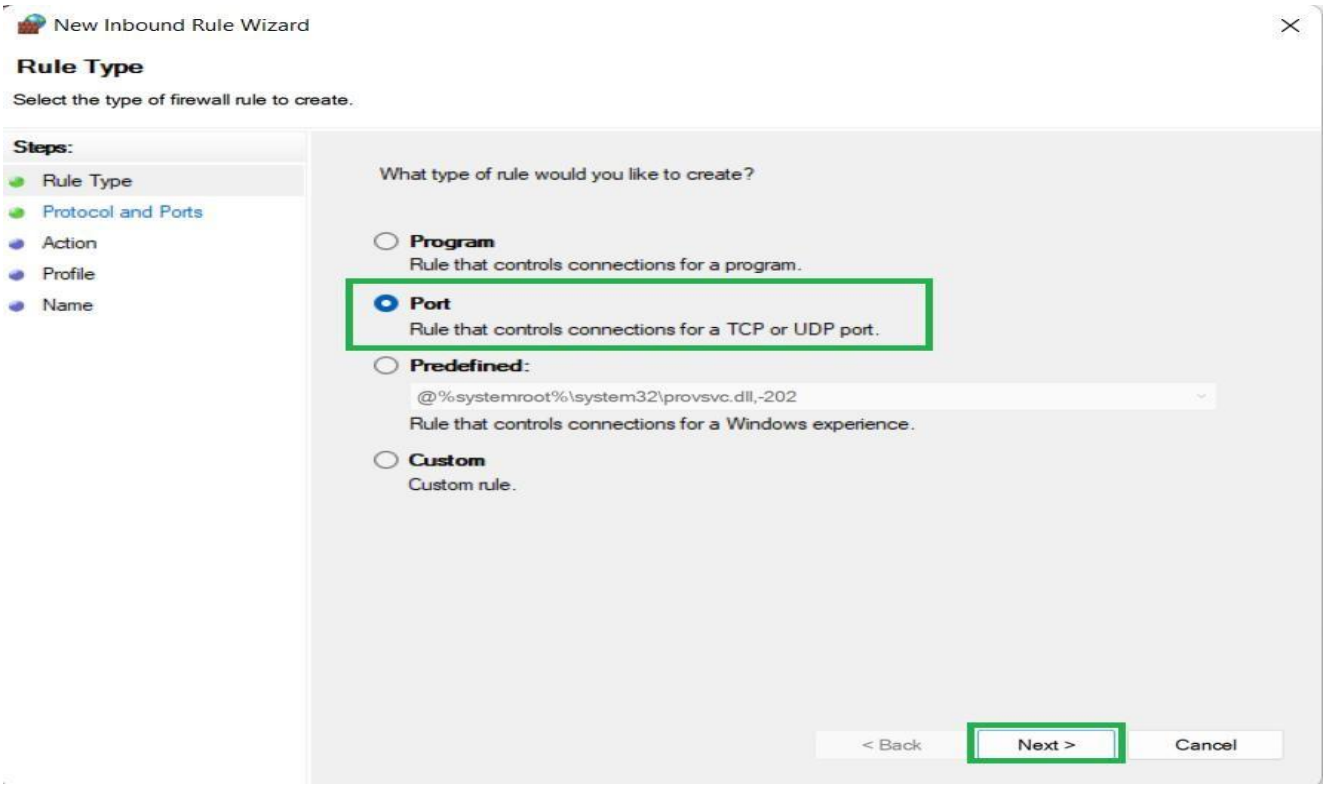
Step 9: The left pane has several options:

- Inbound rules: Programs, processes, ports can be allowed or denied the incoming transmission of data within this inbound rules.
- Outbound rules: Here we can specify whether data can be sent outwards by that program, process, or port.

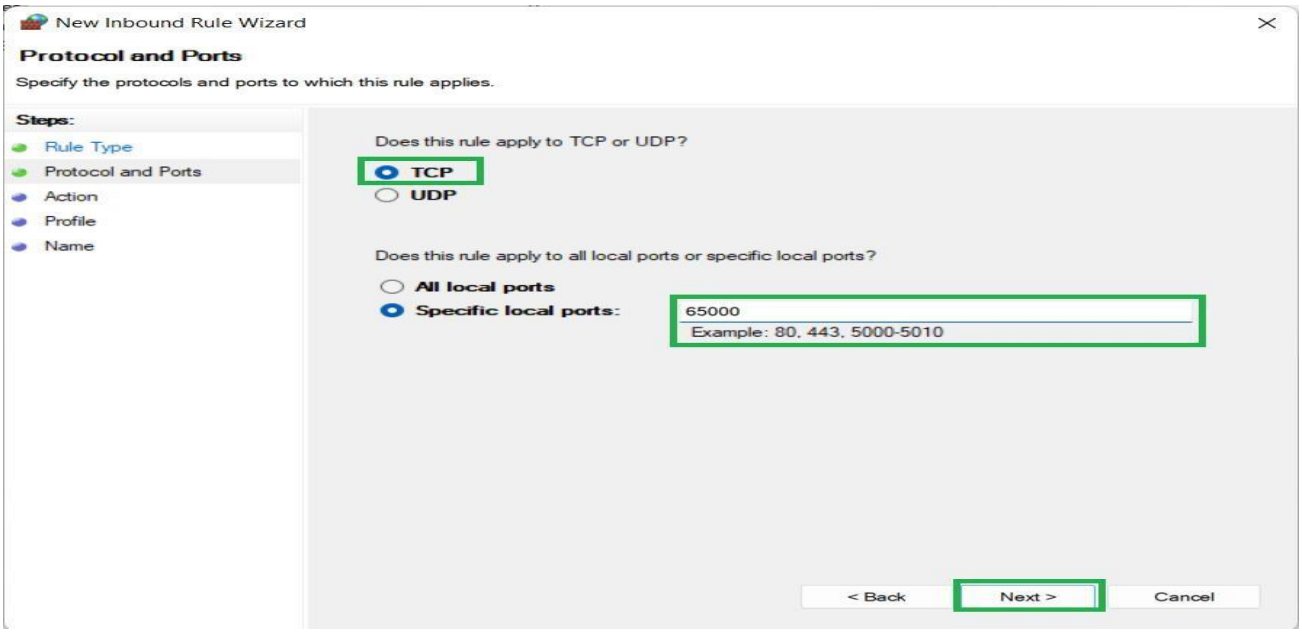
Step 10: To add a new inbound rule, select **Inbound Rules** option, then click **New Rule…** from the right pane.



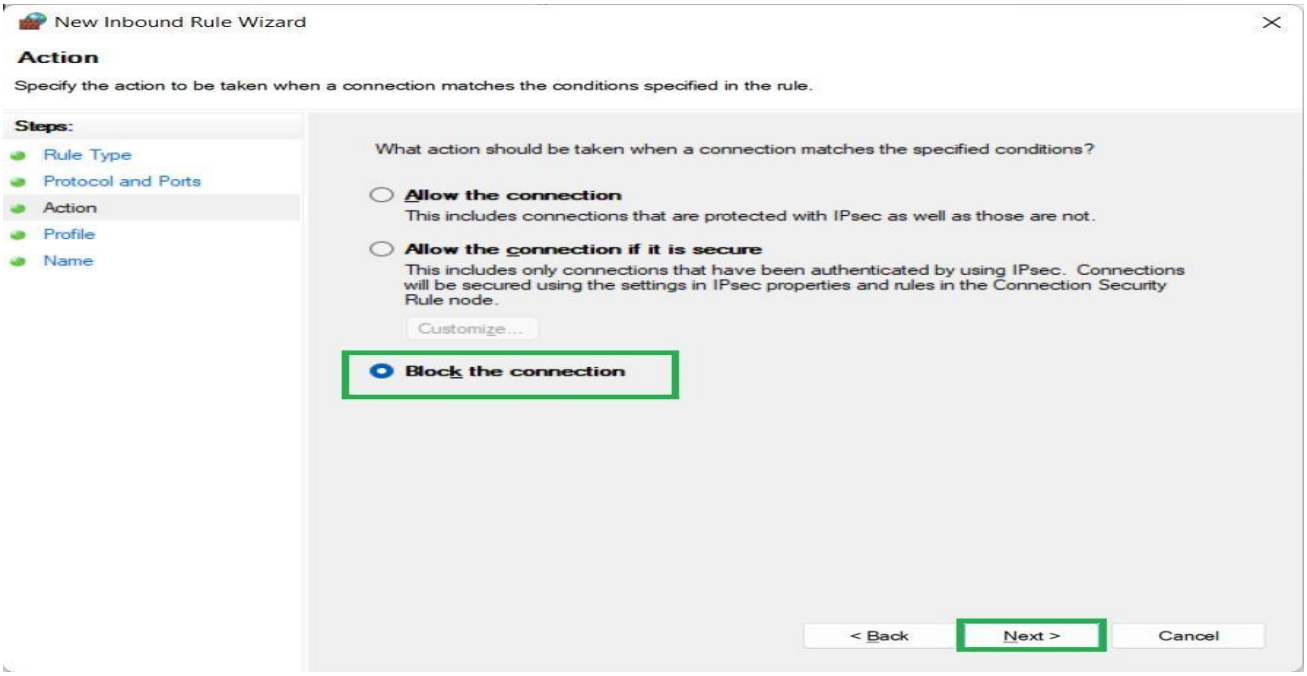
Step 11: Now we will configure an inbound rule for a network port. A **New Inbound Rule Wizard** window pops-up, select Port option and click next.



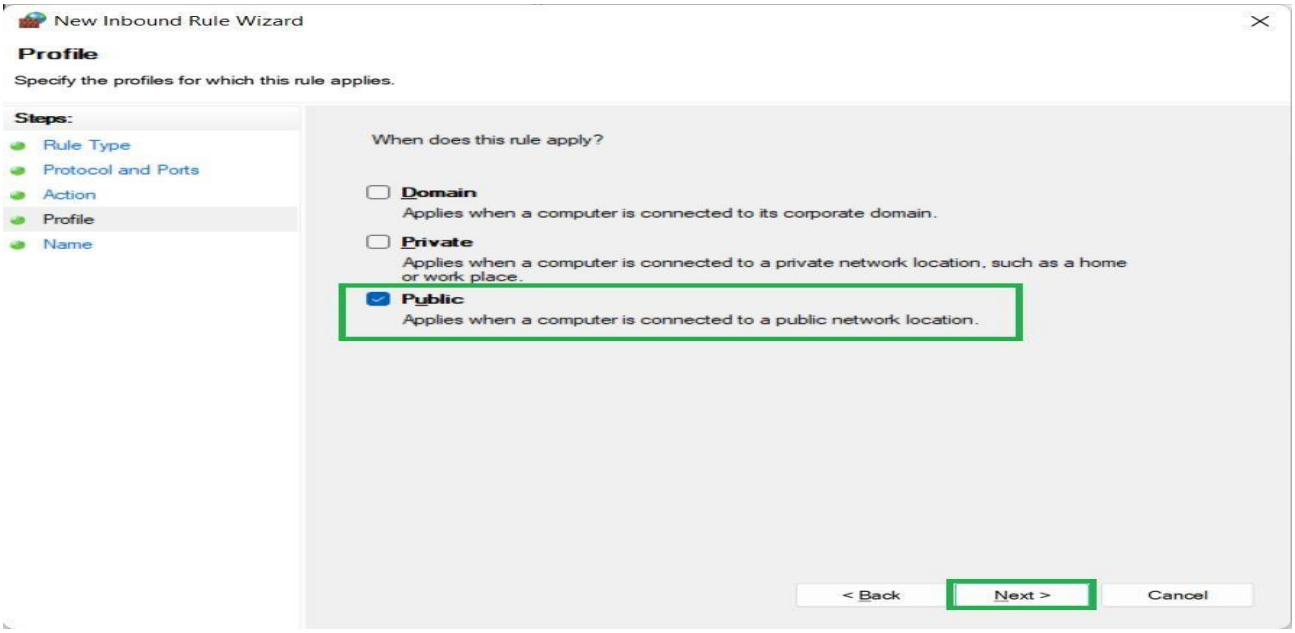
Step 12: Now select **TCP** and specify port number **65000**.



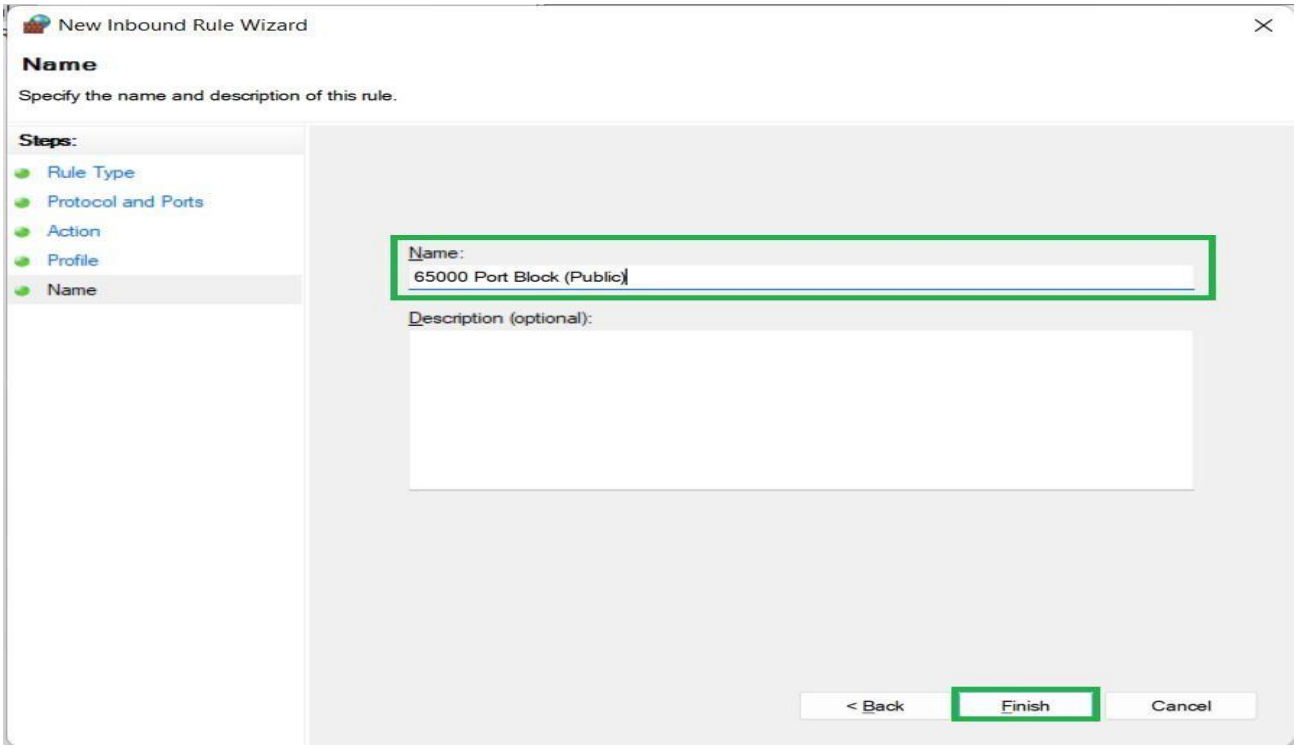
Step 13: Now we can select the action we need to take on this port. We will block the inbound connection by selecting **Block the connection** option then click **Next**.



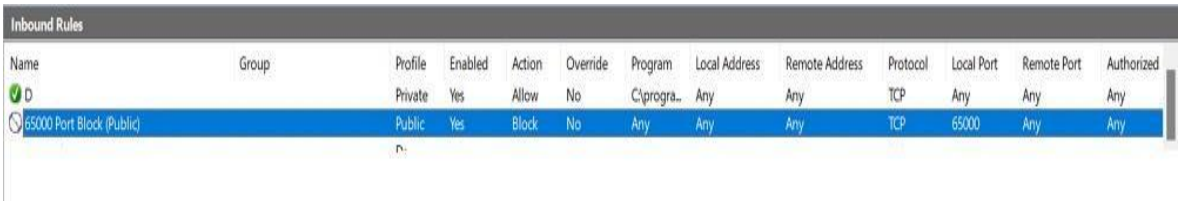
Step 14: Here we can specify when should this rule come into action. We will keep only **Public** option selected and move **Next**.



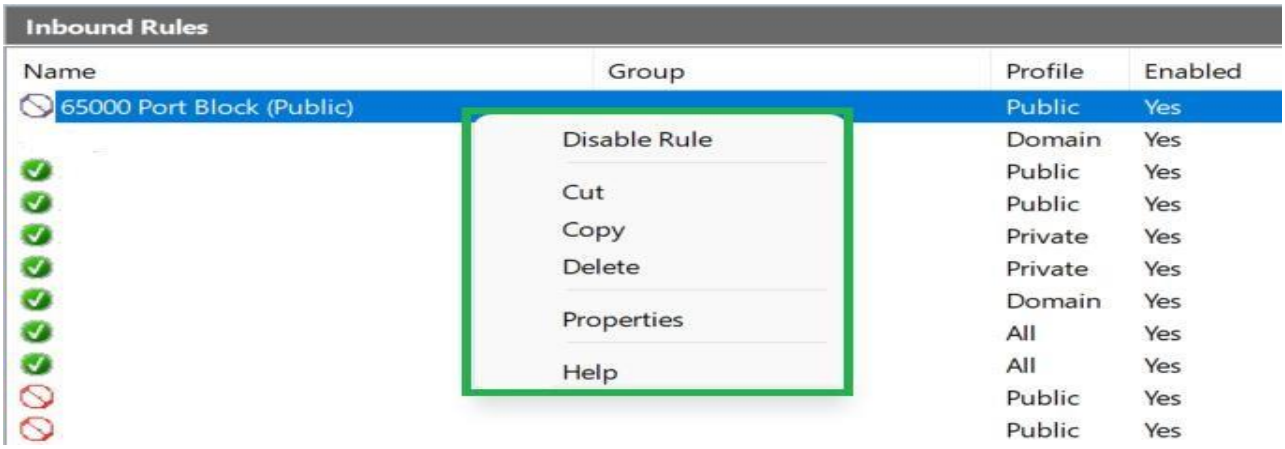
Step 15: This is the last step. Here we provide a name to this rule so that we can keep track of it later in the Inbound rules list. Write the name "**65000 Port Block (Public)**". Click **Finish**.



Step 16: The inbound rule is successfully created. We can find "**65000 Port Block (Public)**" in the Inbound rules list.



Step 17: Right-click the rule we just created and there are multiple options with which it can be **Disabled** or **Deleted**.



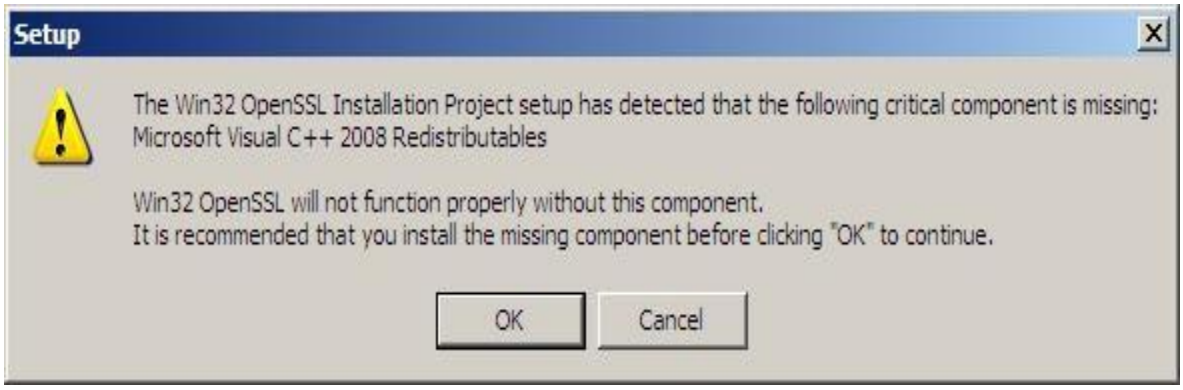
PRACTICAL. 4

AIM:Generating password hashes with OpenSSL.

OpenSSL - Installation under Windows

.

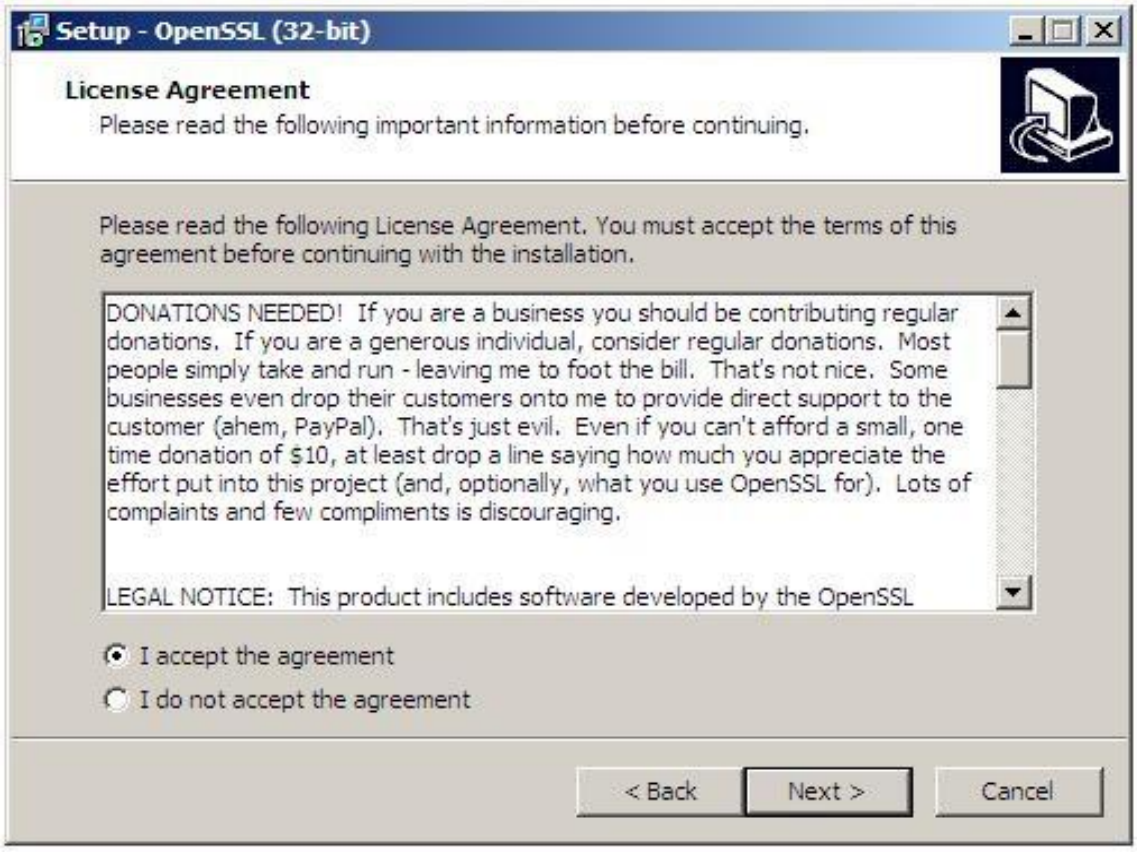
1. Download the OpenSSL for Windows installation package.
2. Double-click the installation file.
3. If the following error message appears, you should install Microsoft Visual C++ 2008 Redistributables. The installation file can be downloaded here.



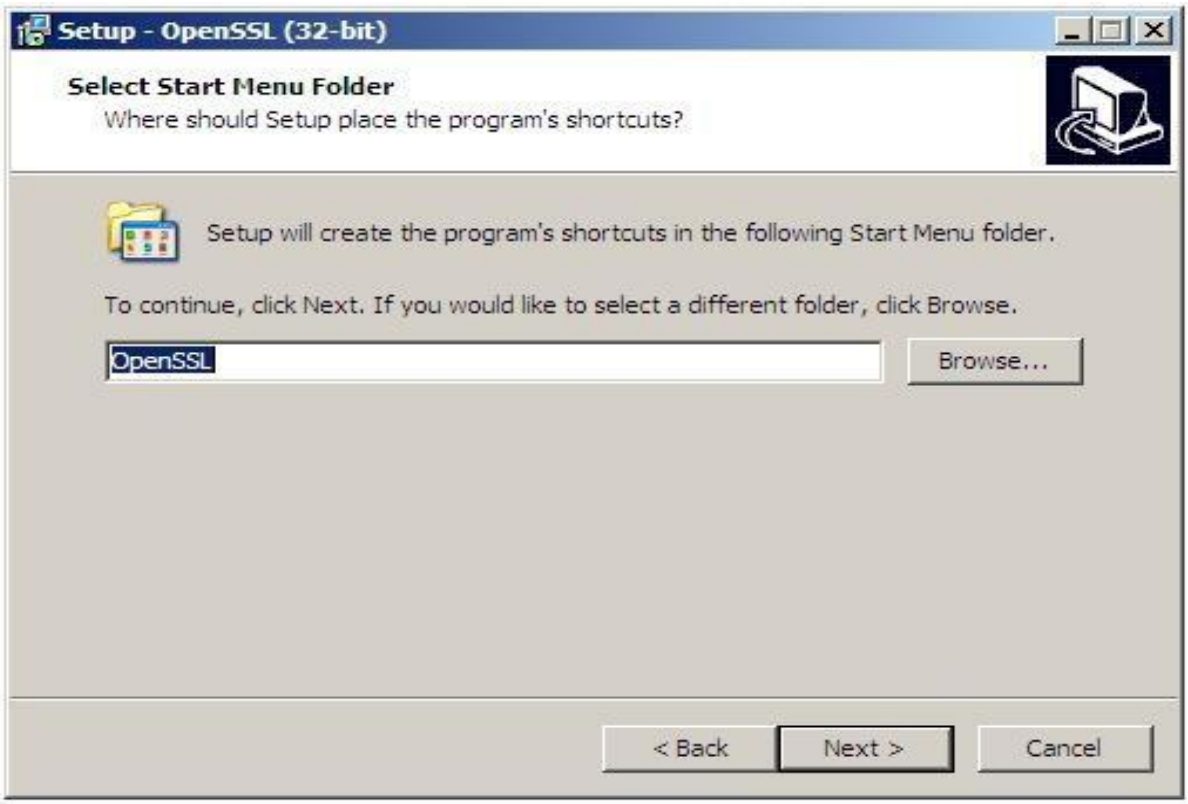
4. Double-click the installation file and click on Next

5. Click on I accept the agreement, followed by Next.

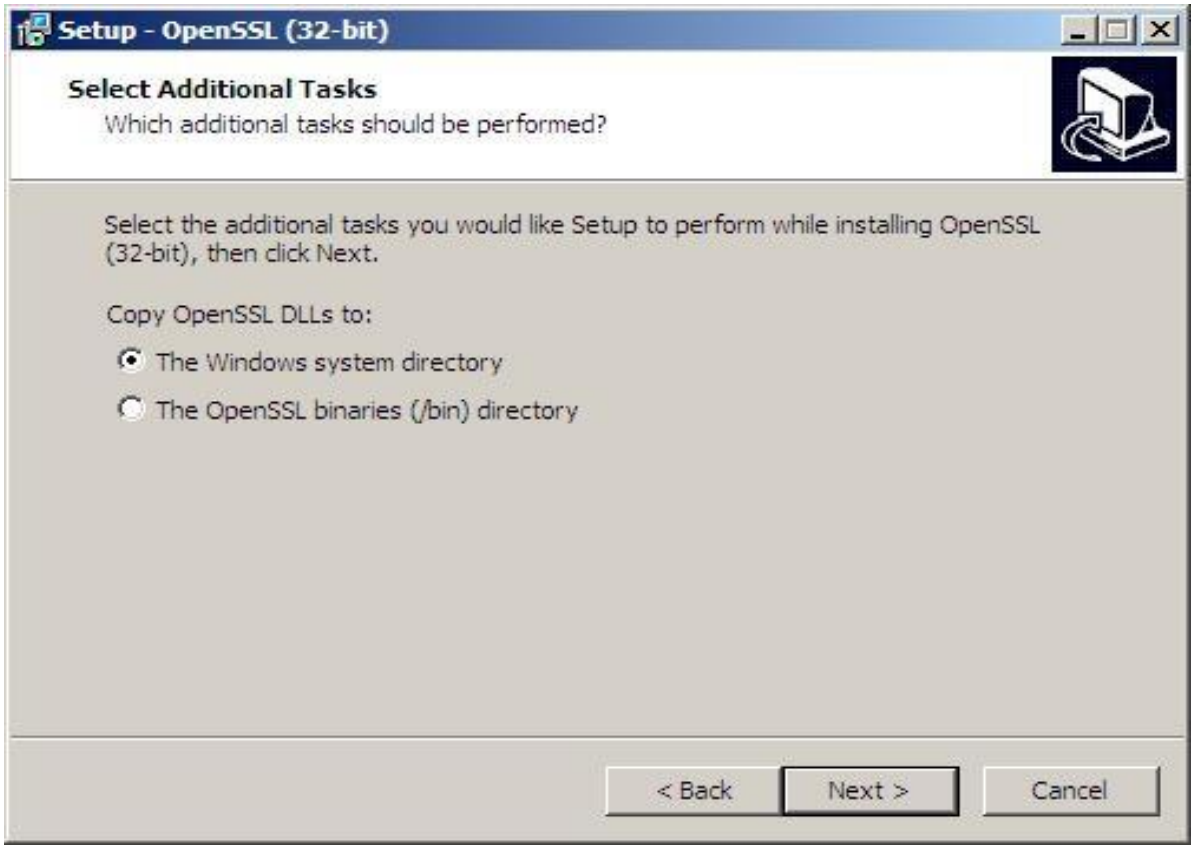
6. Leave the default installation path (C:\OpenSSL-Win32) and click on Next.



7. Leave the default Startmenu folder(OpenSSL) and click on Next.

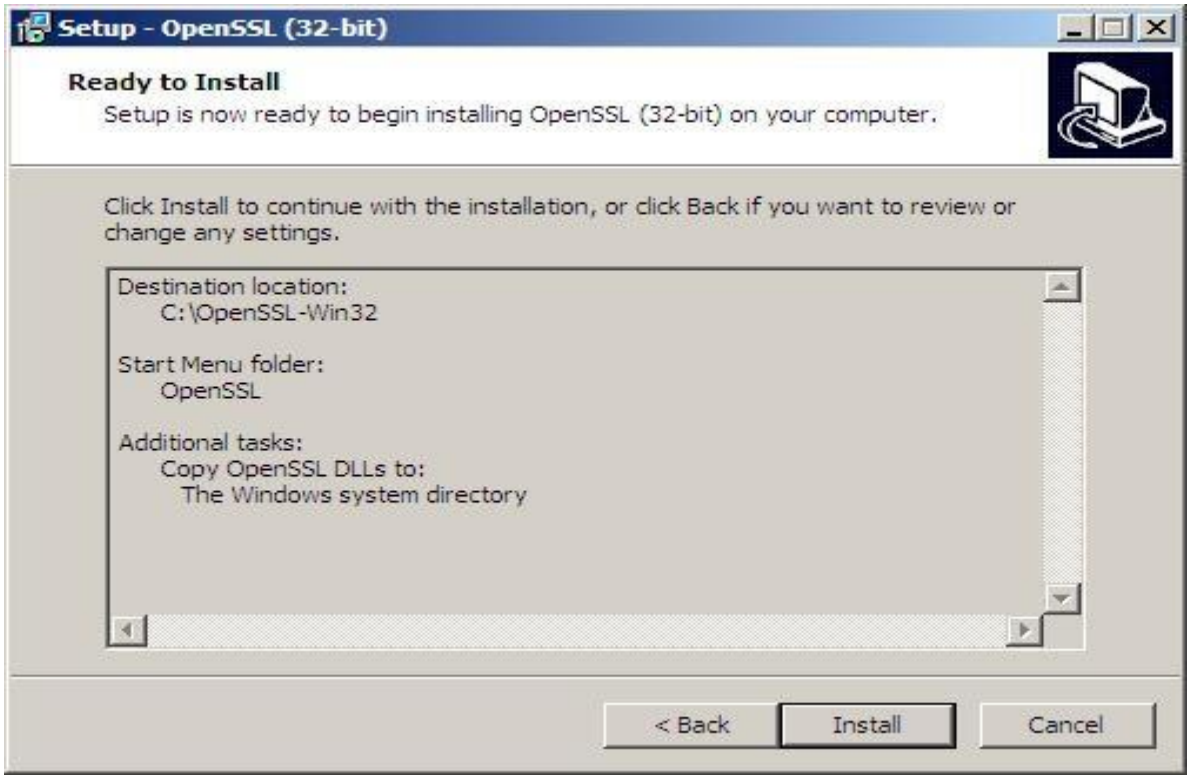


8. Leave the The Windows system directory and click on next



.

9. Click on Install.



10. Click on Finish once the installation has been completed.

Generating Password Hashes Using OpenSSL

Step 1: Open the Terminal

Open a terminal window on your system (Linux/macOS or Git Bash on Windows).

Step 2: Run the Command

To generate a password hash using the **SHA-512** algorithm, run the following command:

```bash
openssl passwd -6 mypassword
```

Output

```swift
$6$DyTboW9bAIdV2RDO$1CMigZAKhERp5J5F8/0T0Lt5Qq8dP5Qh4EZzU8PKR4dKeBbIccsHoCSPVbvhN6NeDhYk3XMo8
```

2. **Using SHA-256 Algorithm**

Command:

```bash
openssl passwd -5 mypassword
```

Output

```perl
$5$Fi7gCT3pZOYx2cfZ$ZJv0.Cz0/MuPOzLDlj8k7zSCG2eYfFVSPToCRDJDbB3
```

3. **Using MD5 Algorithm**

Command:

```bash
openssl passwd -1 mypassword
```

Output

```perl
$1$O4wb0RWv$RqlG41oJzflgfksj6ldOA1
```

PRACTICAL: 5

AIM: Perform a wireless audit of an access point / router and decrypt WEP and WPA.

DESCRIPTION :

NetStumbler (also known as Network Stumbler) aircrack on ubuntu is a tool for windows that facilitates detection of Wireless LANs using the 802.11b, 802.11a and 802.11g WLAN standards. It is one of the Wi-Fi hacking tool which only compatible with windows; this tool also a freeware. With this program, we can search for wireless network which open and infiltrate the network. It's having some compatibility and network adapter issues.

PROCEDURE:

Step 1: Download and install Netstumbler

Step 2: It is highly recommended that your PC should have wireless network card in order to access wireless router.

Step 3: Now Run Netstumbler in record mode and configure wireless card.

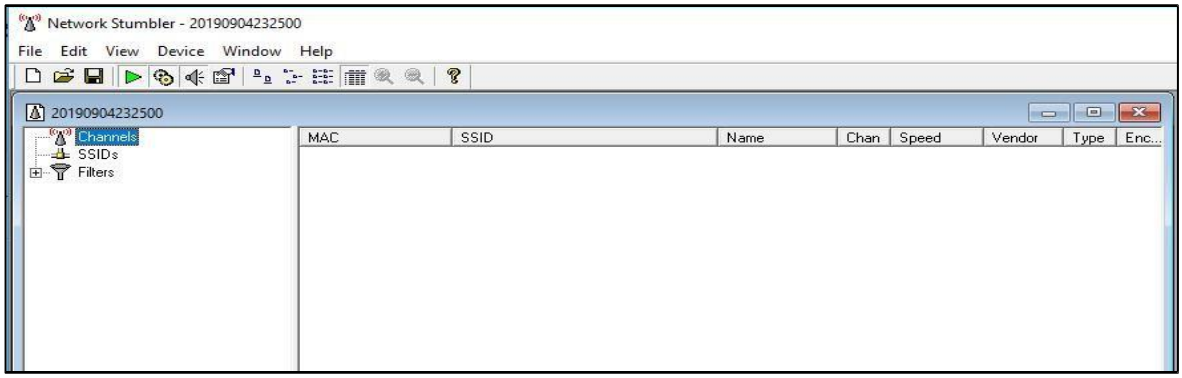
Step 4: There are several indicators regarding the strength of the signal, such as GREEN Indicates Strong, YELLOW and other color indicates a weaker signal, RED indicates a Very weak and GREY indicates a signal loss.

Step 5: Lock symbol with GREEN bubble indicates the Access point has encryption enabled.

Step 6: MAC assigned to Wireless Access Point is displayed on right hand pane.

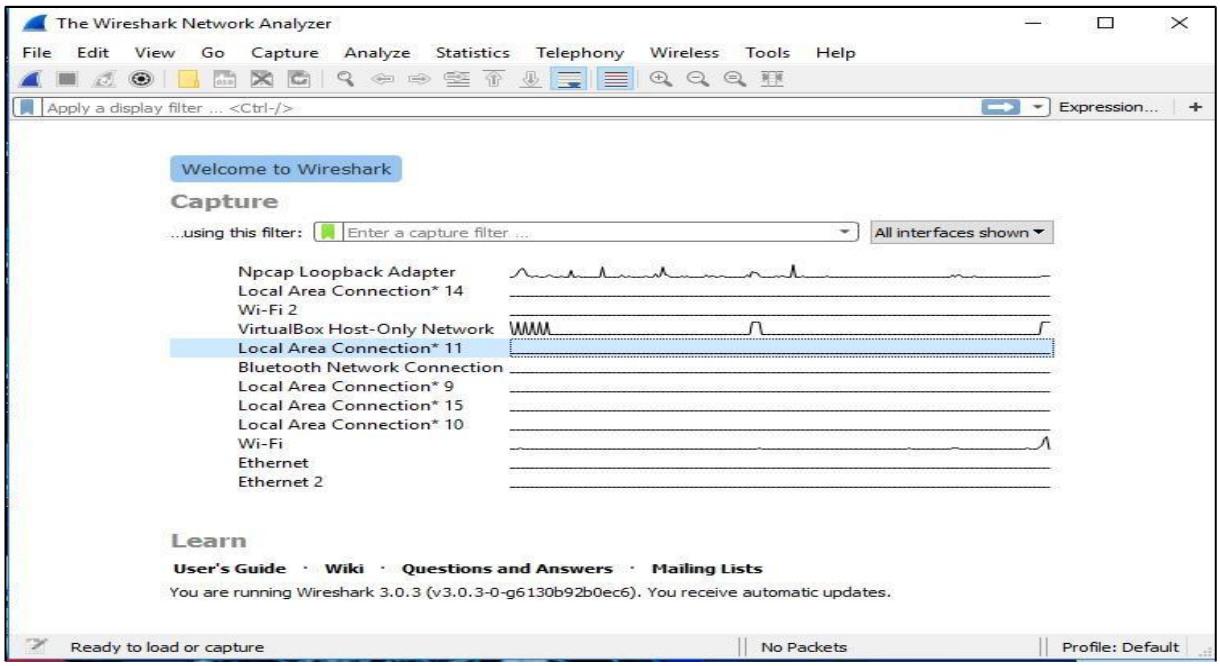
Step 7: The next column displays the Access points Service Set Identifier [SSID] which is useful to crack the password.

Step 8: To decrypt use Wire Shark tool by selecting Edit preferences IEEE 802.11



Step 9: Enter the WEP keys as a string of hexadecimal numbers as A1B2C3D4E5

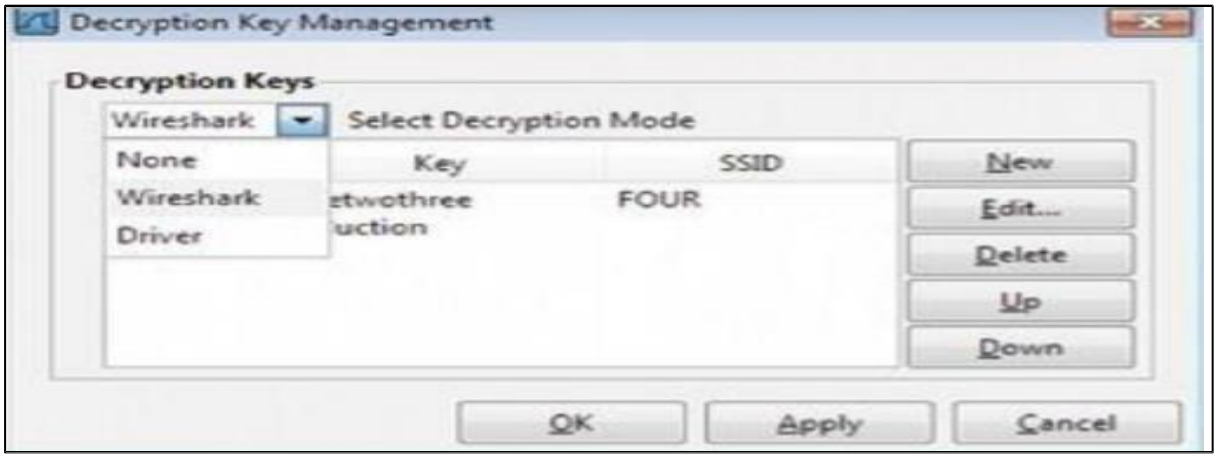
To decrypt use WireShark tool by selecting Edit->preferences->IEEE 802.11 Enter the WEP keys as a string of hexadecimal numbers as A1B2C3D4E5.



Adding Keys: Wireless Toolbar

- If you are using the Windows version of Wireshark and you have an AirPcap adapter you can add decryption keys using the wireless toolbar.
- If the toolbar isn't visible, you can show it by selecting View->Wireless Toolbar. Click on the Decryption Keys. button on the toolbar:

This will open the decryption key management window.
As shown in the window you can select between three decryption modes: None, Wireshark, and Driver:



PRACTICAL: 6

AIM: Setup Honey Pot and monitor the Honey Pot on network.

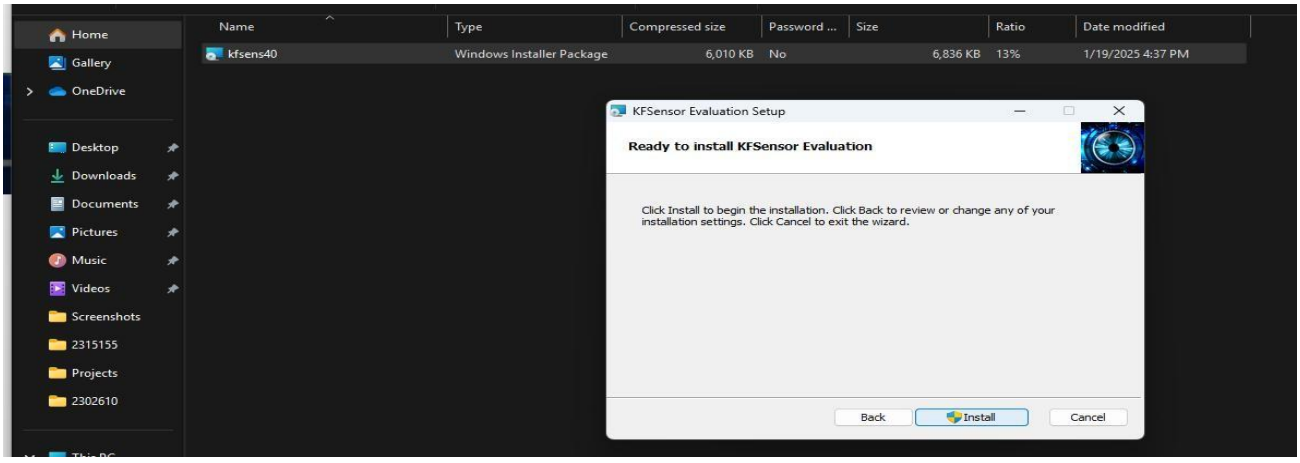
Honey pot:
Honey pot is a devise placed on computer network especially design capture malicious network traffic.

KF Senor:

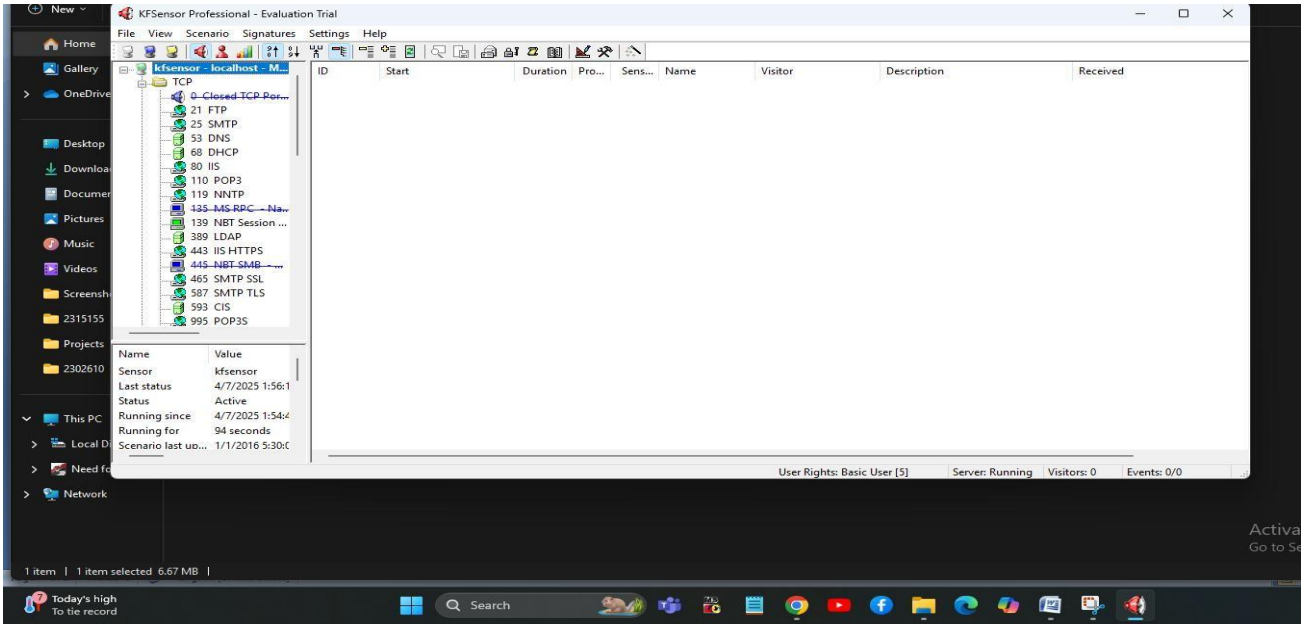
1. Windows based honey pot knows as KF Senor.
2. KF Senor is a tool to setup as honey pot when KF Sensor is running it placed a Siren icon in the windows system tray in the bottom right of the screen.
3. If there are no alerts then green icon is displayed.
4. It detects incoming attack or ports scanning and reports it to you.

Procedure:
1. Download the KF Sensor Evaluation setup file from KF Sensor website:
https://www.kfsensor.net/kfsensor/free-trial/

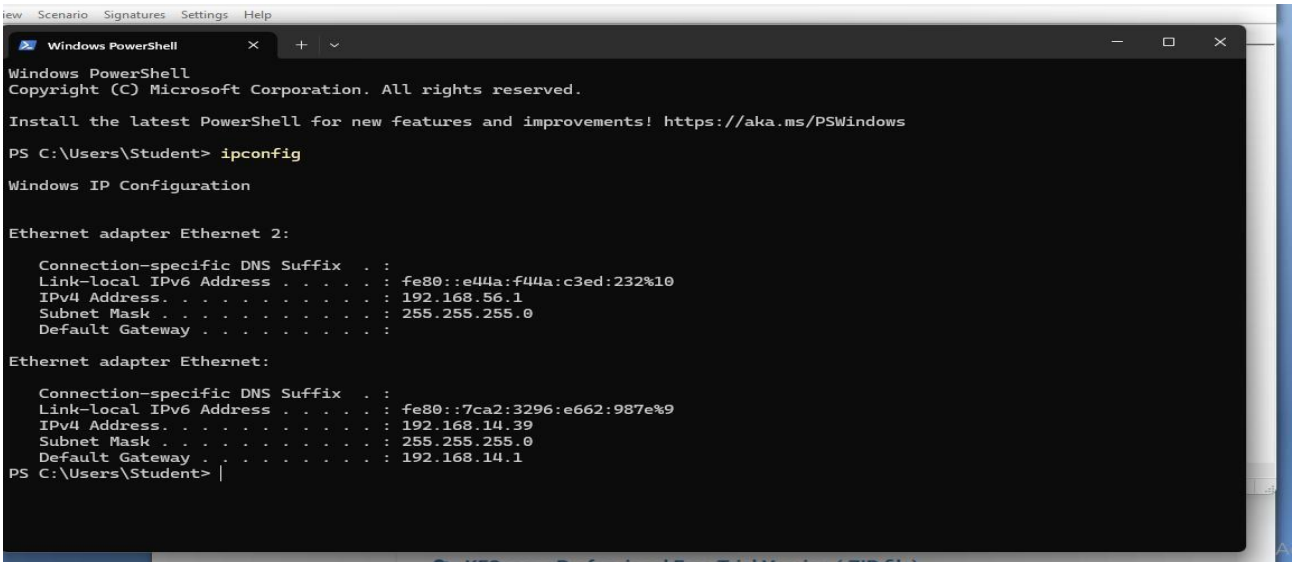
3. Install with license Agreement and appropriate Directory path and click finish.



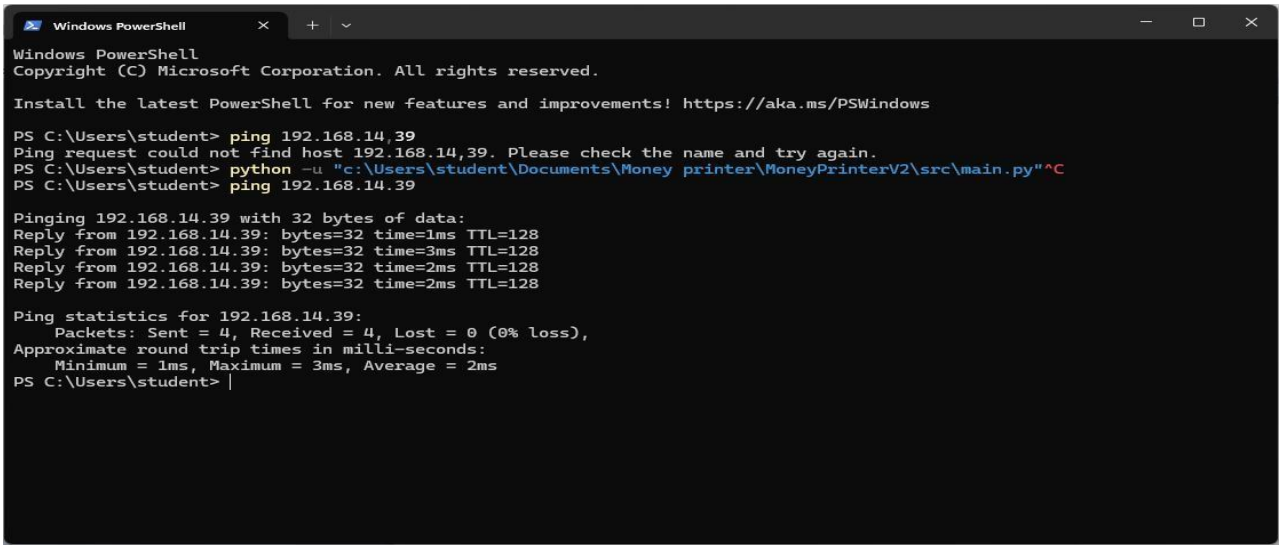
3. Now KF Sensor honey pot is ready to running on the network host.
4. Navigate start > All program > KF Sensor.
5. Right Click on KF Sensor icon and select run as administrator.
6. KF Sensor will look like this:



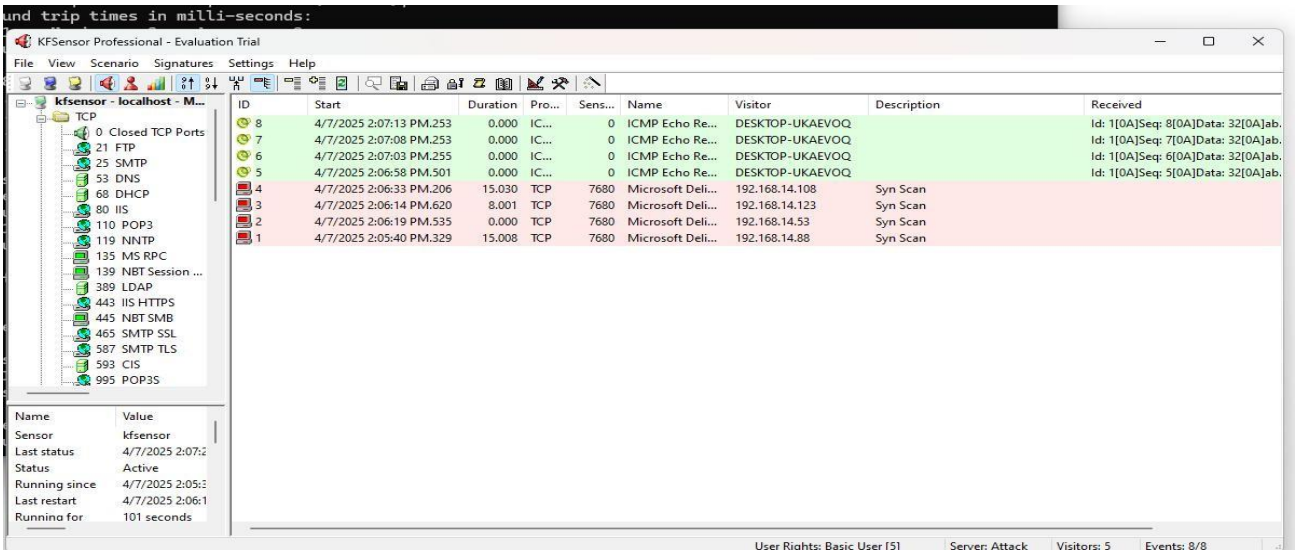
7. Now find the ip address of Honey pot system using" ipconfig" command.
8.



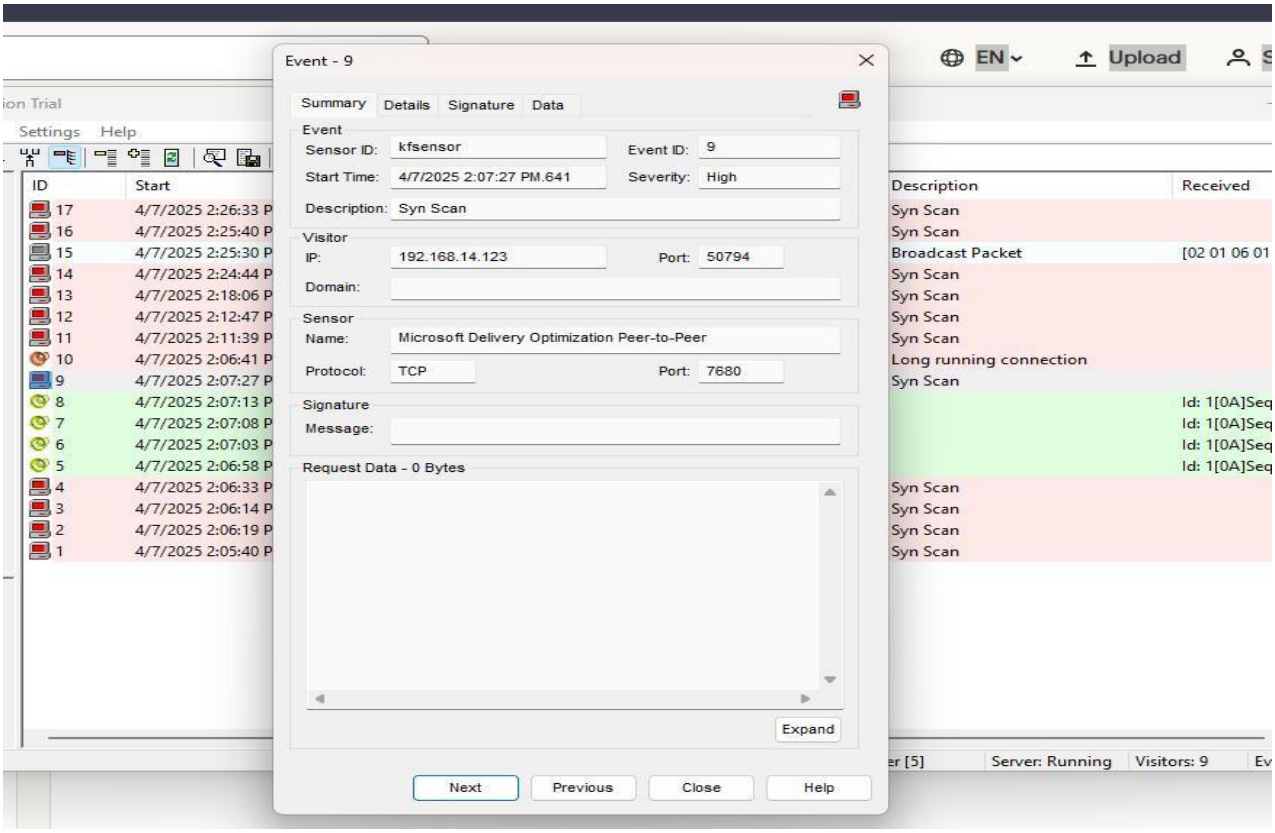
9. For any other system on the network will try to ping the honey pot system using ping command.



10. Then it will display the attack details look like this:



11. Select and open any one of activity and it will show the details about the attack.



PRACTICAL: 7

AIM: Analysis of the security vulnerabilities of e-commerce services.

1. Financial Frauds or Payment Frauds

This type is one of the most typical for eCommerce and dates back to the very first attempts of the businesses going online. Often, scammers used to make unauthorized transactions and immediately wipe out the trails. Or else, they can use the fake emails, accounts, and names, and even IP addresses to look like the real customer.

After they have requested a refund with, for instance, a fake screenshot, most eCommerce platforms basically give them money for nothing, especially if they're not aware of this financial trick.

With being reported in over 70% of all attacks, payment frauds are still one of the top reasons why companies experience huge cost losses.

2. Spam Attacks

Though emails are considered to be the most powerful marketing channel for eCommerce, they are also the typical web security vulnerabilities hackers can easily take advantage of.

The random comments left on the product pages, under your blog posts, or the contact forms can not only harm the customers' trust but also slow down your platform as well.

Needless to say, that one infected link left by a spammer is more than enough to affect your site's speed, provide access to personal customer information and other sensitive data.

Additionally, the spamming activity can become a serious threat to the customers' security as well, which can easily undermine your site's credibility.

3. Triangulation Fraud

One of the most recent and large-scale security vulnerabilities detected nowadays is triangulation fraud. This stands for creating a fake site with an identical interface and products at a cheaper price.

After the customers complete the transaction, they basically donate the money to the criminals, as the products they wanted to purchase simply don't exist and never be shipped to them.

The reason why this type of fraud is harmful to your eCommerce platform is that you can lose your new clients, loyal customers, and their trust as well: no one wants to go back to the site (even with the slight differences in a brand's name or interface) after being cheated there at once.

4. Web Application Security Vulnerabilities

At present, the level of competition in different business areas makes companies do their best to meet all the customers' needs. For online stores, web applications are simply a must to attract more clients to their platform.

For instance, it's essential for eCommerce clients to create the wish lists of the products they want to buy next, look for the featured products, check the special offers and get the personalized list of products they are probably interested in.reatew

The use of smartphones has only enhanced the demand for web app creation. However, having created one is still not that easy as to maintain and update it regularly.

Developers should not only focus on the customer experience and comfortable interface but also on the software security vulnerabilities as well. Having omitted this stage of web app development, you can easily give a green light to the criminals for the attack. They can easily play with fake transactions and refunds, gift cards, and even the critical data of your eCommerce platform.

5. Bot Attack

Some criminals also attack eCommerce sites with bots, that basically act like real users and can hardly be detected by the security system.

This is why bot attack is considered to be one of the common security vulnerabilities you should always keep in mind. Usually, you can check the bot traffic in the site's analytics and get the records about the exact time and details of their behavior.

However, bots are not just fake users that can boost your traffic to slow down the site's speed. Instead, they can also steal the personal information of your customers, record their log-in credentials and bank information, manipulate the products' prices and randomly block them, thus making your eCommerce platform less secure and user-friendly.

6. Brute Force Attacks

Brute-force attacks refer to the hacking method of guessing the system passwords. So far that's one of the most dangerous security vulnerability types that can attack your online store's panel and attempt to get full access to it.

During this attack, the various programs and complex algorithms are used to generate any possible combination to crack your site's password. After that, any scenario is possible: criminals can ask for the reward or steal the client's personal data, send spam offers, etc — all they planned to do since the site owner has lost access to the admin panel.

7. DoS & DDoS Attacks

Many e-commerce websites have incurred losses due to disruptions in their website and overall sales because of DDoS (Distributed Denial of Service) attacks. What happens is that your servers receive a deluge of requests from many untraceable IP addresses causing it to crash and making unavailable to your store visitors.

8. Malware

Hackers may design a malicious software and install on your IT and computer systems without your knowledge. These malicious programs include spyware, viruses, trojan, and ransomware.

The systems of your customers, admins, and other users might have Trojan Horses downloaded on them. These programs can easily swipe any sensitive data that might be present on the infected systems and may also infect your website.

9. Man in The Middle (MITM)

A hacker may listen in on the communication taking place between your e-commerce store and a user. Walgreens Pharmacy Store experienced such an incident. If the user is connected to a vulnerable Wi-Fi or network, such attackers can take advantage of that.

10. e-Skimming

E-skimming involves infecting a website's checkout pages with malicious software. The intention is to steal the clients' personal and payment details.

PRACTICAL:8

AIM:- Case Study on Authentication and Encryption.

Case Study: Authentication and Encryption in Online Banking Systems

Background

Online banking systems are prime targets for cybercriminals due to the sensitivity of financial data. Ensuring secure access and safe data transmission between users and servers is critical. Authentication and encryption are two core pillars that protect these systems.

Part 1: Authentication

Objective

To ensure that users accessing the system are who they claim to be.

Authentication Methods Used

1. Single-Factor Authentication (SFA)
   Example: Username and password.
   Issue: Vulnerable to brute force, phishing.

2. Two-Factor Authentication (2FA)
   Example: Password + One-Time Password (OTP) sent via SMS/email or generated by an app.

3. Multi-Factor Authentication (MFA)
   Example: Password + OTP + Biometrics (fingerprint or facial recognition).

4. Biometric Authentication
   Use Case: Mobile banking apps use device biometrics like Apple Touch ID/Face ID.

Authentication Implementation: Bank of XYZ

- Users must enter their username and password.
- OTP sent to the registered device/email is mandatory.
- Optionally, a biometric scan can be set up for quicker access on mobile.

Security Challenges

- SIM-swap attacks can bypass OTP.
- Biometric spoofing is a low-probability but high-impact threat.
- Phishing websites mimic login pages to harvest credentials.

Mitigation Techniques

- Use of anti-phishing authentication mechanisms (e.g., FIDO2, security keys).
- Time-limited OTPs and device-based risk analysis.
- Regular forced password changes and account activity alerts.

Part 2: Encryption

Objective

To ensure data confidentiality and integrity during transmission and storage.

Types of Encryption Used

1. Symmetric Encryption
   Example: AES (Advanced Encryption Standard)
   Use: Internal data at rest.

2. Asymmetric Encryption
   Example: RSA (Rivest-Shamir-Adleman)
   Use: Key exchange, digital signatures.

3. Transport Layer Security (TLS)
   Use: Encrypts data during transmission (HTTPS).

Encryption Implementation: Bank of XYZ

- Data between the client and server is encrypted via TLS 1.3.
- Customer data stored in the database is encrypted using AES-256.
- RSA is used to establish a secure session before symmetric keys are exchanged**.**

Additional Practices

- Use of HMAC (Hash-based Message Authentication Code) for message integrity.
- Secure key management systems (KMS) to handle key lifecycle.
- Encrypted backups to ensure secure disaster recovery.

Challenges

- Proper key management is complex.
- SSL/TLS vulnerabilities (e.g., Heartbleed) in outdated systems.
- Performance overhead of encryption for real-time transactions.

Mitigation Strategies

- Regular updates and patching of TLS libraries.
- Deployment of hardware security modules (HSMs) for key storage.
- Load balancing to offset encryption/decryption performance hits**.**

Real-World Breach Example: Capital One (2019)

- Cause: Misconfigured AWS server.
- Issue: Although data was encrypted, the attacker gained access due to poor IAM (Identity and Access Management) configuration.
- Lesson: Strong encryption needs equally strong authentication and access control.