NTU Journal of Engineering and Technology (2025) 4 (2) : 47-53
DOI: https://doi.org/10.56286/ntujet.v4i2

IRAQI Academic Scientific Journals

P-ISSN: 2788-9971 E-ISSN: 2788-998X
NTU Journal of Engineering and Technology
Available online at: https://journals.ntu.edu.iq/index.php/NTU-JET/index

Wireless Networks Security Flaws and Hacking Avenues of Attacks

Asmaa Akram Ghanim[1], Mohammed Younis Thanoun[1]
[1]University of Mosul, Collage of Engineering, Electrical Engineering Department
asmaa.22enp38@student.uomosul.edu.iq , myounisth@uomosul.edu.iq

Article Informations

Received: 22-03- 2024,
Revised: 06-07- 2024
Accepted: 12-07-2024,
Published online: 23-06-2025

Corresponding author:
Name: Mohammed Younis Thanoun
Affiliation : University of Mosul, Collage of Engineering, Electrical Engineering Department
Email: myounisth@uomosul.edu.iq

Key Words:
MITM,
ARP Spoofing,
SSL Stripping,
DNS Spoofing,
DoS,
Bettercap.

A B S T R A C T

An access point offers wireless networking to several wireless client nodes in the shared medium when using IEEE 802.11 wireless local area networks in infrastructure mode. The related nodes could be at risk of security attacks. In the field of cybersecurity, it is not sufficient to identify vulnerable points; rather, the difficulty lies in learning how hackers can take advantage of weak points to take countermeasures. This research paper simulates some of the risks caused by an attacker when connecting to an AP, as well as the risks of connecting to open Internet networks in public places, the importance of not using them to transfer personal data, and the need to raise awareness of the importance of protecting wireless networks. The Bettercap tool from the Kali Lunix operating system was used to simulate Address Resolution Protoco (ARP) spoofing attack, Secure Sockets Layer (SSL) Stripping attack, Domain Name System (DNS) spoofing attack, and Denial of Service (DoS) attack, which are based on Man in the Middle (MITM) attacks.

1. Introduction

In the modern world, the Internet has risen to the top of our priority list. Both the Internet and cellphone networks are essential to most of our everyday activities. The dominant platform is social media. Additionally, the convenience of online shopping and banking is growing daily, and it is impossible to achieve without the internet. Because they were required to have access to the Internet, hackers could more easily target them. Hackers mostly aim to steal sensitive information from various organizations, perhaps leading to financial loss [1].

One of the most extensively used wireless technologies in public spaces is Wi-Fi, which offers high-speed networking services for little or no cost. Because wireless clients in IEEE 802.11 infrastructure mode must associate with an access point (AP) in order to communicate wirelessly, Wi-Fi becomes a breeding ground for various cyberattacks, the most prevalent of which is the MITM [2]. Because the attacker and the clients share the same wireless media, it is simple to cause an interruption in service, take frames from the victim nodes, and fabricate frames for spoofing [3]. In the event that customers connect to an IEEE 802.11 wireless network, interact with an AP, and utilize an Internet application, an attacker may try to carry out more sophisticated attacks to infect the clients or access point with malicious material while they are online [4].

There is a lot of research on the risks of MITM attacks based on spoofing. In [5] 2020, the ease of carrying out an ARP spoofing attack using the websploit tool and the wireshark software in Kali Linux was explained, showing the possibility of capturing all user data through this attack, and methods were identified to protect against this attack. In [6] 2021, the implementation of one of the most famous MITM attacks based on ARP spoofing was described. A Raspberry Pi single-board computer was used to carry out the attack, and the research showed the possibility of using the Raspberry Pi to carry out cyber-attacks of this type. In [7] 2021, it was examined if the DNS Security Extensions (DNSSEC) can strengthen DNS security against DNS spoofing and mitigating DNS vulnerabilities. In [8] 2023, a detailed study was presented on DNS spoofing, its risks, resulting threats, countermeasures, and the importance of using DNSSEC. In [9] 2023, the ease of carrying out a DNS spoofing attack and the serious threats resulting from this attack were demonstrated using the Bettercap tool to model DNS spoofing. It also highlighted the importance of enhancing DNSSEC.
This paper uses Kali Lunix's Bettercap tool, an effective social engineering tool, to simulate ARP spoofing attack, SSL Stripping attack, DNS spoofing attack, and DoS attack on a wireless network, showing the risks of vulnerabilities in wireless networks and the damage caused by hackers while connecting to an access point with Suggest countermeasures to avoid this type of attacks.

2. The Theoretical Bases

The MITM attack is considered one of the most dangerous attacks against a wireless network, where a hidden third party controls and eavesdrops on the data transfer between two or more parties and convinces the two hosts that they are communicating with each other directly. An attacker can modify, intercept, change, or replace the target victim's communication traffic in an MITM attack. it can be used to invoke attacks such as a DoS attack, spoofing-based attacks, port hijacking, and session hijacking [10,11].

A spoofing-based MITM attack is a technique used by MITM attackers to trick victims into believing they are legitimate endpoints. The attacker uses spoofing to intercept legitimate communications between two hosts and control the transmitted data, keeping the hosts unaware of the presence of the intermediary. An attacker can spoof several network protocols based on the MITM, such as the Internet Protocol (IP), ARP, DNS, Dynamic Host configuration Protocol (DHCP), and domain name [12,13].

1-ARP Spoofing attack: the ARP converts network layer addresses (IP addresses) into link layer addresses (Media Access Control addresses). The ARP protocol is a request-and-reply mechanism that operates only within the bounds of a single physical network [6]. When a device wants to send data to another device on the same local network, it looks up the Media Access Control (MAC) address of the destination device in the ARP table. If it does not exist, it sends an ARP request containing the IP address of the destination device to all devices on the network. When the requested device receives an ARP request containing its IP address, it sends an ARP response message containing its MAC address [14]. ARP is a stateless protocol, ARP does not perform any authentication, nor does it verify the accuracy of the IP-MAC address match. An attacker exploits this vulnerability and sends a forged ARP message to the local network using ARP spoofing, also known as ARP cache poisoning [15]. Any attacker connected to the wireless local-area network (WLAN) has the ability to send a fake ARP reply message to the victim with their MAC address associated with the target host's IP address. If the router is the target host and the attacker additionally

sends, the attacker will receive all traffic going from the victim to the target [16].

2-DNS Spoofing: the DNS is one of the basic protocols within the Transmission Control Protocol/Internet Protocol (TCP/IP) suite. It is used to connect the server and the client device by translating the names of websites into IP addresses in digital notation [17]. DNS allows people to browse the web more easily by avoiding the need to save IP addresses Because of the way the system works, it transmits data in plain text, security attacks can be easily launched against it [18]. Attack using DNS spoofing an attacker must know how to use an ARP spoofing attack to intercept traffic between the client and the gateway router. At this point, an attacker can read DNS messages and produce a response message with the same query identifier and a fake name server IP address, or they can change the nameserver's IP address in the DNS response message. The IP address is spoofed in both cases so that the attacker gains an advantage [19]. There are several variations of DNS spoofing, such as Remote DNS Spoofing, in which the attacker is not on the victim's network, and Local DNS Spoofing, in which the attacker and victim are on the same local network [20]. DNS spoofing can have serious repercussions, such as the dissemination of malware, the interception of communications, and phishing campaigns that steal confidential data [21].

3-DoS-based ARP Spoofing attacks are prevalent and simple to execute inside a network segment. DoS and packet sniffing and manipulation can be accomplished with DoS-based ARP assaults [22]. A host typically loses Internet access as a result of DoS assaults. One can accomplish this by either using ARP cache poisoning or ARP cache overflow. In the former case, the gateway router's physical address is modified to an invalid address, resulting in the loss of all messages. In the latter case, false data overloads the ARP cache, triggering the system to shut down the network link [23]. It is crucial to note that a DoS attack will occur if the malicious host modifies the ARP caches of the two target hosts without turning on IP packet routing. In this case, the two hosts will be unable to exchange packets, the malicious host in this instance does not transfer the received packets to their intended destination. When we take into account that routers and gateways can also be poisoned, this becomes even more potent. By launching a MITM attack on the host and the WLAN router, it is possible to intercept all of the host's Internet traffic [5].

4-SSL Stripping Attack: SSL protocols are among those created for providing security (secure transactions/secure transfers) for any network communication. This protocol is usually used together with other protocols, such as Hypertext transfer protocol secure (HTTPS), to offer a secure implementation of the service and finally create secure channels over unreliable networks [24].

An attacker can view and control packets when they execute a MITM attack or ARP spoofing attack using packet sniffing, which gives them access to all client-to-gateway traffic. The data will be transmitted in plaintext if web traffic is transmitted and received via the Hypertext Transfer Protocol (HTTP), making it vulnerable to capture, reading, and change by an attacker. But, even if the attacker manages to grab the packet, they won't be able to read the message if the victim accesses HTTPS web pages, which combine the HTTP and SSL protocols. This is because the text is encrypted using to the SSL protocol. However, using a method known as SSL stripping, an attacker can stop the user from accessing HTTPS pages and only allow them to view the HTTP version of the website [11].

The webserver receives an HTTPS request from the client and uses the Internet to send back the requested web page through an encrypted SSL tunnel. However, if an attacker is proxying all of this traffic, he or she can change the request to point to an HTTP page rather than an HTTPS page. There is no additional layer of encryption between the client and the webserver in the protocol being used, but the web page remains unchanged. The client attempts to authenticate with the webserver using its credentials after receiving the HTTP page; however, the attacker intercepts the plaintext credentials. Using these credentials, the attacker will start a fresh HTTPS session with the HTTPS server. The server will then consider this connection to be valid and approve it. The HTTP session between the attacker and the victim is the first to form, and the session between the attacker and the webserver is the second. This will result in information theft and unencrypted credentials being disclosed [25,10].

3. The Proposed Methodology

The research methodology includes the following steps as show in (Fig.1), network sniffing, identifying vulnerabilities, ARP spoofing attack, network eavesdropping, password capture, SSL Stripping, DNS spoofing attack, redirection of URL requests, and DoS attack.

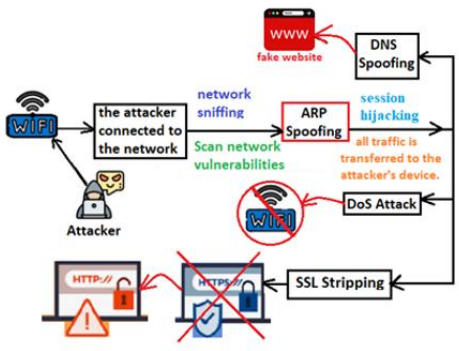

Fig. 1. the steps of the work.

In order to implement MITM attacks, a fully functional virtual laboratory is necessary. The

hardware and software elements that are used to establish a controlled environment for experimentation are described in this section. which make it possible to use the Bettercap tool and guarantee a safe environment for examining network defences and vulnerabilities.

Computer workstation A powerful computer that can support virtualization and network simulation. It should also have enough RAM, storage, and processing capacity. We also need a router that can replicate a network environment so that MITM spoofing simulations and network vulnerability assessments can be carried out. When taking the examinations at home, you can also use your local network if you have permission to do so. home local network was used for this test. For network monitoring and communications, an additional external source is also required. In this study, we utilize the UGREEN USB Wi-Fi Adapter (AC1300 and 5dBi).

VMware is multi-platform virtualization software; was used in this research to install Kali Linux 2023, which plays the role of the attacker, and Windows 10 as the victim.

Kali Linux 2023.2, is an operating system built for hacking and penetrating systems. Building your own hacking tool to compromise or attack systems is time consuming and quite arduous and tedious. Now a days, existing tools like Kali Linux facilitate this task [26].

Bettercap v2.32.0 (built for Linux amd64 with go.21.0), is a cybersecurity tool of choice for many security researchers, red teams, and reverse engineers. It can be used for Wi-Fi hacking and reconnaissance tasks [27]. The programming language Go is used to create Bettercap. it is also well-known for its ability to execute many kinds of man-in-the-middle (MITM) attacks on a network, change HTTP, HTTPS, and TCP traffic in real time, sniff credentials, and much more [9,28]

Apache2 Web Server, Through the web service, was delivered over the Internet by the Apache HTTP Server, a free and open-source web server. It is currently the most widely used HTTP client and completely supports all operating systems, including Windows, Linux, UNIX, and others [29].

4. Results And Discussions

Since the attacker aims to penetrate the network and establish an independent connection with the victims without their knowledge, the MITM attack is considered one of the most common and deadly active attacks. To initiate the attack, both the attacker's machine (the Kali operating system) and the victim's machine (the Windows 10 operating system) are needed. First, the ARP cache table at the victim's device is shown in (Fig.2).

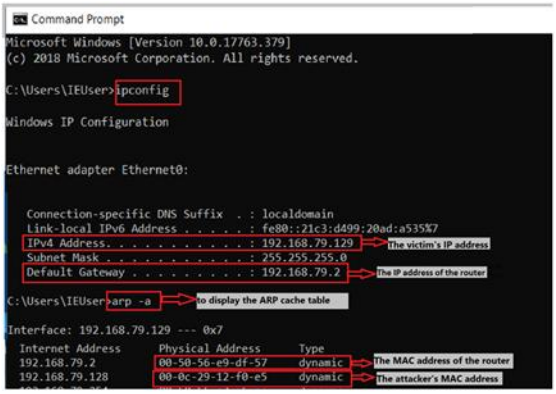

Fig. 2. ARP cache table on victim devise Before a ARP spoofing attack.

The Bettercap tool contains many modules available to perform different tasks. The (events.stream) module runs by default and is responsible for transmitting what happens within the network by transferring records and clients in the network.

In order to read the ARP cache table periodically, the (net.recon) module is used. While the (net.probe) module is used to discover existing and newly added clients in the network, which sends various test packets to all those connected to the network so that the (net.recon) module can discover them, as shown in (Fig.3), the (net.probe) module uses the (net.sniff) module, which specializes in sniffing and jamming network packets We can see all the packets that pass through the network and the websites that customers browse, as shown in (Fig.4). Through these modules, it is possible to identify weak points in the network, choose the victim, and sniff the websites that he visits.

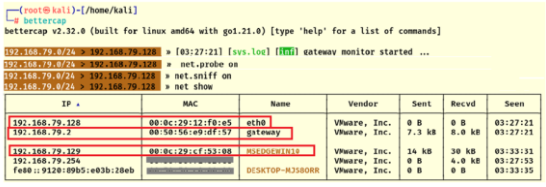

Fig. 3. view the IP addresses and MAC addresses of every connected client.

Fig. 4. network sniffing packets.

ARP spoofing allows the attacker to act as a man in the middle. The victim and the gateway are attacked at the same time by activating

(arp.spoof.fullduplex), then the target is selected, and then the ARP spoofing attack begins, as show in (Fig.5).

Fig. 5. Start ARP spoofing attack.

Now if the ARP table is displayed on the victim's device, it will be as shown in (Fig.6), which means that the victim believes that the router's MAC address is the same as the attacker's MAC address, and at the same time, the router believes that the victim's MAC address is the same as the attacker's MAC address.

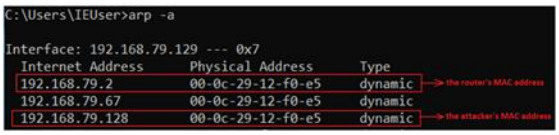

Fig. 6. ARP cache table on victim devise after a ARP spoofing attack.

When the victim browses any site, all traffic is transferred to the attacker's device. When the victim browses the HTTP website, the information packets are transmitted without encryption, and an attacker can easily capture all the credentials, Gmail, and passwords that are written which show in (Fig.7).

Fig. 7. traffic between the victim and the getaway.

This strategy is used for HTTP websites, not HTTPS. An SSL stripping attack and an ARP spoofing attack are performed in order to make this strategy work on websites that use the HTTPS protocol. Bettercap and hstshijack caplets are used in this attack, as shown in (Fig.8). The victim's SSL certificate will be removed by SSL strip, but the requests will be sent to the server over HTTPS, as show in (Fig.9).

Fig. 8. start SSL Stripping Attack.

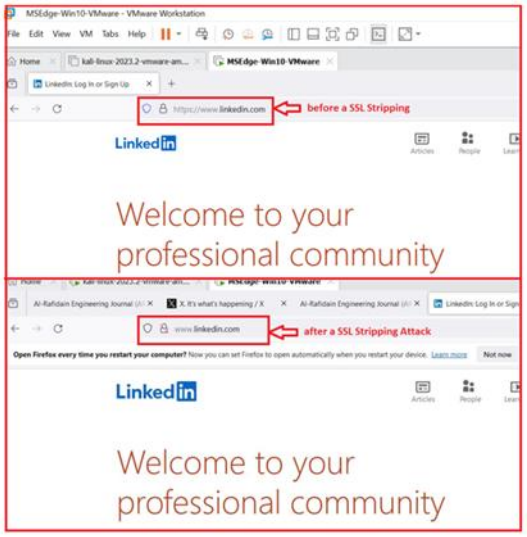

Fig. 9. SSLstrip detects HTTPS URLs and replaces them with HTTP links on victim devise after a SSL Stripping Attack.

By using ARP spoofing and DNS spoofing to redirect uniform resource locator requests Uniform Resource Locator (URL) to a web page we have prepared in this work, the URL request will be redirected to the local web browser of Kali Linux, "Apache2." The network sniffing module (net.sniff) helps in knowing what websites the victim is browsing and determining the web address that will be redirected.for the example if the victim request the Amazon website. The domain and local web can be specified through the command "dns.spoof.domains", and then the attack “dns.spoof on" will start as shown in (Fig.10) When the victim requests the Amazon website, the request is redirected to the server that the attacker prepared, as shown in (Fig.11) The Bettercap tool, through the "dns.spoof.all" module, provides the ability to respond to all DNS requests for the victim's device instead of a specific domain (Amazon).

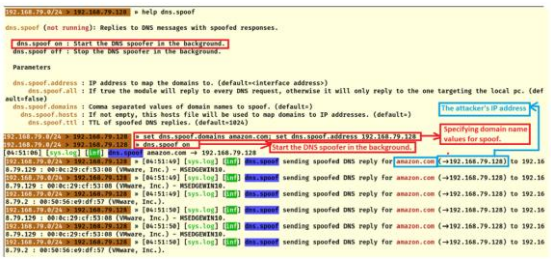

Fig. 10. start a DNS Spoofing attack.

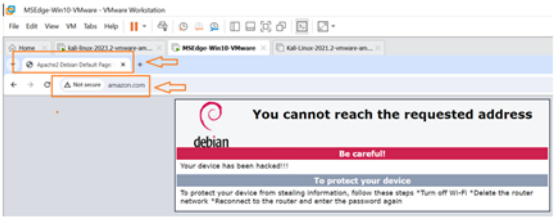

Fig. 11. Redirect the URL request to the local web browser for "Apache2". on the victim's device.

In this research, the local server was transformed to display the message “Your device has been hacked.” usually, attackers transform the local server into a login page for Google, Gmail, Facebook, etc., so that they can steal personal data without the victim’s knowledge.

The "arp.ban on" command is used to perform DoS-based ARP spoofing attacks, as show in (Fig.12) This attack is done by poisoning the ARP cache without allowing the IP packet to be forwarded. This will prevent the exchange of packages between the victim and the smuggler. In this case, the attacker destroys incoming packets instead of forwarding them to the approved interface, causing Internet service to stop.

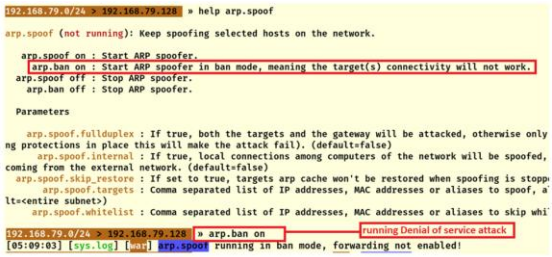

Fig. 12. Start a DoS attack.

5. Countermeasures

1-Man-in-the-middle attacks can only be carried out when the attacker is connected to the access point, so the first step to avoiding these attacks is to protect Wi-Fi networks from being hacked by using the latest encryption standard Wi-Fi Protected Access 3 (WPA3), choosing a strong password, and hiding the Wi-Fi network.

2. The user must never connect to unreliable or insecure networks. He or she should never connect to the internet if they are unsure of a reliable source.

3. It is necessary to use a Virtual Private Network (VPN) that hides the IP address when connecting to open Internet networks in public places that are considered the most vulnerable to MITM attacks.

4. The user ought to avoid entering his login information on any public network. He should never enter sensitive data over open or public networks; he should only trust his own network. With the use of an MITM attack, data on unsecure networks can be easily located. The user must constantly search for the https certificate, even if he does not need to enter sensitive data. The attacker can easily remove it with an SSL strip.

5. Use Domain Name System Security Extensions (DNSSEC) to avoid DNS spoofing. Use ARP-spoofing detection programmers and activate the firewall.

6. Conclusion

Security is becoming more and more important. Everyone who uses the Internet should be aware of potential threats and take certain precautions to stay safe. Data security and privacy are in dire need now. If a user ignores security precautions when using the Internet, sensitive information such as a username and password can be easily intercepted. We've seen Bettercap make it easy to sniff user credentials, hijack sessions, sniff packets, redirect URL requests to fake websites, and do denial of service. This research explains the vulnerabilities found in local area network protocols and how attackers exploit them by implementing MITM attacks such as ARP spoofing, SSL spoofing, DNS spoofing, and DoS. Through this research, it was clarified how important it is to carry out attacks within a secure virtual environment to determine the danger of exploiting vulnerabilities by attackers and the necessity of addressing network weaknesses, as well as proposing some countermeasures, to enable the user to stop data theft. The importance of awareness of the dangers of network penetration by hackers and the danger of using open Wi-Fi networks in public places, which are considered easy prey for hackers.

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. Netw. Commun. Secur., vol. 8, no. 7, pp. 52–58, 2020, doi: 10.13140/RG.2.2.22752.81928.

[2] W. Kim, S. Kim, and H. Lim, “Malicious Data Frame Injection Attack without Seizing Association in IEEE 802.11 Wireless LANs,” IEEE Access, vol. 9, pp. 16649–16660, 2021, doi: 10.1109/ACCESS.2021.3054130.

[3] Y. Jeong, H. Kim, and H. J. Jo, “ASD: ARP spoofing detector using openwrt,” Secur. Commun. Netw., vol. 2022, 2022.

[4] P. Satam and S. Hariri, “WIDS: An anomaly based intrusion detection system for Wi-Fi (IEEE 802.11) protocol,” IEEE Trans. Netw. Serv. Manag., vol. 18, no. 1, pp. 1077–1091, 2020.

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

[6] A. Idiyatullin and P. E. Abdulkin, “A Research of MITM Attacks in Wi-Fi Networks Using Single-

board Computer," in Proc. 2021 IEEE Conf. Russian Young Res. Electr. Electron. Eng. (ElConRus), pp. 396–400, 2021, doi: 10.1109/ElConRus51938.2021.9396241.

[7] R. Houser et al., "A comprehensive measurement-based investigation of DNS hijacking," in Proc. 40th Int. Symp. Reliable Distrib. Syst. (SRDS), pp. 210–221, 2021.

[8] D. Yang et al., "A deep dive into DNS behavior and query failures," Comput. Netw., vol. 214, p. 109131, 2022.

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

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

[11] A. R. Chordiya, S. Majumder, and A. Y. Javaid, "Man-in-the-Middle (MITM) Attack Based Hijacking of HTTP Traffic Using Open Source Tools," in Proc. IEEE Int. Conf. Electro Inf. Technol., pp. 438–443, 2018, doi: 10.1109/EIT.2018.8500144.

[12] S. M. Morsy and D. Nashat, "D-ARP: An Efficient Scheme to Detect and Prevent ARP Spoofing," IEEE Access, vol. 10, pp. 49142–49153, 2022, doi: 10.1109/ACCESS.2022.3172329.

[13] M. Conti, N. Dragoni, and V. Lesyk, "A Survey of Man in the Middle Attacks," IEEE Commun. Surv. Tutor., vol. 18, no. 3, pp. 2027–2051, 2016, doi: 10.1109/COMST.2016.2548426.

[14] B. Scott et al., "An interactive visualization tool for teaching ARP spoofing attack," in Proc. IEEE Front. Educ. Conf. (FIE), pp. 1–5, 2017.

[15] A. Brown, Assessing and Developing Two Educational Tools on ARP Spoofing Attacks, Ph.D. dissertation, North Carolina Agricultural and Technical State University, 2018.

[16] A. Kawshan, "Create ARP Spoofing Attack Using Scapy," May 2022, doi: 10.13140/RG.2.2.19490.09923.

[17] I. Voronov and K. Gnezdilov, "Determining OS and Applications by DNS Traffic Analysis," in Proc. 2021 IEEE Conf. Russian Young Res. Electr. Electron. Eng. (ElConRus), pp. 72–76, 2021, doi: 10.1109/ElConRus51938.2021.9396085.

[18] F. Hock and P. Kortiš, "Design, implementation and monitoring of the firewall system for a DNS server protection," in Proc. ICETA 2016 - 14th IEEE Int. Conf. Emerg. ELearn. Technol. Appl., pp. 91–96, 2016, doi: 10.1109/ICETA.2016.7802040.

[19] M. A. Hussain et al., "DNS Protection against Spoofing and Poisoning Attacks," in Proc. 3rd Int. Conf. Inf. Sci. Control Eng. (ICISCE), pp. 1308–1312, 2016, doi: 10.1109/ICISCE.2016.279.

[20] Q. Li, X. Qi, J. Liu, and H. Han, "Design and implementation of traditional DNS protocol," in Proc. Int. Conf. Comput. Technol., Electron. Commun. (ICCTEC), pp. 1384–1390, 2017, doi: 10.1109/ICCTEC.2017.00303.

[21] 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 Health Technol., vol. 8, no. 4, 2022, doi: 10.4108/eetpht.v8i4.3081.

[22] Z. Trabelsi and W. El-Hajj, "On investigating ARP spoofing security solutions," Int. J. Internet Protocol Technol., vol. 5, no. 1–2, pp. 92–100, 2010, doi: 10.1504/IJIPT.2010.032618.

[23] J. Belenguer and C. T. Calafate, "A low-cost embedded IDS to monitor and prevent Man-in-the-Middle attacks on wired LAN environments," in Proc. Int. Conf. Emerg. Secur. Inf., Syst., Technol. (SECURWARE), pp. 122–127, 2007, doi: 10.1109/SECUREWARE.2007.4385321.

[24] Z. Li, G. Xiong, and L. Guo, "Unveiling SSL/TLS MITM Hosts in the Wild," in Proc. 2020 IEEE 3rd Int. Conf. Inf. Syst. Comput. Aided Educ. (ICISCAE), pp. 141–145, 2020, doi: 10.1109/ICISCAE51034.2020.9236866.

[25] C. P. Kohlios and T. Hayajneh, "A comprehensive attack flow model and security analysis for Wi-Fi and WPA3," Electronics, vol. 7, no. 11, p. 284, 2018.

[26] T. Ariyadi and M. R. Pohan, "Implementation of Penetration Testing Tools to Test Wi-Fi Security Levels at the Directorate of Innovation and Business Incubators," J. Penelit. Pendidik. IPA, vol. 9, no. 12, pp. 10768–10775, 2023, doi: 10.29303/jppipa.v9i12.5551.

[27] S. Shakya, R. Bestak, R. Palanisamy, and K. A. Kamel, Mobile Computing and Sustainable Informatics. [Online]. Available: http://www.springer.com/series/15362

[28] A. Yeboah-Ofori and A. Hawsh, "Effects of Cyberattacks on Virtual Reality and Augmented Reality Technologies for People with Disabilities," in Proc. 2023 IEEE Int. Smart Cities Conf. (ISC2), 2023, doi: 10.1109/ISC257844.2023.10293659.

[29] 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.