Executive Summary

This report outlines the comprehensive security assessment conducted on the network and systems of TechGadgets Online. The assessment aimed to identify vulnerabilities, assess their potential impact, and provide mitigation recommendations. The process included a combination of automated tools and manual analysis.

Assessment Process

1. Scope

The assessment focused on TechGadgets Online's network infrastructure, covering IP ranges and specific systems associated with the organization. The evaluation included network infrastructure, web applications, and potential points of entry.

2. Tools Used

Nmap: For network discovery and vulnerability scanning.

Nessus: For in-depth vulnerability scanning.

Manual Analysis: To validate automated findings and identify additional issues.

3. Methodology

Reconnaissance: Gathered information about the target systems.

Scanning: Conducted network and service discovery using Nmap.

Vulnerability Assessment: Utilized Nessus for detailed vulnerability scans.

Web Application Testing: Assessed web applications for common vulnerabilities.

Manual Analysis: Examined specific configurations and potential risks.

Findings

1. Network Infrastructure

1.1 Open Ports

Ports 53, 80, and 443 are open on the target system.

Identified services include DNS (dnsmasq) and web servers (GoAhead-Webs PeerSec-MatrixSSL).

1.2 Vulnerabilities

SSL POODLE vulnerability detected on port 443.

Limited filtering and potential vulnerabilities on various services.

2. Web Applications

2.1 Identified Issues

Web server uses outdated protocols and ciphers.

Multiple HTTP methods are allowed, posing a potential security risk.

PHPMyAdmin may be vulnerable to local file inclusion (CVE-2005-3299).

2.2 SSL/TLS Configuration

Weak SSL/TLS configurations on the web server.

Lack of Perfect Forward Secrecy (PFS) and outdated encryption standards.

3. Operating System

3.1 OS Detection

Aggressive OS guesses suggest the system is likely a Linux-based router or gateway.

3.2 Identified Risks

Default configurations and potential vulnerabilities in the operating system.

Lack of precise OS identification due to non-ideal testing conditions.

Mitigation Recommendations

1. Network Infrastructure

1.1 Open Ports

Implement proper ingress and egress filtering to restrict unnecessary traffic.

Regularly update and patch services to address known vulnerabilities.

1.2 SSL POODLE Vulnerability

Disable SSLv3 and implement secure SSL/TLS configurations.

Monitor and update SSL/TLS configurations regularly.

2. Web Applications

2.1 SSL/TLS Configuration

Update web server configurations to enforce secure SSL/TLS standards.

Review and tighten security settings on web servers.

2.2 PHPMyAdmin Vulnerability

If PHPMyAdmin is not essential, consider removing it.

If necessary, update PHPMyAdmin to the latest version to address potential vulnerabilities.

3. Operating System

3.1 General Recommendations

Apply OS updates and patches regularly.

Conduct a thorough review of default configurations to enhance security.

Conclusion

The security assessment identified potential vulnerabilities in the network infrastructure, web applications, and the operating system of TechGadgets Online. Implementing the provided mitigation recommendations will enhance the overall security posture. Regular monitoring, patching, and proactive measures are crucial for maintaining a resilient and secure environment.

Next Steps

Implementation of Mitigations:

Execute the recommended mitigations based on priorities.

Continuous Monitoring:

Implement continuous monitoring solutions to detect and respond to emerging threats.

Regular Assessments:

Conduct periodic security assessments to stay ahead of evolving security risks.

Staff Training:

Provide ongoing security training for IT staff to ensure awareness of the latest security best practices.