NetSPI™

Sample Security Audit Report

Wireless Network Penetration Test

ACME Inc. | July 31, 2024

Welcome to the NetSPI Platform
Findings by Status and Severity
Top Vulnerable Assets
Engagements
Web Application Penetration Test

© NetSPI Proprietary and Confidential

Contents

Chapter 1 | Engagement Summary ---3

1.1 Engagement Objectives ...3

1.2 Scope & Timeframe ...3

1.3 Summary of Findings ...4

Chapter 2 | Technical Detail ---5

2.1 Overview ...5

2.2 High Severity Findings ...7

2.2.1 WPA/WPA2 PSK Enabled on Corporate Network ---7

2.2.2 WPA2 PSK with PMKID Enabled ---8

2.3 Medium Severity Findings ...10

2.3.1 Open Wireless Network with a Captive Portal --- 10

2.3.2 Weak Configuration - Wireless Network Access Control Bypass - DNS Tunneling 11

2.3.3 Wireless Network - Undetected Control Bypass - MAC Spoofing on a Guest Network--- 13

2.3.4 Wireless Network - WPA/WPA2 PSK Enabled on an IoT/BYOD Wireless Network 15

2.3.5 WPA2 PSK with PMKID Enabled --- 17

2.4 Low Severity Findings ...18

2.4.1 Wireless Network - WPA/WPA2 PSK Enabled on an Untrusted/Guest Wireless Network--- 18

Appendix A | NetSPI Contact Information ---20

Appendix B | Wireless Penetration Test Methodology ---21

Appendix C | Risk Management Approach Overview ---23

Revision History ...24

NetSPI Sample
NetSPI Sample
NetSPI Sample

Chapter 1 | Engagement Summary

NetSPI performed a penetration test of ACME, Inc.'s wireless networks to identify vulnerabilities, determine the level of risk they present to ACME, Inc., and provide actionable recommendations to reduce this risk. NetSPI compiled this report to provide ACME, Inc. with detailed information on each vulnerability discovered within the wireless implementation, including potential business impacts and specific remediation instructions.

1.1 Engagement Objectives

NetSPI's primary goal within this engagement was to provide ACME, Inc. with an understanding of the current level of security that exists in their wireless configuration.

NetSPI completed the following objectives to accomplish this goal:

- Identified vulnerabilities and configuration weaknesses associated with the infrastructure wireless implementation
- Identified vulnerabilities and configuration weaknesses associated with the endpoint wireless implementation
- Compared ACME, Inc.'s current security measures with industry best practices
- Provided recommendations that ACME, Inc. can implement to mitigate threats and vulnerabilities and meet industry best practices.

1.2 Scope & Timeframe

Testing and verification were performed between July 08, 2024 and July 12, 2024. The scope of this engagement was limited to testing if unauthorized access could be obtained to in-scope infrastructure and client devices from the perspective of an anonymous attacker. All other tests including, but not limited to exploitation of software vulnerabilities, denial-of-service, and social engineering attacks were out of scope.

NetSPI conducted the tests using a production version of the wireless implementation. All other applications, servers, and networks were out of scope. All testing and verification were conducted remotely using a NUC placed in ACME, Inc.'s offices.

The following SSIDs were in scope:

SSID	IP RANGE
ACME-SECURE	Not Provided
ACME-BIOMED	Not Provided
ACME-GUEST	REDACTED
ACME-PROVIDER	REDACTED
ACME-WLAN	Not Provided
ACME-BYOD	REDACTED
ACME-BYOD-NET	REDACTED
ACME-EMPLOYEE	REDACTED
ACME-Clinical	Not Provided
ACME-Medical	Not Provided

NetSPI Sample
NetSPI Sample
NetSPI Sample

1.3 Summary of Findings

NetSPI's assessment of the ACME network revealed the following vulnerabilities:

- 2 high severity vulnerabilities
- 5 medium severity vulnerabilities
- 1 low severity vulnerability

VULNERABILITY NAME	SEVERITY
WPA/WPA2 PSK Enabled on Corporate Network	High
WPA2 PSK with PMKID Enabled	High
Open Wireless Network with a Captive Portal	Medium
Weak Configuration - Wireless Network Access Control Bypass - DNS Tunneling	Medium
Wireless Network - Undetected Control Bypass - MAC Spoofing on a Guest Network	Medium
Wireless Network - WPA/WPA2 PSK Enabled on an IoT/BYOD Wireless Network	Medium
WPA2 PSK with PMKID Enabled	Medium
Wireless Network - WPA/WPA2 PSK Enabled on an Untrusted/Guest Wireless Network	Low

TABLE 1: FINDINGS SUMMARY

NetSPI Sample
NetSPI Sample
NetSPI Sample

Chapter 2 | **Technical Detail**

2.1 **Overview**

The detailed findings section contains the analysis and documentation of the vulnerabilities identified within the wireless environment. This analysis included:

- Identifying vulnerabilities and configuration weaknesses associated with the infrastructure wireless implementation.
- Identifying vulnerabilities and configuration weaknesses associated with the endpoint wireless implementation.
- Comparing ACME, Inc.'s current security measures with industry best practices
- Providing recommendations that ACME, Inc. can implement to mitigate threats and vulnerabilities and meet industry best practices.

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 wireless network and its associated resources. The following table summarizes the three severity levels:

LEVEL	SEVERITY	DESCRIPTION
3	High	Vulnerabilities that result in unauthorized access to wireless networks, systems, or applications.
2	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.
1	Low	Vulnerabilities that result in the exposure version information or non-critical configuration information. Implementation of weak password policies and procedures. Informational findings that may not require any remediation.

TABLE 2: SEVERITY REFERENCES

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. As a result, the severity ratings in this document will not clearly represent the overall risk to an organization for each vulnerability instance.

Vulnerability Details: Comprehensive explanation of the vulnerability that was found, including a high-level summary of how the vulnerability works.

Affected Hosts and Services: Specific hosts and associated services on which the vulnerability was found.

Business Impact: The potential business impact of the vulnerability, should it be exploited.

Recommendation: NetSPI's solution for repairing the vulnerability or mitigating the problem if no fix is yet available.

Verification: Screenshot or sample data from one instance of the finding showing how NetSPI has verified the finding manually, when possible.

NetSPI Sample

NetSPI Sample

NetSPI Sample

References: Additional resources that have more information on the vulnerability. Resources may include vendor web sites or third-party announcements. These sources include those listed in Table 3.

CODE	DESCRIPTION	INFO
CERT	Computer Emergency Response Team advisory	www.cert.org
CVE	Common Vulnerabilities and Exposures	www.cve.mitre.org
BID	Bugtraq ID	www.securityfocus.com/bid/bugtraqid
MS	Microsoft Security Bulletins	www.microsoft.com
MSKB	Microsoft Knowledge Base	www.microsoft.com
USCERT	United States Computer Emergency Readiness Team advisory	www.us-cert.gov

TABLE 3: VULNERABILITY REFERENCES

Other external resource listings include vendor reference numbers for vulnerabilities and patches.

NetSPI Sample
NetSPI Sample
NetSPI Sample

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 a Wireless Network Penetration Testing engagement and see how our team can help you secure your wireless networks.

- 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!

© NetSPI Proprietary and Confidential