Grenze International Journal of Engineering and Technology, June Issue

IoT based WiFi Penetration Testing Toolkit

S.Tamilselvi[1], R. Akash[2], A. Akshaya priya[3] and M. Hariharan[4]
[1-4]SRM Valliammai Engineering College/Department of Cyber Security, Chengalpattu, India
Email: tamilselvi.cys@srmvalliammai.ac.in, {akashcyber2020, aakshayapriya27, hariharanmadesh1802}@gmail.com

***Abstract*— This Project is a security-related applications. It makes use of technological and computer techniques. In existing methodology the device gather data like ssid, mac address from any nearby device and applied as a deauth(Jammer) which effectively shut down internet access. The ESP 8266 module is mostly used by this gadget. Wi-Fi Module is a part of the chip which perform Wi-Fi related functionalities. The Proposed methodology is sending de-authentication signals in order to cut off other networks, this module connect to any nearby device and only establish a connection to itself when the code scripts are run. Once linked, it create a large number of faux clones in an effort to confuse the user. We customize the chip to meet our needs because it includes inbuilt configuration software for versatility. This project works on combining Wi-Fi deauther or Jammer, Wi-Fi cloner or spoofer, Wi-Fi reconnaissance, Wi-Fi monitoring, and Wi-Fi DOS attack in one. All the module functions are combined by using Arduino IDE. In the world of wireless networking and remote control systems, this Wi-Fi module is important.**

Index Terms— **ESP12e module, IOT, Monitoring, DOS, Traffic analysis, Information gathering, Cloning, Deauth, Signal Block**

I. INTRODUCTION

Robust communication powers, network accessibility, and integrated sensors with a variety of functions have helped smart phones develop into potential mobile computing devices. They are able to offer crucial details about how people move around in their surroundings. By examining the wireless connection between client devices and the Access Points (APs), which is increasingly common due to advancements in wireless communication, it is useful to gain user information, including location, movement, and other behavior. Home automation systems and wireless IoT devices connect with one another and the internet using various wireless standards and protocols. The most widely used ones include Wi-Fi, Bluetooth, Zigbee, Z-Wave, and Lora WAN. Different levels of security and encryption are present in each of them, as well as unique features, advantages, and disadvantages. The devices that are connected to the internet which act as command and control points to communicate with other networked devices and store crucial data. Since we added more modules to the ESP8266, including a Wi-Fi deauther or jammer, a Wi-Fi cloner or spoofer, and a Wi-Fi reconnaissance module all in one, we are utilizing it instead. It act as jammer which shut down internet access in nearby surrounding. It use both hardware and software. This device uses an ESP8266 module, which includes a built-in Wi-Fi module to control its functions. This module connects to any nearby device by sending out de-authentication packets to block out other networks. It going to link to itself when the scripts are executed. Once linked, it attempts to deceive the user by producing a large number of fake clones.The sniffing system which provides user device information.

II. LITERATURE SURVEY

To identify the environmental security features associated with the current setup of the devices connected to the

Grenze ID: 01.GIJET.10.2.149

802.11 network, a penetration testing technique is established [1]. It use these techniques to create a topology of components needed for an inexpensive Wi-Fi sensing system and to create a low-cost Wi-Fi detecting system with edge ESP32 IoT microcontroller devices [2]. A multi-user authentication method that uses a single pair of common Wi-Fi devices to authenticate several users. The core concept is to profile Wi-Fi signals' multipath components and utilize them to uniquely describe each user for multi-user authentication [3]. The concept of a smart device is becoming more widely accepted. Our lives are becoming easier since web and software system technologies are readily available. One of the key components of the Internet of Things might be a smart home[4].
[5]A CDRA jammer is used to block calls at prisons which is used to increase integrity and confidentiality. Jammer offer security by reducing Wi-Fi annoyances at specific locations.
The authors of [6] [7] can gather information from any nearby device just by being in the same neighborhood.[8] The benefits of being omnipresent, device-free, and non-intrusive make the Wi-Fi-based behavior recognition (WBR) technology stand out among other behavior identification techniques. [9] This drives the creation of caching-as-a-service, in which content providers can store data on edge gadgets and networks and utilize it to strategically fill caches to enhance the experience of users in the network of interest. [10][11] Device recognition, one of the various forms of information that may be gathered through traffic on the network categorizing, has been a subject of discussion since the inception of the Internet. Studies examining both Wi-Fi and Ethernet data revealed that traffic characterization was able to accurately recognize a variety of data including IoT device kinds and phone app activity, smart devices Wi-Fi sensing through MIMO-OFDM.
[12][13] This device is capable of stopping numerous findings that show the types of attacks that spread, their inability to withstand them, and their speed. Wi-Fi packets can be detected and wireless traffic can be analyzed by a real-time wireless sniffing system. This offers a chance to get understanding of how people using mobile devices interact with their surroundings. One significant drawback of this concept is its vulnerability to wireless information loss, which is exacerbated by the absence of a clear specification for the practical implementation of Wi-Fi sniffers. [14][15] In recent years, there has been a lot of attention paid to indoor human monitoring, identification, and detection as critical enablers of creating smart environments, like smart homes, smart stores, and smart museums. Because of its widespread availability and affordability, Wi-Fi-based techniques have drawn the attention of numerous researchers among all RF-based technologies.
[16][17][18] The rapid advancement of telecommunication standards, which is rapidly approaching the deployment of 5G, forces us to find new approaches for delivering network services in places where radio network services are not available. The protocols' vulnerabilities for a significant number of denial-of-service (DoS) attacks are discussed, along with some workable solutions to prevent or lessen the impact of the assaults. This audit archive enhances the danger model that ought to be applied to secure communications based on WSN and IoT. It looks at many scenarios, a broad range of possible threats, and security requirements in WSN- and IoT-based communications. A logical structure of security and trust is seen to safeguard the show in WSN and IoT.
[19][20] The malicious behaviour pattern from Common Attack Pattern Enumerations and Classifications database. Attack graphs are used in the analysis to integrate several domains with regard to network, device, and human vulnerabilities. The interconnection of sensor networks, Bluetooth, Wi-Fi, GSM, LTE, Sigfix networks incur multiplied security challenges as compared to their individual issues.

III. ARCHITECTURE DIAGRAM

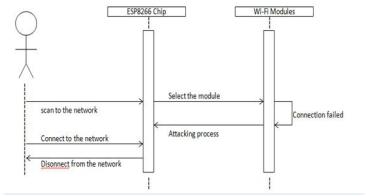

Figure 1: System flow diagram

This fig 1 shows the sequence of the modules. The user enters through the Wi-Fi modules to the particular network. [4]The microcontroller collects the data from the linked network. Each module has own function to gather the required information. Once connected, it can also fool the user by creating dozens of phony clones. This gadget can be used as a WiFi jammer, WiFi cloner, WiFi reconnaissance, WiFi monitor, and WiFi DOS all in one when kept within a variable range. The ESP 8266 can be configured to meet our needs because it includes integrated configuration software for versatility.

IV. METHODOLOGY

A. Wi-Fi Jammer

Wi-Fi connection is blocked or jammed by jamming the Wi-Fi network, and even people who know the password are unable to join to that Wi-Fi network. A small Microcontroller ESP12E, commonly known as a Wi-Fi module or NodeMCU, which is used for this. We are jamming the network with a Python script.

The process of flashing the Deauther firmware onto an ESP8266 board for the purpose of creating a Wi-Fi Deauthentication tool.

Step 1: Download the .bin file for your specific ESP8266 board from deauther.com.
Step 2: Open the website esp.huhn.me in a compatible browser (such as Chrome).
Step 3: Connect your ESP8266 board to your computer via USB.
Step 4: Use the provided interface to establish a connection to your ESP8266 board and select the appropriate serial port.
Step 5: Choose the Deauther .bin file you downloaded earlier.
Step 6: Click the "Program" button to flash the Deauther firmware onto your ESP8266 board.
Step 7: After flashing, navigate to deauther folder and open the esp8266_deauther.ino file with the arduinoIDE software.
Step 8: In the software, go to File > Preferences and add Additional Boards Manager Packages.
Step 9: Now go to Tools > Board > Board Manager, search for deauther, and install the Deauther ESP8266 Boards.
Step 10: Select your specific ESP8266 board from the Tools> Board menu and ensure that it is set to "Deauther ESP8266 Boards" (not ESP8266 Modules).
Step 11: Plug in device and select COM port from the Tools > Port menu.
Step 12: Optionally, to reset any previous settings, select Tools > Erase Flash > All Flash Contents.
Step 13: Finally, click upload button in the Arduino IDE to add the Deauther firmware to the ESP8266 board.

The process of attacking are given below

Step 1: Scan the Access point.
Step 2: Select the Access Point which you want to attack.
Step 3: Click on attack tab and deauth option.
Step 4: Select START button to perform attack and click on STOP button to end the attack.

B. Wi-Fi Spoofing

Wi-Fi cloning or spoofing is the act of using an existing access point's Wi-Fi access data by pushing a buttonThe SSID is written down. After that, use a device like a Wi-Fi Pineapple to establish a fresh account with that exact SSID.

Devices that are connected are unable to distinguish between authentic connections and false ones.

Wi-Fi cloning is also called as beacon which is used to clone Wi-Fi network using an ESP8266 module. These are the steps to beacon:

(i) *Set up the ESP8266*: Connect the ESP8266 module to a microcontroller or development board, and program it using the Arduino IDE or other compatible development environments.
(ii) *Configuration*: Select the target button, and start connection the appropriate functions in the ESP8266 library to set the SSID (Wi-Fi network name) and password to match those of the target network. This step effectively "clones" the network's settings onto the ESP8266 module.
(iii) *Connect to the network*: Utilize the ESP8266's Wi-Fi connection functions to establish a connection to the cloned network using the cloned SSID and password. Then Select stop button once the work over.

C. Wi-Fi reconnaissance

Wi-Fi reconnaissance, also known as wireless network reconnaissance or Wi-Fi scanning, involves the process of actively or passively gathering information about wireless networks in a particular area. Wi-Fi reconnaissance used for various purposes, including network troubleshooting, security auditing, and understanding the surrounding Wi-Fi landscape.

(i) *Set up the ESP8266*: Open the attacking application and select the Wi-Fi reconnaissance option.
(ii) *Program the ESP8266*: Select the Recconaissance program to configure the ESP8266 to utilize the ESP8266's capabilities to scan for nearby Wi-Fi networks.
(iii) *Interpret the Results*: Analyze the information collected during the scan, including the names (SSIDs) and signal strengths of nearby networks. Use this information for Wi-Fi reconnaissance, such as identifying available networks, signal strengths, and potentially detecting rogue networks. Select stop button after gathering the data.

D. Wi-Fi monitor

The process of gathering and examining data on Wi-Fi networks in order to learn more about their functionality, security, and usage is known as Wi-Fi monitoring. It entails monitoring connected devices, network traffic, signal strength, and other pertinent variables to guarantee smooth functioning and address any possible problems.
Following steps to monitor the Wi-Fi traffic
Step1: After configuring Wi-Fi modules into the ESP8266 chip. Select the Monitor option to identify the victim network.
Step2: Monitoring the packets using oled display, obtaining data packets sent across the Wi-Fi network and storing them. Shows information such as source and destination addresses, signal strength, and data payload. Then click to stop the connection.

E. Wi-Fi DoS

Wi-Fi Denial of Service (DoS) attack involves several stages. In the beginning identifies a target Wi-Fi network and proceeds to craft malicious packets designed to exploit vulnerabilities or overwhelm the network.
Following process to take Wi-Fi dos.
Step1: select the target ssid.
Step2: Sending of forged Deauthentication or disassociation frames to disconnect devices from the target Wi-Fi network, causing service disruption.
Step3: After sending forged frames check the process of the work on victim system.
Step4: Stop the sending packets.
There are several ways to overload network resources and cause connectivity problems, including sending too many beacon frames, too many identification requests, or even jamming signals. Additionally, attackers may exploit vulnerabilities in network protocols or security mechanisms, employing techniques like brute force attacks or attempting to crack encryption keys. It's important to note that conducting Wi-Fi DoS attacks is illegal and unethical without explicit authorization, and understanding these processes serves as a means of raising awareness about potential security threats in the digital landscape.

V. DISCUSSION

Device recognition, one of the various forms of information that may be gathered through traffic on the network categorizing, has been a subject of discussion. Examining internet data revealed that traffic characterization was able to accurately recognize a variety of data including IoT device and phone app activity. These earlier studies made the assumption that traffic was as it would appear to a network observer who is gathering TCP/IP level packets. This expose reveals the device's identifiable and helpful network features. For example, the authors of observe that many IoT devices using the port number of their destination utilize a single characteristic signature. It is necessary to assess the security and functionality of such a fundamental device during the attack simulation in order to build a range of projects that deal with the Web connected Issues and impact system security. It gives stronger security measures, mitigate vulnerabilities, and enhance their overall cyber security resilience. Using the ESP8266 for packet sniffing allows security professionals to capture and analyze network traffic. It provide the types of data flowing through the network, potential security vulnerabilities, and areas for improvement in data protection. In Deauthentication attacks can result in the temporary disruption of Wi-Fi connectivity for targeted devices. The outcome demonstrates the network's resilience to such attacks and identifies potential security measures that need improvement. The ESP8266 can be used to scan and identify Wi-Fi networks, revealing information about network names, signal strength, and security protocols. The results can help security professionals assess the visibility of a network and identify potential points of entry.

VI. CONCLUSION

The methodology has given its compact size and low price, this microcontroller's capacity to scan surrounding devices for networks. It is incredible how many networks it instantly link to, how quickly it stop a device from connecting, and how quickly it spot an active Wi-Fi attack. Cybercriminals continue to be intrigued by the ESP 8266's possibilities. The NodeMCU, which is a prototype board powered by the ESP 8266 may be used to either detect hackers attacking our large system due to its compact size and low cost. This module is less expensive than a Raspberry Pi, and the impact of these devices is minimal. With the use of this method, security products that creatively exploit big WPA2 Wi-Fi protocol flaws can be created. One of the ESP8266's most potent capabilities is the ability to generate practically any type of packet from scratch. Instead of this ESP32 is introduced to enhance

the features. The WPA3 standard advances this strategy by making Deauth packets challenging to forge, though most networks will continue to be vulnerable until the new standard is widely adopted. Additionally, in an effort to make the kit more functional.

REFERENCES

[1] D. Koutras, P. Dimitrellos, P. Kotzanikolaou and C. Douligeris, "Automated Wi-Fi Incident Detection Attack Tool on 802.11 Networks," IEEE Symposium on Computers and Communications (ISCC), Gammarth, Tunisia, 2023, pp. 464-469, doi: 10.1109/ISCC58397.2023.10218077.

[2] S. M. Hernandez and E. Bulut, "Wi-Fi Sensing on the Edge: Signal Processing Techniques and Challenges for Real-World Systems," IEEE Communications Surveys & Tutorials, 2023 ,vol. 25, no. 1, pp. 46-76, Firstquarter, doi: 10.1109/COMST.2022.3209144.

[3] H. Kong, L. Lu, J. Yu, Y. Chen, X. Xu and F. Lyu, "Toward Multi-User Authentication Using Wi-Fi Signals," IEEE/ACM Transactions on Networking, Oct. 2023, vol. 31, no. 5, pp. 2117-2132, doi: 10.1109/TNET.2023.3237686.

[4] R. Niranjana, A. S, V. M and V. S, "Effectual Home Automation using ESP32 NodeMCU," International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2022, pp. 1-5, doi: 10.1109/ICACRS55517.2022.10028992.

[5] S. Bhushan and R. S. Yaduvanshi, "Cylindrical Dielectric Resonator Antenna for Wi-Fi Jammer for blocking Wi-Fi calls at prison," IEEE 6th Conference on Information and Communication Technology (CICT), Gwalior, India, 2022,pp. 1-4, doi: 10.1109/CIC T566 98.2022.9997924.

[6] R. Singh, R. Thakkar, M. Thakkar, U. Rote, S. Patil and B. Ingle, "Wi-Fi Deauth and Cloning using ESP8266," 5th International Conference on Advances in Science and Technology (ICAST), Mumbai, India, 2022, pp. 1-5, doi: 10.1109/ICAST55766.2022.10039517.

[7] M. Alyami, I. Alharbi, C. Zou, Y. Solihin and K. Ackerman, "Wi-Fi-based IoT Devices Profiling Attack based on Eavesdropping of Encrypted Wi-Fi Traffic," 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2022, pp. 385-392, doi: 10.1109/CCNC49033.2022.9700674.

[8] J. Liu, Y. He, C. Xiao, J. Han, L. Cheng and K. Ren, "Physical-World Attack towards Wi-Fi-based Behavior Recognition," IEEE INFOCOM - IEEE Conference on Computer Communications, London, United Kingdom, 2022, pp. 400-409, doi: 10.1109/INFOCOM48880.2022.9796920.

[9] L. Chhangte, N. Karamchandani, D. Manjunath and E. Viterbo, "Towards a Distributed Caching Service at the Wi-Fi Edge Using Wi-Cache," IEEE Transactions on Network and Service Management, Dec. 2021, vol. 18, no. 4, pp. 4489-4502, , doi: 10.1109/TNSM.2021.3105496.

[10] M. Alyami, M. Alkhowaiter, M. A. Ghanim, C. Zou and Y. Solihin, "MAC- Layer Traffic Shaping Defense Against Wi-Fi Device Fingerprinting Attacks," IEEE Symposium on Computers and Communications (ISCC), Rhodes, Greece, 2022, pp. 1-7, doi: 110.1109/ISCC55528.2022.9913056.

[11] S. Avallone, P. Imputato, G. Redieteab, C. Ghosh and S. Roy, "Will OFDMA Improve the Performance of 802.11 Wi-Fi Networks?," IEEE Wireless Communications, June 2021, vol. 28, no. 3, pp. 100-107, doi: 10.1109/MWC.001.2000332.

[12] A. Ye, Q. Li, Q. Zhang and B. Cheng, "Detection of Spoofing Attacks in WLAN-Based Positioning Systems Using Wi-Fi Hotspot Tags," IEEE Access, 2020, vol. 8, pp. 39768-39780, doi: 10.1109/ACCESS.2020.2976189.

[13] Z. Zhu, S. Chen and L. Lu, "Research on Real MAC Address Acquisition Technology for WI-FI Connection," 2021 2nd International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT), Shanghai, China, 2021, pp. 561-564

[14] Y. Li, J. Barthelemy, S. Sun, P. Perez and B. Moran, "A Case Study of Wi-Fi Sniffing Performance Evaluation," IEEE Access, 2020, vol. 8, pp. 129224-129235,doi: 10.1109/ACCESS.2020.3008533.

[15] Y. He, Y. Chen, Y. Hu and B. Zeng, "Wi-Fi Vision: Sensing, Recognition, and Detection With Commodity MIMO-OFDM Wi-Fi," IEEE Internet of Things Journal, Sept. 2020, vol. 7, no. 9, pp. 8296-8317, doi: 10.1109/JIOT.2020.2989426.

[16] C. Capota, S. Halunga, O. Fratu, S. Eugen and P. Mădălin, "Security Aspects and Vulnerabilities in Authentication Process Wi-Fi Calling – RF measurements," 2021 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Bucharest, Romania, 2021.

[17] Y. Meng, J. Li etal, "Revealing Your Mobile Password via Wi-Fi Signals: Attacks and Countermeasures", IEEE Transactions on Mobile Computing, 1 Feb. 2020, vol. 19, no. 2, pp. 432-449, doi: 10.1109/ TMC. 2019.2893338.

[18] A. Raghuprasad, S. Padmanabhan etal, "Security Analysis and Prevention of Attacks on iot Devices", International Conference on ICCSP,2022 pp. 0876- 0880, doi: 10.1109/ICCSP48568.2020.9182055.

[19] Tripathi, A. Thakur etal, "Attack Graphs for Standalone Non-Public 5G Networks", IEEE FNWF, 2022, pp. 158-163, doi: 10.1109/FNWF 55208. 2022.00036.

[20] M. F. Ashfaq, M. Malik etal, "Classification of IoT based DDoS Attack using Machine Learning Techniques", 16th International Conference on IMCOM, 2022, pp. 1-6, doi: 10.1109/IMCOM53663.2022.9721740.