Exploiting Flaws in A Wifi Network

Mrinal Sharma
Btech-Student, SCOPE
VIT Vellore
Vellore, India

Rohan Gupta
Btech-Student, SCOPE
VIT Vellore
Vellore, India

Harsh Rajpal
Btech-Student, SCOPE
VIT Vellore
Vellore, India

***Abstract*—In today's world, cybersecurity is required everywhere. It is a worldwide industry that will face a global shortage of more than 2.2 million information security specialists by 2022. Over the past few decades, almost all our systems have been entirely digitized. Because of their high speed and accuracy, accounting and communications have become almost completely digital. However, such systems are prone to attacks. Not physical attacks but cyber-attacks. A cyber-attack can maliciously disable computers, steal data, or use a breached computer as a launch point for other attacks. If not managed properly, it can cause the loss of critical data and leakage of private information into the public, resulting in losses upwards of billions of dollars. Thus, knowledge and prevention of such attacks are of utmost importance.**

Keywords— ARP Poisoning, DOS, SQL Injection, Exploitation, Mitigation, Kali Linux, Authentication, Middle-man, Packet Tracing.

I. INTRODUCTION

Each year, over 30 million cyber-attacks occur. It is expected to cost the world $10.5 Trillion annually by 2025. So, we must understand the techniques used to execute such attacks and what measures can be adopted to prevent them. This paper demonstrates some of the most common types of cyberattacks, such as ARP Poisoning, DOS attacks, and SQL Injections.

● ARP Poisoning (also known as ARP Spoofing) is a type of cyber-attack carried out over a Local Area Network (LAN) that involves sending malicious ARP packets to a default gateway on a LAN to change the pairings in its IP to MAC address table.

● A Denial-of-Service attack (DoS attack) is a cyber-attack that aims to render a computer or network resource inaccessible to its intended users by sabotaging the operations of a host connected to the Internet for an extended period.

● SQL injection is a flaw in online security that enables an attacker to obstruct database requests made by an application. Attackers frequently can update or remove this data, which results in long-lasting modifications to the application's content or behaviour. We also work to provide sound mitigation techniques that can deter such attacks.

II. LITERATURE SURVEY

This study aims to summarize the body of knowledge and develop a comprehensive taxonomy of Wi-Fi network attacks [1]. In this study, a novel and practical keystroke inference framework, WindTalker, is introduced that can be used to infer the sensitive keystrokes on a mobile device through WIFI-based side-channel information [2]. To design an effective yet lightweight WIFI localization privacy algorithm, this paper proposes reinforcing dummy techniques with plausible dummy locations to resist the attacks [3]. This paper proposes a method for detecting spoofing and Sybil attacks using the same techniques [4]. In this paper, "EvilScout," is proposed, an evil twin detection and mitigation framework that utilizes the information of the IP prefix distribution by the Legitimate Access Point [5]. The article here discusses different attack vectors of Wi-Fi networks and how they can be exploited [6]. The main contribution is to analyze the technology offered in the new Wi-Fi Protected Access III (WPA3) security scheme and provide the first comprehensive security analysis and discussion to determine whether it has addressed the vulnerabilities of its predecessor [7]. This article discusses how technology like the 802.11n standard with flaws is helping in spreading malware as the same exploit can be used on a wide array of devices using the same standards [8]. This article goes beyond Wi-Fi networks and showcases radios' weaknesses, potential Internet attacks, etc. [9]. This study focuses on conducting organized vulnerability testing on the WIFI capabilities of a vehicle infotainment system to determine the weaknesses of the automotive infotainment system [10]. In this paper, we have studied the impact of DDoS and EDDoS on WIFI smart home devices. It focuses on IoT devices' connection and energy consumption when they are under attack. Three major conclusions were drawn [11]. In this research, we have learned how to protect data in open WIFI as it can be easily accessed by anyone on the network [12]. In this study, we looked at wireless communication designs and protocols, security challenges, the types of threats utilized to launch an assault, and their answers [13]. In this study, we have studied and tested the application of secure interaction over WIFI signals. We have tested how various factors can be merged to make the system more secure [14]. This article highlights the various methods of penetration testing Kali Linux offer. We can explore all kinds of vulnerabilities to 4 provide the best defense against hackers [15]. This article showcases weaknesses in radios and potential attacks over the Internet and goes beyond Wi-Fi networks [16]. They conducted the first security investigation utilizing commodity devices on operational Wi-Fi calling services in three major US operators' networks. They reveal that present Wi-Fi calling security isn't foolproof and point out three flaws [17]. They create two proof of concept attacks by exploiting them: user privacy leakage and telephone harassment or denial of voice service (THDoS), bypassing the security defenses placed on mobile devices and network infrastructure [18]. Wdev-Fuzzer is a fuzzer that may be used to find security flaws in Wi-Fi device drivers, according to this study. Their preliminary tests with a Windows Mobile 5 device driver show that Wdev-Fuzzer can detect previously undetected issues [19]. They suggest two efficient jamming techniques: low-data rate random jamming and protocol-aware RF jamming based on shot noise. They also developed a tight upper bound for the duration and number of shot noise pulses in Wi-Fi, GSM, and WiMax networks [20]. This work investigates the Wi-Fi calling security requirements that attackers can utilize to reveal users' locations, device technical details, access to sensitive data, and DoS attacks. They tested the protocol for various DoS assaults before coming up with some effective remedies to avoid or mitigate the effects of the attacks [21]. Using this approach, they investigated the remaining available capacity in terms of available WIFI throughput that could be distributed over the transferred LTE users. Then the minimum required number of WIFI APs supporting the LTE network for efficient traffic offloading using this approach [22]. They look into the joint channel, power, and carrier sense threshold allocation problem in IEEE 802.11ac networks, demonstrating that the current practice of using narrower channels at maximum power when the deployment is dense yields significantly worse performance than a solution using the widest possible channel at much lower power [23]. This article describes a passive device-free FDS for smart homes based on a commodity WIFI framework, primarily made up of two hardware platforms and client applications [24]. An integrated space and earth network system is proposed to provide users with a ubiquitous wireless network connection. Three communication methods' technologies and obstacles are sorted out, and the ways they might be integrated and utilized are evaluated through significant research and analysis [25]. They described a system called WIFI Doppler Frequency Shift (WiDFS) in this paper, which uses channel state information (CSI) acquired from commercial-off-the-shelf (COTS) WIFI devices to enable single-target real-time passive tracking. They consider a typical system design that includes a single antenna transmitter and a three-antenna receiver, but their technique can be easily adapted to various configurations [26].

III. PROBLEM STATEMENT:

In the present world, every person uses the Internet and is vulnerable to internet-based attacks if certain precautions are not taken. Cyber-attacks can cause immeasurable damages to a company. They can cause substantial damages such as stopping services, ruining the public's trust in a company, and leaking critical information that may affect corporate survival. Attacks like DOS have become one of the most prominent forms of cybercrime over the last few years. Thus, before finding a solution to these problems, one must be able to perform and understand these attacks.

IV. THEORETICAL BACKGROUND:

The WPA2 protocol is hard to hack but not impossible. A few vulnerabilities had been discovered long back, and since it is a widespread protocol, it has been used by all modern devices for protection and hackers for intrusion. This protocol allows disconnecting a device with a single de-auth packet, for which a person does not need to be connected. This can be misused in many ways, some of which will be demonstrated in our project.

V. OVERVIEW OF THE PROPOSED SYSTEM

A. *Proposed Methodology*

We will be using different methods to carry out our network-based attacks:

1. DoS attack: We try sending spoofed packets of information that hit every computer in a targeted network, taking advantage of misconfigured network devices.

2. ARP spoofing: We will use arpspoof to perform ARP poisoning in a LAN environment using a VMware workstation in which we have installed Kali Linux and driftnet and urlsnarf to sniff the local traffic in LAN.

3. SQL injection: To conduct a SQL Injection attack, we look for user inputs that are open to vulnerability on the website or in the web application. Such user input is used directly in a SQL query on a web page or web application with a SQL Injection vulnerability. We can make input content. This material is the main component of the attack and is frequently referred to as a malicious payload. The database is then used to perform malicious SQL commands after sending this content.

B. *Algorithm and Steps Explanation:*

1. Denial of Service on a home network

   An attempt to disable a computer system or network so its intended users cannot access it is known as a denial-of-service (DoS) attack. DoS attacks achieve this by sending information that causes crashes or by saturating the target with traffic. In both situations, the DoS attack denies expected services or resources to legitimate users (i.e., employees, members, or account holders). DoS attacks frequently target the web servers of well-known companies, including banking, media, and business firms, as well as governmental and commercial institutions. DoS attacks can cost the victim a lot of time and money to deal with, even though they typically do not result in the loss or theft of crucial data or other assets. We are trying to implement the DOS attack on a home network modem in this implementation. Requirements – A WIFI adapter, Kali Linux, Python. In this attack, the WIFI adapter initially scans for various networks in the vicinity; when it gets the WIFI address which has to be attacked then, it starts scanning which all devices are connected with the particular WIFI, and with the help of airplay-ng, it finds out the MAC addresses of all the connected devices and the modem. Now it starts sending the DE authentication packets to the modem on behalf of the other connected devices.

2. ARP-Spoofing

   ARP spoofing, also referred to as ARP poisoning, is a Man in the Middle attack that enables attackers to eavesdrop on network device communication. This is how the attack operates:

   ● The attacker needs to have network access. The attacker uses a spoofing tool, such as Arp spoof or driftnet, to send out forged ARP responses after scanning the network to find the IP addresses of at least two devices. Let's say these are a workstation and a router.

- The fake responses claim that the attacker's MAC address is the correct MAC address for both the workstation's and router's IP addresses. The router and workstation are tricked into connecting to the attacker's machine rather than to each other. This is how the attack operates:
- Continue routing the communications as-is—the attacker can sniff the packets and steal data, except if it is transferred over an encrypted channel like HTTPS.
- Perform session hijacking—if the attacker obtains a session ID, they can gain access to accounts the user is currently logged into.
- Alter communication—for example, pushing a malicious file or website to the workstation.

3. SQL Injection

A SQL injection attack involves inserting, or "injecting," a SQL query through the application's input data from the client. A successful SQL injection exploits can read sensitive data from the database, change database data (Insert/Update/Delete), perform database administration operations (like shutting down the DBMS), and recover the content of a specific file on the DBMS file system. In some cases, issue commands to the operating system. To interfere with predefined SQL commands, SQL commands are injected into data-plane input in SQL injection attacks.

- SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.
- SQL Injection is very common with PHP and ASP applications due to the prevalence of older functional interfaces. Due to the nature of programmatic interfaces available, J2EE and ASP.NET applications are less likely to have easily exploited SQL injections.
- The attacker’s skill and imagination limit the severity of SQL Injection attacks and, to a lesser extent, defence in depth countermeasures, such as low privilege connections to the database server. In general, consider SQL Injection a high impact severity.

C. *Architecture for the Proposed System*

a) The DOS attack Diagram

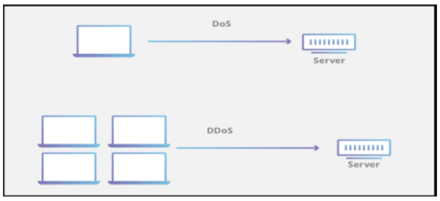

Fig. 1. The DOS – attack diagram

b) ARP Spoofing

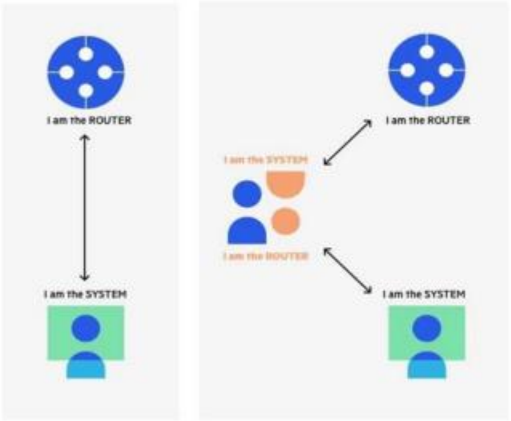

Fig. 2. The ARP spoofing attacker pretends to be both sides of a network communication channel

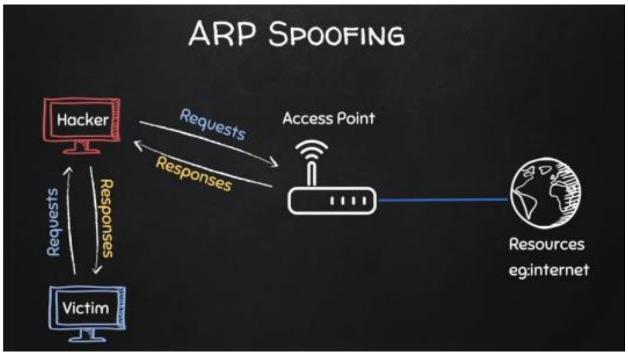

Fig. 3. Pictorial demonstration of ARP spoofing

CONCLUSIONS AND FUTURE WORK

In conclusion, we have demonstrated how we can use a better cap on Linux to execute a Man-in-the-Middle attack. Such an attack would allow us to connect the client and the router and view private data via captured packets. We have also proposed a viable method to prevent and detect it. Then we have also carried out a DoS attack using Kali Linux, a Linux distribution made specifically for pen-testing. After launching the attack, we can see the hosts and the clients connected to the network won’t be able to access the Internet as it gets disconnected indefinitely. This attack is so powerful that the client won’t be able to connect back to the same network till the time the attack is going on. We have also worked out how an SQL Injection attack can be carried out and have developed an extensive framework to prevent it. For future work, we can include some more common types of network attacks such as Botnets, DNS Spoofing and Packet Sniffers, and like this project, we can test methods and protocols to prevent them.

RESULTS AND DISCUSSIONS

Simple actions to minimize security risks and address system vulnerabilities are insufficient; Instead, a seamless policy implementation process supported by solid procedures is required. The security development process necessitates a full awareness of a system's assets and the identification of potential vulnerabilities and threats. Furthermore, knowing about prospective assaults allows system developers to decide better where monies should be invested. It's critical to research the many types of attack actors and figure out which ones are most likely to assault a system. It's easier to see which threat could exploit which system weakness after describing and documenting all threats and their respective actors. To reach their goals or objectives, attackers use various methods, tools, and strategies to exploit vulnerabilities in a system. To avoid potential damage, an organization must first understand the motives and capabilities of the attackers. When a vulnerability impacts the security of a network or a cryptographic system, it risks many devices or services. In situations like these, it's critical that the victim remains calm and assesses the vulnerability's theoretical and practical risks. To estimate the vulnerability's possible impact, it's also a good idea to consider the available security measures.

One of the key concerns and challenges raised by any vulnerability is the manufacturers' willingness to respond to such situations and plan and distribute patches to their products on time without leaving them vulnerable. Because internet-connected gadgets are becoming more common, it's critical to concentrate on keeping this ecosystem safe, especially since we've already seen security events aimed at jeopardizing cyber security. More research is needed to fill the gaps in information about threats and cybercrime and provide the essential methods to prevent possible attacks by lessening prospective threats and their repercussions.

REFERENCES

[1] Mark Vink, A Comprehensive Taxonomy of Wi-Fi Attacks, Master Thesis Cyber Security, Radboud University Nijmegen

[2] Yan Meng, Jinlei Li, Haojin Zhu, Senior Member, IEEE, Xiaohui Liang, Member, IEEE, Yao Liu, Member, IEEE, and Na Ruan, Member, IEEE, Revealing Your Mobile Password via WIFI Signals: Attacks and Countermeasures, IEEE transactions on mobile computing, Vol. 14, No. 8, August 2015.

[3] Ping Zhao, Member, IEEE, Wuwu Liu, Guanglin Zhang, Member, IEEE, Zongpeng Li, Senior Member, IEEE, and Lin Wang, Senior Member, IEEE, Preserving Privacy in WIFI Localization with Plausible Dummy Locations, IEEE Transactions On Vehicular Technology.

[4] Yingying Chen, Member, IEEE, Jie Yang, Student Member, IEEE, Wade Trappe, Member, IEEE, and Richard P. Martin, Member, IEEE, Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks, IEEE Transactions On Vehicular Technology, Vol. 59, No. 5, June 2010.

[5] Pragati Shrivastava, Mohd Saalim Jamal, and Kotaro Kataoka, EvilScout: Detection and Mitigation of Evil Twin Attack in SDN Enabled WIFI, IEEE Transactions On Network And Service Management, Vol. 17, No. 1, March 2020.

[6] Hal Berghel and Jacob Uecker, WIFI Attack Vectors, Digital Village.

[7] Christopher P. Kohlios, Thaier Hayajneh, A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3, Fordham Center for Cybersecurity, Fordham University, New York, NY 10023, USA.

[8] Hao Hu, Steven Myers, Vittoria Colizza, and Alessandro Vespignani, WIFI networks and malware epidemiology, February 3, 2009.

[9] K. Brima, I. Opurum, R. Zolotyi (Ternopil Ivan Puluj National Technical University), Research of Wi-Fi systems protection efficiency.

[10] E. F. M. Josephlal and S. Adepu, "Vulnerability Analysis of an Automotive InfotainmentSystem's WIFI Capability," 2019 IEEE 19th International Symposium on High AssuranceSystems Engineering (HASE).

[11] B. Tushir, Y. Dalal, B. Dezfouli, and Y. Liu, "A Quantitative Study of DDoS and E-DDoSAttacks on WIFI Smart Home Devices," in IEEE Internet of Things Journal, vol. 8, no. 8,pp. 6282-6292, 15 April15, 2021.

[12] E. Al Neyadi, S. Al Shehhi, A. Al Shehhi, N.Al Hashimi, M. Qbea'H and S. Alrabaee, "Discovering Public Wi-Fi Vulnerabilities Using Raspberry Pi and Kali Linux," 2020 12thAnnual Undergraduate Research Conference on Applied Computing (URC), 2020.

[13] Nazir, Rashid & Laghari, Asif & Kumar, Kamlesh & David, Shibin & Ali, Munwar (2021). Survey on Wireless Network Security. Archives of Computational Methods in Engineering.

[14] Y. Zhao et al., "Device-Free Secure Interaction With Hand Gestures in WIFI-Enabled IoTEnvironment," in IEEE Internet of Things Journal.

[15] Lu, He-Jun, and Yang Yu. "Research on WIFI Penetration Testing with Kali Linux."Complexity 2021.

[16] Brima, K., I. Opurum, and R. Zolotyi. "Research of WIFI systems protection efficiency."Матеріали VIнауково-технічної конференції „Інформаційні моделі, системи татехнології " (2018).

[17] T. Xie et al., "The Untold Secrets of WIFI-Calling Services: Vulnerabilities, Attacks, and Countermeasures," in IEEE Transactions on Mobile Computing.

[18] T. Xie, G. -H. Tu, C. -Y. Li, C. Peng, J. Li, and M. Zhang, "The Dark Side of Operational Wi-Fi Calling Services," 2018 IEEE Conference on Communications and Network Security (CNS), 2018.

[19] M. Mendonca and N. F. Neves, "Fuzzing Wi-Fi Drivers to Locate Security Vulnerabilities," 10th IEEE High Assurance Systems Engineering Symposium.

[20] A. Hussain, N. A. Saqib, U. Qamar, M. Zia, and H. Mahmood, "Protocol-aware radio frequency jamming in Wi-Fi and commercial wireless networks," in Journal of Communications and Networks.

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

[22] D. Saliba, R. Imad, S. Houcke and B. E. Hassan, "WIFI Dimensioning to offload LTE in 5G Networks," 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), 2019.

[23] S. Malekmohammadi, C. Rosenberg and R. Stanica, "On the Use of Wide Channels in WIFI Networks," 2019 IEEE 44th Conference on Local Computer Networks (LCN), 2019.

[24] J. Ding and Y. Wang, "A WIFI-Based Smart Home Fall Detection System Using Recurrent Neural Network," in IEEE Transactions on Consumer Electronics.

[25] C. Zeyu, "6G, LIFI, and WIFI Wireless Systems: Challenges, Development and Prospects," 2021 18th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), 2021.

[26] Z. Wang, J. A. Zhang, M. Xu, and J. Guo, "Single-Target Real-Time Passive WIFI Tracking," in IEEE Transactions on Mobile Computing.