INTERN CAREER
"WE SPEAK DATA"

# Cybersecurity Internship:

# Task 1: Risk Assesment

By Yasmeen Seedat

# Cybersecurity Risk Assessment

## Introduction:

Cybersecurity risk assessment is a critical process used by organizations to identify, analyze, and evaluate risks associated with their information technology and cybersecurity environments. The aim is to understand the potential threats to their IT assets (including data, hardware, software, and networks) and the vulnerabilities that could be exploited by those threats.

**Steps involved in a cybersecurity risk assessment:**

1.Threat Identification:
1.1. Asset Identification:
1.2. Threats  Identification for assets
2. Vulnerability scanning and Identification
3. Risk Analysis
4. Mitigation Strategies

## System Setup for assessment

The system to be assessed comprises of the following types of software:

- **Network monitoring tools:**These tools help track network performance and security.

- **Vulnerability scanning tools:** These tools help identify security weaknesses in networks, systems and applications.

- **Penetration testing tools:** These tools simulate cyber attacks to identify weaknesses,determine potential impact of cyber attacks and test effectiveness of security measures.

- **Firewall and Intrusion detection systems:** Firewalls act as barriers between internal and untrusted external networks. IDS  monitors network traffic to determine potential threats.

- **Data Loss Prevention tools:** These tools prevent unauthorized access to sensitive data and prevent sensitive data from leaving or being transmitted outside the organization’s network.

# 1. Threat Identification:

Identifying threats and vulnerabilities is an important part of the risk assessment process and is crucial to understanding how to prevent a system  from being comprised

## 1.1.  Asset Identification:

Assets of the business need to be identified to understand what is valuable to the business and what impact a threat to each asset would have on the business.

**Asset Groups Identified:**

1. **Hardware:** (Example :Server, Desktop computers,etc.)
2. **Software**: (Example: CRM,Security software and tools, etc)
3. **Data:** (Example: Customer Data, Employees records, Business activities , etc)

## 1.2.Threats to Asset Groups:

### 1.Hardware:

**Value:** High. Critical for business operations**.**

**Threat Sources:**

- ***Naturel*** (Natural disasters)
- ***Human*** (malicious and accidental)
- ***Technical*** (e.g. Hardware failures, software bugs)
- ***Environmental*** (e.g. power outages, pollution)

**Threat Types:**

- Malicious attacks: e.g. hacking, malware, phishing, insider sabotage, theft.
- Poor security practices
- natural disasters
- Hardware failure
- Software bugs
- Power Outage

**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:

**Value:** High. Critical for business operations**.**

**Threat Sources:**

- ***Human*** (malicious and accidental)
- ***Technical*** (e.g. Hardware failures, software bugs)
- ***Environmental*** (e.g. power outages, pollution)

**Threat Types:**

- Malicious attacks: e.g. hacking, malware, phishing, insider sabotage, Denial of service.

- Poor security practices

- Software bugs and vulnerabilities
- Power outages

**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:

**Value:** High. Critical for business operations**.**

**Threat Sources:**

- ***Human*** (malicious and accidental)
- ***Technical*** (e.g. Hardware failures, software bugs)
- ***Environmental*** (e.g. power outages, pollution)

**Threat Types:**

- Malicious attacks: e.g. hacking, malware, phishing, insider sabotage, Denial of service.
- Data entry errors
- Accidental deletion
- Poor security practices
- Software bugs and vulnerabilities
- Power outages

**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.

## Examples of Potential  Vullnerabilities:

- Lack of physical security
- Inadequate security software, configurations and tools
- Outdated software or drivers
- Existence of software bugs
- Unpatched software
- Weak authentication: e.g. weak passwords
- Employees not trained in cyber awareness

## 2. Vulnerability Scanning:

Vulnerability scans are used to identify security weaknesses and flaws in systems .

**Tools used:**

- Nmap
- Nessus
- Wireshark

## 1.Nmap:

Nmap is a network scanning tool used for network mapping, vulnerability assessment and network security auditing.

**Nmap scan results:**

nmap scan report for system ip address
Host is up (0.0015s latency).
Not shown: 8055 closed tcp ports (reset)

| PORT | STATE | SERVICE | VERSION |
|---|---|---|---|
| 135/tcp | open | msrpc | Microsoft Windows RPC |
| 137/tcp | filtered | netbios-ns | |
| 139/tcp | open | netbios-ssn | Microsoft Windows netbios-ssn |
| 445/tcp | open | microsoft-ds? | |
| 5040/tcp | open | unknown | |

An open state means that there is a service listening on that port, and it is not blocked by a firewall. Filtered means that there is something blocking connections to that port like a firewall.

- Port 135 is open for msrpc and the version is Microsoft Windows RPC.
- Port 137 is filtered for netbios-ns.
- Port 139 is open for netbios-ssn and the version is Microsoft Windows netbios-ssn.
- Port 445 is open for microsoft-ds.
- Port 5040 is open for an unknown service.

## 2.Nessus:

Nessus is a remote vulnerability scanning tool used to discover any vulnerabilities in systems.

**Vulnerabilities found:**

### 1.SMB Signing not required:

**Severity:** **Medium**

(CVSS v3.0 Base Score 5.3)

**Description:**
Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server

### 2. SSL Certificate Cannot Be Trusted:

**Severity:** **Medium**

**(**CVSS v3.0 Base Score 6.5)

**Description**
The server's X.509 certificate cannot be trusted. This could make it easier to carry out man-in-the-middle attacks against the remote host.

### 3.Wireshark:

Wireshark is a packet analyser used for network troubleshooting. It is used to trace connections, view the contents of suspect network transactions and identify bursts of network traffic.

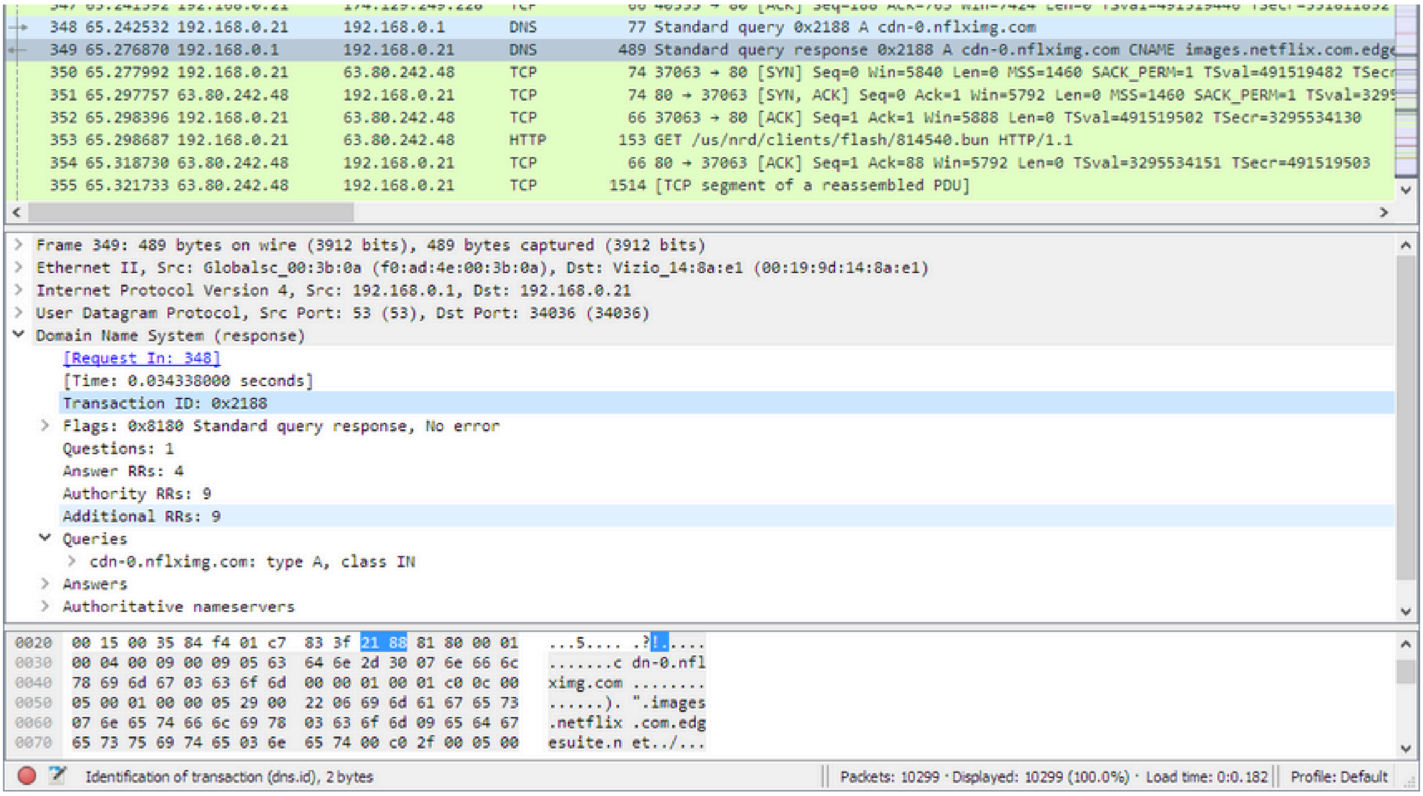
**Wireshark can help with:**

- **Network Troubleshooting:** Wireshark allows network administrators to capture and inspect individual packets to identify issues with network traffic or behavior.

- **Security Analysis:** By examining the data packets flowing through the network, Wireshark can help identify suspicious activities, such as potential network intrusions.

- **Network Performance Analysis:** Wireshark can analyze traffic patterns over time, helping administrators understand usage trends and optimize network performance accordingly.

## Scan Example:



```
348 65.242532 192.168.0.21   192.168.0.1    DNS    77 Standard query 0x2188 A cdn-0.nflximg.com
349 65.276870 192.168.0.1    192.168.0.21   DNS   489 Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge
350 65.277992 192.168.0.21   63.80.242.48   TCP    74 37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr
351 65.297757 63.80.242.48   192.168.0.21   TCP    74 80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295
352 65.298396 192.168.0.21   63.80.242.48   TCP    66 37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
353 65.298687 192.168.0.21   63.80.242.48   HTTP  153 GET /us/nrd/clients/flash/814540.bun HTTP/1.1
354 65.318730 63.80.242.48   192.168.0.21   TCP    66 80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
355 65.321733 63.80.242.48   192.168.0.21   TCP  1514 [TCP segment of a reassembled PDU]
```

```
> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
> Ethernet II, Src: Globalsc_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)
v Domain Name System (response)
    [Request In: 348]
    [Time: 0.034338000 seconds]
    Transaction ID: 0x2188
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 9
    Additional RRs: 9
  v Queries
    > cdn-0.nflximg.com: type A, class IN
  > Answers
  > Authoritative nameservers
```

```
0020  00 15 00 35 84 f4 01 c7  83 3f 21 88 81 80 00 01   ...5.... .?!.....
0030  00 04 00 09 00 09 05 63  64 6e 2d 30 07 6e 66 6c   .......c dn-0.nfl
0040  78 69 6d 67 03 63 6f 6d  00 00 01 00 01 c0 0c 00   ximg.com ........
0050  05 00 01 00 00 05 29 00  22 06 69 6d 61 67 65 73   ......). ".images
0060  07 6e 65 74 66 6c 69 78  03 63 6f 6d 09 65 64 67   .netflix .com.edg
0070  65 73 75 69 74 65 03 6e  65 74 00 c0 2f 00 05 00   esuite.n et../...
```

Identification of transaction (dns.id), 2 bytes | Packets: 10299 · Displayed: 10299 (100.0%) · Load time: 0:0.182 | Profile: Default

**IP Section:** Includes source and destination IP Addresses and port numbers

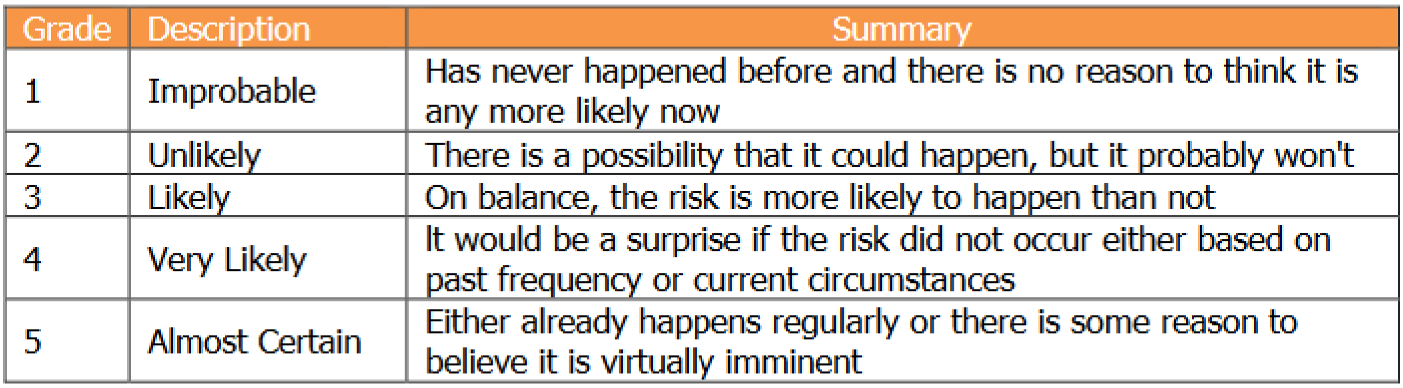
**User Diagram Protocol:** This is the transport section. It includes transport layer information

**Domain Name System (response)**: This is the application section. This includes the application layer information.

# 3.Risk Analysis:

Risk analysis helps organizations understand the potential impacts of various risks and allows them to make informed decisions on how to address these risks.

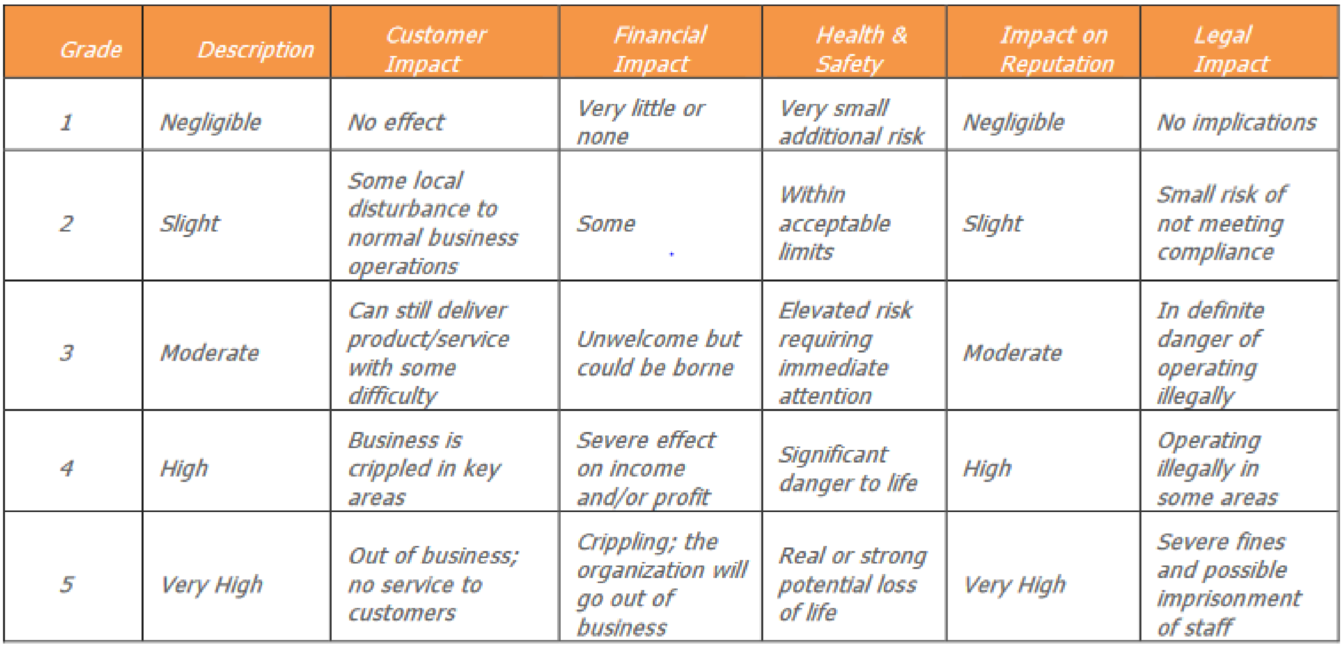
**The following table was used to assess the likelihood of exploitation of each risk:**



| Grade | Description | Summary |
|---|---|---|
| 1 | Improbable | Has never happened before and there is no reason to think it is any more likely now |
| 2 | Unlikely | There is a possibility that it could happen, but it probably won't |
| 3 | Likely | On balance, the risk is more likely to happen than not |
| 4 | Very Likely | It would be a surprise if the risk did not occur either based on past frequency or current circumstances |
| 5 | Almost Certain | Either already happens regularly or there is some reason to believe it is virtually imminent |

*Table 1: Risk Likelihood Guidance*

**The following table was used to assess the impact of each risk: :**



| *Grade* | *Description* | *Customer Impact* | *Financial Impact* | *Health & Safety* | *Impact on Reputation* | *Legal Impact* |
|---|---|---|---|---|---|---|
| *1* | *Negligible* | *No effect* | *Very little or none* | *Very small additional risk* | *Negligible* | *No implications* |
| *2* | *Slight* | *Some local disturbance to normal business operations* | *Some* | *Within acceptable limits* | *Slight* | *Small risk of not meeting compliance* |
| *3* | *Moderate* | *Can still deliver product/service with some difficulty* | *Unwelcome but could be borne* | *Elevated risk requiring immediate attention* | *Moderate* | *In definite danger of operating illegally* |
| *4* | *High* | *Business is crippled in key areas* | *Severe effect on income and/or profit* | *Significant danger to life* | *High* | *Operating illegally in some areas* |
| *5* | *Very High* | *Out of business; no service to customers* | *Crippling; the organization will go out of business* | *Real or strong potential loss of life* | *Very High* | *Severe fines and possible imprisonment of staff* |

*Table 2: Risk Impact Guidance*

## Risk Classification:

Risk score = Likelihood x Impact

This risk score is used to determine risk classification as outlined below:

- **High**: 12 or more
- **Medium**: 5 to 10 inclusive
- **Low**: 1 to 4 inclusive

## 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.

### 2. SSL Certificate Cannot Be Trusted:

**Risk 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.

Based on the risk classification the first vulnerability should be the highest priority. This has a high likelihood of being exploited and poses a great risk to the system and organization. The next priority should be the second vulnerability. This also poses a great risk to the system and organization and is likely to be exploited.

## 4. Mitigation Strategies for High Risk Vulnerabilities:

All these mitigation strategies can be applied to the high risk SMB vulnerability identified. To solve this vulnerability the message signing in the host's configuration needs to be enforced.

- Regularly update systems, and software. Security patches should also be regularly applied to systems and software. This helps address known vulnerabilities.

- Separate critical assets into different network zones to limit the spread of an attack if vulnerabilities are exploited.

- Regularly conduct vulnerability assessments to identify and address new vulnerabilities.

- Implement a backup and recovery solution so if data were to be lost or the system were to be exploited, the system could be recovered.

- Implement strict access control measures to ensure there’s no one who can access data or information that they are not authorized to access.

- Encrypt sensitive data before transmission and during transmission.This helps mitigate the impact of data breaches.

## Recommendations to address identified risks:

- Implement Technology controls such as firewalls and monitoring and detection tools like Intrusion detection systems.

- Educate employees and stakeholders on their roles in risk management, focusing on areas like cybersecurity, safety, and quality control.

- Regularly conduct security assessments like penetration tests, vulnerability scans and security audits to identify and address new vulnerabilities and threats to the system.

- Conduct incident response simulation exercises to train and prepare the incident response team for potential exploits or attacks. Implement an incident response plan.

# Summary of Risk Assessment:

During the risk assessment we identified and evaluated potential threats and vulnerabilities to the system. The risks were analyzed and evaluated based on their impact and likelihood.

## Assessment outcomes:

- Identified Assets, threats and vulnerabilities of the system and organization.
- Evaluated the vulnerabilities based on their potential risks
- Analyzed the risks based on their impact, likelihood and risk classification
- Prioritized risks based on their risk classification.
- Mitigation strategies suggested

## Proposed 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 .

# Report prepared by:

**Name:** Yasmeen Seedat | Cyber Security Intern

**Intern Email:** yseedat57@gmail.com

**Intern LinkedIn :** Yasmeen Seedat