­

|  |
| --- |
|  |
| Network Security |
|  |
| Network security |
| Stu188448 |
| Jerry Bent |
| 3000 |

**Network Security Configuration Report**

**1. Executive Summary**

Provide a brief overview of the report, including the purpose, scope, and summary of findings and recommendations.

**1.1 Purpose**

Implementing new network security solution for and existing infrastructure ,besides initiating new site for the company

**1.2 Scope**

Reviewing the current security flows and implementing all necessary security configurations for the current network infrastructure

**1.3 Summary of Findings**

Summarize the key findings of the network security assessment.

**1.4 Recommendations**

Provide a brief summary of the recommendations based on the findings.

**2. Introduction**

Describe the background of the company, the importance of network security, and the objectives of the network security assessment.

**3. Current Network Configuration**

Current network configuration is not implemneting any type of security configurations nesides not following and security standards policy.

* Routing is not implemented between network segments
* Switching is not implemented properly (no vlans ,not stp nothing is implemented in regards to the security best practice policy )
* No Management vlan
* Access lists is not implemented
* Poor network segmentation

**3.1 Network Topology**

* Diagram of the network architecture.
* Description of network segments (e.g., LAN, WAN, DMZ).

**3.2 Hardware Components**

* List of network devices (e.g., routers, switches, firewalls).
* Specifications and configurations of each device.

**3.3 Software Components**

* Operating systems and versions.
* Network security software (e.g., antivirus, intrusion detection/prevention systems).

**4. Security Policies and Procedures**

Outline the current security policies and procedures in place.

**4.1 Access Control Policies**

* User authentication and authorization mechanisms.
* Password policies.

**4.2 Data Protection Policies**

* Data encryption methods.
* Data backup and recovery procedures.

**4.3 Incident Response Plan**

* Procedures for detecting and responding to security incidents.
* Roles and responsibilities during an incident.

**5. Vulnerability Assessment**

Identify potential vulnerabilities in the network configuration.

**5.1 Network Scanning Results**

* Summary of network scanning tools used.
* List of vulnerabilities detected (e.g., open ports, outdated software).

**5.2 Penetration Testing Results**

* Overview of penetration testing methods.
* Summary of findings from penetration tests.

**6. Risk Analysis**

Analyze the risks associated with the identified vulnerabilities.

**6.1 Risk Identification**

* List of identified risks.
* Potential impact of each risk on the organization.

**6.2 Risk Mitigation Strategies**

* Strategies to mitigate identified risks.
* Prioritization of risk mitigation efforts.

**7. Recommendations**

Provide detailed recommendations to improve network security.

**7.1 Network Configuration Improvements**

* Recommendations for hardware and software upgrades.
* Network segmentation strategies.

**7.2 Policy and Procedure Enhancements**

* Suggestions for improving security policies and procedures.
* Training and awareness programs for employees.

**7.3 Implementation Plan**

* Timeline for implementing the recommended improvements.
* Resources required for implementation.

**8. Conclusion**

Summarize the overall findings and the importance of implementing the recommendations to enhance network security.

**9. Appendices**

Include any additional information that supports the report, such as detailed scan results, configuration files, and references.

**9.1 Glossary**

Define technical terms and abbreviations used in the report.

**9.2 References**

List of sources and references used in the report.

**9.3 Supporting Documents**

* Copies of network diagrams.
* Detailed vulnerability scan reports.