The IJICS (International Journal of Informatics and Computer Science)
Vol 5 No 1, March 2021, Page 7-15
ISSN 2548-8384 (online), ISSN 2548-8449 (print)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/ijics/index
DOI 10.30865/ijics.v5i1.2764

Simulation and Analysis of Network Security Performance Using Attack Vector Method for Public Wifi Communication

Andy Susanto, Wahyu Kusuma Raharja

Departement Electrical Engineering Master Program, Gunadarma University, Depok, Indonesia
Email: [1,*]andys37@gmail.com, [2]wahyukr@staff.gunadarma.ac.id
Coressponding Author: andys37@gmail.com
Submitted: **09/01/2021**; Accepted: **16/02/2021**; Published: **29/03/2021**

Abstract−The use of wifi networks in public spaces has a risk of robbery of user access data in cyberspace, such as banking transactions, social media and other online access. The threat of Man In The Middle Attack (MITM) attacks is carried out on public wifi networks to gain access to user information by illegal means. The attack vector simulation process is carried out on the site access exampleriset.com/dvwa/login.php. ARP Poisoning attack with Ettercap device performs interception and manipulation which provides 08: 00: 27: 25: 22: 99 MAC address information to the target. Session Hijacking attack simulations are carried out using a cookie manager plugin on the HTTP and HTTPS protocols. SSL Stripping attacks by better intercepting and downgrading HTTPS to HTTP communication protocols. Poisoning ARP attacks get information from targets such as Mobile IP MAC Address 192.168.3.249 F4: 09: D8: EA: EC: E7 and Server 192.168.3.5 08: 00; 27: CC: 59: OE and user: admin Passed: password. The results of the Session Hijacking attack on the HTTP protocol get a session id in the form of phpsessiid = 4f1pnfr081e4jero11truspb60 \ r \ n which is used the specified session id time without entering user authentication. The Session Hijacking attack on the HTTPS protocol was unsuccessful and the SSL Striping attack on the HTTPS protocol was unsuccessful.

Keywords: Man in The Middle Attack; Arp Posioning; Attack Vector; Session Hijacking; Wifi

1. INTRODUCTION

By continuing to develop rapidly in the digital era, information technology is always developing and increasingly advanced. As today, everything is made easier and more economical with the "Internet". Wireless networking has become the main goal for many attackers, because it is very easy to enter any wireless network during public wireless network connectivity [1]

Based on the 2018 APJII survey report, the growth of internet users from 2017 to 2018 has almost reached 28 million, this is a very large growth compared to previous years. Field data were taken from March 9 to April 14 2019 [2]. According to the 2018 statistical analysis report, there will be around 75 billion devices by 2025 connected to the internet with various connectivity media. Statistics show the number of connected devices worldwide from 2015 to 2025. Currently several social networks such as Facebook and Twitter are becoming the largest and most important sources of information, data exchange, and online services based on their fast growth [3]. Wireless technology has become popular in its use in everyday life both for business, study, and even digital social interaction [4]. In line with its development in fulfilling high mobility and flexible services, a technology that is capable of providing these needs is present, namely Wireless Fidelity (WiFi) technology [5] .

Public areas such as recreation areas, airports, hotels and coffee shops now provide free internet connection services as an added advantage of their use [6] and the many threats associated with the Man in the Middle Attack cyber attack [7]. So it is necessary to pay attention to the connection between the wifi network and the server from the threat of hackers. Because of these problems, an important need now is to help minimize and anticipate users when accessing public wifi networks from hacking crimes. One of the things that can be done is to simulate the Man in The Middle Attack technique on a public wifi network identified in its function and analyze the sniffer through a WLAN (Wireless Local Area Network) traffic study. The simulation results obtained are recommendations for public space managers and users in utilizing public wifi networks.

The literature review process for this research relates to the theories from previous related research journals.

Table 1. Related Work

No	Title	Method	Spesificatiom	Result
1	A Prototype of IoT based remote Controllerf car for pentesting wireless Networks	Concept, method of attack, and Security defense strategy	Raspbery PI, AirCrack, Access Point	Finds vulnerabilities that an attacker could exploit.
2	Potential Threat Analysis Hypertext Transfer Protocol and Secure Hypertext Transfer Protocol of Public WiFi Users (Batam Case)	Attack Method and process Forensic	Wireshark, Ettercap, Acces Point	Intercept and analyze http and https packets to produce comprehensive data on user behavior in accessing Public Wifi in Batam
3	Wi-Fi Security Level Analysis for Minimizing Cybercrime	Attack Method	Wireshark, Ettercap, Acces Point	Obtaining data on the percentage of successful

No	Title	Method	Spesificatiom	Result
				attacks on public WiFi networks
4	Static Forensics Investigation Analysis Man In The Middle Attack Based on ARP Poisoning	Forensic Process	Wireshark, Access Point	Obtain data on the percentage of successful attacks on public WiFi networks in Y. Analyze and find digital evidence in the form of information, data traffic from the results of MITM attacks
5	Security and Attack Vector Analysis of IOT Devices	*Attack Vector*	Osram Lightify *Smart Bulbs*, TPLink Smart Plug, Speaker Amazon Echo Dot, Access Point	Research and review through testing security of home automation devices via Wifi network

Previous research has been shown in table 1 using research methods such as concepts, attack methods, forensic processes and attack vectors. The linkage of this method is very important in the concept process, methodology, and testing of security performance research on a public wifi network system platform. Specifically for the Attack vector, it is a cyber attack carried out on a wifi network against a connected device by obtaining information about the intended website access, user account, and credentials. Optimal public wifi network security performance is an indicator of cyberattacks.

The purpose of this paper is to design a public wifi network simulation platform using a WLAN network architecture and simulate the MITM vector attack and analyze the performance of the wifi network simulation platform based on the MITM vector attack method.

2. RESEARCH METHODOLOGY

2.1 Research Methods

The research will be conducted in four stages, namely:

1. Problem Analysis.
   Problem analysis is a temporary study to identify problems from the background and provide alternative solutions to problem solving. Identification of the problem is that the use of wifi networks in public spaces has the risk of theft of user access data when carrying out banking transactions, social media, other online access and potential attack vector threats, especially MITM attacks on wifi networks are very dangerous for theft of user access data, so that managers Wi-Fi networks in public spaces need to improve network security and the community as users is expected not to use public space wifi networks for banking transactions, social media and other private online access. In building a public wifi network system in this study, hardware is needed in the form of Access Point Wireless, a GSM 4G modem, while the software needed is a Winbox tool.
2. Literature Review Search
   The literature review process is carried out by searching for related theories from research journals, and other literature that has previously been carried out to obtain a theoretical basis, so that it can be used so that research concepts can be developed.
3. System Design
   Starting from problem identification and approaches from several existing studies. System design to support research uses several supporting tools such as hardware in the form of Access Point Wireless, GSM 4G modem, while the software required is in the form of Virtual Box, Ubuntu Server Operating System, Kali Linux Operating System, Ubuntu Desktop Operating System, Bettercap tools, Ettercap tools, Cookie Manager extension tools, Winbox tools and Wireshark tools.
4. System Testing and Discussion
   Determining measurement variables as the standard for system testing, namely carrying out the Attack Vector attack process within the scope of the MITM technique by tapping and manipulating data on user access to sites based on HTTP and HTTPS protocols.

The stages used in this study can be described the fishbone shape.

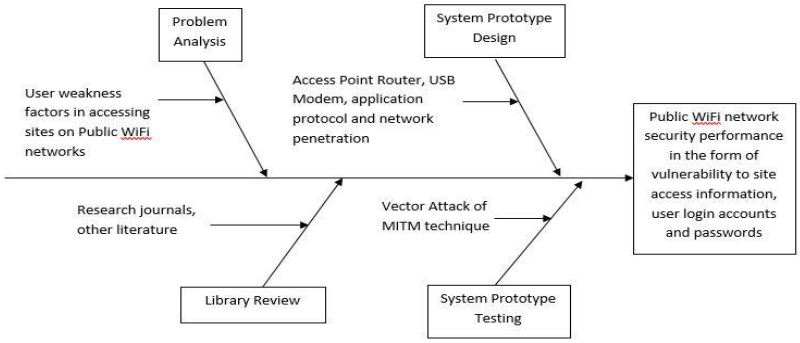


Figure 1. Flow of Research Methods with Fishbone

2.2 System Design

In the research design, supporting tools are needed to support the design of a public wifi network system consisting of hardware in the form of a Mikrotik RB951Ui-2HND Access Point Router, 4G GSM Wingle USB Modem and software in the form of Virtual Box, Ubuntu Server Operating System, Kali Linux Operating System, Ubuntu Desktop Operating System, bettercap tools, Ettercap tools, Cookie Manager extension tools and wireshark tools. The design is shown in fig 2.

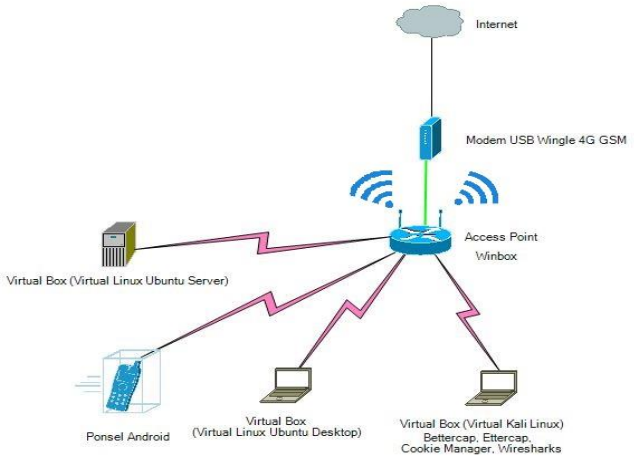


Figure 2. Topology Design of Public Wifi Network System

2.3 System Workflow

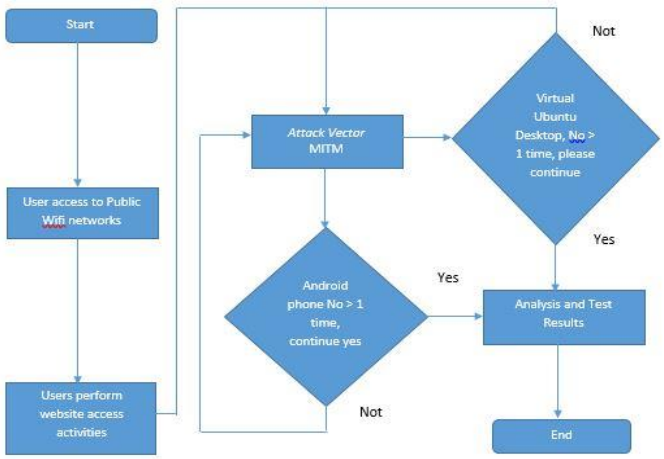


Figure 3. System Operation Process

Based on Figure 3, the system operational process can be explained as follows:

1. Users make network connections to public wifi without using user authentication and passwords.
2. The user successfully enters the public wifi network, and starts browsing the desired site.

3. The testing variable is carrying out the attack vector process method within the scope of the MITM technique in public wifi networks by intercepting, tapping and manipulating data traffic on user browsing access to the site. There are 3 types of attacks carried out, including:
   a. ARP Poisoning, connects the attacker's MAC address to the IP address to be attacked and intercepts data on the ARP protocol.
   b. Session Hijacking, retrieval of session IDs when accessing HTTP and HTTPS protocol sites.
   c. SSL Stripping, decreases communication when the HTTPS protocol site accesses to HTTP between the client and server.
4. Simulated attacks are carried out on 2 devices, namely virtual desktop computers and mobile devices connected to the wifi network and access to the site. The attack test on the device was carried out once successfully and 1 time not.
5. Researchers conduct test analysis of MITM attacks carried out on testing variables which include interception, tapping and manipulation of data traffic.
6. Researchers will get test result data in the form of access information, user accounts and passwords when browsing to sites on a wifi network.

3. RESULT AND DISCUSSION

3.1 Integration of System Prototype Design

The Integration Process of System Prototype Design is to create a network architecture using a WLAN (Wireless Local Area Network) network with a star topology. Mikrotik supports USB (Universal Serial Bus) communication, which is connected to a USB modem that is equipped with a GSM 4G LTE cellular connection. 2.4 GHz frequency setting on the proxy for wifi signal spreaders as data communication using a wireless network from a computer or cellphone, naming SSID (Service Set Identifier) with the name public wifi.

Network routing settings on Mikrotik to connect to the internet network, giving IP DHCP (Dynamic Host Configuration Protocol). Some settings on Mikrotik use the Winbox tools. Settings are also made on the modem for cellular connection access. The installation of Wireshark, Ettercap, Bettercap and cookie manager tools is carried out on the Kali Linux Operating System virtual machine as the attacker's computer. Virtual machine with Linux Ubuntu Desktop operating system and smartphone based on android. The system prototype in this study is defined as an integrated device so that it can carry out the real data retrieval process on the user's computer and smartphone in the form of the values of the parameters from the results of recording and attack on public wifi networks as shown in Figure 4.

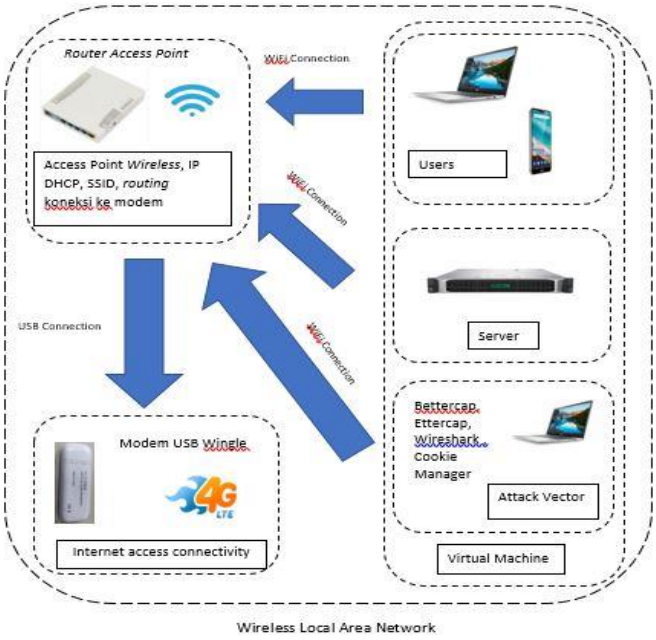


Figure 4. Integration of System Prototype Design

Implementation of the design and construction of a public wifi network system prototype with a Mikrotik RB951Ui-2HND wireless router and a 4G GSM Wingle USB modem.

	Name	Type	Actual MTU	L2 MTU	Tx	Rx
	ether1	Ethernet	1500	1598	0 bps	0 bps
	ether2	Ethernet	1500	1598	0 bps	0 bps
	ether3	Ethernet	1500	1598	0 bps	0 bps
	ether4	Ethernet	1500	1598	0 bps	0 bps
	ether5	Ethernet	1500	1598	0 bps	0 bps
R	ppp-out1	PPP C...	1500		1744 bps	0 bps
R	wlan1	Wirele...	1500	1600	71.6 kbps	7.8 kbps

Figure 5. Interface List on Mikrotik Devices

Figure 5 is a list interface on a proxy device, Ethernet port 2 is used for a network cable connection connecting a network card on a laptop to determine the IP address on the virtual web server (Ubuntu 18.04 operating system) in the Virtual Box, used for the testing machine virtual web server. Wlan1 is a wireless access to data connection with a frequency of 2.4 GHz which forms a public wifi network based on LAN topology (Local Area Network). Internet access is routed via the GSM PPout1 Modem. The data transmission path is given in the status of Tx information and data reception is in the Rx information status in bps (bits per second).

Making 3 virtual machines is done to replace the physical server device and PC. The virtual server operating system used is Ubuntu 18.04 LTS, the virtual desktop operating system uses Ubuntu 18.04.5, the operating system as the attacker is Kali Linux 2020 and the mobile device used is the Android 6.01 operating system. The web application used is DVWA (Damn Vulnerable Web Application) which is a special application for security vulnerability testing, run using the Apache web server application by running on the HTTP protocol domain access http://exampleriset.com/dvwa and the HTTPS https: // exampleriset.com/dvwa.

3.2 Simulation Testing

In this study, the initial stage is carried out the scanning process will be carried out for a few minutes. The preliminary data collection process techniques include:

a. Examination of the existence of public wifi network architecture
b. Identify devices connected to public wifi networks using the nmap application, to find out the user's IP and MAC address.
c. Identify public wifi network security vulnerabilities
d. After knowing the existence and security of the previous stages, planning an attack testing simulation is carried out.

```
Nmap scan report for 192.168.3.1
Host is up (0.0017s latency).
MAC Address: 6C:3B:6B:E8:78:1D (Routerboard.com)
Nmap scan report for 192.168.3.5
Host is up (0.0011s latency).
MAC Address: 08:00:27:CC:59:0E (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.3.249
Host is up (0.018s latency).
MAC Address: F4:09:D8:EA:EC:E7 (Samsung Electro-mechanics(thailand))
Nmap scan report for 192.168.3.252
Host is up (0.00045s latency).
MAC Address: 08:00:27:5F:B5:F6 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.3.254
Host is up (0.00016s latency).
MAC Address: D8:5D:E2:DA:D2:25 (Hon Hai Precision Ind.)
Nmap scan report for 192.168.3.253
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.03 seconds
```

Figure 6. Scanning for Devices Connected On Public Wifi Network Using NMAP

In Figure 6, the researcher scans for devices connected to a public wifi network using the NMAP tools and information shows that the host is currently active in one network segment, there are several connected devices. In this case the researcher searches for currently active hosts or targets via TCP ACK and ICMP echo request packets and identifies 6 actively connected devices.

Furthermore, this research carried out testing of MITM's attack vector technique, several test scenarios with testing variable parameters including interception, tapping and manipulation of data traffic. The types of testing the MITM attack vector technique include:

a. ARP Posioning, attacking the ARP protocol to connect the attacker's MAC address to the virtual desktop IP address and the user's mobile phone as the target object.
b. Session Hijacking, intercepts the HTTP, HTTPS protocols and retrieves session id.
c. SSL Stripping, reduce data traffic communication on the HTTPS to HTTP protocol.

Information on attack vector testing on a public wifi network system platform in the form of destination site access, user access rights and passwords.Stages of the test scenario carried out are shown in Figure 7.

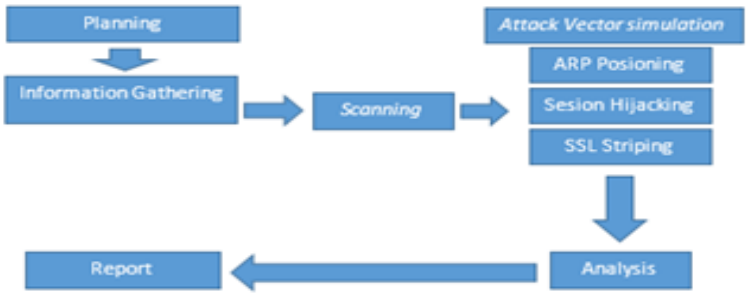


Figure 7. Flowchart Simulation Test

3.3 Analysis

At this stage, the file analysis obtained from the test is checked to determine the MITM attack on the public wifi network in accordance with the objectives of each attack vector method, from the test carried out the next stage, namely the test analysis. The MITM attack with the ARP Poisoning method connects the attacker's MAC address to the virtual IP address of the desktop computer via the ARP protocol and responds to the virtual desktop computer with a MAC address that has been manipulated and is considered to be the MAC address of the site provider server. Virtual servers and virtual desktop computers cannot distinguish between eavesdropping attacks and MAC address manipulation against the use of IP addresses.

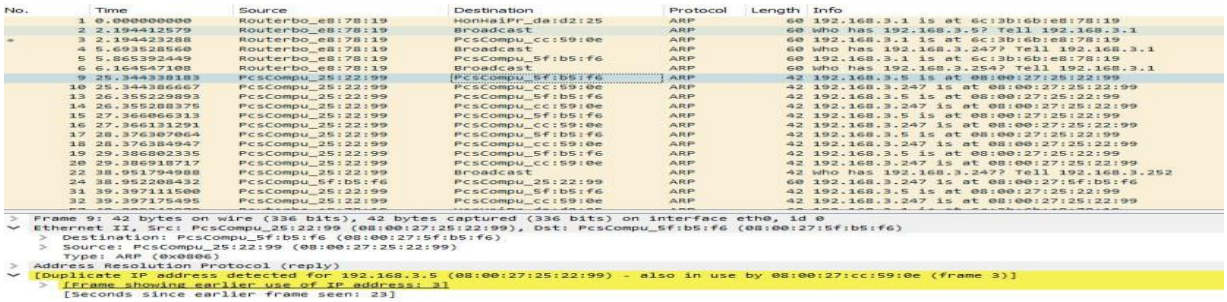


Figure 8. ARP Poisoning Attack Log Files Manipulation of Virtual Server MAC Addresses

The log file is obtained from the Wireshark application as shown in Figure 8, a virtual desktop computer accesses the url site on the browser http://exampleriset.com/dvwa on a virtual server with IP 192.168.3.5 MAC address 08: 00: 27: cc: 59: 0e. The attacker intercepts through the ARP protocol as in the blue sign, the user is directed to the attacker's computer and given a manipulated MAC address 08: 00: 27: 25: 22: 99 which is considered a server, in this process the user can still access the site by using Fixed IP. In the yellow sign, the IP server used with the MAC address 08: 00: 27: 25: 22: 99 is the same as the IP used with the MAC address 08: 00: 27: cc: 59: 0e. Virtual desktop computers cannot distinguish the MAC address of the server, only knowing the destination IP. The attacker also manipulates the MAC address of the virtual desktop computer to inform the virtual server. The virtual server cannot also distinguish the MAC address of the virtual desktop computer that has been manipulated by an attacker. In the blue sign the attacker informs the virtual server, on the yellow sign the desktop computer IP is monitored with a MAC address 08: 00: 27: 25: 22: 99 the same as the IP used with the MAC address 08: 00: 27: 5f: b5: f6 like shown in Figure 8.

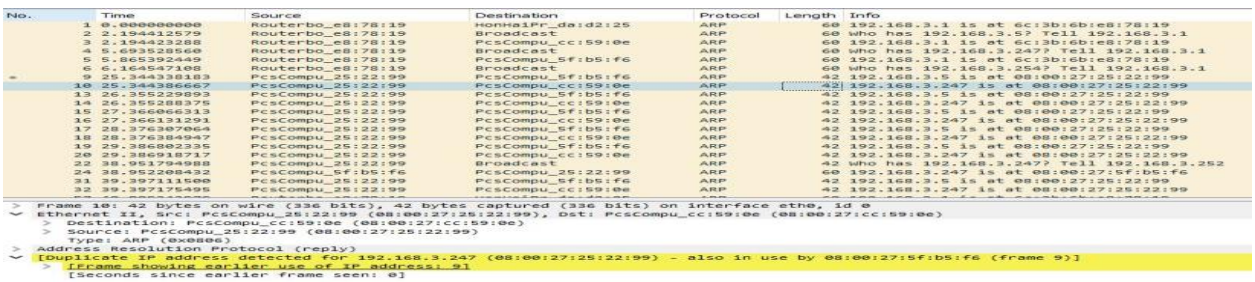


Figure 9. ARP Poisoning Attack Log File Manipulation Virtual MAC Address Desktop Computer

In testing ARP Poisoning attacks carried out via the HTTP protocol using the ettercap application, information is obtained in the form of target site access, user login and password as shown in Figure 10.

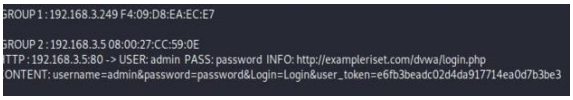
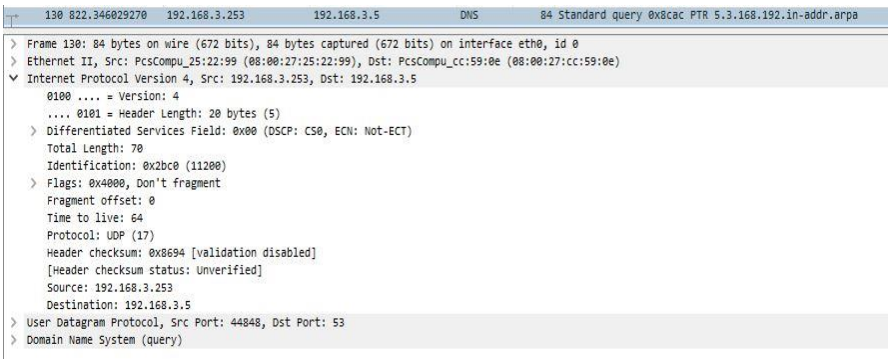


Figure 10. Results of ARP Poisoning Attacks Over HTTP Protocol

Analysis of the next stage of attack vector testing is session hijacking attacks. In Figure 11, a yellow square box indicates a mobile device with an IP address of 192.168.3.249 accessing the virtual server with an IP address of 192.168.3.5 using the HTTP protocol. Detailed information is shown on the intended site access, namely exampleriset.com, access using the Mozilla browser and the operating system for the mobile device used, namely Android 6.01. The purple square box displays the session ID of the cooker in the form of PHPSESSIID = 75vmoqpel2156t0e7tcsgvj8mv \ r \ n which the attacker will use. The session ID obtained is used by an attacker to perform session hijacking using the cookie manager tool, without using user login authentication and password from the user, the attacker can enter the site.

Figure. 11 Site Access ID Log Files From Mobile Phone Via HTTP Protocol

Testing analysis for session hijacking attacks on the HTTPS protocol does not get the cookie ID session data in the log file using wireshark. The next attack vector analysis is the SSL Stripping method with bettercap tools, on virtual testing of desktop computers and mobile devices access to the https://exampleriset.com/dvwa site and analysis of the access process via the HTTPS protocol, data passing through the DNS protocol is found as shown in Figure 12 for communication virtual desktop computer access to the virtual server.



\

Figure. 12 Communication Virtual Desktop Computer Access to Virtual Server

In Figure 13, for the virtual server response communication access to a virtual desktop computer, information is obtained with the response status query no such name PTR. Analysis of the test on the SSL Striping method found no user access authentication data.

Figure. 13 Communication Virtual Server Response To Virtual Desktop Computer

The following is a summary of the analysis with the MITM Attack Vector test scenario on a public wifi network shown in table 2.

Table 2. Summary of the Analysis

Type of Attack Vector	Analysis	Result
ARP Poisoning	In testing simulated data traffic attacks on the ARP protocol against virtual desktops, the attacker intercepts and manipulates MAC address information provision to virtual desktops and virtual servers, namely 08: 00: 27: 25: 22:99. Likewise testing on cellphones.	ARP Poisoning attack against the ARP protocol on a public wifi network simulation platform has been successfully implemented, data traffic between virtual desktops and virtual servers and cell phones with virtual servers can intercept and manipulate MAC address information provision.
Session Hijacking on the HTTP protocol	Obtaining intercepts of access rights and password information from the virtual desktop that is currently accessing the web server in the form phpsessiid = 4f1pnfr081e4jero11truspb60 \ r \ n and on the phone phpsessiid = 75vmoqpel21 56t0e7tcsgvj8mv \ r \ n .	Session Hijacking attack on HTTP protocol was implemented successfully with cookie manager plugin using phpsessi id without entering access rights and password.
Session Hijacking on the HTTPS protocol	Not getting userid and password information from the client in the form of a php session id	The session hijacking attack on the HTTPS protocol did not successfully intercept the session id
SSL Stripping	The attack simulation only obtains information with the response status of the query no such name PTR when virtual desktops and mobile phones access https://exampleriset.com/dvwa	The SSL Striping attack hasn't worked to downgrade the HTTPS to HTTP protocol

The summary of the analysis obtained through the MITM attack vector technique with 3 types of ARP Poisoning attacks, Session Hijacking and SSL Stripping against the public wifi network system simulation platform capable of manipulating attacks providing MAC Address information against the ARP protocol and sessiid tapping on the HTTP protocol, for testing simulation attacks on the HTTPS protocol get the status information response to a query no such name PTR.

4. CONCLUSION

The public wifi network system simulation platform can optimally be used in testing the MITM attack vector technique on the security performance of the public wifi network system simulation platform. Simulation testing of ARP poisoning attacks on the ARP protocol results in data traffic being intercepted and manipulated by providing MAC address information 08: 00: 27: 25: 22: 99.In testing the type of session hijacking attack on HTTP protocol data traffic, it is able to intercept virtual desktop access data on access rights and passwords in the form of phpsesiid 4f1pnfr081e4jero11truspb60 \ r \ n and mobile access form phpsesiid 75vmoqpel2156t0e7tcsgvj8mv \ r \ n. Testing session hijacking attack types on HTTPS protocol data traffic cannot be intercepted and manipulated. The simulation process of the type of SSL stripping attack is done by decreasing data traffic on the HTTPS to HTTP protocol so that the query response status no such name is obtained. Data traffic via the HTTP protocol on a public wifi network system simulation platform can be intercepted, intercepted and manipulated. In the HTTPS protocol, data is optimally encrypted. Further research is expected to develop a system platform design with adequate physical hardware, provision of different website applications, and implementation in real public spaces so that security performance testing is more optimal according to several Information Security Management Standards SNI ISO/IEC 27001 covering aspects of governance and risk management.

REFERENCES

[1] D. Mukhopadhyay, S. Karmakar, A. Meshram, and A. Jadhav, "A Prototype of IoT based Remote Controlled Car for Pentesting Wireless Networks," *2019 Glob. Conf. Adv. Technol. GCAT 2019*, pp. 1–7, 2019, doi: 10.1109/GCAT47503.2019.8978354.

[2] APJII, "Penetrasi & Profil Perilaku Pengguna Internet Indonesia Tahun 2018," *Apjii*, p. 51, 2019, [Online]. Available: www.apjii.or.id.

[3] A. Koyun and E. Al Janabi, "Social Engineering Attacks," *J. Multidiscip. Eng. Sci. Technol.*, vol. 4, no. 6, pp. 2458–9403, 2017.

[4] T. Radivilova and H. A. Hassan, "Test for penetration in Wi-Fi network: Attacks on WPA2-PSK and WPA2-enterprise," *2nd Int. Conf. Inf. Telecommun. Technol. Radio Electron. UkrMiCo 2017 - Proc.*, pp. 5–8, 2017, doi: 10.1109/UkrMiCo.2017.8095429.

[5] A. Susila, I. Riadi, and Y. Prayudi, "Wi-Fi Security Level Analysis for Minimizing Cybercrime," *Int. J. Comput. Appl.*, vol. 164, no. 7, pp. 35–39, 2017, doi: 10.5120/ijca2017913667.

[6] P. Fiadino, P. Casas, M. Schiavone, and A. D'Alconzo, "Online Social Networks anatomy: On the analysis of Facebook and WhatsApp in cellular networks," *Proc. 2015 14th IFIP Netw. Conf. IFIP Netw. 2015*, 2015, doi:

10.1109/IFIPNetworking.2015.7145326.
[7] H. Aldawood and G. Skinner, "Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review," *Proc. 2018 IEEE Int. Conf. Teaching, Assessment, Learn. Eng. TALE 2018*, no. October 2019, pp. 62–68, 2019, doi: 10.1109/TALE.2018.8615162.
[8] M. Z. A. B. Marc Capellupo, Jimmy Liranzo and G. W. Thaier Hayajneh, "Security and Attack Vector Analysis of IoT Devices," *Springer Int. Publ. AG 2017*, vol. 1, pp. 593–606, 2017, doi: 10.1007/978-3-319-72395-2.
[9] Y. Mardiana and J. Sahputra, "Analisa Performansi Protokol TCP , UDP dan SCTP," *J. Media Infotama*, vol. 13, no. 2, pp. 73–84, 2017.
[10] D. Harjowinoto, A. Noertjahyana, and J. Andjarwirawan, "Vulnerability Testing pada Sistem Administrasi Rumah Sakit X," *J. Infra*, vol. 4, no. 1, p. pp.227-p.232, 2016.
[11] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *Comput. Secur.*, vol. 38, pp. 97–102, 2013, doi: 10.1016/j.cose.2013.04.004.
[12] M. J. Islami, "Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index," *Masy. Telemat. Dan Inf. J. Penelit. Teknol. Inf. dan Komun.*, vol. 8, no. 2, p. 137, 2018, doi: 10.17933/mti.v8i2.108.
[13] Mulyadi and D. Rahayu, "Indonesia National Cybersecurity Review: Before and after Establishment National Cyber and Crypto Agency (BSSN)," *2018 6th Int. Conf. Cyber IT Serv. Manag. CITSM 2018*, no. Citsm, pp. 1–6, 2019, doi: 10.1109/CITSM.2018.8674265.
[14] Khairunnisa and Sutarti, "Perancangan Dan Analisis Keamanan Jaringan Nirkabel Dari Serangan Ddos (Distributed Denial of Service) Berbasis Honeypot," *J. PROSISKO*, vol. 4, no. 2, p. 8, 2017.
[15] R. Hartley, D. Medlin, and Z. Houlik, "Ethical Hacking: Educating Future Cybersecurity Professionals," *Proc. EDSIG Conf.*, no. October, pp. 1–10, 2017, [Online]. Available: http://iscap.info.