WIRELESS ANALYSIS AND ASSESSMENT TOOL

BY

GARY CHOI

A THESIS (AN ADVANCED DESIGN PROJECT) SUBMITTED TO THE FACULTY OF SAINT MARTIN’S UNIVERSITY IN PARTIAL FULLFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF CIVIL ENGINEERING

SAINT MARTIN’S UNIVERSITY

DATE

CSC 598(3) CERTIFICATE OF APPROVAL

WIRELESS ANALYSIS AND ASSESSMENT TOOL

BY

GARY CHOI

Contents

1. [**Abstract** **4**](#Abstract)
2. [**Disclaimer** **4**](#Disclaimers)
3. [**Purpose** **5**](#Purpose)
4. [**Terminology** **6**](#Terminology)
5. [**Vulnerability Criteria** **7**](#Vulnerability)

[**5.1 Evil Twin** **7**](#Vulnerability_Evil)

[**5.2 Encryption** **8**](#Vulnerability_Encryption)

[**5.3 Cipher** **10**](#Vulnerability_Cipher)

1. [**Process** **12**](#Process)

[**6.1 Confirming the Environment** **12**](#Process_Confirming)

[**6.2 WLAN to Scanning Mode** **14**](#Process_WLAN)

[**6.3 Scanning** **15**](#Process_Scanning)

[**6.4 Recover** **16**](#Process_Recover)

[**6.5 Result** **16**](#Process_Result)

1. [**Usage** **23**](#Usage)
2. [**References** **25**](#Reference)

**Abstract**

This project will produce the Wireless Analysis and Assessment Tool using the network software, Aircrack-ng with python. Aircrack-ng consists of a detector, packet sniffer, WEP/WPA/WPA2-PSK cracker with analyzing 802.11 wireless LANs. This tool can be significantly beneficial for users to assess their wireless security and prevent Wi-Fi Attacks. However, it requires users to have a great understanding of physical networking interfaces, Wireless networks, 802.11 Security, Linux, and much more. By producing an automated Wireless Analysis and Assessment Tool, anyone with a Linux client will be able to perform the following: the assessment and detection of wireless vulnerabilities by navigating the User Interface and providing suggestions to the user.

**Disclaimers**

The information presented in this document is provided as-is and without warranty. Vulnerability assessments are a “point in time” analysis, and as such, it is possible that something in the environment could have changed since the result when the program was run. Also, it is possible that new vulnerabilities may have been discovered since the tests were run. Also, this program must be used at authorized locations on authorized devices.

**Purpose**

Wi-Fi is one of the most common ways to access to internet from a mobile device. Anyone would probably be able to find Wi-Fi from almost anywhere, considering that most households, malls, coffee shops, and even some transportation have Wi-Fi hotspots available. However, according to the article, security expert discovers that all Wi-Fi networks are vulnerable to hacking (Hern, 2017). This program will allow the user to analyze and assess the Wireless Access Point to check if the device is compromised and its vulnerability.

**Terminology**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| BSSID | BSSID is a basic service set identifier which is a 48-bit label that conforms to MAC-48 conventions. An infrastructure BSSID is usually non-configurable, in which case it is either preset during manufacture or mathematically derived from a preset value such as a serial number or a MAC address of another network interface. |
| ESSID | The ESSID is an electronic marker or identifier that serves as an identification and address for your computer or network device to connect to a wireless router or access point and then access the internet. |
| FI | FI(Financial Information) is data about the monetary transactions of a person or business.  Ex) Your credit card information, bank information, PayPal credential, etc. |
| MITM | MITM(Man in the Middle) attack is a cyberattack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other, as the attacker has inserted themselves between the two parties. |
| PHI | PHI(Protected Health Information) is any information in a medical record that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service, such as a diagnosis or treatment. |
| PII | PII(Personal Identifiable Information) is any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. |
| Session Hijacking | Session hijacking, sometimes also known as cookie hijacking, is the exploitation of a valid computer session—sometimes also called a session key—to gain unauthorized access to information or services in a computer system. |
| Sudo | sudo is a program for Unix-like computer operating systems that enables users to run programs with the security privileges of another user, by default, the superuser. It stands for “superuser do” |
| WAP | WAP(Wireless access point) is a networking hardware device that allows other Wi-Fi devices to connect to a wired network. |
| Wlan | WLAN (A wireless LAN) is a wireless device network that links two or more devices using wireless communication to form a local area network (LAN). |

**Vulnerability Criteria**

1. Evil Twin

*Description*

An evil twin is a fraudulent Wi-Fi access point that appears to be legitimate but is set up to eavesdrop on wireless communications. The evil twin is the wireless LAN equivalent of the phishing scam. This type of attack may be used to steal the passwords of unsuspecting users, either by monitoring their connections or by phishing, which involves setting up a fraudulent website and luring people there. (Security, What is an evil twin attack? 2021)

*Risks*

Evil twin attacks pose a significant cybersecurity risk for both end-users and businesses. (Security, What is an evil twin attack? 2021)

*Possible Damage*

To USERS

Hackers often use evil twin attacks to gain access to personal user data like login credentials, bank transactions, and credit card information. This is especially dangerous for users who use the same username and password for multiple accounts since the hacker could gain access to all of them by monitoring just one login attempt. (Security, What is an evil twin attack? 2021)

To Business

If a user logs into their company’s portal while connected to an evil twin network, the hacker can gain access to the company website using the employee’s credentials. This poses a significant cybersecurity risk as hackers can then access company data or plant malware in the system. (Security, What is an evil twin attack? 2021)

*Suggestion*

1. Disable auto-connect features in your devices

If auto-connect features are on, the device will connect to the hacker device when the hacker attacks WAP.

2. Avoid using Sensitive information (Personal Identifiable Information, Financial information, Protected Health Information, etc.)

Hackers could capture the data you send.

3. Use VPN

VPN encrypts your data on the internet. (Ensure to use secure VPN service with strong encryption protocols

1. Encryption

*Description*

Encryption is the process of converting traffic using the cipher.

There are no apparent physical borders in WLANs because it’s using radio waves. Therefore WLAN can be listened to by anyone within the range and potentially connect to other traffics. The encryption for WLAN keeps data private, so only the appropriate parties can understand the data.

*Risks*

Whenever encryption is cracked, the hacker could read the traffic that might contain the user’s credentials, PII, or even financial information and alter the traffic by performing a Man-in-the-Middle(MITM) attack.

*Possible Damage*

There are indefinite damages that could happen to the user and/or the business. It could expose the user’s credentials for social media or email systems, leak sensitive information, or cause secondary damage such as uses for crimes like scams or fraud. Moreover, the hacker could perform a “Session Hijack” on your bank screen or PayPal and process financial transactions.

1. OPEN

*Description*

There is no encryption in the traffic.

*Suggestion*

1. Utilize the Encryption.
2. Avoid using Sensitive information (Personal Identifiable Information, Financial information, Protected Health Information, etc.)
3. WEP

*Description*

In WEP authentication, a wireless device sends an authentication request to the access point, which will reply with a 64-bit or 128-bit challenge in cleartext. The client will sign that challenge with the shared secret key and send it back to the access point. The AP will decrypt the signed message using the same shared key as the client did and verify the challenge sent.

Because WEP uses 64-bit or 128-bit challenge to grant access, the hacker only needs to know the challenge code, not the actual password.

*Strength*

According to aircrack-ng documentation, 64-bit WEP can usually be cracked in less than 5 minutes (generally less than 60 seconds), and 128-bit usually takes 30 minutes to an hour.

Also, the result from the article, “Vulnerability issues on research in WLAN encryption algorithms WEP WPA/WPA2 Personal,” took around a minute or two for 64-bit WEP and three to four minutes for 128-bit WEP.

*Suggestion*

1. Utilize better Encryption with Chipher.
2. Avoid using Sensitive information (Personal Identifiable Information, Financial information, Protected Health Information, etc.)
3. WPA

*Description*

WPA is the next version of encryption after WEP. It can provide security and ensure that only authorized users can access the WLAN. It uses improved RC4 data encryption that uses Temporary Key Integrity Protocol(TKIP) and 802.1x authentication.

WPA is stronger than WEP, but it uses TKIP cipher, which is depreciated by WPA2-AES and vulnerable to MIC key recovery attacks, Chop-Chop Attack, etc.

However, WPA is compatible with the older software; users might require to use it.

*Strength*

WPA is way stronger than WEP, but there are multiple attacks for the TKIP cipher.

*Suggestion*

1. Upgrade to WPA2 after confirming all devices and software supports WPA2.
2. Avoid using Sensitive information (Personal Identifiable Information, Financial information, Protected Health Information, etc.)
3. WPA2

*Description*

WPA2 is an updated version of WPA using the Advanced Encryption Standard (AES) instead of TKIP. It requires significant amounts of processing power compared to WPA; older devices or software may be slow or not working at all.

*Strength*

WPA2 is more secure than WEP and WPA and has only a few known vulnerability attacks.

1. Cipher

*Description*

Cipher is a method (algorithm) used for the encryption process.

*Risks*

If encryption is deciphered, the hacker can see all the traffic in cleartext. If there is SI in the traffic, a data leak could occur.

*Possible Damage*

There are indefinite damages that could happen to the user and/or the business. It could expose the user’s credentials for social media or email systems, leak sensitive information, or cause secondary damage such as uses for crimes like scams or fraud.

1. PSK

*Description*

PSK uses both TKIP and AES. Because AES requires significant amounts of processing power compared to WPA, the older device may be slow or not working at all. PSK will primarily enable AES, but it will switch to TKIP when the connection is slow or not working.

1. Advanced Encryption Standard(AES) / Chaining Message Authentication Code Protocol(CCMP)

*Description*

AES is a collection of ciphers that are available in 128-bit block size and key length in 128, 192, or 256-bit. AES standard comes with a more secure protocol than TKIP and is the most commonly used cipher. It is a publicly accessible cipher that was approved by NSA.

1. (Temporary Key Integrity Protocol) TKIP

*Description*

TKIP was developed to improve the security of WEP. TKIP wraps the WEP by adding extra code at the beginning and end of every data packet. It uses the same 4RC data encryption with new security characteristics such as per-packet key hashing, sequence counter, etc.

*Suggestion*

1. Use AES cipher after confirming the compatibility of all devices and software.
2. Avoid using Sensitive information (Personal Identifiable Information, Financial information, Protected Health Information, etc.)

**Process**

WAAT is consists of 5 phases: Confirm the environment, Wlan to Scanning mode, Scan, Recover, Result

1. Confirming the Environment

Text

Description automatically generated

1. Check if it runs as Sudo

By checking SUDO\_UID in os.environ.key variable.

1. Check if an aircrack-ng package is installed

By using the command ‘dpkg-query’

A screenshot of a computer

Description automatically generated with medium confidence

If the aircrack-ng is installed, it will return some value; otherwise, it will return 0.

1. Check if the wlan interface is available

By Using the command ‘iwconfig’ to check available wlan and save it as a list. If the length of the list is 0, return the error.

1. WLAN to Scanning Mode

Text

Description automatically generated

* 1. Ask for Selection
  2. Save selected wlan to variable wlan\_using
  3. Kill all the conflict processes to switch to monitoring mode

By using the command ‘airmon-ng check kill’

* 1. Switch wlan to monitoring mode

By using the command ‘airmon-ng start [wlan\_using]’

1. Scanning Wireless Access point and Dump the list to csv file
   1. Backup old csv filesText

      Description automatically generated
      1. This occurs only when .csv file is found from the folder.

Checking by using file\_name variable in os.listdir().

* + 1. If an old csv file is found, create a folder and back up it with a timestamp
  1. Scanning with the output of csv

By using the command ‘sudo airodump-ng -w WAP\_list –write-internal 1 –output-format csv [wlan\_using]mon’

* 1. Text

     Description automatically generatedLoad csv file from the step b and dump it into the Hashtable
     1. Define the field name
     2. Create a Dictionary with field names and indicator
     3. Using Loop to dump data into the Dictionary. (While dumping, all indicator is set to Green)
     4. Clear the screen and show data from the Dictionary until the User inputs ‘Ctrl + C’.

1. Recover

Recovering process in 2 steps: Stop the monitoring mode, start network manager.



1. Result
   1. Checking Evil Twins

A screenshot of a computer

Description automatically generated with medium confidence

* + 1. Checking Evil Twins by checking if there’s a duplicate SSID

By using List to compare ESSID

* + 1. Update Indicator if Evil Twin Found.
    2. Clear the list.
  1. Text

     Description automatically generatedUpdate indicator
     1. Update Indicator for each category
     2. Update Alert Indicator
  2. The user selects the device wishes to check  
     Text

     Description automatically generated
  3. Defining Pages
     1. Page 1 – Dashboard (Main Page)

Page 1 will show an overall indicator from the result.

Text

Description automatically generated

* + 1. Page 2 – Evil Twin

Text

Description automatically generated

* + 1. Page 3 - Encryption
       1. OPN

Text

Description automatically generated

* + - 1. WEP

Text

Description automatically generated

* + - 1. WPA

Text

Description automatically generated

* + 1. Page 4 - Cipher
       1. None

A picture containing graphical user interface

Description automatically generated

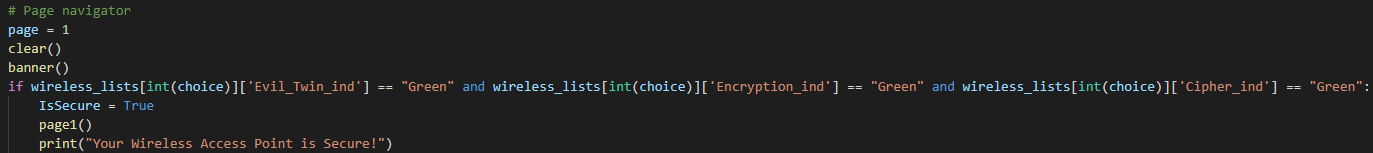
* + - 1. TKIP

A picture containing graphical user interface

Description automatically generated

* 1. Page Navigating

Users will navigate pages with A or D input.

If all indicator is green, return “Your Wireless Access Point is Secure!” and exit the program

* + 1. Call Main Page

A picture containing text

Description automatically generated

* + 1. “A” input

Text

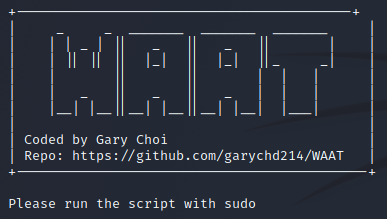
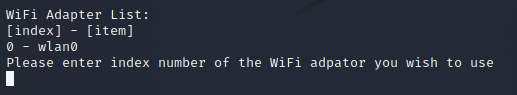
Description automatically generated

* + 1. “D” input

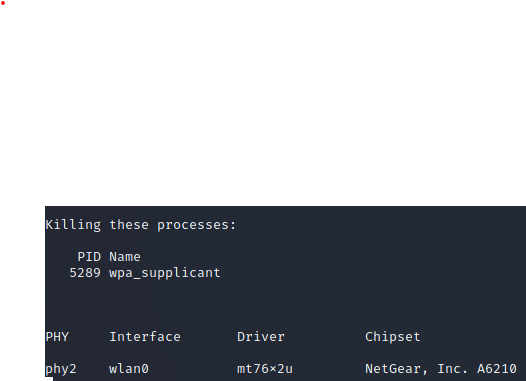
Text

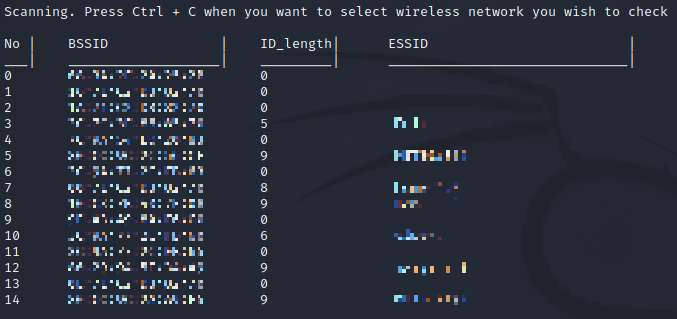
Description automatically generated

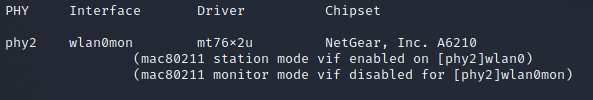
**Usage**

1. Confirming the Environment
   1. Check if it runs with sudo
   2. Check if a Wi-Fi adapter is available and selection
      1. If any Wi-Fi adapter is available
      2. If no Wi-Fi adapter is availableText

         Description automatically generated
   3. Check if the Aircrack-ng package is availableText

      Description automatically generated
2. Switch Wi-Fi Adapter to Monitoring mode
3. List the scanned WAP



1. Recover Wi-Fi Adapter from Monitoring mode
2. Select the WAP to analyze and assess.

**Reference**

*Aircrack-ng*. aircrack. (n.d.). Retrieved March 5, 2022, from https://www.aircrack-ng.org/doku.php?id=aircrack-ng

Ioannis, L., Simeon, V., & Sotirios, P. (2013). *Vulnerability issues on research in WLAN encryption algorithms WEP WPA/WPA2 Personal* . Faculty of Mathematics & Natural Science – FMNS 2013. Retrieved March 5, 2022, from https://inis.iaea.org/collection/NCLCollectionStore/\_Public/46/130/46130069.pdf

Pew Research Center. (2021, November 23). *Demographics of Internet and home broadband usage in the United States*. Pew Research Center: Internet, Science & Tech. Retrieved March 5, 2022, from https://www.pewresearch.org/internet/fact-sheet/internet-broadband/

Qamar, A. (2021, June 7). *How to avoid becoming a victim of an evil twin attack*. TechGenix. Retrieved March 5, 2022, from https://techgenix.com/protect-against-evil-twin-attack/

Security, P. (2021, December 13). *What is an evil twin attack?* Panda Security Mediacenter. Retrieved March 5, 2022, from https://www.pandasecurity.com/en/mediacenter/security/what-is-an-evil-twin-attack/

Wikimedia Foundation. (2021, July 25). *Evil twin (wireless networks)*. Wikipedia. Retrieved March 5, 2022, from https://en.wikipedia.org/wiki/Evil\_twin\_(wireless\_networks)