|  |  |
| --- | --- |
| **Name** : Muhammad Zain-Ul-Abideen | **Domain** : Cyber Security |
| **CID** : DEP6384 | **Task Instructor** : Noor-Us-Sama |
| **Topic** : Incident Response Plan Development | **Tools** : OpenVas (GVM), NMap, Fail2Ban, Ubuntu FireWall And WireShark |

**Task 3**

**Developing Incident Response Plans:**

**1. Objective:** Create a plan for responding to security incidents.

**2. Description:** Develop a structured approach for responding to and managing security incidents. Ensure the plan minimizes damage and facilitates quick recovery

**3. Key Steps:**

1. Identifying potential security incidents and scenarios.
2. Defining roles and responsibilities for the response team.
3. Developing step-by-step response procedures.
4. Conducting training and simulation exercises.
5. Reviewing and updating the plan regularly.

**1. Potential Security Incidents & Scenarios**

**Answer :** A cybersecurity incident is any event that threatens the confidentiality, integrity, or availability of information system. These incidents include malware, data breaches, phishing, and unauthorized access. Following are potential security incidents and scenarios we will be targeting and finding correct response features and mechanisms for them in this task.

**Incident: Brute Force Attack and Unauthorized Access Attempts**

A brute force attack is being attempted on my ubuntu servers, targeting SSH and HTTP services. The attacker is using automated tools to attempt multiple login combinations in order to gain unauthorized access to the system. These unauthorized access attempts could lead to a breach, potentially compromising sensitive information and other critical systems.

### ****Incident: Exploitation of Unpatched Vulnerabilities****

### An attacker is exploiting known vulnerabilities in my ubuntu server's software which are exposed to the internet. The attacker might be using automated tools to find and exploit these vulnerabilities, potentially gaining unauthorized access or escalating privileges.

### ****Incident: Suspicious Network Activity or Anomalous Traffic****

### Unusual network traffic patterns are detected, such as unexpected large volumes of traffic to the ports, which could indicate a Distributed Denial of Service (DDoS) attack or data exfiltration attempt.

### ****Incident: Zero-Day Exploit Detection****

### A zero-day exploit targeting HTTP services has been identified in the wild, and your system may be vulnerable due to unpatched software or default configurations.

### ****Incident: Insider Threat or Misconfiguration****

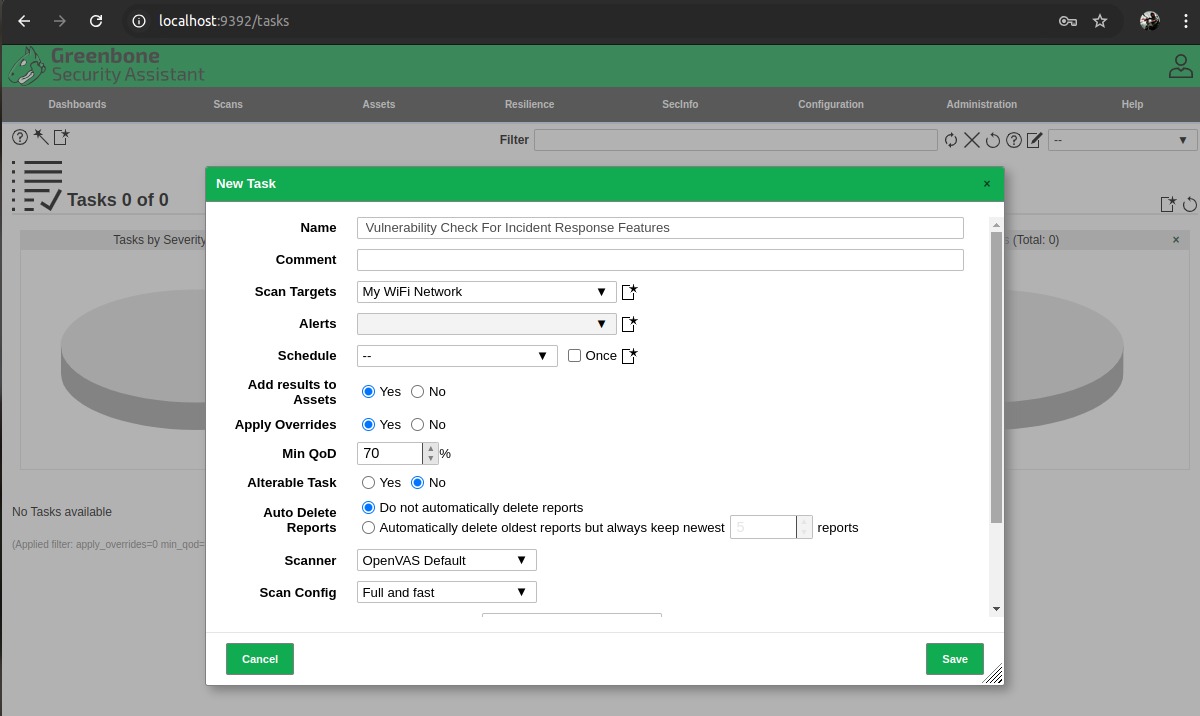
### An insider or a misconfiguration accidentally exposes services to unauthorized users, increasing the risk of exploitation.

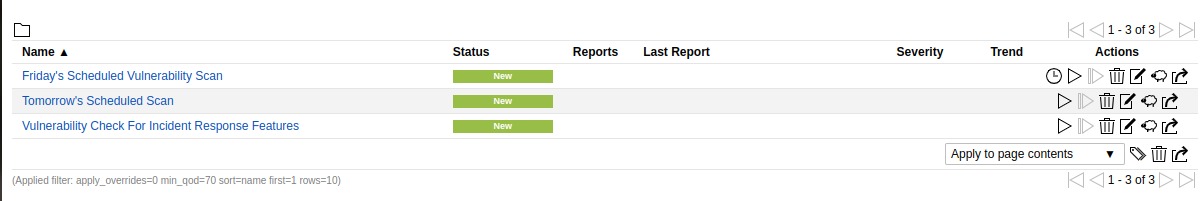
**3. Response Procedures:**

**Tool 1 : Conduct Vulnerability Scanning with GVM and OpenVAS:**

We will use **GVM** (**Greenbone Vulnerability Manager**) in collaboration with **Openvas** to scan our network for **Vulnerabilities** on a regular basis and we will also keep further more risk assessment and scans scheduled for later too. The **Target** network is my **Wi-Fi Network** (**192.168.0.112**)

**(Scroll Down)**

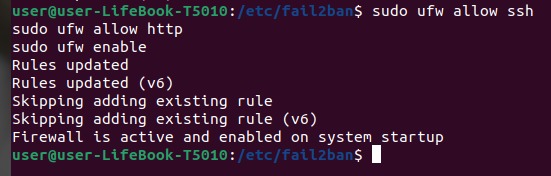




We run **a Vulnerability Scan** using **GVM** (**Greenbone Vulnerability Manager**) with **Openvas** to detect any vulnerabilities that the attacker might be attempting to exploit. This will help us in identifying and prioritizing patches or configuration changes needed to secure our system. Use **GVM** with **Openvas** to identify and correct vulnerabilities that need immediate attention and patching. We must ensure that the system isn't being exploited through known **Vulnerabilities**, which contributes to the suspicious activity. On the other hand we must also identify any weaknesses that has allowed the credential compromise, such as outdated software or configuration flaws and errors. Lastly we could run comprehensive scans to identify and prioritize vulnerabilities that need urgent attention and correct any **Misconfigurations** or vulnerabilities that could have been exposed.

**Tool 2 : Block SSH and HTTP Traffic:**

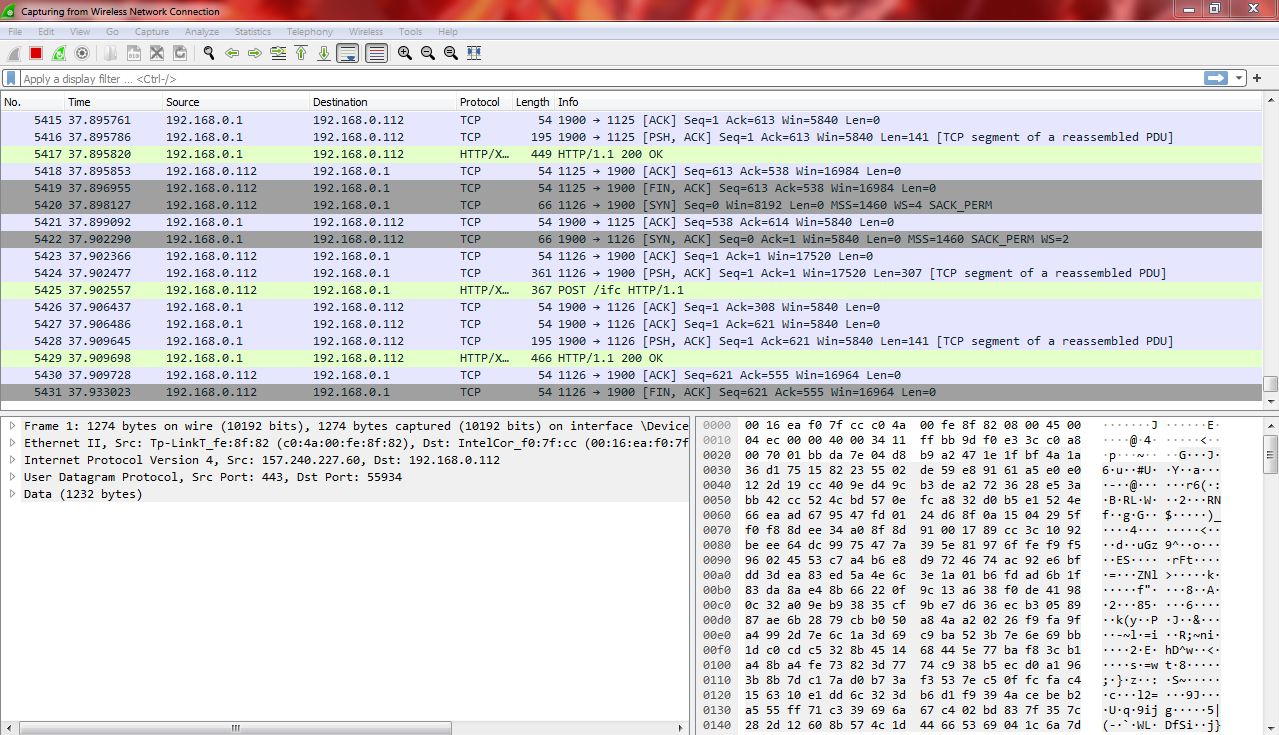
We will block all **SSH** and **HTTP** traffic using the **Ubuntu Firewall** to prevent further **Unauthorized Login** attempts and block these services to prevent the attacker from using the compromised credentials to gain further access.



This will stop the attacker's access point, reducing the risk of a successful **Brute Force Attack** and will temporarily block these services to prevent further exploitation while assessing the vulnerability and applying patches. By using this tool we cut off access to these services to prevent the attack from progressing and to protect **Sensitive Data**. As a precautionary measure, we also block access to these services until more information is available and patches can be applied.

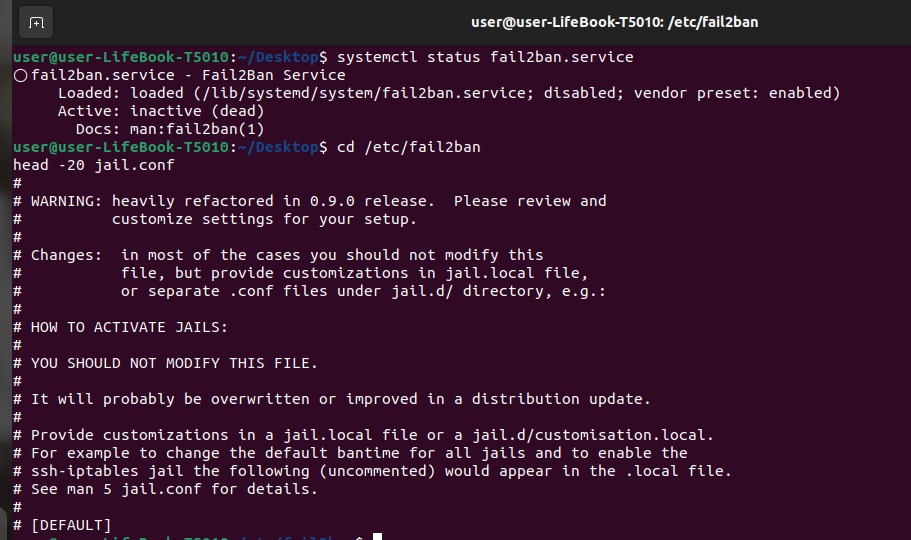
**Tool 3 : Deploy Wireshark:**

By using **Wireshark** we can **Capture** and analyze **Network Traffic** to identify the source and nature of the suspicious activity. This helps to determine whether the traffic is part of a malicious operation like **Data Exfiltration** or **Unauthorized Communication.**



We can easily confirm whether any vulnerabilities are being exploited by examining the details of network interactions. Here our **IP Address** is **192.168.0.112** and we can easily monitor its activities.

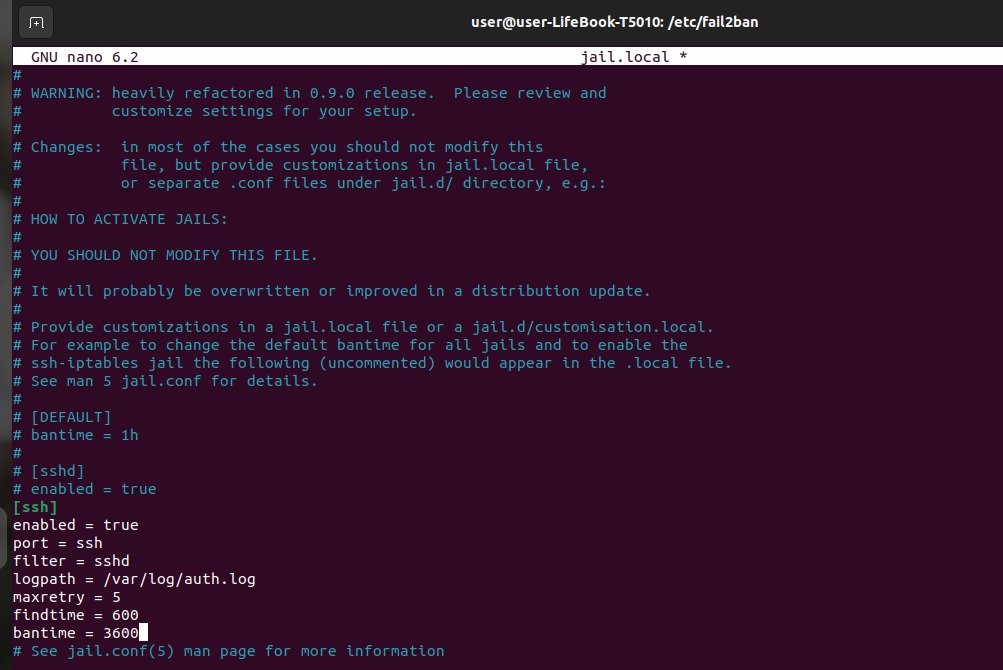
**Tool 4 : Deploy Fail2ban:**

****

Furthermore we will implement **Fail2ban** to **Monitor** log files and automatically block **IP Addresses** that repeatedly **Fail** to log in via **SSH**. This will help to mitigate **Brute Force** attempts by blocking the source IP addresses of the attack. First we configure **Fail2Ban** as done above using the **Commands.** Then we open the **Configuration File** to add our own **Preferences** using following **Commands.**



**(Scroll Down)**



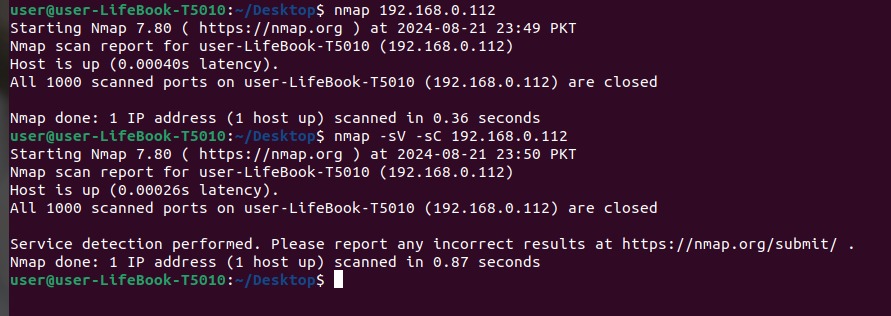


Then we add our own Preferences in the **Jail.Local File** before saving it and restarting the **Fail2Ban**. We use **Fail2ban** here to block **IPs** attempting to exploit the **Vulnerabilities**, limiting the attacker's ability to continue probing the server. Automatically block **IPs** that go through suspicious behavior, such as repeated connection attempts or high number of requests, to mitigate the attack. It will strengthen and also defends by blocking **IP addresses** attempting to use compromised credentials.

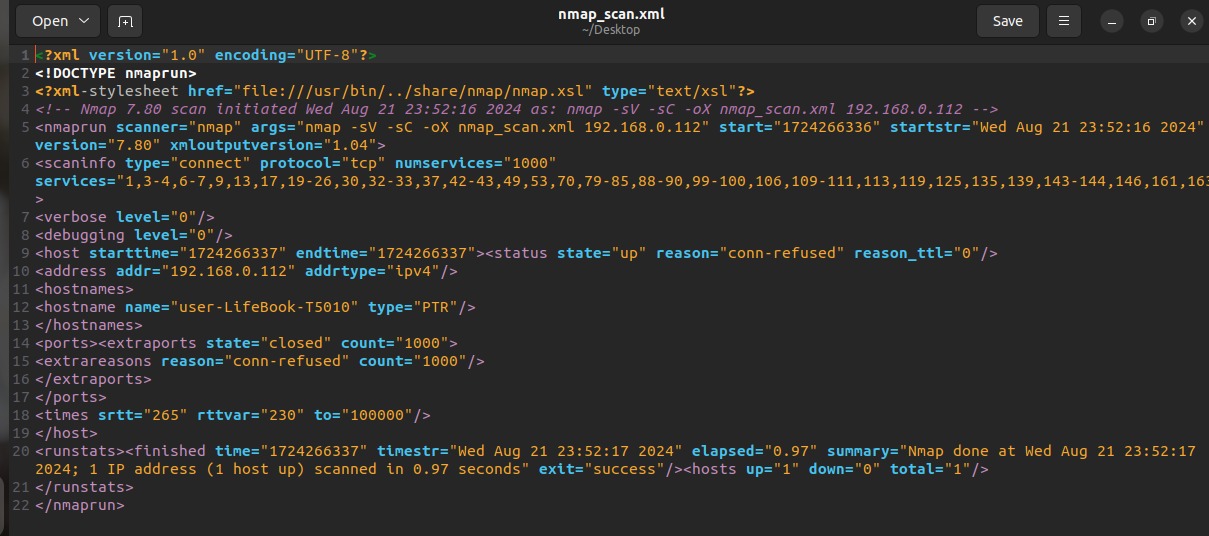
**Tool 5 : Use Nmap to Scan for Active Threats:**

Moving on we conduct a **Network Scan** using **Nmap** to identify any active connections, open ports, or suspicious services that the attacker may be exploiting. This will help in understanding the extent of the attack and in identifying any backdoors or unauthorized services.

**(Scroll Down)**



Here as you can see my **IP Domain** which is **192.168.0.112** came in perfect condition and **Nmap** even generates a report for us which will shows no **Vulnerabilities** or **Flaws** in the **Network** so it is not exploited as observed below.



So the main of motive of using **Nmap** was to scan the network to identify any unusual open ports or services that may have been exploited and to perform a network scan to identify the source of the anomalous traffic and any compromised system. We can also check for any **Unauthorized** or **Unexpected Services** that the attacker might have established using the compromised credentials with respect to scanning for any indicators of compromise or signs that the **zero-day exploit** has been used against the system.

From above techniques we can conclude that **Incident Response** is crucial for minimizing damage, protecting data, and reducing downtime during cyber threats. It prevents escalation, ensures compliance, preserves trust, and strengthens overall security.

### ****4. Conducting Training and Simulation Exercises****

**We have** to ensure that the incident response team is prepared to handle real world cybersecurity problems efficiently, it's important to conduct regular training and simulation exercises.

* **Simulate Attacks:** Create realistic scenarios, such as a simulated **Brute Force Attack** or N**etwork Intrusion,** to test the team's ability to detect, respond, and mitigate threats.
* **Hands-On Practice:** Use tools like the **Ubuntu firewall, Fail2ban, Wireshark, Nmap**, and **GVM (OpenVAS)** during simulations to provide hands-on experience with the actual tools used in incident response.
* **Evaluate Performance:** Assess the team's response time, decision-making, and effectiveness during the exercises. Identify any gaps in knowledge or procedures that need improvement.
* **Iterative Learning:** Use the results of these simulations to refine skills and update protocols, ensuring that the team is well-prepared for any real incidents.

### ****5. Reviewing and Updating the Plan Regularly****

The cybersecurity domain is constantly changing, with new threats emerging and existing ones holding on. Regularly reviewing and updating the **Incident Response** Plan ensures that it remains effective and relevant.

* **Regular Assessments:** Regularly review the **Incident Response** Plan to ensure it aligns with the latest cybersecurity threats, tools, and best practices.
* **Incorporate Feedback:** Use insights gained from previous incidents and simulation exercises to update the plan, addressing any weaknesses or new challenges identified.
* **Updated Tools:** Ensure that the tools used in incident response, such as **Wireshark, Nmap**, **and GVM (OpenVAS)**, are up-to-date and that staff are trained on any new features or technologies.
* **Continuous Improvement:** Normalize a culture of continuous improvement by encouraging regular feedback from the incident response team and other stakeholders, ensuring the plan evolves alongside emerging threats.