**ROGUE ACCESS POINT ATTACK**

1. **DESCRIPTION OF ROGUE AP**

A *Rogue Access Point* (Rogue AP) is an *unauthorized* wireless access point plugged into a corporate and secure WLAN that the network administrator usually does not know about its existence. These Rogue Access Points are frequently part of a coordinated attack; however, without the proper awareness program of users, it is easy to fall victim to the attack. [1]

It is essential to mention the difference between Rogue AP and Evil Twin:

A *Rogue AP* is physically plugged into a network, granting users access to the secure network. An *Evil Twin* can also be within the network's physical parameters; however, it is not part of the network and does not inflict damage by directly compromising its security. [1]

Some reasons exist to believe an access point is a rogue:

* First, the SSID of the AP is neither the SSID of the secured network nor listed in the permitted SSID list.
* The AP is masquerading as one of the secured SSIDs.
* The AP is an Ad-Hoc AP formed directly between two client devices.
* Management features disabled, for instance, SNMP, HTTP and Telnet.
* The MAC address of the AP is not listed in the ARP table.
* The AP operates in bridge mode.
* The AP is in the rogue list, added previously by the administrator.

Rogue clients are classified into: [2]

* *Members*: A secured identified member.
* *Neighbour*: Trusted device in a permitted third-party list.
* *Suspect*: Not enough information to define if it is or not a rogue; the administrator makes the decision.
* *Rogue*: Proved unauthorized access point.

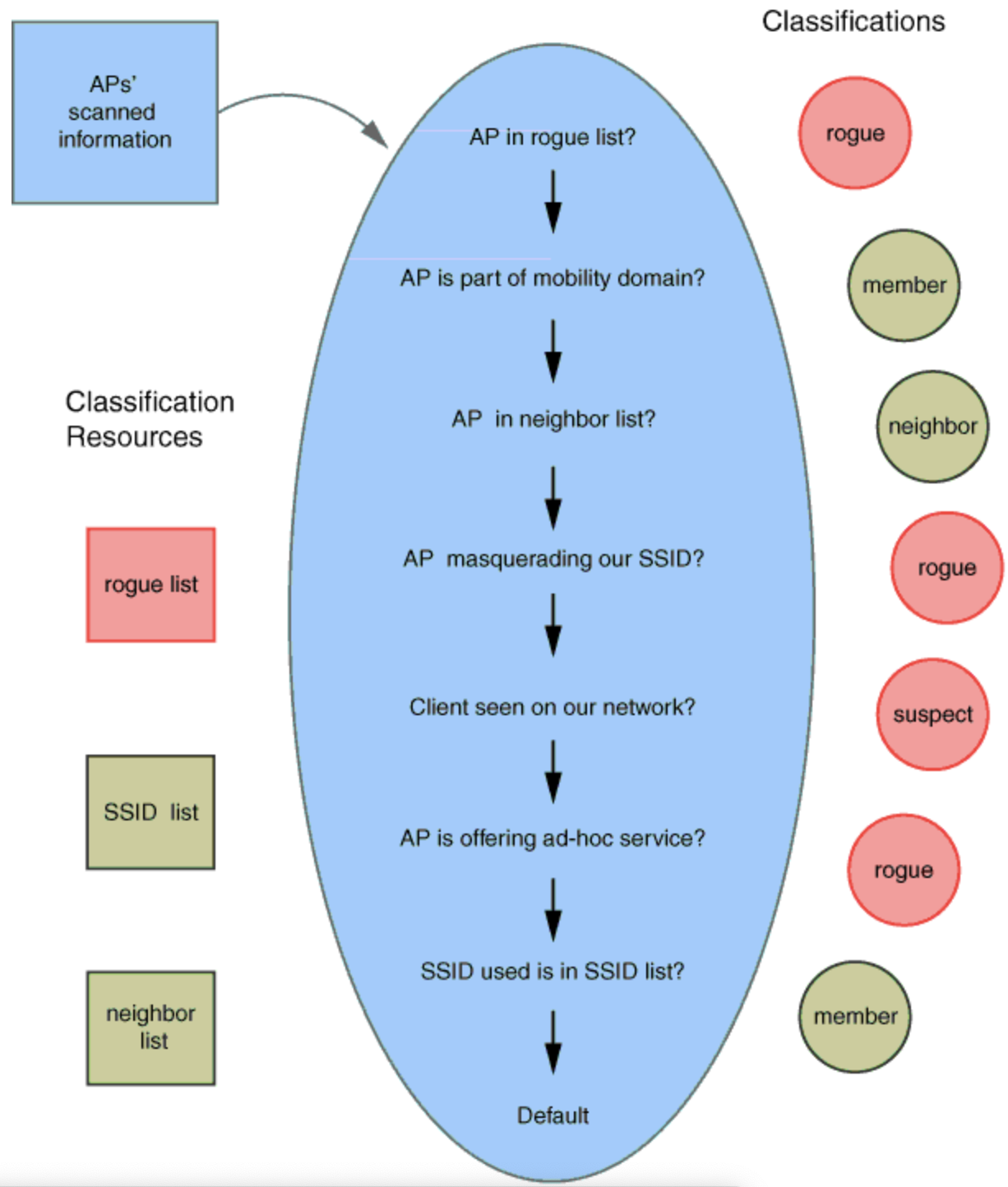
****

Fig.1. How scanned information is used to classify Aps [2]

1. **POSSIBLE ATTACKS WITH A ROGUE AP**

* *Man-in-the-middle attack*: The attacker relays messages between the victims, making them believe their connection is private.
* *Flood*: By flooding the network with useless data, creates a Denial of Service (DoS).
* *Infected Broadcast*: Send fake SSID advertising attractive features, so once the user connects to the fake SSID, this will be added to their client’s wireless configuration, and the client starts to broadcast the fake SSID. [2]

1. **TOOLS FOR ROGUE AP**

There are known tools to recreate a Rogue AP:

*Wifiphisher*:

* This tool creates a Man-in-the-middle attack against wireless clients performing associations to access points.
* It also can be customized by using a third-party login page. [3]

Aircrack-ng suite:

* This tool collects packet captures and exports data to text for use in third-party tools.
* Performs replay attacks and de-authentication attacks by packet injection.
* It can attack WEP. WPA and WPA-2 pre-shared keys. [4]

Airmon-ng:

* It is used for enabling and disabling monitor mode on the wireless adapter.
* Also, it is used to check if any processes interfere with the aircrack-ng tool. [5]

Airodump-ng:

* Captures packets of raw 802.11 frames.
* Collects WPA handshakes.
* Captures weak WEP initialization.
* It can show information about the MAC address of the AP, signal level, number of beacon frames, number of captured data packets, channel number, speed, encryption algorithm, cipher detected, authentication protocol used and the SSID of the network. [6]

Aireplay-ng:

* It is used to inject frames and generate traffic for later use.
* It can also be used for the following attacks: de-authentication, fake authentication, packet replay, ARP request replay, KoreK chop-chop, fragmentation, cafe-latte, WPA migration (Cisco exclusively) and injection test. [7]

Airgeddon:

* It can manage the interface mode (monitor and controlled).
* Supports 2.4 and 5 GHz.
* Captures the WPA/WPA-2 handshake.
* Offline password cracking for WPA/WPA2.
* Evil-twin and WPS attacks. [8]

1. **COUNTERMEASURES TO ROGUE ATTACK**

The following are some countermeasures to avoid Rogue AP:

* Disabling SSID Masquerade and Bridging features.
* By default, unknown devices could be classified as Rogue AP.
* Use active access scanning in addition to passive scanning.
* Add known rogue intruders.
* Use certificates in the WLAN and controller.
* Use managed switches on your network and access lists to allow only specific MAC addresses; you can also include the physical ports of connection.
* Investigate wireless bridge frames and eliminate the source.
* Use static IP’s for a new AP register instead of a DHCP service.
* Perform regular sweeps of the physical spaces.
* Establish policies that only authorized IT staff can connect networking devices.
* Use hardware-based micro-segmentation to isolate endpoints onto their own protected micro-segments; this strengthens defences against lateral movements and increases granular control.
* Use network-wide Intrusion Detection and Prevention System (IDS/IPS).

**BRUTE FORCE ATTACK AGAINST THE 4-WAY HANDSHAKE OF WPA/WPA2**

1. **DEFINITION OF WPA-PSK**

The definition of PSK (pre-shared key) is based on users using an initial secure channel to deliver a key to send later messages where the encryption depends on the initial PSK.

WPA-PSK encrypts data transmission in 128 bits and is controlled by a password generated by the end user.

WPA-PSK can be used with AES standards and does not require a central server; it is usually designed for home or small networks. [9][10]

1. **PAIRWISE MASTER KEY GENERATION**

Starting with the PSK, each device stores a PMK (pairwise master key) until the PSK or SSID changes.

If a client tries to connect, a protocol named 4-Way Handshake is initialized to generate a PTK (pairwise transient key). The objective of the key is to encrypt the data between a client and the access point; this key usually changes at least 65,535 packets.

PMK is computed using PBKDF2 (password-based key derivation function 2), which reduces vulnerabilities to brute force attacks because of the high computational cost. [10]

WPA protocol generates the PMK as:

**PMK = PBKDF2 (HMAC-SHA1, PSK, SSID, 4096, 256)**

Diagram

Description automatically generated

Fig.2. PMK equation [10]

1. **4-WAY HANDSHAKE**

The goal of the 4-Way Handshake is to provide mutual authentication based on a PMK to negotiate a new PTK session key.

The PTK results from the PMK, two nonces and the MAC addresses of the client and the authenticator. [11]

Diagram

Description automatically generated

Fig.3. 4-Way Handshake Diagram [11]

Steps:

1. The AP sends an Authenticator Nonce (ANonce) to the client (STA).
2. The STA builds the PTK and sends its own Nonce (SNonce) to the AP; this way, it protects the frame with a Message Integrity Code (MIC).
3. The AP generates and sends the Group Temporary Key (GTK) and a sequence number. In addition, a MIC is used to protect the frame and prevent tampering.
4. Finally, the STA sends an acknowledgement to the AP indicating it is ready for encryption. [11]
5. **CRACKING THE 4-WAY HANDSHAKE**

To carry out the attack, the attacker can use the tool Crunch and Airgeddon; the last one **was** **previously mentioned** and described in the Rogue AP attack.

Crunch is a word list generator where an attacker can specify a standard character set or any set of characters to generate word lists created through a combination and permutation of a group of characters. It also allows the attacker to set the number of characters and list size. [12]

Steps:

1. Monitoring/Scanning:

First, the network interface must be enabled to allow active monitoring mode in the attacker interface. [12]

1. Capture Packets:

In this step, Airgeddon captures 802.11 frames.

This tool shows a table with the following information: BSSID (Basic Service Set Identifier), MAC address, the channel the device is broadcasting on, encryption used, and the Extended Service Set Identification (ESSID) of the network or the Service Ser Identifier SSID. [13]

1. Capture 4-Way Handshake

Users must be revoked from the network to force them to re-authenticate to capture the 4-Way Handshake.

Then, during user re-authentication, Airgeddon captures the packets with the 4-Way Handshake. [13]

1. Cracking the password

Users must be revoked from the network to force them to re-authenticate to capture the 4-Way Handshake.

Here the attacker uses *Crunch* for the Brute Force method; the initial parameters must be set to direct the attack. This means that if the attacker has clues to the password, he can choose the options he deems convenient to make the attack shorter but effective.

For example, if the attacker chooses the only number option, starting at 000000000 and incrementing the value each turn, it will go until 999999999. Each time check the new value captured in the 4-Way Handshake. [13]

1. **COUNTERMEASURES**

The following are some countermeasures to avoid this attack:

* Changing the default Wi-Fi password to something complex and longer will increase the time; theoretically, it would take an attacker to crack it.
* Make an asset review frequently by looking at all connected devices to the Wi-Fi.
* Implement whitelisting by configuring only the MAC addresses of the devices we want to connect to the Wi-Fi.
* Be aware of some misbehaviours of the devices in the network, for instance, frequent Wi-Fi disconnection, slow internet surfing, etc. [13]

1. **REFERENCES**

[1] BYOS. How to protect against Rogue Access Points on Wi-Fi. Accessed: March 7, 2023. [Online] <https://www.byos.io/blog/how-to-protect-against-rogue-access-points-on-wi-fi>

[2] Juniper. Understanding Rogue Access Points. Accessed: March 7, 2023. [Online] <https://www.juniper.net/documentation/en_US/junos-space-apps/network-director4.0/topics/concept/wireless-rogue-ap.html>

# [3] Kali.org. Wifiphisher Tool Documentation. Accessed: March 8, 2023. [Online] <https://www.kali.org/tools/wifiphisher/>

# [4] Aircrack-Ng Official Website Aircrack-ng.org. Accessed: March 8, 2023. [Online] <https://www.aircrack-ng.org/>

# [5] Airmon-ng Documentation Aircrack-ng.org. Accessed: March 9, 2023. [Online] <https://www.aircrack-ng.org/doku.php?id=airmon-ng>

# [6] Airodump-ng Documentation Kali Tools. Accessed: March 9, 2023. [Online] <https://en.kali.tools/?p=367#:~:text=airodump%2Dng%20%2D%20a%20wireless%20packet,of%20the%20found%20access%20points>.

# [7] Aireplay-ng Documentation Aircrack-ng.org. Accessed: March 10, 2023. [Online] <https://www.aircrack-ng.org/doku.php?id=aireplay-ng#:~:text=Description,WEP%20and%20WPA%2DPSK%20keys>.

# [8] Kali.org. Airgeddon Tool Documentation. Accessed: March 10, 2023. [Online] <https://www.kali.org/tools/airgeddon/>

# [9] Wi-Fi Protected Access Pre-Shared Key. Accessed: March 12, 2023. [Online] <https://www.techopedia.com/definition/22921/wi-fi-protected-access-pre-shared-key-wpa-psk>

# [10] How does WPA/WPA2 Wifi security work, and how to crack it? Accessed: March 16, 2023. [Online] <https://cylab.be/blog/32/how-does-wpawpa2-wifi-security-work-and-how-to-crack-it?accept-cookies=1>

# [11] The University of Hawai’i-West O’ahu. Taking advantage of the 4-Way Handshake. Accessed: March 18, 2023. [Online] <https://westoahu.hawaii.edu/cyber/forensics-weekly-executive-summmaries/taking-advantage-of-the-4-way-handshake/>

# [12] Kali.org. Crunch Tool Documentation. Accessed: March 18, 2023. [Online] <https://www.kali.org/tools/crunch/>

# [13] James Weston. Wi-Fi Attacks – Cracking the Handshake. Accessed: March 18, 2023. [Online] <https://westoahu.hawaii.edu/cyber/forensics-weekly-executive-summmaries/taking-advantage-of-the-4-way-handshake/>