Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 03 March 2024

Design and Implementation of Attack Flow Model Using ESP8266: Wireless Networks

Reddyvari Venkateswara Reddy, Punyaban Patel, Yamjala Sanjana,
Adaboina Jyoshitha Reddy, Mittapalli Tejashwini
Professor, Department of CSE(Cyber Security),CMR College of Engineering & Technology, Hyderabad, India
Professor, Department of CSE(Cyber Security),CMR College of Engineering & Technology, Hyderabad, India
B. Tech Student, Department of CSE(Cyber Security),CMR College of Engineering & Technology, Hyderabad,India

Abstract— A network of computers that uses wireless data links between its nodes is called a wireless network or WLAN. Instead of using physical cables to connect devices, wireless networks use radio waves or infrared signals to send data between computer systems, cell phones, tablets, and other network-enabled devices. They're also frequently called access points (APs). Due to the multiple vulnerabilities in this wireless network, we conducted a pentest to identify any weaknesses or vulnerabilities. The purpose of this project is to evaluate the security of WPA/WPA2 wireless network passwords by designing and implementing a tool and utilizing the ESP-8266 controller to learn how users are tricked by fraudulent router login pages. This paper also includes counter measures to prevent attacks and enhance the security model on wireless networks.

***Keywords*-WLAN, ESP-8266, pentest, WPA/WPA2.**

1. INTRODUCTION

Wi-Fi, an abbreviation for Wireless Fidelity, is a wireless alternative to usually wired Local Area Networks and has become necessary in many settings, such as homes, offices, and training facilities. The IEEE (Institute of Electrical and Electronics Engineers) published a standard in 1997 called Wireless Local Area Network (WLAN) configuration instructions. Devices could now establish wireless links with one another because to this. The current three main security methods for IEEE 802.11 wireless technology are WiFi Protected Access (WPA), Wi-Fi Equivalent Privacy (WEP), and Wi-Fi Protected Access II (WPA2). The Wi-Fi Alliance has made fourth-generation Wi-Fi Protected Access III (WPA3) available to the general public. This occurred on June 25, 2018. These wireless protocols encrypt data as it passes over the network to guard against unwanted access. However, there are still a number of flaws that we may use to get illegal access to any kind of wireless network. Wi-Fi uses radio frequency (RF) to transmit data over the air. Additional advantages of Wi-Fi include internet access and fast data transmission. In a Wi-Fi network, the most important component is an access point (AP).

An access point is the point of connection for every device in a network.

2. LITERATURE REVIEW

Amith Raj Megalapete Puttaraju and Rekha Jayaram, "A Study on 802.11 Wireless Routers Hacking Techniques and Security Encryption Levels," focus on wireless routers, encryption techniques, and hacking methods using software like Aircrack and WiFite.

Page [3] delves into the introduction of wireless routers, IEEE 802.11 specifications, and various hacking techniques such as denial of service, man-in-the-middle, and assaults using brute force. It also discusses different encryption levels and features of routers, including MAC address filtering and firewalls. Page [4] covers topics such as MAC address spoofing, flooding with associations, and forged dissociation about the security of wireless networks. It also provides insights into the significance of MAC address filtering and the many openings these attacks may present.

Page [5] discusses ARP poisoning, session hijacking, war driving, and war chalking as potential security threats in wireless networks.It also discusses how hackers and other invaders use root kits, sniffers, exploits, and vulnerability scanners.

Page [6] focuses on the location of access points, secure protocols, wireless virtual private networks, intrusion detection systems, and wireless auditing as security measures for wireless networks. It also includes a table showing results and observations related to different encryption levels of Wi-Fi networks.

The study's references and citations are included on page [7], along with connections to other websites and publications that are mentioned throughout the document. It also provides additional information on topics such as WLAN security systems, wireless network security attacks, and automated Wi-Fi cracking techniques.

Se-Hwan Kwon, and Dea-Woo ,"Hacking and Security of Encrypted Access Points in Wireless Network" highlights the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 03 March 2024

increasing use of wireless networks by smartphone and tablet users in public facilities. It highlights the necessity to research hacking and the security of WPA and WPA2 encrypted access points (APs), as well as the possible security hazards connected to using unsecured wireless networks.The page also provides an abstract of the study, outlining the focus on WPA and WPA2 encryption systems, AP hacking processes, and the proposed approach to enhancing wireless LAN security.

Page [2] Figures the status of wireless internet terminals, showing the percentage of various devices used to access wireless internet. Additionally, it discusses the concept of Access Points (APs) as devices that connect wired and wireless LANs, and the encryption methods used in APs, specifically WPA and WPA2. It provides an overview of the security standards and encryption techniques employed in WPA and WPA2, emphasizing their importance in ensuring user authentication and data encryption.

Page [3] delves into the threats to wireless networks, including unauthorized access points, wireless LAN card modes, and potential security breaches. It also addresses the dangers and instances of wireless network hacking in the US, mentioning events such as the TJX data dump. It also highlights how important it is to understand and address security risks. Regarding wireless networks, particularly in view of the growing number of people using smartphones and tablets to access the internet wirelessly.

The experimental setting for breaking into encrypted wireless Access Points (APs) utilizing WPA and WPA2 is the main topic of page [4]. It explains how to use programs like Backtrack 4 and Aircrack to record and retrieve a wireless AP's password. It also describes how to hack WPA and WPA2 passwords and suggests a security plan considering the findings of the experiment.

3. WI-FI ENCRYPTION TYPES

Various kinds of techniques are discussed below:

1.Wired Equivalent Privacy(WEP)

The first encryption technique to help with wireless network authentication and data privacy was WEP. In 1997, it was first released. To ensure to protect link level data during wireless transmission, WEP is a component of the IEEE 802.11 network. Information is encrypted by WEP using a technique known as RC4 (Rivest Cipher 4). Each data packet in this is encrypted at the AP, and upon receiving it is decrypted. WEP makes sure that every packet has a distinct 24-bit Initialization Vector (IV), which is just plain text contained in the packet.

One of WEP's features is false data packet broadcasting primary flaws. An attacker may easily falsify an authentication message using WEP as it uses shared key authentication. Understanding a shared WEP key is proven by the encryption of a challenge in shared key authentication. The encryption stream used by RC4 can be discovered by an attacker through a look at the encrypted key and the challenge. The attacker may use the same stream in the future.The WEP protocol has an additional flaw that is the initialization vector is reused.

2.Wi-Fi Protected Access(WPA)

In 2003, the Alliance of WiFi created WPA to fix the problems of WEP. Version 1 was designed to fix the cryptographic problems in WEP without requiring new hardware and uses the Temporal Key Integrity Protocol (TKIP) for encryption. A distinct 128-bit key is generated dynamically for every packet. The PreShared Key (PSK), a static key, is used to initiate communication between two devices. A 256-bit key, which is never transmitted over the air, is used by the wireless devices for authentication. The Message Integrity Code (MIC) key and the encryption key are produced using the PSK.

There are numerous serious issues with the WPA protocol. Initially, the more advanced AES algorithm is not used, but rather the RC4 technique. If two or more RC4 keys are computed under the same IV, an attacker may quickly ascertain the Temporal Key (TK). The WPA-PSK setup is the next area of weakness. When a password is used carelessly, it can be attacked by brute force. In the event that the password comprises less than 20 characters, one could execute a dictionary attack.

3. Wi-Fi Protected Access 2(WPA2):

A security protocol called Wi-Fi Protected Access 2, or WPA2, was developed to increase the security of wireless networks in general and Wi-Fi networks in particular. It is an improvement over WPA since it uses stronger encryption and authentication techniques. Block Chaining Message Authentication Code Protocol (CCMP) in Counter Mode with cipher was introduced by WPA2. Advanced Encryption Standard (AES) encryption, used in WPA2, is a more dependable method. To generate keys in WPA2, a four-way handshake is necessary. To hack WPA/WPA2, we need to retrieve the network handshake packet. The "4-way handshake" packet is the only one that contains information that can help crack a password. Every time a user connects to the AP, a 4-way handshake occurs between the user and AP. The Counter mode (CTR) utilized in CCMP is based on the Cipher-Block Chaining (CBC) message authentication code of AES.

Data confidentiality is ensured by CTR, while authenticity and integrity are ensured by CBC message authentication code. The 128–256 keys in 32-bit sequences are supported by the AES block cipher algorithm. Both the key's and the block's lengths are selected separately.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 03 March 2024

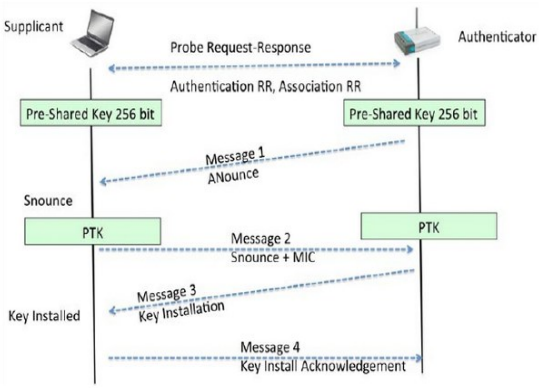


Fig 3.1 Four-way Handshake

One drawback of WPA2 is that its deployment requires updated hardware. Today's new hardware is all capable of supporting WPA2. However, it can be expensive to replace every piece of hardware in an existing network with new hardware that supports CCMP and AES.

4.TYPES OF MODES FOR WIFI

There are classified as discussed below:

1.Managed Mode
A Wi-Fi card acts like a regular client device connecting to a wireless network when it is in managed mode. It is able to connect to wireless router and engage in standard network functions including packet sending and receiving. For regular network connectivity, most Wi-Fi cards operate in managed mode, which is the default setting.

2. Monitor Mode
A unique operating mode called "Monitor mode," sometimes referred to as "RFMON" (Radio Frequency MONitor) mode, allows the Wi-Fi card to monitor all traffic on a given wireless channel passively without connecting to any particular access point. When in monitor mode, the Wi-Fi card records all wireless packets in the air, including ones that aren't meant for it, such those that are sent back and forth between AP and other devices. For packet sniffing, troubleshooting, security auditing, and network analysis, this mode is frequently used.

5.METHODOLOGY

1.Wi-Fi password Cracking
Steps Involved in Cracking Wi-Fi password:

The first step includes connecting the Wi-Fi adapter i.e.. TP-LINK Wireless Network Adapter (TL-WN722N) to the system and converting the default Managed Mode to Monitor Mode with the help of WLAN adapter. In this paper, we also discuss about the tool we have designed for password cracking “Wireless PassCrack”.

i.Channel Hopping: When the wireless system card is set to the listening mode, it can capture all the data channels that the network card can receive. We can jump on different channels and find the access points available within the network.
ii. Involved Access points: We obtain all the possible information about the involved access points in a specific channel. The SSID (Service Set Identifier) and BSSID (Basic Service Set Identifier) are present on these access points. An access point (AP) in wireless networking transmits the specific network identity (SSID) to identify a given wireless network. When users search for available networks on their devices, this is essentially the name of the Wi-Fi network that they are connected to. A BSSID is a unique identifier assigned to each Basic Service Set (BSS). A base station system (BSS) is a network of wirelessly communicating stations, typically made up of an access point (AP) and the client devices connected to it. It is comparable to a Media Access Control (MAC) address, that is a special identifier assigned to each network interface.
iii. Select the target access point : We select a single and specific target access point or SSID we want to hack.
iv. Packets capturing : In Wi-Fi networks, packet capture entails selecting an access point, then intercepting and collecting data packets that are transmitted between the connected devices and the access point. Once selected, the packet capturing tool records every wireless packet sent over the air within the network of the selected access point.
v. Details about devices linked to the target AP: We obtain all of the device-related data connected to the target AP, including the MAC address, IP address, and transmission packets as well as the handshake that takes place during the device-access point handshake.
vi. Capturing the Handshake: Usually, the client device and the AP exchange the following messages during the handshake:
Request for Authentication: The client device contacts the AP to request an authentication.
Response to Authentication Request: The AP replies to the request for authentication, signaling the fact that it is prepared to verify the client's identity.
Association Request: Possess the ability to join the network , the client device sends an association request to the AP.
Association Response: The client's request to join the network is either accepted or rejected by the AP in response to the association request.
Four-Way Handshake: The four-way handshake starts after the association request from the client is approved. To be capable of establishing encryption keys and secure the data transmission, the client and the AP exchange four messages during this handshake.
vii. Decrypt the key: Using the traditional brute force technique, we decrypt the key found in the handshake file. The captured data packet is cracked by the created password dictionary and the result is shown.The password appears in the “KEY FOUND” option. And the attack of brute force is successful.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 03 March 2024

2. EVIL-TWIN ATTACK using ESP-8266

The ESP8266 is a low-cost Wi-Fi microprocessor that is made in Shanghai, China by Espressif Systems and includes integrated TCP/IP networking software and microcontroller functionality. Microcontrollers can establish basic TCP/IP connections and connect to a Wi-Fi network with the help of this little module. Using IEEE 802.11 bgn, the ESP8266 module allows microcontrollers to connect to 2.4 GHz Wi-Fi.

This can be split into two parts:
1. Deauthentication attack
2. Evil-Twin attack

De-authentication Attack:

Among the most well-liked creations based on ESP8266 is esp8266 deauther, which enables users to use ESP8266 to attack Wi-Fi networks. Wireless network operations can be disrupted with by the esp8266 deauther through the transmission of deauthentication frames. This application is usable by ethical hackers and security researchers to evaluate wireless infrastructure security and find flaws. With the aim to execute a thorough pen test with the esp8266, it offers extra very helpful tools. We can find all the base stations and the access points available within the network and should select a target access point and start sending de-authentication frames to that access point, this implies disconnecting any gadget linked to that wireless access point.

Fig 5.1 ESP-8266 processor

Evil-Twin Attack:

An Evil-Twin attack can be performed by taking advantage of users confidence in well-known network names to trick them into connecting to rogue access points. Evil-Twin hotspots are Wi-Fi networks that mimic actual AP functions.

A Evil-Twin is typically used by hackers to carry out Wi-Fi phishing. Following the creation of the Evil-Twin, So as to complete the task, the user must connect the Wi-Fi phishing client penetration test. To accomplish the attack's goal, the packet capture tool is utilized to record every data packet that the client connected to the Evil-Twin sends and receives. The client is forced to detach and rejoin to the pseudo-AP a few times in order to pass through the network scanning. In the interest to trick unsuspecting customers into connecting, hackers set up rogue wireless access points with SSIDs that seem like real networks. Once connected, private information is accessible to attackers. being transferred across the network, giving them the access to intercept data, steal login credentials, or carry out more malicious actions. This attack vector highlights how important it is to have strong Wi-Fi security measures in place, like avoiding connecting to unprotected networks, using encryption methods like WPA2 or WPA3, and being cautious about confirming the legitimacy of networks, especially in public or high-risk areas. All packets going through the target AP are recorded using Wireshark to choose the wlan0mon interface for data capture. Specific packets may then be filtered and examined to obtain the required information.

7. SECURING WLAN NETWORKS

1.Set up firewalls on routers and access points to limit incoming and outgoing data according to pre-established criteria. By doing this, you can guard against outside dangers and stop unwanted access.

2.Regularly patch security flaws and make sure all network equipment, including routers, access points, and other devices, are running the most recent security features by updating their firmware.

3.Encourage consumers to connect to public or untrusted Wi-Fi networks via Virtual Private Networks (VPNs). With VPNs, all data transmitted between the device and the VPN server to provide security and privacy.

4.Intrusion Detection/Prevention Systems (IDS/IPS): Utilize IDS/IPS programs to keep an eye on network traffic for unusual activity and to automatically detect and report security concerns to administrators.

5.Users should be made aware of recommended practices for Wi-Fi security, which include avoiding unprotected networks, spotting phishing attempts, and routinely updating hardware and software.

6.Alter the default passwords. The majority of network equipment, such as wireless access points, come with default administrator passwords pre-configured to make configuration easier. Because these default passwords are so easily obtained online, they offer very little security.

7.Keep your antivirus program up to date. Update your virus definitions and install antivirus software. Additional capabilities of many antivirus products include the ability to identify or guard against spyware and adware.

8.Two-Factor-Authentication

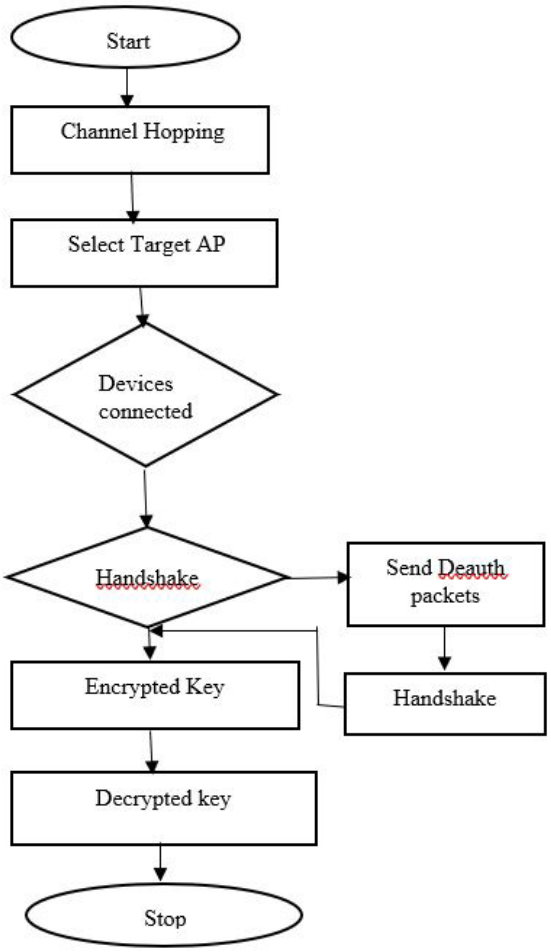
An additional level of protection is added to the login process using two-factor authentication. Users must input a code provided by an authenticator app in addition to their login and password. As a result, it is more challenging for someone to enter the network without authorization.

Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 03 March 2024

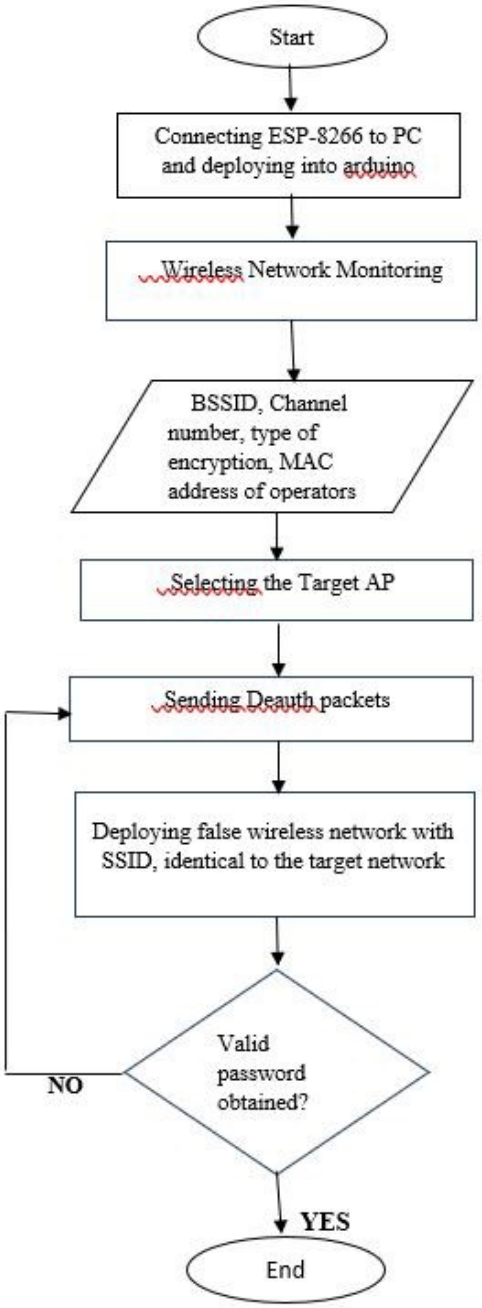
FLOW DIAGRAM

The flow diagram of the Wireless pass cracker is as follows:



FLOW DIAGRAM

The flow chart of the ESP8266 microcontroller model works as follows :



International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Volume 13, Issue 03 March 2024

RESULTS & DISCUSSIONS

To obtain the encrypted key, which is subsequently decoded into a plain-text password, the same process is followed. The method via which one gets the password required to access the Wi-Fi router takes up the most time during an intrusion. As a result, the time needed to obtain various passwords is calculated.

Password	Words Used	Time Required
123456780	9	1 hour 20 minutes
12345abce	9	1 hour 59 minutes
12345AdCg	9	2 hours 23 minutes
123453@T*	10	4 hour 49 minutes
123#4&56&98	11	Unable to determine

It is evident that using alphanumeric and symbol words makes it extremely difficult for the gadget to decipher the password. Following an attempt to crack the password for at least seven hours, the laptop being used to decode fails the decryption process. The password containing alphanumeric and symbols takes a long time to process.

8. CONCLUSION

This study presents the penetration test flow and key techniques of the wireless network, analyzing the vulnerabilities of the Wi-Fi network and popular encryption techniques. The different phases and technical techniques of the Wi-Fi penetration test grounded in Kali Linux are detailed in detail. The usefulness of Kali Linux-based Wi-Fi penetration test techniques, such as Wi-Fi password cracking, listening, scanning, grabbing, and Evil-Twin spoofing, is confirmed by a simulation experiment used to test the target Wi-Fi network. It makes a positive difference in the Wi-Fi network's security assessment.

9. FUTURE SCOPE

Furthermore, because any device that is electronically connected possesses the capacity to be dangerous, people and organizations need to be cautious when interacting with strange or suspicious connections or gadgets. To ensure that assist consumers and organizations in identifying possible risks related to their wireless devices, we want to continue our work on behavioral analysis of wireless devices for the purpose of looking for any signs of compromise or contamination.

9. REFERENCES

[1] Amith Raj M.P,Sneha H.R,Bindu Bhargavi S.M, Rekha Jayaram(2020) “A Study on 802.11 Wireless Routers Hacking Techniques and Security Encryption Levels”

[2] Se-Hwan Kwon, and Dea-Woo Park (2012)“Hacking and Security of Encrypted Access points in Wireless Network”

[3] 2010 2nd International Conference on Education Technology and Computer (ICETC). Wireless Hacking - A WiFi Hack by Cracking WEP.S Vinjosh Reddy, K SaiRamani, K Rijutha, Sk Mohammad Ali, CR. Pradeep Reddy

[4] http://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters/ - HTG Explains: The Difference Between WEP, WPA, and WPA2 Wireless Encryption (and Why It Matters)

[5] Securing Wi-Fi Networks, Kjell J. Hole, Erlend Dyrnes, Per Thorsheim

[6] V. Kumkar, A. Tiwari, P. Tiwari et al., “Vulnerabilities of wireless security protocols (WEP and WPA2),” International Journal of Advanced Research in Computer Engineering & Technology, vol. 1, no. 2, pp. 34–38, 2012.

[7] M. A. L. Joseph, “Web penetration testing with Kali Linux,” Computers & Security, vol. 1, no. 09, p. 40, 2013.

[8] H. Mustafa and W. Xu, "CETAD: Detecting evil twin access point attacks in wireless hotspots", 2014 IEEE Conference on Communications and Network Security, pp. 238-246, 2014.

[9] B. Xu, M. Peng, Q. F. Zhou, and X. Cheng, “Fake access point localization based on optimal reference points,” 2018 IEEE 4th International Conference on Computer and Communications (ICCC), pp. 784–788, 2018.

[10] Carballal, Fernandez-Lozano, Wi-Fi Handshake: Analysis of password patterns in Wi-Fi networks,2022.