**Wireless Security Assessment**

|  |  |
| --- | --- |
| **Client Name:** | **Dates of Assessment** |
| **Testers Name:** | **Client Contact:** |

Purpose of the Assessment:

|  |  |
| --- | --- |
| * Regulatory Requirement | * Contractual Requirement |
| * Suspected Compromise | * Risk Assessment |
| * Hardening Exercise | * Other |

Type of Wi-Fi Access

|  |  |
| --- | --- |
| * Café Style (No Auth, No Intranet) | * Authenticated (Auth Required, No Intranet) |
| * Integrated (Auth Required, Direct Intranet) |  |

Authentication

|  |  |
| --- | --- |
| * Open | * WPA/2 |
| * WEP | * WPA Enterprise |

Additional Controls

|  |  |
| --- | --- |
| * MAC Filtering | * Hidden ESSID |

List Access Points In Scope:

|  |  |  |
| --- | --- | --- |
| ESSID | BSSID | Channel |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

Were Any ESSID’s found matching the client’s naming convention but not listed in the client’s inventory (“Rogue” access points)?

* Yes
* No

If yes, list them here for future investigation.

Network Coverage Map

(Insert map showing signal coverage)

List All Likely Attack Locations

1. *Example: Sheraton Hotel upper floors*

Policy Review

* Acceptable Use Policy
* Wireless Segregation Policy
* Minimum Baseline Configuration for WAPs

**Password (Key)**

Pre-Shared Key Obtained:

* Yes
* No

Key Length

(A Wi-FI password can be anywhere from 8-64 characters and use any printable ASCII character)

* 8-10 characters (Higher Risk)
* 10-14 characters (Lower Risk)
* Greater than 14 (Lowest Risk)

Was the password found in any well-known word lists?

* Yes
* No

Is the password easily guessable (I.e. used client’s name, phone, etc)?

* Yes
* No

Key Complexity (n of 4)

1 of 4: High Risk

2 of 4: High Risk

3 of 4: Lower Risk

4 of 4: Lowest Risk

* Upper (A-Z)
* Lower (a-z)
* Numeric (0-9)
* Special (!@#$)

**Wi-Fi Protected Set-up (WPS)**

Is WPS enabled on any of the devices?

* Yes
* No

Note: WPS enabled devices can easily be identified using “wash –I mon0.”

WPS allows attackers to easily obtain the network key so should be disabled.

If WPS is enabled, is there a lock out period?

* Yes
* No

Note: If you find a device with WPS enabled, you can test for a brute force vulnerability using the reaver tool (reaver –I mon0 –b <bssid of target>)

**Unauthorized Devices**

Were there any rogue (unauthorized) devices or systems connected to the network?

* Yes
* No

Note: Only complete this if there is governance prohibiting unauthorized devices and only scan the network if this is part of the scope of work (SOW). To identify unauthorized devices run nmap –O followed by the IP range.

Were there any access points found attached to the network not on the client’s inventory list? (“Rogue” access points)?

* Yes
* No

If yes, list them here for future investigation.

**Segregation**

Was the management console accessible without a physical connection?

* Yes (Higher Risk)
* No (Lower Risk)

Was the client’s intranet accessible directly from the wireless network?

* Yes (Higher Risk)
* No (Lower Risk)
* N/A

Is there a DMZ enabled?

* Yes
* No

If yes and if authorized list the devices found in the DMZ.