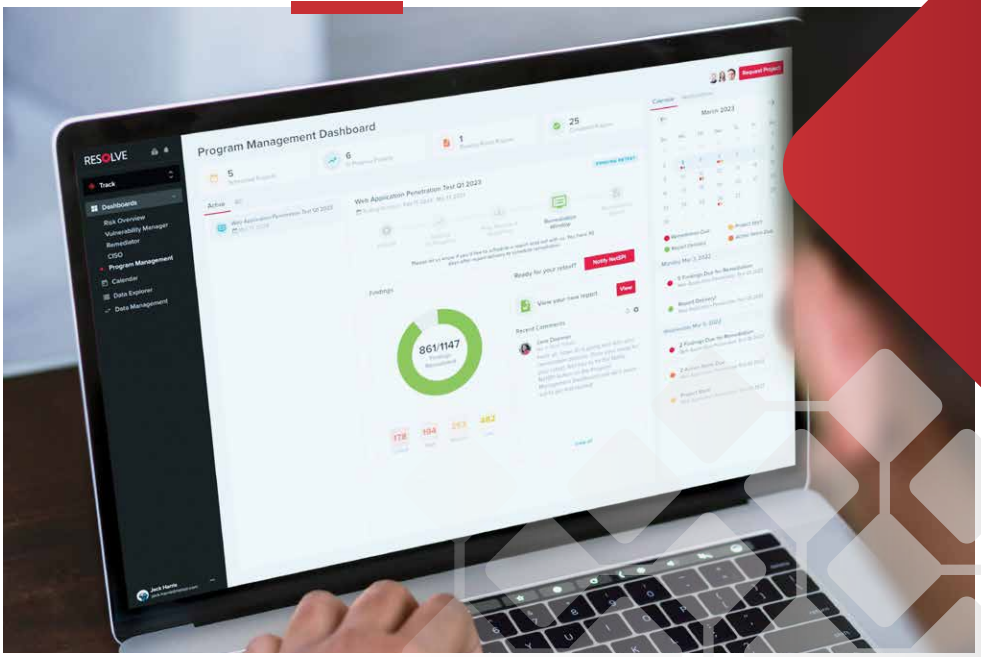
NETSPI®

Acme Co. | September 8, 2023

Sample Security Audit Report

EXTERNAL NETWORK PENETRATION TESTING



NETSPI

Contents

Chapter 1 | Executive Summary ---- 4

1.1 Project Objectives 4

1.2 Summary of Results 4

1.3 Summary of Recommendations 4

Chapter 2 | Project Overview ---- 5

2.1 Constraints 5

2.2 Approach 5

Chapter 3 | Vulnerability Summary ---- 6

Chapter 4 | Penetration Test Attack Narrative ---- 8

4.1 Attack Narrative Summary 8

4.2 Attack Narrative Details 8

Chapter 5 | Vulnerability Details ---- 13

5.1 Overview 13

5.2 Critical Severity Findings 15

5.2.1 SQL Injection ---- 15

5.2.2 Sensitive Information Disclosure - Public GitHub Repository ---- 21

5.2.3 Sensitive Information Disclosure - web.config ---- 23

5.2.4 Vulnerable Version - Apache Log4j Remote Code Execution ---- 24

5.2.5 Weak or Default Password - FTP Anonymous ---- 31

5.2.6 Weak or Default Password - Windows ---- 33

5.3 High Severity Findings 37

5.3.1 Cisco ASA Path Traversal (CVE-2020-3452) ---- 37

5.3.2 Unsupported Version - Microsoft Exchange Server ---- 40

5.3.3 Vulnerable Version - High - Apache Tomcat ---- 42

5.4 Medium Severity Findings 44

5.4.1 Database Service Available - Microsoft SQL Server ---- 44

5.4.2 Information Disclosure - Apache - Server-Status ---- 45

5.4.3 Insecure Protocol - FTP ---- 47

5.4.4 Weak Configuration - MFA Not Enabled - Office 365 ---- 48

5.5 Low Severity Findings 51

5.5.1 Information Disclosure - NTLM Response - Domain Information ---- 51

5.5.2 Weak Configuration - SMTP - DMARC Record Not Set ---- 52

5.5.3 Weak Configuration - SSL/TLS - Deprecated Protocol ---- 53

5.5.4 Weak Configuration - SSL/TLS - Self-Signed Certificate ---- 55

5.5.5 Weak Configuration - SSL/TLS - Weak Hashing Algorithm used to Sign Certificate 56

Appendix A | NetSPI Contact Information ---- 58

Appendix B | Systems in Scope ---- 59

Appendix C | Methodology ---------- **60**
Appendix D | Risk Management Approach Overview ---------- **62**
Appendix E | Security Toolkit Reference ---------- **63**
Revision History *64*

Chapter 1 | Executive Summary

Between June 12, 2023 and June 16, 2023 NetSPI performed a penetration test against Acme Co.'s external network infrastructure and attempted to gain unauthorized access to high value systems, applications, and sensitive information.

1.1 Project Objectives

The primary objectives during this project were to:

- Identify network, system, and application layer vulnerabilities that exist in Acme Co.'s external network environment from the perspective of an unauthenticated attacker.
- Provide Acme Co. with an understanding of the potential impact vulnerabilities could have by leveraging them to gain access to critical resources.
- Provide Acme Co. with a prioritized remediation approach to address the identified vulnerabilities.

1.2 Summary of Results

NetSPI gained unauthorized access to Acme Co. systems, web applications, and sensitive information. A few of the vulnerabilities appear to be widespread throughout the organization. However, most of vulnerabilities only affect a few assets. This was primarily due to:

- Web application vulnerabilities
- Publicly accessible sensitive information
- Software containing known vulnerabilities
- Insecure protocols
- Weak or default passwords
- Weak system configurations

1.3 Summary of Recommendations

NetSPI recommends remediating identified vulnerabilities using the prioritized approach below.

- Address all vulnerabilities that were used to gain unauthorized access to systems, applications, and sensitive information (entry points).
- Address issues required to be remediated by internal policy or external regulation.
- Address vulnerabilities highlighted in the Penetration Test Attack Narrative chapter that contributed to accessing sensitive information within the environment.
- Address high severity vulnerabilities that have the potential to be a threat but were not exploited during the penetration test.
- Address remaining medium severity vulnerabilities.
- Address program level gaps that are linked to high impact vulnerabilities.

NETSPI®

WANT TO SEE THE FULL SAMPLE SECURITY AUDIT REPORT?

Every engagement with NetSPI will provide you with a PDF report of findings, as well as access to NetSPI's Penetration Testing as a Service (PTaaS) platform, delivering streamlined vulnerability management, team communication, and real-time updates. In this sample report, you will gain insights into vulnerabilities and misconfigurations that we might find during an External Network Penetration Testing engagement and see how our team can help you secure your web applications.

- Project Overview: Objectives, Scope & Timeframe, and Findings Summary
- Technical Detail: Critical, High, Medium, and Low severity findings
- Testing Methodology
- Risk Management Approach

SHOW ME THE SAMPLE SECURITY AUDIT REPORT!