8. Formal Report for TechSecure Solutions

Prepared by: Ross Moravec / A00322717

1. Introduction

This report provides a detailed summary of the work completed to secure TechSecure Solutions' network infrastructure as part of the midterm project. The project focused on several key areas, including configuring firewalls, securing Windows and Linux systems, setting up Active Directory, implementing continuous monitoring through Wazuh, conducting a vulnerability assessment, and developing a comprehensive security plan.

Each part of the project (Parts 1 through 7) has been documented separately with relevant screenshots appended at the end of each document. The screenshots were included in the individual documents due to the wide and all-encompassing nature of each part. Including them in this formal report would have made it cumbersome, so they are referenced here for easy navigation.

This report serves as a high-level overview, summarizing the actions taken, results achieved, and key findings. The list of screenshots and their locations is provided for reference.

---

2. Overview of Work Completed (Parts 1-7)

Part 1: Firewall Setup

The OPNsense firewall at **192.168.1.1** was configured to protect the network by blocking unauthorized access and allowing secure remote connections. The goal was to restrict access to critical services while minimizing the attack surface by blocking unnecessary ports.

- **Summary**: The firewall rules were carefully configured to permit essential services such as SSH for remote administration and HTTP/HTTPS for necessary services. Unused ports were blocked to reduce exposure to attacks.
- **Key Features**:
    - Implemented firewall rules to restrict SSH access to specific IP ranges.
    - Allowed only HTTP/HTTPS traffic while blocking other unnecessary ports.
    - Considered VPN integration to further secure remote connections.

- **Tools Used**: OPNsense was used to configure firewall rules and manage traffic filtering.

Reference: Detailed screenshots of the firewall setup can be found in **1. Firewall Setup**.

Part 2: Windows and Linux Systems Hardening

System hardening was applied to both Windows and Linux environments to secure access and minimize vulnerabilities. The focus was on enforcing strong authentication mechanisms, disabling unnecessary services, and limiting administrative privileges.

- **Summary**: Both Windows and Linux systems were secured by applying strong password policies, enabling key-based SSH authentication, and removing unnecessary services to reduce the potential attack surface.
- **Key Features**:
    - Key-based SSH authentication was enforced on Linux systems, eliminating password-based logins.
    - Strong password policies and account lockout settings were applied to Windows systems through Group Policy.
    - Unnecessary services were disabled on both platforms to minimize the attack vectors.
- **Tools Used**: Group Policy Management for Windows hardening and SSH configuration files for Linux.

Reference: Screenshots of the hardening steps are available in **2. Windows and Linux Systems (Hardening Policies)**.

Part 3: Active Directory Configuration

Active Directory (AD) was set up to centralize user account management and apply security policies across the network. The AD configuration was designed to enforce role-based access control and apply security policies consistently.

- **Summary**: The Active Directory Domain Controller was configured with organizational units (OUs) and security groups to manage users and their access privileges. Group Policy was used to enforce security measures, such as password policies and login restrictions.

- **Key Features**:
    - Organizational units were created to group users based on their roles.
    - Security groups and Group Policy were used to enforce password complexity, account lockouts, and login restrictions.
    - Integrated Windows VMs into the domain for centralized management and policy enforcement.
- **Tools Used**: Active Directory Domain Services, Group Policy Management Console (GPMC), and PowerShell for advanced configuration.

Reference: Screenshots documenting the Active Directory setup can be found in **3. Active Directory Configuration**.

Part 4: Wazuh Implementation

Wazuh was deployed as a continuous monitoring solution to track security events, detect suspicious activity, and provide real-time alerts. The Wazuh server aggregates logs from multiple VMs to centralize security event analysis.

- **Summary**: Wazuh agents were installed across all key virtual machines to provide continuous security monitoring. The server was configured to generate alerts for abnormal activities such as failed login attempts and potential security breaches.
- **Key Features**:
    - Real-time monitoring and alerting based on predefined security rules.
    - Centralized log collection for easy incident analysis and correlation.
    - Alerts for suspicious activity such as failed SSH login attempts or unauthorized access to critical services.
- **Tools Used**: Wazuh agents for log collection and monitoring, Wazuh dashboard for managing alerts.

Reference: Screenshots from the Wazuh dashboard, including alert setups and log aggregation, are available in **4. Wazuh Implementation**.

Part 5: Vulnerability Testing

A thorough vulnerability assessment was conducted using Nmap/Zenmap to scan the network for open ports, services, and potential vulnerabilities. The goal was to identify weak points in the network and recommend corrective actions to strengthen the security posture.

- **Summary**: The vulnerability scan identified open ports, outdated services, and other potential vulnerabilities. Recommendations were provided to close unused ports, update outdated software, and enforce encryption.
- **Key Features**:
    - Open ports on critical systems were identified, including SSH, HTTP, and SMB services.
    - Outdated services were flagged for updates to prevent exploitation of known vulnerabilities.
    - Recommended the use of encryption for services transmitting sensitive data.
- **Tools Used**: Nmap and Zenmap for scanning and analyzing network services.

Reference: The detailed scan results, along with corrective actions, are available in **5. Vulnerability Testing**. Screenshots of the Nmap scan outputs are included.

Part 6: Escalate_Win VM

A detailed examination of the Windows VM was conducted to identify privilege escalation vulnerabilities and address potential security gaps. Administrative privileges were restricted, and the system was hardened to prevent exploitation.

- **Summary**: Privilege escalation vulnerabilities were mitigated by limiting administrative access, patching known vulnerabilities, and improving malware detection systems.
- **Key Features**:
    - Restricted unnecessary administrative privileges to prevent abuse.
    - Regular patching of the Windows VM to ensure all vulnerabilities were addressed.
    - Enhanced malware detection using built-in Windows Defender.

- **Tools Used**: Windows Group Policy, Windows Defender, and PowerShell for system hardening.

Reference: Screenshots and detailed configurations for securing the Windows VM are available in **6. Escalate_Win VM**.

Part 7: Security Plan

A comprehensive security plan was developed to protect TechSecure Solutions' network infrastructure. The plan includes a network topology, risk assessment, and key security strategies, such as least privilege and defense-in-depth.

- **Summary**: The security plan outlines how TechSecure Solutions will protect its network by applying the principles of least privilege and defense-in-depth. This involves segmenting the network, securing sensitive systems, and implementing continuous monitoring.
- **Key Features**:
    - Network segmentation to isolate sensitive systems and services.
    - Continuous monitoring using Wazuh to detect threats in real time.
    - Encryption of sensitive communications and regular patch management to prevent exploitation.
- **Tools Used**: OPNsense Firewall for network segmentation, Wazuh for monitoring, and TLS/SSL for encryption.

Reference: The complete security plan is available in **7. Security Plan**, including the network topology diagram and risk assessment.

---

3. List of Screenshots

The following is a reference list for the screenshots included in each of the documents:

- **Firewall Setup Screenshots**: Available in **1. Firewall Setup**.
- **Windows and Linux Systems Hardening Screenshots**: Available in **2. Windows and Linux Systems (Hardening Policies)**.
- **Active Directory Configuration Screenshots**: Available in **3. Active Directory Configuration**.

- **Wazuh Monitoring and Alerts Screenshots**: Available in **4. Wazuh Implementation**.
- **Vulnerability Scan Results Screenshots**: Available in **5. Vulnerability Testing**.
- **Escalate_Win VM Hardening Screenshots**: Available in **6. Escalate_Win VM**.
- **Network Diagram and Security Plan Screenshots**: Available in **7. Security Plan**.

This allows for easy navigation to the appropriate visual documentation for each part of the project.

---

4. Conclusion

The midterm project has successfully laid the foundation for a robust and secure network infrastructure at TechSecure Solutions. Each phase of the project was critical in addressing key vulnerabilities and reinforcing security across the network. By configuring firewalls, hardening systems, centralizing access control through Active Directory, and implementing continuous monitoring with Wazuh, TechSecure Solutions is now better equipped to detect, prevent, and respond to security threats.

The security plan developed as part of this project will guide ongoing efforts to maintain the security posture of the network. Regular vulnerability assessments, patch management, and security monitoring will ensure that the infrastructure remains resilient against evolving threats.