Internship Report

Intern: Suvhankar Dutta
Internship Organization: Redynox
Duration: 1 Month

1. Introduction

Task 1: Introduction to Network Security Basics

1. **Learn Network Security Concepts:**

🔐 1. Viruses

* Definition: Malicious code that attaches itself to legitimate files or programs and spreads when executed.

* Threat: Corrupts, deletes, or modifies files; slows down systems.

* Example: File-infector virus, Macro virus.

🪱 2. Worms

* Definition: Self-replicating malware that spreads through networks without human action.

* Threat: Consumes bandwidth, slows down networks, causes system crashes.

* Example: SQL Slammer, WannaCry worm.

🐴 3. Trojans (Trojan Horses)

* Definition: Malicious programs disguised as legitimate software.

* Threat: Creates backdoors, steals data, allows remote access.

* Example: Remote Access Trojans (RATs), Banker Trojans.

📧 4. Phishing Attacks

* Definition: Fraudulent attempts to obtain sensitive information by pretending to be a trustworthy entity via email, message, or website.

* Threat: Data theft (passwords, credit card details), identity theft.

* Example: Fake bank login pages, fraudulent emails asking for personal info.

🕵️ 5. Man-in-the-Middle (MITM) Attacks

* Definition: Attacker intercepts communication between two parties.

* Threat: Steals or alters data being transmitted.

* Example: Eavesdropping on login credentials over unsecured Wi-Fi.

🔓 6. Denial of Service (DoS) / Distributed DoS (DDoS)

* Definition: Overwhelms a server or network with traffic to make it unavailable.

* Threat: Disrupts service for users and businesses.

* Example: Flooding a website with millions of requests to crash it.

👨‍💼 7. Insider Threats

* Definition: Security risks originating from employees or others with access.

* Threat: Data theft, system sabotage, accidental breaches.

* Example: An employee stealing confidential company data.

🔍 8. Spyware

* Definition: Software that secretly monitors user activity and sends data to attackers.

* Threat: Theft of credentials, surveillance.

* Example: Key loggers, tracking cookies.

💣 9. Ransomware

* Definition: Malware that encrypts user data and demands payment to restore access.

* Threat: Data loss, financial damage, downtime.

* Example: WannaCry, Locky.

📱 10. Adware

* Definition: Unwanted software that displays ads and may track user activity.

* Threat: Privacy invasion, slows down devices.

* Example: Pop-ups, browser redirects.

basic security concepts that are essential in protecting networks and systems:

🔥 1. Firewalls

* Definition: A firewall is a security device (hardware or software) that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

* Purpose: Blocks unauthorized access while permitting legitimate communication.

* Types:

  * Packet-filtering firewall

  * Stateful inspection firewall

  * Next-generation firewall (NGFW)

* Example: Preventing unknown IP addresses from accessing your computer or server.

🔐 2. Encryption

* Definition: The process of converting data into a coded format (ciphertext) so only authorized parties can understand it.

* Purpose: Protects data confidentiality during storage and transmission.

* Types:

  * Symmetric encryption (same key for encryption/decryption) – e.g., AES

  * Asymmetric encryption (public and private keys) – e.g., RSA

* Example: HTTPS uses encryption to protect data exchanged between your browser and websites.

🛠️ 3. Secure Network Configurations

* Definition: The practice of setting up and maintaining network systems in a secure manner to minimize vulnerabilities.

* Key Practices:

  * Disabling unused ports and services

  * Changing default passwords

  * Implementing strong access control

  * Regular patching and updating

  * Using secure protocols (like SSH instead of Telnet)

* Purpose: Reduces the attack surface and prevents unauthorized access.

* Example: Configuring a router to block unused ports and enable WPA3 encryption for Wi-Fi.

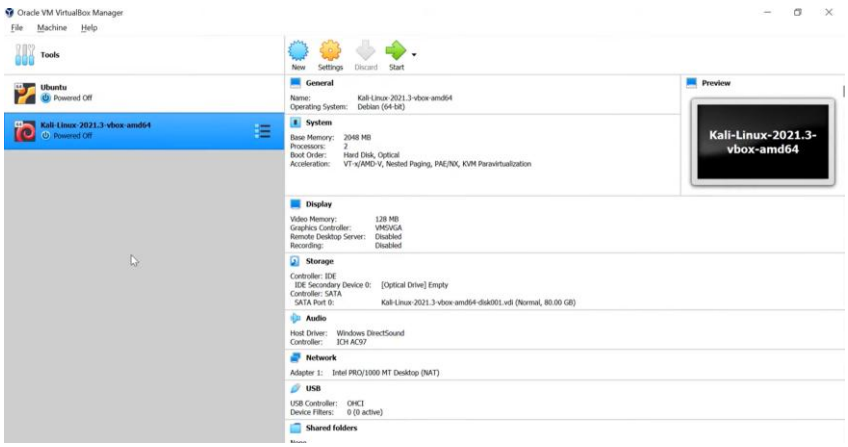
Summary Table:

Concept	Purpose	Example
🔥 Firewall	Control network traffic	Block traffic from suspicious IPs
🔐 Encryption	Protect data confidentiality	HTTPS, VPN, encrypted emails
🛠️ Secure Configuration	Strengthen system/network security	Disable unused ports, change default logins

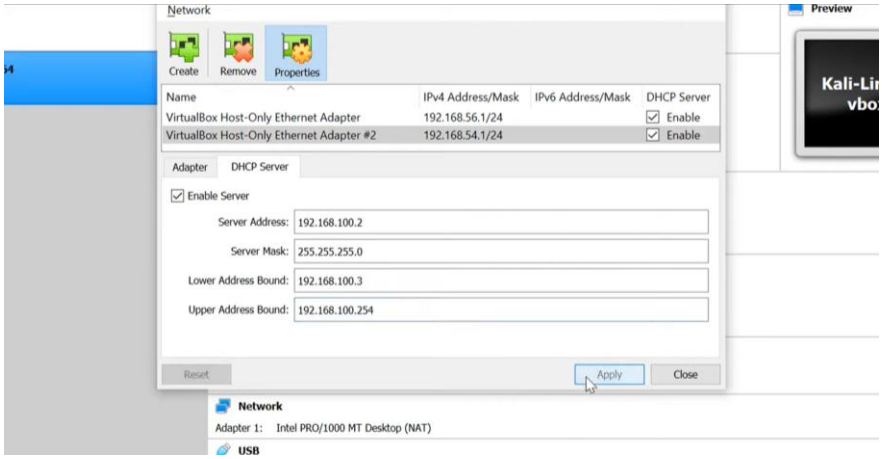
2. Implement Basic Security Measures:

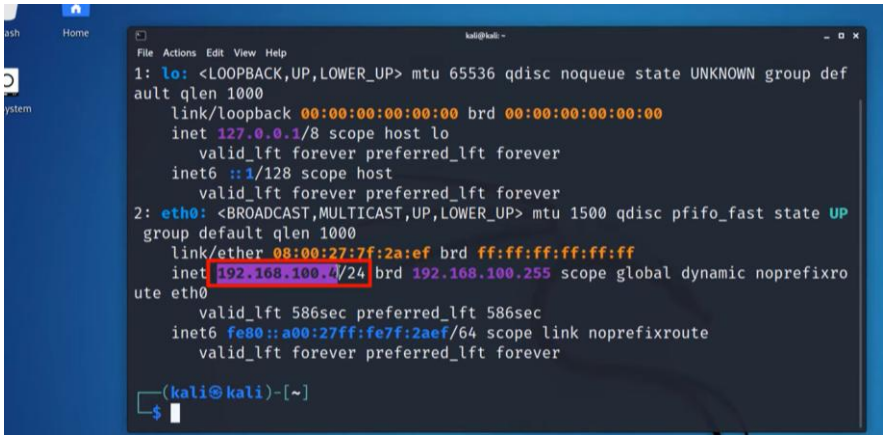
Set up a simple network environment, such as your home network or a virtual lab with a router and one or two connected devices.

Instructions are provided for creating a virtual network in Oracle VM VirtualBox. The process includes setting up a host-only adapter, configuring DHCP settings, and connecting virtual machines (Ubuntu and Kali Linux) to the same subnet. Verification steps ensure both machines can communicate effectively through ping tests.

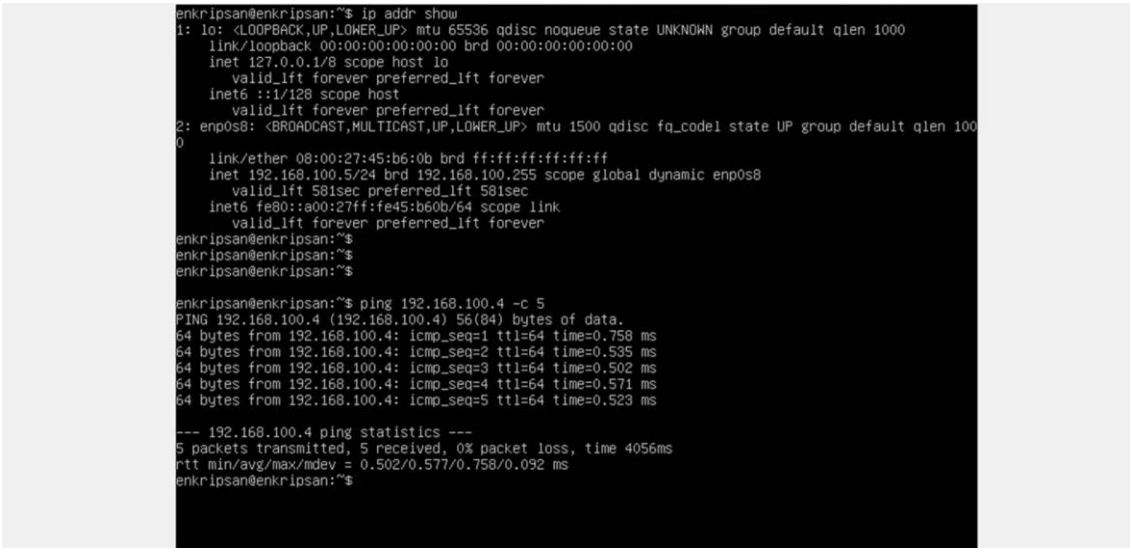


Highlights: Creating a virtual network in Oracle VM VirtualBox allows multiple virtual machines to communicate within the same subnet. This setup enhances network management and testing capabilities for users. -Setting up a host-only network adapter is crucial for isolating communication between virtual machines.





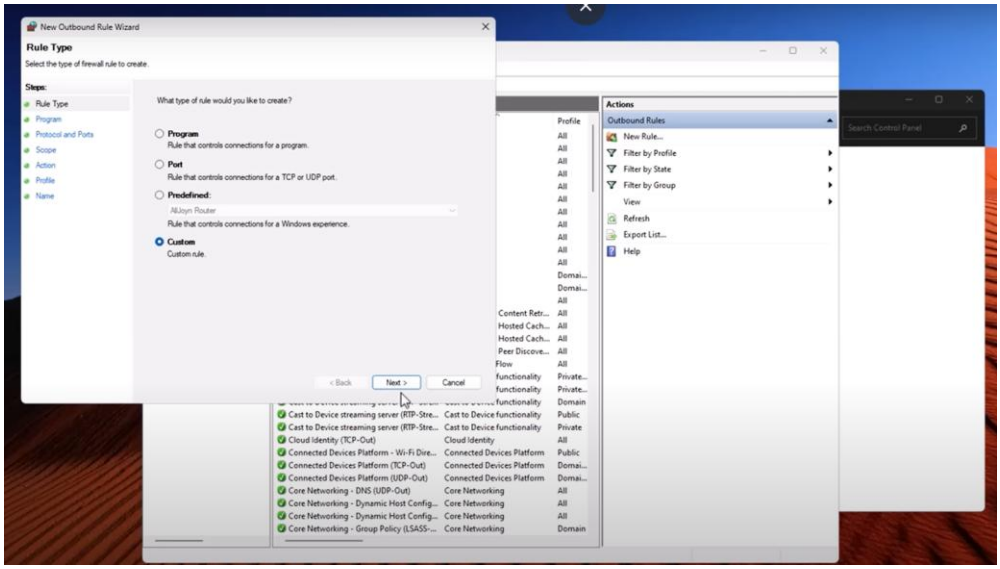
This ensures that the VMs can interact without external network interference. -Configuring the DHCP server enables automatic IP address assignment within the specified subnet. This simplifies the network setup process and minimizes manual configuration errors. -Disabling the default network adapter on each VM ensures that they only connect through the newly created network.



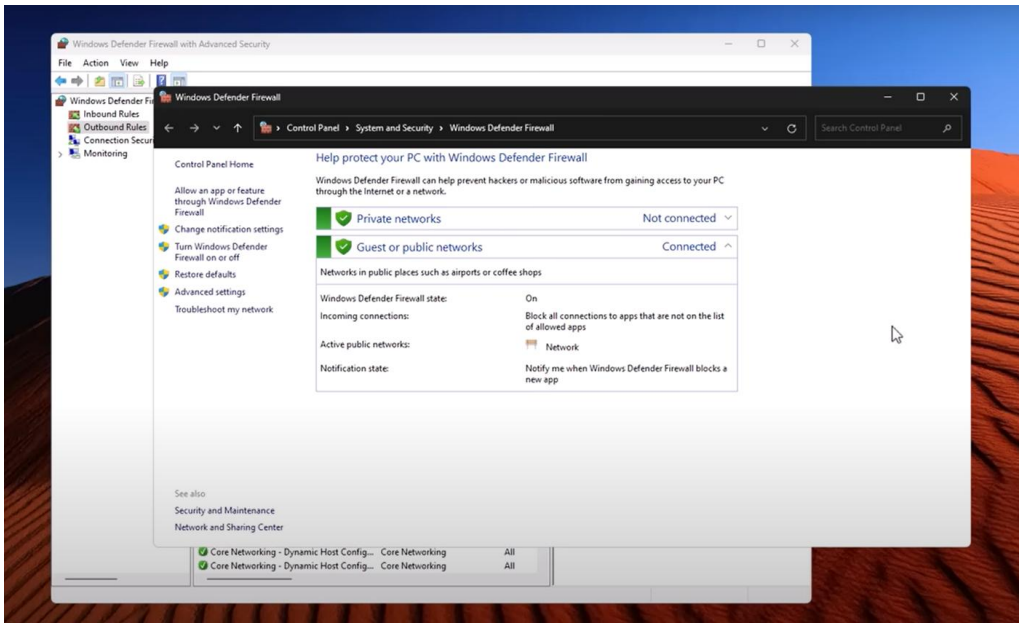
This step is important to maintain the virtual network's integrity. Creating and configuring a virtual network in Oracle VirtualBox allows multiple virtual machines to communicate effectively.

This process involves assigning IP addresses and verifying connectivity between hosts. -To begin, power on a Linux virtual machine and run the command 'ip addr' to check the assigned IP address from the created subnet range. -After verifying the first machine's IP address, repeat the process on a second Linux machine to ensure it also receives an IP from the same subnet. -Finally, use the ping command to test connectivity between the two hosts, confirming they can communicate as expected within the same subnet.

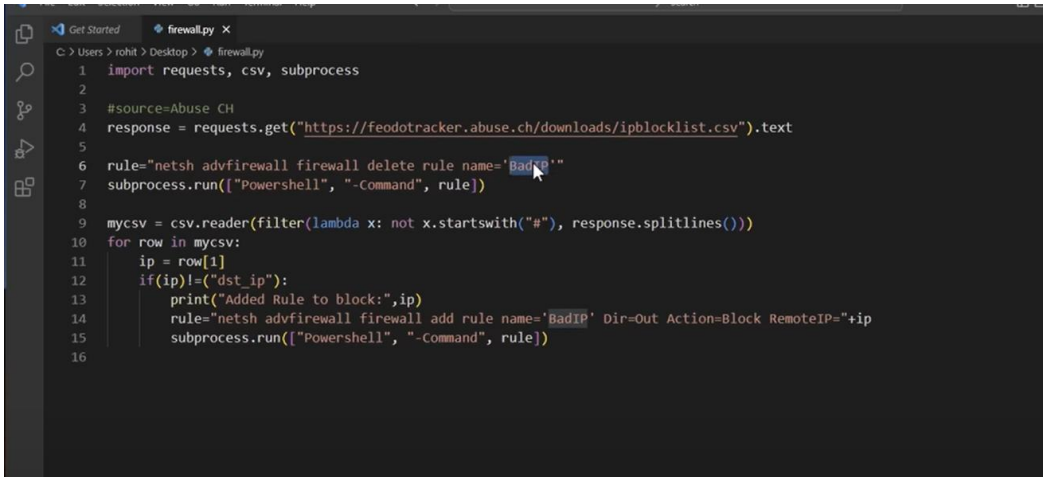
Enable and configure a basic firewall (e.g., Windows Defender Firewall) to block unauthorized access.



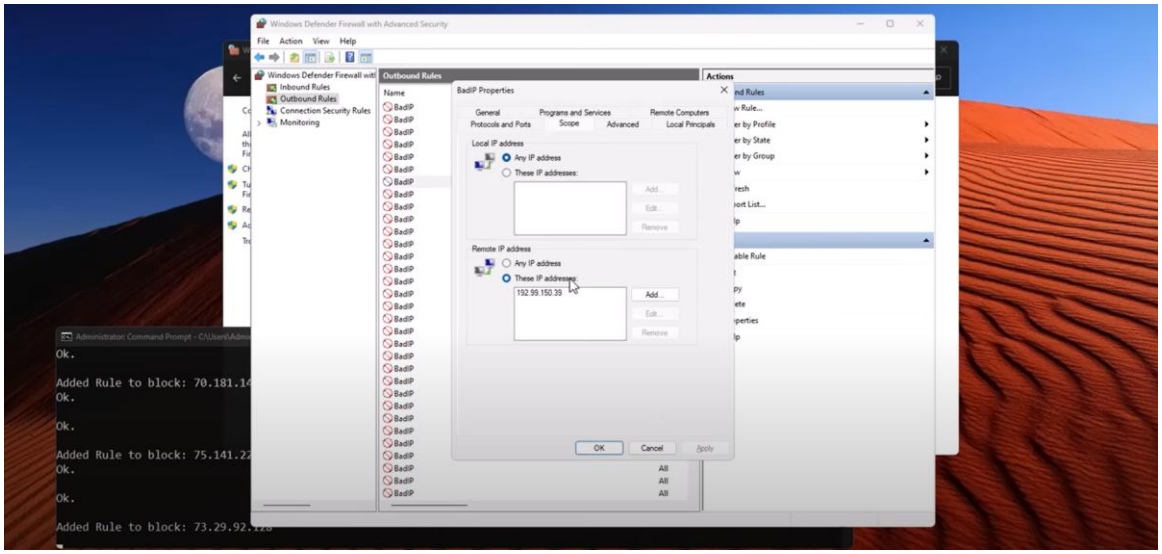
Windows Firewall can be enhanced to block malicious IPs through automation. By using a script, users can regularly update a blacklist of harmful IP addresses, ensuring better protection against hackers and malware. The video also promotes a Discord workshop for community engagement and further learning about network security.



Highlights: Windows Firewall is not just a passive protector; it actively filters traffic and can be customized to enhance security. Users can create specific rules to block malicious IP addresses effectively. -Many users are unaware of the extensive rules that Windows Firewall operates with, which filter incoming and outgoing traffic. Understanding these

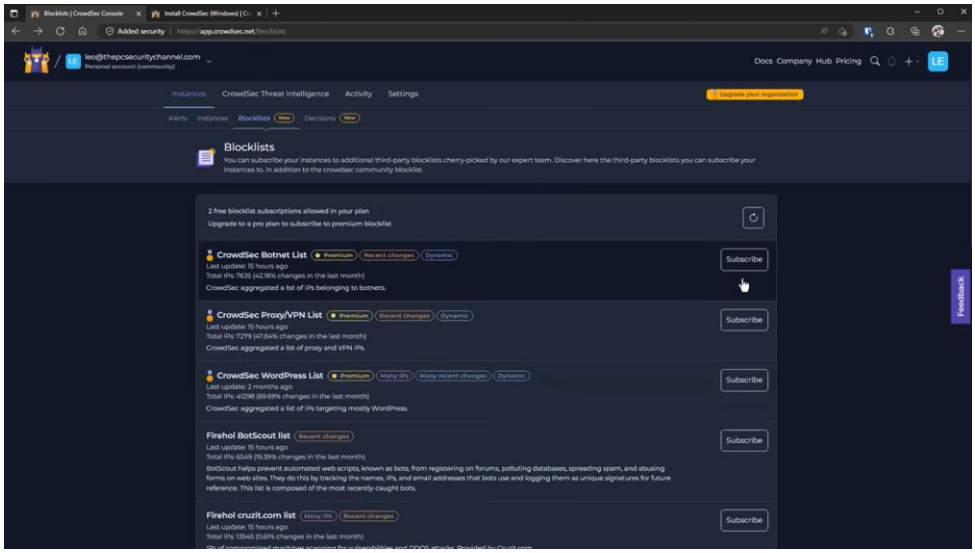


rules is crucial for better security management. -The importance of creating exceptions for applications that connect in non-standard ways emphasizes the need for user awareness. Users often overlook this aspect until prompted by alerts. -Using automation and scripts can simplify the process of updating and managing firewall rules.



This allows users to block multiple malicious IPs efficiently instead of doing it manually. Automating the process of blocking malicious IPs is essential for cybersecurity. This video demonstrates how to efficiently retrieve and manage a list of harmful IP addresses. -Using resources like abuse.ch and URLhaus, users can find lists of malicious servers and domains. These lists help in blocking potential malware threats effectively. -The video showcases a simple script that automates the updating of blocked IP lists. This ensures that the firewall settings remain current and effective against new threats. -Understanding the format of the IP

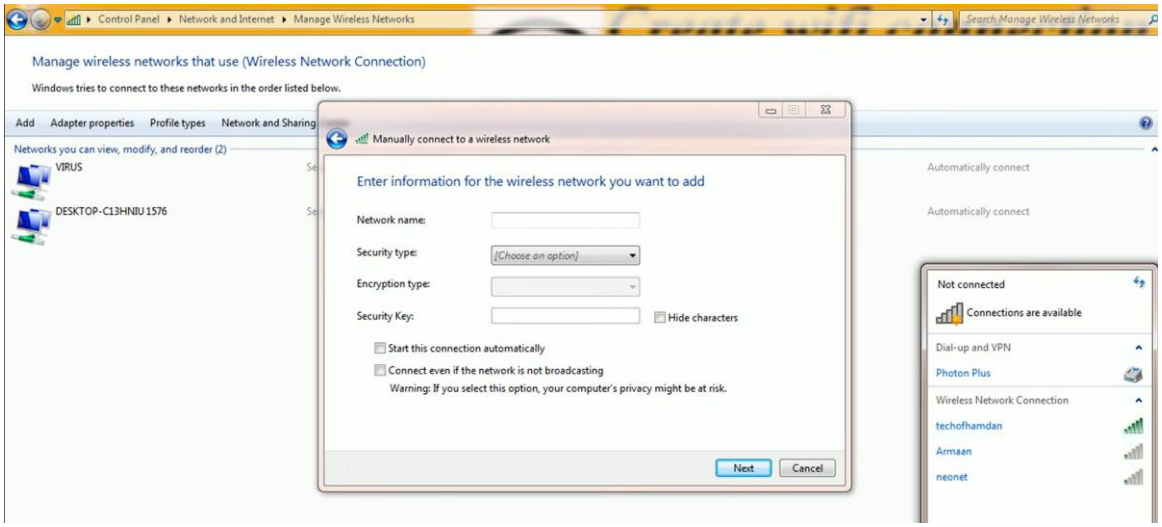
lists is crucial for the automation process.



The video explains how to convert CSV data into a usable format for firewall rules. Dynamic IP management is crucial for cybersecurity, as IP addresses can change and become malicious over time. Implementing scripts that adaptively block these IPs is essential for effective network protection. -The process begins by deleting existing rules to ensure that new scripts operate on a fresh set of parameters, preventing outdated rules from interfering. -Using a CSV reader and Lambda filter allows the script to exclude comment lines, focusing solely on the valid IP addresses that need to be processed. -The script generates commands to block specific IPs, illustrating how automation can enhance firewall management and safeguard against threats like DDoS attacks. Utilizing scripts to add rules for IP addresses is an effective method for enhancing network security. This process can be applied across various firewall software solutions for better protection. -The script displays the added IP addresses in real-time, showcasing how rules can be integrated into the system seamlessly. This visual feedback is crucial for monitoring. -CrowdSec is introduced as an open-source intrusion detection system, providing users with an automated way to manage block lists. This system simplifies the security process significantly. -CrowdSec allows users to add custom rules and implement captchas for certain IPs, enhancing user interactions while maintaining security. This feature adds flexibility to the blocking process. Crowdsourced security tools are becoming more accessible for home users, allowing them to enhance their protection against malicious threats. These tools leverage community input to identify and classify security risks effectively. -Community involvement plays a crucial role in identifying false positives and confirming malware, empowering users to contribute to their own security. This collaborative approach enhances overall protection. -The ease of deploying these security tools makes them ideal for home servers and personal use, providing a low barrier to entry for users. They are user-friendly and continuously updated. -Participating in events like Discord discussions can foster community engagement and provide users with detailed guidance on network security practices. These interactions promote learning and collaboration.

Set up basic security configurations, such as changing default passwords and enabling network encryption (WPA2 or WPA3).

Different wireless security protocols like WEP, WPA, WPA2, and WPA3 ensure Wi-Fi networks are secure. WEP is outdated and vulnerable, while WPA2 uses AES for stronger protection. WPA3, introduced in 2018, enhances security further. WPS simplifies device connections, and Access Control allows blocking specific devices for added security.



Highlights: Wireless security methods are crucial for protecting networks from unauthorized access. This video discusses various protocols, including WEP, WPA, and WPA2, that enhance Wi-Fi security. -WEP was the first wireless security protocol introduced in 1999, but it became obsolete due to its vulnerability to hacking. Its 40-bit encryption key proved insufficient for modern security needs. -WPA, or Wi-Fi Protected Access, was created to address the weaknesses of WEP. It employs TKIP, which dynamically changes encryption keys to enhance data integrity. -WPA2 further improves security by requiring stronger encryption methods compared to WPA. This evolution of protocols reflects the ongoing need for robust wireless security measures. WPA2 uses AES encryption, making it significantly more secure than the older WPA protocol that relies on TKIP. This enhancement greatly protects networks against brute-force attacks and unauthorized access. -Older routers may still have WEP as an option, but it's outdated and considered insecure. Newer routers typically eliminate WEP due to its vulnerabilities. -The mixed security option allows both WPA and WPA2, catering to compatibility with older devices. However, using TKIP alongside AES can compromise network security. -WPA3, introduced in 2018, enhances wireless security with advanced protocols and increased protection against password guessing. It aims to simplify Wi-Fi security for users. WPS, or Wi-Fi Protected Setup, simplifies the process of connecting devices to a wireless network without needing a password. It's particularly beneficial for users unfamiliar with wireless technology. -The push button method of WPS allows users to connect devices by simply

pressing buttons on both the router and the device. This method is user-friendly and convenient. -WPS can also utilize a PIN number for connection, which offers an alternative for devices that do not support the push button method. This adds flexibility in device connectivity. -Access Control, or MAC Filtering, adds an extra layer of security by allowing or blocking devices based on their unique MAC addresses. This enhances the overall safety of the network.

Summary of Network Threats Researched:

During my internship at Redynox, I explored the following **network threats**:

1. **Viruses** – Corrupt and modify files; spread through infected programs.
2. **Worms** – Self-replicating malware that consumes bandwidth.
3. **Trojans** – Disguised programs that create backdoors.
4. **Phishing Attacks** – Fake emails or websites that steal personal info.
5. **Man-in-the-Middle (MITM)** – Intercepts communications over insecure channels.
6. **DoS/DDoS Attacks** – Overwhelm servers to make them unavailable.
7. **Insider Threats** – Internal users misusing access.
8. **Spyware** – Secretly logs user activity.
9. **Ransomware** – Encrypts files and demands payment.
10. **Adware** – Displays unwanted ads and collects data.

Security Measures Implemented:

1. **Virtual Network Setup in VirtualBox**:
    - Created isolated host-only networks using DHCP.
    - Ensured IP communication between Kali Linux and Ubuntu VMs.
2. **Firewall Configuration (Windows Defender Firewall)**:
    - Enabled firewall with custom rules to block malicious IPs.
    - Automated IP blacklisting using a script and threat intelligence sources like abuse.ch.
3. **Secure Network Configurations**:
    - Disabled unused ports and default credentials.
    - Used secure protocols like SSH.

4. **Wireless Encryption and Access Control**:
    - Configured WPA2/WPA3 for Wi-Fi security.
    - Enabled MAC address filtering to restrict device access.

Wireshark Traffic Capture Description:

While testing virtual machine connectivity, **Wireshark** was used to analyze packet traffic:

- **IP Assignment Verification**: Captured DHCP packets to confirm dynamic IP allocation.
- **Ping Test Packets**: Captured ICMP echo requests/replies to ensure VM-to-VM communication.
- **Normal vs. Suspicious Traffic**: Noted clean DNS and HTTP traffic patterns for analysis.

You may attach screenshots showing IP addresses (via ip addr), ping success, or filtered Wireshark traffic for better illustration.

Discussion on Security Measure Effectiveness:

These basic security practices significantly improve network protection:

- **Firewalls** filter unauthorized access and suspicious traffic.
- **Encryption** secures sensitive data from eavesdropping.
- **Proper configurations** reduce vulnerabilities and human error.
- **Traffic monitoring (e.g., Wireshark)** helps detect anomalies early.
- **Access controls** limit exposure to external threats.

Combined, these tools and practices create a **strong defense-in-depth strategy** for any network environment.

Reflection on Security Best Practices

In larger, more complex networks—such as enterprise or cloud-based environments—additional security measures are essential to ensure robust protection. These include **Intrusion Detection and Prevention Systems (IDPS)** to monitor and respond to threats in real-time, **Network Segmentation** to isolate critical resources, **Multi-Factor Authentication (MFA)** for user access, **Zero Trust Architecture** to verify every access request, and **SIEM (Security Information and Event Management)** tools to analyze logs and detect suspicious patterns. Regular **penetration testing** and **automated patch management** also help in proactively addressing vulnerabilities.

Educating Others About Network Security

To help others understand the importance of network security in everyday life, I would explain how easily their personal data—like bank credentials or private messages—can be stolen on an unsecured Wi-Fi network. Using real-life examples like phishing emails or social media scams, I would stress the need for strong passwords, two-factor authentication, and caution while clicking unknown links. I would also demonstrate simple steps like enabling firewalls, updating software, and using VPNs. By connecting security to their daily habits, I aim to make people more alert and proactive in protecting their digital footprint.