I.J. Wireless and Microwave Technologies, **2025, 5, 34-46**
Published Online on October 8, 2025 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2025.05.03

Wi-Fi Attacks by Exploiting ARP and DNS Vulnerabilities: A Security Study

Asmaa A. Ghanim*
Department of Electrical Engineering, University of Mosul, Mosul, Iraq
E-mail: asmaa.22enp38@student.uomosul.edu.iq
ORCID iD: https://orcid.org/0009-0002-3563-6642
*Corresponding Author

Mohammed Y. Thanoun
Department of Electrical Engineering, University of Mosul, Mosul, Iraq
E-mail: myounisth@uomosul.edu.iq
ORCID iD: https://orcid.org/0000-0002-2852-3917

Received: 11 October, 2024; Revised: 21 May, 2025; Accepted: 16 July, 2025; Published: 08 October, 2025

Abstract: This research aims to evaluate the security risks associated with open wireless networks, especially Man-in-the-Middle (MITM) attacks that exploit the Address Resolution Protocol (ARP) and Domain Name System (DNS). The penetration testing process was conducted by creating a secure and controlled laboratory and using a set of tools available in Kali Linux to demonstrate how attackers can exploit these vulnerabilities to gain unauthorized access to victims' devices, steal their sensitive data, and control their devices remotely The research focused on analyzing the effectiveness of social engineering (phishing) attacks under MITM attacks, where a fake web page was created to trick victims into entering their personal data and another web page was created to try to trick victims into downloading malware consisting of an attack payload that aims to create a Reverse Transmission-Control-Protocol (TCP) shell that enables the hacker to explore the target device and execute code using the Metasploit framework. The research results showed the effectiveness of combining ARP and DNS spoofing with phishing attacks and malware injection attacks. The results also showed that open wireless networks are highly vulnerable to attacks and that end users are the weakest link in the security chain. The research also emphasizes the need to develop more effective security solutions to protect core protocols such as ARP and DNS.

Index Terms: MITM, ARP Spoofing, DNS Spoofing, Phishing Attack, Reverse TCP Shell, Metasploit Framework, Bettercap

1. Introduction

The Internet has become the most important thing in life in the current world. The majority of daily tasks, including online banking, social media usage, and online shopping, now require the internet and mobile networks. People are becoming more and more dependent on the internet, which makes them easier targets for hackers. The primary goal of hackers is to steal confidential data from different companies, which might result in losses of money [1]. The wireless network linking to nearly everything that exists. Wi-Fi is undoubtedly present in everything and everywhere these days. By 2030, there will be more than 17 billion residential WLAN devices in the world [2]. Due to the volume of private and sensitive data that can be accessed via this network, Wi-Fi security has become essential. Wi-Fi networks provide more than 75% of the data sent over the Internet to mobile phones [3], making them an attractive target for numerous security risks. The endeavor to secure the Wi-Fi network is growing due to security risks like hacking, data theft, and other forms of attacks [4].The majority of individuals are unaware of the dangers they run when their local networks are compromised or linked to an unidentified network. It is vital to research consumer WLAN security practices and increase knowledge of the possible consequences connected with user misconduct in order to encourage the use of the most recent WLAN standards and security protocols [5]. As a result, there is now a demand for ethical hacking, or network security testing, as well as for giving consumers and companies security advice. Many businesses, including Microsoft, Google, and banks, support ethical hacking in order to fix network vulnerabilities and provide the hacker with a substantial financial incentive. Furthermore, there are plenty of network specialists available to assess corporate networks for vulnerabilities and offer best practices and suggestions to strengthen network security

[6].Penetration testing delivers benefits such as minimizing financial loss, compliance with industry regulations, customers and shareholders, maintaining corporate images, and proactively reducing detected hazards before they arise [7].This research aims to conduct a penetration test using Kali Linux to test MITM attacks that require the attacker and victim to be on the same network to demonstrate the risks of hacking a Wi-Fi network and at the same time clarify the risks of connecting to open networks in public places that are more vulnerable to this type of attack and work to identify vulnerabilities and potential risks associated with Address Resolution Protocol (ARP) spoofing and Domain Name System (DNS) spoofing and test the effectiveness of social engineering methods to obtain personal data and use the Metasploit framework to hack a computer running Windows 10, by creating a malicious program consisting of an attack payload that aims to create a backdoor that enables the hacker to explore the target device and execute code. The target device is tested for threat analysis after the code is successfully executed. And its behavior and the risks it poses are analyzed.

2. Related Works

In 2020, Füsun Yavuzer Aslan and Bora Aslan used the websploit tool in Kali Linux to find a way to simply carry out a Man-in-the-Middle (MITM) assault. The Wireshark application was used to evaluate the attack moment. Cybersecurity privacy policies are being broken by these assaults, which allow for the collection of all user data on the network and the listening in on communication between two connections. Then, different strategies to prevent ARP Spoofing or to ensure safety were discussed [8].

To assist researchers and new students in deploying and utilizing the Metasploit framework as a teaching tool, Mujahid Tabassum, Tripti Sharma, et al. talked about ethical hacking, penetration testing, and practical experiments in 2021. They gave an example of how an attack using the Reverse Transmission-Control-Protocol Shell (TCP) may be carried out on a Windows 7 laptop. Using Kali Linux tools, ethical hacking and penetration testing were finished. These techniques secure networks by finding common flaws and turning on the necessary defenses. Lastly, security improvements and mitigating actions were suggested to fend off hacker attempts [6].

Abhishek Arote and Umakant Mandawkar discussed some of the fundamentals of penetration testing in 2021. They also assessed the tools and exploits that were already available and used the Metasploit framework to test the penetration of an Android mobile phone through a Reverse Transmission-Control-Protocol Shell attack and the use of framework and tool exploits. The significance of penetration testing is also covered because it is an all-inclusive technique for locating weaknesses in a system and has several advantages, including preventing financial loss and proactively removing threats to which the system might be vulnerable [9].

Regarding social engineering attacks, Ammar Naser, Mahmoud Jazzar, and others [10] proposed in 2021 to analyze phishing attacks as a form of social engineering, simulating a process occurring between two devices on two different networks. Their study focused on how victims are tricked into entering personal information via a fake email that leads to a fake website, and emphasized the importance of user awareness as a primary line of defense [10].

In 2023, Rafael Santiago Solivan submitted a master's thesis aimed at investigating the capabilities of Bettercap in scanning network vulnerabilities and simulating DNS spoofing and phishing attacks. His project featured a controlled virtual lab environment, focused on the ease of identifying and manipulating devices within the network, and emphasized the importance of preventative measures and increased awareness of cyber threats [11].

While previous studies have explored single attacks or attacks that require user spoofing via direct links, our research highlights the powerful effectiveness and impact of combining basic network attacks (ARP/DNS spoofing) with social engineering and malware injection, achieving intrusion without requiring direct user interaction with external links or files. This highlights a new level of threat in open wireless network environments and underscores the need for proactive security awareness and preventative defenses.

3. Theoretical Background

This research will present three types of attacks that wireless networks are exposed to, as follows:

3.1 Man In the Middle Attacks

A very risky wireless network assault known as a Man-in-the-Middle (MITM) attack occurs when a third party, disguising themselves, intercepts and listens in on data transmissions, leading hosts to believe they are speaking with one other directly. Further attacks may also be sparked by it [12]. An attacker can deceive victims into thinking their device is a genuine endpoint by using a spoofing-based MITM attack. By using spoofing, the attacker can influence the transmitted data and intercept genuine communications between hosts, keeping the hosts uninformed of the middleman's presence. Numerous network protocols, including Internet Protocol (IP), Address Resolution Protocol (ARP), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and domain names, are susceptible to spoofing by an attacker [13,14].

The ARP protocol is stateless, conducts no authentication, and does not check the accuracy of address matches (IP-MAC). By employing an ARP spoofing attack, sometimes referred to as ARP cache poisoning, attackers take advantage of this vulnerability and transmit a fake ARP message to the local network [15]. as illustrated in Fig.1.

Traffic between the user and the access point can be intercepted and a DNS spoofing attack can be carried out by executing an ARP spoofing attack. The attacker can read DNS communications and construct a response message with the same query identifier and IP address of a fake name server, or he can modify the IP address of the name server in the DNS response message to the address of the false name server. As seen in Fig.2, the attacker can spoof the IP address in both situations and route the targeted device to a bogus website. Serious repercussions from DNS spoofing include the dissemination of malware, communication interception, and social engineering assaults that pilfer private information [16,17].

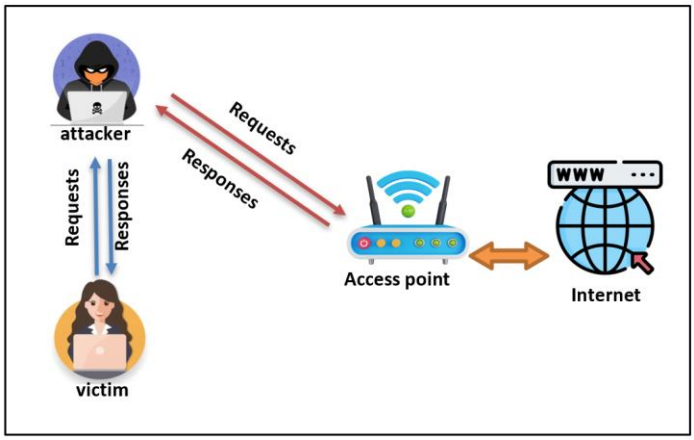

Fig. 1. ARP Spoofing Attack [18]

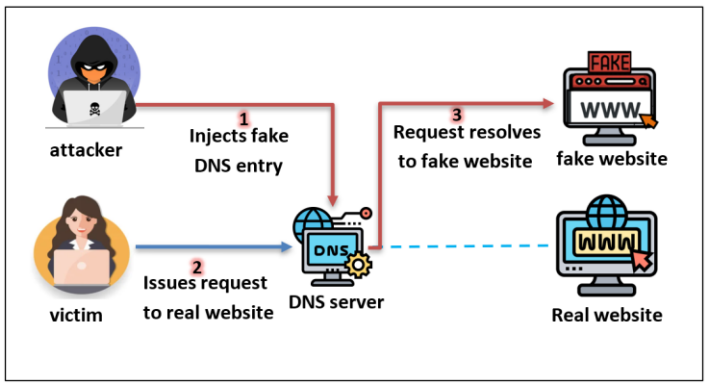

Fig. 2. DNS Spoofing Attack [19]

3.2 Social Engineering Attacks

Social engineering has posed a serious security threat to Internet users as well as infrastructure, data and cyberspace operations [20]. Social engineering remains the greatest threat to all companies, even with the most sophisticated security measures in place, including robust firewalls, encryption techniques, intrusion prevention systems, and intrusion detection systems [21]. This is because an attacker cannot directly target a system that does not possess technological weaknesses; instead, he leverages the human element to carry out malevolent activities. The most potent security assaults nowadays are thought to be social engineering ones [22]. The attacker manipulates users' minds to make them disobey security procedures. A significant degree of expertise is required for the social engineer (the attacker) to execute a successful social engineering attack, including the capacity to influence the victim with the help of the right technology. It is impractical to rely solely on technological solutions to thwart such attacks since social engineers can still manipulate human users in an attempt to get private data or grant unwanted access [23]. Hackers employ a range of strategies to trick consumers into falling for social engineering scams. Cybercriminals, for instance, launch widespread phishing attempts to deceive people into opening infected attachments or links, allowing the thieves to either steal confidential information or lock down victims' devices and demand a ransom to unlock them [21]. Fake websites, often known as fake software, are another method of social engineering assault that deceives victims into thinking they are reliable and well-known websites or software. When a victim provides a phony website with their actual login credentials, the attacker gains access to the victim's credentials and can use them to access legitimate websites, including online financial accounts. One of these dangers is the Tabnabbing attack, which consists of a spoof website that mimics the login page of a well-known website that the victim frequently accesses, such Facebook, Twitter, or online banking. While concentrating on something else, victims input their login credentials. The malevolent assailant takes advantage of the victims' faith in these websites to acquire their login credentials [20,24].

3.3 Malware Attacks

An attacker can use malware to take control of, compromise, or destroy a single computer or network of computers. When an infected file is viewed, malware that has lain dormant for some time will start to act and inflict harm. Depending on what kind of malware it is, clicking on it can cause it to spread to other files and apps on the device. Trojans, viruses, and adware are examples of malware [25]. Malware that operates on a target system similarly to a Trojan horse is known as a payload [26]. Below are some of the types of payloads:

3.3.1 Backdoor

A backdoor is a computer method that allows one to get around authentication in a piece of software or network system covertly. To enable an administrator to access the system and carry out routine upkeep or software debugging, this gateway was built. Because the system administrator developed the backdoor, it is challenging for a particular user to find or understand. The backdoor, however, is referred to as a secret gateway since hackers can utilize it to enter the system illegally. A backdoor has various definitions and purposes, one of which is an entry point in a remote management application that certain devices usually employ for routine software system maintenance and upkeep [27].

3.3.2 Reverse Transmission-Control-Protocol Shell

One useful tool for remotely breaking into computers and networks fast is the Reverse TCP Shell. Its use of the victim's device to initiate a connection request to the attacker [28]. is what gives it its efficiency and resilience, as illustrated in Fig.3. One kind of backdoor that the attacker opens on the victim's machine remotely is called a reverse TCP shell. It allows the attacker to remotely run commands on the compromised device and carry them out without the victim's awareness. Since outgoing traffic comes from the host—the vulnerability that creates the backdoor connection—the firewall only looks at incoming traffic and ignores outgoing traffic. For the attack to be carried out, the victim has to establish the connection to the payload (Reverse TCP Shell). After the victim runs the payload, the attacker can use a webcam to capture images, access files, watch the screen, sniff packets, and take screenshots [26].

3.3.3 Bind Shell

The Bind Shell module operates by opening a port on the victim's workstation and then abusing the system by the attacker during the connection initiation to the open port, the connection request from the attacker to the victim. There are multiple methods to use the link shell, including using it with different payloads and ports and protocols [29].

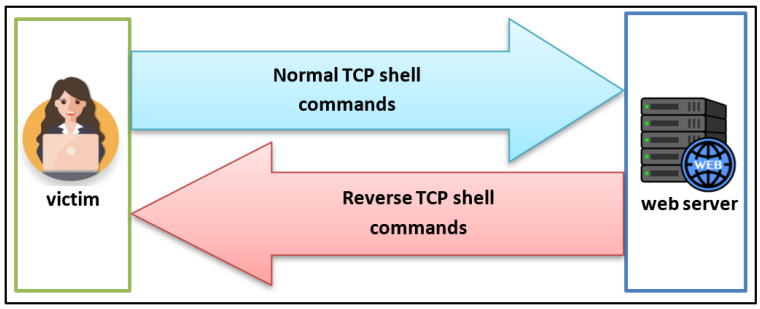

Fig. 3. The difference between regular communication and reverse communication [26]

4. Methodology

The possibility of obtaining the victim's personal information and injecting malware will be tested by the attacker connecting to the victim's wireless network. A wireless laboratory is established in this research to conduct penetration testing (ethical hacking) experiments in a safe and controlled environment.

4.1 Hardware Requirements

1. A mobile phone (realme, V3.0) was used as an access point.
2. A laptop (Razer, DESKTOP-MJS8ORR, RAM=16GB) with both the attacker's system and the victim's system installed as virtual machines.
3. A Wi-Fi adapter that supports Monitor mode and packet injection. An external Wi-Fi adapter (ALFA, AWUS036NH, USB Adapter) was used.

4.2 Software Requirements

1. VMware is a software that allows creating virtual machines inside a real computer. It was used to install the Kali Linux 2023.2 operating system that plays the role of the attacker, and the Windows 10 operating system that plays the role of the victim.

2. Install the following tools on the Kali Linux system: Bettercap, Metasploit Framework, Msfvenom, Toolkit, Apache2.

4.3 Suggested Penetration Testing Model

To increase the chances of success of cyber-attacks, it is very important to follow a specific penetration plan. Advance planning helps to accurately identify vulnerabilities, develop an effective attack strategy, reduce the risk of detection of the attack, and focus on the main objectives of the attack and avoid deviation from them. Fig.4. shows the diagram of the proposed penetration testing model.

The proposed model includes how to hack the communication channels between the victim and the access point and passively eavesdrop on the data and make changes to it. Fig.5 represents the network structure before and after the ARP spoofing attack. Once the communication channels between the victim and the access point are controlled and the ARP spoofing test is successful, the attacker moves on to the DNS spoofing test. By executing a DNS spoofing attack, the victim is redirected to fake web pages that have been prepared in advance to display a fake version of a login page for a known website (phishing attack), or display a fake advertisement that prompts the victim to download a malicious payload (malware injection) that leads to a reverse connection to the attacker's device.

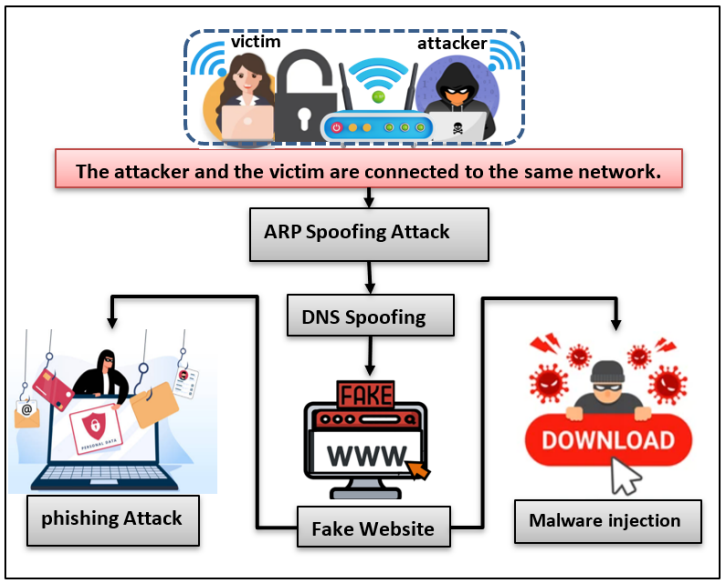

Fig. 4. Suggested Penetration Testing Model

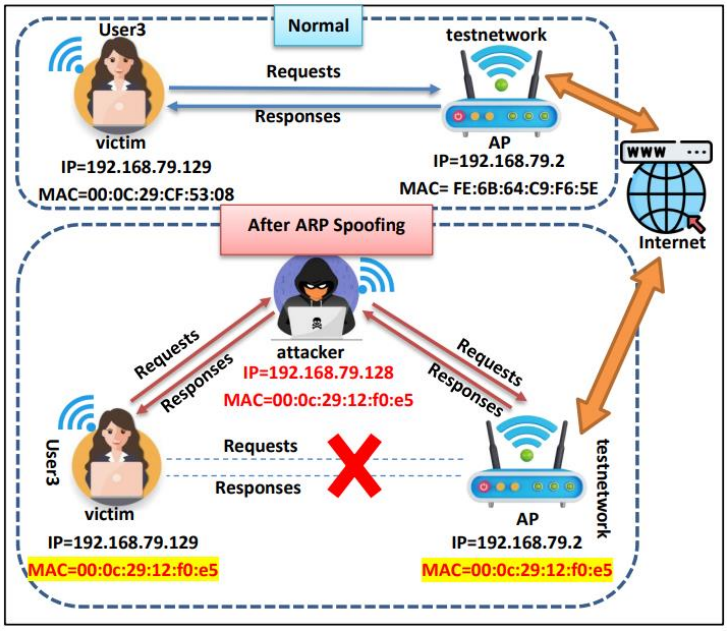

Fig. 5. Home network architecture before and after ARP spoofing attack

5. Practical Steps and Results

In Kali Linux, root privileges must be obtained in order to obtain all administrative privileges, such as modifying and deleting system files, installing and running tools, giving software commands, and having full control over the system and executing attacks.

It is also necessary to check whether there is an effective wireless connection and to find and stop processes that may cause problems when hacking, so that the tools work smoothly, and to create a secure operating environment before running the hacking tools. One of the main elements that must be stopped is the Network Manager. Stopping it makes the process of detecting the attacker's wireless connection impossible, and thus the attacker can bypass some security applications, as shown in Fig.6 Using the "airmon-ng" tool to stop the network manager.

The wireless adapter (Wi-Fi Adapter) is connected to the attacker's device via (USB) ports. Using the "iwconfig" tool, the interface name of the connected wireless adapter is displayed, which is (wlan0), as shown in Fig.6. Using the "airmon-ng" tool, the wireless connection is enabled in monitor mode, as shown in Fig.7. When monitoring mode is enabled, an attacker can capture all data packets within the range of the wireless adapter. The goal here is to capture data packets and traffic for the target network.

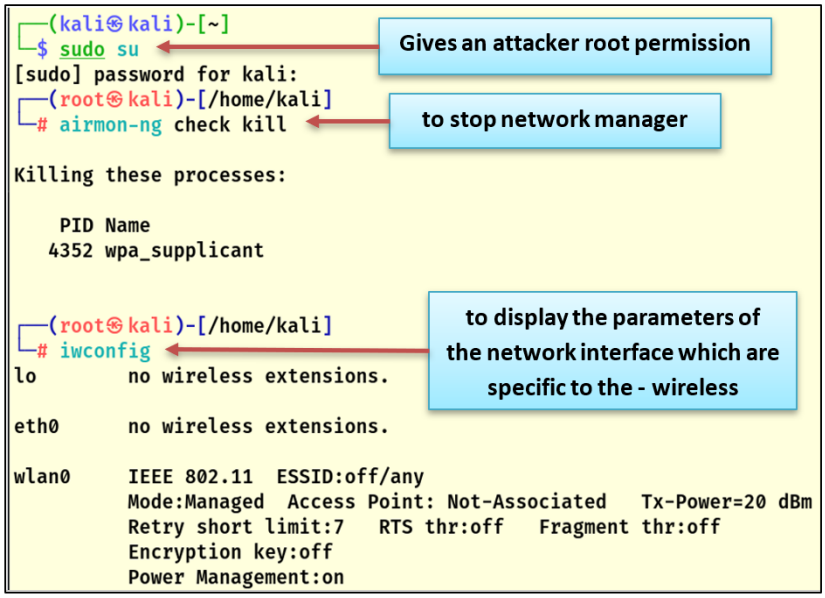

Fig. 6. Stop Network Manager and remaining interfering processes and identify the network interface.

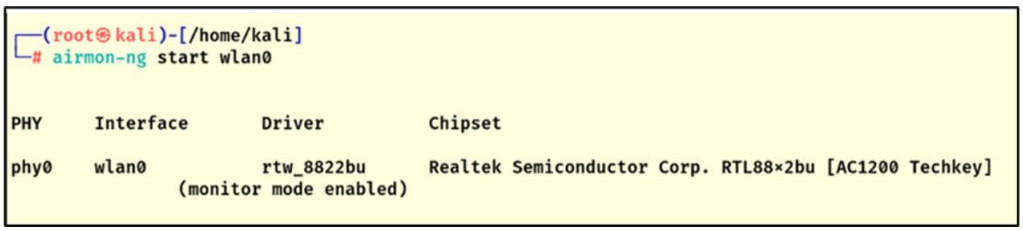

Fig. 7. Enable monitoring mode

Bettercap is a multi-module tool that can be used for many activities. By delivering network data and users, the events.stream module—which is utilized by default—is in charge of relaying what is occurring within the network. The net.recon module is used to read the ARP cache table on a regular basis. Net.sniff module is specialized in sniffing and jamming network packets, whereas the net.probe module is used to find both new and current clients in the network by sending various test packets to everyone connected to the network so that the net.recon module can detect them. These modules allow for the identification of network vulnerabilities, the selection of the victim, and the viewing of the websites he visits. As illustrated in Fig.8, the victim and the access point are attacked simultaneously by turning on the arp.spoof.fullduplex module, which determines the victim's IP address. Next, the ARP spoofing attack is initiated by turning on the arp.spooof module.

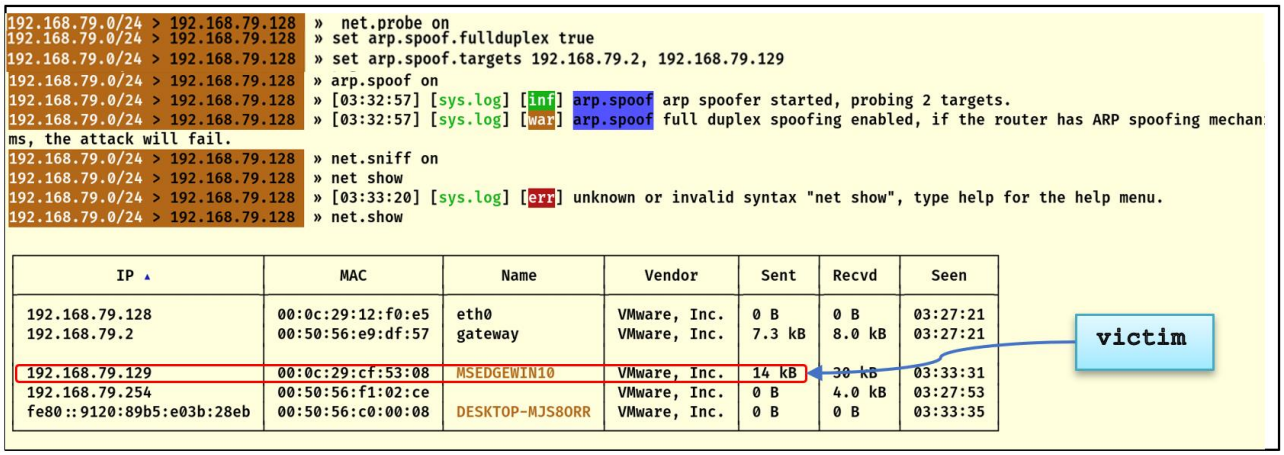

Fig. 8. ARP spoofing attack has started.

Now, if the victim's computer's ARP cache table is reexamined, as illustrated in Fig.9, the victim will think that the access point's MAC address and the attacker's MAC address are the same, while the access point will think that the victim and the attacker have the same MAC address.

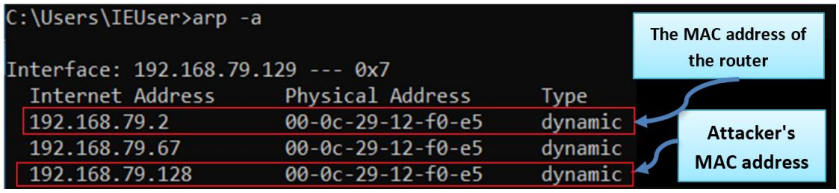

Fig. 9. ARP cache table on the victim machine after an ARP spoofing attack

The web pages that the victim browses can be manipulated by redirecting URL requests to a real or fake web page specified by the attacker using ARP spoofing and DNS spoofing attacks. To make the DNS spoofing attack more advanced and dangerous, it has been combined with the most common social engineering attack known as phishing attack, where a fake copy of the Google account login page is created on the local browser (localhost) of the attacker's device. The cloning process is done using the "Toolkit" tool. To increase the chance of deceiving the victim, all DNS requests will be redirected to the local server by activating the "dns.spoof.domains all" module in the "Bettercap" tool as shown in Fig.10, i.e. the fake login page will appear as a restricted gateway to force the victim to enter his email and password. For example, when searching for Amazon on the victim's device, the DNS request will be directed to the attacker's device address, as shown in the Fig.11, which will display a fake version of the Google account login page. Once the victim enters the login information, it is easily captured by the "Bettercap" tool, as shown in Fig.12.

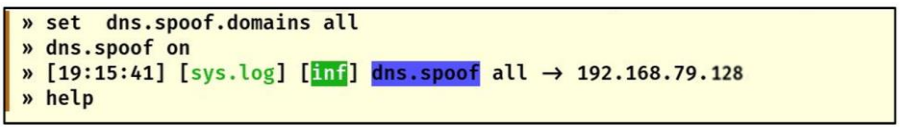

Fig. 10. DNS spoofing attack started

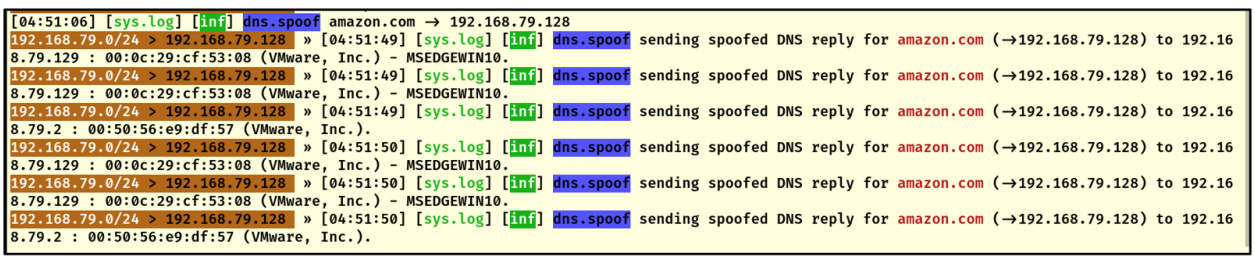

Fig. 11. Respond to DNS requests to the local server

It is also possible to inject malware using ARP spoofing, DNS spoofing, and the local server "Apache2". By creating a payload: The payload is a malicious executable file, using the "msfvenom" tool, different malicious payloads can be created. As shown in Fig.13, where (-p windows/meterpreter/reverse_tcp) specifies the type of payload, which is a reverse connection payload that allows the attacker to remotely control the victim's machine, (x86) i.e. the payload runs on a (32bit) architecture, (LHOST=192.168.79.144) is the (IP) address of the attacker's machine that will receive the reverse connection, and (LPORT=7777) is an unused gateway number on the attacker's machine that the reverse connection request is received on. (-f exe) specifies that the resulting file runs on Windows. The type of the victim device, whether Windows or Android, can be determined through the (net.recon) module in the "bettercap" tool, as shown in Fig.8. This is considered one of the disadvantages of not changing the default name of the device, so the attacker can determine the type of payload needed. Finally, the payload file is saved with the name (application.exe) in the path (/var/www/html).

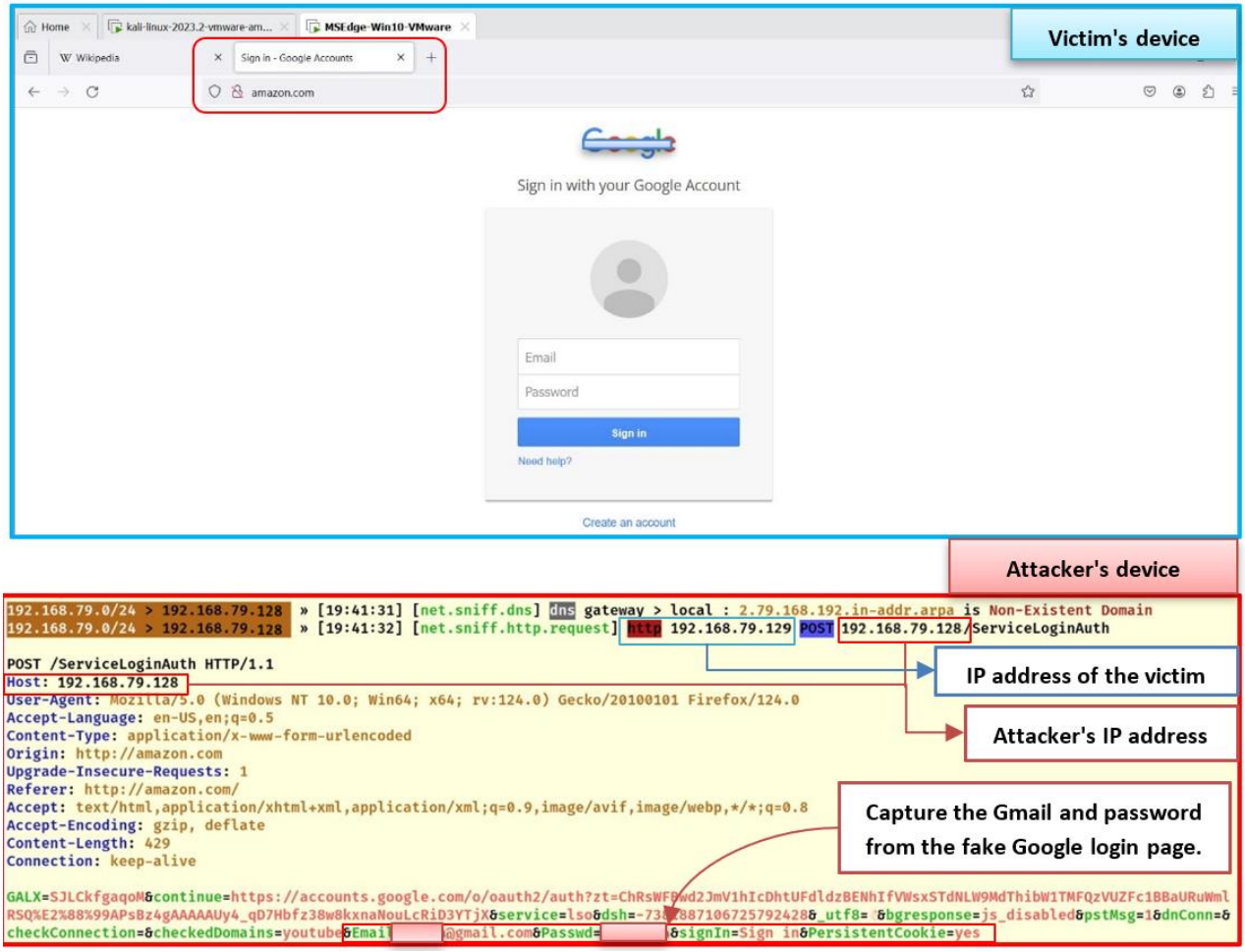

Fig. 12. Show fake login page and capture gmail and password

Fig. 13. Create an executable payload file

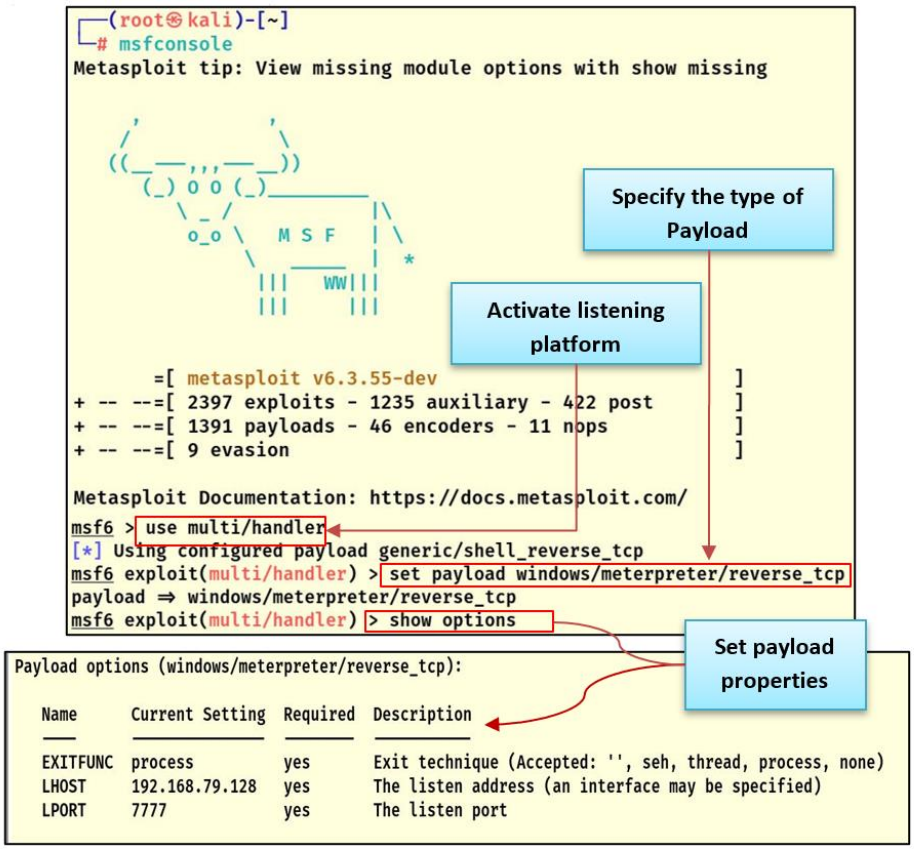

Fig. 14. Setting up the listening platform

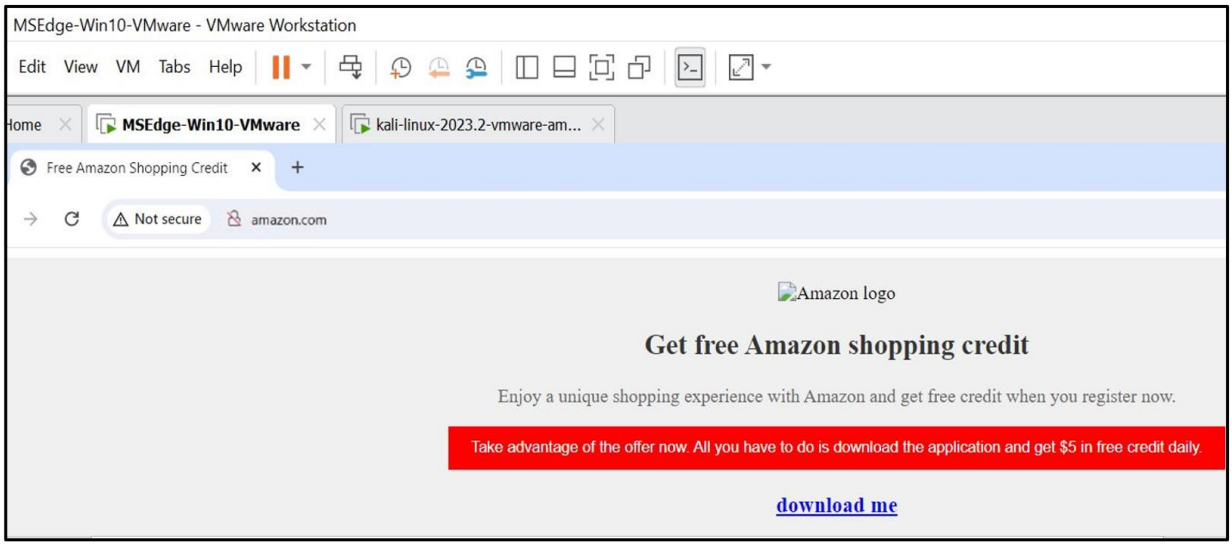

Fig. 15. The fake advertisement that appears on the victim's screen

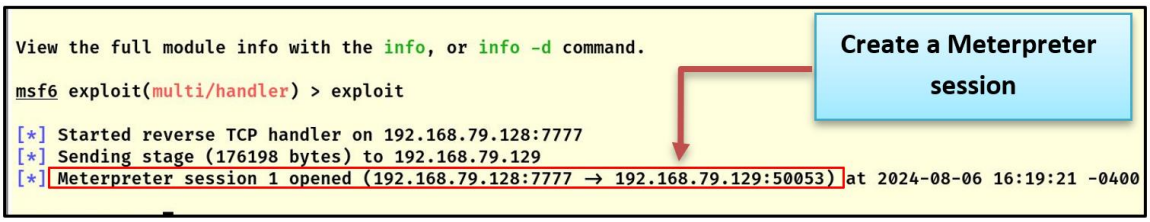

Fig. 16. Payload execution by victim and communication and exploitation session initiated

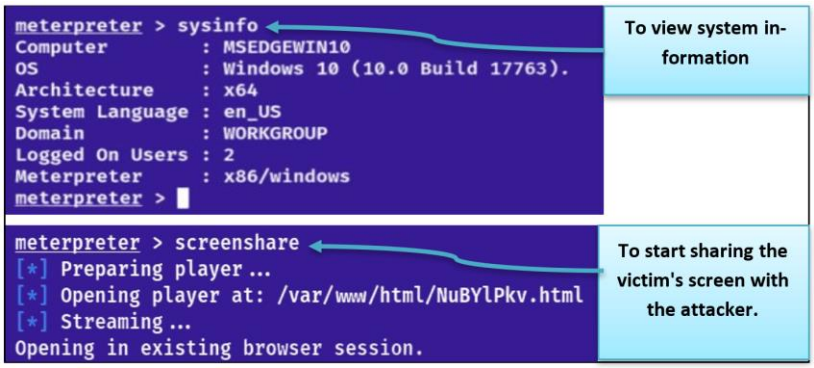

Fig. 17. Exploitation session (Meterpreter)

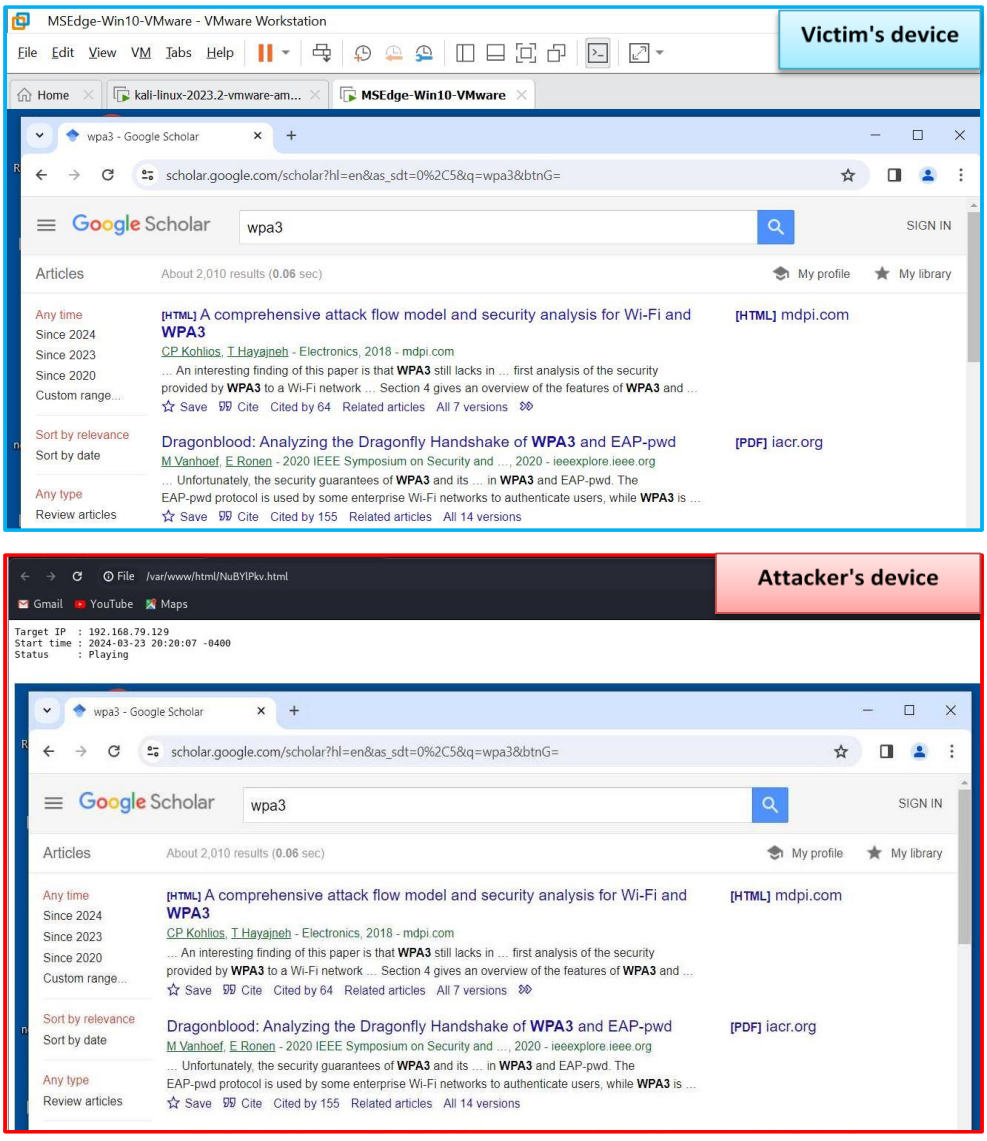

Fig. 18. Start sharing the victim's screen with the attacker

A listening platform is configured for the victim device using the Metasploit tool, then the handler is activated to receive the reverse shell connection from the victim device and determine the properties of the received payload as shown in Fig.14.

The payload is sent to the target device in different ways, such as email by attaching the malicious file to a convincing email message, or it can be encrypted by merging and encrypting it with another file such as an application, image, pdf file, link or video in a Trojan style to be more convincing and to prevent it from being easily detected by the victim and antivirus programs. In this experiment, the payload is uploaded as is (without encryption) to a fraudulent

website that asks the victim to download and run it, where we will reprogram the local server "Apache2" in HTML, to display an advertisement trying to trick the victim into downloading an application to get free credit as shown in Fig.15, and by spoofing (DNS), we redirect (URL) requests to the local browser. The application will be a (Reverse TCP Shell Payload) payload. This payload opens a shell (or command prompt) to control the target through the (TCP) port. Once the connection is established (the fake application is loaded on the victim's device and the Handler receives the reverse connection request from the victim's device) as shown in Fig.16, the attacker will be able to initiate an exploitation session to control the target system using the interactive interface (Meterpreter), enabling the attacker to execute commands on the operating system such as, transferring files, logging keystrokes, and performing many other tasks.

Through the exploitation session, it is possible to display basic information about the victim's system, and also the screenshare command to share the victim's system screen with the attacker is one of the commands available within the Meterpreter session, as shown in Fig.17, where the victim's screen is broadcast live on the attacker's web browser, as in Fig.18.

6. Countermeasures

Based on the result of the Wi-Fi penetration test, the study suggests the following practices:

- Raise user security awareness:

1. Beware of untrusted public networks: Avoid connecting to public Wi-Fi networks that request personal information such as name, phone number, or email address, as hackers can exploit these as entry points for their attacks.
2. Raise awareness of phishing risks: Users should be educated about recognizing the signs of online fraud and the risks of clicking on unknown links or downloading files from untrusted sources, even if they appear legitimate.
3. Avoid sensitive activities on public networks: It is strongly recommended not to conduct banking transactions, log in to sensitive accounts, or exchange confidential information when connected to public Wi-Fi networks.
4. Check website security (HTTPS): Before entering any credentials, ensure the page is encrypted and uses the HTTPS protocol, not HTTP, and that it is not a fake version.
5. Enable two-factor authentication: To add an additional layer of security, users should enable two-factor authentication, especially on accounts containing sensitive personal information.

- Technical Measures to Protect Networks and Systems:

1. Using Virtual Private Networks (VPNs): Routing traffic through a Virtual Private Network (VPN) is an effective way to reduce the risk of MITM attacks. Using a VPN encrypts traffic within the tunnel, making it difficult for an attacker to inspect or manipulate it.
2. Monitoring ARP Activity: It is recommended to use specialized software or hardware to monitor ARP activity on the network and trigger alerts when detecting any unusual patterns that may indicate an ARP spoofing attack.
3. Configuring Static DHCP Tables (for specific environments): In traditional static networks with a limited number of devices, specific MAC addresses can be assigned to static IP addresses and locked in the router. This method prevents attackers from changing these addresses, but it is not practical in dynamic networks with a large number of users.
4. Continuously Update Security Software: Antivirus software and intrusion detection and prevention systems must be updated regularly to ensure they are able to detect and respond to the latest threats and malware.

7. Conclusions and Discussion

By conducting a series of penetration tests in a secure and controlled environment, this study has demonstrated the feasibility and effectiveness of combined attacks that combine ARP spoofing and DNS spoofing with phishing and malware injection techniques. The main contribution of our research is to demonstrate how vulnerabilities in open wireless networks can be successfully exploited to redirect traffic to phishing pages or to deliver malicious payloads (Reverse TCP Shell) to victim devices indirectly, without requiring user interaction via external links. The results achieved highlight the severity and ease of implementing these combined attacks, highlighting critical vulnerabilities in cybersecurity. ARP spoofing enables an attacker to intercept and modify data, and DNS spoofing facilitates seamless redirection of victims to malicious websites, exploiting users' trust and lack of awareness of the hidden risks in open wireless networks. The experiment also demonstrated the success of using network attacks to deliver malware (Reverse TCP Payload) and gain complete control over the targeted device. Countermeasures have been proposed to counter these threats.

References

[1] C. Ndubuisi, F. Soomro, D. Javeed, U. Mohammedbadamasi, C. O. Ndubuisi, and M. Asif, "Man in the Middle Attacks: Analysis, Motivation and Prevention," *Int. J. Comput. Networks Commun. Secur.*, vol. 8, no. 7, pp. 52–58, 2020, doi: 10.13140/RG.2.2.22752.81928.

[2] S. Lindroos, A. Hakkala, and S. Virtanen, "A systematic methodology for continuous WLAN abundance and security analysis," *Comput. Networks*, vol. 197, no. July, p. 108359, 2021, doi: 10.1016/j.comnet.2021.108359.

[3] D. Gao *et al.*, "A nationwide census on wifi security threats: prevalence, riskiness, and the economics," in *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*, 2021, pp. 242–255.

[4] M. A. Adiguna and B. W. Widagdo, "Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus: Router Tp-Link Mercusys Mw302r)," *J. SISKOM-KB (Sistem Komput. dan Kecerdasan Buatan)*, vol. 5, no. 2, pp. 1–8, 2022.

[5] S. Lindroos, A. Hakkala, and S. Virtanen, "A systematic methodology for continuous WLAN abundance and security analysis," *Comput. Networks*, vol. 197, p. 108359, 2021.

[6] M. Tabassum, T. Sharma, and S. Mohanan, "Ethical Hacking and Penetrate Testing using Kali and Metasploit Framework Ethical Hacking and Penetrate Testing using Kali and Metasploit Framework Mujahid Tabassum Saju Mohanan Department of IT , University of Technology and Department of IT , University," no. July, 2021.

[7] N. K. Zuin and V. Selvarajah, "A Case Study : SYN Flood Attack Launched Through Metasploit," vol. 4, no. Iciic, pp. 520–525, 2021.

[8] F. Y. Aslan, "Man-in-the-Middle Attack with WebSploit Tool," vol. 7, no. 8, pp. 12541–12544, 2020.

[9] A. Arote and U. Mandawkar, "Android Hacking in Kali Linux Using Metasploit Framework," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 3307, pp. 497–504, 2021, doi: 10.32628/cseit2173111.

[10] A. Naser, M. Jazzar, D. Eleyan, and A. Eleyan, "Social Engineering Attacks: A Phishing Case Simulation," *Res. Gate*, vol. 10, no. 3, pp. 2277–8616, 2021.

[11] R. Santiago Solivan, "Network Security Assessment using Bettercap: DNS Spoofing and How to Mitigate," *Comput. Sci.*, 2023.

[12] B. Pingle, A. Mairaj, and A. Y. Javaid, "Real-World Man-in-the-Middle (MITM) Attack Implementation Using Open Source Tools for Instructional Use," *IEEE Int. Conf. Electro Inf. Technol.*, vol. 2018-May, pp. 192–197, 2018, doi: 10.1109/EIT.2018.8500082.

[13] S. M. Morsy and D. Nashat, "D-ARP: An Efficient Scheme to Detect and Prevent ARP Spoofing," *IEEE Access*, vol. 10, no. November, pp. 49142–49153, 2022, doi: 10.1109/ACCESS.2022.3172329.

[14] M. Conti, N. Dragoni, and V. Lesyk, "A Survey of Man in the Middle Attacks," Jul. 01, 2016, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/COMST.2016.2548426.

[15] Z. Trabelsi and W. El-Hajj, "ARP spoofing: A comparative study for education purposes," *Proc. 2009 Inf. Secur. Curric. Dev. Annu. Conf. InfoSecCD'09*, no. September 2009, pp. 60–66, 2009, doi: 10.1145/1940976.1940989.

[16] M. A. Hussain, H. Jin, Z. A. Hussien, Z. A. Abduljabbar, S. H. Abbdal, and A. Ibrahim, "DNS Protection against Spoofing and Poisoning Attacks," *Proc. - 2016 3rd Int. Conf. Inf. Sci. Control Eng. ICISCE 2016*, pp. 1308–1312, 2016, doi: 10.1109/ICISCE.2016.279.

[17] A. Sabitha Banu and G. Padmavathi, "Hybrid Detection and Mitigation of DNS Protocol MITM attack based on Firefly algorithm with Elliptical Curve Cryptography," *EAI Endorsed Trans. Pervasive Heal. Technol.*, vol. 8, no. 4, 2022, doi: 10.4108/eetpht.v8i4.3081.

[18] A. A. Isah, A.-B. Adamu, A. Awal, A. A. Babajo, and A. Adamu, "A REVIEW OF WIRELESS NETWORKS: WLAN SECURITY AND THREATS," 2022. [Online]. Available: https://aspjournals.org/ajset/index.php/ajset

[19] P. Cisar and R. Pinter, "Some ethical hacking possibilities in Kali Linux environment," *J. Appl. Tech. Educ. Sci. jATES*, vol. 9, no. 4, pp. 129–149, 2019, [Online]. Available: http://doi.org/10.24368/jates.v9i4.139http://jates.org

[20] Z. Wang, L. Sun, and H. Zhu, "Defining Social Engineering in Cybersecurity," *IEEE Access*, vol. 8, pp. 85094–85115, 2020, doi: 10.1109/ACCESS.2020.2992807.

[21] N. N. Pokrovskaia and S. O. Snisarenko, "Social engineering and digital technologies for the security of the social capital'development," in *2017 International Conference" Quality Management, Transport and Information Security, Information Technologies"(IT&QM&IS)*, IEEE, 2017, pp. 16–18.

[22] A. M. Aroyo, F. Rea, G. Sandini, and A. Sciutti, "Trust and social engineering in human robot interaction: Will a robot make you disclose sensitive information, conform to its recommendations or gamble?," *IEEE Robot. Autom. Lett.*, vol. 3, no. 4, pp. 3701–3708, 2018.

[23] A. Yasin, R. Fatima, L. Liu, A. Yasin, and J. Wang, "Contemplating social engineering studies and attack scenarios: A review study," *Secur. Priv.*, vol. 2, no. 4, p. e73, 2019.

[24] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," *Futur. Internet*, vol. 11, no. 4, 2019, doi: 10.3390/FI11040089.

[25] G. P. Bhatraju, U. Shanmugam, and B. Indira, "Malware Analysis for Proactive Defence on Cyber Threat Vulnerabilities," in *2023 Innovations in Power and Advanced Computing Technologies (i-PACT)*, IEEE, 2023, pp. 1–7.

[26] Y. Kolli, T. K. Mohd, and A. Y. Javaid, "Remote Desktop Backdoor Implementation with Reverse TCP Payload using Open Source Tools for Instructional Use," *2018 IEEE 9th Annu. Inf. Technol. Electron. Mob. Commun. Conf. IEMCON 2018*, no. November, pp. 444–450, 2018, doi: 10.1109/IEMCON.2018.8614801.

[27] A. Hamadi and E. Lisova, "Investigating vulnerabilities in a home network with Kali Linux," no. February, 2019, [Online]. Available: http://urn.kb.se/resolve?urn=urn:nbn:se:mdh:diva-42612

[28] A. Manglani, T. Desai, P. Shah, and V. Ukani, "Optimized Reverse TCP Shell Using One-Time Persistent Connection," in *Innovations in Information and Communication Technologies (IICT-2020) Proceedings of International Conference on ICRIHE-2020, Delhi, India: IICT-2020*, Springer, 2021, pp. 351–358.

[29] E. Nyberg and L. Dinis Ferreira, "Antivirus performance in detecting Metasploit payloads: A Case Study on Anti-Virus Effectiveness," 2023.

Authors' Profiles

Asmaa Akram Ghanim completed the B.S. in electrical engineering/ electronic and communication from the University of Mosul, Iraq, in 2020 and received the M.Sc. degree in electronic and communication in 2025. She is interested in the field of computer networks and communication and cybersecurity.

Mohammed Younis Thanoun completed the B.S. in electrical engineering/ electronic and communication from the University of Mosul, Iraq, in 1991 and received the M.Sc. degree in electronic and communication in 2000 and Ph.D. in 2011 from Mosul University. He is interested in the field of computer networks and communication and he has published research papers in Deep Learning, SDN, machine learning algorithms and cybersecurity engineering He has been working as an assistant professor at the University of Mosul since 2021. He is a member of the computer networks lab in the Electrical Dept. / Engineering College.

How to cite this paper: Asmaa A. Ghanim, Mohammed Y. Thanoun, "Wi-Fi Attacks by Exploiting ARP and DNS Vulnerabilities: A Security Study", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.15, No.5, pp. 34-46, 2025. DOI:10.5815/ijwmt.2025.05.03