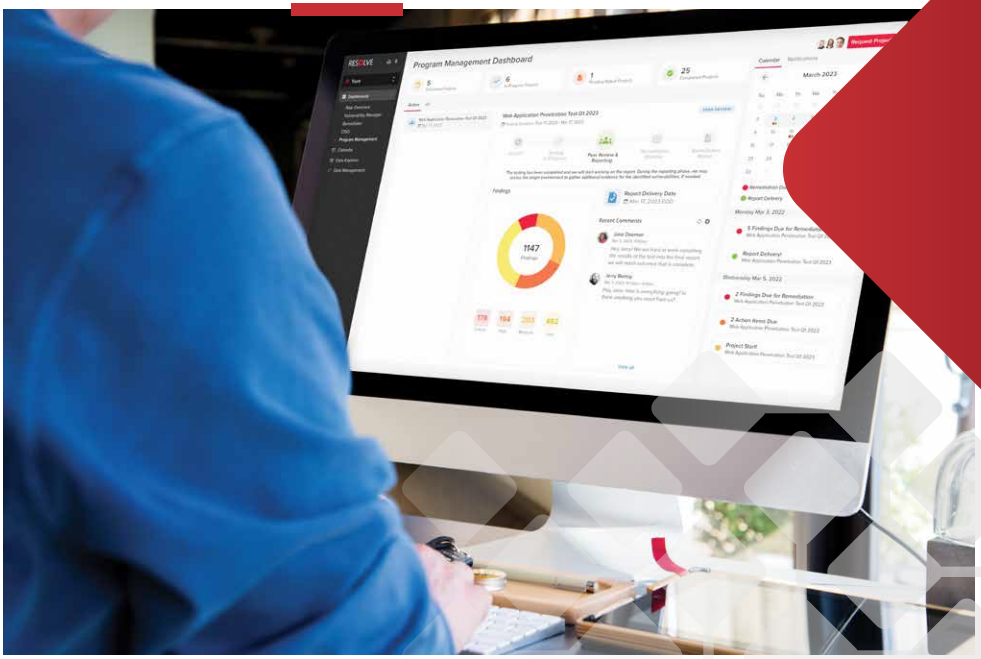
NETSPI®

XYZ Industries | September 4, 2023

# Sample Security Audit Report

## AWS CLOUD PENETRATION TESTING



NETSPI

## Contents





**XYZ Industries: Report generated from an independent AWS lab environment. No client data or NetSPI internal resources were used.*

# Chapter 1 | Executive Summary

Between June 19, 2023 and June 20, 2023 NetSPI performed a penetration test against XYZ Industries' AWS cloud 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 XYZ Industries' cloud environment from the perspective of an unauthenticated attacker.
- Identify configuration-based issues related to the deployment of infrastructure and services in the cloud, from the perspective of an authenticated account in the cloud environment.
- Provide XYZ Industries with an understanding of the potential impact vulnerabilities could have by leveraging them to gain access to critical resources.
- Provide XYZ Industries with a prioritized remediation approach to address the identified vulnerabilities.

## 1.2 Summary of Results

NetSPI gained unauthorized access to XYZ Industries 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 Available Cloud Resources
- Excessive IAM Permissions

## 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 (Criticals).
- 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 privilege escalation and lateral movement 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.

## Chapter 2 | Project Overview

All testing was conducted between June 19, 2023 and June 20, 2023. Below is a summary of the project scope, constraints, and approach.

The following resources were in scope for the test:

- Review of 1 AWS account (123456789012)
- Authenticated configuration review was performed using the AWS Managed Policy arn:aws:iam::aws:policy/ReadOnlyAccess
- Configuration review of the AWS environment includes:
    - Review of utilized AWS service configurations (including, but not limited to):
        - CloudFormation Stacks: 1
        - CloudFront Distributions: 1
        - EC2 Instances: 2
        - IAM Managed Policies: 5
        - Lambda Functions: 1
        - S3 Buckets: 2
- All systems on the network during privilege escalation and data targeting tasks.

## 2.1 Constraints

Per the statement of work, the project constraints included:

- Testing could occur 24/7
- Testing from the perspective of an unauthenticated attacker over the Internet
- Intrusion Prevention System (IPS) exceptions were put in place for NetSPI test systems to increase accuracy and prevent project delays

## 2.2 Approach

The approach NetSPI used during the penetration test was based on the NIST 800-53 special publication, PCI DSS penetration test requirements, PCI DSS penetration test guidelines, and industry best practices.

During testing NetSPI attempted to complete the following tasks:

- Discover live systems and services
- Identify vulnerabilities
- Exploit vulnerabilities
- Escalate application, local, and domain user privileges
- Evaluate and bypass controls used to isolate sensitive system and data
- Gain unauthorized access to sensitive system and data

The following types of attacks were attempted during the penetration test.

- Exploitation of known operating system and application vulnerabilities
- Exploitation of common network protocol and Active Directory vulnerabilities
- Exploitation of common web application vulnerabilities

All other types of attacks were out of scope. Out of scope attacks include but are not limited to: the exploitation of vulnerabilities likely to cause service disruptions, phishing emails, phishing phone calls, and physical penetration.

## Chapter 3 | Vulnerability Summary

Each of the vulnerabilities identified during the project has been assigned a severity ranking. This ranking is assigned according to the following measure.

| LEVEL | SEVERITY | CVSS SCORE | DESCRIPTION |
|---|---|---|---|
| 4 | Critical | 9.0 - 10.0 | Vulnerabilities that were exploited to gain initial access to the in-scope systems, applications, or sensitive data. |
| 3 | High | 7.0 - 9.0 | Vulnerabilities with the potential to provide direct, unauthorized, remote access to protected networks, systems, application functionality, or sensitive data.<br>Example: Code execution, arbitrary file read/write, persistent code injection, PHI/PCI data exposure. |
| 2 | Medium | 4.0 - 6.9 | Vulnerabilities that could potentially be used to escalate existing privileges, reflected (require user interaction or second tier execution), or expose sensitive configuration information.<br>Example: Cross-site scripting, open SMTP relay, clear text storage of passwords/sensitive data, cleartext management protocols. |
| 1 | Low | 0.0 - 3.9 | Vulnerabilities that disclose non-critical host information, non-critical weak cryptography configurations, and best practices that don't directly lead to unauthorized access to protected networks, systems, application functionality, or sensitive data.<br>Example: Most SSL findings, RDP findings etc. |

**TABLE 1: SEVERITY REFERENCES**

NetSPI performed comprehensive vulnerability enumeration against 1 AWS account and 5 network assets within the account which revealed the following vulnerabilities:

- 1 critical severity vulnerability
- 3 high severity vulnerabilities
- 2 medium severity vulnerability

| VULNERABILITY NAME | SEVERITY | CATEGORY | ASSETS |
|---|---|---|---|
| Sensitive Information Disclosure - Plaintext Secret Access Key Discovered - AWS | Critical | Configuration | 1 |
| Bucket with Public Permissions - S3 - AWS | High | Configuration | 1 |
| Excessive Privileges - Public Access to IAM Role - AWS | High | Configuration | 1 |
| Server-Side Request Forgery | High | Code Change | 1 |
| Cleartext Password - CloudFormation Template - AWS | Medium | Configuration | 1 |
| Insufficient Ingress Filtering - EC2 - AWS | Medium | Configuration | 1 |

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 AWS Cloud 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!**