ALBUS SECURITY

Wifi Attack Session 01

Computer network security is founded on three main principles: confidentiality, integrity, and availability. Achieving true security requires addressing all three principles. Neglecting any of these aspects can leave a network vulnerable to attacks. Attackers typically aim to compromise one or more of these core security principles.

Confidentiality ensures that sensitive information is kept secret and accessible only to authorized individuals. In network security, this is often achieved through data encryption, which converts readable data into unreadable text.

Integrity means the data remains accurate and unchanged. In network security, this ensures that a message has not been tampered with—no part of it has been altered or rearranged. To ensure integrity, a cryptographic checksum is used to verify that the message remains unaltered.

Availability ensures that data is accessible and usable when needed by authorized users. An attack on availability, such as a Denial of Service (DoS) attack, prevents users or devices from accessing a particular service or application.

Introduction To Wifi

WiFi, short for "Wireless Fidelity," is a technology that allows devices to connect to a network and communicate with each other using radio waves without the need for physical cables. It is commonly used for providing internet access to devices like smartphones, laptops, tablets, and smart home devices.

WiFi operates mainly in the 2.4 GHz and 5 GHz frequency bands. The 2.4 GHz band provides broader coverage but slower speeds, while the 5 GHz band offers faster speeds but shorter range. WiFi technology is based on the IEEE 802.11 family of standards. Common standards include 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax (also known as WiFi 6).

© 2024 Albus Security. All rights reserved.

ALBUS SECURITY

Important Terms

Access Point - An Access Point is a device that connects wireless devices to a wired network, typically providing internet access. It acts as a central hub for transmitting and receiving data within the network.

Service Set Identifier (SSID) - The SSID, or Service Set Identifier, is the name of the WiFi network that is broadcast to users. This human-readable identifier allows users to identify and select the network they wish to connect to from a list of available networks.

The SSID groups devices into the same network and manages connections within that network. Access Points broadcast the SSID, enabling client devices to find and display the network name, which helps users select the correct network from potentially many available options. Network administrators can customize the SSID to provide a recognizable name, such as "HomeWiFi" or "OfficeNetwork," making it easier for users to identify and connect to the appropriate network.

Basic Service Set Identifier (BSSID) -The BSSID, or Basic Service Set Identifier, is a unique 48-bit address assigned to each Access Point (AP) within a wireless network. This identifier is similar to a MAC address and ensures that each AP can be uniquely distinguished, especially in environments with multiple access points. Typically, the BSSID is the MAC address of the AP's wireless interface.

It plays a crucial role in network management by helping devices connect to the correct AP within a network. When a device scans for available WiFi networks, it receives information about the BSSID of each network, allowing it to accurately identify and connect to the desired network.

Wifi Security Protocols

Security protocols in the context of computer networks, including WiFi networks, refer to standardized procedures and mechanisms designed to ensure the confidentiality, integrity, and availability of data transmitted over the network. These protocols establish guidelines and rules for secure communication, authentication, encryption, and access control. Here's an in-depth look at security protocols.

- WEP (Wired Equivalent Privacy)
- WPA (Wi-Fi Protected Access)
- WPA2
- WPA3

© 2024 Albus Security. All rights reserved.

WEP (Wired Equivalent Privacy)

WEP was the first encryption protocol used in WiFi networks. It aimed to provide security comparable to wired networks but has significant vulnerabilities. WEP uses a shared key authentication mechanism and employs RC4 encryption with a 40-bit or 104-bit key size. However, due to weaknesses in key management and encryption methods, WEP can be easily compromised through brute-force attacks. As a result, it is no longer considered secure and is rarely used today.

WPA (Wi-Fi Protected Access)

WPA was introduced as a temporary improvement over WEP while the more robust WPA2 was being developed. It addressed many of WEP's weaknesses by implementing TKIP (Temporal Key Integrity Protocol) encryption and introducing stronger key management techniques. WPA also supports both passphrase-based authentication (WPA-PSK) for home users and enterprise-grade authentication using a centralized authentication server (WPA-Enterprise).

WPA2

WPA2 represents a significant advancement in WiFi security and has been widely adopted as the standard protocol. It uses AES (Advanced Encryption Standard) encryption, which is much stronger and more secure than the RC4-based encryption used in WEP and TKIP. WPA2-PSK (Pre-Shared Key) mode is commonly used in home networks, while WPA2-Enterprise employs IEEE 802.1X authentication, which provides enhanced security features suitable for enterprise environments. Despite its strengths, WPA2 is susceptible to attacks like brute-force attacks on weak passwords.

WPA3

WPA3 is the latest iteration of WiFi security protocols, designed to address vulnerabilities identified in WPA2 and provide stronger protections for WiFi networks.

© 2024 Albus Security. All rights reserved.

ALBUS SECURITY

Wifi Attack

WiFi attacks refer to malicious activities aimed at exploiting vulnerabilities in wireless networks to compromise their security or disrupt their normal operation. These attacks target weaknesses in WiFi protocols, encryption methods, authentication mechanisms, or configurations to gain unauthorized access, intercept data, or perform other malicious actions.

- Deauthentication Attacks
- Eavesdropping
- Man-in-the-Middle (MITM) Attacks
- Denial-of-Service (DoS) Attacks
- Distributed Denial-of-Service (DDoS) Attacks
- Evil Twin Attacks
- Rogue Access Point Attacks
- Authentication Attacks
- Passive Attacks
- Active Attacks
- Spoofing Attacks
- Packet Sniffing
- Packet Injection
- Replay Attacks
- Jamming Attacks
- Bluetooth and Zigbee Interference
- Brute-Force Attacks
- WPS (Wi-Fi Protected Setup) PIN Cracking
- Honeypot Attacks
- Karma Attacks
- Social Engineering Attacks
- Phishing Attacks
- DNS Spoofing Attacks
- MAC Address Spoofing
- War-driving
- SSID Cloaking
- Signal Jamming
- Cryptographic Attacks
- Channel Interference

© 2024 Albus Security. All rights reserved.

De-authentication Attack

A de-authentication attack is a type of attack targeting wireless networks, where the attacker forcibly disconnects devices (clients) from a WiFi access point (AP) by sending specially crafted de-authentication frames.

De-authentication attacks exploit the IEEE 802.11 standard, which allows APs to send de-authentication frames to disconnect clients. Attackers can impersonate the AP or send de-authentication frames directly to the targeted client.

Attackers can perform de-authentication attacks using tools like `airplay-ng` from the Aircrack-ng suite. These tools allow them to send a high volume of de-authentication frames continuously, causing the target device to repeatedly disconnect and attempt to reconnect to the network.

Steps For Exploitation

1. Ensure your WiFi adapter supports packet injection and Monitor mode. *(type ifconfig then it shows wlan0 configuration)*

2. airdump-ng <interface> - is used to gather necessary information about the target wireless network and its connected clients before launching a de-authentication attack. This information includes the BSSID of the target access point (AP) and the MAC addresses of the clients connected to it.

© 2024 Albus Security. All rights reserved.

Note -

When you run `airodump-ng <interface>`, you need to note the following:

- **BSSID**: The MAC address of the target AP. This is crucial as you need to specify the AP you want to attack.
- **Channel**: The channel number on which the target AP is operating. You need this information to focus your attack on the specific channel.
- **Client MAC Addresses**: The MAC addresses of the clients connected to the target AP. De-authentication attacks are often aimed at specific clients or all clients connected to the AP.

With the BSSID and the client MAC addresses, you can proceed to the next step using `aireplay-ng` to launch the de-authentication attack.

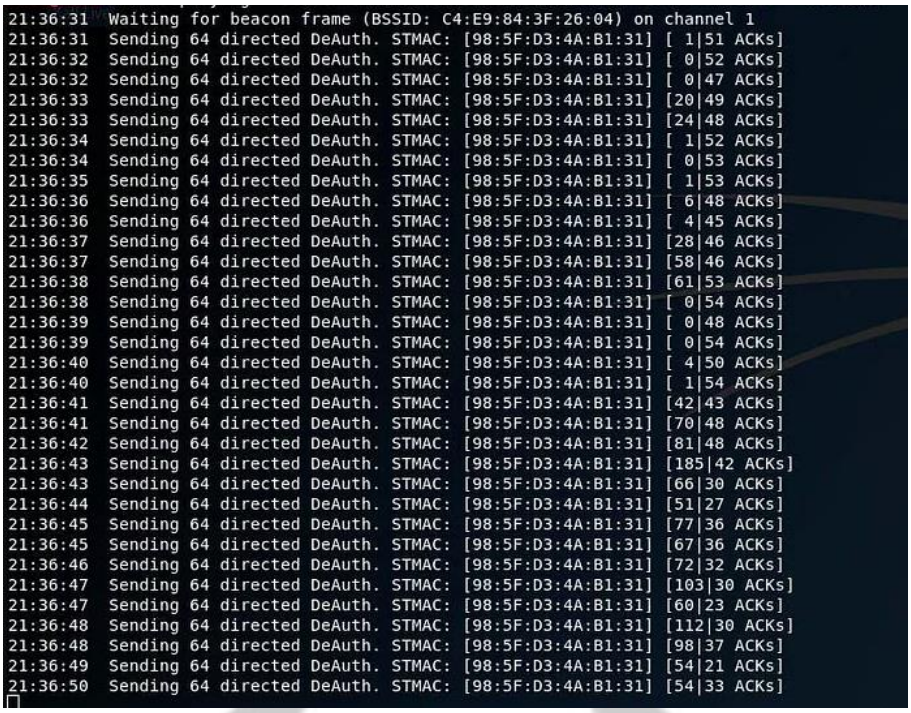
3. De-authenticate All Clients from AP -

`sudo aireplay-ng –deauth 0 -a [BSSID] <INTERFACE>` This Command help attacker to disconnect all clients from a WiFi access point (AP).

```
sudo aireplay-ng –deauth 0 -a [BSSID] -c [CLIENT-MAC]
<INTERFACE>
```

- Replace **[BSSID]** with the MAC address of the target AP.
- Replace **[Client_MAC]** with the MAC address of the specific client.
- `--deauth 0`: Sends de-authentication packets continuously until you stop it.

© 2024 Albus Security. All rights reserved.



This document is created because of an intern's request. If you want PDF resources for all the listed attacks above, let me know, and I'll try to provide practical resources for every WiFi attack. Make sure to connect your WiFi adapter before performing the attacks; otherwise, you might face issues with your pre-defined interface.

© 2024 Albus Security. All rights reserved.