NetSPI™

Sample Security Audit Report

External Attack Surface Management (EASM)

September 24, 2024

NetSPI™

Contents

Chapter 1 | External Attack Surface Management

1.1 Project Overview

Below is a summary of the scope, constraints, and approach for continuous penetration testing within EASM. The scope for continuous penetration testing includes:

- All systems, applications, IPs, and domain that were discovered with verified ownership
- Data discovered from third parties during OSINT activities
- Privilege escalation where possible

1.2 Constraints

The constraints for continuous penetration testing include:

- Testing from the perspective of an unauthenticated attacker over the Internet

1.3 Approach

Continuous Penetration Testing by the Attack Surface Management Operations Team focuses on discovering and exploring high impact vulnerabilities.

The approach NetSPI uses during continuous penetration testing is 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 completes 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 data

The following types of attacks are attempted during continuous penetration testing.

- 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 are 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.

1.4 Vulnerability Summary

The following vulnerabilities were discovered as part of NetSPI's External Attack Surface Management. This report may not encompass all vulnerabilities discovered and may represent only a subset of all potential threats.

NAME	SEVERITY	STATUS
Log4Shell (CVE-2021-44228	Critical	Verified

Chapter 2 | Technical Detail

2.1 Overview

The detailed findings section contains the analysis and documentation of the vulnerabilities identified within your external attack surface. This analysis included:

- Identifying potential vulnerabilities associated with the NetSPI Platform application
- Assigning appropriate severity rankings to valid vulnerabilities and risks
- Formulating useful action-based recommendations that can improve the security posture of the IT environment

Vulnerabilities are grouped according to severity. Information for each of the vulnerabilities includes the following:

Name: The name of the vulnerability.

Severity: Each of the vulnerabilities has been assigned a severity based on its impact to the application and its associated resources. The following table summarizes the severity levels:

SEVERITY	DESCRIPTION
Critical	Vulnerabilities that were exploited to gain initial access to targeted systems, applications, or sensitive data.
High	Vulnerabilities within the potential to provide access to systems, applications, or sensitive data.
Medium	Vulnerabilities that result in the exposure of session data or security configuration information. Unencrypted transmission of sensitive data or use of weak encryption methods.
Low	Vulnerabilities that result in the exposure version information or non-critical configuration information. Implementation of weak password policies and procedures.
Informational	Vulnerabilities that provide additional informational about a target, but do not expose an increased risk.

The severity ratings in this document are based upon industry standard and do not necessarily take into consideration the environment in which the vulnerabilities exist, other controls that may be implemented within that environment, or an organization's classification of the information or functionality.

Asset and Affected URL: Specific assets and associated services on which the vulnerability was found.

Vulnerability Details and Remediation Instructions: Comprehensive explanation of the vulnerability that was found, including a high-level summary of how the vulnerability works and NetSPI's solution for repairing the vulnerability or mitigating the problem if no fix is yet available.

Verification: Screenshot and sample data from the vulnerability showing how NetSPI has verified the finding manually, when possible.

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 The NetSPI Platform, delivering streamlined vulnerability management, team communication, and real-time updates. In this sample report, gain insights into vulnerabilities and misconfigurations that we might find during an External Attack Surface Management (EASM) engagement and see how our team can help you secure your environments.

- 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!