Hands-On Network Risk Assessment Using Nessus Essentials

Introduction

With digital systems growing more complex every day, so do the risks that threaten them. Vulnerabilities in operating systems, services, and applications can become easy targets for attackers if left unchecked. To stay ahead, cybersecurity professionals need reliable tools to uncover and fix these security gaps before they're exploited. This project is centered on the practical use of Nessus Essentials, a popular and powerful vulnerability scanner, in a controlled lab setup. By scanning virtual machines like Metasploitable and Windows 11, the objective is to identify potential security issues, understand their severity, and prioritize necessary fixes. Through this hands-on experience, the project aims to simulate real-world network assessments, sharpen vulnerability analysis skills, and build confidence in communicating technical risks in a clear and actionable way.

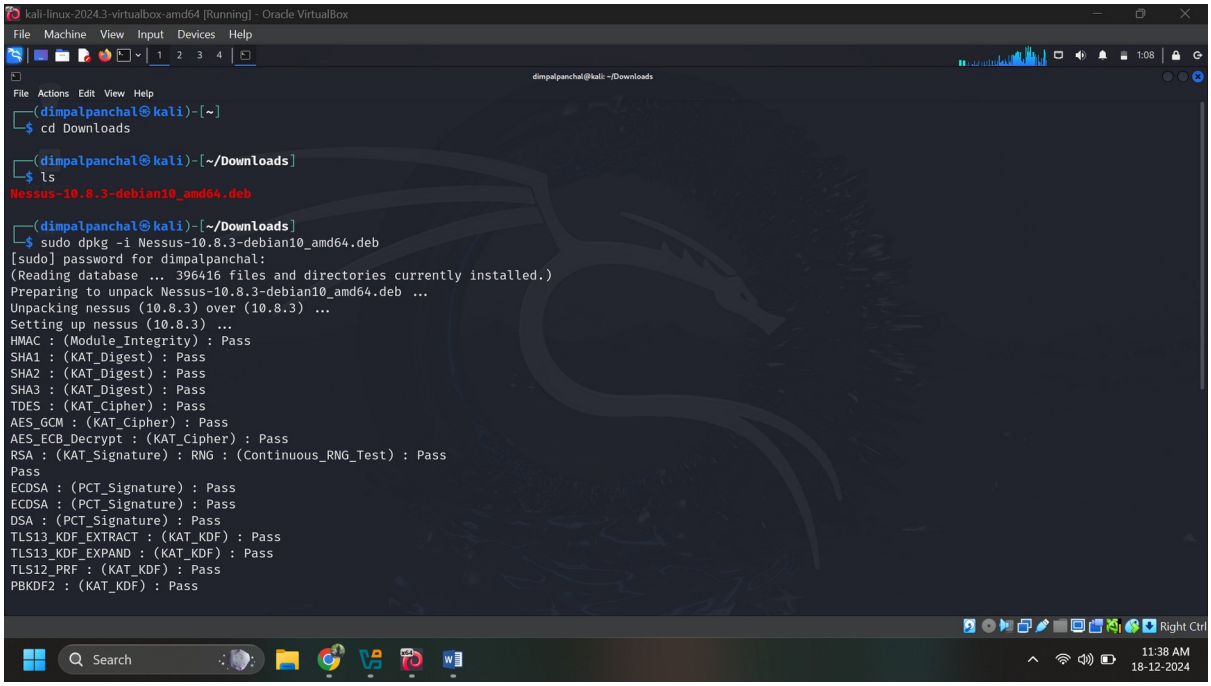
Step 1: Download and Install Nessus

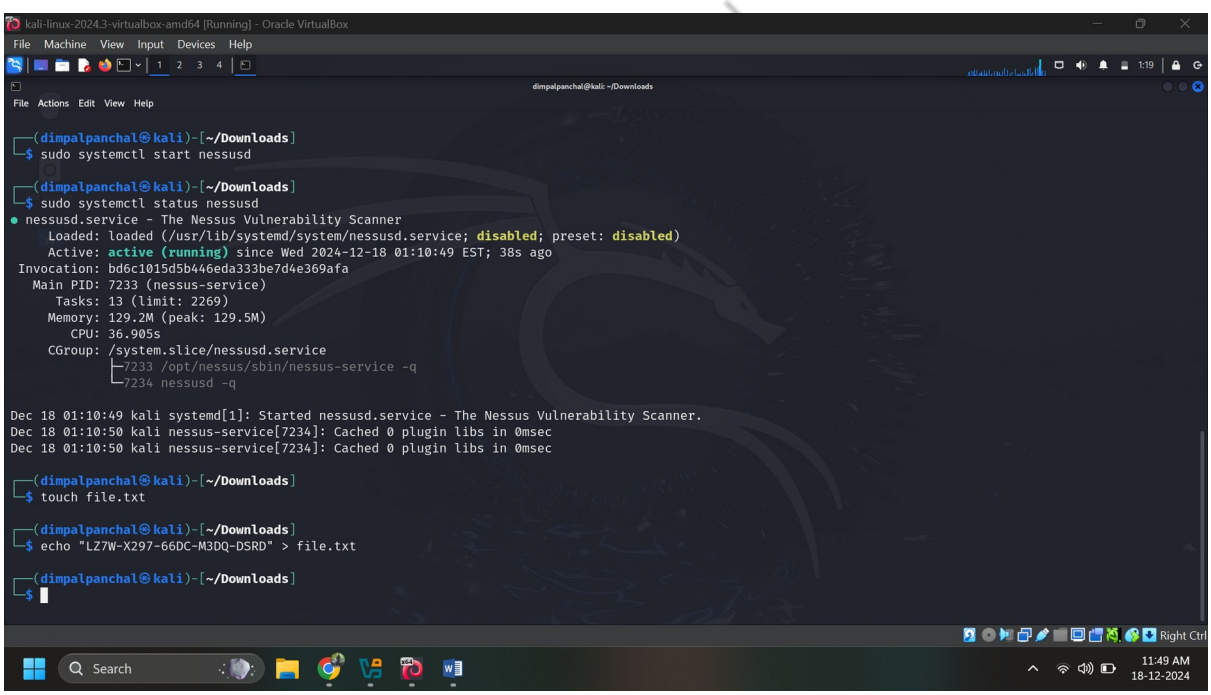
1. **Go to the Tenable Nessus download page**: Nessus Download Page

2. **Select the Nessus Essentials version** (this is free and sufficient for lab work).
3. **Get your activation code** by signing up for an account.
4. **Download the Nessus installer** for your Linux distribution (e.g., Nessus-10.7.2-debian9_amd64.deb).

Command to Install Nessus:

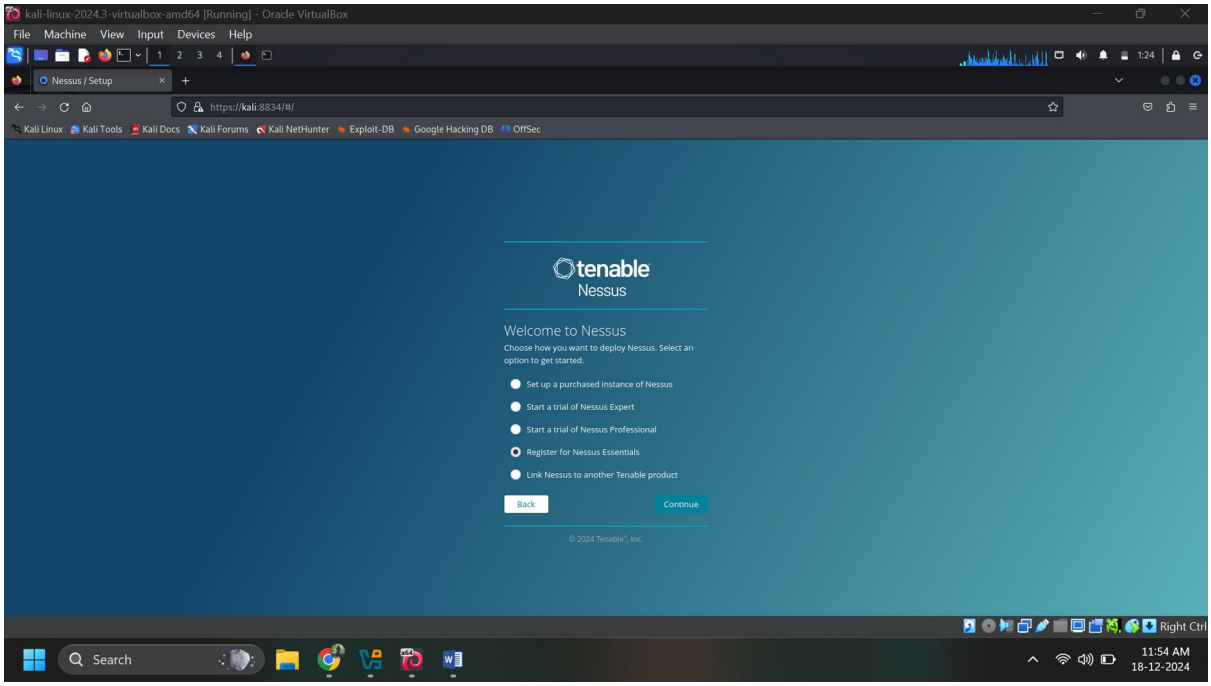
- dpkg -i Nessus-10.7.2-debian9_amd64.deb
- /etc/init.d/nessusd start

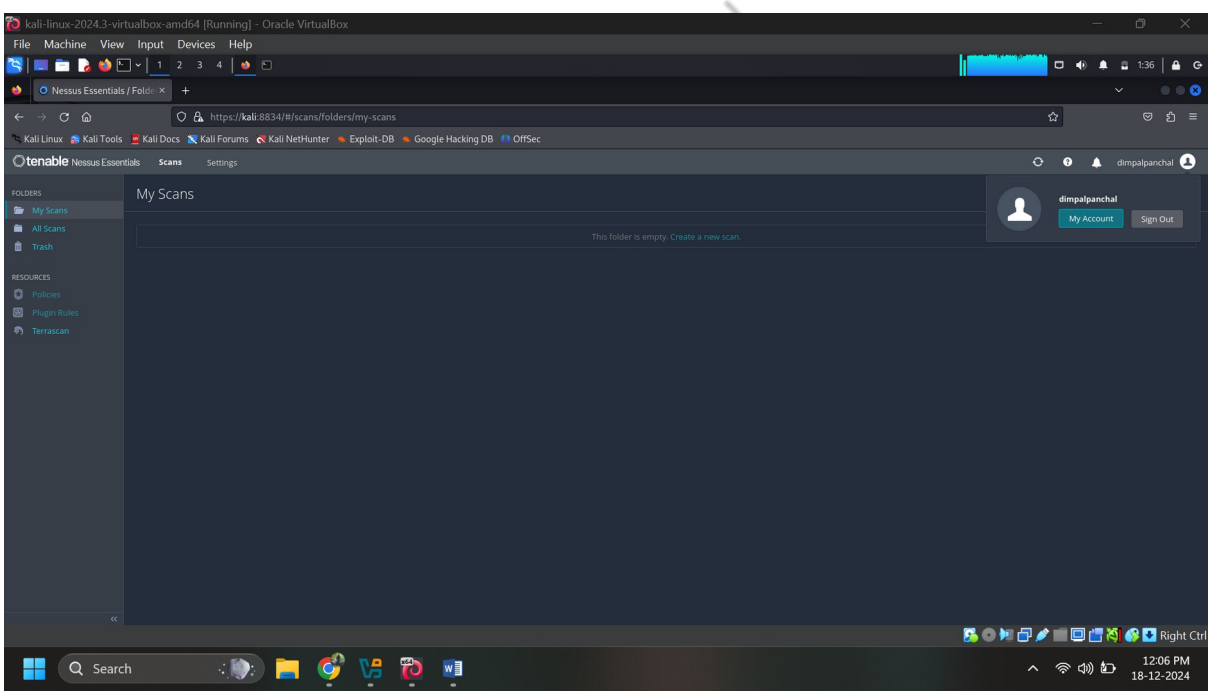




Set up Nessus by following the on-screen instructions:

- Enter your **activation code**.
- **Create an administrator account** for Nessus.
- **Wait for the plugin updates** to complete



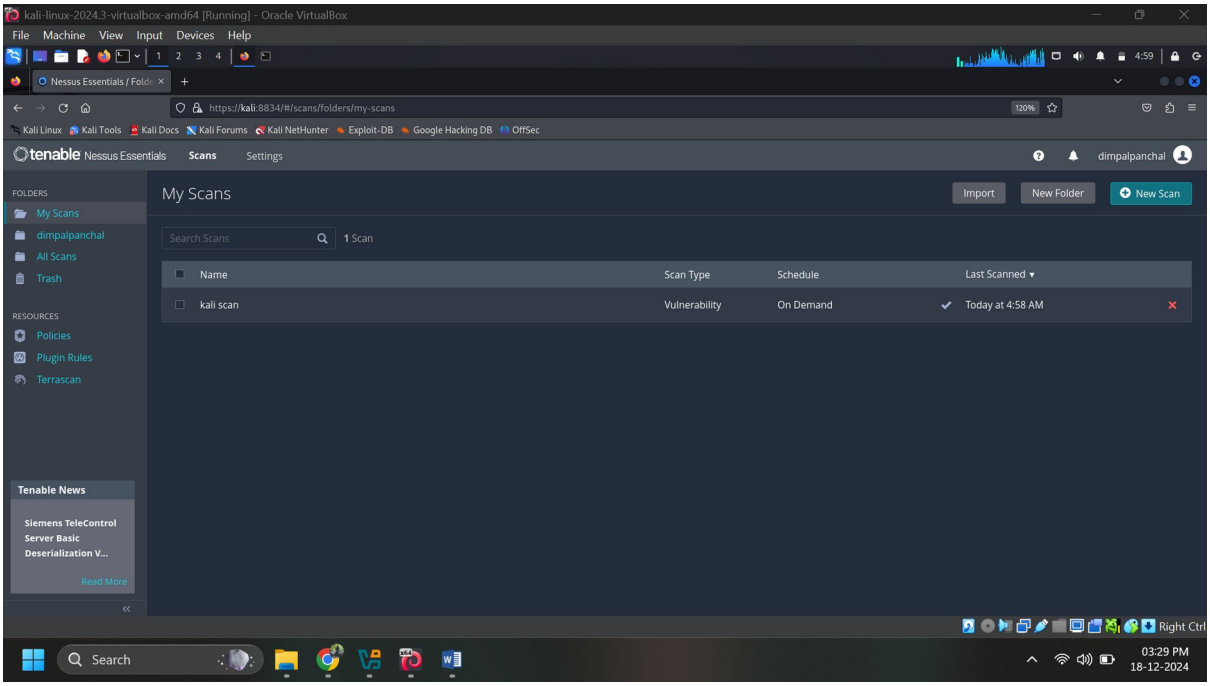


Step 2: Install IIS with FTP on Metasploit

1. **Open Windows Features**:
   - Press Win + S and search for **Turn Windows features on or off**.

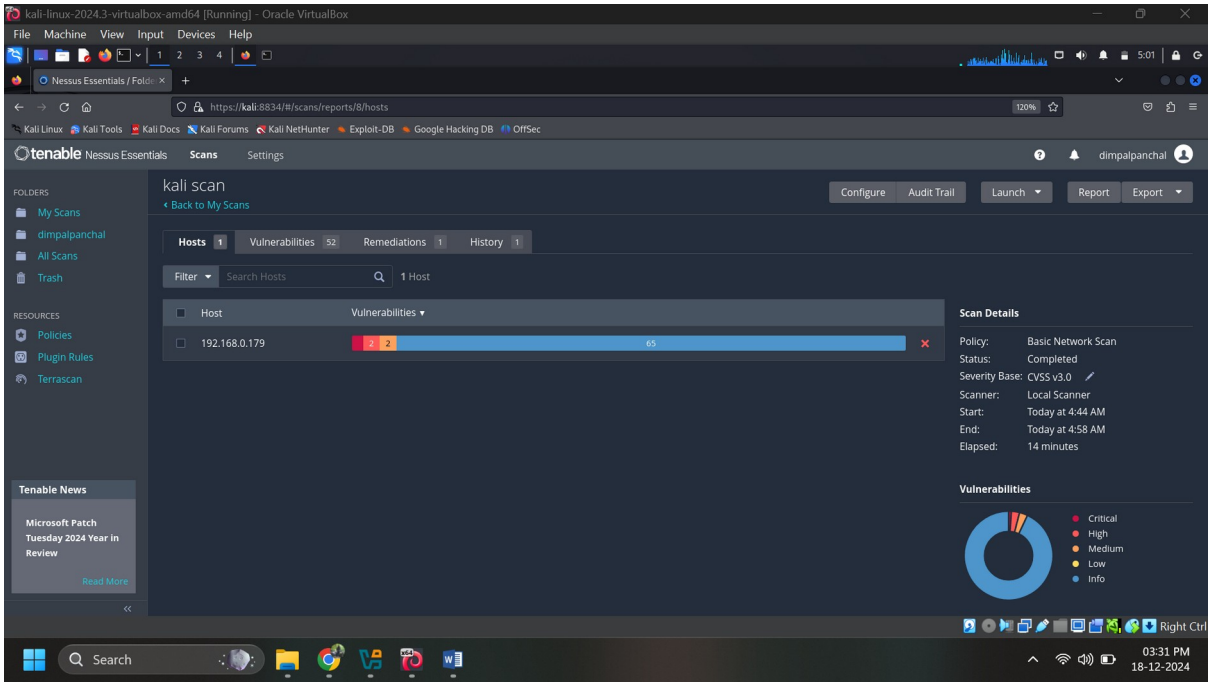
- Check the boxes for **Internet Information Services (IIS)** and **FTP Server**.
- Click **OK** to install.

2. **Configure FTP Site**:
   - Open **IIS Manager** (Win + S → Search for IIS).
   - Create a new **FTP site**:
     - Right-click **Sites** → Select **Add FTP Site**.
     - Specify a name and **physical path** for the FTP content.
     - Configure **binding** and **authentication settings**



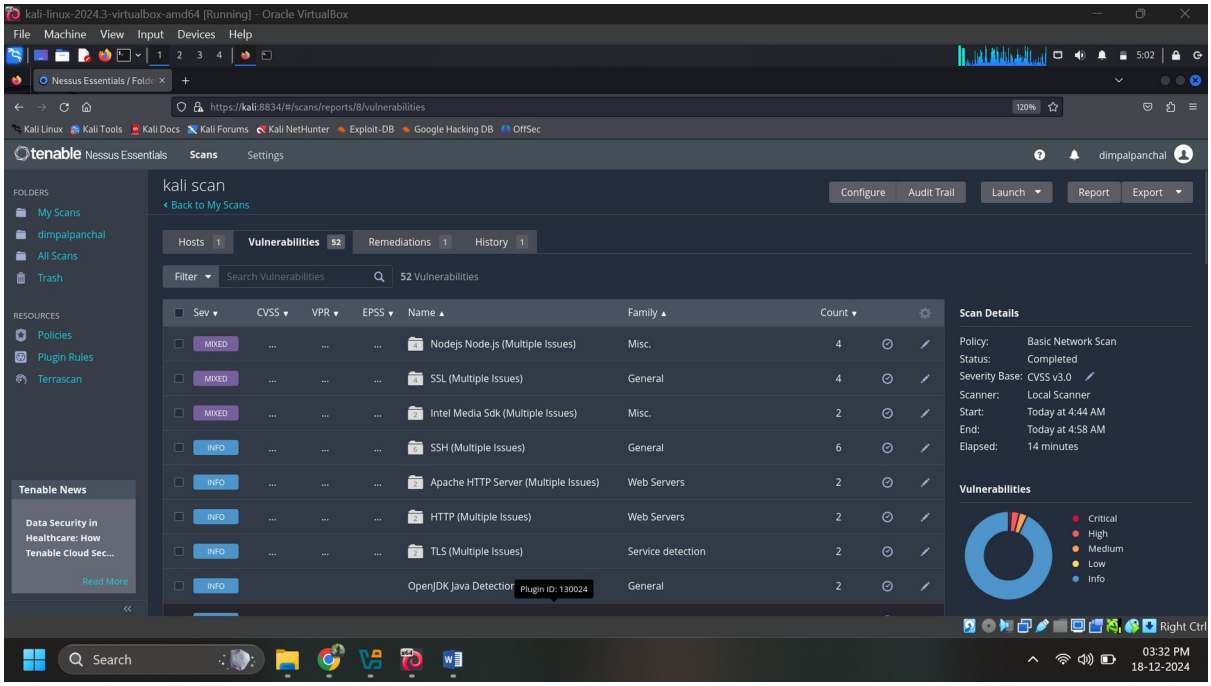
Step 3: Set up Scanning Targets (VMs)

1. **Metasploitable**: Make sure you have Metasploitable 2 installed and running in VMware.
2. **Metasploit**: Have your Metasploit VM running.
3. **Ubuntu (Optional)**: If you have an Ubuntu VM, ensure it is active for scanning.



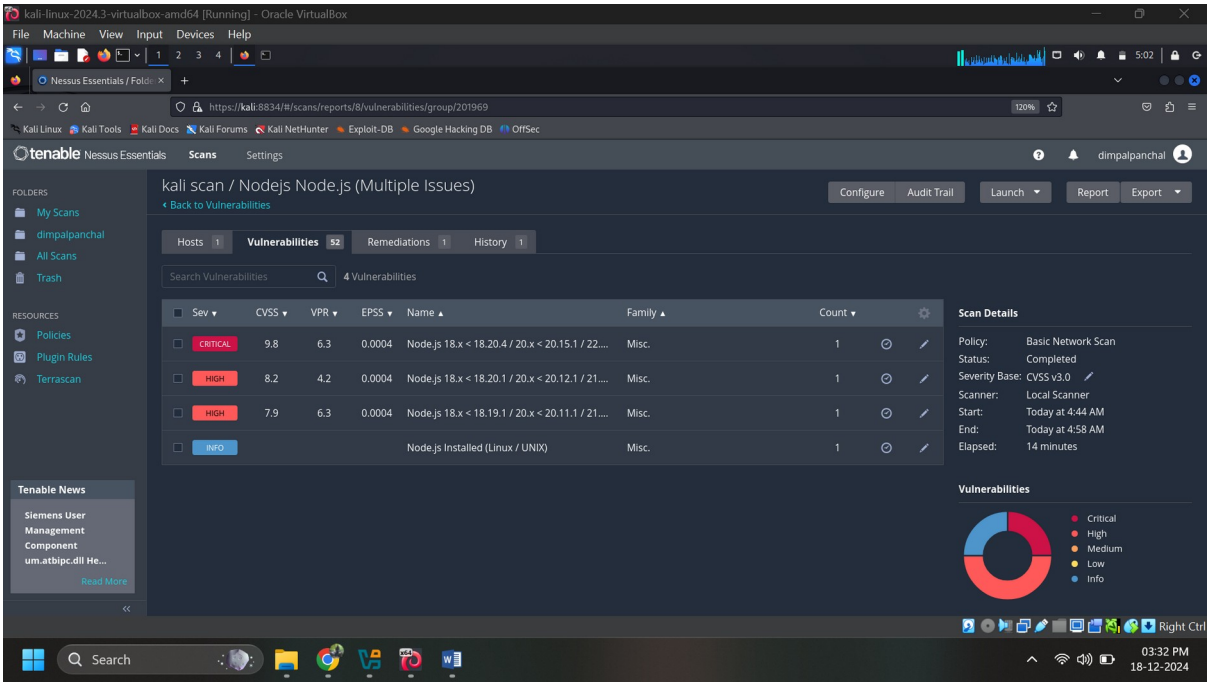
Step 4: Configure Nessus for Vulnerability Scanning

1. **Login to Nessus** via https://<your-hostname>:8834/.
2. **Create a new scan**:
   - Go to **Scans → New Scan**.
   - Select **Basic Network Scan**.
   - Set the target to scan your **VMs (Metasploitable, Windows 11, Ubuntu)** by entering their IP addresses.
3. **Customize the scan policy**:
   - You can customize scanning settings like **port scanning**, **plugin selection**, and **scan intensity** to suit the target environment.
4. **Run the Scan**: Click **Launch Scan** after configuring the targets.



Step 5: Analyse Vulnerabilities

1. **Wait for the scan to complete** (this may take some time depending on the size of the target environment).
2. **View the results**:
    - After the scan, go to the **Results** tab to see the detected vulnerabilities.
    - Vulnerabilities are listed with their severity: **Critical, High, Medium, Low**.
3. **Analyse** the vulnerabilities and note:
    - Severity level.
    - The number of occurrences.
    - Potential impact (e.g., exploitation details, system exposure).

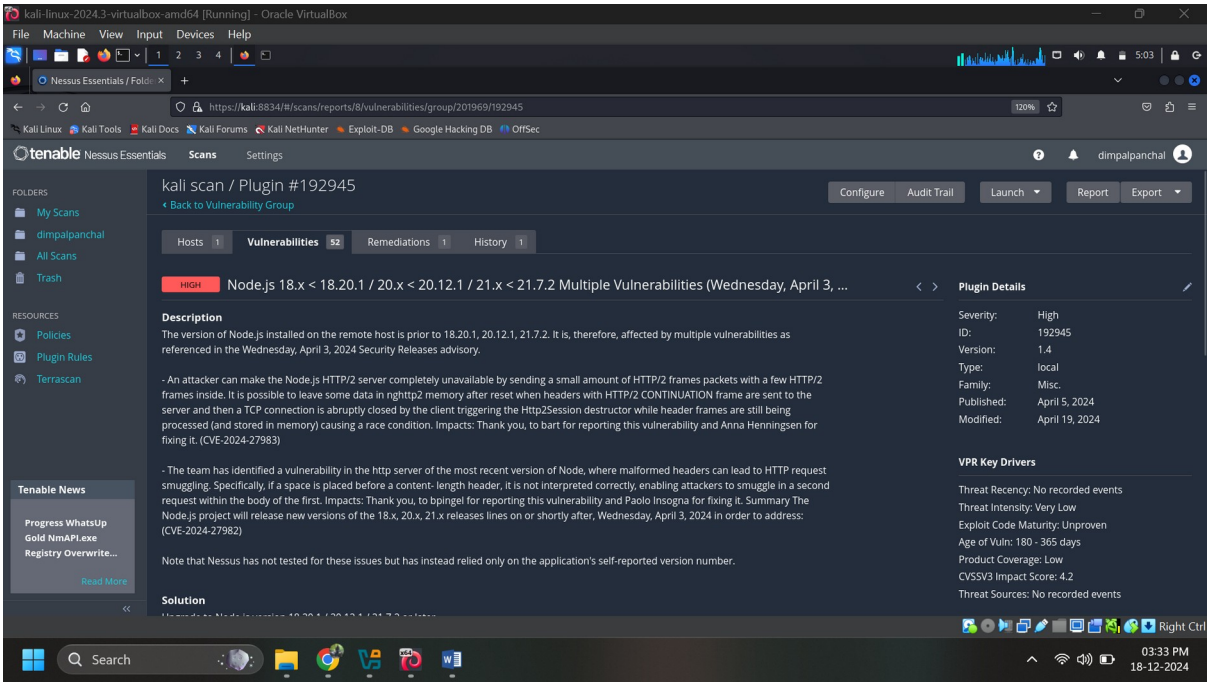


Step 6: Generate and Download Nessus Report

1. Go to the **completed scan** and select **Export**.
2. Choose a format for the report (e.g., PDF or HTML) and download it.

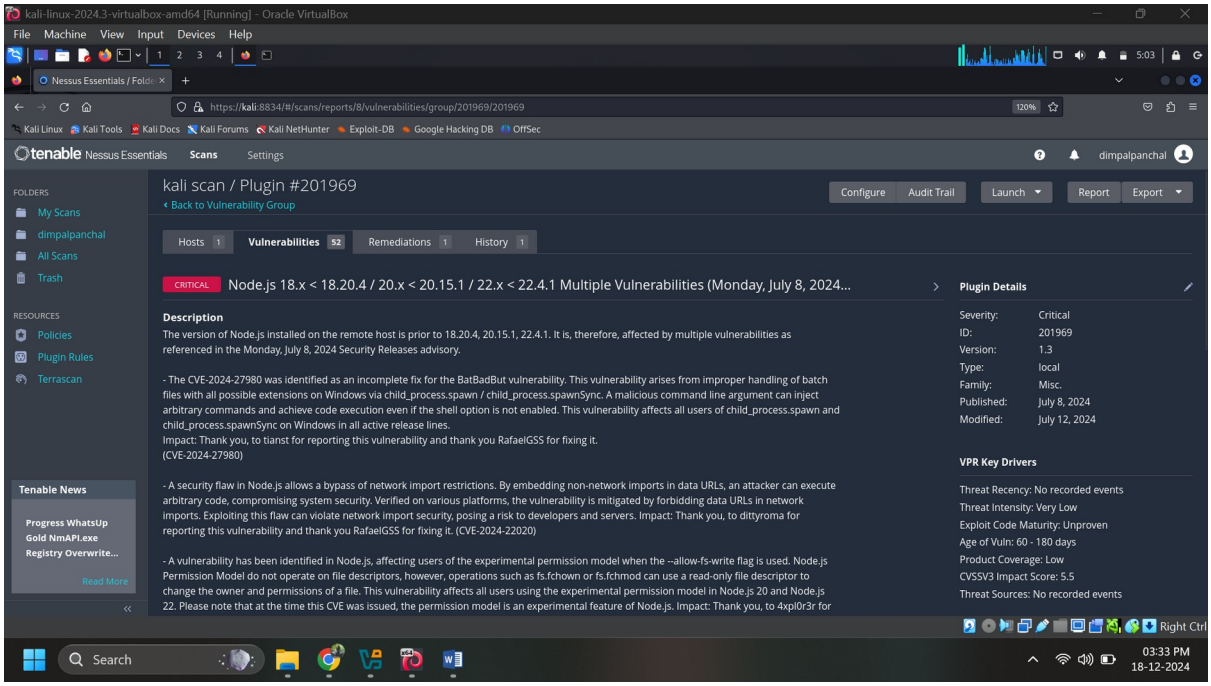
Step 7: Write-up of the Findings

1. **Summarize the findings** of the vulnerability scan:
   - What are the most critical vulnerabilities?
   - How many vulnerabilities were found?
   - Which systems are most vulnerable?
2. **Prioritize vulnerabilities**:
   - Focus on the **critical and high-severity vulnerabilities** first.
   - Consider factors such as **exploitability, potential impact**, and whether the vulnerabilities are on mission-critical systems.
3. **Recommendations**:
   - Propose remediation strategies for the top vulnerabilities (e.g., patching software, updating configurations, or disabling services).



Step 8: Collaborate with Stakeholders

1. **Create a mock communication** outlining the findings:
   - Write a brief report addressed to **system administrators or IT managers**.
   - Emphasize the **critical vulnerabilities** that require immediate action.
   - Suggest timelines for remediation.
2. **Attach the Nessus report** and your written analysis.



Conclusion

In conclusion, the successful implementation and use of the Nessus Vulnerability Scanner allowed for the identification of various security weaknesses across the lab environment. By conducting a comprehensive scan of the systems, several critical and high-priority vulnerabilities were uncovered, providing clear guidance on areas that require immediate attention. Through detailed analysis, prioritization, and the generation of a vulnerability report, this project demonstrated how Nessus can significantly enhance an organization’s ability to safeguard its network against potential security threats. The hands-on experience gained from this exercise is invaluable in understanding how vulnerability management tools contribute to reducing risks and preventing future attacks.