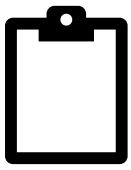
# CYBER SECURITY INTERN

## Task One:

## Risk Assessment Report



## Presented by:

**Tanaka Mushedhe**

**Providing a Small Office/Home Office (SOHO) networking system as my sample network for assessment so as to find threats and vulnerabilities within it;**

## WHAT IS A SOHO?

It refers to a small-scale computing and networking environment, typically found in the context of small businesses, home-based businesses, or individual home users.

Some key characteristics of a SOHO network system include:

1. Scale:
    - SOHO networks are usually limited in size, with a small number of connected devices, typically ranging from a few to a few dozen.
    - The network infrastructure is relatively simple, with a focus on basic connectivity and functionality.
2. Equipment:
    - Common SOHO network devices include routers, switches, wireless access points, desktop computers, laptops, and various peripheral devices like printers and scanners.

- The equipment is often consumer-grade or small-business-oriented, rather than enterprise-class hardware.

3. Network Topology:
    - SOHO networks often have a simple star or bus topology, with a central router or gateway device connecting the various devices.
    - Wireless connectivity is commonly used to provide flexibility and ease of access for mobile devices.
4. IT Support:
    - SOHO networks typically have limited or no dedicated IT support, with the owner or a few employees responsible for managing and maintaining the network.
    - The level of technical expertise may vary, and the focus is on providing basic functionality rather than advanced network management.

## 1. Networking design of the SOHO system


Router, **192.168.1.1**

**192.168.1.3**

*Wireless Access Point*

*Switch,* ***192.168.1.2***

***192.168.1.4***

Printer

***192.168.1.5***

Desktop

## The Setup and operation;

The flow of internet access in this SOHO network system is as follows:

1. Router: The router connects the entire SOHO network to the internet, providing the main gateway and basic firewall protection.

2. Switch: The switch connects the wired devices, such as the desktop computer and wired printer, to the network. It also connects the wireless access point, allowing wireless devices to access the network.

3. Wired Devices: The desktop computer and wired printer connect directly to the switch and can access the internet through the router.

4. Wireless Devices: The laptops connect to the wireless access point, which then connects to the switch. This allows the wireless devices to access the internet through the router.

This setup provides a common SOHO network topology, where the router acts as the central point of internet connectivity, the switch handles the wired network connections, and the wireless access point enables wireless devices to join the network.

## POTENTIAL THREATS AND VULNERABILTIES WITHIN THE SOHO NETWORKING;

| COMPONENT | POTENTIAL THREAT | POTENTIAL VULNERABILTY |
|---|---|---|
| Router | Unauthorized access to the router, Distributed Denial of Service (DDoS) attacks | Weak or default administrative credentials, Outdated firmware with known security vulnerabilities, Misconfigured firewall settings or open ports, Lack of advanced security features (e.g., VPN, intrusion detection) |
| Switch | Unauthorized access to the switch, Exploitation of switch vulnerabilities to disrupt network traffic, Insider threats (e.g., rogue employees) | Weak or default administrative credentials, Outdated firmware with known security vulnerabilities, Lack of port security and MAC address filtering, Insufficient network segmentation or VLAN configuration |
| Wireless Access Point | Unauthorized access to the wireless network, Eavesdropping on wireless traffic, Exploitation of wireless | Use of weak or outdated wireless encryption protocols, Weak wireless network passwords, Lack of wireless network |

| | | |
|---|---|---|
| | vulnerabilities to gain access | segmentation or guest network capabilities, Rogue access points or unauthorized wireless devices |
| Printer | Unauthorized access to the printer, Exploitation of printer vulnerabilities to disrupt operations, Printer as an entry point for network compromise | Weak or default administrative credentials, Outdated firmware with known security vulnerabilities, Lack of access control and user authentication, Unprotected wireless or network connectivity |
| Desktop | Malware and ransomware infections, Data breaches due to unauthorized access, Phishing and social engineering attacks | Unpatched or outdated operating systems and applications, Lack of antivirus/anti-malware protection, Weak user authentication (e.g., weak passwords), Insufficient data backup and recovery processes |
| Laptop | Malware and ransomware infections, Data | Unpatched or outdated operating systems and |

| | | |
|---|---|---|
| | breaches due to loss or theft of the device, Exploitation of vulnerabilities while on public networks. | applications, Lack of encryption for sensitive data stored on the device, Weak user authentication (e.g., weak passwords), Lack of remote data wiping or device tracking capabilities |

## Conducting Vulnerability Scanning

Vulnerability scanning is an important security practice in a SOHO (Small Office/Home Office) network environment. It involves the process of identifying and assessing potential vulnerabilities or weaknesses in the system, network, or devices that could be exploited by malicious actors;

## Utilizing Nmap as our vulnerability scanner within the SOHO

## What is Nmap

Nmap, short for "Network Mapper," is a powerful open-source network scanning tool used to discover hosts and services on a computer network. It allows you to gather information about the devices connected to the network, such as open ports, operating systems, and services running on those devices. Nmap is commonly used by cybersecurity professionals to assess network security, identify vulnerabilities, and detect potential threats. It is a versatile tool that can be used for both security audits and network inventory management.

## Six port states recognized by Nmap :

Open: Port accepts TCP/UDP connections; service available.

Closed: Port rejects connections; host reachable.

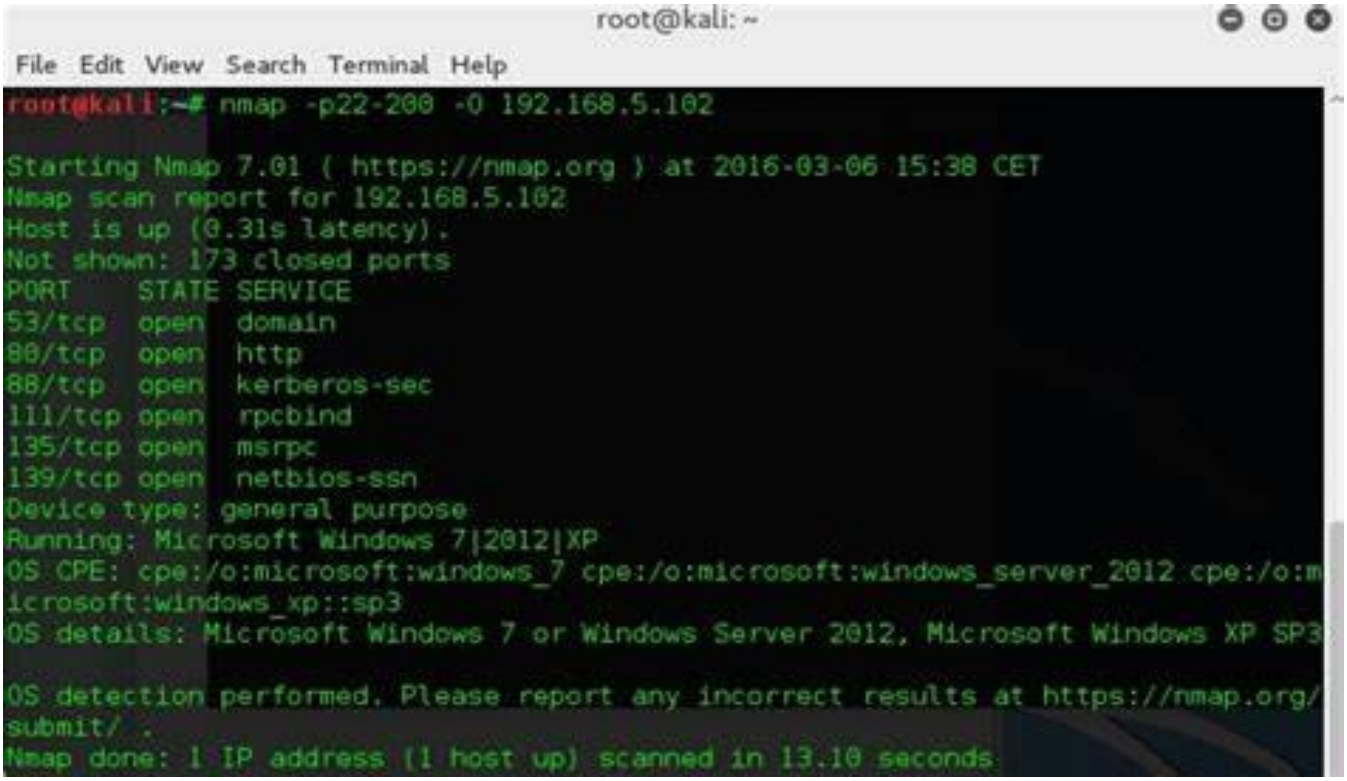
Filtered: Probes blocked; port status unknown.

Unfiltered: Port reachable; status unknown.

Open|Filtered: No response; could be open or filtered.

Closed|Filtered: No response; could be closed or filtered.

## After carefully running the command line interfaced tool, the following extract was presentable findings;




**Elaboration;**

Based on the Nmap scan report, the scan was conducted on the host with the IP address 192.168.5.102. The scan, using Nmap version 7.0.1, revealed that the host is up and running Microsoft Windows 7 operating system.

The scan detected a total of 173 closed ports on the host. However, there are several open ports and services identified, such as port 53/tcp (DNS), port 88/tcp (Kerberos-sec), port 111/tcp (rpcbind), port 135/tcp (msrpc), and port 139/tcp (netbios-ssn). These services could potentially pose security risks if not properly secured.

The hostname of the device is listed as root@kali, indicating that the scan was performed from a device running Kali Linux. The device type is labeled as general purpose, and the operating system is identified as Microsoft Windows 7. The executable path is specified

as cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012, suggesting compatibility with both Windows 7 and Windows Server 2012.

**Second Cybersecurity tool used in scanning vulnerability;**

**Nessus**

Nessus is a widely-used vulnerability scanning tool that helps to identify security vulnerabilities, misconfigurations, and potential threats in networks, systems, and applications. It is known for its comprehensive scanning capabilities, which allow organizations to conduct thorough security assessments and prioritize remediation efforts effectively.

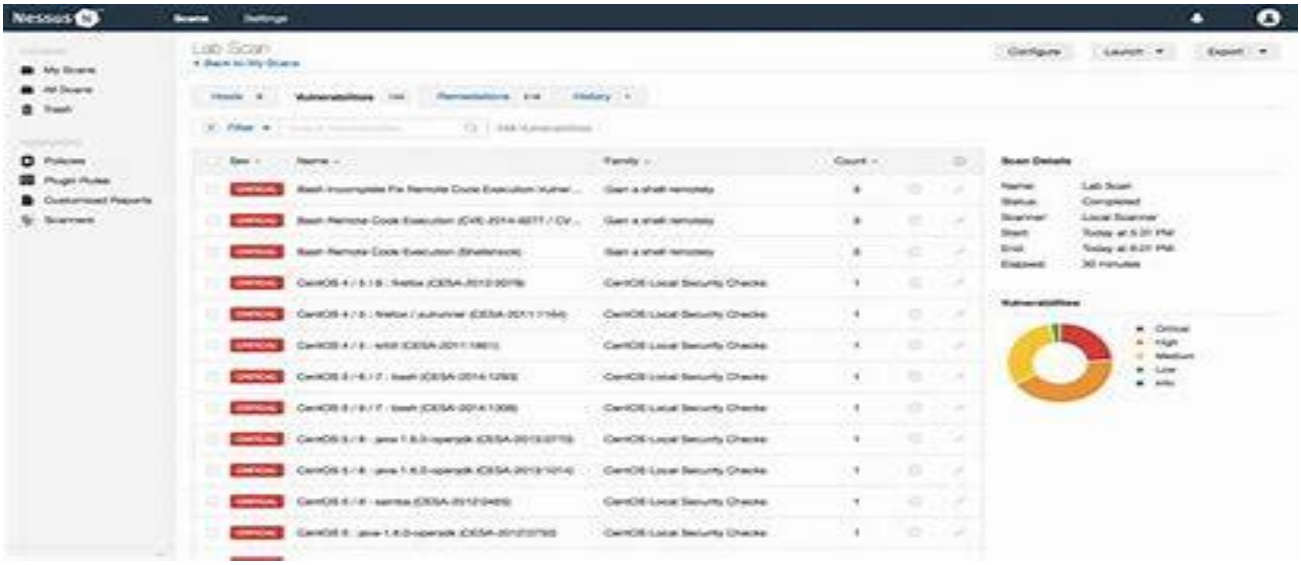
Nessus performs active scans to detect vulnerabilities by sending specially crafted packets to target hosts and analyzing their responses. It provides detailed reports with remediation recommendations, allowing organizations to address security weaknesses proactively. Nessus can scan a variety of target types, including servers, workstations, network devices, databases, and web applications.

The tool is popular among security professionals for its ease of use, extensive vulnerability database, and customizable scanning options. Organizations utilize Nessus to enhance their cybersecurity posture, comply with regulatory requirements, and protect sensitive data from potential cyber threats.


***Creating a New Scan:***

Click "New Scan", configure scan settings including targets, scan template, and schedule, then launch the scan to assess network vulnerabilities.

**Results of the Scan**



**Elaboration;**

This image shows a Nessus vulnerability scanning report, which provides detailed information about various security vulnerabilities detected in the scanned environment.

Here's a breakdown of the key information presented in the image:

1. The report lists a number of vulnerabilities, each with a unique ID, name, and description.
2. For each vulnerability, the report provides details such as the family it belongs to, the severity level (Critical, High, Medium, Low), the number of hosts affected, and the associated CVE (Common Vulnerabilities and Exposures) references.
3. The vulnerabilities are sorted by severity, with the most critical vulnerabilities listed first.
4. The "Plugin Output" section provides additional information about each vulnerability, such as the affected software versions, potential impact, and recommended remediation steps.
5. The bottom-right pie chart provides a visual summary of the vulnerability distribution across the different severity levels.

## Identified Vulnerabilities, their severity and potential impact

## Router Vulnerabilities

### 1. Weak or default administrative credentials:

**Potential Impacts:**

- Unauthorized access to the router's administrative interface and configuration settings
- Ability to modify router settings, including network parameters, firewall rules, and access controls
- Potential to use the compromised router as a launching point for further attacks on the SOHO network
- Exposure of sensitive information, such as network topology or user credentials, stored on the router

**Severity: High**

Weak or default administrative credentials pose a high-severity threat, as they can enable attackers to gain full control over the router and potentially the entire SOHO network. This vulnerability can have significant consequences, including data breaches, system compromises, and network-based attacks.

### 2. Outdated firmware with known security vulnerabilities:

**Potential Impacts:**

- Exploitation of known vulnerabilities in the router's firmware, leading to remote code execution or denial of service

- Potential for attackers to gain unauthorized access to the router and the SOHO network

- Disruption of network services and availability due to successful exploitation

- Inability to mitigate known vulnerabilities, leaving the network exposed to potential attacks

**Severity: High**

Outdated firmware with known security vulnerabilities is a high-severity issue, as it can enable attackers to compromise the router and potentially gain access to the entire SOHO network. Regularly updating router firmware and addressing known vulnerabilities is crucial to maintain a secure network infrastructure.

**3. Misconfigured firewall settings or open ports:**

**Potential Impacts:**

- Unauthorized access to the SOHO network through open ports or misconfigured firewall rules

- Exposure of internal network resources and devices to potential attackers

- Potential for attackers to use the SOHO network as a launching point for further attacks

- Increased risk of data breaches, system compromises, and network-based threats

**Severity: Moderate to High**

Misconfigured firewall settings or open ports can pose a moderate to high-severity threat, depending on the specific configuration and the type of network resources exposed. While they may not directly lead to a complete system compromise, they can provide attackers with an entry point into the SOHO network, increasing the risk of various security incidents.

**4. Lack of advanced security features (e.g., VPN, intrusion detection) in a router:**

**Potential Impacts:**

- Reduced overall network security and increased vulnerability to various attacks

- Inability to effectively detect and respond to network-based threats, such as unauthorized access or malicious activities

- Lack of secure remote access mechanisms, exposing the SOHO network to potential compromise

**Severity: Moderate to High**

The lack of advanced security features in a SOHO router can pose a moderate to high-severity threat, depending on the specific security requirements and the nature of the SOHO network. While it may not directly lead to a system compromise, the absence of these features can limit the overall security posture and increase the vulnerability to various attacks.

In summary, weak or default administrative credentials, outdated firmware with known security vulnerabilities, misconfigured firewall settings or open ports, and the lack of advanced security features in a SOHO router are all security vulnerabilities that can have significant impacts on the overall security and resilience of the SOHO network. Addressing these issues through robust router configuration, regular firmware updates, and the implementation of advanced security measures is crucial for SOHO organizations to mitigate these risks and maintain a secure and reliable network infrastructure.

## Switch Vulnerabilities

Certainly, let's examine the severity and potential impacts of various switch-related security vulnerabilities within a SOHO (Small Office/Home Office) environment:

### 1. Weak or default administrative credentials:

**Potential Impacts:**

- Unauthorized access to the switch's administrative interface and configuration settings

- Ability to modify switch settings, including VLAN configurations, port security, and access controls

- Potential to use the compromised switch as a launching point for further attacks on the SOHO network

- Exposure of sensitive information, such as network topology or user credentials, stored on the switch

**Severity: High**

Weak or default administrative credentials pose a high-severity threat, as they can enable attackers to gain full control over the switch and potentially the entire SOHO network. This vulnerability can have significant consequences, including data breaches, system compromises, and network-based attacks.

**2. Outdated firmware with known security vulnerabilities:**

**Potential Impacts:**

- Exploitation of known vulnerabilities in the switch's firmware, leading to remote code execution or denial of service

- Potential for attackers to gain unauthorized access to the switch and the SOHO network

- Disruption of network services and availability due to successful exploitation

- Inability to mitigate known vulnerabilities, leaving the network exposed to potential attacks

**Severity: High**

Outdated firmware with known security vulnerabilities is a high-severity issue, as it can enable attackers to compromise the switch and potentially gain access to the entire SOHO network. Regularly updating switch firmware and addressing known vulnerabilities is crucial to maintain a secure network infrastructure.

**3. Lack of port security and MAC address filtering:**

**Potential Impacts:**

- Unauthorized access to the SOHO network through unsecured switch ports

- Ability for attackers to spoof MAC addresses and gain access to network resources

- Increased risk of network-based attacks, such as ARP spoofing or DHCP spoofing

**Severity: Moderate to High**

The lack of port security and MAC address filtering on a SOHO switch can pose a moderate to high-severity threat, depending on the specific network configuration and the potential exposure of sensitive resources. While it may not directly lead to a complete

system compromise, it can provide attackers with an entry point into the SOHO network, increasing the risk of various security incidents.

**4. Insufficient network segmentation or VLAN configuration:**

**Potential Impacts:**

- Lack of proper network isolation and segmentation, allowing attackers to move laterally across the SOHO network

- Exposure of sensitive network resources to unauthorized access or compromise

- Increased risk of data breaches, system compromises, and the spread of malware within the SOHO network

**Severity: Moderate to High**

Insufficient network segmentation or VLAN configuration can pose a moderate to high-severity threat, depending on the specific network architecture and the sensitivity of the resources within the SOHO network. Proper network segmentation and VLAN configuration are essential to limit the spread of threats and contain the impact of a potential security breach.

In summary, weak or default administrative credentials, outdated firmware with known security vulnerabilities, lack of port security and MAC address filtering, and insufficient network segmentation or VLAN configuration in a SOHO switch are all security vulnerabilities that can have significant impacts on the overall security and

resilience of the SOHO network. Addressing these issues through robust switch configuration, regular firmware updates, and the implementation of advanced security measures is crucial for SOHO organizations to mitigate these risks and maintain a secure and reliable network infrastructure.

## Wireless Access Point

Certainly, let's examine the severity and potential impacts of various wireless-related security vulnerabilities within a SOHO (Small Office/Home Office) environment:

### 1. Use of weak or outdated wireless encryption protocols:

**Potential Impacts:**

- Ability for attackers to easily decrypt and intercept wireless network traffic
- Exposure of sensitive information, such as login credentials, financial data, or confidential documents
- Potential for attackers to gain unauthorized access to the SOHO network and resources

**Severity: High**

The use of weak or outdated wireless encryption protocols, such as WEP or TKIP, is a high-severity vulnerability. These protocols are known to be insecure and can be easily cracked, allowing attackers

to gain access to the wireless network and potentially the entire SOHO network.

**2. Weak wireless network passwords:**

**Potential Impacts:**

- Brute-force attacks or guessable passwords allowing unauthorized access to the wireless network

- Exposure of the SOHO network to various attacks, such as eavesdropping, man-in-the-middle attacks, or lateral movement within the network

**Severity: High**

Weak or easily guessable wireless network passwords pose a high-severity threat, as they can enable attackers to gain access to the wireless network and potentially the SOHO network resources.

**3. Lack of wireless network segmentation or guest network capabilities:**

**Potential Impacts:**

- Inability to isolate guest or untrusted wireless devices from the main SOHO network

- Increased risk of lateral movement and the spread of threats within the SOHO network

- Potential for guest or untrusted devices to access sensitive resources or network segments

**Severity: Moderate to High**

The lack of wireless network segmentation or guest network capabilities can pose a moderate to high-severity threat, depending on the specific network configuration and the sensitivity of the resources within the SOHO network. Proper network segmentation and the implementation of guest network capabilities are essential to limit the exposure of the SOHO network to potential threats originating from wireless devices.

**4. Rogue access points or unauthorized wireless devices:**

**Potential Impacts:**

- Ability for attackers to set up rogue access points and conduct man-in-the-middle attacks or eavesdrop on wireless traffic

- Unauthorized access to the SOHO network through connected wireless devices

- Potential for attackers to use the rogue access point as a launching point for further attacks on the SOHO network

**Severity: High**

The presence of rogue access points or unauthorized wireless devices within a SOHO network poses a high-severity threat, as it can enable attackers to gain unauthorized access to the network and potentially compromise the overall security of the SOHO environment.

In summary, the use of weak or outdated wireless encryption protocols, weak wireless network passwords, lack of wireless network segmentation or guest network capabilities, and the presence of rogue access points or unauthorized wireless devices are all security vulnerabilities that can have significant impacts on the overall security and resilience of a SOHO wireless network. Addressing these issues through the implementation of strong encryption protocols, robust password policies, proper network segmentation, and proactive wireless network monitoring is crucial for SOHO organizations to mitigate these risks and maintain a secure and reliable wireless infrastructure.

## Desktop Vulnerabilities

Certainly, let's examine the severity and potential impacts of various security vulnerabilities related to a desktop computer within a SOHO (Small Office/Home Office) environment:

### 1. Weak or default administrative credentials:

**Potential Impacts:**

**-** Unauthorized access to the desktop's administrative features and system settings

- Ability to install malware, access sensitive data, or perform other malicious activities

- Potential for the compromised desktop to be used as a launching point for further attacks on the SOHO network

**Severity: High**

Weak or default administrative credentials on a desktop computer pose a high-severity threat, as they can enable attackers to gain full control over the system and potentially the entire SOHO network. This vulnerability can have significant consequences, including data breaches, system compromises, and network-based attacks.

**2.Outdated firmware or software with known security vulnerabilities:**

**Potential Impacts:**

- Exploitation of known vulnerabilities in the desktop's software or firmware, leading to remote code execution or privilege escalation

- Potential for attackers to gain unauthorized access to the desktop and the SOHO network

- Disruption of desktop functionality and availability due to successful exploitation

- Inability to mitigate known vulnerabilities, leaving the desktop and the network exposed to potential attacks

**Severity: High**

Outdated firmware or software with known security vulnerabilities is a high-severity issue, as it can enable attackers to compromise the desktop and potentially gain access to the entire SOHO network. Regularly updating desktop software and addressing known vulnerabilities is crucial to maintain a secure computing environment.

**3. Lack of access control and user authentication:**

**Potential Impacts:**

- Unauthorized access to the desktop and its resources

- Exposure of sensitive data or system configurations to unauthorized individuals

- Potential for malicious activities, such as data theft, system modifications, or the installation of malware

**Severity: High**

The lack of robust access control and user authentication mechanisms on a desktop computer poses a high-severity threat, as it can enable unauthorized individuals to gain access to the system

and its resources, potentially leading to data breaches, system compromises, and other security incidents.

**4. Unprotected wireless or network connectivity:**

**Potential Impacts:**

- Ability for attackers to access the desktop remotely through unprotected wireless or network connections

- Potential for eavesdropping, man-in-the-middle attacks, or the introduction of malware into the SOHO network

- Increased risk of data breaches or unauthorized access to sensitive information stored on the desktop

**Severity: High**

Unprotected wireless or network connectivity on a desktop computer within a SOHO environment is a high-severity vulnerability, as it can enable attackers to remotely access the system and potentially the entire SOHO network. Proper network segmentation, the use of strong encryption protocols, and the implementation of secure remote access mechanisms are crucial to mitigate this risk.

In summary, weak or default administrative credentials, outdated firmware or software with known security vulnerabilities, lack of access control and user authentication, and unprotected wireless or network connectivity are all security vulnerabilities that can have significant impacts on the overall security and resilience of a desktop

computer within a SOHO environment. Addressing these issues through the implementation of strong access controls, regular software updates, robust authentication mechanisms, and secure network connectivity is crucial for SOHO organizations to maintain a secure and reliable computing infrastructure.

## Laptop Vulnerabilities

### 1. Unpatched or outdated operating systems and applications:

**Potential Impacts:**

- Exploitation of known vulnerabilities by attackers, leading to remote code execution, data breaches, or system takeover

- Inability to mitigate the latest security threats, leaving the laptop and potentially the SOHO network exposed

- Disruption of laptop functionality and availability due to successful exploitation of vulnerabilities

**Severity: High**

Unpatched or outdated operating systems and applications on a laptop computer pose a high-severity threat, as they can enable attackers to exploit known vulnerabilities and compromise the system. Regularly updating the laptop's software is crucial to maintain a secure computing environment and mitigate the risks associated with these vulnerabilities.

### 2. Lack of encryption for sensitive data stored on the device:

**Potential Impacts:**

- Exposure of sensitive information, such as confidential documents, login credentials, or financial data, in the event of laptop theft or loss

- Potential for unauthorized access to sensitive data, leading to data breaches and compliance issues

**Severity: High**

The lack of encryption for sensitive data stored on a laptop computer within a SOHO environment is a high-severity vulnerability, as it can enable attackers to access and potentially misuse sensitive information in the event of the laptop being lost or stolen. Implementing robust data encryption mechanisms is essential to protect sensitive information and mitigate the risks associated with data breaches.

**3. Weak user authentication (e.g. weak passwords):**

**Potential Impacts:**

- Unauthorized access to the laptop and its resources, including sensitive data or SOHO network resources

- Potential for attackers to use the compromised laptop as a launching point for further attacks on the SOHO network

- Exposure of the SOHO network to various threats, such as data breaches, lateral movement, or the installation of malware

**Severity: High**

Weak user authentication, such as the use of weak or easily guessable passwords, on a laptop computer within a SOHO environment poses a high-severity threat, as it can enable attackers to gain unauthorized access to the system and potentially the entire SOHO network. Implementing strong password policies and multi-factor authentication mechanisms is crucial to mitigate this risk.

**4. Lack of remote data wiping or device tracking capabilities:**

**Potential Impacts:**

- Inability to remotely wipe sensitive data from a lost or stolen laptop, leading to potential data breaches

- Difficulty in locating and recovering a lost or stolen laptop, increasing the risk of data exposure and unauthorized access

**Severity: Moderate to High**

The lack of remote data wiping or device tracking capabilities for a laptop computer within a SOHO environment can pose a moderate to high-severity threat, depending on the sensitivity of the data stored on the device and the potential impact of a data breach. Implementing these capabilities can help mitigate the risks associated with the loss or theft of a laptop by enabling remote data wiping and facilitating the recovery of the device.

In summary, unpatched or outdated operating systems and applications, lack of encryption for sensitive data stored on the device, weak user authentication, and the lack of remote data wiping or device tracking capabilities are all security vulnerabilities that can have significant impacts on the overall security and resilience of a laptop computer within a SOHO environment. Addressing these issues through regular software updates, data encryption, strong authentication mechanisms, and the implementation of remote management capabilities is crucial for SOHO organizations to maintain a secure and reliable computing infrastructure.

## Risk analysis

a method for locating, evaluating, and ranking hazards to a system or business so that treatment and mitigation decisions can be made with knowledge.

**Level of severity:**

Impact degree of hazards:

High: Significantly disrupts or breaches.

Moderate: Causes partial outages or unwanted entry.

Low: Only slightly disrupts or exposes a restricted area.

## Probability

**Probability of a risk event:**

High: A high potential for abuse.

Medium: Needs certain conditions, moderate possibility.

Low: Seldom occurring circumstances, high work, or low chance.

First priority:

Level of urgency for action:

Critical: Due to its extreme severity, it needs to be attended to right now.

as well as probability.

High: Response to significant vulnerabilities must be swift.

Medium: Needs prompt mitigation to have a moderate impact and

Probability.

| **Device** | **Vulnerability** | **Severity** | **Likelihood** | **Priorities** |
|---|---|---|---|---|
| **Router** | Weak or default administrative credentials | High | High | High |
| | Weak or default administrative credentials | High | High | Moderate |

| | | | | |
|---|---|---|---|---|
| | Lack of robust access control and user authentication | High | High | Moderate |
| | Unprotected wireless or network connectivity | High | High | High |
| **Switch** | Weak or default administrative credentials | High | High | High |
| | Outdated firmware with known vulnerabilities | High | High | Moderate |
| | Lack of access control and user authentication | High | High | Moderate |
| | Unprotected network connectivity | High | High | High |
| **Wireless Access Point** | Weak or default administrative credential | High | High | High |
| | Outdated firmware with known vulnerabilities | High | High | Moderate |
| | Outdated firmware with known vulnerabilities | High | High | Moderate |

| | | | | |
|---|---|---|---|---|
| | Unprotected wireless connectivity | High | High | High |
| **Desktop** | Weak or default administrative credentials | High | High | High |
| | Outdated firmware or software with known vulnerabilities | High | High | Moderate |
| | Lack of access control and user authentication | High | High | Moderate |
| | Unprotected wireless or network connectivity | High | High | Moderate |
| **Laptop** | Unpatched or outdated operating systems and applications | High | High | Moderate |
| | Lack of remote data wiping or device tracking capabilities | High | High | Moderate |
| | Lack of encryption for sensitive data stored on the device | High | High | Moderate |

| | | | | |
|---|---|---|---|---|
| | Weak user authentication | Moderate to High | Moderate | Moderate |

## Suggested Recommendations to address identified Risks

| Device | Vulnerability | Recommended Solution |
|---|---|---|
| **Router** | Weak or default administrative credentials | • Implement strong and unique administrator passwords<br>• Enable two-factor authentication for administrative access |
| | Outdated firmware with known vulnerabilities | • **Regularly Update Firmware**: Check the manufacturer's website for firmware updates and apply them promptly.<br>• **Monitor Security Advisories**: Subscribe to security advisories from the manufacturer for timely information on vulnerabilities and patches. |
| | Lack of robust access control and | • **Limit User Access**: Create user accounts with specific permissions and avoid |

| | | |
|---|---|---|
| | user authentication | using a single account for all configurations.<br>• **Implement Strong Passwords**: Change default usernames and passwords to complex, unique credentials for both router access and Wi-Fi connections. |
| | Unprotected wireless or network connectivity | • **Use Guest Networks**: Set up a separate guest network for visitors to keep the primary network more secure.<br>• **Disable WPS (Wi-Fi Protected Setup)**: Turn off WPS to eliminate vulnerabilities associated with this feature. |
| | Weak or default administrative credentials | • **Change Default Credentials**: Immediately modify any default administrative usernames and |

| | | |
|---|---|---|
| | | passwords upon installation.<br>• **Use Strong, Unique Credentials**: Create complex, unique passwords that combine letters, numbers, and special characters. |
| | Unprotected network connectivity | • **Disable Unused Services**: Turn off any unnecessary services (e.g., Telnet, SSH, UPnP) that could expose the router to vulnerabilities.<br>• **Implement Firewall Rules**: Configure the router's built-in firewall to restrict inbound and outbound traffic based on your security needs. |
| **Wireless Access Point** | Weak or default administrative credentials | • **Change Default Credentials**: Immediately update default usernames and passwords to complex, unique ones. |

| | | |
|---|---|---|
| | Outdated firmware with known vulnerabilities | • **Regularly Update Firmware**: Check for firmware updates from the manufacturer and apply them as soon as they become available.<br>- |
| | Lack of access control and user authentication | • **Implement Role-Based Access Control**: Set up user accounts with specific permissions to limit access to sensitive settings. |
| | Unprotected wireless connectivity | • **Enable WPA3 or WPA2 Encryption**: Use the latest security protocols to encrypt wireless communication, ensuring data protection. |
| **Desktop** | Weak or default administrative credentials | • Implement strong and unique administrator passwords<br>• Enable two-factor authentication for administrative access |

| | | |
|---|---|---|
| | Outdated firmware or software with known vulnerabilities | • Regularly check for and install operating system and application updates<br>• Enable automatic software update checks and installations |
| | Lack of access control and user authentication | • Implement role-based access control<br>• Enforce strong password policies<br>• Enable multi-factor authentication for user access |
| | Unprotected wireless or network connectivity | • Configure firewall rules to limit network connectivity<br>• Use a VPN for remote access to the SOHO network |
| **Laptop** | Unpatched or outdated operating systems and applications | • Regularly check for and install operating system and application updates<br>• Enable automatic software update checks and installations |
| | Lack of encryption for sensitive data | • Implement full-disk encryption (e.g., |

| | | |
|---|---|---|
| | stored on the device | BitLocker, FileVault, or VeraCrypt)<br>• Encrypt sensitive files and folders |
| | Weak user authentication (e.g., weak passwords) | • Enforce strong password policies<br>• Enable multi-factor authentication for user access |
| | Lack of remote data wiping or device tracking capabilities | • Implement a mobile device management (MDM) solution<br>• Enable remote data wiping and device tracking features |