Name : Sheharyar Khalid.

Internship: Cyber Security.

Task no: 1.

Organization: DEP.

Task:

**1. Conducting a Risk Assessment**

**Risk Assessment Spreadsheet**

**1. Identify Assets**

| **Asset ID** | **Asset Name** | **Asset Description** | **Owner** | **Location** |
| --- | --- | --- | --- | --- |
| 1 | Web Server | Hosts company website and web apps | IT Department | Data Center 1 |
| 2 | Database Server | Stores customer data and transactions | IT Department | Data Center 1 |
| 3 | Workstations | Employee computers | IT Department | Office Floor 1 |
| 4 | Router | Network router | IT Department | Data Center 1 |
| 5 | Firewall | Network firewall | IT Department | Data Center 1 |

**2. Identify Threats**

| **Threat ID** | **Threat Description** | **Relevant Assets** |
| --- | --- | --- |
| 1 | Unauthorized access to database | Database Server |
| 2 | Malware infection on workstations | Workstations |
| 3 | Denial of Service (DoS) attack on web server | Web Server |
| 4 | Physical theft of router | Router |
| 5 | Misconfiguration of firewall | Firewall |

**3. Assess Vulnerabilities**

| **Vulnerability ID** | **Vulnerability Description** | **Affected Asset** | **Known Exploit** |
| --- | --- | --- | --- |
| 1 | Weak password policy on database server | Database Server | Yes |
| 2 | Outdated antivirus software on workstations | Workstations | No |
| 3 | Unpatched software on web server | Web Server | Yes |
| 4 | Unsecured physical access to router | Router | No |
| 5 | Inadequate firewall rules configuration | Firewall | Yes |

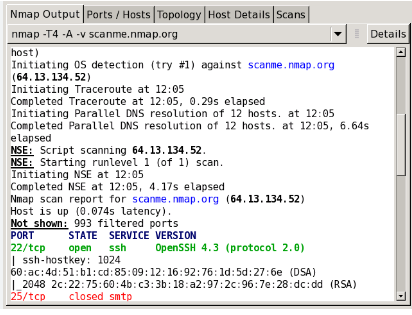
**4. Evaluate Impact and Likelihood**

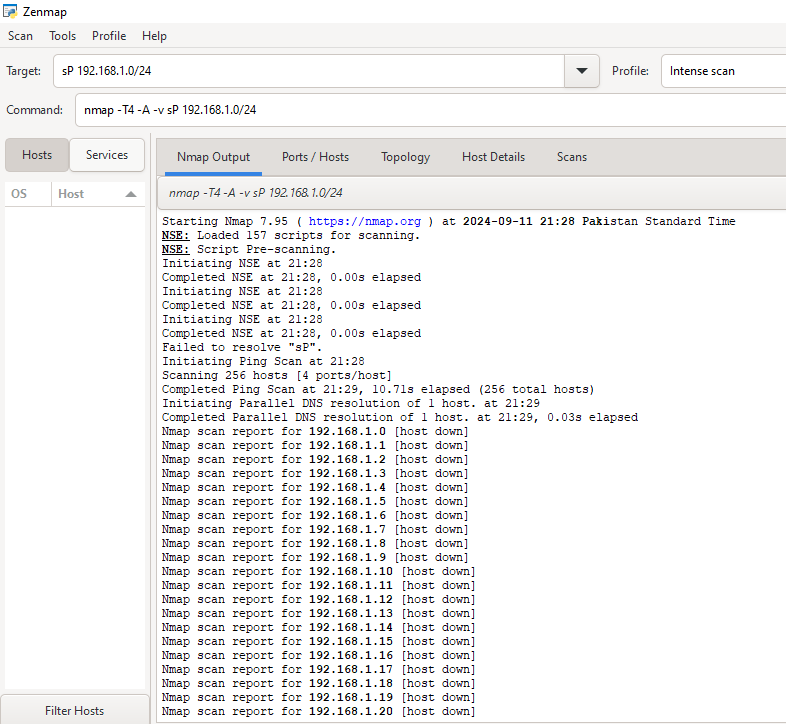
| **Threat ID** | **Vulnerability ID** | **Impact (1-5)** | **Likelihood (1-5)** | **Risk Level (Impact x Likelihood)** |
| --- | --- | --- | --- | --- |
| 1 | 1 | 5 | 3 | 15 |
| 2 | 2 | 3 | 4 | 12 |
| 3 | 3 | 4 | 3 | 12 |
| 4 | 4 | 4 | 2 | 8 |
| 5 | 5 | 3 | 3 | 9 |

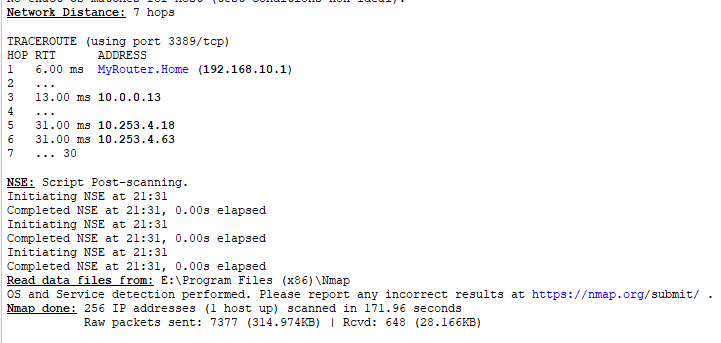
**Explanation:**

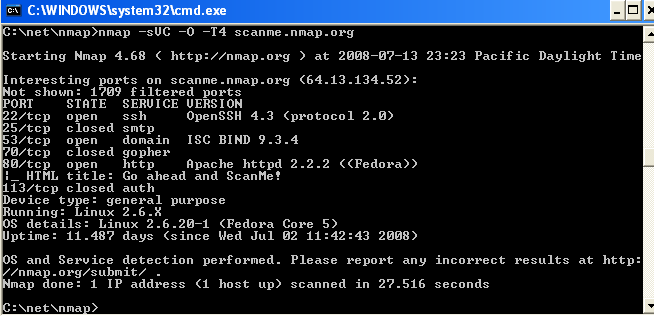
* **Assets:** Critical components of your network, including servers, workstations, and network devices.
* **Threats:** Potential risks that could harm the assets.
* **Vulnerabilities:** Weaknesses or gaps in the system that could be exploited by threats.
* **Impact:** How severe the consequences would be if the threat exploited the vulnerability (1 being minimal and 5 being catastrophic).
* **Likelihood:** The probability of the threat exploiting the vulnerability (1 being rare and 5 being highly likely).
* **Risk Level:** Calculated as Impact x Likelihood to prioritize the risks.

**Task no 2:**









Task 3:

**Objective: Ensure Security Policies are Adequate**

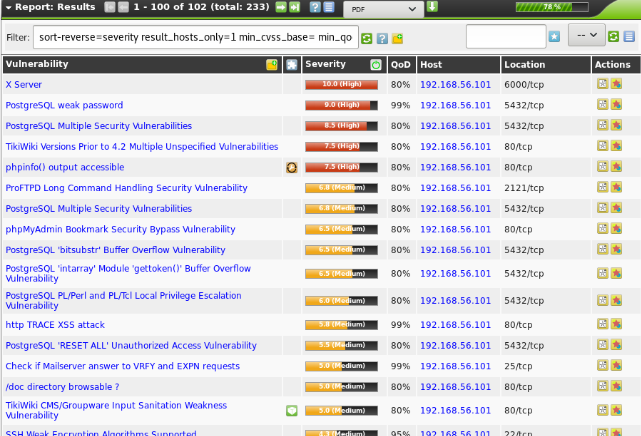
**Steps:**

1. **Policy Review**:
   * **Action**: Review existing security policies and procedures in detail.
   * **Focus Areas**:
     + Password Management
     + Access Control
     + Data Encryption
     + Incident Response Plan
     + Employee Training Requirements
   * **Example Questions**:
     + Are password policies in line with best practices (e.g., minimum length, complexity, and expiration)?
     + Is access to critical systems restricted based on roles and responsibilities?
     + Are encryption standards compliant with industry regulations (e.g., AES-256)?
     + Is there a clear, tested incident response plan in place for potential breaches?
     + How often are security awareness training programs conducted?
2. **Interview Staff**:
   * **Action**: Conduct informal interviews with key IT personnel to gauge how well the policies are implemented in practice.
   * **Participants**: IT Manager, System Administrator, Network Security Officer
   * **Focus Areas**:
     + Understanding of Policies
     + Practical Challenges
     + Suggestions for Improvement
   * **Example Questions**:
     + How well do current policies align with day-to-day practices?
     + What are the main challenges in enforcing these policies?
     + Do you think the incident response plan is effective and understood by the team?
     + What improvements or updates to security policies would you recommend?

**Outcome:**

* Identify any gaps between documented policies and actual practices.
* Document recommendations for policy updates or improvements based on feedback from staff and findings from the policy review.

OpenVAS:



Conclusion:

In conclusion, conducting a thorough risk assessment, scanning for vulnerabilities, and reviewing security policies are essential steps in identifying potential threats and improving the security posture of a network. By cataloging assets, assessing threats and vulnerabilities, and using tools like Nmap and OpenVAS, organizations can detect weaknesses and address security gaps. Reviewing policies and gathering insights from IT staff ensures that procedures are up-to-date and effectively implemented. Finally, compiling these findings into a comprehensive report allows for clear communication of risks and actionable recommendations for enhanced network security.