

Implementation of Penetration Testing Tools to Test Wi-Fi Security Levels at the Directorate of Innovation and Business Incubators

Tamsir Ariyadi^{1*}, M. Rizky Pohan²

¹Department of Computer Engineering, Universitas Bina Darma, Palembang, Indonesia.

²Department of Computer Engineering, Universitas Bina Darma, Palembang, Indonesia.

Received:

Revised:

Accepted:

Published:

Corresponding Author:

Author Name*:

Email*:

DOI:

© 2023 The Authors. This open access article is distributed under a (CC-BY License)



Phone*: +62...

Abstract: Wi-Fi networks have become a critical infrastructure in many organisations, including the Directorate of Innovation and Business Incubator. However, potential vulnerabilities in Wi-Fi networks also increase as technology advances. Therefore, testing is needed to identify and address security that can harm network users. This research aims to implement penetration testing tools in testing the security level of Wi-Fi networks at the Directorate of Innovation and Business Incubator. The penetration testing method is used to test security and assess the level of resistance to attacks on Wi-Fi in the form of simulated attacks. One of the operating systems that provides penetration testing tools that meet the needs of testing is linux times. the tools used in the penetration testing process are airmon-ng, airodump-ng, aireplay-ng, aircrack-ng, macchanger, ettercap and wireshark. The results showed that the Wi-Fi security of the Directorate of Innovation and Business Incubator still needs to be improved where the results of the four types of attacks only one failed, namely MAC Spoofing. In addition, the tests on Denial of Service, Cracking The Encryption, and Man-in-the-Middle attacks were successful. The application of anticipation by increasing Wi-Fi security based on the attacks that have been carried out can prevent these attacks.

Keywords: Wi-Fi, Penetration Testing, Tool, Security, Kali Linux

Introduction

In the increasingly rapidly developing digital era, wireless connectivity, especially Wi-Fi networks, has become important infrastructure in various organizations (Efe & Kaplan, 2019). Wi-Fi (Wireless Fidelity) is a technology that allows electronic devices, such as computers, smartphones, or tablets, to connect to an internet network or local network (LAN) without using physical cables. Wi-Fi uses IEEE 802.11 standard technology to transmit data via radio waves, which allows practical and efficient internet access and wireless

communications (Suroto, 2018). Wi-Fi provides easy internet access needed by staff, students, visitors and various devices connected to the network, all of which play an important role in supporting daily activities and innovation at the Directorate of Innovation and Business Incubators (DIIB).

However, the existence of a Wi-Fi network does not escape cyber attacks carried out by irresponsible parties which can result in harm to other people (Adiguna & Widagdo, 2022). Based on data from the National Cyber and Crypto Agency (BSSN) in 2022, Indonesia recorded around 370.02 million cyber attack incidents. This figure shows an increase of 38.72% from

How to Cite:

Example: Susilawati, S., Doyan, A., Mulyadi, L., & Hakim, S. (2019). Growth of tin oxide thin film by aluminum and fluorine doping using spin coating Sol-Gel techniques. *Jurnal Penelitian Pendidikan IPA*, 1(1), 1-4. <https://doi.org/10.29303/jppipa.v1i1.264>

the previous year, where around 266.74 million cyber attacks were recorded in Indonesia (Pratiwi, 2022). Therefore, Wi-Fi network security is crucial considering the large amount of sensitive data and confidential information that can be accessed via this network. Security threats such as hacking, data theft and attacks of various types increasingly intensify the need to protect Wi-Fi (Haeruddin & Kurniadi, 2021).

The Directorate of Innovation and Business Incubator (DIIB) is a directorate at Bina Darma University that focuses on developing innovation and providing support for business growth from student and lecturer innovation. DIIB also uses the Wi-Fi network as infrastructure to help meet information needs such as accessing the internet, opening social media, carrying out online transactions and the like. The Wi-Fi network provided by the Directorate of Innovation and Business Incubators has implemented the WPA2-PSK security system on the access points used to connect to the network. However, using WPA2-PSK security alone on Wi-Fi without any additional security configuration still has many loopholes that can be exploited with the increasing level of complexity of cyber attacks and the variety of techniques used by attackers, this is very dangerous for Wi-Fi network users in DIIB because it does not rule out the possibility of attacks on the network.

Based on the problems above, identifying security weaknesses in the network is an important step to deal with existing threats. In this case, penetration testing is an effective method for testing and exposing security weaknesses in a system or network (Wahyudi et al., 2019). Penetration testing on Wi-Fi involves a deliberate effort to test the security of a wireless network using techniques and methods similar to attacks that can be carried out by attackers such as Denial of Service, Password Cracking, Spoofing, and Man in the Middle (MITM) attacks (Saraun et al., 2022).

In carrying out penetration testing, the use of various tools is key in simulating attacks to test the security level of a system or network. To carry out effective penetration testing on Wi-Fi networks, tools are needed that have various functionalities, such as network scanning, exploitation and monitoring (Kongara, 2023). Kali Linux is a Linux distribution specifically developed for penetration testing and computer security purposes (Rusdi & Prasti, 2019). Kali Linux provides many tools and applications that are integrated by default to support penetration testing activities. In it, there are various important tools that are ready to be used to carry out penetration testing on Wi-Fi networks such as aircrack-ng, wireshark and other tools (Kyei & Asante, 2020).

This research aims to implement penetration testing tools to test the level of Wi-Fi network security applied at the Directorate of Innovation and Business Incubator, especially in facing the threat of cyber attacks that have the potential to disrupt and harm users. In this research, penetration testing will be carried out by simulating several types of attacks, including Denial of Service, Cracking the Encryption, MAC Spoofing, and Man-in-the-Middle using tools available in the Kali Linux operating system (Gunawan et al., 2018). Thus, this research specifically aims to determine potential security gaps that can be exploited by various wireless network attacks that have the potential to threaten the Wi-Fi used by the Directorate of Innovation and Business Incubators.

Previous research has carried out a lot of penetration testing to test the security of Wi-Fi networks. For example, research by (Lu & Yu, 2021) shows experimental results that the Wi-Fi network penetration testing method with Kali Linux has a good effect in improving Wi-Fi network security evaluation. Research conducted by (Adhi Prakosa, 2020) also identified common attacks on Wi-Fi networks by using penetration testing methods and providing data as material to strengthen network security.

Method

The research method used is the penetration testing method which refers to the NIST SP 800-115 standard (Astriani, 2021). According to (Alamanni, 2015) the penetration testing method is a method that simulates attacks on a system or network to identify configuration errors, vulnerabilities or security violations and related exploits that can be used by real attackers to gain access to a system or network. The NIST SP 800-115 penetration testing method consists of several stages, namely the planning, discovery, attack, and reporting stages (Santoso et al., 2022).

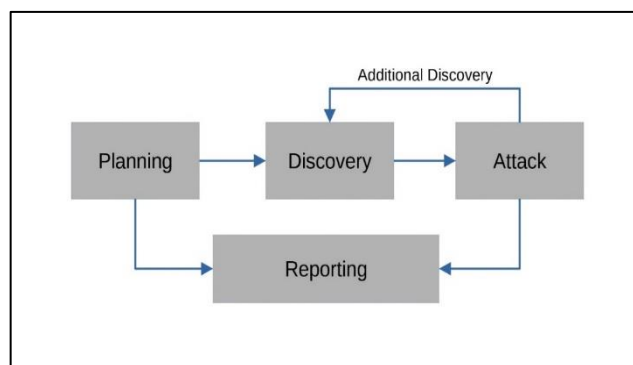


Figure 1. NIST SP 800-115 method

This research requires the kali linux operating system to perform penetration testing on Wi-Fi networks (Ariyadi et al., 2023). The kali linux operating system is specifically designed for penetration testing purposes and has various tools that can be used to test network security (Sitompul et al., 2023). The penetration testing tool that will be used in this research is based on the evaluation of attacks that will be carried out on the Wi-Fi network of the Directorate of Innovation and Business Incubator.

Table 2. Tools penetration testing

Attack	Tool	Version
Denila of service	Airmon-ng	1.7
	Airodump-ng	1.7
	Aireplay-ng	1.7
Cracking the Encryption	Airmon-ng	1.7
	Airodump-ng	1.7
	Aireplay-ng	1.7
	Aircrack-ng	1.7
MAC Spoofing	Airmon-ng	1.7
	Airodump-ng	1.7
Man-in-the-Middle	Ettercap	0.8.3.1
	Wireshark	4.0.7

In this test, several test steps and their explanations, as for the flowchart image of the testing technique can be seen in Figure 2.

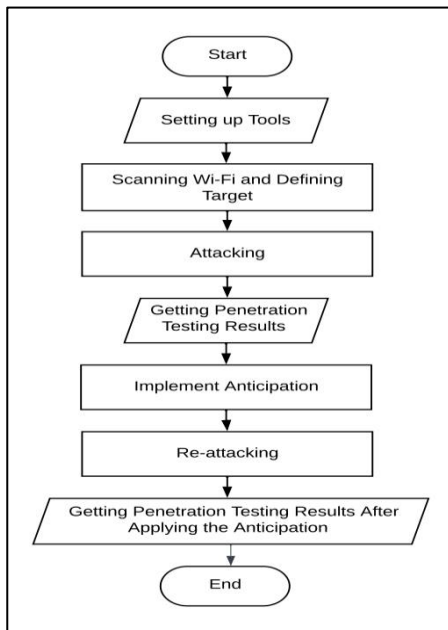


Figure 2. Flowchart

The first step in the testing flow is to prepare penetration testing tools that will be used in testing and ensure that the tools are ready to use and in accordance

with research needs. Next, scanning the Wi-Fi network and determining the target to be tested. After scanning, then carry out attacks using penetration testing tools that are suitable for testing Wi-Fi network security. From this process will get the results of a successful attack. After getting the results of penetration testing, the researcher will apply anticipation of a successful attack. Furthermore, re-attack the network that has been applied anticipation. From all the processes that have been carried out, we will get the overall results of each testing process.

The researcher collected information about the network topology, devices used, existing security and analysed the information found to identify potential vulnerabilities that may exist in the system on the Directorate of Innovation and Business Incubator's Wi-Fi network.

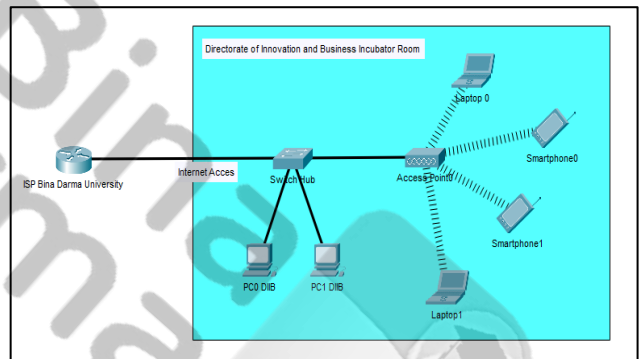


Figure 3. Network topology

In Figure 2.6 the Directorate of Innovation and Business Incubator room uses a switch to connect computers in the room using a LAN cable and an access point that emits signals to connect devices such as laptops, smartphones, and others wirelessly in order to access the internet. The penetration test targets in this research are access points and devices connected to the wireless network. The Wi-Fi network system running at the Directorate of Innovation and Business Incubator uses the WPA2-PSK (Wi-Fi Protected Access 2 Pre-Shared Key) security system with the default configuration on the access point (Indira Reddy & Srikanth, 2019). WPA2-PSK security is a security mechanism used to protect Wi-Fi networks from attacks and unauthorised access. WPA2-PSK uses symmetric encryption using a pre-shared key, also known as a passphrase or password (Chang et al., 2019).

Researchers conducted information searches and identified a number of vulnerabilities in Wi-Fi networks that would be used as a basis for testing attacks. The results of the vulnerability analysis conducted by researchers can be seen in table.

Table 3. Vulnerability analysis

Vulnerability	Information	Potential Attacks Identified
No Firewall	No firewall that enforces network traffic control or access rules	Potential Denial of Service (DoS) attacks, spoofing
Configuration Weaknesses	The use of WPA2-PSK encryption, which is the encryption standard on Wi-Fi networks, still has loopholes for cracking.	Potential cracking the encryption attacks
Authentication Weaknesses	Use of weak authentication or still using automatic authentication mechanisms on user devices	Potential attack of cracking the encryption, making it easier for attackers to get the WPA key
Weaknesses of MAC filtering	No MAC restrictions on devices connected to the network	Potential unauthorised access, MAC Spoofing
Lack of Monitoring	No monitoring of network traffic or suspicious activity	Potential man-in-the-middle attack
Lack of Security Awareness	Unwary users use Wi-Fi networks to access the internet related to important data	Potential man-in-the-middle attacks, data theft

Result and Discussion

This stage is the core stage in the research where researchers will simulate Denial of Service (DoS), Encryption Cracking, MAC Spoofing, and Man-in-the-Middle (MITM) attacks based on the results of the discovery stage using the tools and flow that have been determined at the planning stage.

The results of denial of service attacks using the tools airmon-ng, airodump-ng, and aireplay-ng. In the results of the attack, the Wi-Fi network of the Directorate of Innovation and Business Incubator can still be attacked by sending a deauthentication frame to the access point so that users cannot connect to the network until the attack is stopped or the deauthentication frame is no longer sent. This is because the Deauthentication frame is used in Wi-Fi networks to forcibly disconnect the connection between the device and the access point can be seen in the figure..

```

(ky@kali)-[~]
└─$ sudo aireplay-ng -0 0 -a D8:A4:91:08:37:DF wlan1
12:58:54 Waiting for beacon frame (BSSID: D8:A4:91:08:37:DF) on channel 5
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
12:58:54 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:A4:91:08:37:DF]
12:58:54 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:A4:91:08:37:DF]
12:58:55 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:A4:91:08:37:DF]
12:58:55 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:A4:91:08:37:DF]
12:58:56 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:A4:91:08:37:DF]
12:58:56 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:A4:91:08:37:DF]
12:58:57 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:A4:91:08:37:DF]
12:58:57 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:A4:91:08:37:DF]
12:58:58 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:A4:91:08:37:DF]
12:58:58 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:A4:91:08:37:DF]
12:58:59 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:A4:91:08:37:DF]
12:58:59 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:A4:91:08:37:DF]
12:58:59 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:A4:91:08:37:DF]
12:59:00 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:A4:91:08:37:DF]
12:59:00 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:A4:91:08:37:DF]
12:59:01 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:A4:91:08:37:DF]
12:59:01 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:A4:91:08:37:DF]
12:59:02 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:A4:91:08:37:DF]
12:59:02 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:A4:91:08:37:DF]
12:59:03 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:A4:91:08:37:DF]
12:59:03 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:A4:91:08:37:DF]
12:59:04 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:A4:91:08:37:DF]
12:59:04 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:A4:91:08:37:DF]
12:59:05 Sending DeAuth (code 7) to broadcast -- BSSID: [D8:A4:91:08:37:DF]
    
```

Figure 4. Denial of Service attack

The results of the encryption cracking attack using the tools airmon-ng, airodump-ng, aireplay-ng, and aircrack-ng were successful. This attack poses a serious potential risk to network security and data privacy that must be strictly maintained. In the results of the attack, the Wi-Fi network encryption security of the Directorate of Innovation and Business Incubator can still be cracked using brute force techniques to break the WPA key encryption with the aim of obtaining the password that has been applied to the access point. The results of this attack reveal that the security system used, in this case the WPA key encryption, is not strong enough to protect the network from brute force attacks.

```

Aircrack-ng 1.7

[00:01:55] 58176/1679616 keys tested (510.50 k/s)

Time left: 52 minutes, 56 seconds                               3.46%

KEY FOUND! [ diib2023 ]

Master Key   : 82 A1 4C 6A E9 D8 07 76 C9 26 51 E4 3C A4 AD A2
              95 A9 AC 67 02 71 77 60 DB 98 8F 7A 87 F7 20 4D

Transient Key : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
              00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
              00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
              00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC   : 76 D4 52 FB 62 B3 EF 06 CD 70 19 96 D2 E6 5D 4A
    
```

Figure 5. Result Cracking the Encryption

The results of the MAC spoofing attack using the airmon-ng, airodump-ng, and macchanger tools. In the results of this attack, researchers were unable to connect to a Wi-Fi network using the MAC address of a device that was already connected to the network. This is because the access point cannot provide connection access to two MAC addresses of the same device. This attack was successful when the device left the network. This suggests that Wi-Fi network security is well organised in terms of managing connected devices. These results show the importance of careful device management in Wi-Fi networks, as well as the ability of

access points to detect and restrict unauthorised access. At the same time, however, the results also show that this kind of attack still has the potential to be costly if proper precautions are not taken.

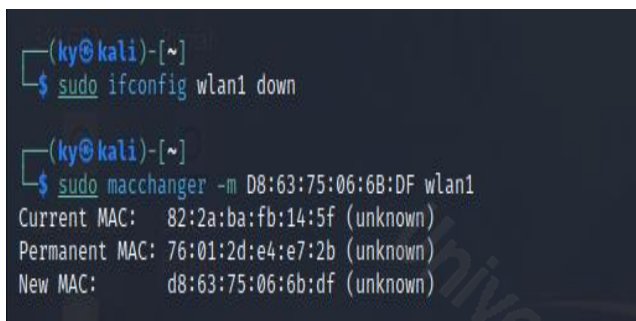


Figure 6. MAC Spoofing

The results of man-in-the-middle attacks using ettercap and wireshark tools. In the results of the attack successfully obtained sensitive user login information with sniffing techniques using ettercap. This attack can sniff websites with HTTP and HTTPS protocols combined with SSLstrip which can downgrade the HTTPS protocol to HTTP.

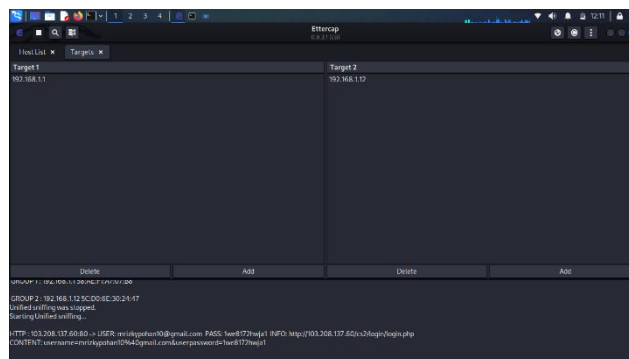


Figure 7. Man-in-the-Middle attack

From the overall results, this testing activity was carried out in order to determine the level of security of the Wi-Fi network at the Directorate of Innovation and Business Incubator. In the penetration testing process, researchers conducted four types of attacks, namely denial of service, cracking the encryption, MAC spoofing, and man-in-the-middle using penetration testing tools. The results of all attack processes can be seen in Table 4.

Table 4. Penetration testing result

Attack type	Required information	Tools used	Status	Description
Denial of Service	Channel and BSSID access point	Airmon-ng, Airodump-ng, Aireplay-ng	Success	Successfully disconnect Wi-Fi
Cracking the Encryption	Channel and BSSID access point, Handshake user, Database wordlist	Airmon-ng, Airodump-ng, Aireplay-ng, Aircrack-ng	Success	Successfully obtained Wi-Fi password
MAC Spoofing	MAC address of the user connected to the network	Airmon-ng, Airodump-ng, Macchanger	Fail	Failed to connect to Wi-Fi network with fake MAC
Man-in-the-Middle	IP address access point and IP address user	Ettercap, Wireshark	Success	Successfully get user data both HTTP and HTTPS protocols

After conducting a series of tests on the security conditions of the existing Wi-Fi network at the Directorate of Innovation and Business Incubator, researchers have successfully identified various vulnerabilities and weak points in the network infrastructure. These results are the basis for ongoing

anticipation to increase the level of Wi-Fi network security from attacks that could potentially threaten network users. The security improvements that will be implemented based on the results of the penetration testing that has been carried out can be seen in table 5.

Table 5. Implement anticipation

Improvement	Description
Firewall Configuration	Enable the firewall feature on the access point
WPA3 Encryption Configuration	Use better encryption and provide a password with a length of 15 characters, a combination of uppercase letters, lowercase letters, numbers and symbols.
MAC filtering whitelist configuration	Allows only registered MACs to connect to the network.
AP Isolation Configuration	Restricts communication between hosts on the same network

The next step is testing after applying anticipation, this is done to find out whether the retest

produces different results from the results that have been carried out in security testing on the Wi-Fi network

of the Directorate of Innovation and Business Incubator. The retesting process is carried out exactly the same as the previous test by carrying out four types of attacks, namely denial of service, cracking the encryption, MAC spoofing, and man-in-the-middle using penetration testing tools. From all the processes carried out, the improvement status can be seen in table 6. This table provides a clear picture of whether the implemented

corrective actions are successful in increasing the level of network security.

Table 6. Penetration testing result after applying anticipation

Attack type	Required information	Tools used	Status	Description
Denial of Service	Channel and BSSID access point	Airmon-ng, Airodump-ng, Aireplay-ng	Fail	Unsuccessfully disconnecting Wi-Fi
Cracking the Encryption	Channel and BSSID access point, Handshake user, Database wordlist	Airmon-ng, Airodump-ng, Aireplay-ng, Aircrack-ng	Fail	Unsuccessful in obtaining Wi-Fi password
MAC Spoofing	MAC address of the user connected to the network	Airmon-ng, Airodump-ng, Macchanger	Fail	Failed to connect to Wi-Fi network with fake MAC
Man-in-the-Middle	IP address access point and IP address user	Ettercap, Wireshark	Fail	Unable to get IP Address during scanning

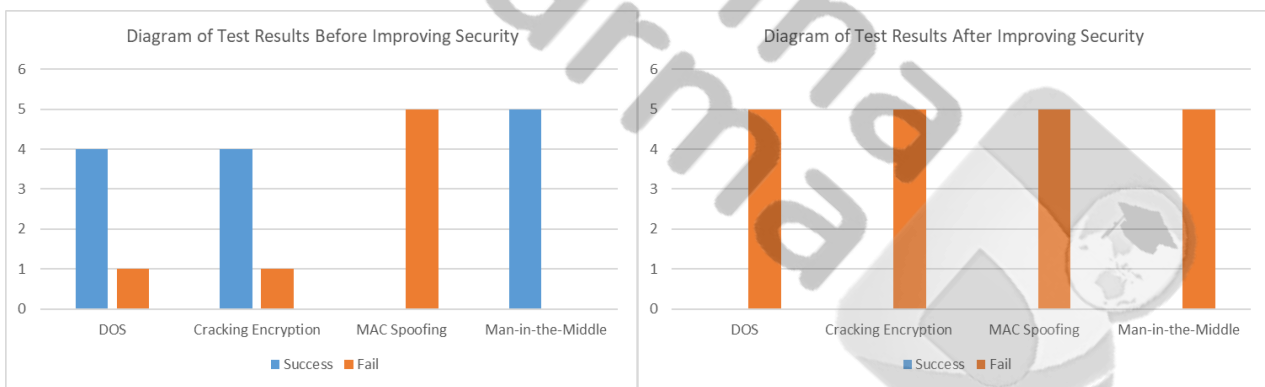


Figure 8. Testing Comparison

In Figure 8, the denial of service, encryption cracking, MAC spoofing, and man-in-the-middle attacks were tested 5 times each. From the diagram, it can be seen that the denial of service attack has a high scale with 4 successful attacks and 1 failure. The encryption cracking attack was also successfully carried out 4 times and 1 failure, the MAC spoofing attack has a fairly small scale with 1 success and 4 failures. The man-in-the-middle attack was successfully carried out 5 times without failure, so it has the highest scale of other attacks.

In Figure 8, denial of service, encryption cracking, MAC spoofing, and man-in-the-middle attacks were tested 5 times each. From the diagram, it can be seen that by increasing the security of attacks such as denial of service is successfully prevented without any successful attack attempts, these results have a high scale. The encryption cracking attack after improving encryption security successfully counteracted the

cracking attack 5 times this result shows a very good improvement. MAC spoofing and man-in-the-middle attacks also have a very good scale, where all attack attempts cannot be successfully carried out after increasing security on the Wi-Fi network.

Conclusion

Based on research on Wi-Fi network security testing that has been carried out at the Directorate of Innovation and Business Incubator using penetration testing tools, it can be concluded that Wi-Fi network security at the Directorate of Innovation and Business Incubator needs to be improved. This is evidenced by Denial of Service, Cracking the encryption and Man-in-the-Middle attacks that can be exploited using penetration testing tools. Denial of Service attacks cause all devices connected to the Wi-Fi network to be

disconnected and unable to connect to the network. This attack can be anticipated by implementing a firewall and WPA3 security. Cracking the encryption attack causes the password on the access point to be found or cracked with brute force techniques. This attack can be anticipated by implementing WPA3 encryption and complex password combinations. The application of whitelist MAC filtering on access points has a positive impact on network users because it makes it difficult for attackers to connect to the network with fake MAC addresses. Man-in-the-Middle attacks are successful in obtaining important target data and important information about users. This attack can be anticipated by implementing AP isolation on the access point, by limiting communication between users can avoid potential Man-in-the-Middle attacks.

Acknowledgments

The author would like to thank the supervisors from the Computer Engineering Department of Bina Darma University for the knowledge and financial support provided in this research.

Author Contributions

Authors listed in this article contributed to the research and development of the article.

Funding

This research uses the author's personal funds.

Conflicts of Interest

In writing this article, we sincerely declare that there are no conflicts of interest that may affect the objectivity and integrity of the results.

References

- Adhi Prakosa, B. (2020). Security Analysis of Wireless Local Area Network (WLAN) Network with the Penetration Testing Method. *Jurnal Mantik*, 4(3), 1658–1662. <https://iocscience.org/ejournal/index.php/mantik>
- Adiguna, M. A., & Widagdo, B. W. (2022). Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus : Router Tp-Link Mercusys Mw302r). *Jurnal SISKOM-KB (Sistem Komputer Dan Kecerdasan Buatan)*, 5(2), 1–8. <https://doi.org/10.47970/siskom-kb.v5i2.268>
- Alamanni, M. (2015). Kali Linux Wireless Penetration Testing Essentials. In *Community experience distilled*. www.packtpub.com
- Ariyadi, T., Widodo, T. L., Apriyanti, N., & Kirana, F. S. (2023). Analisis Kerentanan Keamanan Sistem Informasi Akademik Universitas Bina Darma Menggunakan OWASP. *Techno.Com*, 22(2), 418–429. <https://doi.org/10.33633/tc.v22i2.7562>
- Astriani, T. (2021). Analisa Kerentanan Pada Vulnerable Docker Menggunakan Scanner Openvas Dan Docker Scan Dengan Acuan Standar Nist 800-115. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, 8(4), 2041–2050. <https://doi.org/10.35957/jatisi.v8i4.1232>
- Chang, T. H., Chen, C. M., Hsiao, H. W., & Lai, G. H. (2019). Cracking of wpa and wpa2 using gpus and rule-based method. *Intelligent Automation and Soft Computing*, 25(1), 183–192. <https://doi.org/10.31209/2018.100000054>
- Efe, A., & Kaplan, M. B. (2019). *Multidisciplinary Studies and Innovative Technologies Wi-Fi Security Analysis For E & M-Government Applications*. 86–98.
- Gunawan, T. S., Lim, M. K., Kartiwi, M., Malik, N. A., & Ismail, N. (2018). Penetration testing using Kali linux: SQL injection, XSS, wordpres, and WPA2 attacks. *Indonesian Journal of Electrical Engineering and Computer Science*, 12(2), 729–737. <https://doi.org/10.11591/ijeecs.v12.i2.pp729-737>
- Haeruddin, H., & Kurniadi, A. (2021). Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus: TP-Link Archer A6). *CoMBInES-Conference on Management ...*, 1(1), 508–515. <https://journal.uib.ac.id/index.php/combines/article/view/4475>
- Indira Reddy, B., & Srikanth, V. (2019). Review on Wireless Security Protocols (WEP, WPA, WPA2 & WPA3). *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 5(4), 28–35. <https://doi.org/10.32628/cseit1953127>
- Kongara, D. (2023). A Process of Penetration Testing Using Various Tools. *Mesopotamian Journal of Cyber Security*, August, 94–104. <https://doi.org/10.58496/mjcs/2023/014>
- Kyei, M., & Asante, M. (2020). Penetration Testing of IEEE 802.11 Encryption Protocols using Kali Linux Hacking Tools. *International Journal of Computer Applications*, 176(32), 26–33. <https://doi.org/10.5120/ijca2020920365>
- Lu, H. J., & Yu, Y. (2021). Research on WiFi Penetration Testing with Kali Linux. *Complexity*, 2021. <https://doi.org/10.1155/2021/5570001>
- Pratiwi, F. S. (2022). *BSSN Catat 370,02 Juta Serangan Siber ke Indonesia pada 2022*. <https://dataindonesia.id/internet/detail/bssn-catat-37002-juta-serangan-siber-ke-indonesia->

pada-2022

- Rusdi, M. I., & Prasti, D. (2019). Penetration Testing Pada Jaringan Wifi Menggunakan Kali Linux. *Seminar Nasional Teknologi Informasi Dan Komputer 2019*, 260–269.
- Santoso, N. A., Ainurohman, M., & Kurniawan, R. D. (2022). Penerapan Metode Penetrasiion Testing Pada Keamanan Jaringan Nirkabel. *Jurnal Responsif : Riset Sains Dan Informatika*, 4(2), 162–167. <https://doi.org/10.51977/jti.v4i2.831>
- Saraun, A., Lumenta, A. S. M., & Sengkey, D. F. (2022). Analisa Keamanan Jaringan Nirkabel IEEE 802.11 pada Kantor Dinas Pendidikan Kabupaten Minahasa. *Jurnal Teknik Informatika*, 17(1), 565–572. <https://doi.org/10.35793/JTI.17.1.2022.35321>
- Sitompul, A. T., Cahyadi, F., Informatika, J. T., Teknik, F., Maritim, U., & Ali, R. (2023). ANALISIS PENERAPAN METODE PENETRATION TESTING PADA KEAMANAN JARINGAN WLAN (Studi Kasus : Universitas Maritim Raja Ali Haji). *Jurnal Hasil Penelitian Dan Industri Terapan*, 12(01), 23–29.
- Suroto. (2018). Wlan security: Threats and countermeasures. *International Journal on Informatics Visualization*, 2(4), 232–238. <https://doi.org/10.30630/joiv.2.4.133>
- Wahyudi, E., Luthfi, E. T., & Efendi, M. M. (2019). Wireless Penetration Testing Method To Analyze WPA2-PSK System Security And Captive Portal ISSN : 2087-894 Jurnal Explore STMIK Mataram – Volume 9 No 1 Tahun 2019 ISSN : 2087-894. *Jurnal Explore STMIK Mataram*, 9(1), 1–7.