**Cybersecurity Risk Assessment**

A cybersecurity risk assessment is the continuous process of identifying and analyzing vulnerabilities in organizations so they can determine the potential impact of attacks and implement the most effective security practices to minimize the risks.

This process also aids the organizational decision-makers in assessing the security posture of the organization, evaluating how capable the organization is of managing the defense of critical assets and data in response to changes, and whether improvements are necessary.  
  
 As part of the risk assessment, the following objectives are set:

1. **Frame the risk:**  
   - Identify the threats and vulnerabilities that increase the risk, so better decision-making can be implemented in communicating the risk management processes to foster awareness and understanding among all parties involved and to take appropriate preventative measures.
2. **Assess the risk:**- Determine the severity that each threat poses so that mitigation or avoidance strategies can be designed for improved safety and control over potential outcomes.
3. **Respond to the risk:**- Develop an action plan to reduce the impact of the overall risk on the organization's people and resources.
4. **Monitor the risk:**  
   - Continuous and consistent monitoring to prevent or mitigate potential losses.
5. **Threat identification:** - Identifying and analyzing any events that could negatively impact organizational assets, providing unique perspectives on threats and how to mitigate them.  
    - Main types of threats:

|  |  |  |
| --- | --- | --- |
|  | **Internal Threats** | **External Threats** |
| **Define** | Stem from the insides of any organization to exploit the system or implement damage. | This relates to malicious actors attempting to gain unauthorized access to the network of the targeted organization. |
| **Causes** | Due to the abuse of extended privileges given to trusted employees of organizations and the non-vigilant security practices. | Due to the system vulnerabilities to gain initial access. |
| **Examples** | * Mishandling data. * Inviting malware into the network by accessing malicious emails from websites. * Facilitating outside attacks by connecting infected USBs into the system. | * Social engineering. * Malware. * Hacking. |
| **Preventions** | * Encryption. * Use of action monitoring software. * Control internal access to sensitive data. | * Vulnerability scanning and patch management. * Cyber awareness training. * Endpoint Detection and Response. |

**N.B: The prevention of both internal and external threats can be applied to both.**

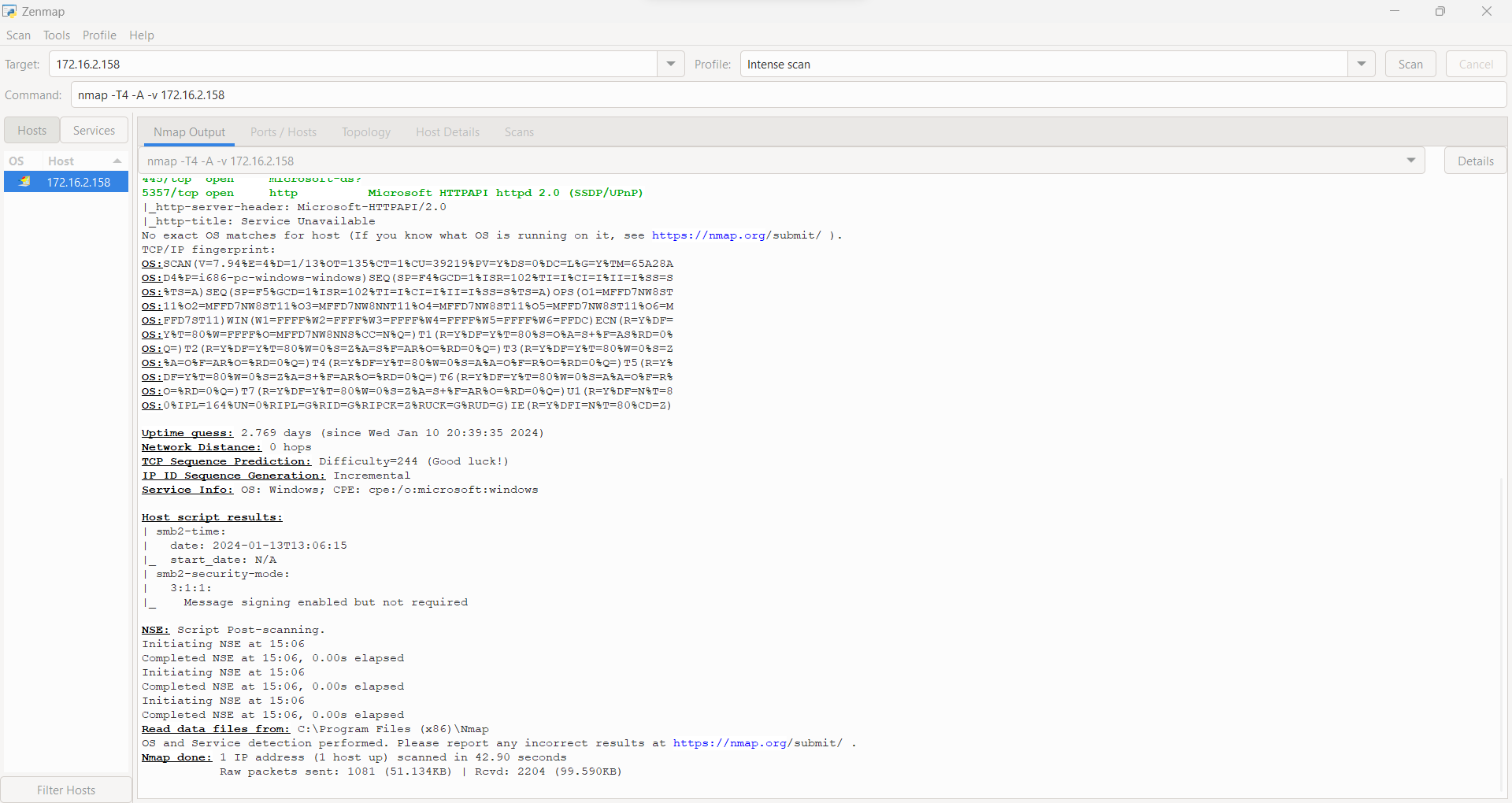
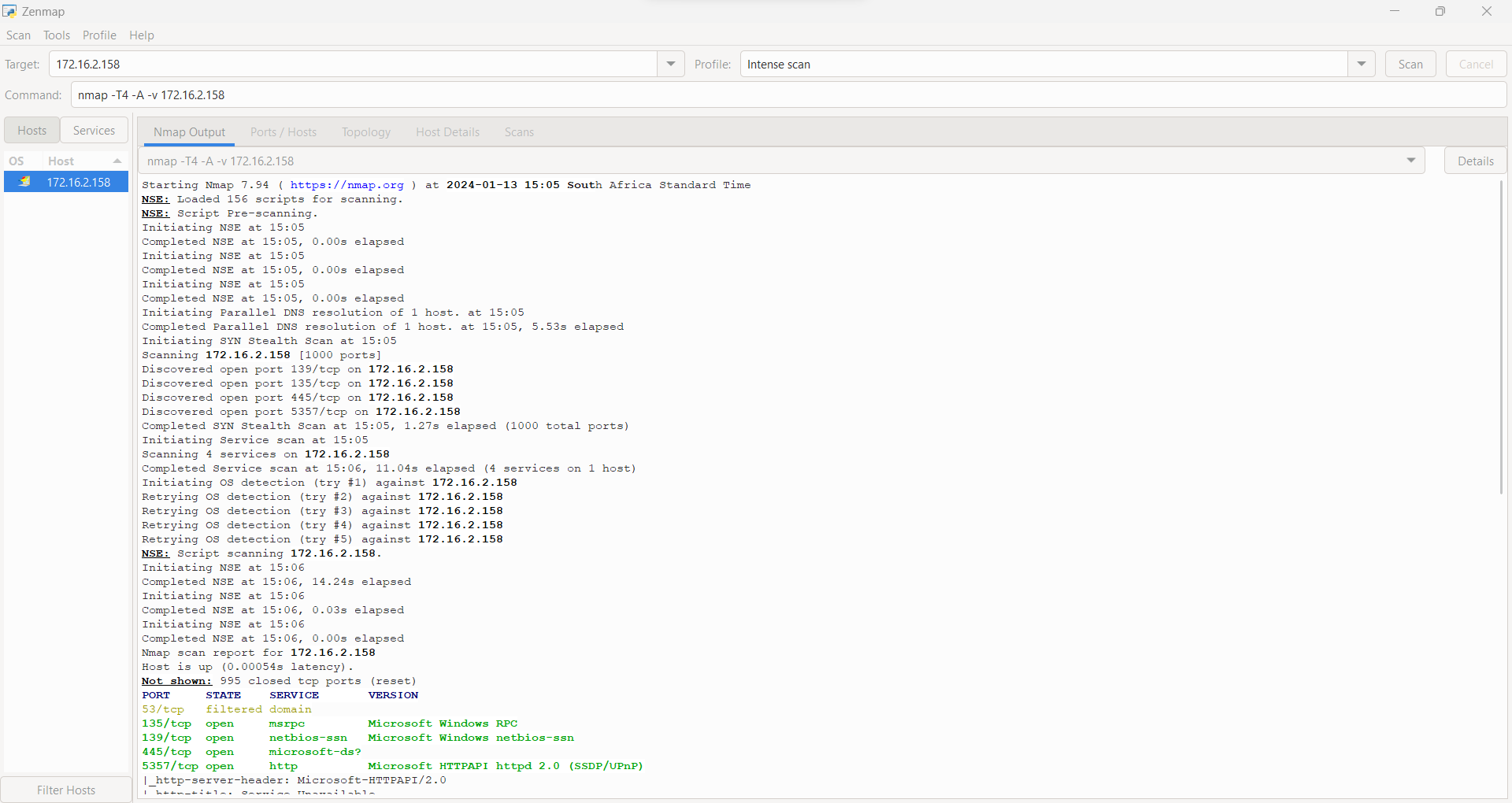
1. **Vulnerability scanning**  
   - The evaluation of systems, networks, or applications of assets for security weaknesses that can be exploited by internal or external actors.  
     
   - As a result, vulnerabilities can be detected early and addressed before they can be exploited, thereby ensuring compliance with regulations, reducing risk and cost, and improving security.

- Use of vulnerability scanning tools to discover hosts and services on a computer network by sending packets and analyzing the responses. Below are a few examples of tools used:

1. Acunetix
2. Nessus
3. Nmap
4. Burp Suite.

**N.B: It’s important to choose the right tool for the job based on the type and size of the system being scanned.**

**Vulnerability scan report:**



The scan above indicates:

1. **TCP**(**Transmission Control Protocol**) – a connection-oriented protocol that ensures reliable and ordered data delivery.
2. **Open state** – indicating ports or services that can be accessed by other network devices and therefore can be exploited.
3. **Port 135(msrpc):**

**Use:** Server Message Block(SMB)

**Risk:**

- Vulnerability to SMB attacks.  
- Lack of encryption.  
- Remote code execution.  
- Exposure to file and printing services.

**Mitigation:**

- Implement network segmentation  
- Firewall configuration  
- Enable encryption  
- Enforce authentication

1. **Port 139(netbios ssn):**

**Use:** Server Message Block(SMB)

**Risk:**

- Network-based attacks.

- Spread of malware.

- Potential exposure to unauthorized access.

**Mitigation:** - Regular Patching.

- Monitoring and Logging.

- Encryption

1. **Port 445(microsoft ds?):**

**Use:** Server Message Block(SMB)

**Risk:**  
 - Exposure to Data Theft

- Data Tampering

- Denial of Service(DoS)

**Mitigation:**  
 - Regular security audits

- Disable Unused Services

- Endpoint protection

1. **Port 5357(HTTP):**

**Use:** Network Discovery Protocols(WS-Discovery)

**Risk:**

- Information disclosure.

- Unauthorized access.

- Potential for Service Disruption

**Mitigation:**  
 - Network monitoring.

- Security Patching

- Firewall Configuration

1. **Filtered state** – indicating access to a port or service is blocked by a firewall and therefore can’t be exploited.
2. **Port 53(domain)**

**Use:** Domain Name System(DNS)

**Risk:**

- Distributed Denial of Service(DDoS)

- Information Disclosure

**Mitigation:**

- DNS firewall

- Access Control Lists(ACLs)

1. **Version** – provides information about the specific version of the service or application running on the identified ports.   
   This information is valuable for understanding potential vulnerabilities associated with specific software versions and determining appropriate security measures.
2. **Risk analysis:**  
   - The analysis entails examining each risk to the security of an organization’s systems, devices, and data and prioritizing the potential threats.

- It helps identify and analyze the potential impact that could adversely affect key business initiatives or projects.

- This process is performed to help organizations avoid or mitigate those risks.

The following are the objectives of the risk analysis:

1. **Risk probability:**  
   - Determine the occurrence of a threat or vulnerability.  
   - Helps organizations prioritize their resources and efforts in addressing the most probable and impactful security risks.
2. **Risk impact:**  
   - Determine the magnitude of the consequence of the occurrence of a risk on the organization.  
   - Helps in evaluating the potential implications on business operations.
3. **Risk exposure:**  
   - A combination of risk probability and risk impact.  
   - Gauges the potential extern of harm from security risks.  
   - Helps determine how best to allocate resources to minimize exposure effectively.

**Overall recommendation**

1. **Implement access controls**

- Multi-factor authentication.

- Review and update user access rights.

1. **Employee training and awareness**

- Educating employees about security best practices, phishing awareness, and social engineering tactics.

1. **Regular security assessments:**

- Vulnerability scanning.  
- Penetration testing.  
- Security audits.

1. **Data Backup and Recovery:**

- External hard drives or USB plates.  
- Cloud-based.

1. **Incident response plan:**

- Communication protocols.  
- Containment and eradication.  
- Recovery and post-incident analysis.

1. **Security Governance:**  
    - Implement playbooks.
2. **Continuous monitoring:**  
    - Logs (records of events that occur within an organization’s system).  
    - Endpoint Detections and Response(EDR).  
    - Security Information and Event Management(SIEM) products.
3. **Regular patch updates:**  
    - Frequent update and upgrade of software.