Sinkron: Jurnal dan Penelitian Teknik Informatika
Volume 6, Number 1, January 2022
DOI : https://doi.org/10.33395/sinkron.v7i1.11249
e-ISSN : 2541-2019
p-ISSN : 2541-044X

# Analysis and Evaluation of Wireless Network Security with the Penetration Testing Execution Standard (PTES)

**Method Deuis Nur Astrida[1)*], Agung Restu Saputra[2)], Akhmad Ikhza Assaufi[3)]**
[1)2)3)]Amikom Purwokerto University, Indonesia
deuisnurastrida@email.com, [2)]agungrestusaputra@email.com, [3)]akhmadikhza@email.com

**Submitted** : Dec 20, 2021 | **Accepted** : Jan 8, 2022 | **Published** : Jan 13, 2022

**Abstract:** The use of computer networks in an agency aims to facilitate communication and data transfer between devices. The network that can be applied can be using wireless media or LAN cable. At SMP XYZ, most of the computers still use wireless networks. Based on the findings in the field, it was found that there was no user management problem. Therefore, an analysis and audit of the network security system is needed to ensure that the network security system at SMP XYZ is safe and running well. In conducting this analysis, a tool is needed which will be used as a benchmark to determine the security of the wireless network. The tools used are Penetration Testing Execution Standard (PTES) which is one of the tools to become a standard in analyzing or auditing network security systems in a company in this case, namely analyzing and auditing wireless network security systems. After conducting an analysis based on these tools, there are still many security holes in the XYZ wireless SMP that allow outsiders to illegally access and obtain vulnerabilities in terms of WPA2 cracking, DoS, wireless router password cracking, and access point isolation so that it can be said that network security at SMP XYZ is still not safe.

**Keywords:** Security, network, network security, Penetration Testing Execution Standard, PTES

## INTRODUCTION

The rapid development of technology is directly proportional to the development of the media used, including media that uses cables and wireless or what we usually call wireless. Wireless media has several advantages, including being easier and more flexible in its use. Along with the development of technology is also increasing crime in cyberspace. Even if we observe, the level of crime in cyberspace is getting more and more varied the motives used. For that we need a good network security to handle these problems.

SMP XYZ as one of the IT-based schools in Banyumas district, has used a wireless network to facilitate communication and data transfer. XYZ Junior High School has 3 floors where the 1st floor has 13 rooms, the 2nd floor has 11 rooms, and the 3rd floor has 4 rooms. Each floor has an access point as a wireless network that covers all rooms on each floor where the number of access points used is 17 units.

Existing wireless devices use WPA2-PSK security which has a weakness, namely the wifi password can be hacked. This dominant use of wireless also has a more vulnerable network attack threat than the use of a LAN network. In addition, user management has not yet been implemented, resulting in bandwidth leakage and allowing illegal access to occur.

In accordance with the problems that occurred above, the IT party from the school needs to do more analysis of the wireless network in SMP XYZ. In conducting analysis and audit of the network security, IT requires tools that will become a standard in conducting analysis. The tools to be used are Penetration Testing Execution Standard which is one of the tools developed by the pentest organization to become a standard in analyzing or auditing network security systems in a company in this case, namely analyzing and auditing wireless network security systems at SMP XYZ.

In previous studies using PTES to test sniffing, port scanning, wireless scanning, bruteforce on the West Java Provincial Health Office wireless network and concluded that the West Java Provincial Health Office's wireless network security system is still very vulnerable to attacks. (Adi, 2020)

*name of corresponding author

e-ISSN : 2541-2019
p-ISSN : 2541-044X

Yoel Novaliano, used PTES to conduct research on network security on public internet services on Klik Pratama Bhakti Medika and the results obtained from the four parameters of the attacks carried out, three were successfully carried out in one trial. From these experiments, it can be concluded that the wireless network security system at Klik Pratama Bhakti Medika is quite safe, but can still be attacked through MAC Address bypassing attacks, ARP Spoofing, and Man In The Middle Attack. For more secure security, MAC Filtering can be activated and for passwords using a combination of numbers, symbols, capital letters and lowercase letters, a minimum of 8 characters.

Dennis Nigel Cunong, used PTES to conduct security risk analysis research on the website of the investment agency and one-stop government integrated service at XYZ and the results showed that the XYZ local government website still has many security holes that hackers can exploit to attack the website. There are 1 high risk security hole, 4 medium risk security hole, and 9 low risk security hole. With the discovery of all security holes, XYZ local government can easily develop websites. For further research, it is recommended to use different tools and different methods to

find different security vulnerabilities. This research can also be a reference for everyone in conducting a security audit of a website, both in terms of the methods and tools used.

## LITERATURE REVIEW

**1. Computer**

Networks A computer network is a set of "interconnections" between 2 or more autonomous computers connected by wired or wireless transmission media. If a computer can make other computers restart, shutdown, or perform other controls, then those computers are not autonomous (does not control other computers with full access). (M. Syafrizal, 2005)

**2. WLAN**

Network Wireless local network or WLAN is a local area network that uses radio wave media. (W.Komputer, 2006) Wireless LAN here can be defined as a flexible data communication system that can be used to replace or add existing LAN network to provide additional functionality in the concept of computer networks in general. The functions offered here can be in the form of reliable connectivity in connection with user mobility. (A.Satria, 2011)

WLAN networks have the following advantages:

a. Low maintenance costs
b. Easy to develop

WLAN networks also have weaknesses in the form of:

a. Having a large delay in sending data.
b. Often the signal is blocked.
c. Data security is not guaranteed

**3. Network Security Network**

security is one of the important things in monitoring and preventing unauthorized and harmful misuse of network resources.

a. Confidentiality
   Confidentiality requires that information or data can only be accessed by authorized parties.
b. Integrity
   Integrity, which requires that information can only be changed by authorized parties.
c. Availability
   Availability requires that information be available to authorized parties when needed.
d. Authentication
   Authentication which requires that the sender of information can be identified correctly and there is a guarantee that the identity obtained is not fake.
e. Nonrepudiation
   Nonrepudiation requires that neither the sender nor the recipient of the information can deny the sending and receiving of messages.

**4. Penetration Testing Standard**

Penetration Testing Execution Standard consists of seven main parts. It covers everything related to penetration testing from the initial communication and reasoning behind the pentest, through the information gathering and threat modeling phases where the tester works behind the layers to gain a better understanding of the organization being tested, through vulnerability research, exploits and after. exploitation. PTES has 7 stages to implement, starting from Pre engagement, Interactions to reporting. The following are PTES stages which are shown in Figure 1 below: (N.WK, 2012).

*name of corresponding author

Sinkron: Jurnal dan Penelitian Teknik Informatika
Volume 6, Number 1, January 2022
DOI : https://doi.org/10.33395/sinkron.v7i1.11249
e-ISSN : 2541-2019
p-ISSN : 2541-044X


Fig. 1 Penetration testing execution standard

following is an explanation of the stages in the Penetration Testing Execution Standard (PTES): (The PTES team, 2017)

a. Pre-Engagement
This section aims to provide and explain tools and techniques that assist in the preparation steps of pen testing . Information can be obtained from various sources including from the experience of testers who have done pentesting for years. This step is very important before starting the pentesting step. Pentesting does not have to be confrontational, because pentesting activities should not be about being hacked or not, but about identifying business risks that can be attacked.

b. Intelligence Gathering
At this stage, collecting information about pentesting. The purpose of the information obtained is to provide and design actions to be carried out in accordance with the agreement of the target.

c. Threat Modeling
This stage will identify the threat modeling approach needed for pentesting. The focus of this standard depends on the company's business processes and business assets. The threat modeling phase is very important for testers and companies, because this modeling can provide clarity on risks and target priorities.

d. Vulnerability Analysis
This stage will identify the threat modeling approach needed for pentesting. The focus of this standard depends on the company's business processes and business assets. The threat modeling phase is very important for testers and companies, because this modeling can provide clarity on risks and target priorities.

e. Exploitation
At this stage does not only focus on building access to the system. Because at this stage it is very necessary good planning and making the right decisions. The main focus of exploitation is to identify entry points to target websites that have high (important) values. If the vulnerability analysis stage is completed correctly, the list of high-value targets should be met. At the end of the attack should consider the probability of success and the highest impact on the target.

f. Post-Exploitation The
purpose of post-exploitation is to determine the value of the website and conduct consultations in order to provide advice on the defense of the website. The website is assessed from data that has high sensitivity in the form of identity data, financial data and planning data. The methods described in this step are intended to help the tester identify and document sensitive data, identify configuration settings, communication channels, and relationships with other network devices that can be used to gain further access to the network, and set one or more methods of accessing the website.

g. Reporting The
purpose of this stage is to determine the value of vulnerability and maintain to be able to control when used. The level of value is determined from the level of sensitivity of the data stored in it and its use. This stage is intended to help testers identify and document sensitive data, identify configuration results, communication channels, and relationships with other network devices that can be used to gain further access.

## METHOD

The research method used to analyze wireless network security systems is using penetration testing execution standards using interview data collection methods, literature methods and observation. The following is the proposed research model:

*name of corresponding author

Sinkron: Jurnal dan Penelitian Teknik Informatika
Volume 6, Number 1, January 2022
DOI : https://doi.org/10.33395/sinkron.v7i1.11249
e-ISSN : 2541-2019
p-ISSN : 2541-044X

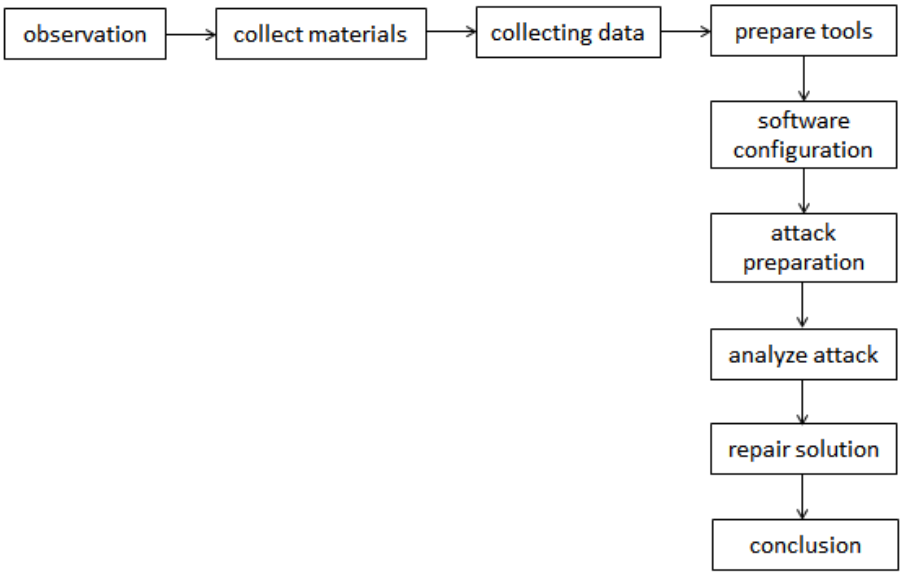


Fig. 2 Research flow chart

## RESULT

The current wireless network security system at SMP XYZ is an infrastructure-based WLAN. To consider network security, it is necessary to pay attention to the weak points in the security system and the presence of attacks from outsiders. The following is an overview of the existing network infrastructure at SMP XYZ for now.

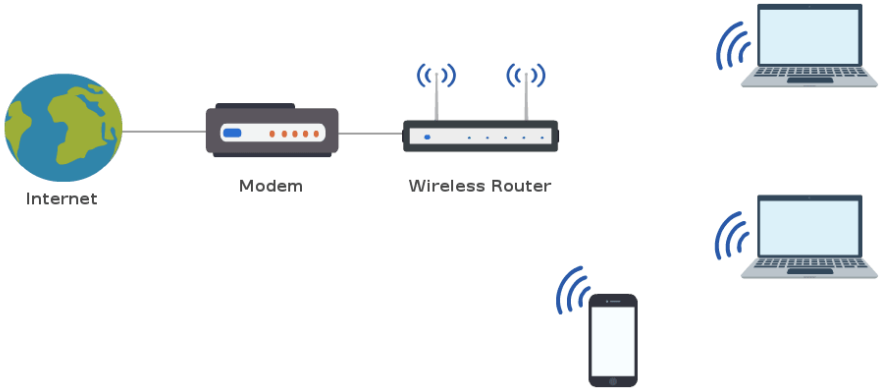


Fig. 3 Current network architecture

system on SMP XYZ is not strong enough in terms of network security. This is because user management has not been implemented so that bandwidth leaks occur and allow illegal access to occur.

In this case, network security needs to be improved to make it more secure. So in this study, the author conducted a network security analysis using the penetration testing method.

The following is a table of attacks that will be analyzed on the XYZ SMP network.

Table 1
Security Attack Type

| Testing | Attack Limit | Tools |
|---|---|---|
| WPA2 Cracking | The attack was carried out on a wireless network that uses the WPA security type, WPA 2 | Aircrack-ng app on kali linux |
| DoS | The attack was carried out on the access point network device | Kali linux |
| Passwordd Router Wireless Cracking | Attack on router password | Web browser |
| Access Point Isolation | Performing attacks between clients | Net cut |

## DISCUSSIONS

### Security Analysis

To implement the framework that has been prepared, the author performs a simulation to determine the security of the Wireless Local Area Network (WLAN) network at SMP XYZ by using the Penetration Testing method, *name of corresponding author

e-ISSN : 2541-2019
p-ISSN : 2541-044X

namely by using aircrack application tools, kali linux, web browser, and net cut . Penetration Testing carried out is the type of Overt pentest where the author conducts network security testing with the knowledge of the agency.

WLAN network security testing using the penetration testing execution standard (PTES) method is as follows:

a) Information Gathering

This process is carried out to find out information about the WLAN network to be tested. In the previous chapter, questions were asked using the interview method to related sources.

1) Network penetration test questions
From the results of interviews with related sources, information was obtained about penetration tests that must be carried out on the XYZ SMP network because with this penetration test it will be known how far the network security is at the school. The author is given time to simulate this penetration test when office hours have ended so as not to interfere with the activities of teachers and other students. For this penetration test, approximately 30 IP (Internet Protocol) addresses are tested and there is no impact on other devices because this penetration test is a simulation.
2) Wireless network penetration test
questions For questions about the wireless network penetration test, the author knows that there are 30 active wireless devices at SMP XYZ during working hours. And for wireless connections at this school, it can be accessed by outsiders (in this case guests) by entering a wireless password. The type of security used is WPA2-PSK. So far no one has tried to attack via SMP XYZ's wireless network.
3) Physical penetration test
questions For questions about the physical penetration test, the author received information that at SMP XYZ there is no Standard Operating Procedure (SOP) for network access, because there is no IT division for that section and for security around the school, CCTV cameras have been installed in various areas. corner of the room.
4) System administrator questions
From the results of interviews with related sources, the authors get information that the operating system is not always updated, and there is no software for monitoring the system or monitoring the use of wireless networks in schools. Because this school does not have a server computer, data back up is done privately with an external hard drive.

b) Preliminary Analysis

This process is carried out to determine the type of action and the need for penetration testing. After the initial analysis is done, the author can immediately run the standard execution penetration testing (PTES) process on the WLAN network at SMP XYZ. The actions that will be taken in the test include:

1) Testing the WPA2 Cracking attack using the Aircrack-ng tool on the Kali Linux application.
2) DoS by using Kali Linux tools.
3) Passwordd Router Wireless Cracking using web browser tools.
4) Access Point Isolation using Net cut tools.

c) Attacking

This process is carried out to penetrate the network with various kinds of attacks. Attacking actions for penetration into WLAN networks. Tests were carried out using Cracking attack testing, DoS, Passwordd Router Wireless Cracking, Access Point Isolation.

1) Testing the WPA2 Cracking attack using the Aircrack-ng tool on the Kali Linux application. at this stage the WPA2 Key search process is carried out using Aircrack-ng. At this stage, the password for the access point "mokletjaya" has been found on the target wifi and it is concluded that the WPA2 Key can be cracked.

*name of corresponding author

Sinkron: Jurnal dan Penelitian Teknik Informatika
Volume 6, Number 1, January 2022
DOI : https://doi.org/10.33395/sinkron.v7i1.11249
e-ISSN : 2541-2019
p-ISSN : 2541-044X

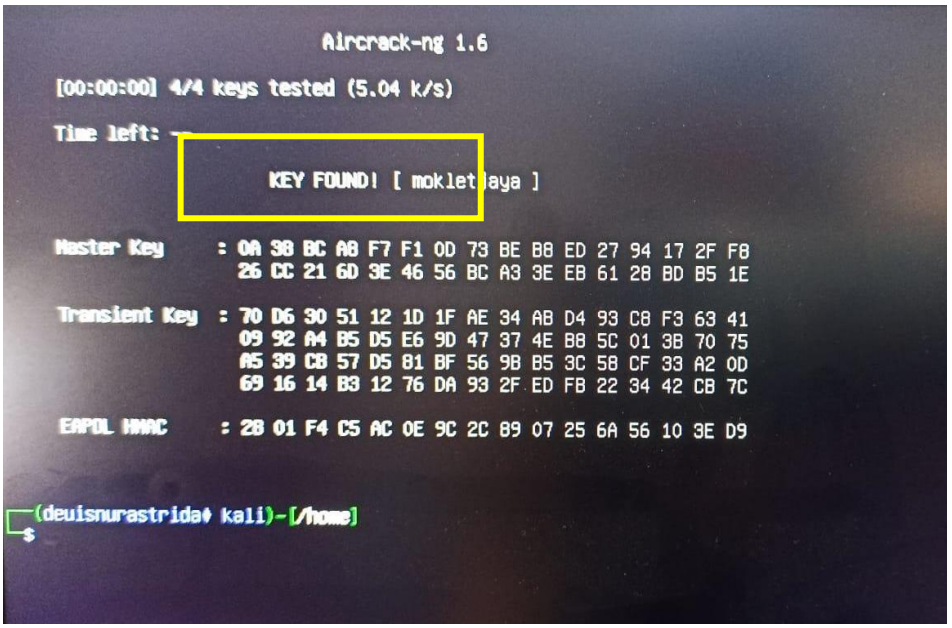


Fig. 4 Results of WPA Cracking

2) DoS using Kali Linux tools.
The second stage of DoS, at this stage the password for the access point "mokletjaya" has been found on the target wifi and it is concluded that the WPA2 Key can be cracked. At this stage, the DoS process is carried out to disconnect the wireless network at SMP XYZ.

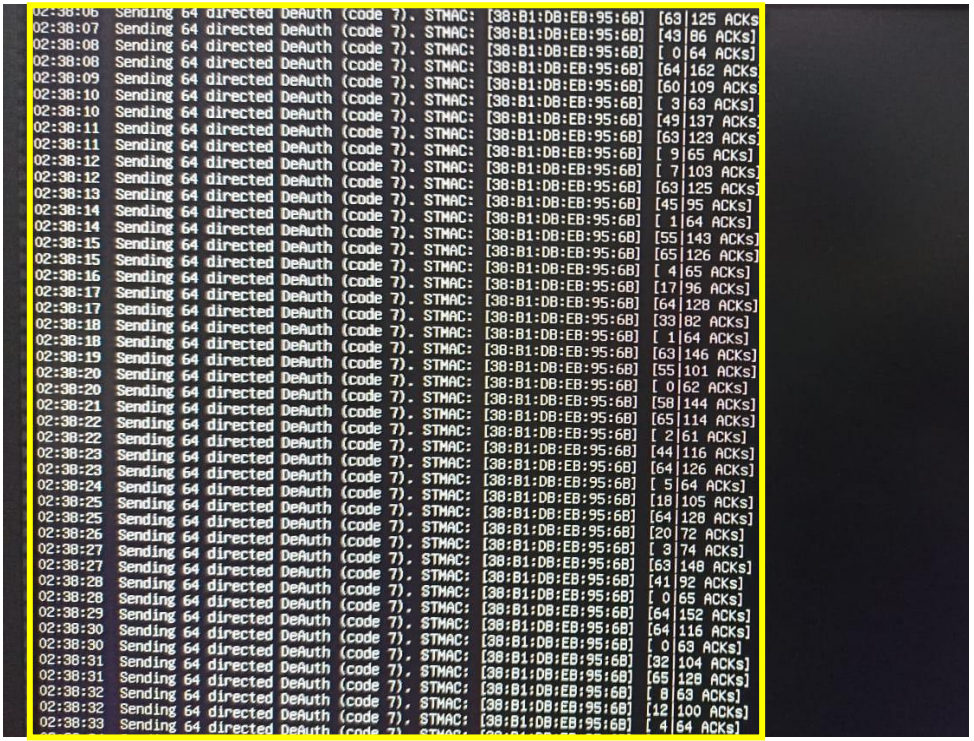


Fig. 5 Results of DoS

3) Passwordd Router Wireless Cracking using web browser tools.
The third stage is the wireless router login password cracking, at this stage the cracking process is carried out to enter the wireless router login so that access rights can be changed such as limiting users, adding the number of SSIDs in one Access Point, and changing the wireless password and SSID name.

4) Access Point Isolation using Net cut tools.
The fourth stage is Access Point Isolation, at this stage testing is carried out on the access point to find out whether the access point has turned on the access point isolation feature on the access point. The results of scanning the host on the ettercap application on kali linux found hosts, it can be concluded that

*name of corresponding author

Sinkron: Jurnal dan Penelitian Teknik Informatika
Volume 6, Number 1, January 2022
DOI : https://doi.org/10.33395/sinkron.v7i1.11249
e-ISSN : 2541-2019
p-ISSN : 2541-044X

the access point does not turn on the access point isolation feature on the access point. This can have an impact on attacks from within or Client to Client. And the last stage in penetration is Gaining Access, this stage is the process stage to use or use the password or WPA key obtained in the penetration process.

**Test Results**

From all the testing stages that have been carried out, the authors can convey the results of the Penetration Testing Execution Standard on the Wireless Local Area Network (WLAN) network carried out at SMP XYZ. The following is a report from the security test results:

Table 2
Results of the Penetration Testing Execution Standard

| Attack Type | Information | Tools | Attack Result |
|---|---|---|---|
| WPA2 Cracking | The attack was carried out on a wireless network that uses the WPA security type, WPA 2 | Aircrack-ng app on kali linux | WPA2 Key can be cracked |
| DoS | The attack was carried out on the access point network device | Kali linux | Client connection in the access point is very easy to disconnect, it only requires the MAC Address and SSID of the Access Point |
| Passwordd Router Wireless Cracking | Attack on router password | Web browser | The level of vulnerability is high because the access point only uses the default password |
| Access Point Isolation | Performing attacks between clients | Net cut | Clients can attack Client or Client to Client only by equating client workgroups |

**Proposed Security Analysis**

After testing the network security gap using the Penetration TestingExecution Standard method on the Wireless Local Area Network (WLAN) network at SMP XYZ, the authors propose a better network security infrastructure. The following is a table of the vulnerability fix solutions proposed by the author to SMP XYZ.

Table 3
Suggested Vulnerability Fixing Solution

| No | Attack | Vulnerability | Repair Solution |
|---|---|---|---|
| 1 | WPA2 Cracking | Successfully got a valid wifi password | Use a unique and strong WPA2 Key of at least 15 characters |
| 2 | DoS | Network connection is easy to disconnect | Using sectoral antennas as wireless network antennas |
| 3 | Passwordd Router Wireless Cracking | Successfully got the Username and Password to login on the Wireless Web Router | Use a unique and strong password of at least 15character |
| 4 | Access Point Isolation | Fellow clients can PING and can be exposed to ARP Poisoning attacks | Configuring AP Isolation on Access Point |

## CONCLUSION

conclusion from the research conducted is that there are still many security holes in the XYZ SMP wireless that allow outsiders to access freely. By using the penetration testing method, we obtain vulnerabilities in terms of WPA2 cracking, DoS, wireless router password cracking, and access point isolation so that vulnerabilities in the XYZ SMP wireless network can be identified. Every vulnerability found has been given a fix solution so that the existing risk can be reduced. With the vulnerability testing that has been carried out and providing solutions to reduce this risk, it is hoped that wireless use activities at XYZ SMP can run more safely.

## ACKNOWLEDGMENT (*optional*)

## REFERENCES

Adrian, A., & Setiyadi, A. (n.d.). *ANALISIS KEAMANAN JARINGAN DENGAN METODE PENETRATION TESTING EXECUTION STANDARD (PTES) DI DINAS KESEHATAN PROVINSI JAWA BARAT*.

Aufan, O. :, & Rosadi, I. (n.d.). *ANALISIS KEAMANAN SISTEM INFORMASI AKADEMIK DENGAN WEB PENETRAION TESTING*.

*name of corresponding author

e-ISSN : 2541-2019
p-ISSN : 2541-044X

Chandra, D. W. (2014). *Program Studi Teknik Informatika Fakultas Teknologi Informasi Universitas Kristen Satya Wacana Salatiga Oktober 2014 Program Studi Teknik Informatika Fakultas Teknologi Informasi Universitas Kristen Satya Wacana Salatiga Oktober 2014*.

Cunong, D. N., Saputra, M., & Puspitasari, W. (2020). *ANALYSIS OF OROS MODELER DATA REPORTING PROCESS TO SAP HANA IN ACTIVITY BASED COSTING FOR INDONESIA TELECOMMUNICATION INDUSTRY*. *7*(1).

FAKHRI, A. (2020). Analisis Resiko Keamanan Terhadap Website Dinas Penanaman Modal Dan Pelayanan Terpadu Satu Pintu Pemerintahan Xyz Menggunakan Standar Penetration Testing Execution Standard (Ptes). *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699. https://repository.telkomuniversity.ac.id/home/catalog/id/156954/slug/analisis-resiko-keamanan-terhadap-website-dinas-penanaman-modal-dan-pelayanan-terpadu-satu-pintu-pemerintahan-xyz-menggunakan-standar-penetration-testing-execution-standard-ptes-.html

Ismail, R. W., & Pramudita, R. (2020). *Metode Penetration Testing pada Keamanan Jaringan Wireless Wardriving PT. Puma Makmur Aneka Engineering Bekasi*. *5*(1), 53–62. https://nvd.nist.gov/vuln-metrics/cvss

Samsumar, L. D., Gunawan, K., Program, D., Manajemen, S., Program, D., & Komputerisasi, S. (2017). Analisis Dan Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel ( Wireless Lan ); Studi. *Ilmiah Teknologi Informasi Terapan*, *IV*(1), 73–82.

Sari, M. W., & Hardyanto, H. (2016). Implementasi Aplikasi Monitoring Pengendalian Pintu Gerbang Rumah Menggunakan App Inventor Berbasis Android. *Eksis*, *09*(1), 20–28.

Susanto, M. I., Hasad, A., & Bakri, M. A. (2019). Sistem Proteksi Jaringan Wlan Terhadap Serangan Wireless Hacking. *JREC (Journal of Electrical and Electronics)*, *7*(1), 25–34. https://jurnal.unismabekasi.ac.id/index.php/jrec/article/download/1762/1489

Testing, P., Jaringan, S., Untuk, K., Keamanan, K., Dengan, S., Metode, M., Ilmiah, A., Informasi, F. T., &

*name of corresponding author