Internship Report On

Cyber Security

At

The Red Users

Submitted By

RATHVA ROSHANKUMAR

(1 Dec 2024 - 31 Dec 2024)

Task 1: Introduction to Network Security Basics

Objective: Understand the basics of network security by learning about different types of network threats and how to implement basic security measures. This task will introduce you to the foundational concepts of securing a small network.

Skills: Basic Network Security, Threat Identification, Security Best Practices

Tools: Firewall (Windows Defender Firewall or a basic hardware firewall), Wireshark

Introduction to Network Security Basics:

Network security is the practice of protecting computer networks from unauthorized access, attacks, or damage. Just like physical assets need protection, digital assets, including data and systems, must also be secured to ensure privacy, integrity, and availability.

Key Concepts:

1. Confidentiality:

Ensures that sensitive information is only accessible to authorized users. Example: Passwords, personal data.

2. Integrity:

Ensures that data is transmitted without unauthorized changes or corruption. Example: Financial transactions' data.

3. Availability:

Ensures that authorized users have access to the data and services when needed. Example: Website uptime.

4. Authentication:
The process of verifying the identity of a user or system. Example: Username/password login.

5. Authorization:
Determines the level of access granted to authenticated users. Example: Admin access vs Regular user permissions.

Common Network Security Threats:

- **Digital Arrest**
- **Viruses**
- **Phishing**
- **DoS/DDoS**
- **Man-in-the-Middle (MitM)**
- **SQL Injection**
- **Cross-Site Scripting (XSS)**
- **Drive-By Downloads**

1. Digital Arrest :

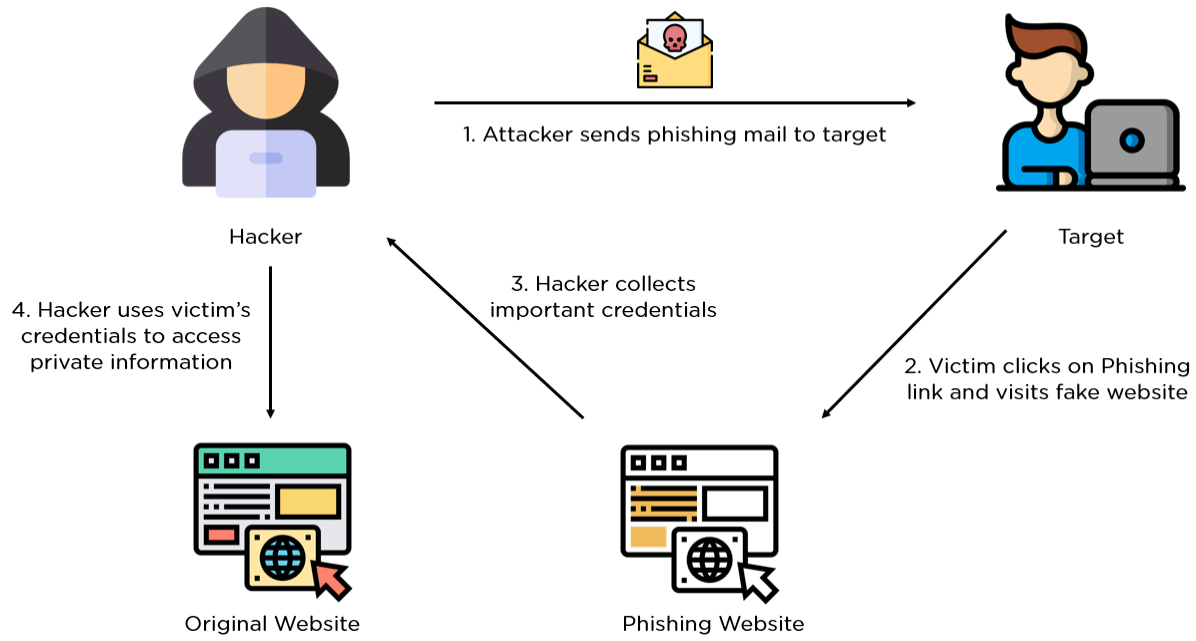
→**The Digital Arrest** Scam is a rising form of fraud in India where cybercriminals impersonate police officers or government officials and threaten victims with legal action or arrest if they don't comply. The scam usually starts with a phone call or message claiming that the victim's name is involved in a criminal case, such as tax evasion or fraud, and that an arrest warrant has been issued. The fraudsters create panic by claiming severe penalties or jail time and demand immediate payment or personal information, such as bank details or OTPs, to resolve the issue. They often use fake caller IDs or spoofed numbers to appear as legitimate government agencies, making it harder for the victim to recognize the fraud. This scam takes advantage of people's fear and lack of awareness, causing them to act impulsively. To avoid falling victim, individuals should verify the caller's identity, never share sensitive information over the phone, and report such incidents to authorities immediately. Staying calm and cautious is key to preventing this scam.

2. Viruses:

→**A computer virus** is a malicious program that infiltrates systems to disrupt operations, steal data, or damage resources. Modern viruses are more sophisticated, often combining with other malware like ransomware or spyware to increase impact. Unlike older viruses that relied on floppy disks or basic file sharing to spread, today's viruses exploit advanced techniques like malicious macros in documents, infected software downloads, and network vulnerabilities to propagate. Some viruses, like Polymorphic Viruses, can mutate their code to evade detection by antivirus tools. Recent examples include Emotet, which spreads through phishing emails and delivers further payloads. Protecting against modern viruses requires advanced endpoint protection, behavior-based antivirus solutions, and awareness of cybersecurity best practices, such as avoiding suspicious links and regularly updating software.

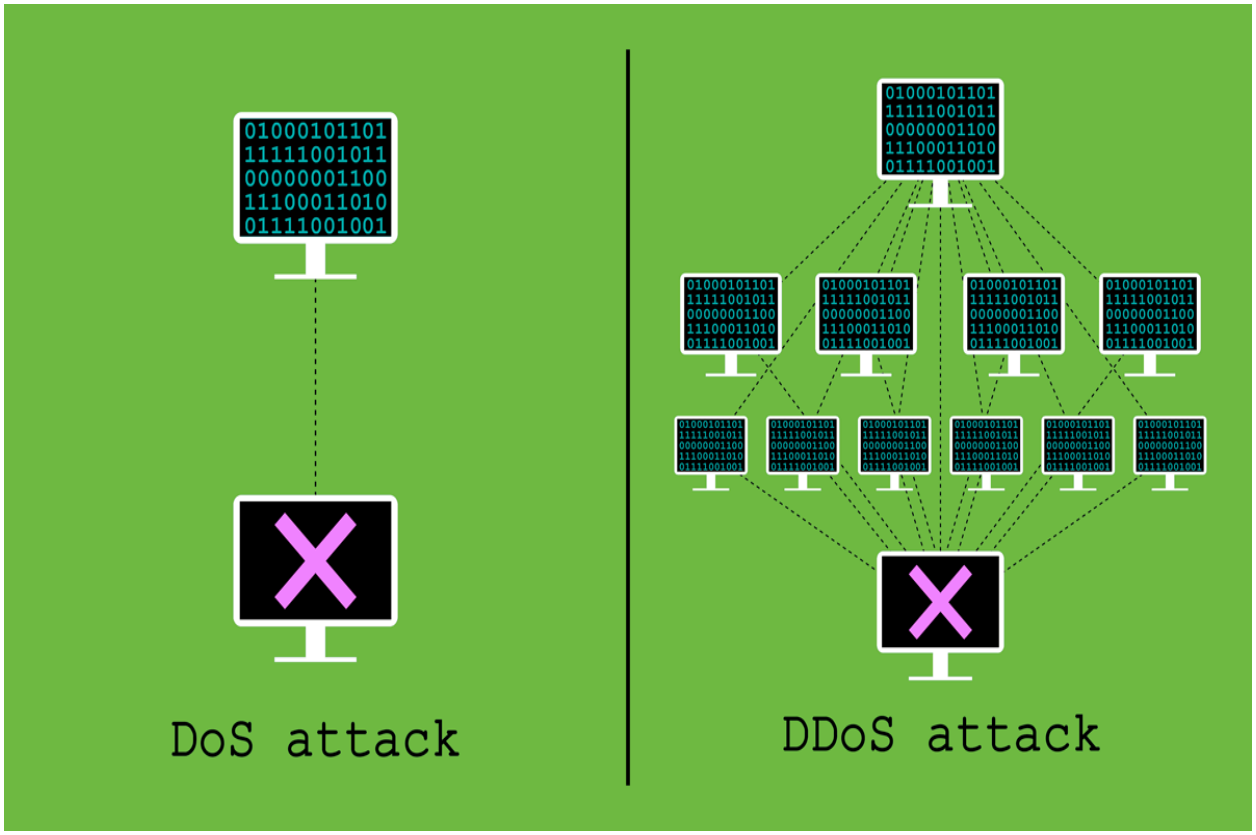
3. Phishing:

→ **Phishing** is a type of cyberattack where attackers trick individuals into revealing sensitive information, such as login credentials, credit card details, or personal data, by pretending to be a trusted entity. Modern phishing attacks often use realistic-looking emails, messages, or websites that mimic legitimate organizations like banks, social media platforms, or government agencies. These messages usually create urgency, such as claiming account suspension or unusual activity, to prompt victims into clicking malicious links or downloading harmful attachments. Recently, spear phishing (targeted phishing) and voice phishing (vishing) have become common, using personalized details to increase credibility. Advanced phishing campaigns, like those leveraging AI, can craft convincing fake communications. To avoid phishing, individuals should verify the source of emails or messages, avoid clicking on unverified links, and use multi-factor authentication for added security.



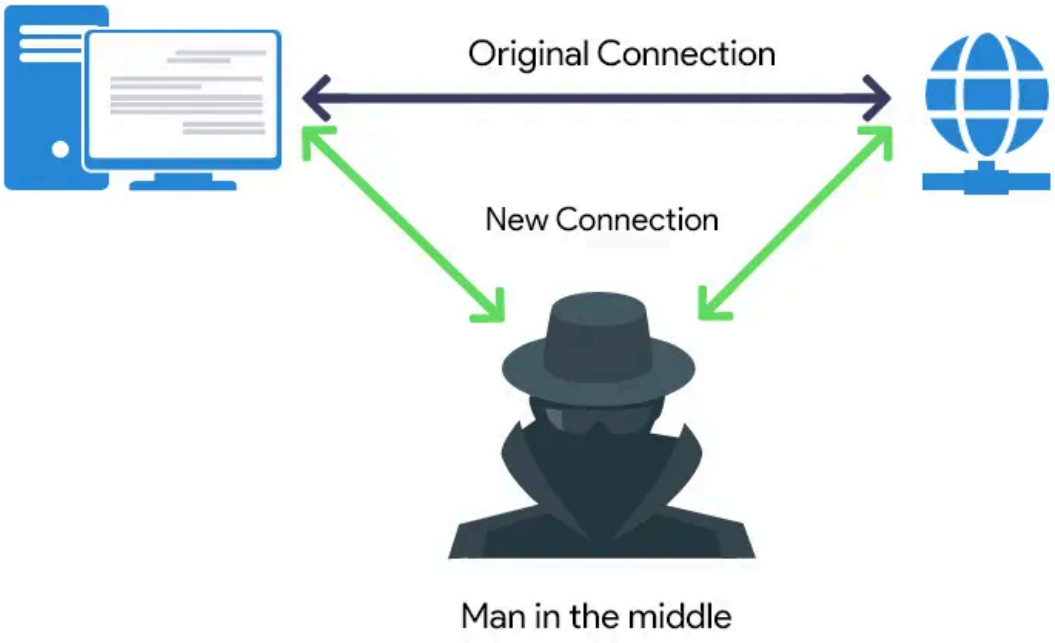
4. DoS/DDoS:

A **Denial of Service (DoS)** attack is a cyberattack aimed at overwhelming a target system, server, or network with excessive traffic or resource requests, rendering it unavailable to legitimate users. In a **Distributed Denial of Service (DDoS)** attack, the traffic originates from multiple compromised systems, often forming a botnet of infected devices worldwide, making it harder to mitigate. These attacks can disrupt online services, cause financial losses, and damage reputations. Modern DDoS attacks often target websites, APIs, or gaming servers, using amplification techniques like **UDP floods**, **SYN floods**, or **DNS reflection** to maximize the impact. Recent attacks leverage **IoT devices** with poor security to create massive botnets. Preventing DoS/DDoS attacks involves implementing **firewalls**, **load balancers**, **anti-DDoS services**, and regularly monitoring network traffic to detect and mitigate threats early.



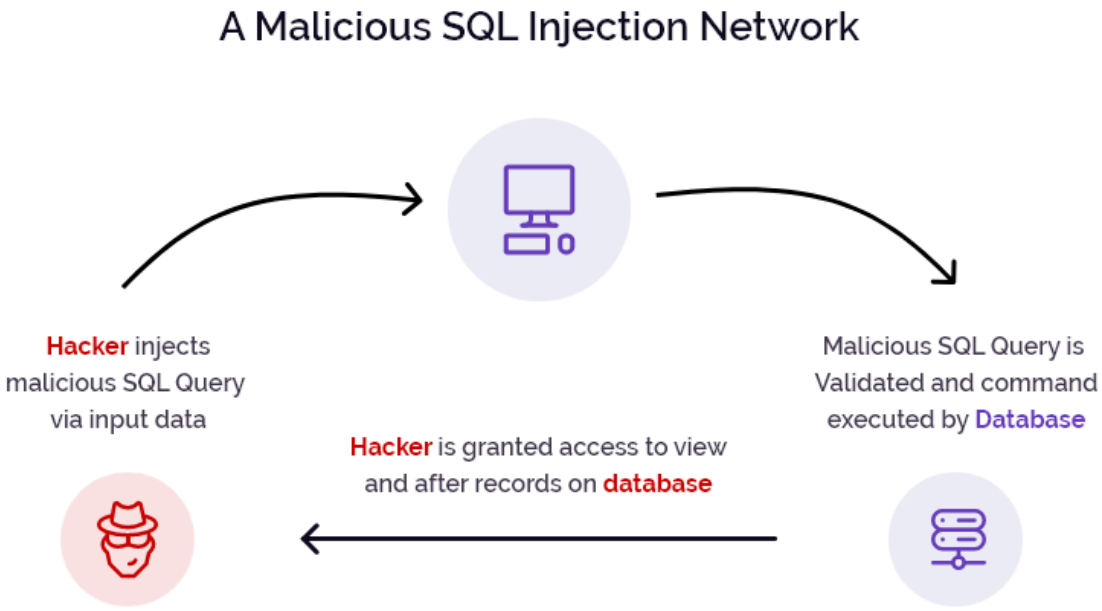
5. Man-in-the-Middle (MitM):

→ **A Man-in-the-Middle (MitM)** attack occurs when an attacker intercepts and potentially alters communication between two parties without their knowledge. The attacker positions themselves between the victim and the intended recipient, allowing them to eavesdrop, steal sensitive data, or inject malicious content into the communication. Common MitM techniques include Wi-Fi eavesdropping, where attackers exploit unsecured public Wi-Fi networks, and session hijacking, where active sessions are intercepted. Advanced methods, like HTTPS spoofing or DNS spoofing, can redirect users to malicious websites. For example, an attacker might capture login credentials during an online banking session. To protect against MitM attacks, individuals should use encrypted connections (HTTPS), avoid using public Wi-Fi without a VPN, and enable two-factor authentication to secure accounts.



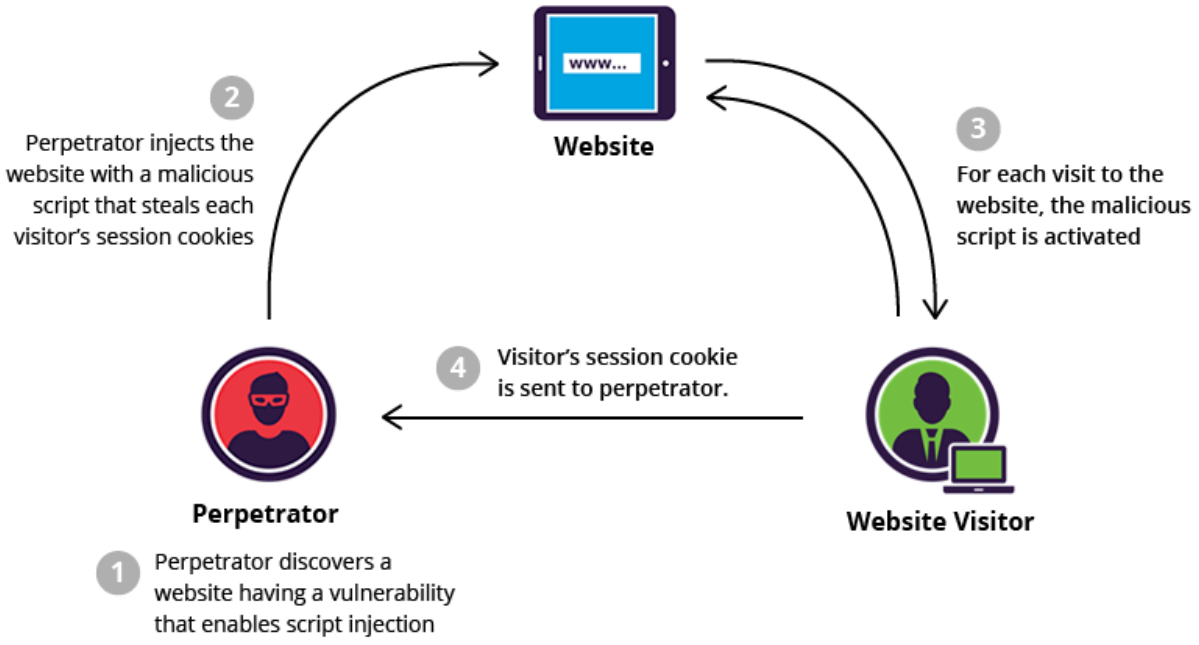
6. SQL Injection:

→ **SQL Injection (SQLi)** is a common web application attack where an attacker exploits vulnerabilities in an application's database query handling. By injecting malicious SQL code into input fields (like login forms or search bars), attackers can manipulate queries to access, modify, or delete sensitive data from the database. For example, instead of entering a username, the attacker might input `' OR '1'='1` to bypass authentication. SQL Injection attacks can expose personal user data, disrupt application functionality, or even allow administrative access to the database. Modern variations include Blind SQL Injection, where the attacker infers data without visible feedback, and Time-Based SQL Injection, where database responses are delayed to confirm vulnerabilities. To prevent SQL Injection, developers should use prepared statements, parameterized queries, and sanitize user inputs effectively, alongside deploying robust web application firewalls (WAFs).



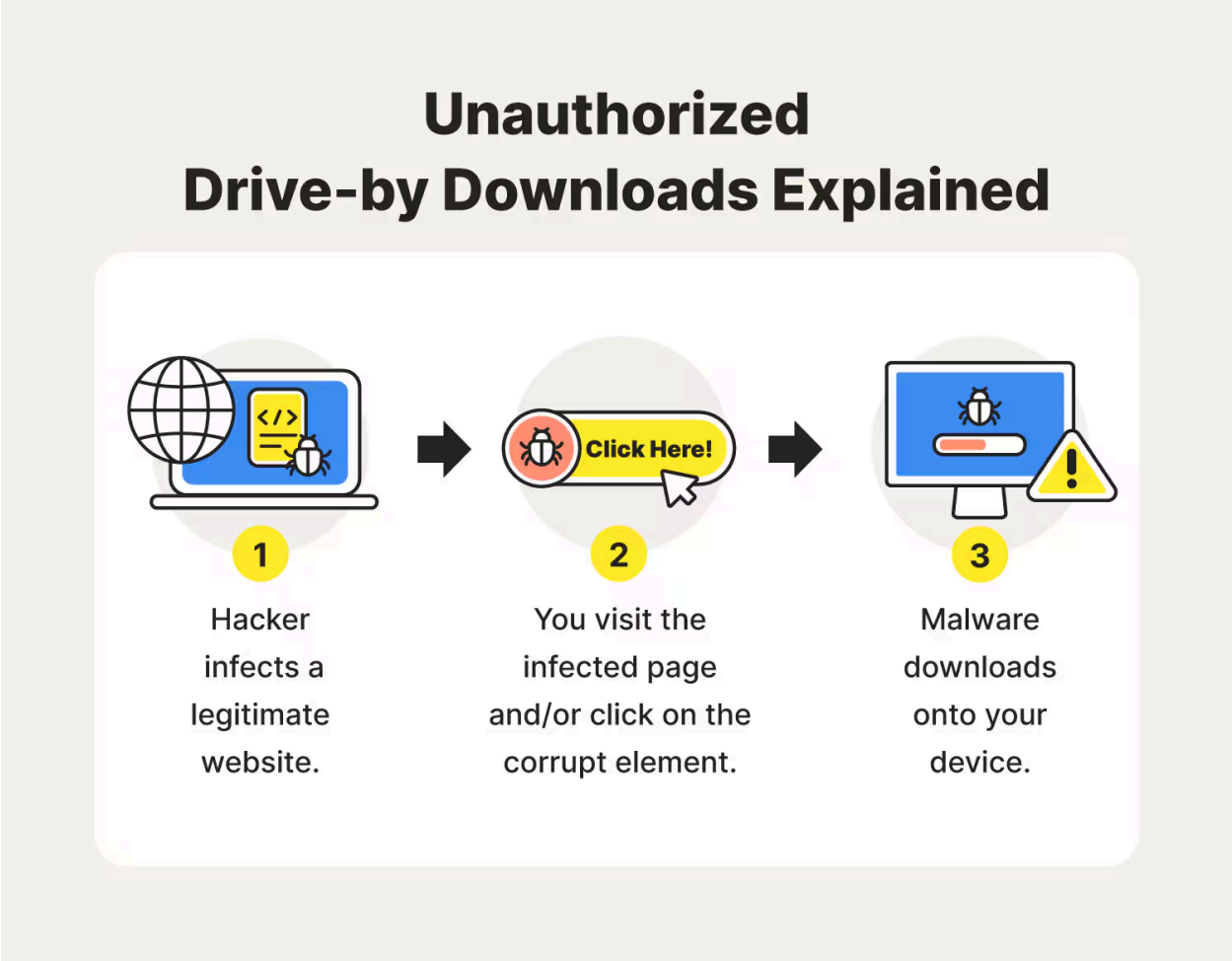
7. Cross-Site Scripting (XSS):

→ **Cross-Site Scripting (XSS)** is a web application vulnerability where attackers inject malicious scripts into trusted websites viewed by other users. This occurs when a web application doesn't properly validate or sanitize user inputs. The injected script is executed in the browser of the victim, potentially stealing sensitive information like cookies, session tokens, or login credentials. XSS attacks are broadly categorized into three types: Stored XSS, where malicious scripts are permanently stored on the server; Reflected XSS, where the payload is immediately reflected in the server response; and DOM-based XSS, where the attack is executed directly within the browser without server interaction. To mitigate XSS, developers should sanitize and encode user inputs, implement Content Security Policies (CSPs), and use secure frameworks that automatically escape output.



8. Drive-By Downloads:

→ **Drive-By Downloads** are a type of cyberattack where malicious software is downloaded onto a user's device without their knowledge or consent. These attacks typically occur when users visit compromised or unsecure websites, often through infected ads (malvertising) or hidden malicious code. Unlike traditional malware attacks, Drive-By Downloads require no user action, such as clicking a link, making them highly dangerous. They exploit vulnerabilities in outdated browsers, plugins, or software to execute automatically. Once downloaded, the malware can steal sensitive information, gain control of the system, or install additional harmful programs. To prevent Drive-By Downloads, users should keep their software updated, use ad-blockers, avoid untrusted websites, and rely on robust antivirus protection.



Understanding Basic Security Concepts

1. Firewalls

- **Definition:**
  A firewall acts as a barrier between a trusted network (such as a private internal network) and an untrusted network (like the internet). It filters incoming and outgoing network traffic based on a set of security rules, determining which traffic is safe and which needs to be blocked.
- **How It Works:**
  Firewalls analyze data packets and decide whether to allow or block them based on predefined rules.
  1. **Allow Rule:** Permits legitimate traffic.
  2. **Deny Rule:** Blocks unauthorized or harmful traffic.
- **Types of Firewalls:**
  1. **Hardware Firewalls:** Installed on physical devices like routers to protect entire networks.
  2. **Software Firewalls:** Installed on individual devices like PCs or servers.
  3. **Cloud-Based Firewalls:** Used in modern infrastructures to secure cloud resources.

2. Encryption

- **Definition:**
  Encryption is the process of converting readable data (plaintext) into an unreadable format (ciphertext) to prevent unauthorized access. Only those with the decryption key can access the original data.
- **Types of Encryption:**
  - **Symmetric Encryption:**
    - Uses the same key for both encryption and decryption.
    - Example: AES (Advanced Encryption Standard).
  - **Asymmetric Encryption:**
    - Uses a pair of keys:
    - **Public Key:** For encryption.

    - **Private Key:** For decryption.
        - Example: RSA (Rivest-Shamir-Adleman).

3. Secure Network Configurations

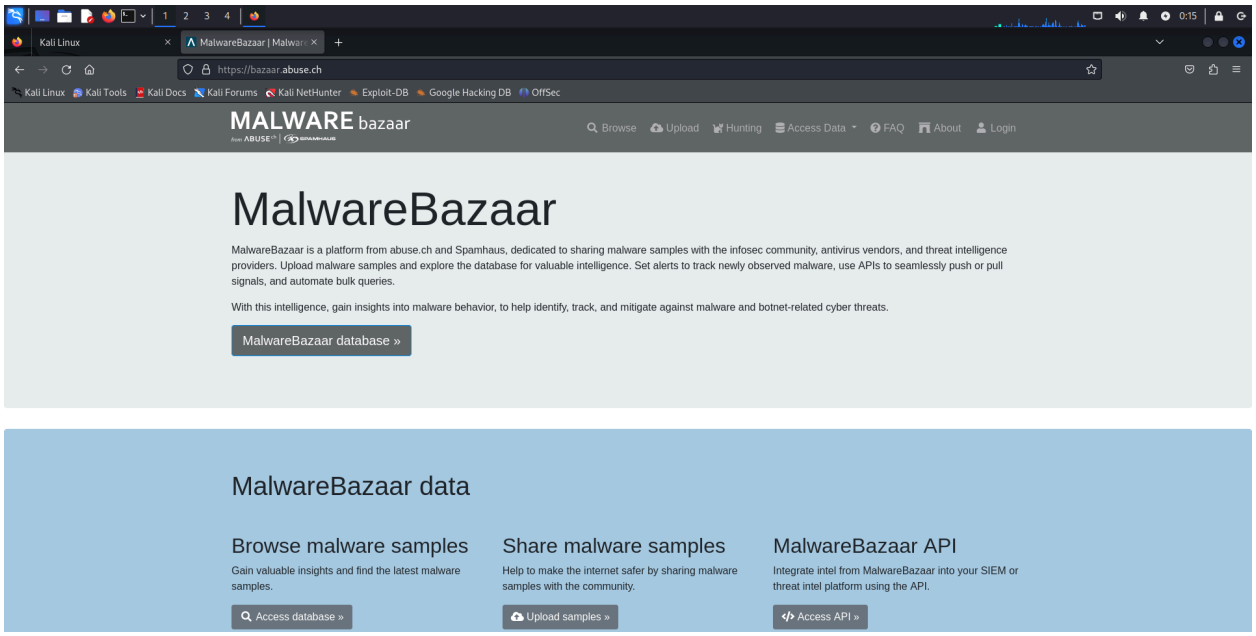
- **Definition:**
  This involves setting up a network in a way that minimizes vulnerabilities and protects it from unauthorized access or attacks.
- **Key Practices:**
    - **Changing Default Credentials:** Replace default usernames and passwords on network devices with strong, unique passwords.
    - **Disabling Unused Services:** Turn off unused network services to reduce the attack surface.
    - **Regular Updates:** Keep network devices and software updated to patch known vulnerabilities.
    - **Network Segmentation:** Divide the network into smaller segments (e.g., public and private zones) to enhance security and contain potential breaches.
    - **Use of VPNs (Virtual Private Networks):** Ensure encrypted communication for remote workers.
    - **Monitoring and Logging:** Continuously monitor network activity and maintain logs for detecting suspicious activities.

- **Implement Basic Security Measures:**

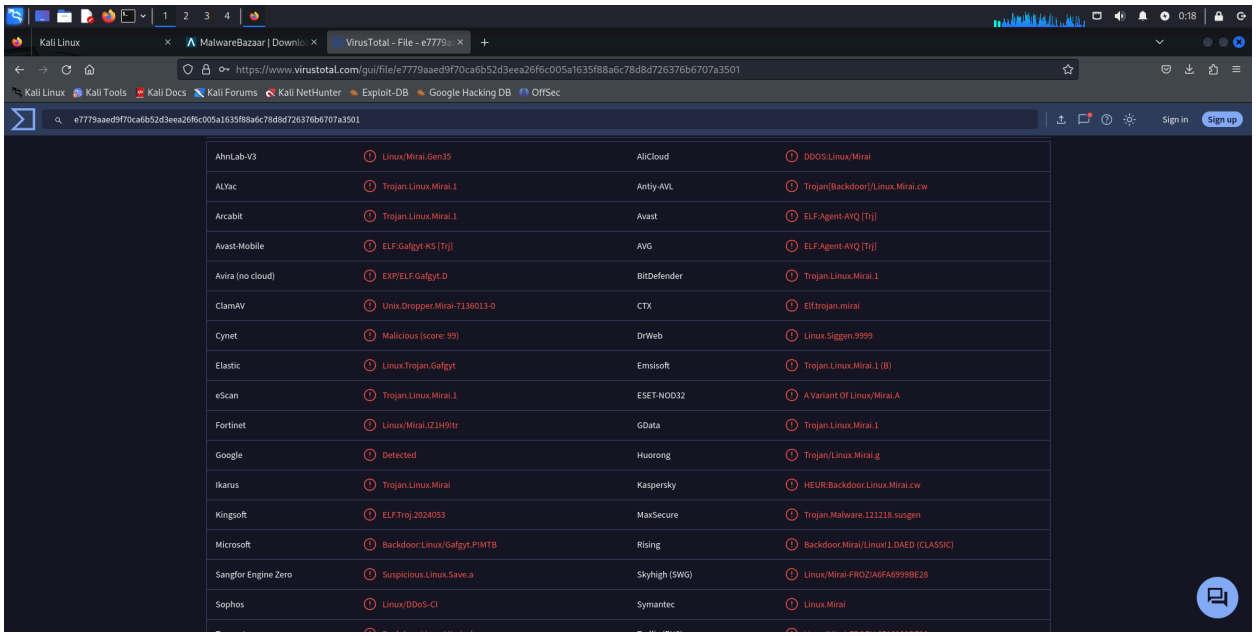
Simple Network Environment:

→ Set up the safe environment using virtual box (kali Linux) for implementation of virus.

Step 2: Downloading the unknown file from the Malware Bazaar Database Website



Step 3:Scanning the folder using VIRUSTOTAL website for detection of virus, Trojan, worms in that file.



Step4:

As per the result we detected that the file contains virus, Trojan Scan with

VIRUSTOTAL:

Always scan files with VIRUSTOTAL before downloading or executing them to check for potential threats.

Enable Controlled Folder Access:

Turn on this feature in Windows Defender to protect sensitive folders from unauthorized changes by malicious applications.

Regularly Update Security Software:

Ensure that Windows Defender and any other security software are updated frequently to recognize the latest threats. Perform Full System Scans: Schedule regular full system scans to detect and remove any hidden malware that may have slipped through.

Enable Ransomware Protection:

Use the anti-ransomware features in Windows Defender to safeguard against ransomware attacks.

Use Reputation-Based Protection:

Activate reputation-based protection in Windows Security to help detect potentially harmful apps and files based on their behavior and history. Use Strong

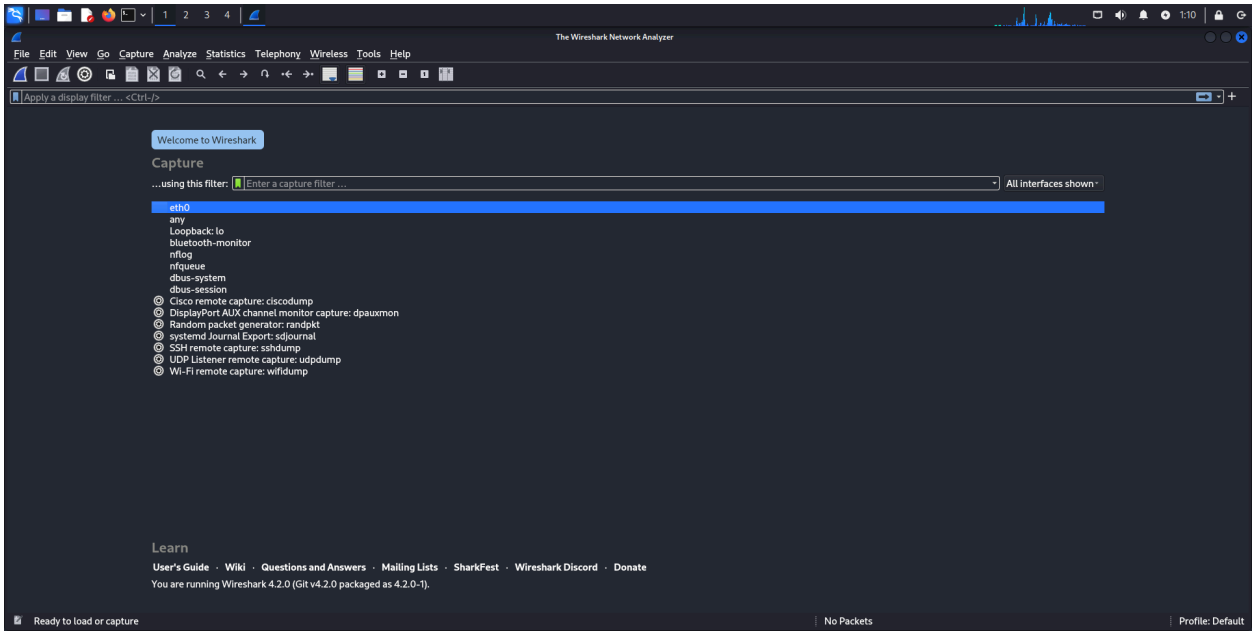
Passwords and Two-Factor Authentication: Strengthen account security by using complex passwords and enabling two-factor authentication where possible.

Monitoring Network Traffic with Wireshark:

Wireshark is a tool for capturing and analyzing network traffic, helping users see what's happening across a network in real time. Imagine it as a digital microscope for network data. Each packet of data sent across the network is like a small piece of information, and Wireshark lets you capture these packets and analyze them in detail.

Install and Set Up Wireshark:

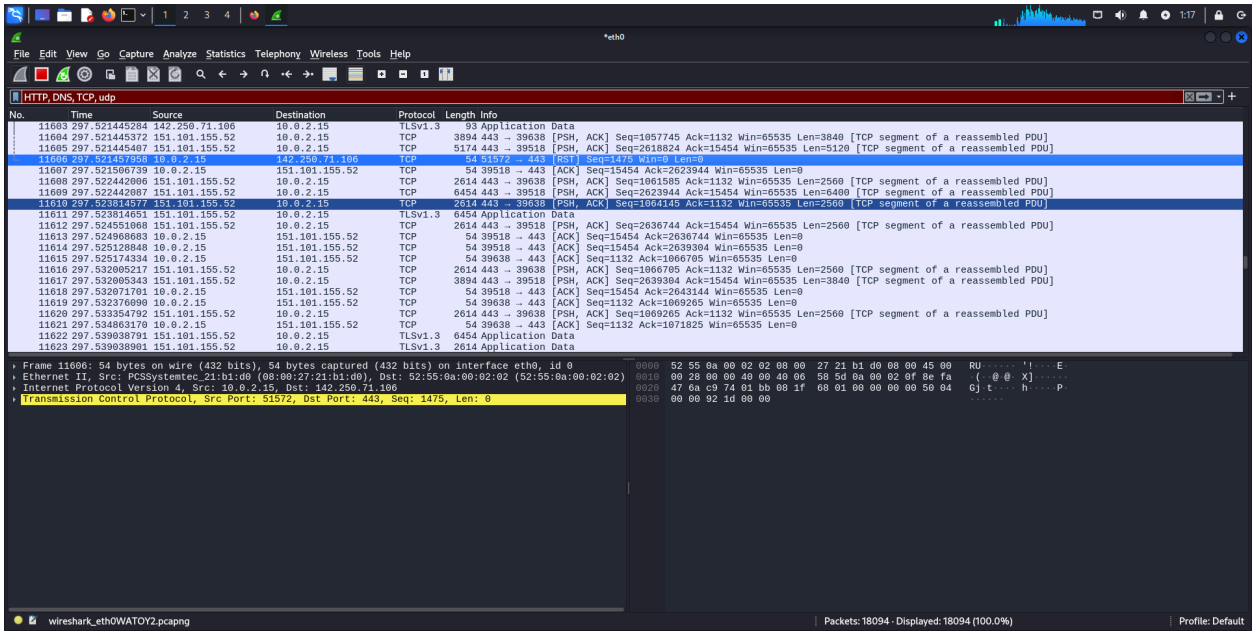
- Install Wireshark on Kali Linux or Windows and open it.



Start Capturing Traffic

● Click on the Start Capturing icon (or press Ctrl+E) to begin capturing packets on the selected interface.

● Wireshark will start displaying live traffic, showing packet details like source, destination, protocol, and time.



Use Display Filters for Targeted Analysis

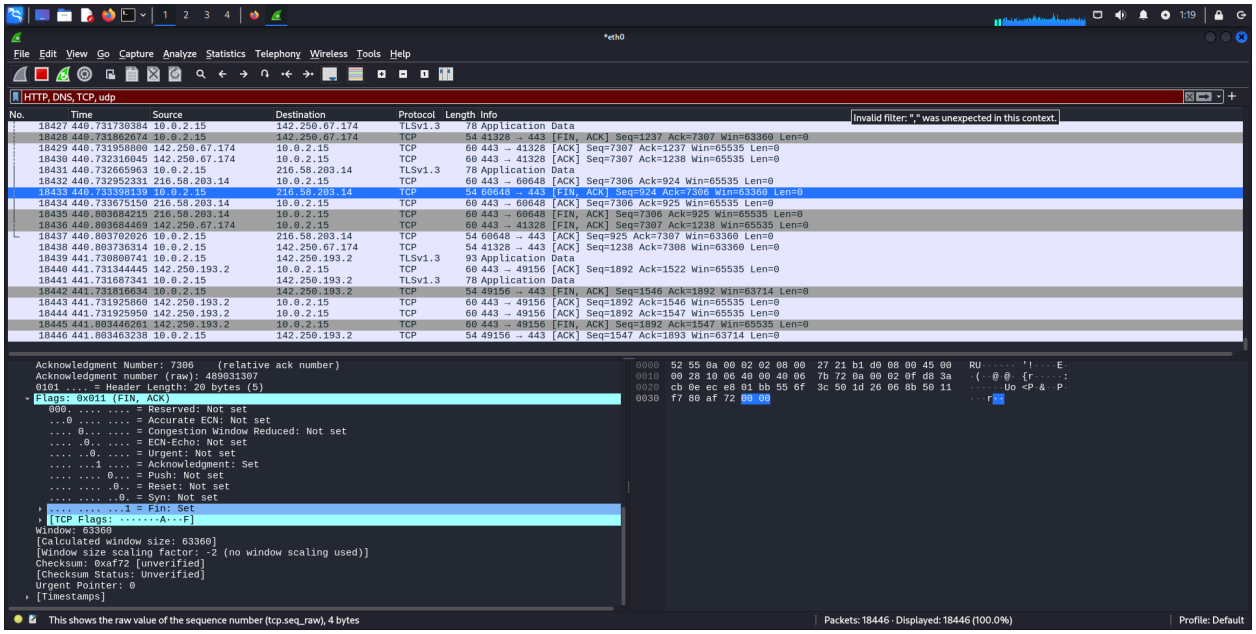
● Apply display filters to further focus on specific types of traffic within the captured data (e.g., HTTP, DNS, ICMP).

● Examples include http (web traffic), tcp.port == 80 (HTTP port traffic), or ip.src == 192.168.1.100 (traffic from a specific source IP).

Monitor Live Traffic

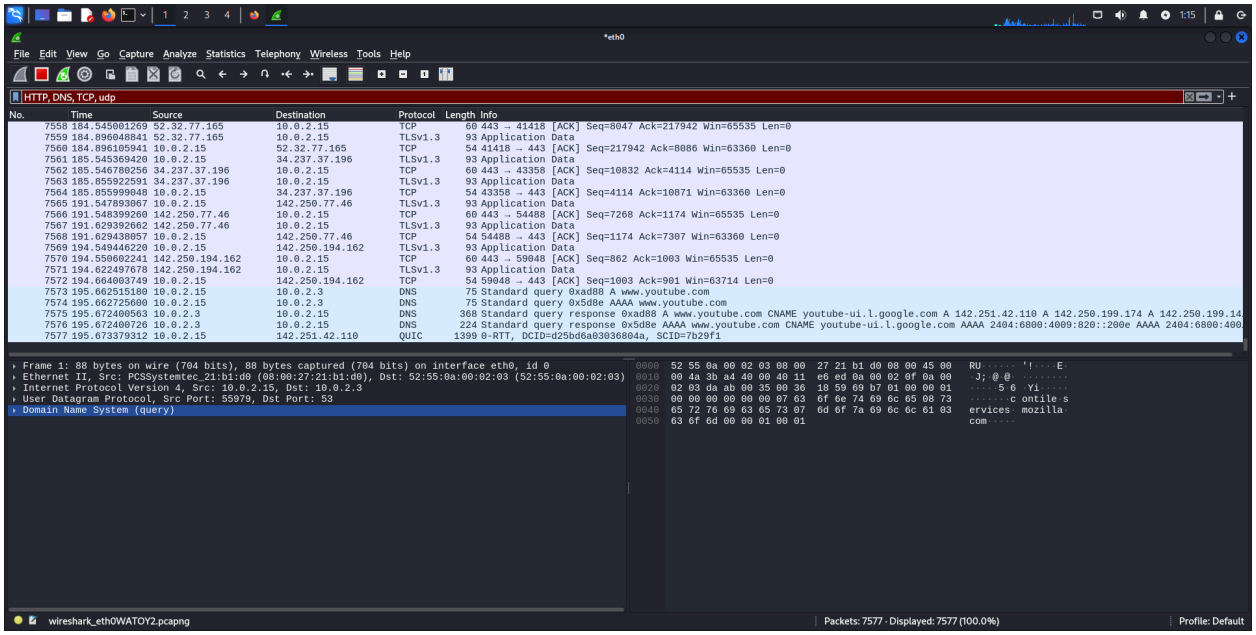
● Observe the packets displayed in real time, with each packet listed by details such as time, source, destination, protocol, and info.

● Click on any packet to see more detailed information in the lower pane, showing layer-by-layer breakdowns like Ethernet, IP, and TCP headers.



Use Display Filters for Targeted Analysis

- Apply display filters to further focus on specific types of traffic within the captured data (e.g., HTTP, DNS, ICMP).
- Examples include http (web traffic), tcp.port == 80 (HTTP port traffic), or ip.src == 192.168.1.100 (traffic from a specific source IP).



Observe Patterns and Identify Anomalies

● Watch for unusual patterns such as repeated requests, large data transfers, or unknown IP addresses that may indicate issues.
● Analyze anomalies like errors, high latency, or potential security threats, such as suspicious or unexpected IP addresses.

Use Color Coding to Differentiate Protocols

● Wireshark color-codes traffic by protocol to make it easier to distinguish types of packets at a glance.
● Customize color codes under View > Coloring Rules to highlight specific protocols or potential security issues.

Stop the Capture When Done

● Once you've gathered sufficient data, click the Stop Capturing icon (or press Ctrl+E again) to stop the packet capture.
● Consider saving your capture data by going to File > Save As for further analysis.