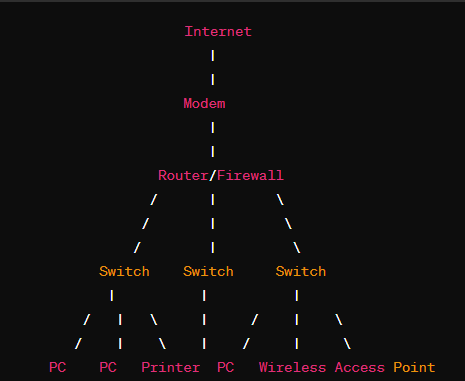
**NETWORK SECURITY VULNERABILITY ASSESSMENT**

**EXECUTIVE SUMMARY:**

This report presents the findings of a comprehensive network security vulnerability assessment conducted on a system’s Local Area Network. The assessment aimed to identify weaknesses and potential risks within the network infrastructure and provide actionable recommendations for improving security posture.



**INTRODUCTION:**

The purpose of this assessment was to evaluate the security of the Local Area Network and identify vulnerabilities that could expose the network to unauthorized access, data breaches, or other security incidents.

**SCOPE OF ASSESSMENT**

1. **Network Infrastructure**
   * Assessment of network devices, including routers, switches, firewalls, and access points.
   * Analysis of network configurations and settings to identify vulnerabilities and misconfigurations.
2. **Data Security**
   * Identification of data leakage risks, including unprotected sensitive data and insecure transmission protocols.
   * Evaluation of access controls and data encryption mechanisms to protect against unauthorized access and data breaches.
3. **Host Systems:**
   * Evaluation of the workstation operating systems for vulnerabilities and weaknesses.
   * Review of installed software, services and applications for known vulnerabilities and insecure configurations.
4. **Physical Security:**
   * Evaluation of physical security measures such as access controls, surveillance systems and environmental controls.

**METHODOLOGY:**

The assessment methodology included a combination of manual network scanning and analysis of the network configuration settings.

**FINDINGS:**

* **Network Infrastructure Vulnerabilities:** The Local Area Network had misconfigured routers and outdated firewalls that created security weaknesses in the network.
* There is also a lack of network monitoring tools which caused a challenge in identifying unusual network activity and responding to it in time.
* **Access Control Weaknesses:** Weak and default passwords on the devices and network equipment makes it easy for attackers to access the LAN. There is a need for strong, unique passwords and two factor authentication.
* **Data Leakage Risks:** There are sensitive data on the network devices that are unprotected. There is also insecure transmission of data thereby, unauthorized users can also gain access to the LAN and be able to view, modify or steal data.

**RISK ASSESSMENT:**

The vulnerabilities were categorized based on severity levels (low-1, medium-2, high-3) considering their potential impact and likelihood of exploitation.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Vulnerability | Threat | Likelihood | Severity | Risk Priority |
| Unauthorized user | Gain access to the LAN and steal or modify sensitive data. | 2 | 2 | 4 |
| Malware Attacks | Unavailability of data due to malware attacks. | 3 | 3 | 9 |
| Physical theft | Stolen laptop can lead to permanent loss of data. | 2 | 3 | 6 |
| Data Breach | Data interception over insecure networks | 2 | 2 | 4 |
| Outdated software | Failure to update OS and Hardware | 3 | 2 | 6 |

**RECOMMENDATIONS:**

* Based on the assessment findings, the following recommendations are provided to increase the security posture of the LAN:
* Strong passwords, access controls and physical security measures should be adopted to mitigate risks.
* Unique passwords and two factor authentication should be employed across devices to prevent unauthorized access.
* Regular patching and updating of system software and applications.
* Sensitive data on the network should be encrypted to protect it.
* Network devices need to be properly configured and regularly audited.
* Network monitoring tools should be employed to help identify unusual network activity.

**CONCLUSION:**

The assessment revealed several vulnerabilities within the Local Area Network that pose significant risks to its security. Addressing these vulnerabilities promptly and implementing the recommended security measures will help mitigate these risks and enhance the overall security posture of the network.