Cybersecurity Risk Assessment

- Cybersecurity Risk Assessment is the process of identifying, analysing, and evaluating potential threats and vulnerabilities in an organization's information systems.
- It aims to assess the potential impact of these risks on the confidentiality, integrity, and availability of sensitive data.
- This process also assists the organizational decision-makers in assessing the security posture of the organization, evaluating how capable the organization of managing the defense of critical assets and data in response to changes, and whether improvements are necessary.
- Its objectives are set:

1. **Frame the risk:**
    - Identify the threats and vulnerabilities that increase the risk, so great and well-mannered decision-making can be implemented in dealing with the risk management processes to foster awareness and understanding in all parties involved and to take appropriate preventative measures.
2. **Assess the risk:**
    - Conducting a comprehensive analysis of assets, determining the likelihood of various scenarios, and assessing the potential impact on confidentiality, integrity, and availability of data.

3.Respond to the risk:

Develop and execute action plans based on the assessed risks. This may involve implementing security measures, updating policies, or even acquiring insurance to transfer certain risks.

A. Threat Identification

- It is the process of systematically recognizing and documenting potential threats that could exploit vulnerabilities in a system.
- The goal is to understand the various ways in which the security of the system could be compromised.
- Main threats that are commonly found

1. Internal threats
    - It refers to potential risks or security vulnerabilities that originate from within an organization.
    - It is caused by the abuse of extended privileges given to trusted employees of organizations and the non-vigilant security practices.
    - Examples of internal threats
        a) Mishandling data
        b) Inviting malware into network by accessing malicious emails from websites
        c) Facilitating outside attacks by connecting infected USBs into the system.
    - Preventions
        a) Encryption
        b) Use of action monitoring software
        c) Control internal access to sensitive data

2. External threats
    - It relates to malicious actors attempting to gain unauthorized access to the network of the targeted organization.
    - It is caused by the system vulnerabilities to gain initial access.
    - Examples of external threats
        a) Social engineering
        b) Malware
        c) Hacking
    - Preventions
        a) Vulnerability scanning and patch management.
        b) Cyber awareness training
        c) Endpoint detection and response

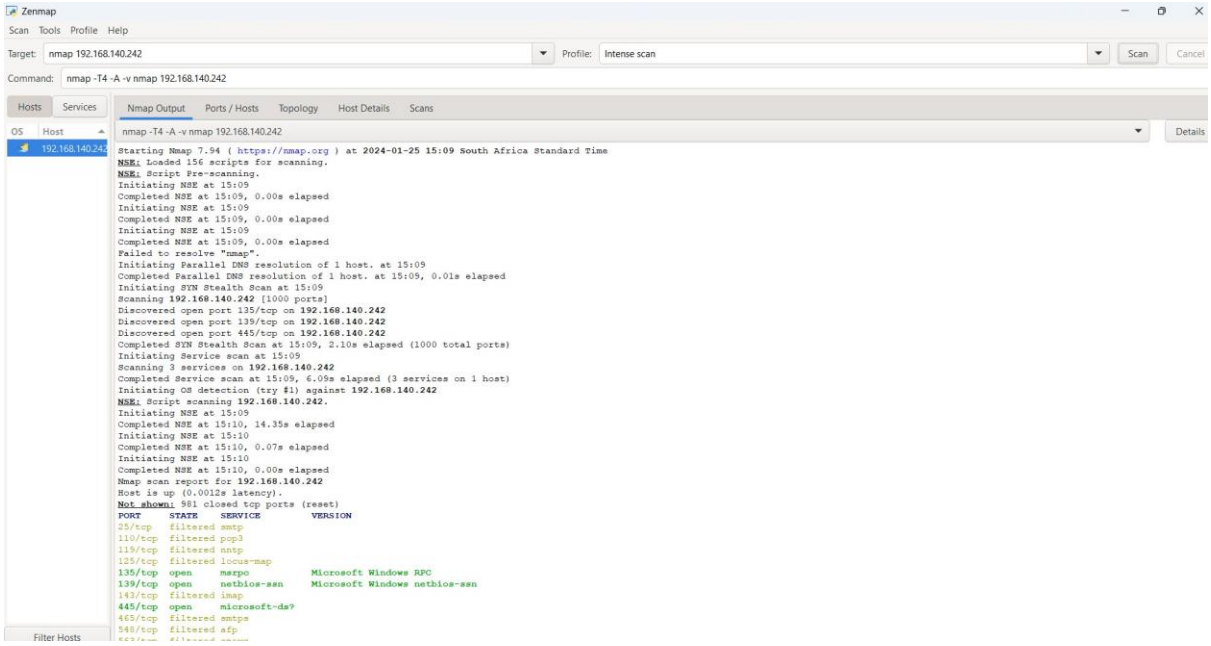
Note: Prevention of both internal and external threats can be applied to both.

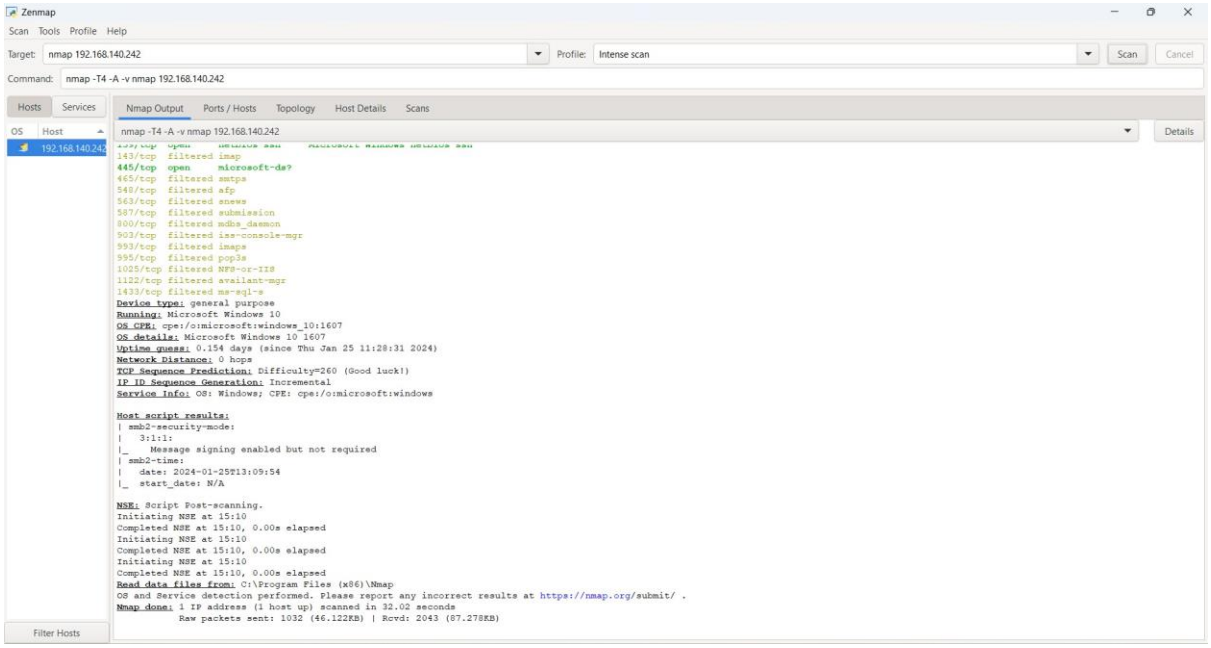
B. Vulnerability Scanning

- **Vulnerability scanning is the security practice that involves systematically scanning a computer system, network, or application to identify and assess potential security vulnerabilities.**
- **Its purpose is to discover weaknesses in the system's defenses that could be exploited by attackers.**
- **Types of weaknesses is software vulnerabilities, misconfigurations, or other security issues that could compromise the confidentiality, integrity, or availability of the system.**
- **Its use of this tool is to discover hosts and services on a computer network by sending packets and analysing the responses.**
- **Other types of tools that can be used like vulnerability scanning are:**
    a) **Nessus**
    b) **Nmap**
    c) **Burp Suite**
    d) **Acunetix**

Note: It's important to choose the right tool for the job based on the type and size of system being scanned.

Vulnerability scan report:





The scan above indicates:

a. TCP (Transmission Control Protocol) – is a connection-orientated communication protocol that operates at the transport layer of the Internet Protocol (IP) suite.

b. Open state – indicate the ports or services that can be accessed by other network devices and can be exploited.

1. Port 135(msrpc):

    1. **Use:** Used for Microsoft Remote Procedure Call (MSRPC) services, facilitating communication between applications on different devices in a network.

2. **Risk:**
    - **Remote Code Execution:** Vulnerabilities in MSRPC services could potentially allow remote code execution, providing an entry point for attackers.
    - **Worm Propagation:** Malicious actors may exploit vulnerabilities on Port 135 to propagate worms across networks.
3. **Mitigation:**
    - **Firewall Rules:** Restrict external access to Port 135, allowing only necessary internal communication.
    - **Patching:** Regularly update and patch systems to address known vulnerabilities.
    - **Network Segmentation:** Isolate critical systems and services to limit the potential impact of a compromise.

2. Port 139(netbios-ssn):

1. **Use:** Associated with the NetBIOS Session Service, providing session-layer services for communication between computers on a local network.
2. **Risk:**
    - **Brute Force Attacks:** Weak or easily guessable passwords may lead to unauthorized access through this port.
    - **Information Disclosure:** NetBIOS services may expose sensitive information about the system.
3. **Mitigation:**
    - **Strong Password Policies:** Enforce strong password policies to mitigate the risk of unauthorized access.
    - **Encryption:** Use encryption for communication over Port 139 to protect sensitive data.
    - **Disable Unnecessary Services:** Disable NetBIOS services if not required for business operations.

3. Port 445(Microsoft-ds):

1. **Use:** Associated with Microsoft-DS (Microsoft Directory Services) and is used for file and printer sharing as well as other network services.
2. **Risk:**
    - **SMB Vulnerabilities:** Security vulnerabilities in Server Message Block (SMB) services on Port 445 may lead to unauthorized access or data exposure.
    - **EternalBlue Exploits:** Port 445 was exploited by the EternalBlue exploit, leading to widespread ransomware attacks.
3. **Mitigation:**
    - **Patching:** Regularly update and patch systems to address SMB vulnerabilities.
    - **Network Segmentation:** Segment networks to contain the impact of a potential compromise.

- **Disable SMBv1:** Disable older SMB versions and use SMBv2 or higher for improved security.

c. Filtered state – indicate access to a port or service is blocked by a firewall and can't be exploited.

1.Port 25(smtps):

1. **Use:**
   - Port 25 is commonly used for SMTP (Simple Mail Transfer Protocol) communication. It is the standard protocol for email transmission and is responsible for sending emails between servers.
2. **Risk:**
   - **Unauthorized Email Relay:** If not properly configured, an open SMTP port can be exploited for unauthorized email relay, allowing attackers to send spam through the server.
   - **Email Spoofing:** Attackers may use open SMTP ports to send emails with forged sender addresses, leading to phishing or other malicious activities.
3. **Mitigation:**
   - **SMTP Authentication:** Enforce SMTP authentication to prevent unauthorized use of the server for relaying emails.
   - **Sender Policy Framework (SPF):** Implement SPF records to specify which servers are authorized to send emails on behalf of a domain.
   - **Rate Limiting:** Implement rate-limiting mechanisms to restrict the number of emails that can be sent within a given timeframe, reducing the impact of spamming attempts.
   - **Monitoring:** Regularly monitor SMTP traffic for unusual patterns or signs of abuse

C. Risk Analysis

- Risk analysis is a systematic process of identifying, assessing, and prioritizing potential risks to an organization's assets, operations, and objectives. It is a fundamental component of risk management, providing valuable insights to make informed decisions about how to mitigate or accept risks.
- It involves evaluating the likelihood and impact of various risks to determine their significance and potential consequences.

key steps involved in risk analysis:

- **Risk Identification:**
  - **Definition:** Identify and enumerate potential risks that could impact the organization.
  - **Methods:** This can be achieved through brainstorming, documentation review, interviews, and analysis of historical data.
- **Risk Assessment:**
  - **Definition:** Evaluate the likelihood and potential impact of each identified risk.

1. **Methods:** Use qualitative and quantitative methods to assess risks. Qualitative methods involve assigning subjective values (high, medium, low), while quantitative methods involve assigning numerical values for likelihood and impact. **Risk Prioritization:**
   - **Definition:** Prioritize risks based on their significance, considering both likelihood and impact.
   - **Methods:** Create risk matrices, risk heat maps, or other tools to visually represent the prioritization of risks.
2. **Risk Mitigation:**
   - **Definition:** Develop and implement strategies to reduce the likelihood or impact of identified risks.
   - **Methods:** This can involve implementing security controls, improving processes, investing in technology, or transferring risk through insurance.
3. **Risk Acceptance:**
   - **Definition:** Decide to accept certain risks if their mitigation is deemed impractical or if the potential impact is deemed acceptable.
   - **Methods:** Organizations may accept certain risks if the cost of mitigation exceeds the potential loss.
4. **Risk Monitoring and Review:**
   - **Definition:** Continuously monitor the risk landscape and periodically review the effectiveness of risk mitigation measures.
   - **Methods:** Regularly update risk assessments, adapt strategies based on changes in the organization or external environment, and learn from past incidents

Key objectives of risk analysis:

1. **Risk Impacts:**
   - **Objective:** Assess the potential consequences or impacts that a risk event could have on the organization's assets, operations, or objectives.
   - **Purpose:** By evaluating the impact of various risks, organizations can prioritize their responses and allocate resources effectively to minimize negative consequences.
2. **Risk Probability:**
   - **Objective:** Determine the likelihood or probability of a risk event occurring.

- **Purpose:** Understanding the probability helps in assessing the likelihood of different risks materializing. This information is crucial for prioritizing risks and focusing mitigation efforts on the most probable and impactful ones.

3. **Risk Exposure:**
    - **Objective:** Calculate the overall risk exposure, which is the product of risk impacts and probabilities.
    - **Purpose:** Risk exposure provides a comprehensive view of the potential harm and likelihood of occurrence. It aids in ranking and comparing risks to make informed decisions on risk management strategies.

D. Overall recommendation

1. **Implement Access Controls:**
    - Enforce multi-factor authentication to enhance user identity verification.
    - Regularly review and update user access rights to ensure appropriate permissions.
2. **Employee Training and Awareness:**
    - Conduct ongoing security awareness programs to educate employees on security best practices.
    - Provide training on recognizing and mitigating phishing attacks and social engineering tactics.
3. **Regular Security Assessments:**
    - Perform regular vulnerability scanning to identify and address potential weaknesses.
    - Conduct penetration testing to simulate real-world attacks and identify system vulnerabilities.
    - Conduct security audits to assess the effectiveness of security controls.
4. **Data Backup and Recovery:**
    - Implement data backup strategies using external hard drives, USB devices, or cloud-based solutions.
    - Ensure regular testing of backup and recovery procedures to verify their effectiveness.
5. **Incident Response Plan:**
    - Develop and maintain an incident response plan with clear communication protocols.
    - Define procedures for incident containment, eradication, recovery, and post-incident analysis.
6. **Security Governance:**
    - Implement playbooks that outline standardized responses to common security incidents.
    - Establish and enforce security policies and procedures to govern security practices.
7. **Continuous Monitoring:**
    - Monitor logs to record events within the organization's system for analysis.

- Implement Endpoint Detection and Response (EDR) solutions.
- Utilize Security Information and Event Management (SIEM) products for comprehensive monitoring.

8. **Regular Patch Updates:**
    - Ensure frequent updates and upgrades of software to address known vulnerabilities.
    - Establish a patch management process to systematically apply updates across the organization.