6300 Corporate Blvd. Suite 200
Baton Rouge, LA 70809
Phone: 225-612-2122
www.tracesecurity.com

Wireless Assessment Report

Organization Name

Date

TraceSecurity

tracesecurity

Table of Contents

tracesecurity

List of Figures

tracesecurity

Document Information

Company	Organization Name
Document Title	Wireless Assessment Report
Date	Date
Classification	Confidential
Document Type	Private

Document Recipients		
Name	Title	Organization
Client Contact Name	Client Contact Title	Organization Name

Document History		
Date	Author	Comments
Date	TraceSecurity	Final

Project Definition

Definition

During the engagement, the ISA reviewed the security features of the wireless network. The ISA reviewed manuals, policies, and procedures for the wireless implementation. The goals of the test also included emulating attacks attempting to breach the wireless network from an attacker's perspective. For this security testing, the evaluators attempt to circumvent the security features of the wireless access points.

Objective

The objective of this engagement is to provide an analysis of the current security program and counter measures implemented at ORGANIZATION NAME. This is achieved by predefining a goal (i.e. circumvent existing firewall and obtain critical data from core processing system), reporting whether that goal was achieved, providing proof of obtaining the defined goal, and documenting the exact process.

Many tools that will be utilized in the engagement are available via the Internet. These tools include mundane programs such as ping, NsLookup, Sam Spade, web browsers, and more complex utilities such as:

Example Tools Used During Engagement

Port Scanners: Zenmap	Anti-Firewall: Zenmap
Sniffers: Wireshark	Wireless Tools: Aircrack-ng, Kismet
Password Crackers: Aircrack-ng	Banner Grabbing Utilities: Netcat

Executive Summary

Executive Summary of Wireless Penetration Test Results

TraceSecurity has just completed a Wireless Assessment of the operational implementation of the ORGANIZATION NAME's wireless networks. The TraceSecurity Information Security Analyst (ISA) utilized a variety of real-world techniques for subverting security controls applied for the protection of the wireless networks and sensitive information. Testing coverage included a suite of widely known and freely available attack methods to complete testing of the wireless networks.

ORGANIZATION NAME provided the ISA with the wireless network names (SSIDs) to be included as part of this testing. Please refer to the Network Mapping section of this report to review the entire list. The ISA performed vulnerability analysis, exploitation, and post-exploitation based on any possible or confirmed vulnerabilities.

The results of this testing indicate that the wireless networks are well secured against many different attack vectors. The majority of vulnerability findings were minor in risk level and mostly attributed to the operational implementation of the wireless networks rather than their security. The testing did not result in any possible access to the internal network, however, the ISA was able to obtain unauthorized access to the guest network. While not deemed High Risk, the most significant areas of concern included weak complexity for the passphrase to authenticate to the guest wireless network and the over transmittal of the effective wireless broadcast range of both of the wireless networks.

The most significant issues are listed below, with additional details and recommendations included in the body of the report. Vulnerabilities should always be addressed in the order of risk level and corresponding criticality of the system or service. Resolving the issues detailed within this report will help to further harden wireless networks against attacks in order to strengthen the organization's overall information security posture.

Remediation Priorities:

- Weak/Default Passwords on Guest Wireless - Medium Risk - The guest wireless network is currently configured with a weak passphrase in order to authenticate the network. Acquiring unauthorized access to this network could allow for an attacker to compromise sensitive information or systems. The ISA also identified cases where some accounts are configured with default credentials to obtain access to an application or service accessible from the guest wireless network. Utilizing weak passwords or default credentials allows an attacker to easily attempt further exploitation of systems and services in order to gain access to sensitive information, interrupt or change the functionality of a device or system, or even compromise the system itself. TraceSecurity recommends ensuring that the guest wireless network passphrase is configured with a strong, complex password as well as ensuring that all system and service default usernames and passwords are changed or disabled. The organization should implement strong, complex passwords for any administrator level accounts.
- Over-Transmittal of Broadcast Range - Low Risk - Wireless network access points are configured to transmit signal strength well beyond the organization's operating floors and building premises. This allows for much easier visibility of the wireless networks to attackers as well as more concealed means of attacking the networks while remaining unnoticed. TraceSecurity recommends reviewing and testing necessary transmit power levels of the APs in order to limit their effective broadcast range within the boundaries of the three office space floors assigned to the organization.

tracesecurity

Section 1: Network Mapping

This section identifies the network resources and services included in the scope for wireless penetration testing. It is focused on technical aspects of the organization's wireless network deployment.

The expected results are the following:

- Target Wireless Access Points
- Wireless Access Point Identification

During the assessment the ISA performed scanning and testing against the following access points:

Figure 1: Target Wireless Access Points

The ISA configured his wireless adapter for monitoring mode and utilized his standard wireless network adapter as well as an Alfa card to begin monitoring for the Wireless Network access points (APs) included in the scope of wireless penetration testing. The ISA identified both APs and confirmed that they were available via a number of different wireless connection channels, as seen in Figure 2.

Figure 2: Wireless Networks - Access Point Identification

```
CH  5 ][ Elapsed: 2 mins ][ 2017-07-17 10:05

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

                   -21       92        0    0  10  54e. WPA2 CCMP   MGT
                   -22      110        0    0  10  54e. WPA2 CCMP   PSK
                   -21      101        0    0  11  54e. WPA2 CCMP   MGT
                   -22      109        2    0  11  54e. WPA2 CCMP   PSK
                   -45      172        0    0   7  54e. WPA2 CCMP   PSK
                   -45      175        0    0   7  54e. WPA2 CCMP   MGT
                   -48       84        0    0   5  54e. WPA2 CCMP   MGT
                   -48       80        0    0   5  54e. WPA2 CCMP   PSK
                   -51       88        0    0   1  54e. WPA2 CCMP   MGT
                   -51      100        0    0   8  54e. WPA2 CCMP   PSK
                   -51       93        0    0   8  54e. WPA2 CCMP   MGT
                   -52       91        0    0   1  54e. WPA2 CCMP   PSK
                   -53       86       18    0   9  54e. WPA2 CCMP   PSK
                   -53       91        0    0   9  54e. WPA2 CCMP   MGT
                   -54      117        0    0   6  54e. WPA2 CCMP   PSK
                   -54      127        0    0   6  54e. WPA2 CCMP   MGT
                   -55       20        1    0   5  54e. WPA2 CCMP   PSK
                   -55       73        0    0   5  54e. WPA2 CCMP   MGT
                   -55       65        0    0   4  54e. WPA2 CCMP   MGT
                   -56       61        0    0   4  54e. WPA2 CCMP   PSK
```

This screenshot provides a brief overview of the activities performed during the mapping phase of wireless penetration testing. Additional scanning and enumeration attempts were performed in order to further verify and fingerprint configurations of the wireless networks

tracesecurity

Section 2: Vulnerability Analysis

This section utilizes information gathered from the previous phases of testing and outlines the attempts to gain any unauthorized access to wireless network deployments in order to verify vulnerabilities present on the networks.

During this phase of testing, the ISA attempts to confirm any configuration issues on wireless devices, capture wireless handshakes, attempt to brute-force and/or dictionary attacks against Pre-Shared Keys (PSKs) or user account password hashes, and much more.

Vulnerability findings verified after further analysis and evaluation are included below. Each finding is categorized by vulnerability type, risk rated, and presented with notes, supporting documentation, and a recommendation. The vulnerabilities are listed in order from the highest risk to the lowest. TraceSecurity encourages the organization to review each of the findings presented and document remediation plans in cases where the risk level is unacceptable.

Weak/Default Passwords on Guest Wireless - Medium Risk

The guest network ([redacted]) is currently configured with a weak passphrase, and default credentials for some application or service accounts were discovered.

The internal wireless network ([redacted]) utilizes 802.1x with a custom RADIUS configuration in order to secure and authenticate connections, thus preventing any attack vectors to compromise the authentication scheme for that wireless network deployment. However, the guest wireless network uses a pre-shared key (PSK) for authentication which only requires entering of a passphrase. The current passphrase lacks complexity and has a short character length. Poorly constructed passphrases can result in the ability to obtain unauthorized access to and use of the wireless network, which would then allow for an attacker to directly attack any unsuspecting victims who are also connected to the guest wireless network and could even permit the compromise of sensitive information on their systems or in their wireless network traffic. Often times, having a strongly configured passphrase for a wireless deployment can make the difference in preventing a successful compromise of sensitive information or systems on this wireless network. Default credentials on service accounts often occur due to gaps in system hardening processes or system redeployment/reconfiguration processes. An attacker can use the presence of this vulnerability to attempt privilege escalation techniques, acquire access to sensitive information, or interrupt/change the functionality of a service or system.
As seen in the following figures the ISA was able to monitor wireless network traffic for the guest wireless deployment, send deauthentication packets to a system/device currently connected to a wireless access point in order to obtain an encrypted version of the passphrase, and then successfully crack the encrypted passphrase.

Figure 3: [redacted] - Monitoring Wireless Network Traffic

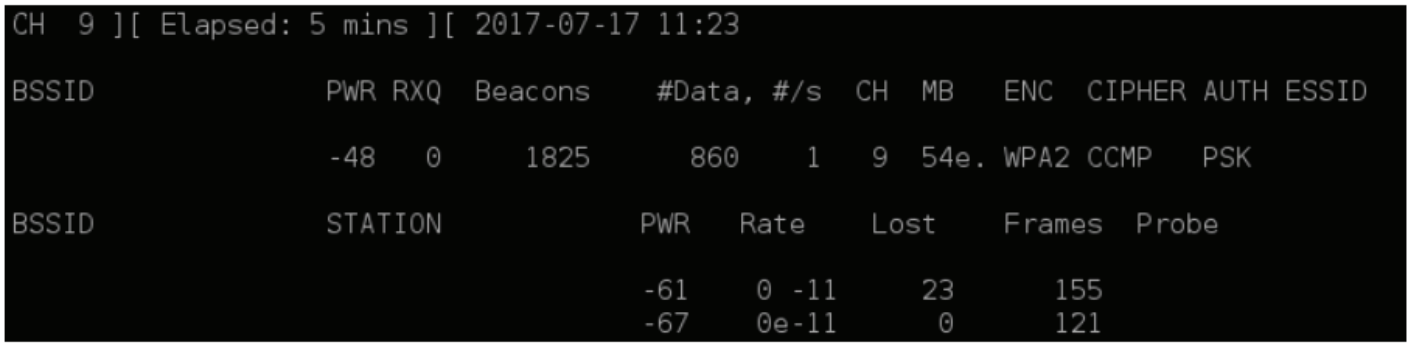


Figure 4: [redacted] - Sending Deauthentication Packets to AP

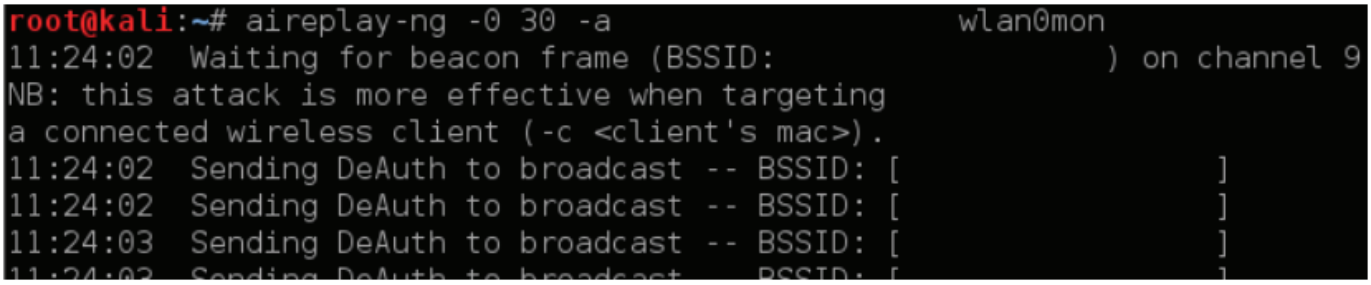


Figure 5: [redacted] - Acquired WPA Handshake to AP by Device

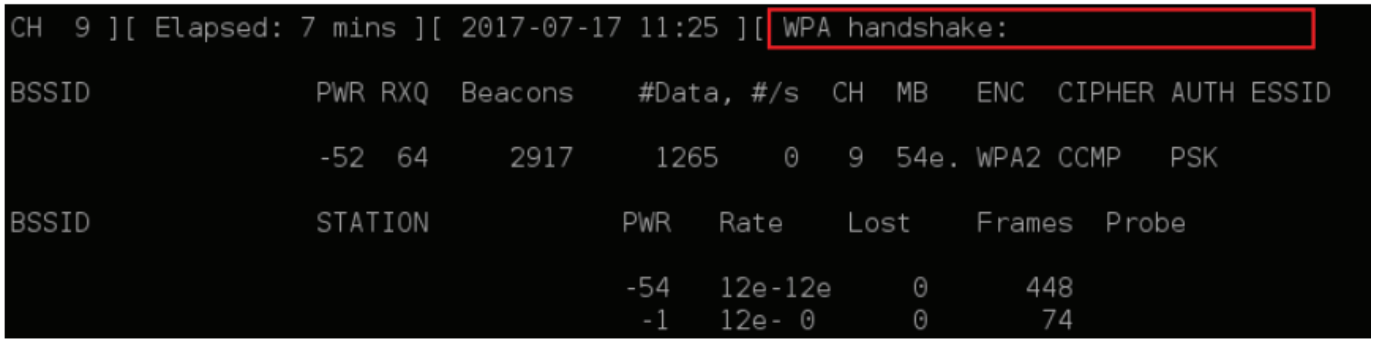


Figure 6: [redacted] - Verification of Encrypted Passphrase Obtained

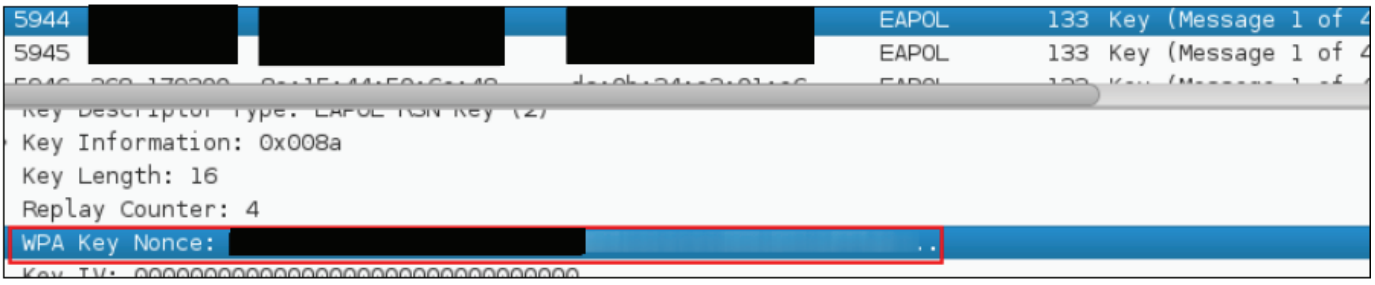


Figure 7: [redacted] - Dictionary Attack Passphrase Crack Successful

```
root@kali:~# cowpatty -r tp     -02.cap -f darkc0de.lst -s "       "
cowpatty 4.6 - WPA-PSK dictionary attack. <       @       .com>

Collected all necessary data to mount crack against WPA2/PSK passphrase.
Starting dictionary attack.  Please be patient.
key no. 1000: 0177161455
key no. 2000: 0b574c13
key no. 3000: 0n100kin6
key no. 4000: 0u7v41u3
key no. 5000: 0v3127im0120u5n355
key no. 6000: 0v312p3n5iv3
key no. 7000: 1 AR
key no. 8000: 1 BER
key no. 9000: 1 BF
key no. 10000: 1 CHI
key no. 11000: 1 DEF
key no. 12000: 1 EL

The PSK is "          ".

12831 passphrases tested in 61.68 seconds:  208.03 passphrases/second
```

This allowed the ISA to establish a legitimate connection to the guest wireless network. Again, this unauthorized access can be used to attack other systems or devices also connected to the guest wireless, consume available bandwidth of the Internet connection for malicious or unlawful purposes, or even attack organization systems and services if accessible. As seen in the following figures, the ISA also discovered default passwords configured for accounts providing some different services for the organization. The majority of available services were tested but not all of them, however, each account configured on these services should be considered as included within the recommendations to follow.

Figure 8: Web Services - Available Hosts Scan

```
################################################################################
#                              EyeWitness v1.0                                 #
################################################################################

Trying to screenshot 36 websites...

Attempting to capture: http://192.        /
Attempting to capture: http://192.         /
Attempting to capture: http://192.         /
```

Figure 9: Web Host - Default Password Sample 1

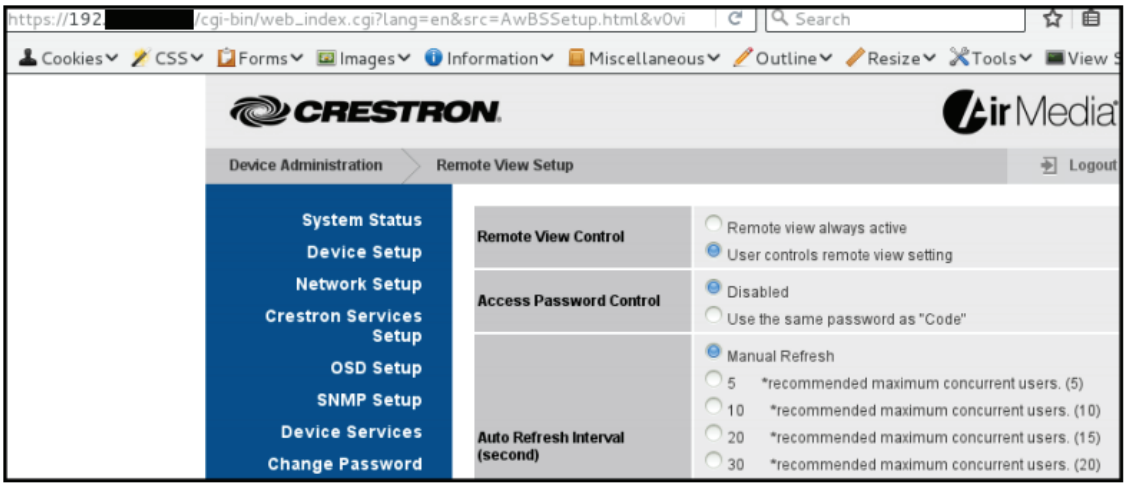
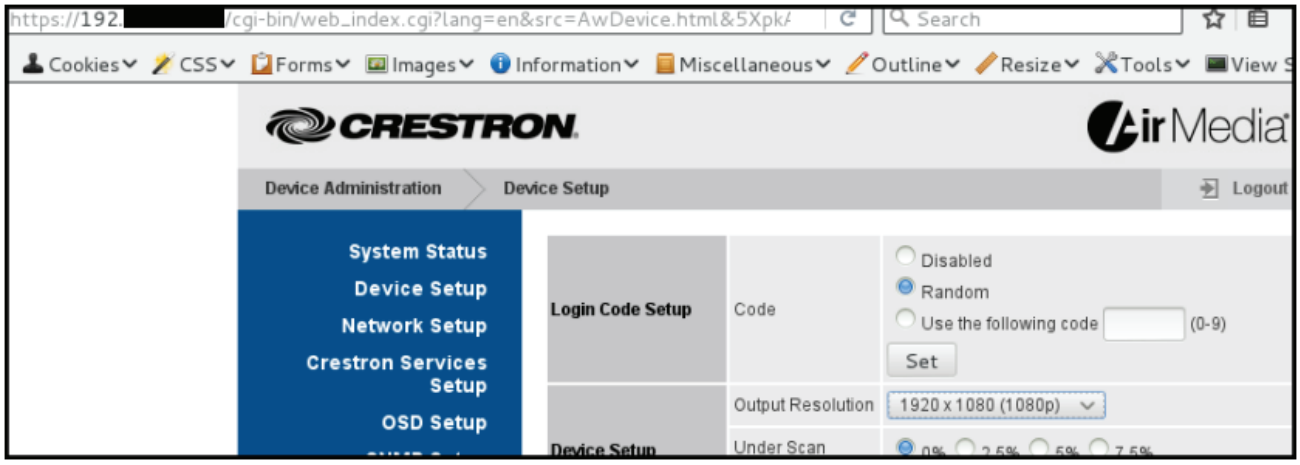


Figure 10: Web Host - Default Password Sample 2



Recommendations

TraceSecurity recommends ensuring that the guest wireless network PSK is configured with a strong, complex passphrase. It should also be noted that this PSK passphrase is available in hard copy and left on some conference room tables, which could be acquired by unauthorized and unrecorded physical access to the 9th floor office space locations of the organization. Therefore, TraceSecurity further recommends that once this passphrase is changed to a value that is more complex, the organization also refrains from providing this passphrase in any hard copy form around the facility premises. TraceSecurity also recommends disabling or renaming default administrator accounts on all interfaces that would allow for a user to modify or view critical system functionality. Furthermore, these implemented passwords should conform to the organization's existing password standards, such as complexity, minimum length, and maximum age. In cases where an interface cannot be configured with strong passwords due to application limitations, TraceSecurity recommends implementing IP-based access rules/filters that would restrict access to these interfaces to a limited scope of IP addresses specific to an admin's system only. Implementing these processes will substantially reduce the effectiveness of any related password-based attacks.

Over-Transmittal of Broadcast Range - Low Risk

During the TX power assessment, it was determined that the gain settings for the wireless APs are configured to spread the signal beyond the three office floor's physical boundaries.

A wireless AP's transmit range (or signal strength) can be set to a variety of levels in order to broadcast wireless network access to a more widespread area. If the broadcast range transmittal is set too high, it allows the wireless network to be much more visible to attackers and will allow them to attempt to compromise the network from distances further away from the organization's facility and in more concealed settings to remain unnoticed.

As seen in the following figures, the wireless APs are configured to transmit signal strength will beyond the organization's premises, including to areas at ground level, floors on lower levels, and even a neighboring parking lot across the street. The [redacted] wireless network transmit strength was well received in all of the testing locations, while the [redacted] wireless network connectivity was intermittent for some of the locations. The signal strengths were measured using an Alfa Wireless Card extender.

Figure 11: Map of Signal Testing Locations

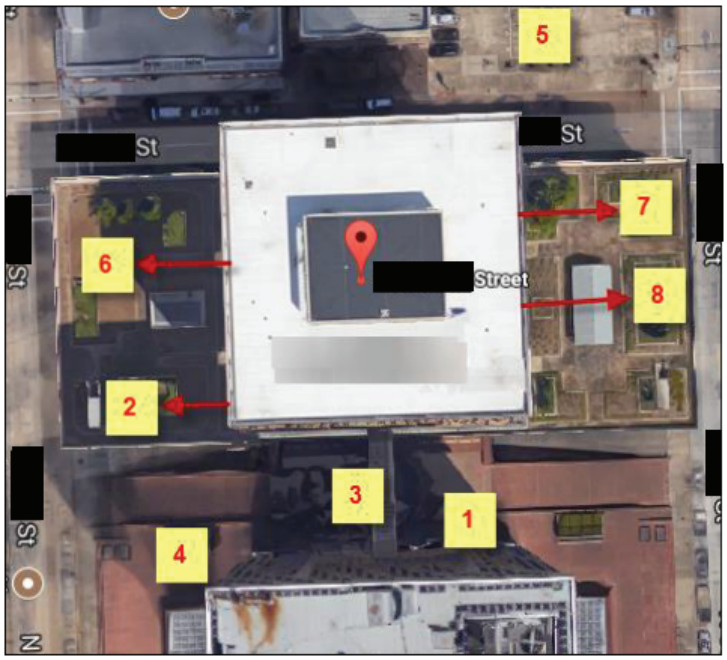


Figure 12: Wireless Signal Strength - Location 1

```
CH  4 ][ Elapsed: 1 min ][ 2017-07-17 15:23 ][

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

                   -47        6        3    0   9  54e. WPA2 CCMP   PSK
                   -53       10        0    0   3  54e. WPA2 CCMP   MGT
```

Figure 13: Wireless Signal Strength - Location 2 - First Floor Suite 102

```
CH  3 ][ Elapsed: 4 mins ][ 2017-07-17 15:29

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

                   -46       25       12    0   9  54e. WPA2 CCMP   PSK
                   -51        1        0    0   3  54e. WPA2 CCMP   PSK
                   -53        5        0    0   4  54e. WPA2 CCMP   MGT
```

Figure 14: Wireless Signal Strength - Location 3

```
CH  5 ][ Elapsed: 8 mins ][ 2017-07-17 15:43 ][

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

                   -55        1        0    0   3  54e. WPA2 CCMP   PSK
                   -46        6        3    0   9  54e. WPA2 CCMP   PSK
```

Figure 15: Wireless Signal Strength - Location 4

```
CH 10 ][ Elapsed: 2 mins ][ 2017-07-17 15:33

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

                   -55        1        0    0   3  54e. WPA2 CCMP   PSK
                   -51        5        5    0   9  54e. WPA2 CCMP   PSK
```

Figure 16: Wireless Signal Strength - Location 5

```
CH  3 ][ Elapsed: 4 mins ][ 2017-07-17 15:39 ][

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

                   -48        6        0    0   6  54e. WPA2 CCMP   MGT
                   -42        1        0    0   6  54e. WPA2 CCMP   PSK
```

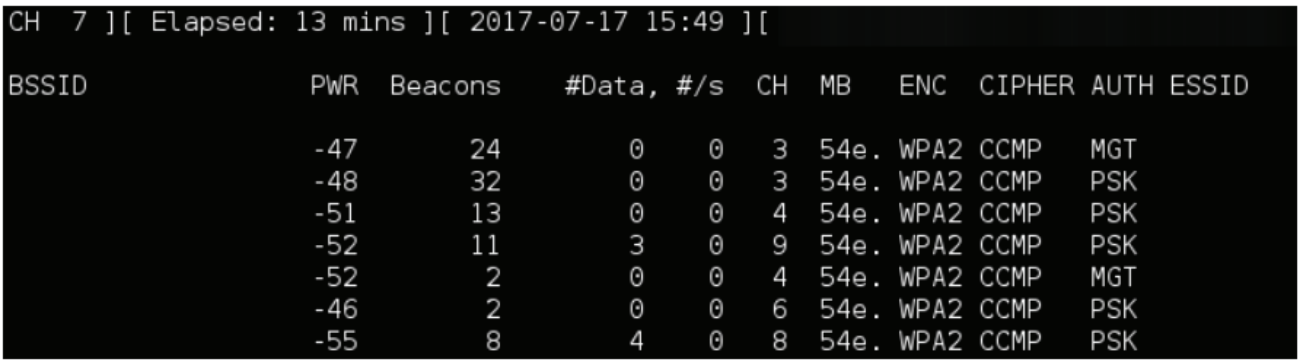
Figure 17: Wireless Signal Strength - Location 6 - Fourth Floor Parking Garage

```
CH  3 ][ Elapsed: 11 mins ][ 2017-07-17 15:46 ][

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

                   -57        8        0    0   3  54e. WPA2 CCMP   MGT
                   -58        8        0    0   3  54e. WPA2 CCMP   PSK
```

Figure 18: Wireless Signal Strength - Location 7 - Fifth Floor Parking Garage

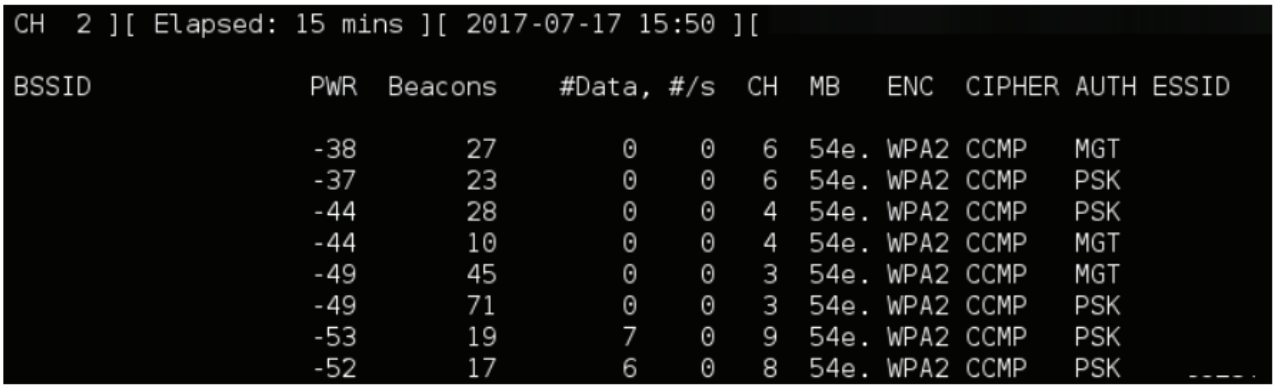


```
CH  7 ][ Elapsed: 13 mins ][ 2017-07-17 15:49 ][

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

                   -47       24        0    0   3  54e. WPA2 CCMP   MGT
                   -48       32        0    0   3  54e. WPA2 CCMP   PSK
                   -51       13        0    0   4  54e. WPA2 CCMP   PSK
                   -52       11        3    0   9  54e. WPA2 CCMP   PSK
                   -52        2        0    0   4  54e. WPA2 CCMP   MGT
                   -46        2        0    0   6  54e. WPA2 CCMP   PSK
                   -55        8        4    0   8  54e. WPA2 CCMP   PSK
```

Figure 19: Wireless Signal Strength - Location 8 - Seventh Floor Parking Garage



```
CH  2 ][ Elapsed: 15 mins ][ 2017-07-17 15:50 ][

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

                   -38       27        0    0   6  54e. WPA2 CCMP   MGT
                   -37       23        0    0   6  54e. WPA2 CCMP   PSK
                   -44       28        0    0   4  54e. WPA2 CCMP   PSK
                   -44       10        0    0   4  54e. WPA2 CCMP   MGT
                   -49       45        0    0   3  54e. WPA2 CCMP   MGT
                   -49       71        0    0   3  54e. WPA2 CCMP   PSK
                   -53       19        7    0   9  54e. WPA2 CCMP   PSK
                   -52       17        6    0   8  54e. WPA2 CCMP   PSK
```

Recommendations

TraceSecurity recommends reviewing and testing necessary transmit power levels of the APs in order to limit their effective broadcast range within the boundaries of the facility premises. TraceSecurity also recommends considering the use of directional antennas which will help focus the RF energy to more defined areas within the facility rather than omnidirectional antennas which spread RF energy equally in all directions.

Section 3: Wireless Network Configuration Assessment

Provided is an overview of the wireless network configuration and implementation of the organization. These items may have been confirmed through technical testing, observation of the configuration of devices or documentation, or through interviews with internal personnel. The table below provides details of each control item reviewed, their implementation status, and recommendations in the case of unimplemented or partially implemented controls.

Control Name	Control Status	Control Notes
Authorization Process for Access	Partially Implemented	[redacted] does not follow a standard and documented process for granting or allowing access to this wireless network. [redacted] has a semi-formal process established, however, it lacks consistency, as some requests are received via ticket, email, or verbal communication. TraceSecurity recommends establishing a more formal authorization process for granting access to the wireless networks.
Documentation of Access Approval	Partially Implemented	[redacted] access approval is not documented, as the passphrase is openly distributed since it is an Internet access wireless network only. [redacted] access approval is documented on occasion via ticket or email, however, it does not follow a standard process for access assignment and approval that would require maintaining such records. TraceSecurity recommends documenting all approval and distribution of [redacted] access assignment to employees in a ticket when access is granted to the wireless network.
Centrally Control and Distribute Internal Network Access to End-Users	Implemented	[redacted] access is provided to employee laptops once their Active Directory account is placed in the appropriate Domain group.
Configure Strong Complexity for Any Password-based Access	Not Implemented	The passphrase assigned for the [redacted] network is weak and susceptible to cracking due to the lack of complexity and short character length. TraceSecurity recommends configuring the wireless network with a strong, complex passphrase.
Rotate Any Password-based Access on a Regular and Frequent Basis	Not Implemented	The passphrase for [redacted] has not been changed in several years. This allows previous employees, contractors, guests, and any other users with knowledge of or the ability

		to crack the weak passphrase to use the Internet connection freely at their disposal while within range. TraceSecurity recommends ensuring that the passphrase for [redacted] is changed on a frequent basis (such as monthly or quarterly) as well as ensuring that no previously used passphrases are reused again in the future during the regular rotation.
Use Strong Encryption	Implemented	[redacted] and [redacted] are configured to use WiFi Protected Access 2 (WPA2) with strong encryption.
Limit/Prevent Guest Wireless Network Access to the Internal Network	Implemented	[redacted] is properly segmented and restricted from accessing the internal network.
Restrict Visibility or Access	Not Implemented	Wireless network access points (APs) are configured to transmit signal strength well beyond the organization's premises. SSIDs are hidden for [redacted] but openly broadcast for [redacted]. TraceSecurity recommends reducing transmit power levels of the APs in order to limit their effective broadcast range within the boundaries of the organization's assigned floor premises.
Configure Terms of Use Banner for Connections	Not Implemented	Initial connections to [redacted] and [redacted] do not result in a landing page confirming any formal user agreement or disclaimer of accessing and using the wireless network. Since this traffic also does not pass through the web content filter, TraceSecurity recommends configuring an official terms of use landing page to be presented when end-users initially establish connection to the wireless network to cover such items as no expectation of privacy, security, etc. TraceSecurity further recommends configuring this wireless network to pass all traffic through a web content filtering and firewall solution and to ensure the wireless network is not used for any malicious or illegal purposes.

Appendix

This section outlines some of the additional testing performed by the ISA that may or may not have led to the successful compromise of wireless networks or sensitive information. Each testing item is categorized and presented with supporting documentation. Details are outlined within the title's description.

Unsuccessful Attack Vectors

Figure A1: [redacted] - Dictionary Attack Passphrase Crack Attempt Unsuccessful 1

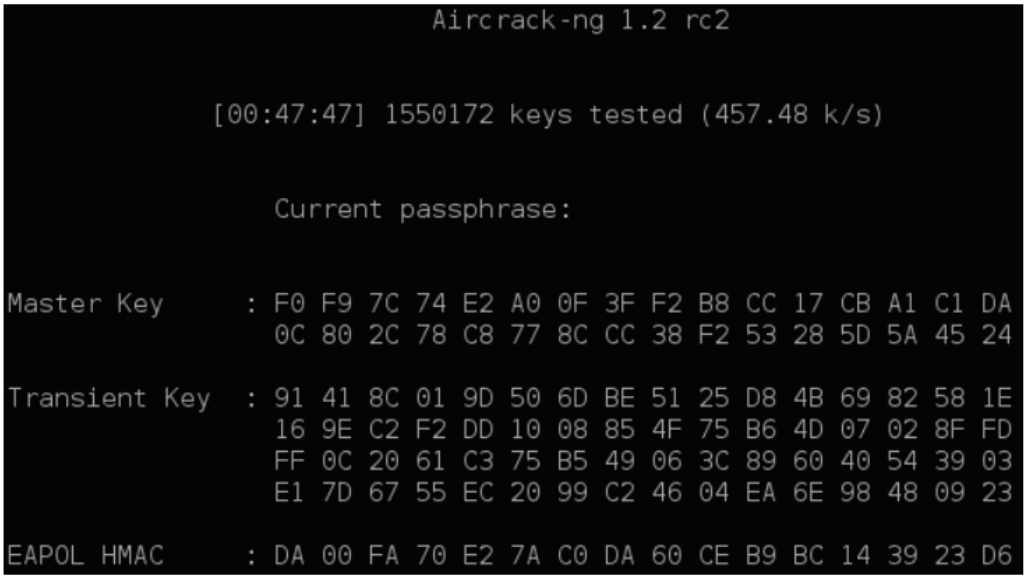


Figure A2: [redacted] - Dictionary Attack Passphrase Crack Attempt Unsuccessful 2