7. Security Plan for TechSecure Solutions

Prepared by: Ross Moravec / A00322717

Introduction

This security plan outlines how TechSecure Solutions will secure its network infrastructure by implementing security best practices and mitigating risks. The plan is designed to protect the company's systems against potential internal and external threats by maintaining a robust security posture through proactive defenses and continuous monitoring.

This document covers:

- A network topology diagram
- A detailed risk assessment
- Key security strategies, including the principles of least privilege and defense-in-depth

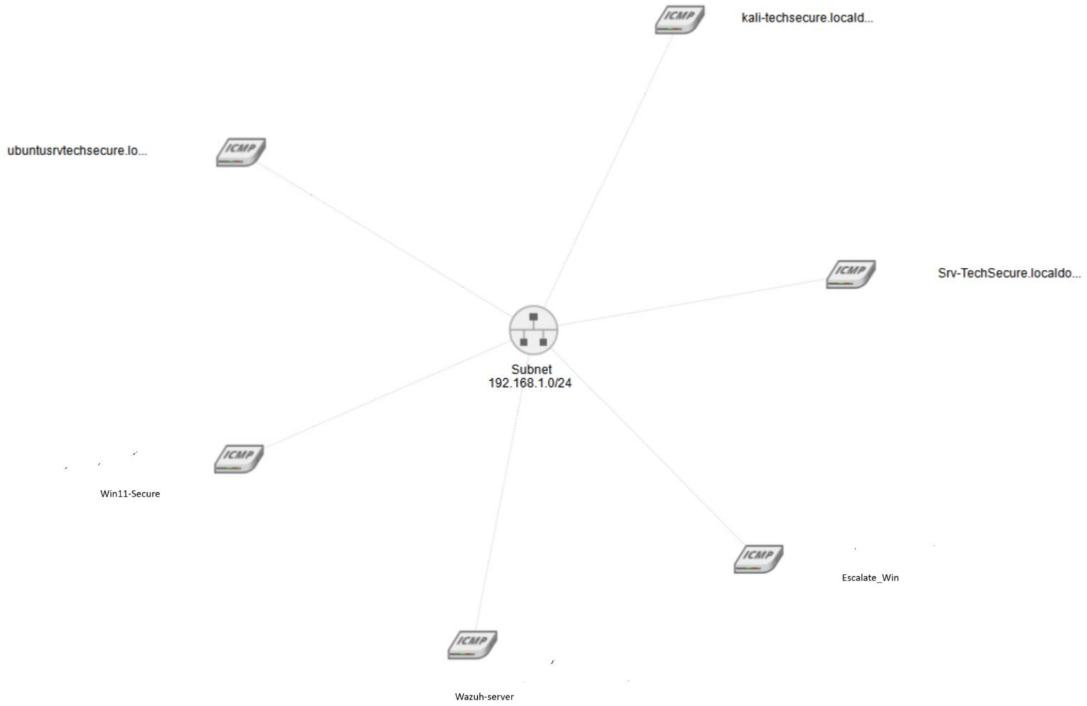
---

Network Topology Diagram

The network for TechSecure Solutions operates within the 192.168.1.0/24 subnet, with various virtual machines (VMs) serving critical functions. Below is a description of the key components within the network:

- **Firewall**: The OPNsense firewall at **192.168.1.1**, which filters traffic between external connections and internal servers, and provides secure remote access via VPN and SSH.
- **Servers**:
    - **Active Directory Domain Controller (Windows Server)** at **192.168.1.101** for centralized user and access management.
    - **Wazuh Security Monitoring Server** at **192.168.1.106**, responsible for continuous security monitoring and log collection.
    - **Ubuntu Server** at **192.168.1.108**, providing additional infrastructure services.
- **Endpoints**:

- **Windows 11 Workstation** at **192.168.1.107**, used by users within the network.
- **Windows 7 Machine** at **192.168.1.116** for legacy compatibility and testing.
- **Kali Linux** at **192.168.1.109**, used for penetration testing and security assessments.



Risk Assessment

This section identifies the key risks present within TechSecure's network infrastructure, their associated vulnerabilities, and the proposed mitigation strategies to address them.

Risk	Vulnerability	Threat	Mitigation
Unauthorized Access	Exposed SSH and RDP services	Brute-force attacks, unauthorized system access	Enforce SSH key-based authentication, restrict access to trusted IP addresses, and implement MFA.

Risk	Vulnerability	Threat	Mitigation
Weak Authentication	Insufficient password policies and lack of 2FA	Credential theft, privilege escalation	Apply strong password policies, enforce 2FA for administrators, and regularly audit privileges.
Data Exfiltration	Exposed SMB and HTTP services without encryption	Data leakage via insecure channels	Restrict external access, encrypt data in transit using TLS/SSL, and limit access with firewall rules.
Outdated Software	Use of legacy software versions with known vulnerabilities	Exploitation of unpatched vulnerabilities	Implement a patch management process and run regular vulnerability scans to detect weak points.
Unencrypted Communications	Self-signed and expired SSL/TLS certificates	MITM attacks, data interception	Use trusted Certificate Authority (CA) certificates and ensure timely renewal of certificates.

Security Strategies

1. Least Privilege

TechSecure Solutions will adopt the principle of least privilege, ensuring that all users, systems, and services have only the access required to perform their tasks, minimizing the attack surface.

- **Implementation**:
  - Role-based access control (RBAC) will be enforced in Active Directory, assigning users to roles based on their responsibilities.
  - Administrative access to sensitive systems (e.g., the firewall, Wazuh server) will be strictly limited to essential personnel.

    - Services and users will be restricted to specific network segments, ensuring that access to sensitive resources is only available to those with a clear need.

---

2. Defense-in-Depth

The defense-in-depth strategy will provide multiple layers of security, ensuring that if one layer fails, subsequent layers will help mitigate the impact.

- **Implementation**:
    - **Network Segmentation**: The network is segmented into different zones using firewall rules to isolate critical services and restrict unnecessary access. For instance, sensitive systems such as the Wazuh server are protected from general user access.
    - **Firewall Rules**: The OPNsense firewall is configured to block all unnecessary inbound and outbound traffic. Services such as HTTP, SMB, and RDP are only accessible to trusted IP addresses.
    - **Continuous Monitoring**: Wazuh provides real-time monitoring, sending alerts for abnormal activities such as failed login attempts, unauthorized access, and suspicious traffic patterns.
    - **Encryption**: All sensitive communications will be encrypted using strong TLS/SSL protocols. Expired and self-signed certificates will be replaced with those from trusted CAs to prevent MITM attacks.
    - **Patch Management**: TechSecure will implement a regular patch management schedule to ensure that all systems and applications are up to date, minimizing the risk of exploitation of known vulnerabilities.

Monitoring and Incident Response

To ensure the continued security of the network, TechSecure Solutions will employ the following monitoring and incident response practices:

- **Continuous Monitoring with Wazuh**: The Wazuh server at **192.168.1.106** is configured to monitor security events across all VMs. This includes detecting suspicious login attempts, monitoring system file changes, and tracking unusual network activity.

- **Alerts and Incident Handling**: Alerts will be configured for any abnormal activity, such as failed login attempts on SSH, suspicious file access, or attempts to exploit services. Immediate action will be taken to investigate and remediate any issues.
- **Log Analysis**: Daily log reviews will ensure that any unusual patterns or potential threats are identified early. Wazuh will aggregate logs from various sources, providing a centralized location for event analysis.
- **Incident Response Plan**: In the event of a breach, TechSecure's incident response team will immediately isolate the affected systems, analyze the attack vector, and restore from secure backups. The team will conduct a root-cause analysis and adjust firewall rules, user permissions, or security policies as needed.

Conclusion

The security plan outlined here ensures that TechSecure Solutions is well-equipped to defend its network against potential threats. By enforcing the principles of least privilege and defense-in-depth, the company's network will be protected from unauthorized access, data exfiltration, and other potential vulnerabilities. Continuous monitoring and a solid incident response process will ensure that any security incidents are quickly detected and resolved, maintaining the overall integrity of the network.