JURNAL INFOTEL
Informatics - Telecommunication - Electronics
Website Jurnal : http://ejournal.st3telkom.ac.id/index.php/infotel
ISSN : 2085-3688; e-ISSN : 2460-0997

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

Tamsir Ariyadi[1*], Irham[2]
[1,2] Department Of Computer Engineering, Bina Darma University
[1,2]Jl. Jendral A. Yani, Plaju, Palembang 30266, Indonesia
*Corresponding email: tamsirariyadi@binadarma.ac.id

Received, Revised, Accepted

Abstract — Advances in information and communication technology continue to grow over time. This causes significant changes in social, economic, and political conditions. One company that requires strong network security is PT PLN (Perusahaan Listrik Negara) Persero, which is a leading energy company in Indonesia. In this case, the need to evaluate network security at PT PLN is very important. This evaluation will help identify vulnerabilities and security gaps that exist in PT PLN's network infrastructure. This 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 exploit. This is evidenced by the results of fifteen tests conducted, only two of which 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 gaps.

Keywords – Security, Vulnerability, Network, PT PLN, Evaluation, Penetration Testing

I. INTRODUCTION

Advances in information and communication technology continue to grow over time.[1][2] This has led to significant changes in social, economic and political conditions.[3][4] In this context, information technology may be described as a double-edged sword because it can have both negative and positive effects.[5][6] It is described as a double-edged sword because it can have both negative and positive effects.[7][8] The positive impact is the emergence of conveniences in the search for information, but it is also balanced by the negative impact with the emergence of various crimes against individuals and groups by utilizing information technology and the internet or often referred to as cybercrime.[9][10]

Network security has become a major concern for companies, especially for companies that have complex and sensitive information technology infrastructure.[11][12] 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.[13][14]

Therefore, along with technological advances, the design of a wireless network security system connected to the internet must be well planned and understood in order to effectively protect the resources on the network and minimize attacks by attackers or hackers.[15][16] 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 cyber crime.[17][18] Computer network security as part of an important system to maintain data validity and integrity.[19][20] Based on this, the researchers formulated the problem in this study, namely how to evaluate the security of the wireless network at the PT PLN UP2D S2JB office so as to produce secure data access from various kinds of crimes.[21][22]

This wireless network security evaluation will help identify vulnerabilities or security gaps that exist in the PT PLN UP2D S2JB wireless network system.[23] 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.[24] In addition, 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.[25]

II. RESEARCH METHOD

This research methodology is shown in Fig. 1, which illustrates the stages of the research. This standard covers everything related to penetration testing from pree-engagement interactions, Intelligence gathering, Threat modelling, Vulnerability analysis, Exploitation, Post Exploitation and Reporting.[26][27]

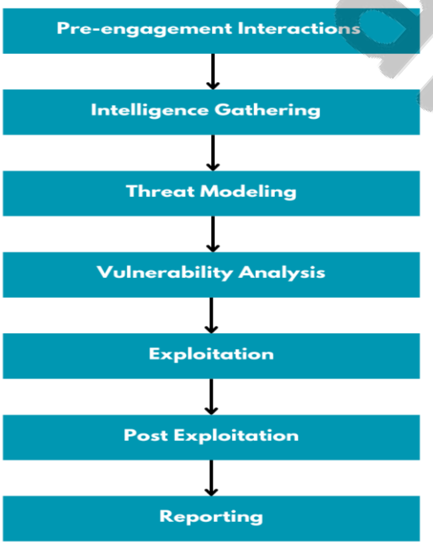


Fig. 1. Research methodology

A. *Pree-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.

B. *Intelligence Gathering*

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.

C. *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 recognised 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 ARP Entries on key network devices such as routers.

D. *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 Intrusion Detection/Prevention Systems (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 The Rogue Access Point attack in the form of 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 internet data access for users connected to the same network. This type of attack can be interpreted as ARP Spoofing / Poisoning.

E. Exploitation

a) Attacking The Infrastruktur

In this type of Attacking The Infrastructure attack, researchers conducted an Aireplay attack or deauthentication 5 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..

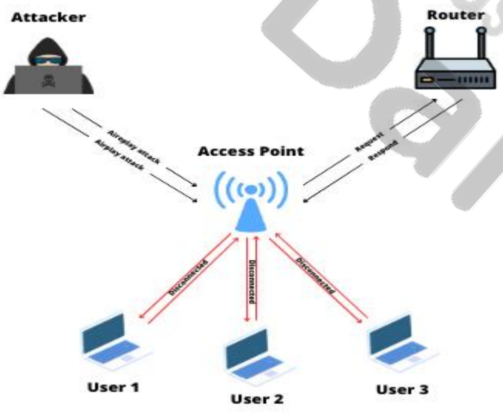
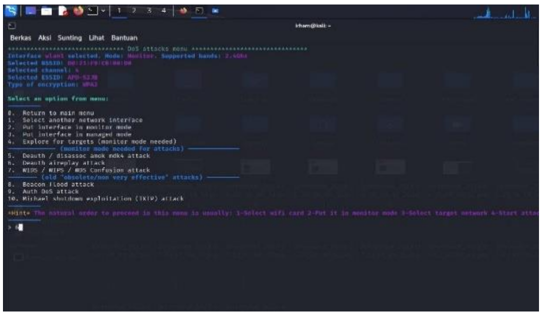


Fig. 2. Deauthentication Aireplay Attack overview

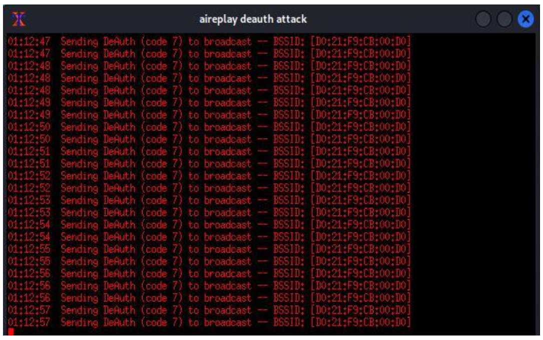
For the demonstration carried out in this attack, researchers used airgeddon (Fig. 3) and to find out whether this attack was successful or not, researchers used wireshark.



```
****************************** DoS attacks menu ******************************
Interface wlan1 selected. Mode: Monitor. Supported bands: 2.4Ghz
Selected BSSID: D0:21:F9:CB:00:D0
Selected channel: 4
Selected ESSID: APD-S2JB
Type of encryption: WPA2

Select an option from menu:
---------
0.  Return to main menu
1.  Select another network interface
2.  Put interface in monitor mode
3.  Put interface in managed mode
4.  Explore for targets (monitor mode needed)
------------- (monitor mode needed for attacks) -------------
5.  Deauth / disassoc amok mdk4 attack
6.  Deauth aireplay attack
7.  WIDS / WIPS / WDS Confusion attack
-------- (old "obsolete/non very effective" attacks) --------
8.  Beacon flood attack
9.  Auth DoS attack
10. Michael shutdown exploitation (TKIP) attack
---------
*Hint* The natural order to proceed in this menu is usually: 1-Select wifi card 2-Put it in monitor mode 3-Select target network 4-Start attac
---------
> 6
```

Fig. 3. Aireplay Deauthentication Command Attack

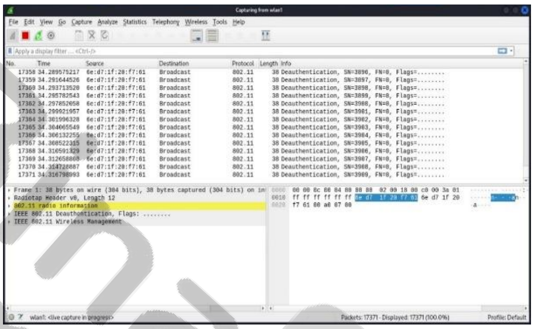
In this display, the researcher typed the number 6 command to start the deauth aireplay attack on the wireless network at PT PLN UP2D S2JB.



```
01:12:47  Sending DeAuth (code 7) to broadcast -- BSSID: [D0:21:F9:CB:00:D0]
01:12:47  Sending DeAuth (code 7) to broadcast -- BSSID: [D0:21:F9:CB:00:D0]
01:12:48  Sending DeAuth (code 7) to broadcast -- BSSID: [D0:21:F9:CB:00:D0]
01:12:48  Sending DeAuth (code 7) to broadcast -- BSSID: [D0:21:F9:CB:00:D0]
01:12:48  Sending DeAuth (code 7) to broadcast -- BSSID: [D0:21:F9:CB:00:D0]
01:12:49  Sending DeAuth (code 7) to broadcast -- BSSID: [D0:21:F9:CB:00:D0]
01:12:49  Sending DeAuth (code 7) to broadcast -- BSSID: [D0:21:F9:CB:00:D0]
01:12:50  Sending DeAuth (code 7) to broadcast -- BSSID: [D0:21:F9:CB:00:D0]
01:12:50  Sending DeAuth (code 7) to broadcast -- BSSID: [D0:21:F9:CB:00:D0]
01:12:51  Sending DeAuth (code 7) to broadcast -- BSSID: [D0:21:F9:CB:00:D0]
01:12:51  Sending DeAuth (code 7) to broadcast -- BSSID: [D0:21:F9:CB:00:D0]
01:12:52  Sending DeAuth (code 7) to broadcast -- BSSID: [D0:21:F9:CB:00:D0]
01:12:52  Sending DeAuth (code 7) to broadcast -- BSSID: [D0:21:F9:CB:00:D0]
01:12:53  Sending DeAuth (code 7) to broadcast -- BSSID: [D0:21:F9:CB:00:D0]
01:12:53  Sending DeAuth (code 7) to broadcast -- BSSID: [D0:21:F9:CB:00:D0]
01:12:54  Sending DeAuth (code 7) to broadcast -- BSSID: [D0:21:F9:CB:00:D0]
01:12:54  Sending DeAuth (code 7) to broadcast -- BSSID: [D0:21:F9:CB:00:D0]
01:12:55  Sending DeAuth (code 7) to broadcast -- BSSID: [D0:21:F9:CB:00:D0]
01:12:55  Sending DeAuth (code 7) to broadcast -- BSSID: [D0:21:F9:CB:00:D0]
01:12:56  Sending DeAuth (code 7) to broadcast -- BSSID: [D0:21:F9:CB:00:D0]
01:12:56  Sending DeAuth (code 7) to broadcast -- BSSID: [D0:21:F9:CB:00:D0]
01:12:56  Sending DeAuth (code 7) to broadcast -- BSSID: [D0:21:F9:CB:00:D0]
01:12:57  Sending DeAuth (code 7) to broadcast -- BSSID: [D0:21:F9:CB:00:D0]
01:12:57  Sending DeAuth (code 7) to broadcast -- BSSID: [D0:21:F9:CB:00:D0]
```

Fig. 4. Deauthentication Aireplay Attack

In (Fig. 4) researchers have launched a deauthentication attack with airgeddon, to be able to prove whether this attack was successful or not, researchers used wireshark.


Capturing from wlan1
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
wlan1: <live capture in progress>
Packets: 17371 · Displayed: 17371 (100.0%)
Profile: Default

```
No.   Time          Source             Destination  Protocol  Length Info
17358 34.289575217  6e:d7:1f:20:f7:61  Broadcast    802.11    38 Deauthentication, SN=3896, FN=0, Flags=........
17359 34.291644526  6e:d7:1f:20:f7:61  Broadcast    802.11    38 Deauthentication, SN=3897, FN=0, Flags=........
17360 34.293713520  6e:d7:1f:20:f7:61  Broadcast    802.11    38 Deauthentication, SN=3898, FN=0, Flags=........
17361 34.295782543  6e:d7:1f:20:f7:61  Broadcast    802.11    38 Deauthentication, SN=3899, FN=0, Flags=........
17362 34.297852058  6e:d7:1f:20:f7:61  Broadcast    802.11    38 Deauthentication, SN=3900, FN=0, Flags=........
17363 34.299921957  6e:d7:1f:20:f7:61  Broadcast    802.11    38 Deauthentication, SN=3901, FN=0, Flags=........
17364 34.301996328  6e:d7:1f:20:f7:61  Broadcast    802.11    38 Deauthentication, SN=3902, FN=0, Flags=........
17365 34.304065549  6e:d7:1f:20:f7:61  Broadcast    802.11    38 Deauthentication, SN=3903, FN=0, Flags=........
17366 34.306132255  6e:d7:1f:20:f7:61  Broadcast    802.11    38 Deauthentication, SN=3904, FN=0, Flags=........
17367 34.308522315  6e:d7:1f:20:f7:61  Broadcast    802.11    38 Deauthentication, SN=3905, FN=0, Flags=........
17368 34.310591329  6e:d7:1f:20:f7:61  Broadcast    802.11    38 Deauthentication, SN=3906, FN=0, Flags=........
17369 34.312658808  6e:d7:1f:20:f7:61  Broadcast    802.11    38 Deauthentication, SN=3907, FN=0, Flags=........
17370 34.314728887  6e:d7:1f:20:f7:61  Broadcast    802.11    38 Deauthentication, SN=3908, FN=0, Flags=........
17371 34.316798993  6e:d7:1f:20:f7:61  Broadcast    802.11    38 Deauthentication, SN=3909, FN=0, Flags=........

> Frame 1: 38 bytes on wire (304 bits), 38 bytes captured (304 bits) on in     0000  00 00 0c 00 04 80 00 00  02 00 18 00 c0 00 3a 01
> Radiotap Header v0, Length 12                                               0010  ff ff ff ff ff ff 6e d7  1f 20 f7 61 6e d7 1f 20
> 802.11 radio information                                                    0020  f7 61 00 a0 07 00
> IEEE 802.11 Deauthentication, Flags: ........
> IEEE 802.11 Wireless Management
```

Fig. 5. *Deauthentication* pada *wireshark*

It can be seen in (Fig. 5) that the researcher successfully performed deauthentication, where the impact of this attack can disconnect all users connected to the network.

b) The Rogue Access Point

In this type of attack The Rogue Access Point was tested 5 times. This type of attack tries to deceive connected network users by creating a fake or unauthorised access point that looks like a legitimate original network and this attack is also carried out in conjunction with deauthentication which aims to disconnect all users connected to the network, so that the user is forced to enter this fake network, When the user tries 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 whether there are vulnerabilities from the user side that can be exploited by researchers.

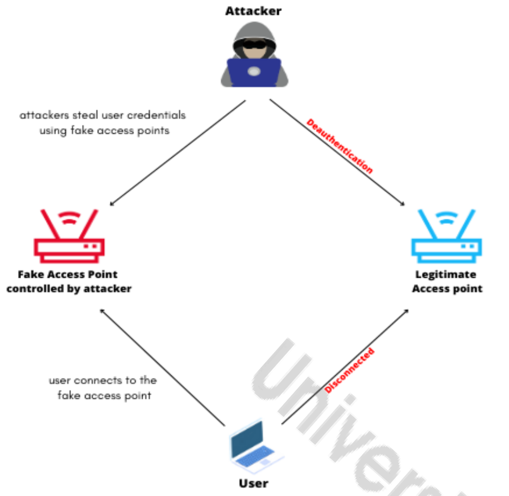

Attacker
attackers steal user credentials using fake access points
Deauthentication
Fake Access Point controlled by attacker
Legitimate Access point
user connects to the fake access point
Disconnected
User

Fig. 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 the captive portal airgeddon.

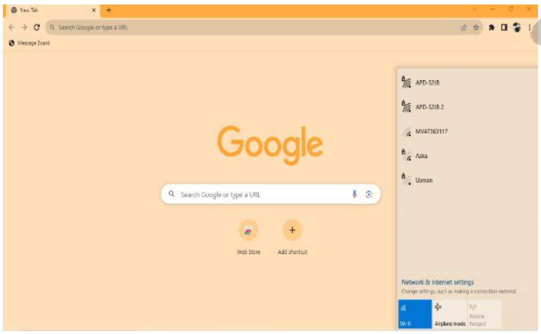
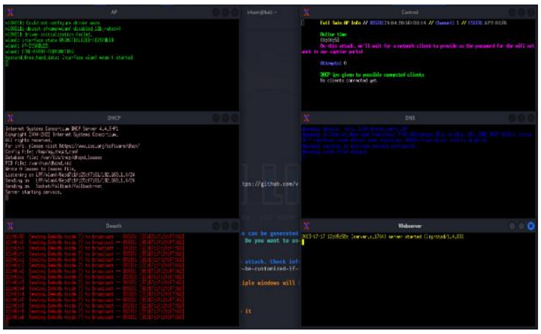

New Tab
Search Google or type a URL
Message Board
Google
Search Google or type a URL
Web Store
Add shortcut
APD-S2JB
APD-S2JB 2
MV47363117
Azka
Usman
Network & Internet settings
Change settings, such as making a connection metered.
Wi-Fi
Airplane mode
Mobile hotspot

Fig. 7. Authorised and unauthorised access points

In (Fig. 7) is a fake access point that has been successfully created by researchers that resembles the original access point with SSID APD-S2JB 2.

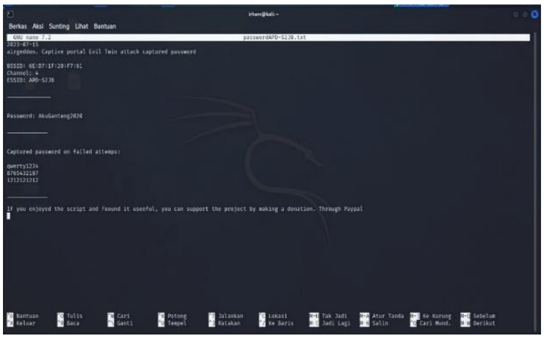


```
Internet Systems Consortium DHCP Server 4.4.3-P1
Copyright 2004-2022 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
[illegible]
Server starting service.
```

```
Evil Twin AP Info // [illegible] // Channel: 1 // ESSID: APD-S2JB
Online time
00:00:53
On this attack, we'll wait for a network client to provide us the password for the wifi network in our captive portal
Attempts: 0
DHCP ips given to possible connected clients
No clients connected yet
```

Fig. 8. Captive portal with airgeddon

In (Fig. 8) we can see the display of the captive portal with airgeddon displaying AP (Access point), DHCP, Deauth, Control, DNS, Web server. If there is one user who wants to connect to this fake access point, all user activities can be seen on this display.



```
  GNU nano 7.2                         passwordAPD-S2JB.txt
2023-07-15
airgeddon. Captive portal Evil Twin attack captured password

BSSID: 6E:D7:1F:20:F7:6L
Channel: 4
ESSID: APD-S2JB

___________

Password: AkuGanteng2020

___________

Captured password on failed attemps:

qwerty1234
8765432187
1212121212

___________

If you enjoyed the script and foound it useeful, you can support the project by making a donation. Through Paypal
```

Fig. 9. Capturing login credentials with txt file

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

c) *Arp Spoofing*

Pada jenis serangan yang terakhir ini, peneliti melakukan serangan yang berupa Arp Spoofing yang dilakukan pengujian sebanyak 5 kali. Arp Spoofing (Address Resolution Protocol Spoofing) merupakan jenis serangan yang bertujuan untuk mengatur lalu lintas jaringan wireless dan memanipulasi tabel ARP (Address Resolution Protocol) pada perangkat dalam sistem jaringan. Serangan ini dapat dikatakan bahwa Attacker berada ditengah – tengah antara user dan jaringan, sehingga data lalu lintas jaringan dapat dikendalikan

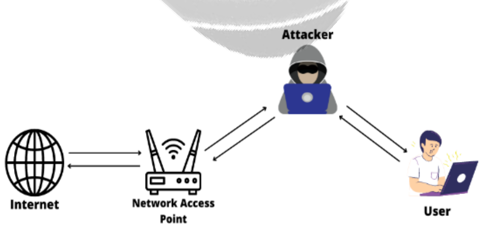
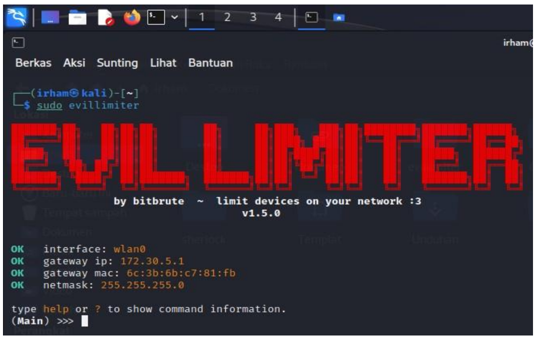


Fig. 10. Overview of Arp Spoofing attack

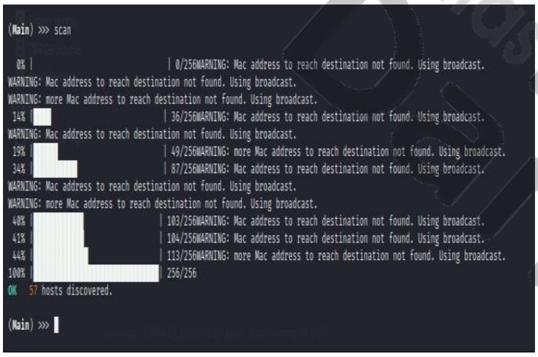
In this last type of attack, researchers conducted an attack in the form of Arp Spoofing which was tested 5 times. Arp Spoofing (Address Resolution Protocol Spoofing) is a type of attack that aims to manage wireless network traffic and manipulate the ARP (Address Resolution Protocol) table on devices in the network system. 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.



```
┌──(irham㉿kali)-[~]
└─$ sudo evillimiter

EVIL LIMITER

          by bitbrute  ~  limit devices on your network :3
                              v1.5.0

OK   interface: wlan0
OK   gateway ip: 172.30.5.1
OK   gateway mac: 6c:3b:6b:c7:81:fb
OK   netmask: 255.255.255.0

type help or ? to show command information.
(Main) >>> █
```

Fig. 11. Initial view of Evil Limiter

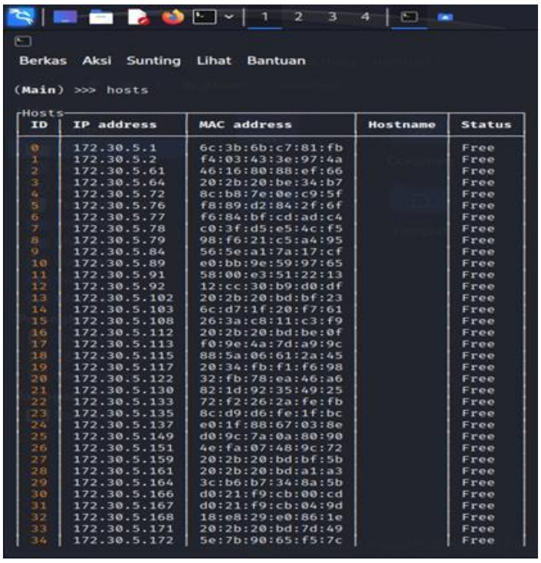
Furthermore, to be able to find out all users connected in the same network, the researcher conducted scanning, namely, in the form of broadcasting on the network system (Fig. 12), the purpose of this broadcasting is to send data to connected users, in order to find out all the hosts on the network.



```
(Main) >>> scan

  0% |                          | 0/256WARNING: Mac address to reach destination not found. Using broadcast.
WARNING: Mac address to reach destination not found. Using broadcast.
WARNING: more Mac address to reach destination not found. Using broadcast.
 14% |███                       | 36/256WARNING: Mac address to reach destination not found. Using broadcast.
WARNING: Mac address to reach destination not found. Using broadcast.
 19% |████                      | 49/256WARNING: more Mac address to reach destination not found. Using broadcast.
 34% |████████                  | 87/256WARNING: Mac address to reach destination not found. Using broadcast.
WARNING: Mac address to reach destination not found. Using broadcast.
WARNING: more Mac address to reach destination not found. Using broadcast.
 40% |██████████                | 103/256WARNING: Mac address to reach destination not found. Using broadcast.
 41% |██████████                | 104/256WARNING: Mac address to reach destination not found. Using broadcast.
 44% |███████████               | 113/256WARNING: more Mac address to reach destination not found. Using broadcast.
100% |██████████████████████████| 256/256
OK   57 hosts discovered.

(Main) >>> █
```

Fig. 12. Scanning with Evil Limiter

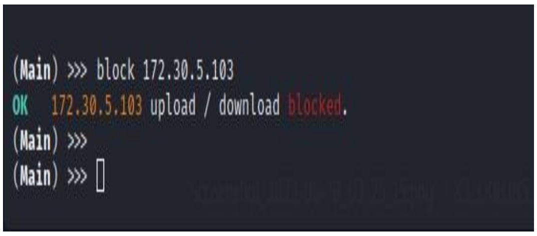
After scanning the network, researchers can find out the Arp table which contains all users connected to the same network,



```
(Main) >>> hosts

┌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  │          │ Free   │
│ 15 │ 172.30.5.108   │ 26:3a:c8:11:c3:f9  │          │ Free   │
│ 16 │ 172.30.5.112   │ 20:2b:20:bd:be:0f  │          │ Free   │
│ 17 │ 172.30.5.113   │ f0:9e:4a:7d:a9:9c  │          │ Free   │
│ 18 │ 172.30.5.115   │ 88:5a:06:61:2a:45  │          │ Free   │
│ 19 │ 172.30.5.117   │ 20:34:fb:f1:f6:98  │          │ Free   │
│ 20 │ 172.30.5.122   │ 32:fb:78:ea:46:a6  │          │ Free   │
│ 21 │ 172.30.5.130   │ 82:1d:92:35:49:25  │          │ Free   │
│ 22 │ 172.30.5.133   │ 72:f2:26:2a:fe:fb  │          │ Free   │
│ 23 │ 172.30.5.135   │ 8c:d9:d6:fe:1f:bc  │          │ Free   │
│ 24 │ 172.30.5.137   │ e0:1f:88:67:03:8e  │          │ Free   │
│ 25 │ 172.30.5.149   │ d0:9c:7a:0a:80:90  │          │ Free   │
│ 26 │ 172.30.5.151   │ 4e:fa:07:48:9c:72  │          │ Free   │
│ 27 │ 172.30.5.159   │ 20:2b:20:bd:bf:5b  │          │ Free   │
│ 28 │ 172.30.5.161   │ 20:2b:20:bd:a1:a3  │          │ Free   │
│ 29 │ 172.30.5.164   │ 3c:b6:b7:34:8a:5b  │          │ Free   │
│ 30 │ 172.30.5.166   │ d0:21:f9:cb:00:cd  │          │ Free   │
│ 31 │ 172.30.5.167   │ d0:21:f9:cb:04:9d  │          │ Free   │
│ 32 │ 172.30.5.168   │ 18:e8:29:e0:86:1e  │          │ Free   │
│ 33 │ 172.30.5.171   │ 20:2b:20:bd:7d:49  │          │ Free   │
│ 34 │ 172.30.5.172   │ 5e:7b:90:65:f5:7c  │          │ Free   │
```

Fig. 13. All users connected to the network

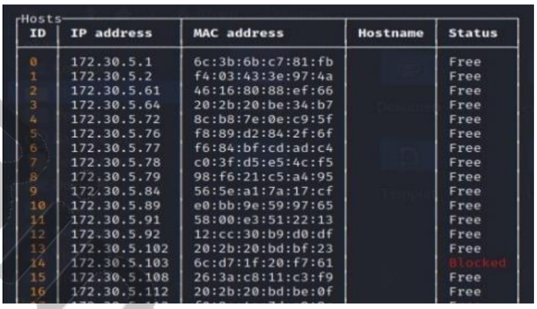
In (Fig. 13) it can be seen that there are IP addresses and MAC addresses of all users connected to the network, then researchers block data access to one of the connected users in testing the security of the network system. By typing the command block [IP user] then Enter on the keyboard.



```
(Main) >>> block 172.30.5.103
OK   172.30.5.103 upload / download blocked.
(Main) >>>
(Main) >>> █
```

Fig. 14. Blocking data access on one of the users

Next, to see if the user has been successfully blocked from accessing data, go back to the hosts in Evil Limiter which will display the Arp table on the network again.



```
┌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    │
```

Fig. 15. User data access successfully blocked

Then, here it can be seen that researchers succeeded in carrying out a 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.

III. RESULT

A. *Reporting*

Based on table 3.1 is the delivery of the results of penetration testing conducted by researchers using the PTES (Penetration Testing Execution Standards) method on the wireless network of the PT PLN UP2D S2JB office.

Table 3. Penetration Testing result

type of attack	Tools	Required data	Test limitations	Testing Results	Status
Attacking The Infrastructure	Airgeddon	WLAN Network SSID	Disconnecting users connected to the WLAN network with Deauthentication	Successful Successfull Successfull Successfull Successfull	Low
The Rogue Access Point	Airgeddon	WLAN Netwo	Cloning the SSID of the WLAN network so	Failed Failed	Medium

		rk SSID	that it resembles the original network Knowing login credentials on a WLAN network	Successfull Successfull Successfull	
Arp Spoofing	Evil Limiter	Attacker must be connected to the WLAN network Users connected to the WLAN network	Block data access of users connected to the WLAN network	Successful Successfull Successfull Successfull Successfull	Low

Based on (table. 3) can be explained as follows;

a) Attacking The Infrastruktur

In this type of attack, researchers succeeded in carrying out Aireplay-ng attacks 5 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 pentesters or attackers in penetration testing on wireless networks.

b) The Rogue Access Point

In this type of attack, researchers managed to attack the rogue access point 3 times in 5 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.

c) Arp Spoofing

In this last type of attack, researchers also managed to do it 5 times. This type of attack is difficult to detect and is also very dangerous because it can cut off user data access so that 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.

B. 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).

Table 4. Improved network security and anticipated attacks

Improved	**Description**
Firewall Configuration	Enable firewall features in the form of Intrusion Detection/Prevention Systems (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 wifi) 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

IV. CONCLUSSION

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. 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 that there is a vulnerability and has not implemented Intrusion Detection / Prevention Systems (IDS / IPS) on the network security system of the PT PLN UP2D S2JB office. The Rogue Access Point type of attack 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 that there are gaps on the user side that can be exploited by attackers. The type of Arp Spoofing attack 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 that there is a vulnerability gap on the sis. Network security evaluation using the Penetration Testing Execution Standards (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 fifteen tests conducted, only three of which 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 gaps.

REFERENCES

[1] D. He, X. Li, S. Chan, J. Gao, and M. Guizani, “Security Analysis of a Space-Based Wireless Network,” *IEEE Netw.*, vol. 33, no. 1, pp. 36–43, 2019, doi: 10.1109/MNET.2018.1800194.

[2] and N. A.-S. A. Barznji, T. Rashid, “Computer Network Simulation of Firewall andVoIP Performance Monitoring,” *Int. J. Online Biomed. Eng.*, vol. 14, no. 9, pp. 4–18, 2018, doi: https://doi.org/10.3991/ijoe.v14i09.8508.

[3] B. Adhi Prakosa, “Security Analysis of Wireless Local Area Network (WLAN) Network with the Penetration Testing Method,” *J. Mantik*, vol. 4, no. 3, pp. 1658–1662, 2020, [Online]. Available: https://iocscience.org/ejournal/index.php/mantik

[4] 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.

[5] E. Wahyudi, E. T. Luthfi, and M. M. Efendi, “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,” *J. Explor. STMIK Mataram*, vol. 9, no. 1, pp. 1–7, 2019.

[6] 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.

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

[8] 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.

[9] A. M. Patel and H. R. Patel, “WiSPNET 2023 - International Conference on Wireless Communications, Signal Processing and Networking,” *WiSPNET 2023 - Int. Conf. Wirel. Commun. Signal Process. Netw.*, pp. 131–134, 2023.

[10] T. Radivilova, L. Kirichenko, D. Ageiev, and V. Bulakh, “Classification methods of machine learning to detect DDoS attacks,” *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.

[11] 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.

[12] H. J. Lu and Y. Yu, “Research on WiFi Penetration Testing with Kali Linux,” *Complexity*, vol. 2021, 2021, doi: 10.1155/2021/5570001.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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,” *Proc. - 2020 12th Annu. Undergrad. Res. Conf. Appl. Comput. URC 2020*, pp. 8–11, 2020, doi: 10.1109/URC49805.2020.9099187.

[18] M. A. Abo-Soliman, “Enterprise WLAN security flaws current attacks and relative mitigations,” *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] 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.

[21] D. Overstreet, H. Wimmer, and R. J. Haddad, “Penetration Testing of the Amazon Echo Digital Voice Assistant Using a Denial-of-Service Attack,” *Conf. Proc. - IEEE SOUTHEASTCON*, vol. 2019-April, 2019, doi: 10.1109/SoutheastCon42311.2019.9020329.

[22] 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.

[23] Y. Khera, D. Kumar, S. Sujay, and N. Garg, “Analysis and Impact of Vulnerability Assessment and Penetration Testing,” *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.

[24] R. Hou, G. Ren, C. Zhou, H. Yue, H. Liu, and J. Liu, “Analysis and research on network security and privacy security in ubiquitous electricity Internet of Things,” *Comput. Commun.*, vol. 158, no. February, pp. 64–72, 2020, doi: 10.1016/j.comcom.2020.04.019.

[25] I. Shadeed Al-Mejibli and D. N. Rasheed 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.

[27] 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.