WIRELESS NETWORK SECURITY ANALYSIS WITH METHOD PENETRATION TESTING EXECUTION STANDARD (PTES) IN WEST JAVA PROVINCIAL HEALTH OFFICE

Adi Adrian[1], Angga Setiyadi[2]

[1,2] *Indonesia Computer University*
Jl. Dipatiukur No. 112-116, Bandung 40132
E-mail : adiadrian346@gmail.com[1], angga.setiyadi@gmail.com[2]

ABSTRACT

West Java Provincial Health Office is one of the service that is on West Java Provincial. Application wired Network LAN not comprehensive on every floor result 60 percent computer West Java Provincial Health Office using wireless network. Wireless networks have more weaknesses compared to wired networks [15]. as in the interview with Mr Agung Aditia as Communication Technology Division. That West Java Provincial Health Office often such disturbances flooding, illegal access. Therefore West Java Provincial Health Office requires analysis and auditing of network security systems in order to ensure that West Java Provincial Health Office both in terms of network security systems, especially wireless networks. Communication Technology Division in doing analysis and audit requires a tool which would become a standard in analyzing network security systems West Java Provincial Health Office. Therefore required a standard tool in the analysis by using Penetration Testing Execution Standard which is one of the tools developed by pentest organitation to be standard in analyzing or auditing network security systems in a company in this case is to analyze and audit wireless network security system West Java Provincial Health Office. The results of tests that have been done among others, sniffing, scanning port, scanning wireless, bruteforce. Then it can be concluded that the wireless network security system West Java Provincial Health Office still very vulnerable to attack.

Keyword: *sniffing, scanning port, scanning wireless, bruteforce, Penetration Testing Execution Standard*

1. *OPENING*

West Java Health Office is one agency that was in West Java province. West Java Health Office currently has 3 floors, 1st floor has 4 rooms, 2nd floor has 8 room, 3rd floor has 4 rooms. Each floor has 2 access point as a wireless network that encompassed the entire room on each floor. The application of network LAN cable has not been thoroughly on each floor resulted in 60 percent of computer health Office of West Java to use the wireless network.

A wireless network that is used to meet the needs of the network form of wireless devices 6 to cover the whole floor in West Java Health Office. Wireless devices using different security include 4 device open (open), and two of the device with a security type of WPA2-PSK. The use of the dominant wireless has a threat of attack on a network that is more vulnerable than the use of the LAN network. It forces the Division ICT to do more penganalisaan against the existing wireless network in West Java Health Office.

Wifi networks have more flaws than with cable network [15]. as in the interview with Mr. Agung Aditia as Division of information technology communication. West Java Health Office that often occur as DOS flooding, illegal access. that same year, in December, January, and February of the year 2017 has been going on the attack against DOS flooding of wifi devices imposes 12 PC and resulted in twelve of these PC cannot access the internet, as well as Provincial Health Office West Java has four open wifi and anyone may access that device. Hence health service needs analysis and audit network security system in order to ensure that the Health Office of West Java province both in terms of its network security system especially wireless network.

Division of information technology Communication in doing analysis and auditing need a tools that will become a standard in analyzing network security system of the province of West Java Health Office. Therefore it takes a standard tools in the analysis using Penetration Testing Execution Standard which is one of the tools developed by pentest organitation to become standard in analyzing or auditing the system network security at a company in this case namely menganalsis and

audit network security system wireless Health Office of West Java province.

1.1 *Mean*

The intention of this research is to analyze the network security system of the province of West Java Health Office using standard penetration testing method of execution, in order for the Division of information technology Communication knowing whether or not the security system wireless network in West Java Health Office.

1.2 The Purpose Of

Tujuan Penelitian ini adalah untuk menginplementasikan metode penetrarion testing execution standard sebagai bahan analisis dan audit sistem keamanan jaringan di Dinas Kesehatan Provinsi Jawa Barat.

1.3 Reaserch Method

As for the method of Research is done to conduct analysis using wireless network security system penetration testing standard execution can be seen in Figure 1.



Figure 1. *Penetration testing execution standard*

A description of the stages of penetration testing standard execution method is as follows:

1. *Pre-engagement*

   Pre-engagement is the stage where a pentester describes activities that will dilakikan to pentest targets (company).

2. *Intelligence Gathering*

   Intelligence gathering is a stage where a pentester trying to collect all the information about the target (the company) which can be obtained with different methods and various media. Intelligence gathering on this research focuses on wireless network.

3. *Threart Modeling*

   Threart Modeling is the definition of the approach to threat modeling. Threat Modeling is required for the implementation of a true penetration testing. Modeling approach that question is the observation of the target that aims to find out the target business processes to be more easily in a decisive attack.

4. *Vulnerability Analysis*

   Vulnerability Analysis the stage is where to find security gaps based on information that has been obtained in advance. Vulnerability analysis aims to find flaws in the system of networks that can be dimaanfaatkan by pentester.

5. *Exploitation*

   Expolition is a stage where the pentester seorangan attack on the target. Although this stage is mostly done with the brute force method without having a unsut precision. A person will only do pentester exploitation when she already knows for sure whether the attack was successful or not, but of course there is the possibility of unexpected in the security systems of the target. However, before an attack, pentester should know if the target has a security loophole that could be in use. An attack in blindly and hope the success is not a productive method. Seorangan pentester always perfecting his analysis first before doing an effective attack.

6. *Post-Exploitation*

   Post Exploitation is a stage where the pentester to the seorangan system of the target tissue and then do an analysis of your existing infrastructure. At this stage a pentester learn the parts in the system and determine the most critical for the target (the company). Here a pentester should be able to connect all parts of the system that is there to explain the impact of the attack or the most massive losses that could be terjasi on the target (the company).

7. *Reporting*

   Reporting are the most important activities in a pentest. A pentester using report (the report) to expound on the company about pentesting performed such as: what to do, how to do it, the risks that could happen and the main thing is how to fix his system.

2. LITERATURE REVIEW

2.1 *Computer Network*

The computer network is the set of "interconnections" between two or more autonomous computer connected with media tranmisi cable or wirelessly (wireless). When a computer can make another computer restart, shutdown, or perform other control, then the computers is not autonomous (not

control the other computers with full access) [1].

2.2 *The types of computer networks*

In general the network type kompter divided into two parts that is peer to peer and client server.

1. *Peer to peer*

Peer to peer is a type of computer network that has a system of work that the client could not be similarly server server cannot be a client.

2. *Client – server*

Client -server is a type of computer network that has a working system that is client and server can be a server can be a client instead.

2.3 LAN Network

Local Area Network (LAN) is a in the limit jarigan by small relative area, generally limited by the environmental area such as an office building, or a school, and are usually not far from around 1 square kilometres. some models usually a LAN configuration, one computer is usually made into a goes through the server, which is used to store software (Software which regulates the activities of the network), or as the software that can be used by computers linked into the local network.

Most use a LAN cable to connect the media between one computer with another computer. LAN is a communications network that is confined to a small area, e.g. a single building or group of buildings. [11]

2.4 WLAN Network

Wireless LAN or WLAN is a local area network that uses radio wave media. [7]

Wireless LAN here can be define as a flexible data communication system that can be used to replace or add to existing LAN network to provide additional functionality in the concept of computer networks in General. Functions on offer here may be due to the reliable connectivity with user mobility. [3]

WLAN network has the following advantages:

a. The cost of cheap

b. easy to develop

WLAN network also have the weakness in the form of :

a. Have a big Delay in the new data.

b. Often the signal is obstructed.

c. Data security less secure

2.5 *Network Security*

Network security is one of the important things in the monitor and prevent abuse of network resources that are not illegal and detrimental.Confidentiality

Confidentiality Is requires that information or data can only be accessed by parties that have the authority.

a. Intergrity

Intergrity that is, it requires that the information can only be changed by the parties who have

b. *Availability*

Availability Is requires that the information available to the parties who have authority when needed

c. Authentication

Authentication ie requires that the sender of an information can be diindentifikasi correctly and no guarantee that the identity that is obtained is not fake.

d. Nonrepudiation

Nonrepudiation is requires that either the sender or receiver of information cannot deny sending and receiving messages.

2.5 *TCP SYN Flood Denial of Service*

TCP SYN Flood Denial of Service attack is a Denial of Service by way of flooding the server with malicious request packages SYN with a fake source IP address. SYN packet is a packet from the client that initiated the formation of a TCP/IP connection, then the server will reply with a SYN-ACK packet, and is equipped with the SYN-ACK-ACK from the client, this process is called the three way handshake. The trick is on the fake source ip

Ficture 2. Penetration testing execution standard

address of the SYN packet packet client. The result of the server will also not get reply SYN-ACK-ACK from the client. But for every client who tries to open a connection, the server will allocate a resource such as memory and time to wait for the arrival of balsan ACK from the client. In this way the attacker spent resource server only to serve the attacker of fake requests.

2.6 *Port Scanning*

Port Scanning Is one way to collect information from the target. That is usually the information obtained in the form of any services provided, and other operating systems – so can determine the next attack

2.7 *Brute force*

Brute Force adalah metode untuk meretas password dengan cara mencoba semua kemungkinan kombinasi yang ada pada *wordlist*. Metode *brute force* dapat dilakukan secara *online* ataupun *offline* yang menjadi kelemahan pada metode ini adalah waktu pengerjaannya yang cukup lama karna akan mencoba satu persatu *password* yang berada pada *wordlist*.

No	Pertanyaan
1	Mengapa harus diadakanya tes penetrasi pada jaringan di Dinas Kesehatan Jawa Barat?
2	Kapan Divisi TIK menginginkan uji penetrasi keamanan ? (Saat jam kantor, Setelah jam kantor, Saat akhir pekan)
4	Berapa banyak alamat ip *internal* yang di ujikan?
5	Berapa banyak alamat ip *eksternal* yang diujikan?
6	Apakah ada perangkat terkena dampak hasil uji penetrasi, seperti (firewall, sistem deteksi, aplikasi firewall)?



2.8 Penetration Testing Standard

Penetration Testing Execution Standard consists of seven main sections. This includes all matters relating to the testing of pentrasi starting from the initial communication and reasoning behind the pentest, through information gathering phase and modeling threats where testers work behind the layer to get a deeper understanding of good about an organization that in trials, through the research of vulnerabilities, exploits and after exploitation. As can be seen in Figure 2

3. ANALYSIS AND TESTING

3.1 *Pre-engagement*

Pre-engagement is the stage where a pentester describes activities pentest would do to the company. As discussed at this stage these are questions.

a. Questions network pentration test

The question of network penetration test is one part of the pre-engagement. The question of network penetration test was created to assist in the interview process to make it easier to provide questions. The question of network penetration test can be seen in table 1.

Tabel 1. Pertanyaan *network pentration test*

b. Question wireless network penetration test

Wireless network penetration test question is a question that the prepare to search for information about the wireless network the target (the company). The question of network penetration test can be seen in table 2.

Tabel 2. Pertanyaan *wireless network penetration test*

No	Pertanyaan
1	Seberapa Banyak Perangkat *wireless* yang aktif di Dinas Kesehatan Jawa Barat ?
2	Apakah *wireless* dapat di akses oleh orang luar, tanpa harus menggunakan hak akses ?
3	Apa jenis keamanan yang digunakan perangkat *wireless* Dinas Kesehatan Provinsi Jawa Barat ?
4	Apakah ada yang pernah mencoba menyerang melalui jaringan *wireless* Dinas Kesehatan Provinsi Jawa Barat?
5	Berapa banyak *user* yang menggunakan jaringan *wireless* di Dinas Kesehatan Jawa Barat?

c. Question physical penetration test

The question physical penetration test have the same usability questions other questions to assist in the collection of information. The question physical penetration test contains about cangkupan research. The question physical penetration test can be seen in table 3.

Tabel 3. Pertanyaan *physical penetration test*

No	Pertanyaan
1	Berapa Lantai yang akan menjadi cangkupan pengujian?
2	Lantai mana saja yang masuk dalam cangkupan pengujian ?

3	Apakah Dinas Kesehatan Provinsi Jawa Barat memiliki *standard operating procedure* (S.O.P) dalam akses, perawatan, dan penanganan jaringan ?
4	Apakah ada berita acara atau dokumentasi tentang keamanan jaringan ?
5	Apakah terdapat kamera *cctv* di Dinas Kesehatan Provinsi Jawa Barat ?

d. Question the system administrator

Question the system administrator is a question that contains about questions that aimed to find out about the system administrator on the target. System administrator questions can be seen in table 4.

Tabel 4. Pertanyaan *administator* sistem

No	Pertanyaan
1	Apakah sistem operasi selalu *update?*
2	Apakah ada perangkat lunak pemantauan sistem?
3	Apakah *Backup* data *server* dilakukan secara teratur ?
4	Kapan terkhir *Restore Backup* data *server* ?

3.2 *intelligence gathering*

Interlligence Gathering is the stage where a pentester trying to gather as much information about the target company can be obtained with different methods and various media. As for the plot owned by intelligence gathering can be seen in Figure 3.

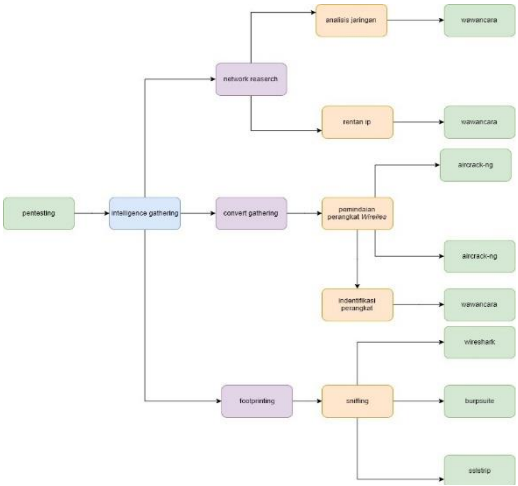


Figure 3. Alur *intelligence gathering*

a. Convert Gatehring

Covert Gathering or is the reconnaissance activities on standard penetration testing methods of execution. reconnaissance aim to know the target (Corporation). Here is a plot of convert gathering can be seen in Figure 4.

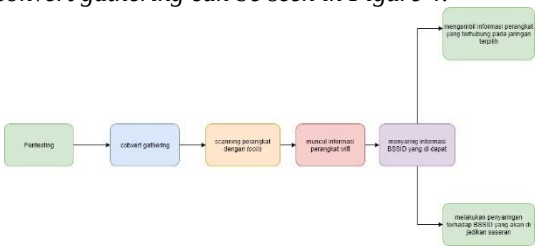


Figure 4. Alur *convert gathering*

b. Footprinting

Footpriting is the information gathering phase consists of the interaction with the target to obtain information by means of test targets. Footpinting testing done in internal footprinting. Footprinting have grooves that can be seen in Figure 5.



Figure 5. Alur *footprinting*

3.2 *Vulnerability Analisys*

Vulnerability Analis is the stage is where to find security gaps based on information that has been obtained in advance. Vulnerability analysis aims to find flaws in network system that can be exploited by an attacker. As for the flow of vulnerability can be seen in Figure 6.

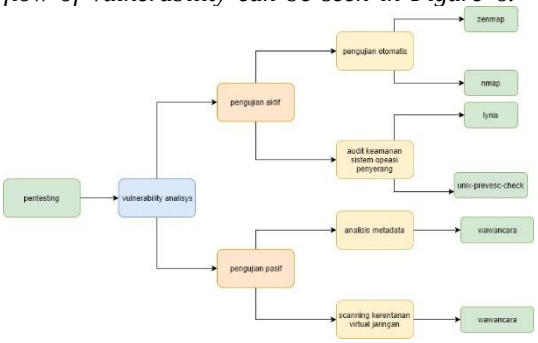


Figure 6. Alur *vulnerability analisis*

4. Implementation and Discussion

4.1 *Explotation*

Exploitation is a stage where the pentester memanpaatkan crack search results obtained from previous information. In other words the exploitation are attacks against the target after

getting information from the target. As for the flow of exploitation can be seen in Figure 7.

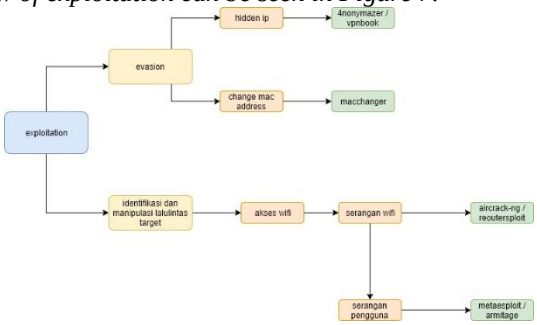


Figure 7. Alur *exploitation*

a. *Evasion*

In doing the penetration should always hide the pentester identity while experimenting to avoid detection is done by the system. then the evasion is a technique to avoid the possibility of a detected attack.

1. **Change the Ipaddress pentester with vpn tools books**

The IP address used by the pentester was 192.168.0.101. Here is a picture of penggilan information pentester interface. Can be seen in Figure 8.

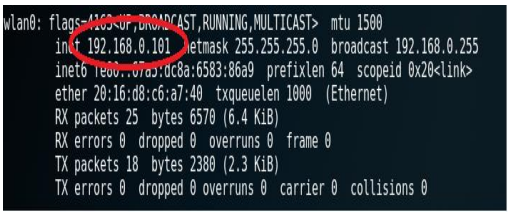


Figure 8. Tampilan *ifconfig*

1. **Meng*install vpnbook***

Langkah untuk menginstall vpnbook dengan menuliskan perintah "*openvpn vpnbook -us2-tcp443.ovpn"* pada terminal *linux* Berikut adalah tampilan dari menginstall vpnbook dapat dilihat pada gambar 9.

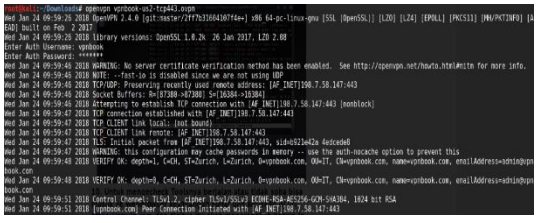


Figure 9. Menginstall vpnbook

2. *Proof ipaddress has been revamped*

To prove that the ipaddress has successfully changed then proved by checking IPS and the region with the following https://cmyip.com site is display ip yan has changed can be seen in Figure 10.



Figure 10. Pembuktian perubahan *ipaddress*

3. *Brute force*

Brute force is a technique to do login by trying everything possible and kominasi from username and passowrd to found the correct combination. As for the plot on brute force can be seen in Figure 11.

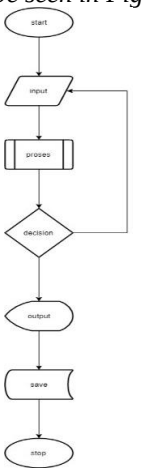


Figure 11. Alur *brute force*

1. *Enable mode montoring interface wlan0*

Tools to use aircrack-ng is required to enable monitoring mode on wlan0 interface using the command "airmon-ng start wlan0". Following is the display of the monitoring

mode can be seen in Figure 12.

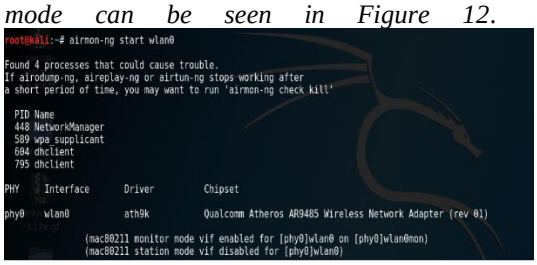


Figure 12. mode monitoring interface wlan0

2. Commands are airodump-ng wlan0mon at the console is used for wireless scanning. Following are the results from the output screen type wlan0mon airodump-ng command can be seen in Figure 13.

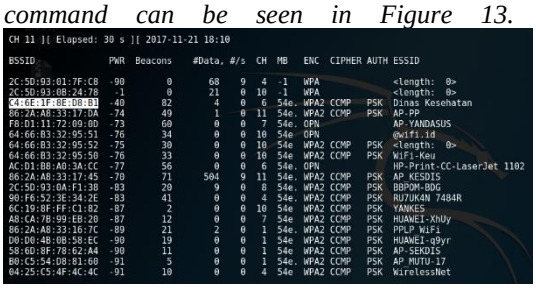


Figure 13. Tampilan hasil dari perintah *airodump-ng wlan0mon*

3. . Command airodump-ng – bssid C4:6E: IF: D8: B1-c 6-w/root/Dekstop/ujicoba2 wlan0mon used to connect or handshake interface device with wireless pentester target. Following is the display of the device handshake. Can be seen in Figure 14.

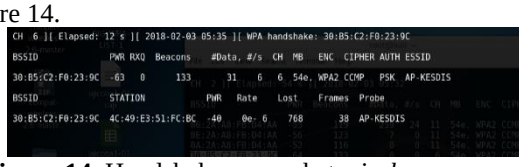


Figure 14. Handshake perangkat *wireless*

4. *Orders the aircrack-ng/root/Dekstop/ujicoba02-01.cap-w/root/Dekstop/WD.lst in use for mengload live and lst file aircrack-ng tools to do bruteforce the wireless devices on the target. Following is the display of aircrack can be seen* in Figure 15.

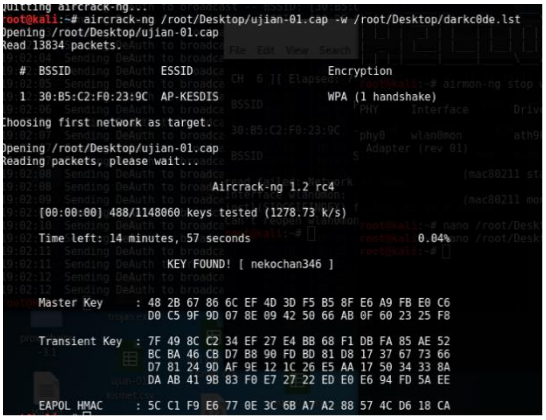


Figure 15. Tampilan aircrack

4.2 *Reporting*

Reporting activities made after penetration testing was completed. The report describes the results and a discussion of each of the phases mentioned in the reports of penetration testing can be used as a basis for advising in this research.

5. Conclusion

Based on the results of the health service in the pentest description of West Java has a lot of loopholes which should be noted by the Division of information technology Communications West Java Health Office because an awful lot of opportunity for anyone to attacking the weaknesses of network security system especially the security of a wireless network.

DAFTAR PUSTAKA

[1] M. Syafrizal, pengantar jaringan komputer, Yogyakarta: Penerbit Andi, 2005.

[2] Admin, "Sejarah," 05 Juni 2014. [Online]. Available: http://www.diskes.jabarprov.go.id/index.php/pages/detail/2014/6. [Accessed 4 Maret 2017].

[3] A. Satria, "PENGEMBANGAN PERANGKAT WIRELESS IDS(INTRUSION DETECTION SYSTEM) BERBASIS EMBEDDED SYSTEM (STUDI KASUS : BADAN NARKOTIKA NASIONAL)," 2011.

[4] A. A. ,. E. Randy Mentang, "PERANCANGAN DAN ANALISIS KEAMANAN JARINGAN NIRKABEL MENGGUNAKAN WIRELESS INTRUSION DETECTION SYSTEM," vol. 5, 2015.

[5] Kairulanam, "SISTEM PENDETEKSI SERANGAN PADA JARINGAN KOMPUTER MENGGUNAKAN SNORT BERBASIS SMS GATEWAY (STUDI KASUS DI TAMAN PINTAR YOGYAKARTA)," 2011.

[6] S. Surianto Rustan, mendisain logo, jakarta: Gramedia Pustaka utama, 2009.

[7] W. Komputer, SPP MENGINSTALASI PERANGKAT JARINGAN KOMPUTER, JAKARTA: PT Elex Media Komputindo, 2006.

[8] D. Ariyus, PENGANTAR ILMU KRIPTOGRAFI Teori, Analisis, dan Implementasi, Yogyakarta: ANDI OFFSET, 2008.

[9] M. D. S. M. T. A. S. Agung baitul Hikmah, CARA CEPAT MEMBANGUN WEBSITE DARI NOL STUDI KASUS WEB DEALER MOTOR, Yogyakarta: Andi OFFSET, 2015.

[10] T. A. Prabawati, TUTORIAL 5 HARI : BELAJAR HACKING DARI NOL, Yogyakarta: CV. ANDI OFFSET, 2010.

[11] B. Irawan, JARINGAN KOMPUTER, YOGYAKARTA: GRAHA ILMU, 2005.

[12] M. Dony Ariyus, INTRUSION DETECTION SYSTEM sistem pendeteksi penyusup pada jaringan komputer, Yogyakarta: CV.ANDI OFFSET, 2007.

[13] H. Alffata, ANALIS & PERANCANGAN SISTEM INFORMASI untuk keunggulan bersaing perusahaan & organisasi modren, Yogyakarta: CV.ANDI OFFSET, 2007.

[14] Z. A. Ricardo Luis Daloca, "NOVEL ALGORITHMS AND TECHNIQUES IN TELECOMMUNICATIONS AND NETWORKING," *an architecture for wireless intrusion detection system using artificial neural networks,* p. 357, 2010.

[15] A. A. A. D. Batara Sakti, "Uji Kelayakan Impletasi SSH sebagai pengaman FTP Server dengan Penetration testing," vol. 2, no. 1, pp. 1-8, 2013.

[16] A. Setiyadi, "Implementasi MITM pada Websploit sebagai Monitoring Aktifitas pengguna dalam Mengakses Internet," pp. 1-8, 2017.