JURNAL INFOTEL
VOL. 16, NO. 1, FEBRUARY 2024, PP. 120–135. DOI:10.20895/INFOTEL.V16I1.1057

RESEARCH ARTICLE

Evaluation of Wireless Network Security with Penetration Testing Method at PT. PLN UP2D S2JB

Tamsir Ariyadi[1,*], Irham[2], and Eko Fajar Cahyadi[3]

[1,2] Department of Computer Engineering, Universitas Bina Darma, Palembang 30266, Indonesia
[3]Department of Telecommunication Engineering, Institut Teknologi Telkom Purwokerto, Purwokerto 53147, Indonesia

*Corresponding email: tamsirariyadi@binadarma.ac.id

Received: October 16, 2023; Revised: December 14, 2023; Accepted: February 6, 2024.

Abstract: Advances in information and communication technology continue to develop over time. This causes significant changes in social, economic, and political conditions. One of the companies that require strong network security is PT. PLN (Perusahaan Listrik Negara) Persero which is the leading energy company in Indonesia. In this case, the a need to evaluate network security at PT. PLN becomes very important. This evaluation will help identify vulnerabilities and security gaps that exist in PT. PLN's network infrastructure. Network security evaluation using the penetration testing execution standards (PTES) method can provide an overview of the vulnerabilities or weaknesses of the network system at PT. PLN UP2D S2JB which has quite a lot of gaps to be exploited. The parameters used in this study are attacking the infrastructure, The rogue access point, and ARP Spoofing to test the wireless network security system. This is evidenced by the results of the 15 tests carried out, only two failed, namely in the type of attack on the rogue access point. The results of penetration testing are very necessary and important as feedback for system managers in fixing existing vulnerabilities.

Keywords: security, vulnerability, network, PT. PLN, evaluation, penetration testing

1 Introduction

Advances in information [1] and communication [2] technology continue to grow over time [3]. This has led to significant changes in social [4], economic and political conditions [5]. In this context [6], information technology may be described as a double-edged

 ISSN: 2085-3688; e-ISSN: 2460-0997

sword because it can have both negative and positive effects [7, 8]. It is described as a double-edged sword [9] because it can have both negative and positive effects [10]. The positive impact is the emergence of conveniences in the search for information [11], but it is also balanced by the negative impact with the emergence of various crimes against individuals [12] and groups by utilizing information technology and the internet or often referred to as cybercrime [13].

Network security has become a major concern for companies, especially for companies that have complex and sensitive information technology infrastructure [14]. One company that requires strong network security is PT. PLN (Perusahaan Listrik Negara) Persero, which is a leading energy company in Indonesia. PT. PLN has an extensive and complex network, covering electricity distribution systems, payment management systems, and internal operations and management systems. The sustainability and operational efficiency of PT. PLN is highly dependent on the availability, integrity, and confidentiality of their network systems [15, 16].

Therefore, along with technological advances, the design of a wireless network security system connected to the internet [17,18] must be well planned and understood to effectively protect the resources on the network and minimize attacks by attackers or hackers [19]. Due to the lack of awareness of administrators or people who act as admins in running the system, while external factors can occur due to weak systems made (configuration) and the large level of cybercrime [20]. Computer network security is part of an important system to maintain data validity and integrity [21]. Based on this, the researchers formulated the problem in this study [22], namely how to evaluate the security of the wireless network at the PT. PLN UP2D S2JB office to produce secure data access from various kinds of crimes [21].

This wireless network security evaluation will help identify vulnerabilities or security gaps that exist in the PT. PLN UP2D S2JB wireless network system [22]. Thus, appropriate preventive and corrective actions can be taken to improve network security and protect PT. PLN UP2D S2JB from existing and potential threats in the future. In addition [23], evaluating network security at PT. PLN UP2D S2JB will also provide confidence to employees in carrying out their work by maintaining a high level of security in managing sensitive data [24, 25].

2 Research Method

This research methodology is shown in Figure 1, which illustrates the stages of the research. This standard covers everything related to penetration testing from pre-engagement interactions, intelligence gathering, Threat modeling, Vulnerability analysis, exploitation, post-exploitation, and reporting [26].

2.1 Pre-engagement

In this initial stage, the researcher made observations on the object to be tested and conducted interviews with the network administrator of PT. PLN UP2D S2JB in order to facilitate research related to the discussion of penetration testing, wireless network, network topology, wireless network penetration test.

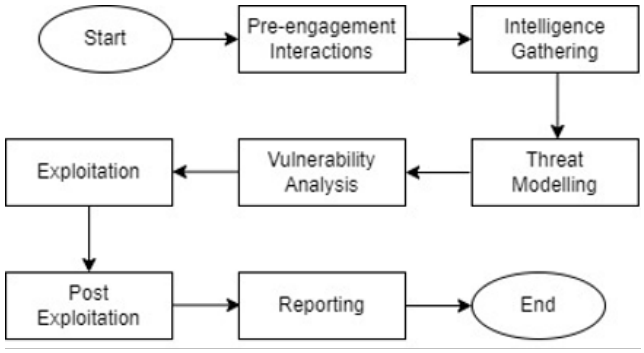


Figure 1: Research methodology.

2.2 Intelligence Gathering

At this stage, researchers collect information that has been obtained from observations and interviews with the network administrator of PT. PLN UP2D S2JB as much as possible in order to facilitate the penetration testing process on the wireless network.

2.3 Threat Modeling

At this stage, researchers identify threats to security gaps that are likely to occur on the wireless network of PT. PLN UP2D S2JB in order to facilitate the determination of the type of attack.

Table 1: Threat Modelling

No	Threat Modelling
1	Not yet implemented strong access point isolation on network security, so attackers can easily carry out attacks.
2	Not actively monitoring network traffic and not detecting suspicious activity, so it is not recognized when there is an attack.
3	Other people whose status is not as an employee of PT. PLN UP2D S2JB who can connect directly to the network by knowing the password that has been applied.
4	Not yet implemented MAC filtering or access restrictions on users
5	Not disabling the auto connect feature on the user's device, allowing the device to automatically connect to the network without the user's consent.
6	There is no awareness of PT. PLN UP2D S2JB employees in the use of wireless networks that are prone to cyber-attacks.
7	Has not implemented strong Intrusion Detection/Prevention Systems (IDS/IPS)on the wireless network security system of PT. PLN UP2D S2JB office.
8	Have not enabled or configured static address resolution protocol (ARP) entries on key network devices such as routers.

2.4 Vulnerability Analysis

This stage is the most important stage, where researchers identify several gaps in network security that aim to determine the type of attack used in penetration testing on the wireless network of PT. PLN UP2D S2JB.

Table 2: Vulnerability Analysis

No	Vulnerability Analysis
1	Not implementing access point isolation or IDS/IPS on the existing network security system can be determined that there is a security gap that can be exploited by researchers with the attacking the infrastructure attack type in the form of (deauthentication) Aireplay-ng, mdk3 and mdk4.
2	The lack of access point isolation in the network security system and also employees who do not fully understand the use of wireless networks where the auto connect feature on the device will be a gap that can be exploited. In this gap, researchers can carry out a type of rogue access point attack in the form of an evil twin on a wireless network, which is a type of attack carried out by creating a fake network that mimics a legitimate network. In this attack, researchers try to create a fake wireless network using the same or very similar SSID (network name) as a legitimate network. After users connect to this fake network, researchers will get information such as login credentials (username and password) and other confidential information.
3	Not activating and configuring static ARP entries and AR P binding in the wireless network security system where this security gap can be exploited by researchers by manipulating the ARP table on the network. In this type of attack, researchers can modify, limit, or block the internet data access for users connected to the same network. This type of attack can be interpreted as ARP spoofing/poisoning.

2.5 Exploitation

2.5.1 Attacking the infrastructure

In this type of infrastructure attack, researchers conducted an Aireplay attack or deauthentication five times on the wireless access point network of the PT. PLN UP2D S2JB office. This type of attack can disconnect users connected to the network so that the user cannot connect to the network during deauthentication and aims to find out the security gaps in the wireless network at the PT. PLN UP2D S2JB office.

In Figure 2 is a scenario of the type of attack attacking the infrastructure where the researcher or attacker tries to attack directly to the object, namely the access point and the impact of this attack will affect the user connected to the access point being attacked so that the connected user will be disconnected from the access point. For a demonstration of this attack, researchers used airgeddon Figure 3 and to find out whether this attack was successful or not, researchers used Wireshark.

In Figure 3 is the initial display in the airgeddon menu for attacking the infrastructure, then the researcher types the number 6 command to start the deauth aireplay attack on the wireless network at PT. PLN UP2D S2JB.

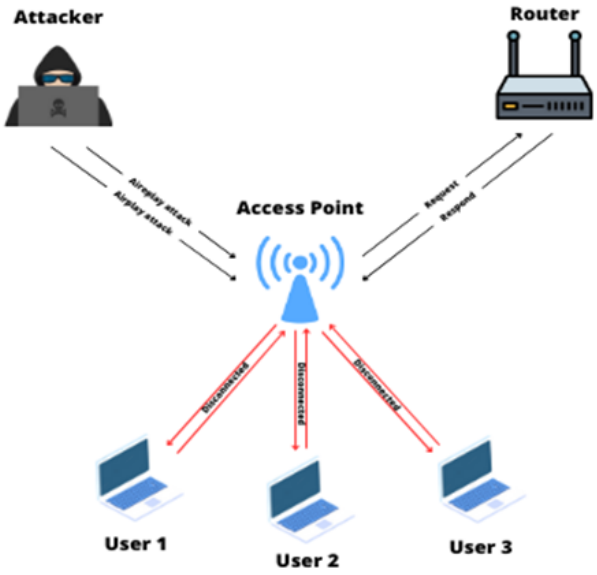


Figure 2: Deauthentication aireplay attack overview.

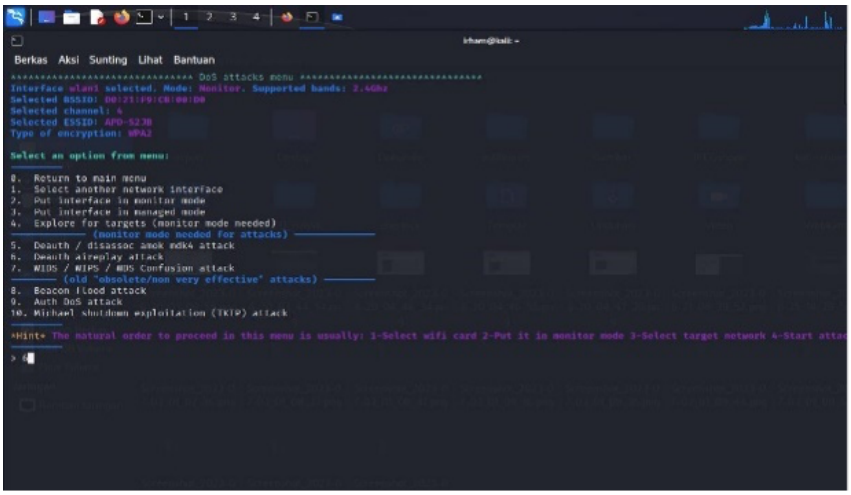


Figure 3: Aireplay deauthentication command attack.

In Figure 4 researchers have launched an aireplay (deauthentication) attack with airgeddon which if this attack is not stopped, the impact of users connected to the network will be disconnected and cannot be reconnected, to be able to prove whether this attack is successful or not, researchers use Wireshark.

It can be seen in Figure 5 that Wireshark can detect deauthentication attacks so it can be said that researchers have successfully carried out this type of attack attacking the in-

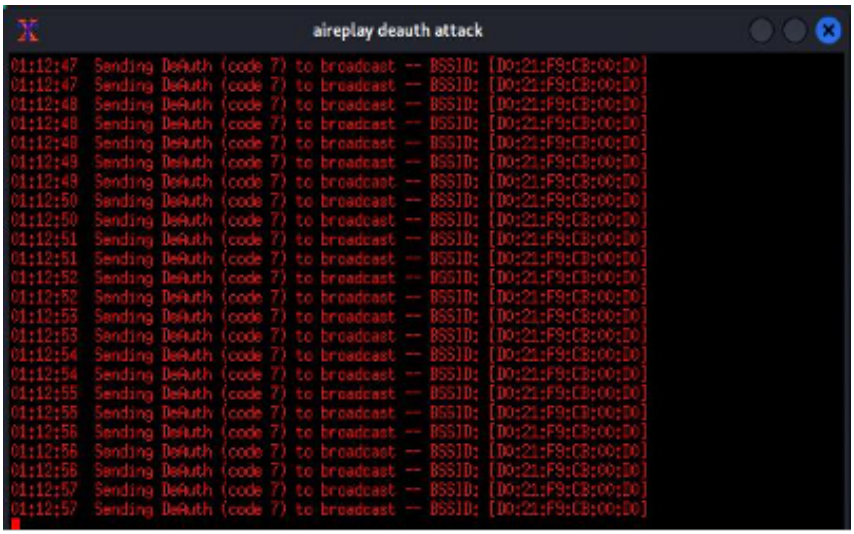


Figure 4: Deauthentication aireplay attack.

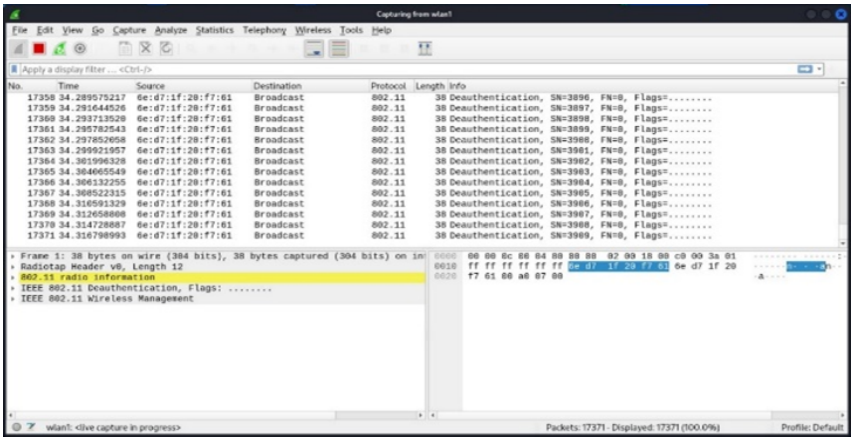


Figure 5: Deauthentication on Wireshark.

frastructure on the access point, where the impact of this attack can disconnect all users connected to the network.

2.5.2 The rogue access point

In this type of attack, the rogue access point was tested five times. In Figure 6 is a scenario of the rogue access point attack type, where this attack is carried out to try to deceive connected network users by creating a fake or unauthorized access point that looks like a legitimate original network this attack is also carried out in conjunction with deauthentication which aims to disconnect all users connected to the network so that users are forced

into the fake network. When users try to connect to this fake access point, all login credentials can be obtained by researchers. The purpose of this type of attack is to find out if there are user-side vulnerabilities that can be exploited by researchers and also to test the existing security on the network.

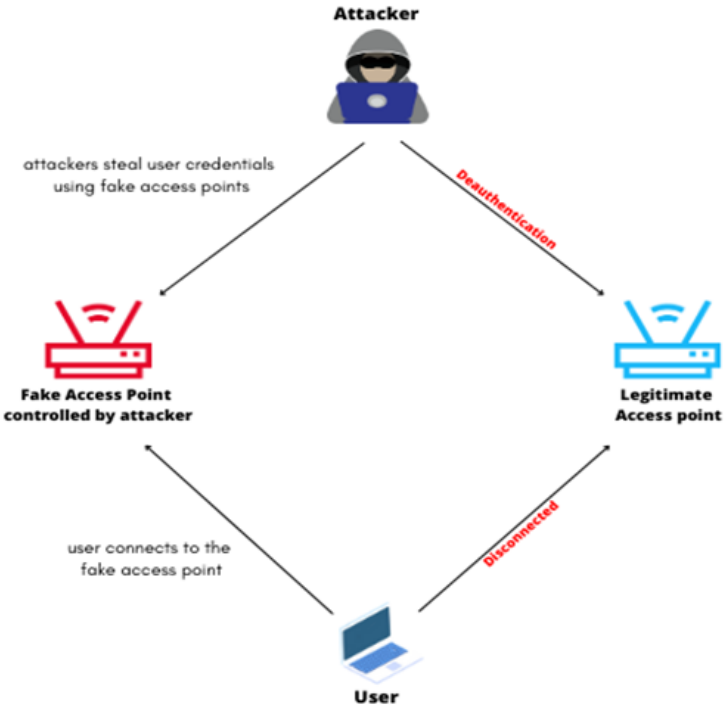


Figure 6: Overview of the rogue access point attack.

For the demonstration carried out in this attack, researchers used the same airgeddon tool as the tool used in the previous type of attack and to find out whether this attack was successful or not airgeddon will display the login credential in the form of a password from the wireless network which can be seen in Figure 8 captive portal airgeddon.

In this type of attack the user connected to the original access point will be disconnected and will be forced to enter this fake SSID so that the user will re-enter the login password.

In Figure 8 is a captive portal view with airgeddon that displays access point (AP), DHCP, Deauth, control, DNS, and web server. If there is one user who wants to connect to this fake SSID, then all user activities can be seen on this display.

In Figure 9 is a view of the login credentials that have been obtained and formed in a.txt file. Because the user trying to connect to this fake SSID, the user will be forced to enter the original login password, which in the end the SSID is not a legitimate access point. Password: AkuGanteng 2020 is the correct login password successfully obtained and there is also a captured password on failed attempts which means that there are users who entered the wrong original network password, if the password entered by the user is wrong, then airgeddon can detect it.

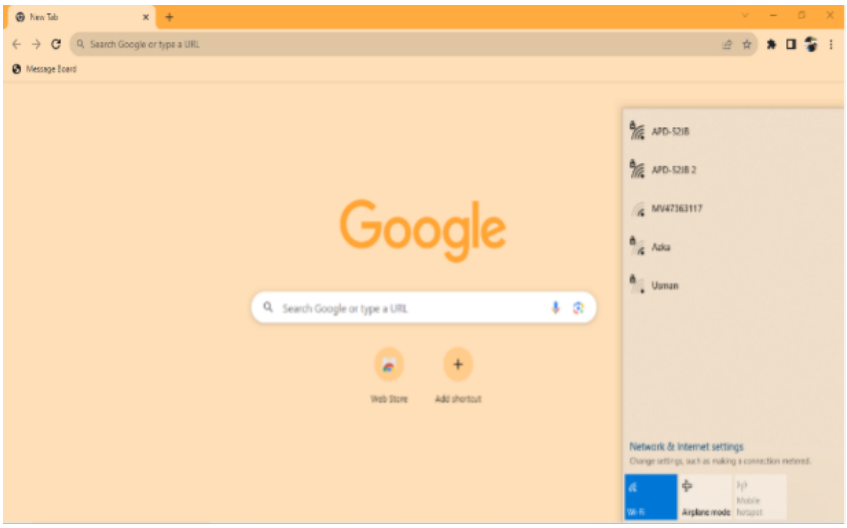


Figure 7: Authorised and unauthorised access point.

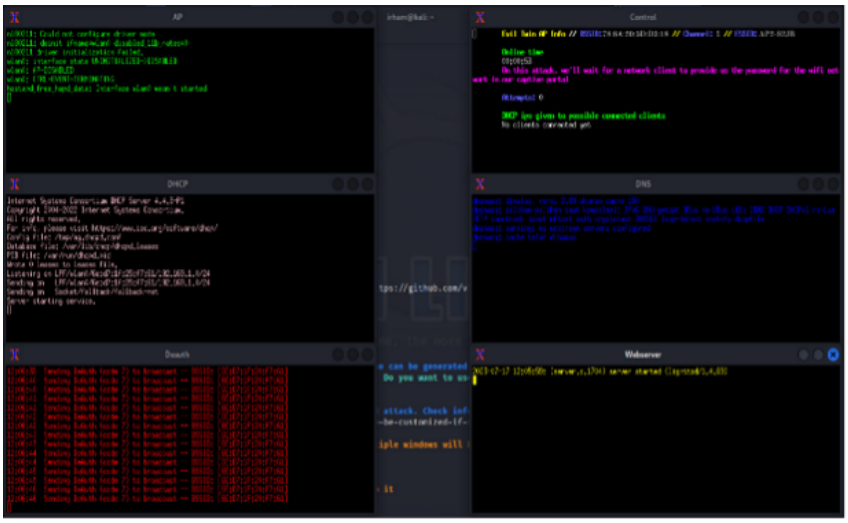


Figure 8: Captive protal with airgeddon.

2.5.3 ARP Spoofing

In this last type of attack, researchers conducted an attack in the form of ARP spoofing which was tested five times. ARP spoofing is a type of attack that aims to manage wireless network traffic and manipulate the ARP table on devices in the network system.

In Figure 10 is a scenario of a type of ARP spoofing attack where this attack can be said that the Attacker is in the middle between the user and the network, so that network traffic data can be controlled. Not only that, this attack can also block access to user data

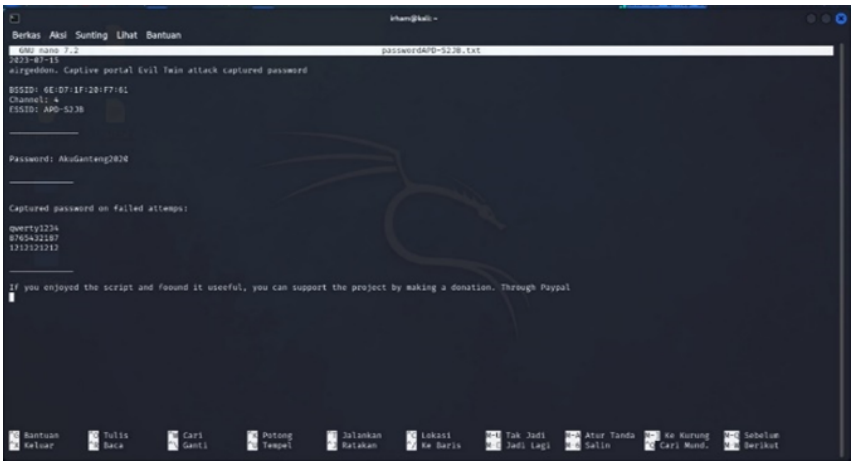


Figure 9: Capturing login credentials with txt file.

connected to the network, even though the user is still connected but cannot access the internet because his data access has been blocked.

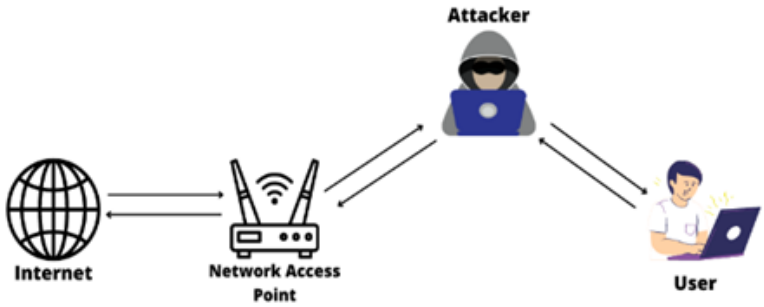


Figure 10: Overview of arp spoofing attack.

To carry out this type of attack, researchers use the evil limiter tool where this tool can effectively carry out this type of ARP spoofing attack which aims to block access to user data connected to the network.

In Figure 11 is the initial appearance of the evil limiter tool where this tool can directly scan interfaces and gateways on the network. Furthermore, to be able to find out all users connected to the network, the researchers conducted scanning, namely in the form of broadcasting on the network system found in Figure 12, the purpose of this broadcasting is to send data to connected users, in order to find out all the hosts on the network.

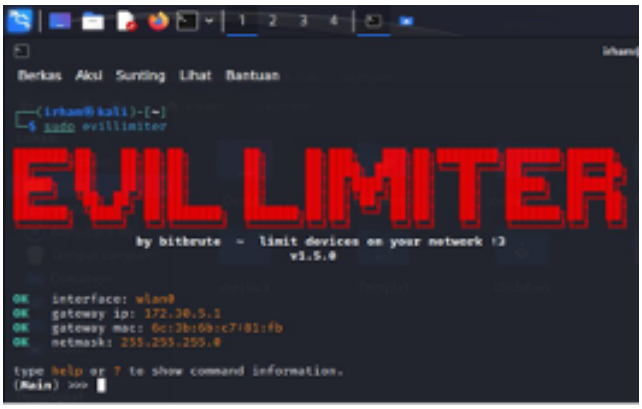


Figure 11: Initial view of evil limiter.

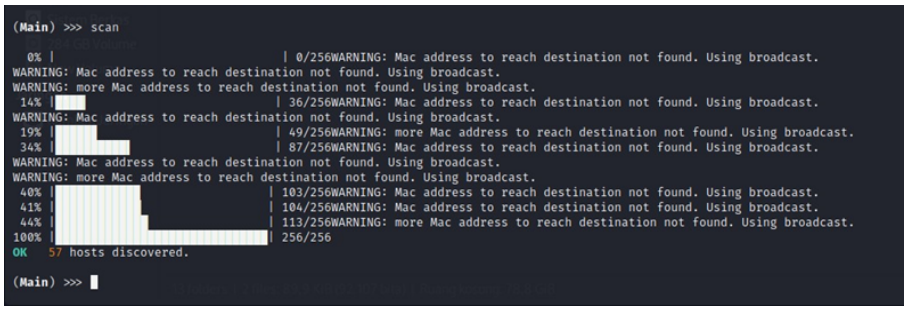


Figure 12: Scanning with evil limiter.

After scanning the network, researchers can find out the ARP table containing all users connected to the same network, in Figure 13 researchers have successfully scanned the network as evidenced by the display of all users who are currently connected.

In Figure 13 it can be seen that there are IP addresses and MAC addresses of all users connected to the network, then researchers block data access to one of the connected users in testing the security of the network system. By typing the command block [IP user] then Enter on the keyboard Figure 14. This command aims to block data access to the user.

Furthermore, to see if the user has successfully blocked data access, the researcher returns to the host evil limiter which aims to display the network ARP table again.

Then, in Figure 15 it can be seen that researchers have successfully carried out this type of ARP Spoofing attack in the form of blocking data access so that the user cannot access the internet even though the user is still connected to the network.

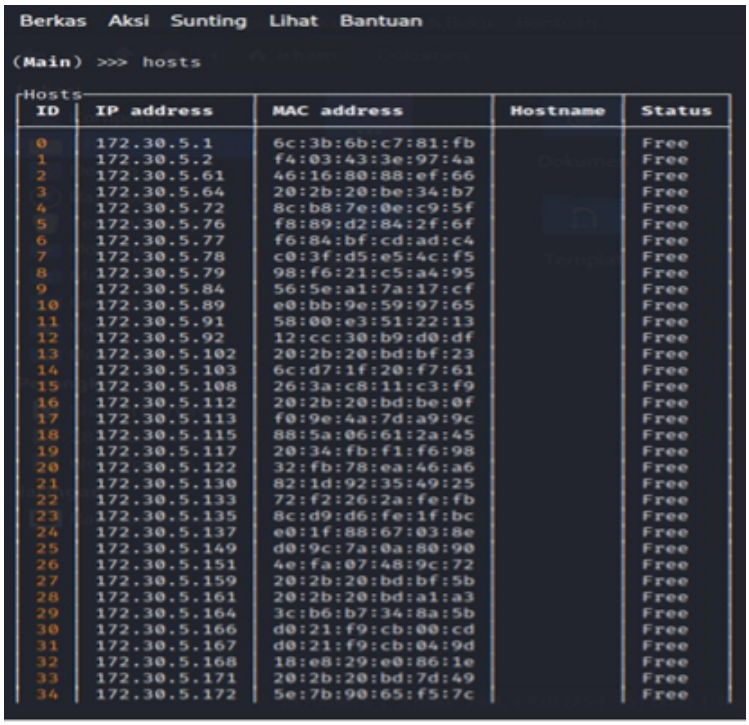


Figure 13: All users connected to the network.

Figure 14: Blocking data access on one of the users.

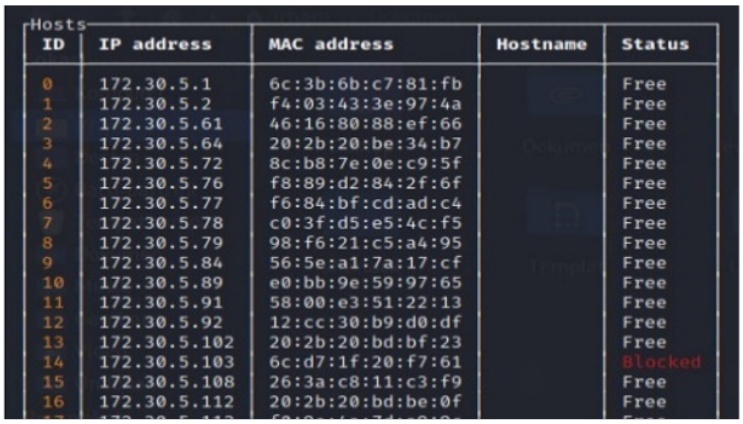
3 Results

3.1 Reporting

Based on Table 3. is the delivery of the results of penetration testing conducted by researchers using the penetration testing execution standards (PTES) method on the wireless network of the PT. PLN UP2D S2JB office.

3.1.1 Attacking the infrastructure

In this type of attack, researchers succeeded in carrying out Aireplay-ng attacks five times, which means that it indicates quite weak network security at the PT. PLN UP2D S2JB office. This type of attack is the most common attack used by pen-testers or attackers in penetration testing on wireless networks.


Hosts

ID	IP address	MAC address	Hostname	Status
0	172.30.5.1	6c:3b:6b:c7:81:fb		Free
1	172.30.5.2	f4:03:43:3e:97:4a		Free
2	172.30.5.61	46:16:80:88:ef:66		Free
3	172.30.5.64	20:2b:20:be:34:b7		Free
4	172.30.5.72	8c:b8:7e:0e:c9:5f		Free
5	172.30.5.76	f8:89:d2:84:2f:6f		Free
6	172.30.5.77	f6:84:bf:cd:ad:c4		Free
7	172.30.5.78	c0:3f:d5:e5:4c:f5		Free
8	172.30.5.79	98:f6:21:c5:a4:95		Free
9	172.30.5.84	56:5e:a1:7a:17:cf		Free
10	172.30.5.89	e0:bb:9e:59:97:65		Free
11	172.30.5.91	58:00:e3:51:22:13		Free
12	172.30.5.92	12:cc:30:b9:d0:df		Free
13	172.30.5.102	20:2b:20:bd:bf:23		Free
14	172.30.5.103	6c:d7:1f:20:f7:61		Blocked
15	172.30.5.108	26:3a:c8:11:c3:f9		Free
16	172.30.5.112	20:2b:20:bd:be:0f		Free

Figure 15: User data access successfully blocked.

3.1.2 The rogue access point

In this type of attack, researchers managed to attack the rogue access point three times in five attacks, which means that the wireless network security at the PT. PLN UP2D S2JB office is still quite weak and there is a gap on the user side which can be exploited by attackers to enter Wi-Fi and steal user data. This greatly affects the security of the company's system which in the future can be utilised by irresponsible attackers.

3.1.3 ARP spoofing

In this last type of attack, researchers also managed to do it five times. This type of attack is difficult to detect and is also very dangerous because it can cut off user data access so this type of attack can affect employee work. If all connected users have their data access cut off on the network with this type of attack, then all employees cannot access the internet. This is very undesirable and can harm the company.

3.2 Anticipate Attacks

Based on what has been done penetration testing by researchers on wireless network security at PT. PLN UP2D S2JB has succeeded in identifying various weaknesses or vulnerabilities that exist in the network security system. So, from the results obtained, sustainable anticipation can be carried out to improve the security of wireless networks from various types of attacks that may potentially threaten network users. The security improvements that can be applied based on the results of the penetration testing that has been carried out can be seen in Table 4.

4 Conclusion

In implementing penetration testing in an institution, licensing is needed because penetration testing involves activities that can be considered as attacks on systems or networks.

Table 3: Threat modelling

Type of Attack	Tools	Required Data	Test Limitations	Testing Results	Status
Attacking the infrastructure	Airgeddon	WLAN network SSID	Disconnecting	Successful Successful Successful Successful Successful	Low
The rogue access point	Airgeddon	WLAN network SSID	Cloning the SSID	Failed Failed Successful Successful Successful	Medium
ARP spoofing	Evil limiter	Attacker	Block data access of users connected to the WLAN network	Successful Successful Successful Successful Successful	Low

So that testing without a valid permit, this action can violate the law and bring legal consequences to the party or person conducting penetration testing. The type of attacking the infrastructure attack that was carried out five times and had the status of successfully disconnecting the connected user can be interpreted as there is a vulnerability and implemented IDS/IPS on the network security system of the PT. PLN UP2D S2JB office. The rogue access point type of attack was carried out five times, three times successful and two of them failed can be interpreted that there are still many employees who do not fully understand the use of wireless networks so there are gaps in the user side that can be exploited by attackers. The type of ARP spoofing attack was carried out five times and with all successful status can be interpreted that ARP binding or static ARP Entries protection has not been implemented so there is a vulnerability gap on the sis. Network security evaluation using the PTES method can provide an overview of the vulnerabilities or weaknesses in a wireless network security system at PT. PLN UP2D S2JB which has many gaps to be exploited. This is evidenced by the results of 15 tests conducted, only three failed, namely in the type of attack the rogue access point. The results of penetration testing are very necessary and important as feedback for system managers in fixing existing vulnerability

Table 4: Improved network security and anticipated attacks

Improved	Description
Firewall configuration	Enable firewall features in the form of IDS/IPS on wireless network security.
WPA3 security configuration	Use security with better encryption and apply passwords with a combination of uppercase, lowercase letters, numbers, and symbols.
Configure ARP binding or static ARP entries protection	Reduces the possibility of ARP spoofing attacks that can be used by attackers to take over communications in the network.
Turn off the automation feature (auto-connect Wi-Fi) on the user's device	Overcoming evil twin attacks that if you want to connect to the network, you must have permission from the user's device.

gaps and for further research development suggestions should add various other types of attacks on different objects.

References

[1] F. Z. Lidanta, A. Almaarif, and A. Budiyono, "Vulnerability analysis of wireless LAN networks using penetration testing execution standard: A case study of cafes in Palembang," in *8th International Conference on ICT for Smart Society: Digital Twin for Smart Society, ICISS 2021 - Proceeding*, 2021. doi: 10.1109/ICISS53185.2021.9533216.

[2] A. I. Kusumarini and H. B. Seta, "Information system security analysis to determine server security vulnerability with penetration testing execution standard (PTES) method at VWX University," in *Proceedings - 3rd International Conference on Informatics, Multimedia, Cyber, and Information System, ICIMCIS 2021*, 2021. doi: 10.1109/ICIMCIS53775.2021.9699285.

[3] M. F. Safitra, M. Lubis, and A. Widjajarto, "Security vulnerability analysis using penetration testing execution standard (PTES): Case study of government's website," *in ACM International Conference Proceeding Series*, 2023. doi: 10.1145/3592307.3592329.

[4] T. S. Gunawan, M. K. Lim, M. Kartiwi, N. A. Malik, and N. Ismail, "Penetration testing using Kali linux: SQL injection, XSS, wordpres, and WPA2 attacks," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 12, no. 2, pp. 729–737, 2018, doi: 10.11591/ijeecs.v12.i2.pp729-737.

[5] D. Overstreet, H. Wimmer, and R. J. Haddad, "Penetration testing of the amazon echo digital voice assistant using a denial-of-service attack," in *Conf. Proc. - IEEE SOUTH-*

EASTCON, vol. 2019-April, 2019, doi: 10.1109/SoutheastCon42311.2019.9020329.

[6] A. O. Barznji, T. A. Rashid, and N. K. Al-Salihi, "Computer network simulation of firewall and VoIP performance monitoring," *Int. J. Online Biomed. Eng.*, vol. 14, no. 9, pp. 4–18, 2018, doi: https://doi.org/10.3991/ijoe.v14i09.8508.

[7] M. Kyei and M. Asante, "Penetration testing of IEEE 802.11 encryption protocols using Kali Linux hacking tools," *Int. J. Comput. Appl.*, vol. 176, no. 32, pp. 26–33, 2020, doi: 10.5120/ijca2020920365.

[8] R. R. Asaad, "Penetration testing: Wireless network attacks method on Kali Linux OS," *Acad. J. Nawroz Univ.*, vol. 10, no. 1, pp. 7–12, 2021, doi: 10.25007/ajnu.v10n1a998.

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

[10] J. Chen, T. Yang, B. He, and L. He, "An analysis and research on wireless network security dataset," in *Proc. - 2021 Int. Conf. Big Data Anal. Comput. Sci. BDACS 2021*, no. June 2021, pp. 80–83, 2021, doi: 10.1109/BDACS53596.2021.00025.

[11] C. Agbeboaye, F. O. Akpojedje, and J. Okoekhian, "Security threats analysis of wireless local area network," *Compusoft*, vol. 7, no. 6, pp. 2773–2779, 2018, doi: 10.6084/ijact.v7i6.722.

[12] Y. Khera, D. Kumar, S. Sujay, and N. Garg, "Analysis and impact of vulnerability assessment and penetration testing," in *Proc. Int. Conf. Mach. Learn. Big Data, Cloud Parallel Comput. Trends, Prespectives Prospect. Com. 2019*, no. February 2019, pp. 525–530, 2019, doi: 10.1109/COMITCon.2019.8862224.

[13] T. Radivilova, L. Kirichenko, D. Ageiev, and V. Bulakh, "Classification methods of machine learning to detect DDoS attacks," in *Proc. 2019 10th IEEE Int. Conf. Intell. Data Acquis. Adv. Comput. Syst. Technol. Appl. IDAACS 2019*, vol. 1, no. April 2020, pp. 207–210, 2019, doi: 10.1109/IDAACS.2019.8924406.

[14] Y. Kristiyanto and Ernastuti, "Analysis of deauthentication attack on IEEE 802.11 connectivity based on IoT technology using external penetration test," *CommIT J.*, vol. 14, no. 1, pp. 45–51, 2020, doi: 10.21512/commit.v14i1.6337.

[15] L. G. Nikolov and V. O. Slavyanov, "Network infrastructure for cybersecurity analysis," in *Proceedings of International Scientific Conference "Defense Technologies", Faculty of Artillery, Air Defense and Communication and Information Systems*, no. October 2018.

[16] E. Al Neyadi, S. Al Shehhi, A. Al Shehhi, N. Al Hashimi, M. Qbea'H, and S. Alrabaee, "Discovering public Wi-Fi vulnerabilities using Raspberry pi and Kali Linux," in *Proc. - 2020 12th Annu. Undergrad. Res. Conf. Appl. Comput. URC 2020*, pp. 8–11, 2020, doi: 10.1109/URC49805.2020.9099187.

[17] T. Ariyadi, T. L. Widodo, N. Apriyanti, and F. S. Kirana, "Analisis kerentanan keamanan sistem informasi akademik Universitas Bina Darma menggunakan OWASP," *Techno.Com*, vol. 22, no. 2, pp. 418–429, 2023, doi: 10.33633/tc.v22i2.7562.

[18] M. A. Abo-Soliman, "Enterprise WLAN security flaws current attacks and relative mitigations," in *ACM Int. Conf. Proceeding Ser., no. August 2018*, 2018, doi: 10.1145/3230833.3230836.

[19] M. G. Al-Hamiri, J. Haider, and H. M. A. Abboodi, "Performance evaluation of WLAN in enterprise WAN with real-time applications based on OPNET modeler," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 21, no. 2, pp. 911–918, 2020, doi: 10.11591/ijeecs.v21.i2.pp911-918.

[20] S. Maesaroh, L. Kusumaningrum, N. Sintawana, D. P. Lazirkha, and R. D. O., "Wireless network security design and analysis using wireless intrusion detection system," *Int. J. Cyber IT Serv. Manag.*, vol. 2, no. 1, pp. 30–39, 2022, doi: 10.34306/ijcitsm.v2i1.74.

[21] H. J. Lu and Y. Yu, "Research on WiFi penetration testing with Kali Linux," *Complexity*, vol. 2021, 2021, doi: 10.1155/2021/5570001.

[22] N. Cifuentes, G. Gatica, and R. Linfati, "Un modelo de programación lineal para el problema de máquinas paralelas no relacionadas en el área de secado de un aserradero en Chile," *Rev. Fac. Ing.*, vol. 26, no. 46, pp. 9–17, 2017, doi: 10.19053/01211129.v26.n46.2017.7309.

[23] A. M. Alsahlany, Z. H. Alfatlawy, and A. R. Almusawy, "Experimental evaluation of different penetration security levels in wireless local area network," *J. Commun.*, vol. 13, no. 12, pp. 723–729, 2018, doi: 10.12720/jcm.13.12.723-729.

[24] Y. Xiao, H. H. Chen, B. Sun, R. Wang, and S. Sethi, "MAC security and security overhead analysis in the IEEE 802.15.4 wireless sensor networks," *Eurasip J. Wirel. Commun. Netw.*, vol. 2006, pp. 1–12, 2006, doi: 10.1155/WCN/2006/93830.

[25] I. S. Al-Mejibli and D. N. R. Alharbe, "Analyzing and evaluating the security standards in wireless network: A review study," *Iraqi J. Comput. Informatics*, vol. 46, no. 1, pp. 32–39, 2020, doi: 10.25195/ijci.v46i1.248.

[26] D. N. Astrida, A. R. Saputra, and A. I. Assaufi, "Analysis and evaluation of wireless network security with the penetration testing execution standard (PTES)," *Sinkron*, vol. 7, no. 1, pp. 147–154, 2022, doi: 10.33395/sinkron.v7i1.11249.