INTERN CAREER

"WE SPEAK DATA"

Cyber Security Internship

Task 1: Cybersecurity Risk Assessment

Topics To Be Covered

1. **Introduction to Cybersecurity Risk Assessment**
2. **Threat Identification**
3. **Vulnerability Scanning**
4. **Risk Analysis**
5. **Mitigation Strategies**
6. **Recommendations**
7. **Comprehensive Report Overview**
8. **summarizing the assessment outcomes**

❖Introduction to Cybersecurity Risk Assessment

Cybersecurity Risk Assessment is the process of identifying and evaluating potential risks to an organization's information systems and data. It helps in understanding the vulnerabilities and threats that could compromise the **confidentiality**, **integrity**, and **availability** of sensitive information. By conducting a risk assessment, organizations can prioritize their security efforts and implement appropriate safeguards to mitigate the identified risks. It's a crucial step in building a strong cybersecurity posture.

Some common vulnerabilities in information systems include

- **Weak Passwords**
- **Outdated Software**
- **Lack of Encryption**
- **Insecure Network Configurations**
- **Inadequate Access Controls**.

These vulnerabilities can leave systems susceptible to attacks such as

- **Unauthorized Access**
- **Data Breaches**
- **Malware Infections**
- **Denial of Service Attacks**

❖ Threat Identification

In cybersecurity risk assessment, threat identification involves identifying potential risks and threats to the security of an organization's systems and data. This process includes analyzing various sources such as known vulnerabilities, external threats, and internal risks. By identifying these threats, organizations can develop strategies to mitigate and manage them effectively.

To identify the threats present in the network, a system setup should be required.

System Setup: following equipments & Tool in Network Architecture

1. Network and system monitoring tools: These tools help to monitor network traffic, detect anomalies, and identify potential security breaches.

2. Vulnerability scanning tools: These tools scan the systems and networks for known vulnerabilities, allowing us to address them before they can be exploited.

3. Penetration testing tools: These tools simulate real-world attacks to identify weaknesses in systems and test their resilience.

4. Security information and event management (SIEM) system: This system collects and analyzes logs from various sources to identify security incidents and provide real-time threat intelligence.

5. Data loss prevention (DLP) tools: These tools help prevent the unauthorized disclosure of sensitive data by monitoring and controlling data transfers.

6. Firewall and intrusion detection/prevention systems (IDS/IPS): These devices protect the network by filtering incoming and outgoing traffic and detecting potential intrusions.

7. Secure configuration management tools: These tools ensure that the systems and devices are configured securely and follow best practices.

Identity potential threats and vulnerabilities within the system.

In a cybersecurity risk assessment, it's important to identify threats and vulnerabilities within the system. Here are some examples:

1. Malware: This includes viruses, ransomware, and other malicious software that can infect the system and compromise data or disrupt operations.

2. Phishing attacks: These are attempts to trick users into revealing sensitive information through deceptive emails, messages, or websites.

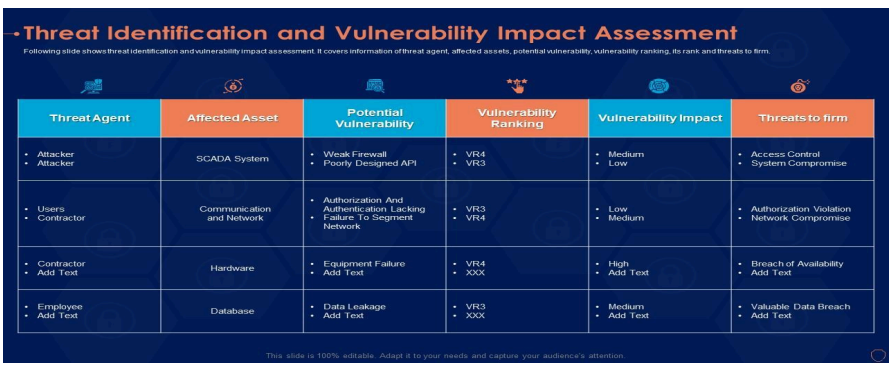
3. Weak authentication: Inadequate password policies or the absence of multi-factor authentication can make it easier for unauthorized individuals to gain access to the system.

4. Unpatched software: Failing to apply software updates and patches can leave the system vulnerable to known security vulnerabilities.

5. Insider threats: This refers to the risk posed by employees or individuals with privileged access who may intentionally or unintentionally misuse or disclose sensitive information.

6. Physical security risks: Poor physical security measures can lead to theft, unauthorized access, or damage to hardware and data.

7. Data breaches: Unauthorized access or disclosure of sensitive data, either through external attacks or insider actions, can result in significant harm to the organization.



Threat Identification and Vulnerability Impact Assessment

Following slide shows threat identification and vulnerability impact assessment. It covers information of threat agent, affected assets, potential vulnerability, vulnerability ranking, its rank and threats to firm.

Threat Agent	Affected Asset	Potential Vulnerability	Vulnerability Ranking	Vulnerability Impact	Threats to firm
• Attacker • Attacker	SCADA System	• Weak Firewall • Poorly Designed API	• VR4 • VR3	• Medium • Low	• Access Control • System Compromise
• Users • Contractor	Communication and Network	• Authorization And Authentication Lacking • Failure To Segment Network	• VR3 • VR4	• Low • Medium	• Authorization Violation • Network Compromise
• Contractor • Add Text	Hardware	• Equipment Failure • Add Text	• VR4 • XXX	• High • Add Text	• Breach of Availability • Add Text
• Employee • Add Text	Database	• Data Leakage • Add Text	• VR3 • XXX	• Medium • Add Text	• Valuable Data Breach • Add Text

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

❖ Vulnerability Scanning

In cybersecurity risk assessment, vulnerability scanning is a crucial step to identify potential weaknesses and vulnerabilities in an organization's systems, networks, and applications. It involves using specialized tools to scan & analyze the infrastructure. By conducting regular vulnerability scans, organizations can proactively identify & mitigate potential risks, enhancing their overall cybersecurity posture.

Nmap, Nessus, and Wireshark are commonly used cybersecurity tools for conducting vulnerability scans in risk assessments.

- **Nmap: Essential for network mapping and security auditing.**
- **Nessus: Effective for vulnerability scanning and assessments.**
- **Wireshark: Useful for network protocol analysis and troubleshooting.**

Brief Overview of each Tool

1. Nmap (Network Mapper): It's a powerful network scanning tool that helps identify open ports, services, and potential vulnerabilities on a network. Nmap's scanning tool provides detailed information about the network, including open ports, services running on those ports, and potential vulnerabilities. It helps in identifying potential entry points for attackers and allows for proactive security measures to be taken.

➔ **Detailed Breakdown of Nmap Scanning Tool Result**

Nmap is a versatile tool that can detect various services running on different ports. Some common services that Nmap can detect include:

- FTP (File Transfer Protocol) on port 21
- Telnet on port 23
- SMTP (Simple Mail Transfer Protocol) on port 25
- DNS (Domain Name System) on port 53
- SNMP (Simple Network Management Protocol) on port 161
- MySQL on port 3306
- PostgreSQL on port 5432
- RDP (Remote Desktop Protocol) on port 3389

Nmap Scan report for port no 192.168.1.1

Host is up (0.043s latency).

Not shown: 998 closed ports

PORT	STATE	SERVICE	VERSION
22/tcp	Open	SSH	OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp	Open	HTTP	Apache httpd 2.4.29 (Ubuntu)
443/tcp	Open	HTTPS	Apache httpd 2.4.29 (Ubuntu)
3389/tcp	Open	RDP	Microsoft Terminal Services

In this example, the Nmap scan was performed on the IP Address **192.168.1.1**. The scan revealed the following information about the open ports:

- Port 22 is open for SSH (Secure Shell) and the detected version is OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
- Port 80 is open for HTTP (Hypertext Transfer Protocol) and it's running Apache httpd 2.4.29 on Ubuntu
- Port 443 is open for HTTPS (HTTP Secure) and it's also running Apache httpd 2.4.29 on Ubuntu
- Port 3389 is open for RDP (Remote Desktop Protocol), indicating the presence of Microsoft Terminal Services.
- Nmap also discovered 998 closed ports that are not accessible.

```
Initiating Ping Scan at 08:10
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 08:10, 0.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:10
Completed Parallel DNS resolution of 1 host. at 08:10, 0.05s elapsed
Initiating SYN Stealth Scan at 08:10
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 80/tcp on 45.33.32.156
Increasing send delay for 45.33.32.156 from 0 to 5 due to 13 out of 41 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 5 to 10 due to 11 out of 29 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 10 to 20 due to 17 out of 56 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 20 to 40 due to 11 out of 28 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 40 to 80 due to max_successful_tryno increase to 4
Increasing send delay for 45.33.32.156 from 80 to 160 due to 11 out of 27 dropped probes since last increase.
Increasing send delay for 45.33.32.156 from 160 to 320 due to 11 out of 22 dropped probes since last increase.
SYN Stealth Scan Timing: About 16.13% done; ETC: 08:13 (0:02:41 remaining)
SYN Stealth Scan Timing: About 25.53% done; ETC: 08:14 (0:02:58 remaining)
Discovered open port 31337/tcp on 45.33.32.156
SYN Stealth Scan Timing: About 39.62% done; ETC: 08:15 (0:02:42 remaining)
SYN Stealth Scan Timing: About 48.93% done; ETC: 08:15 (0:02:22 remaining)
SYN Stealth Scan Timing: About 58.32% done; ETC: 08:15 (0:01:59 remaining)
SYN Stealth Scan Timing: About 67.72% done; ETC: 08:15 (0:01:33 remaining)
Discovered open port 9929/tcp on 45.33.32.156
```

```
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.073s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
PORT     STATE    SERVICE
21/tcp   closed   ftp
22/tcp   open     ssh
23/tcp   closed   telnet
25/tcp   filtered smtp
80/tcp   open     http
110/tcp  closed   pop3
139/tcp  closed   netbios-ssn
443/tcp  closed   https
445/tcp  closed   microsoft-ds
3389/tcp closed   ms-wbt-server
```

2. Nessus: This is a comprehensive vulnerability scanning tool that scans systems for known vulnerabilities. It can identify weaknesses in software configurations, missing patches, and other security issues.

➔ **Detailed Breakdown of Nessus Scanning Tool Result**

1. Vulnerability: CVE-2020-1234

Description: This vulnerability allows remote attackers to execute arbitrary code.

Severity: Critical

Solution: Apply the recommended patch or update the affected software.

2. Vulnerability: CVE-2019-5678

Description: This vulnerability exposes sensitive information to unauthorized users.

Severity: High

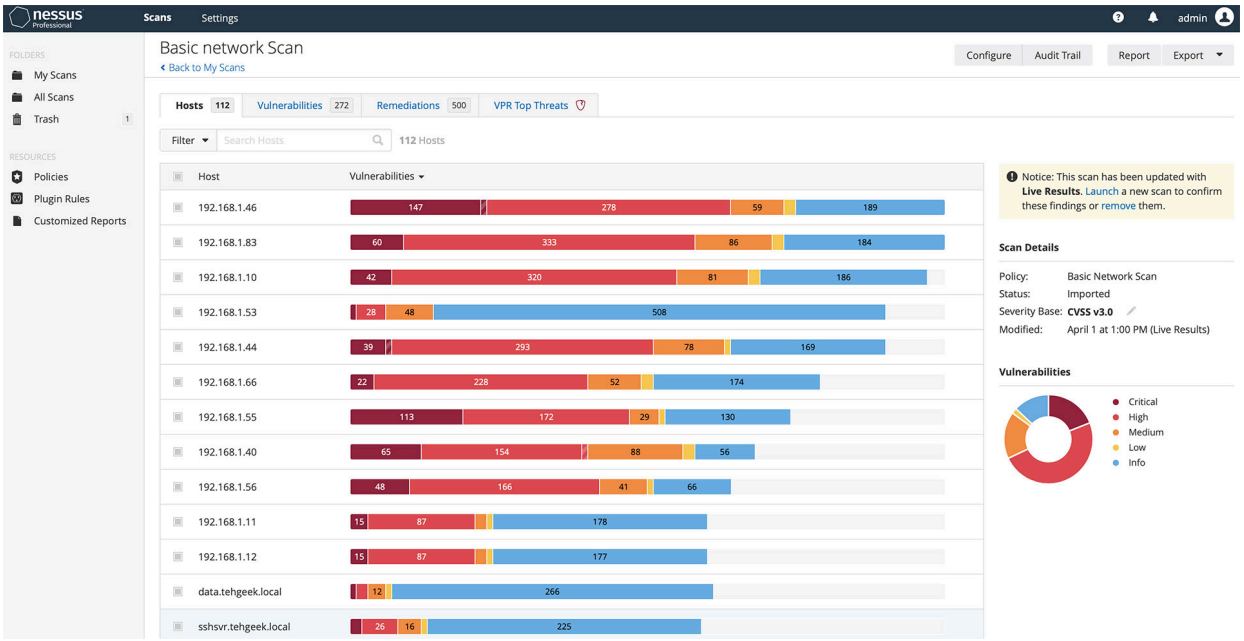
Solution: Implement access controls or apply the recommended fix.

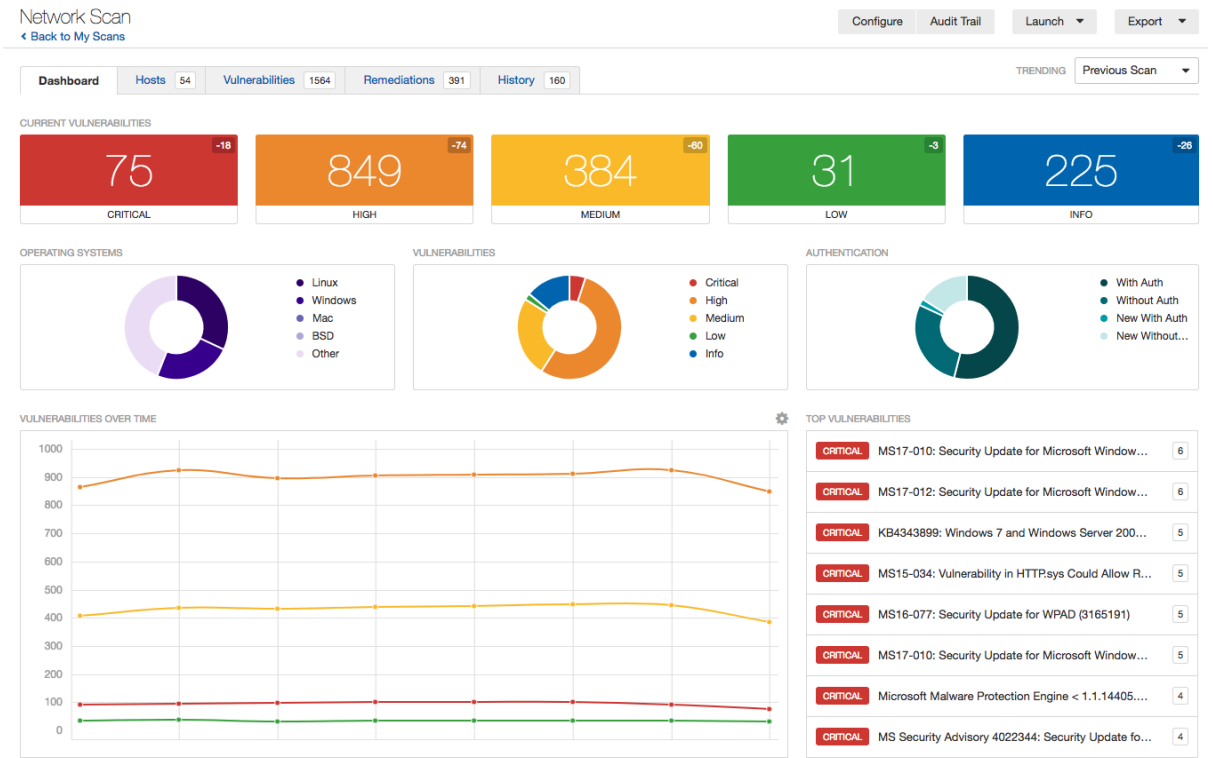
3. Vulnerability: CVE-2018-4321

Description: This vulnerability allows remote attackers to bypass authentication.

Severity: Medium

Solution: Update the affected software or implement additional security measures.





3. Wireshark: It's a network protocol analyzer that captures and analyzes network traffic in real-time. Wireshark can be used to detect and investigate potential security threats, such as suspicious network activity, unauthorized access attempts, or data breaches.

➔ Detailed Breakdown of Wireshark Scanning Tool Result

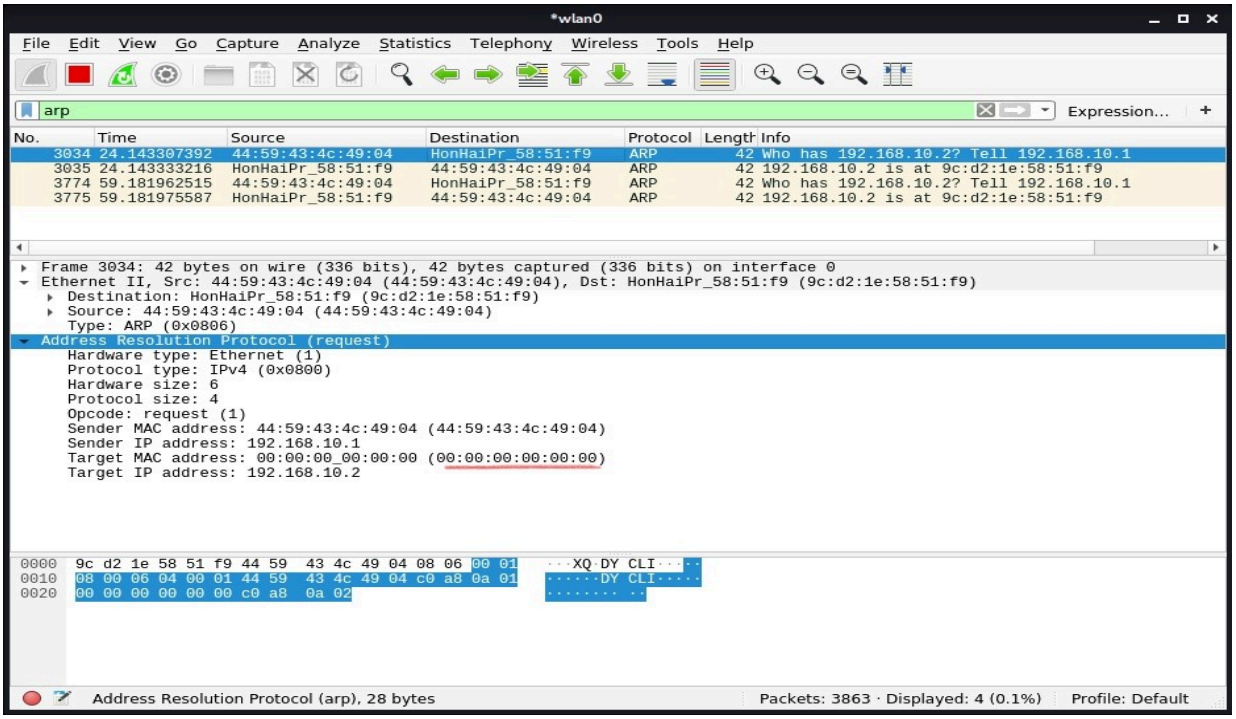
In cybersecurity risk assessment, wireshark can provide valuable insights into network traffic and potential security risks.

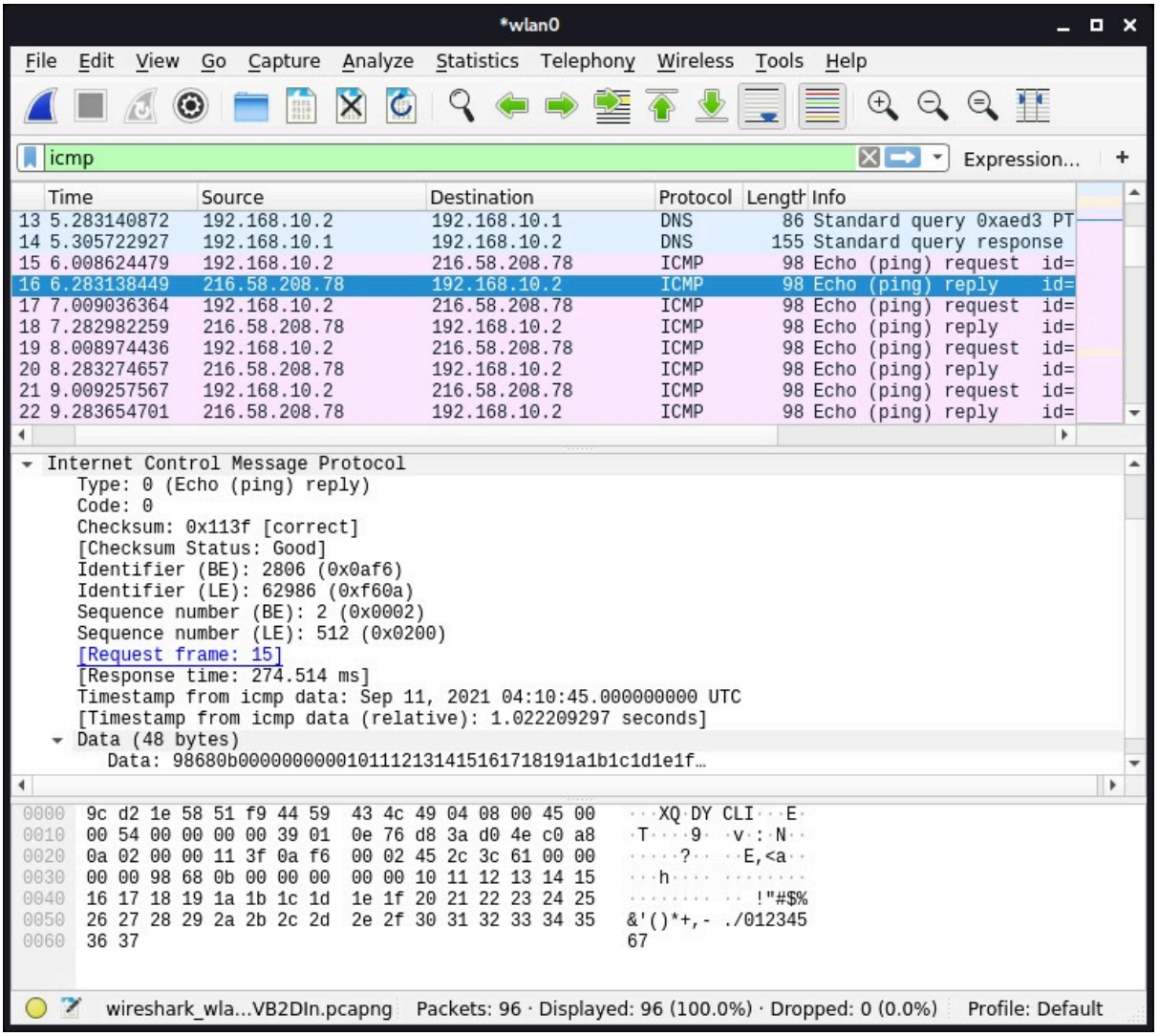
1. Network Traffic Analysis: Wireshark captures and analyzes network packets, allowing you to examine the flow of data, identify suspicious or unauthorized activities, and detect any signs of malicious behavior.

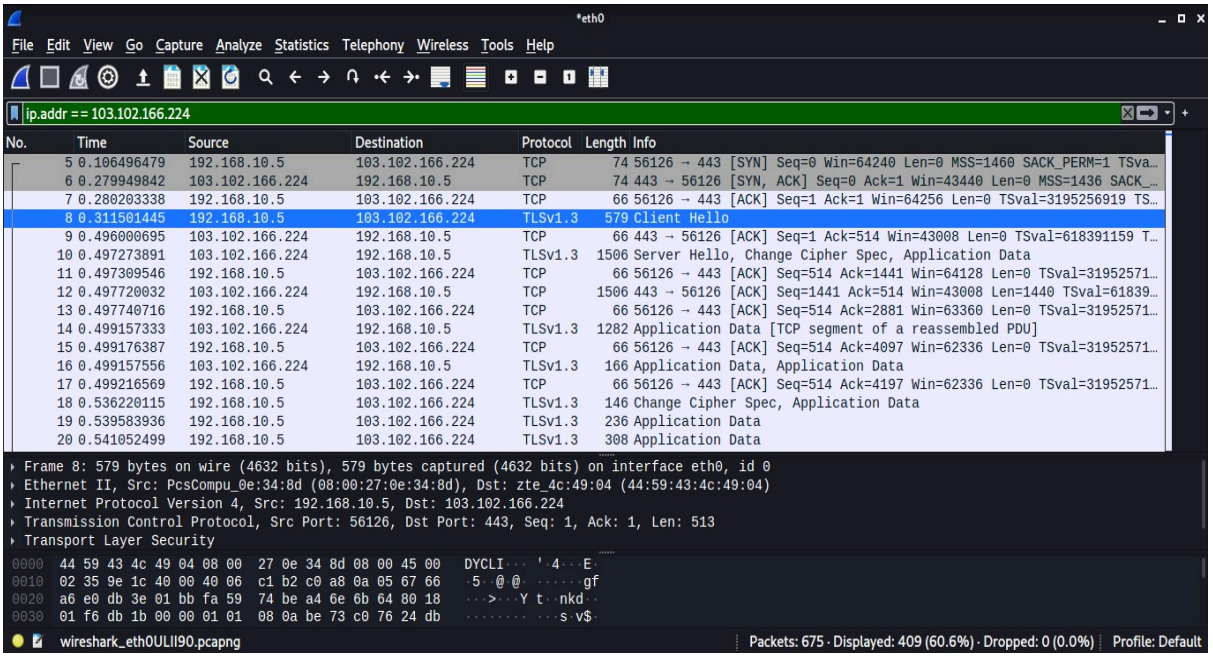
2. Protocol Vulnerabilities: Wireshark can help identify vulnerabilities in network protocols by analyzing packet headers and payloads. It can flag any abnormalities or potential weaknesses that could be exploited by attackers.

3. Unauthorized Access: By examining network traffic, Wireshark can help detect unauthorized access attempts, such as brute-force attacks, password sniffing, or unauthorized connections to sensitive systems.

4. Malware Detection: Wireshark can assist in identifying network traffic patterns associated with malware infections. It may reveal unusual communication patterns, suspicious domains, or malicious payloads

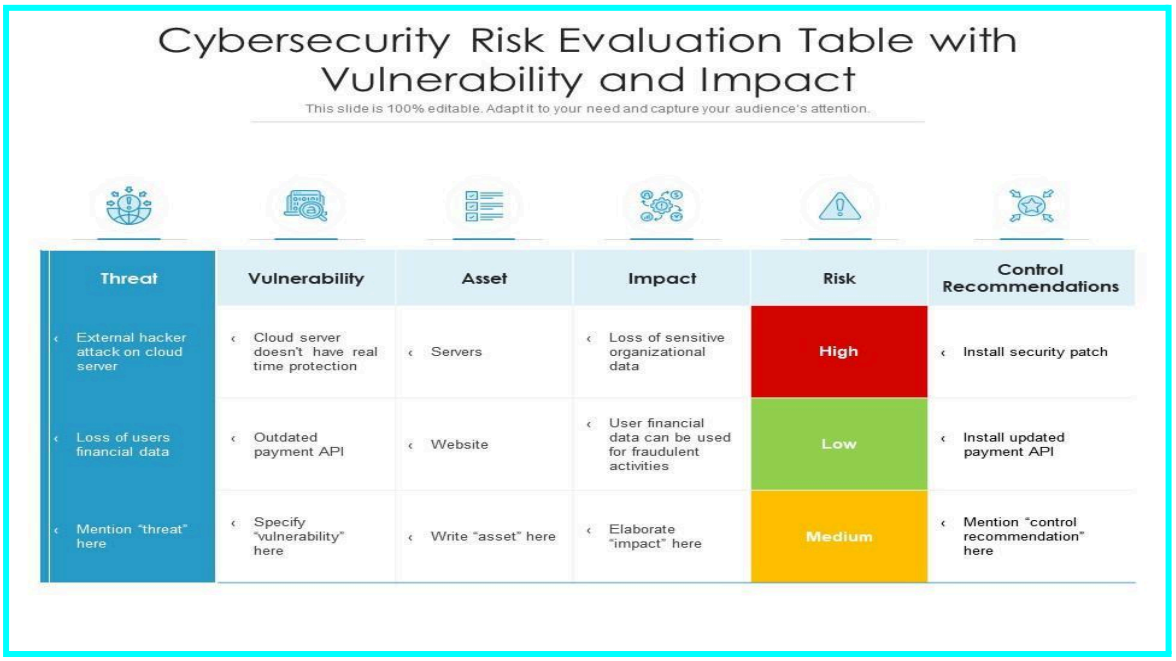



*wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
Expression...
No. Time Source Destination Protocol Length Info
13 5.283140872 192.168.10.2 192.168.10.1 DNS 86 Standard query 0xaed3 PT
14 5.305722927 192.168.10.1 192.168.10.2 DNS 155 Standard query response
15 6.008624479 192.168.10.2 216.58.208.78 ICMP 98 Echo (ping) request id=
16 6.283138449 216.58.208.78 192.168.10.2 ICMP 98 Echo (ping) reply id=
17 7.009036364 192.168.10.2 216.58.208.78 ICMP 98 Echo (ping) request id=
18 7.282982259 216.58.208.78 192.168.10.2 ICMP 98 Echo (ping) reply id=
19 8.008974436 192.168.10.2 216.58.208.78 ICMP 98 Echo (ping) request id=
20 8.283274657 216.58.208.78 192.168.10.2 ICMP 98 Echo (ping) reply id=
21 9.009257567 192.168.10.2 216.58.208.78 ICMP 98 Echo (ping) request id=
22 9.283654701 216.58.208.78 192.168.10.2 ICMP 98 Echo (ping) reply id=
Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0x113f [correct]
[Checksum Status: Good]
Identifier (BE): 2806 (0x0af6)
Identifier (LE): 62986 (0xf60a)
Sequence number (BE): 2 (0x0002)
Sequence number (LE): 512 (0x0200)
[Request frame: 15]
[Response time: 274.514 ms]
Timestamp from icmp data: Sep 11, 2021 04:10:45.000000000 UTC
[Timestamp from icmp data (relative): 1.022209297 seconds]
Data (48 bytes)
Data: 98680b0000000000101112131415161718191a1b1c1d1e1f…
0000 9c d2 1e 58 51 f9 44 59 43 4c 49 04 08 00 45 00
0010 00 54 00 00 00 00 39 01 0e 76 d8 3a d0 4e c0 a8
0020 0a 02 00 00 11 3f 0a f6 00 02 45 2c 3c 61 00 00
0030 00 00 98 68 0b 00 00 00 00 00 10 11 12 13 14 15
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35
0060 36 37
wireshark_wla...VB2DIn.pcapng Packets: 96 · Displayed: 96 (100.0%) · Dropped: 0 (0.0%) Profile: Default


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 103.102.166.224
No. Time Source Destination Protocol Length Info
5 0.106496479 192.168.10.5 103.102.166.224 TCP 74 56126 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSva…
6 0.279949842 103.102.166.224 192.168.10.5 TCP 74 443 → 56126 [SYN, ACK] Seq=0 Ack=1 Win=43440 Len=0 MSS=1436 SACK_…
7 0.280203338 192.168.10.5 103.102.166.224 TCP 66 56126 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3195256919 TS…
8 0.311501445 192.168.10.5 103.102.166.224 TLSv1.3 579 Client Hello
9 0.496000695 103.102.166.224 192.168.10.5 TCP 66 443 → 56126 [ACK] Seq=1 Ack=514 Win=43008 Len=0 TSval=618391159 T…
10 0.497273891 103.102.166.224 192.168.10.5 TLSv1.3 1506 Server Hello, Change Cipher Spec, Application Data
11 0.497309546 192.168.10.5 103.102.166.224 TCP 66 56126 → 443 [ACK] Seq=514 Ack=1441 Win=64128 Len=0 TSval=31952571…
12 0.497720032 103.102.166.224 192.168.10.5 TCP 1506 443 → 56126 [ACK] Seq=1441 Ack=514 Win=43008 Len=1440 TSval=61839…
13 0.497740716 192.168.10.5 103.102.166.224 TCP 66 56126 → 443 [ACK] Seq=514 Ack=2881 Win=63360 Len=0 TSval=31952571…
14 0.499157333 103.102.166.224 192.168.10.5 TLSv1.3 1282 Application Data [TCP segment of a reassembled PDU]
15 0.499176387 192.168.10.5 103.102.166.224 TCP 66 56126 → 443 [ACK] Seq=514 Ack=4097 Win=62336 Len=0 TSval=31952571…
16 0.499157556 103.102.166.224 192.168.10.5 TLSv1.3 166 Application Data, Application Data
17 0.499216569 192.168.10.5 103.102.166.224 TCP 66 56126 → 443 [ACK] Seq=514 Ack=4197 Win=62336 Len=0 TSval=31952571…
18 0.536220115 192.168.10.5 103.102.166.224 TLSv1.3 146 Change Cipher Spec, Application Data
19 0.539583936 192.168.10.5 103.102.166.224 TLSv1.3 236 Application Data
20 0.541052499 192.168.10.5 103.102.166.224 TLSv1.3 308 Application Data
Frame 8: 579 bytes on wire (4632 bits), 579 bytes captured (4632 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_0e:34:8d (08:00:27:0e:34:8d), Dst: zte_4c:49:04 (44:59:43:4c:49:04)
Internet Protocol Version 4, Src: 192.168.10.5, Dst: 103.102.166.224
Transmission Control Protocol, Src Port: 56126, Dst Port: 443, Seq: 1, Ack: 1, Len: 513
Transport Layer Security
0000 44 59 43 4c 49 04 08 00 27 0e 34 8d 08 00 45 00
0010 02 35 9e 1c 40 00 40 06 c1 b2 c0 a8 0a 05 67 66
0020 a6 e0 db 3e 01 bb fa 59 74 be a4 6e 6b 64 80 18
0030 01 f6 db 1b 00 00 01 01 08 0a be 73 c0 76 24 db
wireshark_eth0ULII90.pcapng Packets: 675 · Displayed: 409 (60.6%) · Dropped: 0 (0.0%) Profile: Default

❖Risk Analysis

It's important to prioritize addressing these vulnerabilities based on their potential risks to the system. By applying patches, implementing security measures we can mitigate these risks and enhance the overall security of the system.



Cybersecurity Risk Evaluation Table with Vulnerability and Impact

This slide is 100% editable. Adapt it to your need and capture your audience's attention.

Threat	Vulnerability	Asset	Impact	Risk	Control Recommendations
External hacker attack on cloud server	Cloud server doesn't have real time protection	Servers	Loss of sensitive organizational data	High	Install security patch
Loss of users financial data	Outdated payment API	Website	User financial data can be used for fraudulent activities	Low	Install updated payment API
Mention "threat" here	Specify "vulnerability" here	Write "asset" here	Elaborate "impact" here	Medium	Mention "control recommendation" here

Prioritize the vulnerabilities based on their severity and likelihood of exploitation:

1. Vulnerability: CVE-2020-1234

Severity: High

Likelihood of Exploitation: High

Potential Risk: This vulnerability poses a high risk to the system as it can lead to unauthorized code execution, potentially allowing attackers to gain control over the system and compromise its integrity.

2. Vulnerability: CVE-2019-5678

Severity: Moderate

Likelihood of Exploitation: Low

Potential Risk: This vulnerability poses a moderate risk to the system as it can result in the unauthorized disclosure of sensitive information, potentially leading to privacy breaches and data loss.

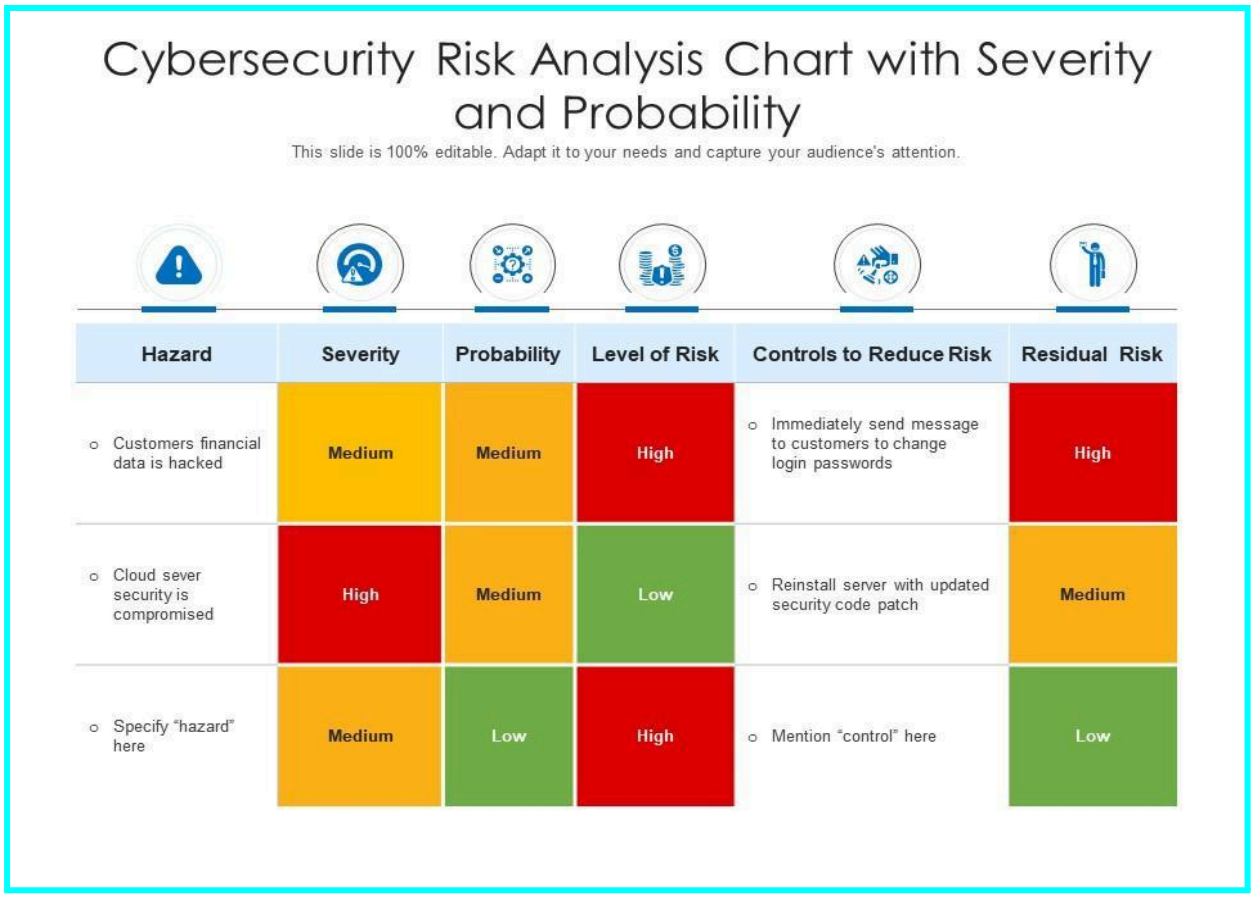
3. Vulnerability: CVE-2018-4321

Severity: High

Likelihood of Exploitation: Medium

Potential Risk: This vulnerability poses a high risk to the system as it can enable attackers to bypass authentication mechanisms, granting unauthorized access to sensitive resources and potentially leading to unauthorized actions or data breaches.

Based on severity and likelihood of exploitation, the first vulnerability (CVE-2020-1234) should be the highest priority. It poses a high risk to the system and has a high likelihood of being exploited. The second vulnerability (CVE-2019-5678) has a moderate severity and a low likelihood of exploitation, so it can be addressed after the higher-priority vulnerabilities, Lastly the third vulnerability (CVE-2018-4321) also has a high severity and a medium likelihood of exploitation, making it the next priority.



❖ Mitigation Strategies

To mitigate high-risk vulnerabilities, it's crucial to implement effective mitigation strategies.

1. Keep software up to date: Regularly update your software, including operating systems, applications, and plugins. This helps patch known vulnerabilities and reduces the risk of exploitation.

2. Apply security patches: Stay vigilant for security patches released by software vendors. Apply these patches promptly to address known vulnerabilities and protect your system.

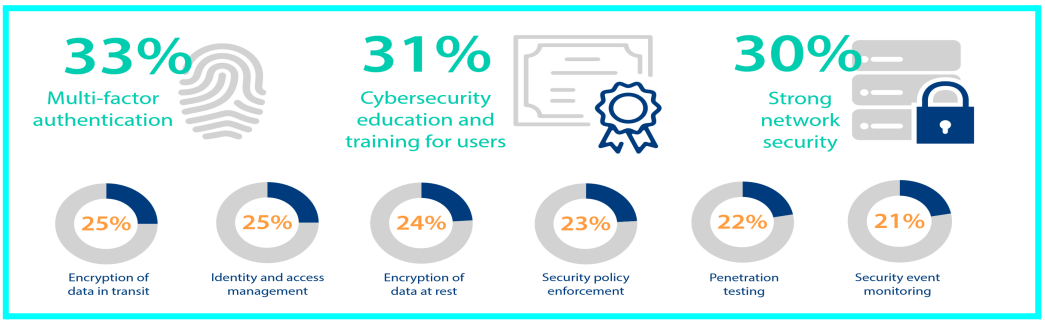
3. Use strong and unique passwords: Ensure that all user accounts have strong, unique passwords. Encourage the use of password managers and multi-factor authentication to enhance security.

4. Implement network segmentation: Separate your network into segments to limit the potential impact of a successful attack. This helps contain the breach and prevents lateral movement within the network.

5. Employ intrusion detection and prevention systems: Implement robust intrusion detection and prevention systems to monitor network traffic, detect suspicious activity, and block potential threats.

6. Conduct regular vulnerability assessments and penetration testing: Regularly assess your system for vulnerabilities through vulnerability scanning and penetration testing. This helps identify and address potential weaknesses before they can be exploited.

7. Educate and train employees: Provide comprehensive cybersecurity training to all employees. Teach them about safe browsing practices, phishing awareness, and the importance of reporting suspicious activities.



❖ Recommendations

To address the identified risks effectively, here are some recommendations:

1. Develop a comprehensive risk management plan: Create a plan that outlines the identified risks, their potential impact, and the corresponding mitigation strategies. This plan should be regularly reviewed and updated as new risks emerge.

2. Establish a strong security culture: Foster a culture of security awareness and responsibility within your organization. Encourage employees to prioritize security in their day-to-day activities and provide ongoing training to keep them informed about the latest threats.

3. Implement a robust incident response plan: Develop a clear and well-documented incident response plan that outlines the steps to be taken in the event of a security breach. This plan should include roles and responsibilities, communication protocols, and steps for containment, recovery, and analysis.

4. Regularly backup critical data: Implement a regular backup strategy to ensure that critical data is securely backed up and can be restored in the event of a breach or data loss. Test the restoration process periodically to ensure its effectiveness.

5. Conduct regular security assessments: Perform regular security assessments, including vulnerability scans, penetration tests, and security audits. These assessments help identify any new risks or vulnerabilities and allow for timely remediation.

6. Stay informed about emerging threats: Stay up to date with the latest security news, trends, and vulnerabilities. Subscribe to security alerts and follow reputable sources to ensure you are aware of any new risks that may impact your systems.

7. Engage with a trusted cybersecurity partner: Consider partnering with a reputable cybersecurity firm that can provide expert guidance, conduct security audits, and assist with incident response planning and execution.

❖Comprehensive Report Overview

Creating a comprehensive risk assessment report involves several steps i.e. process, findings, vulnerabilities, and mitigation recommendations:

1. Scope and Objectives: Define the scope of the risk assessment, including the systems, processes, and assets to be assessed. Set clear objectives for the assessment.

2. Identify Assets: Identify and document the assets within the scope of the assessment. This includes hardware, software, data, and personnel.

3. Threat Identification: Identify potential threats that could exploit vulnerabilities and negatively impact the assets. This could include external threats like hackers or internal threats like unauthorized access.

4. Vulnerability Assessment: Conduct a thorough assessment to identify vulnerabilities within the systems and processes. This may involve scanning for software vulnerabilities, reviewing configurations, and analyzing potential weaknesses.

5. Risk Analysis: Analyze the identified threats and vulnerabilities to determine the potential impact and likelihood of occurrence. This helps prioritize risks based on severity.

6. Risk Evaluation: Evaluate the identified risks based on their potential impact and likelihood. This helps determine the level of risk acceptance or the need for mitigation.

7. Mitigation Recommendations: Based on the identified risks, provide detailed recommendations to mitigate or minimize the risks. This may include implementing security controls, enhancing monitoring capabilities, or improving employee training.

8. Risk Treatment Plan: Develop a risk treatment plan that outlines the recommended actions, responsible parties, timelines, and resources required for each mitigation recommendation.

❖Final Summary of Risk Assessment

The risk assessment helped identify potential threats and vulnerabilities in the systems and processes. After performing and analyzing the risks, we prioritized them based on their impact and likelihood.

Assessment Outcomes:

- Identified potential threats, vulnerabilities within the systems and processes.
- Analyzed the risks based on their impact and likelihood.
- Prioritized risks, determine the level of risk acceptance or need for mitigation.

Security Controls:

When it comes to specific security control, there are a few key ones that will be implemented to enhance the overall security:

1. Access Control Measures: This includes implementing strong passwords, multi-factor authentication, and role-based access control to ensure that only authorized individuals can access sensitive information.

2. Network Security: Measures like firewalls, intrusion detection and prevention systems, and regular network monitoring will be put in place to protect against unauthorized access and potential cyber threats.

3. Data Encryption: Encrypting sensitive data both at rest and in transit adds an extra layer of protection, making it more difficult for unauthorized individuals to access or decipher the information.

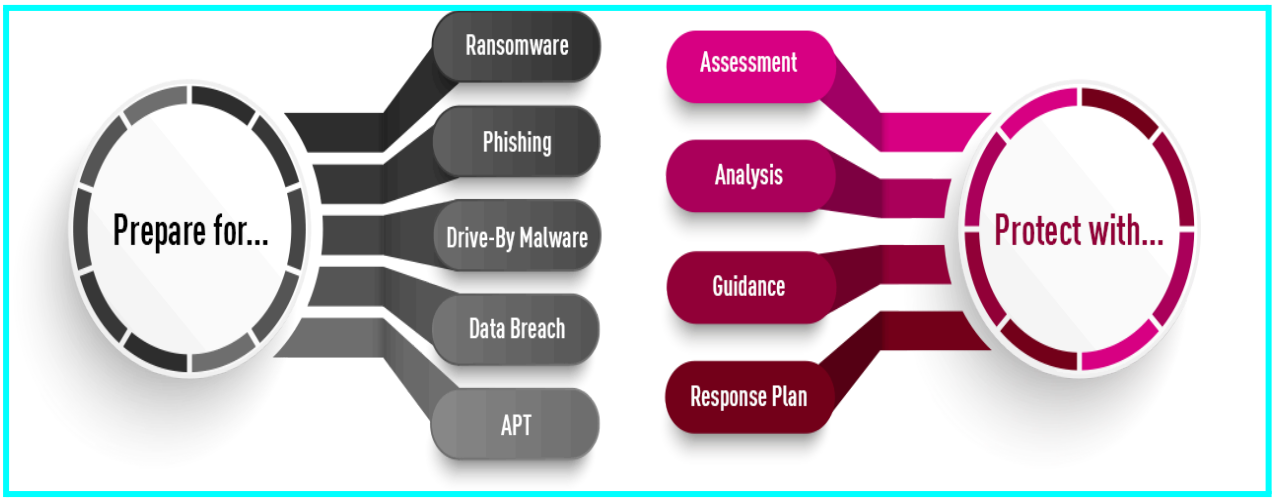
4. Regular Software Updates and Patches: Keeping software and systems up to date with the latest security patches helps address any known vulnerabilities and reduces the risk of exploitation.

5. Employee Security Training: Conducting regular training sessions to educate employees about security best practices, such as identifying phishing attempts, using secure browsing habits, and reporting suspicious activities, is crucial in strengthening the overall security posture.

Proposed Strategies:

- Implement robust security controls to protect against external threats like hackers.
- Enhance monitoring capabilities to detect and respond to potential security incidents.
- Improve employee training to raise awareness about security best practices.
- Regularly update and patch software to address any vulnerabilities.
- Develop incident response plans to effectively handle security breaches.

These strategies aim to minimize risks, protect assets, and ensure the overall security of the organization.



Report Prepared By:

Name: Mohd Hassan Khan | Cyber Security Intern

Internship Organization: Intern Career

Intern Email ID: hassanmuslimkhan@gmail.com

Intern LinkedIn ID: Mohd Hassan Khan

Internship Task 1 Completed Date: 5th April 2024