



Wifi Penetration Test

Prepared for: Sample Inc

COMPLETE REPORT

April 20, 2026

Red Sentry

This engagement was performed in accordance with the Statement of Work, and the procedures were limited to those described in that agreement. The findings and recommendations in this report reflect the systems, scope, and timeframe defined in the Statement of Work.

While every effort was made to provide thorough coverage, no security assessment can identify every possible issue, and results should not be interpreted as a guarantee of complete security.

Contact Information

+1 (888) 337-0467

hello@redsentry.com



TABLE OF CONTENTS

Summary.....	4
Project Overview.....	4
Goals.....	4
Dates.....	4
Findings.....	4
Scope.....	5
Tests Performed.....	6
Findings.....	7
Appendices.....	9

SUMMARY

Project Overview

Sample Company engaged Red Sentry to assess the security of their wireless networks. The following report details the findings identified during the engagement.

Goals

Identify vulnerabilities in the company wireless network from both external and internal perspectives.

Dates

April 08, 2026

April 08, 2026 - April 20, 2026

April 20, 2026

KICKOFF

TESTING PERIOD

DELIVERY

Findings Overview

During the assessment, the testing team identified multiple security findings across the environment.

A finding represents a unique security issue with a distinct root cause.

Instances represent the number of instances where that issue appears within the assessed environment.

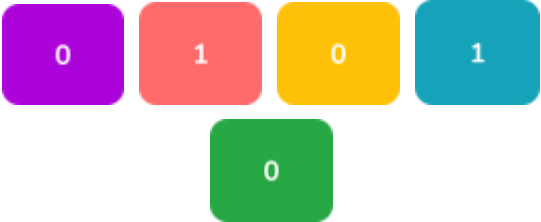
The following table summarizes the identified findings and the number of Instances observed during testing.

Severity	Finding ID	Instances
HIGH	TC3IS2W-F0002	2
LOW	TC3IS2W-F0001	1

Overall Grade



GRADE



Scope

- WIFI-CORP
- WIFI-GUEST

EXECUTIVE SUMMARY

The assessment team conducted a penetration test on the Sample Company's Wireless networks. Overall, the environment needs improvement as 3 issues were detected.

Regarding the severity of the findings, 2 instances of High vulnerability were found, these are related to the team being able to perform WPA2-PSK Password cracking.

Following the severity of the findings, 1 instance of low vulnerability was found. This is related to outdated software.

In summary, to improve the organization's security posture, the assessment team recommends changing periodically the wifi password, implementing better password policies, and updating software periodically.

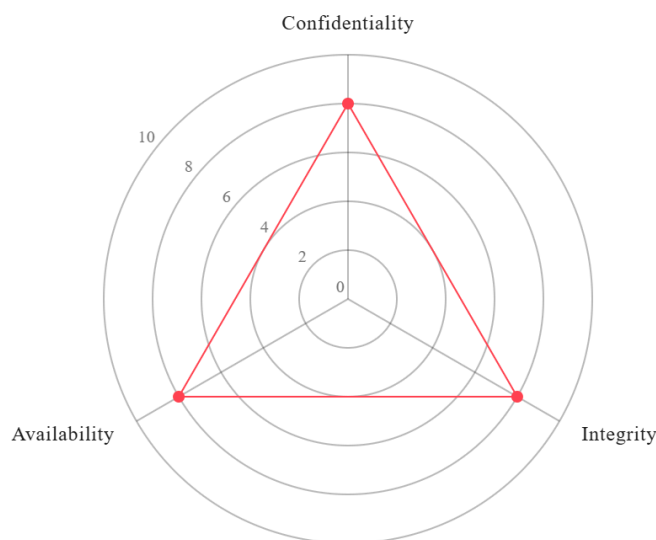


Figure 1: Security risk chart

As the image above shows, the overall risk value is low as the average score is 2.

As a general rule, an area below 4 shows low business impact, between 4 and 7 medium impact, and above 7 high impact.

Test Performed

For this project, the assessment team followed a black box approach to look for common vectors of attack in the target Wi-Fi networks.

Additional security settings

Some Wi-Fi routers have additional security measures, such as deauthentication attack prevention, which can make capturing handshakes more challenging.

Evil Twin attacks

An evil twin attack takes place when an attacker sets up a fake Wi-Fi access point hoping that users will connect to it instead of a legitimate one. When users connect to this access point, all the data they share with the network passes through a server controlled by the attacker.

Handshake capture

Traditional attacks on access points where PSK (pre-shared key) authentication mechanism is enabled. It is possible from an external perspective thanks to the fact that the 4-way handshake passes through the air and can be monitored by adjacent WiFi adapters in monitor mode.

```
===== Attack for Handshake =====
Interface wlan0 selected. Mode: Monitor. Supported bands: 2.4GHz, 5GHz
Selected BSSID:
Selected channel: 149
Selected ESSID:
Type of encryption: WPA2

Select an option from menu:
0. Return to Handshake tools menu
1. Deauth / disassoc attack
2. Deauth aireplay attack
3. WIDS / WIPS / WDS Confusion attack

*Hint* If the Handshake doesn't appear after an attack, try again or change the type of attack
> 1

Type value in seconds (10-100) for timeout or press [Enter] to accept the proposal [100]:
>

Timeout set to 100 seconds

Two windows will be opened. One with the Handshake capturer and other with the attack to force clients to reconnect

Don't close any window manually, script will do when needed. In about 100 seconds maximum you'll know if you've got the Handshake
Press [Enter] key to continue...
```

Figure 2: Reference handshake attack

It should be noted that this type of attack is not applicable to WPA2 Enterprise type of networks since they don't rely on a pre-shared key authentication schema.

The idea behind handshake capture is being able to use a wordlist and a brute-force tool to try to crack it and obtain the passphrase.

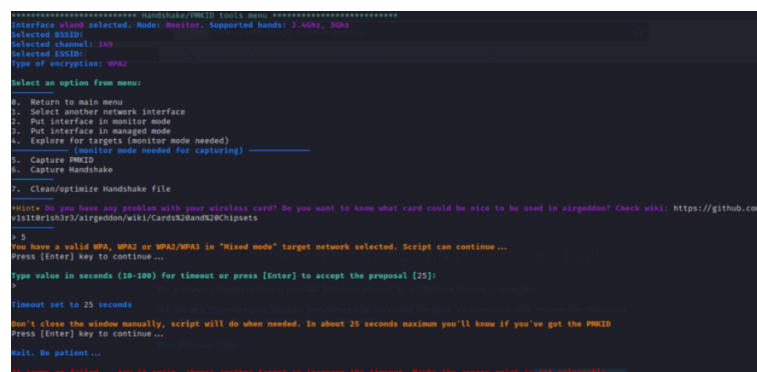
The inability to capture a handshake on a WPA2-PSK Wi-Fi network can be due to several factors.

Lack of traffic

If the network is inactive or has few connected devices, it may be difficult or impossible to capture a handshake.

PMKID capture

Relatedly, the PMKID is a similar attack to the previous one in terms of capturing data for posterior cracking and processing but the way the PMKID capture works it's different.



```
===== Handshake/PMKID tools menu =====
Interface wlan0 selected. Mode: Monitor. Supported bands: 2.4GHz, 5GHz
Selected BSSID:
Selected channel: 149
Selected ESSID:
Type of encryption: WPA2

Select an option from menu:
0. Return to main menu
1. Select another network interface
2. Put interface in monitor mode
3. Put interface in managed mode
4. Explore for targets (monitor mode needed)
5. Capture PMKID (monitor mode needed for capturing)
6. Capture Handshake
7. Clean/optimize Handshake file

Hint: Do you have any problem with your wireless card? Do you want to know what card could be nice to be used in airgeddon? Check wiki: https://github.com/
c101tBr1sh1r3/airgeddon/wiki/Cards%20and%20Chipssets

> 5
You have a valid WPA, WPA2 or WPA3/WPA3 in "Mixed mode" target network selected. Script can continue ...
Press [Enter] key to continue ...

Type value in seconds (10-100) for timeout or press [Enter] to accept the proposal [25]:
25
Timeout set to 25 seconds

Don't close the window manually, script will do when needed. In about 25 seconds maximum you'll know if you've got the PMKID
Press [Enter] key to continue ...

Built. Be patient ...

===== Done ===== Try it again, choose another target or increase the timeout. Maybe the access point is not vulnerable.
```

Figure 3: Reference PMKID attack

This attack doesn't rely on other users, so attackers don't need a third party to interact with the access point to be able to obtain the PMKID and, therefore, the data to be cracked.

Password cracking

This part is only possible if the needed data is captured in the preceding sections.

The assessment team couldn't successfully crack passwords, because no handshakes were captured.

Reconnaissance

After being connected to the network from which to pivot, the assessment team scanned to check which devices were part of the subnet.

Strong passwords

If the Wi-Fi network uses a strong and long WPA2-PSK password, it can make capturing a handshake through brute force attacks more difficult. Weak passwords are more susceptible to these attacks.

Vulnerability scanning

In order to check isolation, first the target network should be unreachable from the initial host and there's no possibility of lateral movement. To perform the latter, we need to assess vulnerabilities in the connected devices.

```
[~]
~$ ls
nmap_vulners_scan.txt  nuclei_2.9.12_linux_amd64.zip  targets
nuclei
nuclei-output.txt

[~]
~$ cat nuclei-output.txt
[xss-deprecated-header] [http] [info] 1; mode=block]
[xss-deprecated-header] [http] [info] [1; mode=block]
[xss-deprecated-header] [http] [info] [1; mode=block]
[xss-deprecated-header] [http] [info] [1; mode=block]
[xss-deprecated-header] [http] [info] [1; mode=block]
[xss-deprecated-header] [http] [info] [1; mode=block]
[xss-deprecated-header] [http] [info] [1; mode=block]
[xss-deprecated-header] [http] [info] [1; mode=block]
[xss-deprecated-header] [http] [info] [1; mode=block]
[xss-deprecated-header] [http] [info] [1; mode=block]
[xss-deprecated-header] [http] [info] [1; mode=block]
[xss-deprecated-header] [http] [info] [1; mode=block]
[ssl-issuer] [ssl] [info]
[ssl-dns-names] [ssl] [info]

[ssl-issuer] [ssl] [info]
[ssl-dns-names] [ssl] [info]
y.com]
[ssl-issuer] [ssl] [info]
[ssl-dns-names] [ssl] [info]

[ssl-issuer] [ssl] [info]
[ssl-dns-names] [ssl] [info]
```

Figure 4: Vulnerability scanning results

After conducting some vulnerability scanning using different tools and analyzing the results, there weren't any findings that could be exploitable in order to gain access to one of the target devices and the corporate network was unreachable from the Wi-Fi environment.

WPS Attacks

WPS uses a PIN as a shared secret to authenticate an access point and a client and provide connection information such as WEP and WPA passwords and keys; The attacks related to WPS were basically brute force attacks.

Wi-Fi Discovery Scan

Based on the test device position, the assessment team analyzes the Wi-Fi signals around its environment to locate and confirm reachability of the target SSIDs.

NUM	ESSID	CH	ENCR	PWR	WPS	CLIENT
1		6	WPA	99db	no	
2		8	WPA-P	76db	no	
3		6	WPA-P	71db	no	
4		6	WPA-E	70db	no	
5		6	WPA-P	70db	no	
6		149	WPA-P	70db	yes	
7		1	WPA-P	65db	yes	
8		60	WPA-P	65db	no	
9		60	WPA-P	65db	no	
10		1	WPA-E	61db	no	
11		6	WPA-P	60db	no	
12		1	WPA-P	59db	no	
13		1	WPA-P	59db	no	
14		157	WPA-E	57db	no	
15		157	WPA-P	56db	no	2
16		157	WPA-P	55db	no	1
17		149	WPA-E	53db	no	
18		149	WPA-P	52db	no	
19		149	WPA-P	52db	no	1
20		11	WPA-P	48db	no	
21		11	WPA-P	43db	no	
22		11	WPA-P	42db	no	

Figure 5: WiFi scan reference image

This initial scan was conducted by using standard built-in tools for Wi-Fi network recognition as well as specific tools. As the image above shows, the SSIDs available were the following:

#	SSID	Encryption	WPA
1	Non-business-network 1	WPA	no
2	Non-business-network 2	WPA-P	no
3	Non-business-network 3	WPA-P	no
4	WIFI-CORP	WPA-E	no
5	WIFI-GUEST	WPA-P	no

Figure 6: List of available SSIDs

Since the assessment team lacks some knowledge about the context of the available WiFi access points, it is recommended to give a closer inspection to this in order to spot any rogue access points that could be used to steal credentials.

Wifi Penetration Test Findings

WPA2-PSK PASSWORD CRACKING

HIGH

Identifier	TC3IS2W-F0002
Severity	High
Instances	2

Description

WPA2-PSK (Pre-Shared Key) is a common security protocol for WiFi networks. If the password is weak or commonly used, it can be cracked using brute force or dictionary attacks.

Instances (2)

- WIFI-CORP
- WIFI-GUEST

Evidence

The assessment revealed a significant vulnerability in the target network's WPA2-PSK security. The network's pre-shared key was susceptible to a brute-force attack due to its weak complexity.

```
***** Attack for Handshake *****
Interface wlan0 selected. Mode: Monitor. Supported bands: 2.4GHz, 5GHz
Selected BSSID:
Selected channel: 149
Selected ESSID:
Type of encryption: WPA2

Select an option from menu:
0. Return to Handshake tools menu
1. Deauth / disassoc anok md4 attack
2. Deauth aireplay attack
3. WIDS / WIPS / WDS Confusion attack

*Hint* If the Handshake doesn't appear after an attack, try again or change the type of attack

> 1

Type value in seconds (10-100) for timeout or press [Enter] to accept the proposal [100]:
1

Timeout set to 100 seconds

Two windows will be opened. One with the Handshake capturer and other with the attack to force clients to reconnect

Don't close any window manually, script will do when needed. In about 100 seconds maximum you'll know if you've got the Handshake
Press [Enter] key to continue...
```

Figure 7: Capturing Handshake

During the assessment, our team successfully captured the WPA2 handshake of the target network. The handshake was then subjected to a dictionary attack using a commonly available wordlist.

```
Aircrack-ng 1.7

[00:00:00] 400/477 keys tested (3716.26 k/s)

Time left: 0 seconds 83.86%

KEY FOUND! [ password123 ]

Master Key :

Transient Key :

EAPOL HMAC :
```

Figure 8: Password cracked

Within a few minutes, the password "password123" was successfully cracked, granting us unauthorized access to the network. This demonstrates that the network is highly vulnerable to external attacks, especially if the attacker possesses the appropriate tools and wordlists.

Steps for Recreation

1. Capture the Handshake with a tool like aireplay-ng using the following command:
 - `aireplay-ng — deauth 0 -a <MAC Address> <interface>`
2. To complete the attack, we need to obtain the key:
 - `Aircrack-ng <handshake> -w /usr/share/wordlists/rockyou.txt`

Recommendations

To mitigate the risk of this issue, the assessment team recommends the following steps

- Enforce strong, complex passwords (minimum 12 characters, including upper/lowercase letters, numbers, and symbols).
- Regularly change WiFi passwords and avoid using easily guessable phrases.
- Implement WPA3 if supported by devices, as it offers stronger encryption.

Resources

About Wi Fi security

<https://www.cybersecura.com/en/post/overview-of-attacks-and-threats-to-wifi-in-2022#:~:text=For%20WPA%2FWPA2%2DPSK%2C,by%20disabling%20Fast%20Roaming%20features>

OUTDATED SOFTWARE

LOW

Identifier	TC3IS2W-F0001
Severity	Low
Instances	1

Description

Outdated software arises when an asset is running an old version of a software. Applications are constantly being updated to fix security bugs and known vulnerabilities (CVEs) that attackers may be able to exploit. Older versions of software are more prone to be easily exploitable.

Instances (1)

- SSID:WIFI-CORP, Hostname: NB01.samplecompany.local,
127.0.0.1/ui/vropspluginui/rest/services/getstatus

Evidence

The assessment team discovered several instances of outdated software that contained known vulnerabilities (CVEs) in one of the in-scope assets. In the table below, we show the vulnerabilities associated with a certain technology version and its corresponding location.

Software	Version	Vulnerabilities	Locations
VMware vCenter Server SOAP API	6.7.0	CVE-2021-21972 CVE-2021-22005 CVE-2021-21985	SSID:WIFI-CORP, Hostname: NB01.samplecompany.local, 127.0.0.1/ui/vropspluginui/rest/serv ices/getstatus

Figure 9: List of vulnerabilities

Even though these vulnerabilities are regarded only as potential threats, it is strongly suggested that these pieces of software are patched and updated in a timely manner. The CVEs listed above are significant vulnerabilities impacting VMware products, each presenting critical security risks. CVE-2021-21972 is a remote code execution vulnerability in the VMware vSphere Client, allowing unauthenticated attackers to execute commands on the underlying operating system of affected servers. CVE-2021-22005 is another critical remote code execution flaw, this time in VMware vCenter Server and Cloud Foundation, enabling attackers to exploit file upload capabilities to execute code. Lastly, CVE-2021-21985 is a vulnerability in the VMware vCenter Server virtual SAN Health Check plug-in, which could allow remote attackers with network access to gain administrative privileges. Collectively, these vulnerabilities expose affected systems to severe risks, including unauthorized data access, system compromise, and potential operational disruptions, underscoring the need for prompt patching and heightened security measures.

Steps for Recreation

1. Perform a network discovery
2. Perform a open ports enumeration
3. Check the services running, and find vulnerabilities related to the services

Recommendations

To mitigate the risk of this issue, the assessment team recommends the following steps

- Update outdated software to the most recent version

Resources

OWASP Testing Guide

https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities

Unmaintained Third Party Components

<https://cwe.mitre.org/data/definitions/1104.html>

APPENDIX (A) SEVERITY DESCRIPTION

The assessment team used the following criteria to rate the findings in this report. Red Sentry derived these risk ratings from the industry and organizations such as OWASP.

The severity of each finding in this report is independent. Finding severity ratings combine direct technical and business impact with the worst-case scenario in an attack chain. The more significant the impact, and the fewer vulnerabilities that must be exploited to achieve that impact, the higher the severity.

Critical

A purple rounded rectangular badge with the word "CRITICAL" in white, uppercase letters.

Vulnerability is an otherwise high-severity issue with additional security implications that could lead to exceptional business impact. Examples: trivial exploit difficulty, business-critical data compromised, bypass of security controls, direct violation of communicated security objectives, and large-scale vulnerability exposure.

High

A red rounded rectangular badge with the word "HIGH" in white, uppercase letters.

Vulnerability may result in direct exposure including, but not limited to: the loss of application control, execution of malicious code, or compromise of underlying host systems. The issue may also create a breach in the confidentiality or integrity of sensitive business data, customer information, and administrative and user accounts. In some instances, this exposure may extend farther in the infrastructure beyond the data and systems associated with the application.

Medium

MEDIUM

Vulnerability does not lead directly to the exposure of critical application functionality, sensitive business and customer data, or application credentials. However, it can be executed multiple times or leveraged in conjunction with another issue to cause direct exposure. Examples include brute-forcing and client-side input validation.

Low

LOW

Vulnerability may result in limited exposure of application control, sensitive business and customer data, or system information. This type of issue provides value only when combined with one or more issues of a higher risk classification. Examples include overly detailed error messages, the disclosure of system versioning information, and minor reliability issues.

Informational

INFO

Finding does not have a direct security impact but represents an opportunity for additional layers of security, is considered a best practice, or has the possibility of turning into an issue over time. Finding is a security-relevant observation that has no direct business impact or exploitability, but may lead to exploitable vulnerabilities. Examples include poor communication between organizations, documentation encouraging poor security practices, or lack of security training.