INTERN CAREER
"WE SPEAK DATA"

# CYBER SECURITY INTERNSHIP

# TASK 1:
# CYBER RISK ASSESSMENT

# ASSESSMENT OUTCOMES:

# IDENTIFICATION OF ASSETS, THREATS AND VULNERABILITIES:

01 Asset groups that are valuable to the business were identified

02 Potential threats for each asset group were identified.

03 The impact of the threats on the confidentiality, integrity and availability of each asset group were assessed.

# ASSET GROUPS IDENTIFIED AND IMPACT ON CIA:

## 1. **HARDWARE:**

**Impact on CIA:**
**(Confidentiality, Integrity and Availability)**

**Confidentiality:**
Data breaches/leaks due to unauthorized access.

**Integrity:**
Data corruption due to malware, Human error, Power outages or Insider sabotage.

**Availability:**
System down due to hardware failure, power outages or malware attacks

## 2. SOFTWARE:

**Impact on CIA:**
**(Confidentiality, Integrity and Availability)**

**Confidentiality:**
Data breaches/leaks due to unauthorized access or insider sabotage.

**Integrity:**
Data corruption due to malware, Human error, Power outages, Insider sabotage, software bugs and vulnerabilities.

**Availability:**
System down due to hardware failure, power outages, malware attacks, software bugs.

## 3.DATA:

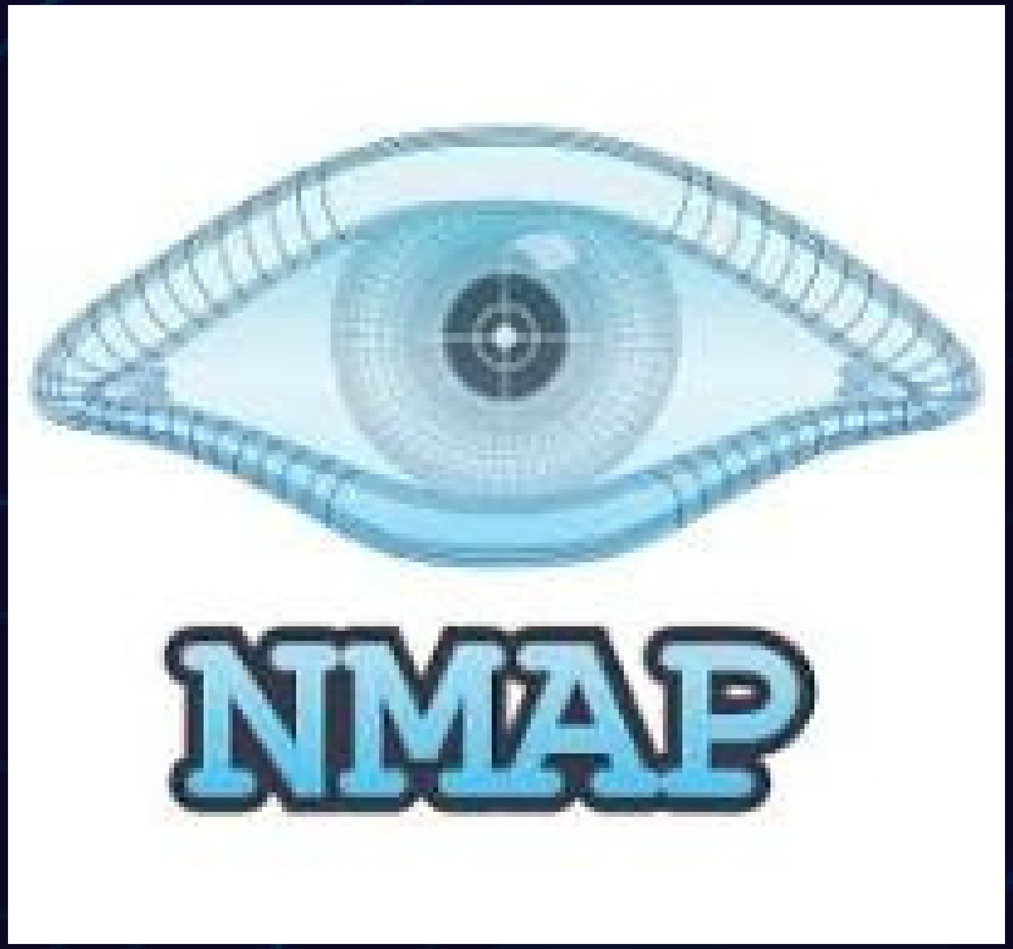
**Impact on CIA:**
**(Confidentiality, Integrity and Availability)**

**Confidentiality:**
**Data breaches/leaks due to unauthorized access or insider sabotage.**

**Integrity:**
Data corruption due to malicious attacks, Human error, Power outages, Hardware failure, Software bugs and vulnerabilities.

**Availability:**
System down due to hardware failure, power outages, malicious attacks, software bugs.

# TOOLS USED FOR VULNERABILITY SCANS:



# VULNERABILITIES AND THEIR POTENTIAL RISKS:

## 1.SMB Signing not required:

**Risk Classification: High**

**Likelihood of Exploitation: 4 Very Likely**

**Impact: 3 Moderate**

**Potential Risk:** An unauthenticated attacker could gain access to and change messages being transmitted without being detected. If signing was required and a message was changed SMB will know the data was tampered with. This compromises confidentiality and integrity of the system and organization.

First Priority

## 2. SSL Certificate Cannot Be Trusted:

**RiRisk Classification: Medium**

**Likelihood of Exploitation: 3 Likely**

**Impact: 3 Moderate**

**Potential Risk:**
This vulnerability can expose sensitive information to attackers. If the SSL certificate gets flagged as invalid by the browser, the data being transferred between the user and the website will be unencrypted thus allowing sensitive data communicated to be stolen. This could result in data breaches and possibly financial loss. This compromises the confidentiality and integrity of the system and organization. This could also lead to the availability of the system being compromised.

**Second Priority**

# PROPOSED MITIGATION STRATEGIES:

- Regularly update and patch software and systems
- Implement network segmentation
- Regularly conduct vulnerability assessments
- Implement Backup and recovery solutions
- Implement strict access control measures.
- Encrypt data before transmission and during transmission .

Studio Shodwe

Home Service About Us Contact

# THANK YOU