GCIR: Greenation Computer and Information Review
E-ISSN: 9999-9999
P-ISSN: 9999-9999
GREENATION PUBLISHER
+62 812-1046-7572 https://greenpub.org/GCIR greenation.info@gmail.com
DOI: https://doi.org/10.38035/gcir.v1i1

Using the Penetration Testing Execution Standard Method (PTES) for Wireless Network Security Analysis

Ridwan[1]
[1]STIE Dewantara, Bogor, Indonesia, ridwans70@gmail.com

Corresponding Author: ridwans70@gmail.com[1]

Abstract: As more people utilize the internet, network security has grown in importance. The internet has an impact on practically every part of life, including the employment. Located in the Tambun Utara District of Bekasi Regency, the Setia Mekar Village Hall office is a public service location. It now relies on a single wireless access point to connect to the internet and uses Wireless Local Area Network (WLAN) technology to meet the demands of the community for a variety of internet-related reasons, including administrative and other services. In order to prevent numerous criminal risks, wireless networks need to be well-secured. As such, a security analysis of the network utilizing the Penetration Testing Execution Standard (PTES) method a framework or set of guidelines used as a reference for conducting network penetration testing is required. The types of attacks that circumvent MAC authentication and ARP spoofing were tested five times using a Kali Linux virtual machine. The results showed that although there were three failures and two successes in cracking the encryption. The test findings indicate that the wireless network security system is fairly secure; however, in order to bolster security and reduce the likelihood of crime, a number of changes to the network architecture and configuration system are required.

Keyword: Network Security, Penetration Testing Execution Standards, WLAN

INTRODUCTION

The advancement of information technology and cybersecurity systems is currently progressing rapidly, with developments in the field of cyberspace, particularly web servers and databases, posing a threat of data and information theft. Therefore, a security assessment is necessary to prevent data theft (Galang Saputra & Parga Zen, 2023). The survey results conducted by the Indonesian Internet Service Providers Association (APJII) in collaboration with the Indonesia Survey Center in 2023 show an increase in the number of internet users by 78.19%, reaching 215.626.156 individuals out of a total population of 275.773.901. The high number of internet users in Indonesia certainly requires supervision and security measures on the system to avoid cybercrime attacks. According to a report from the National Cyber Security Operations Center (Pusopskamsinas) of the Cyber and Crypto Agency (BSSN), there were 403 million traffic anomalies or cyber attacks on Indonesia throughout 2023. The most common

attack patterns were trojan activity and information gathering activities (information collecting) (Budi et al., 2021).

The Setia Mekar Village Office is a public service location situated in the North Tambun District of Bekasi Regency, which currently utilizes Wireless Local Area Network (WLAN) technology as a means of internet access for various purposes, including administrative tasks, storing residents' data on a local computer server, and other services to meet the community's needs. Therefore, network security analysis is necessary to evaluate vulnerabilities in wireless network security systems.

One of the methods used to analyze network security is penetration testing, which is an assessment and analysis method for a computer network system. In this network security analysis, the Penetration Testing Execution Standard (PTES) will be used as a reference for its implementation. PTES is one of the standards or guidelines used as a guide for penetration testing, containing detailed recommendations regarding the methods and techniques used at each stage of the testing (Dasmen et al., 2023).

METHOD

Computer Network System

A computer network is a communications system that enables data or information sharing between two or more connected devices. When devices in a computer network have a network interface card that allows for both wired and wireless connections, data and information exchange as well as resource sharing are made possible (Astuti, n.d.).

Wireless LAN Network

A Wireless Local Area Network is a computer network that uses radio frequencies and infrared as data transmission media. WLAN is often referred to as a wireless network (Gondohanindijo, 2012). The process of wireless communication began with the emergence of radio-based equipment, such as walkie-talkies, remote controls, mobile phones, and other radio devices. The need to make computers portable and easily integrated with existing networks has driven the development of wireless technology (Jumadi et al., 2022).

Computer Network Security System

Network security is a configuration that serves to protect data, maintain confidentiality, integrity, and ensure the availability of access to computer networks. Network security consists of several aspects, and a computer network is considered secure if it meets the following categories (Edi Surya Negara, 2014):

1. Confidentiality
   An aspect of protecting information is to limit third parties' access to that information, ensuring that only the sender and the recipient are aware of it.
2. Integrity
   The aspect of ensuring that information or data can be consistent, accurate, and protected from alteration by other parties, and can only be changed by the sender and receiver.
3. Authentication
   Prioritizing the validity of information users or valid data comes from the original server that is accessed.
4. Availability
   Information or data services can be accessed at any time and their availability is guaranteed when needed.
5. Non Repudiation
   Aspects related to user authentication, when accessing a system or network, users cannot deny having logged into that system or network.

Penetration Testing

Penetration testing is a part of ethical hacking, which involves methods and procedures for testing information security. Penetration testing is an activity aimed at evaluating a system by conducting attacks to identify security vulnerabilities within that system (Maliq Ibrahim et al., 2022). In wireless network security, penetration testing is used to add a firewall to the router, which can reduce the risk of vulnerabilities in the system or data contained within it. Penetration testing has standards or guidelines that can be used as a reference, commonly referred to as the Penetration Testing Execution Standard. (PTES). This standard allows a pentester to focus on exploiting vulnerable areas and selecting appropriate attack techniques (Adiguna & Widagdo, 2022).

Figure 1: Stages of PTES

1. Pre-engagement
   The preparation or agreement stage conducted by the pentester with the service owner to prevent issues related to legal violations and policies.
2. Intelligence Gathering
   The stage of information gathering that can assist the penetration testing process can be derived from several methods, which in this research focuses on penetration testing for wireless network security.
3. Threat Modelling
   The steps to properly conduct a penetration test by using a threat modeling approach to more easily identify attacks on service owners, which in this research pertains to attacks on wireless network systems.
4. Vulnerability Analysis
   The stage of searching for and analyzing information on vulnerabilities in wireless network systems to facilitate the penetration testing process, based on the information obtained from the methods used previously.
5. Exploitation
   The stage of conducting penetration testing involves accessing a wireless network system to identify security vulnerabilities using the employed methods, but this is done after understanding the exploitable security gaps and whether the attacks will succeed or fail.
6. Post Exploitation
   The stage of developing a plan after the exploitation process, as well as analyzing the most vulnerable parts and explaining the areas at risk and their impacts, and ensuring that the previously agreed-upon procedures can be used during the post-exploitation phase.
7. Reporting

The stage of presenting the results report after conducting penetration testing involves reporting the identified risks and how to recommend mitigating the risks associated with the discovered vulnerabilities (Efendi et al., 2024).

RESULTS AND DISCUSSION

Pre-engagement

At this stage, the author provides some general questions to facilitate the interview process regarding network penetration testing, wireless network penetration testing, physical penetration testing, and system administration.

Intelligence gathering

Gather as much information as possible to assist in the wireless network penetration testing process using the data collection methods described above.

Threat Modelling

Identifying threats in security vulnerabilities that may occur to facilitate the determination of attacks.

Table 1: Threat Modeling

No.	Identify Threats
1	WPA2-PSK encryption that is vulnerable to brute force attacks
2	Not enabling the MAC filtering feature on the wireless network
3	Anyone can connect directly by knowing the applied password
4	There are no access restrictions
5	The staff at the Setia Mekar village office do not fully understand the security of wireless network systems
6	Only using one router and SSID for internet access and data sharing

Vulnerability Analysis

Searching for and identifying several security vulnerabilities in the wireless network that will later be used for security testing of the wireless network at the Setia Mekar Village Office.

Table 2: Vulnerability Analysis

No.	Vulnerability Analysis
1	The inactive ARP binding feature can be exploited to manipulate data traffic by disabling network connections, preventing users from connecting. This vulnerability can be tested through ARP Spoofing attacks
2	WPA2-PSK encryption has a security vulnerability that can be attacked using brute force cracking techniques
3	Not applying MAC address restrictions allows for imitation; the security gap in inactive MAC filtering can be exploited through attempts using MAC address bypassing techniques by modifying the MAC address to match one that is already connected

Exploitasi (Attack Simulation Test)

Cracking the encryption

In this attack simulation, the aircrack-ng tools were used to assess the resilience of the wireless network security system employing WPA2-PSK installed at the Setia Mekar Village Hall. The aircrack-ng tool utilized a brute force method, which involves guessing the currently used password. This method requires a collection of words or a wordlist containing potential passwords to assist in the password cracking process, as well as a handshake packet, which is the process of a device connecting to the network. The word collection was carried out through observation and experimentation in the vicinity of the village hall. This implementation was conducted seven times using different wordlists for each trial, followed by matching the words with the handshake packets. The sixth and seventh trials were successful in discovering the used password, which is “des*******10.”

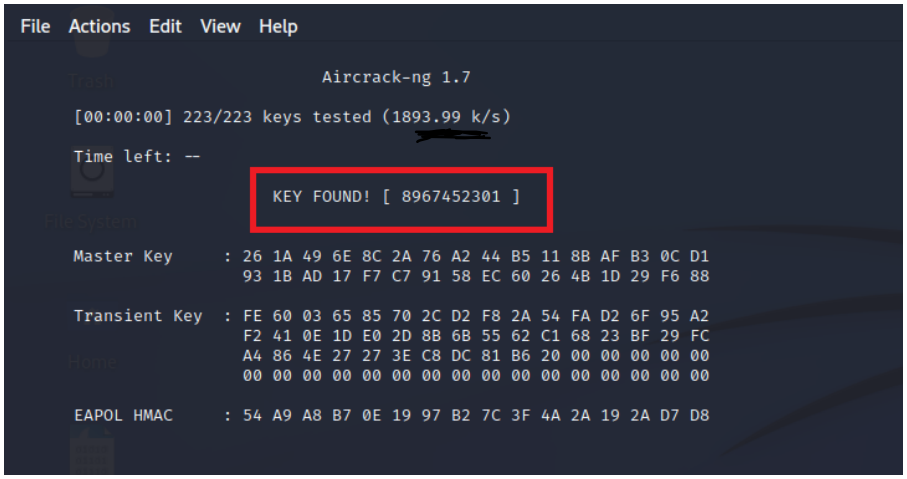

Figure 2. Password Encryption Found

Bypassing Mac Authentication

Bypassing MAC Address is a test that involves changing a device's MAC address to evaluate the implementation of MAC address filtering. In this test, the author used the tool Macchanger, which is available on the Kali Linux operating system. The author made changes to the MAC address value on the network card used to access the internet, conducting this experiment seven times. After the process of changing the MAC address, the author successfully connected to the internet and confirmed that the wireless network did not impose MAC address restrictions.

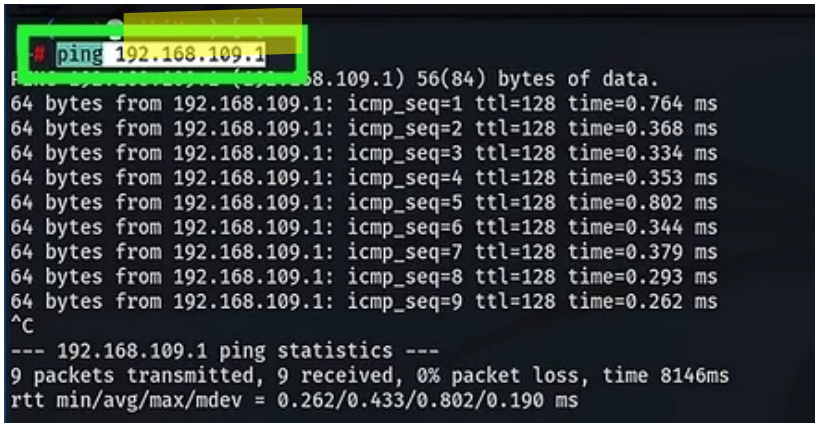

Figure 3: Internet connection testing

ARP Spoofing

ARP Spoofing takes advantage of the security vulnerability in ARP broadcasting by intercepting devices that are currently connected. This test was conducted 7 times using the Murder Death Kill 3 (mdk3) tool to manipulate users by disconnecting the network, making it seem as though they were still connected to the internet, while in reality, the network connection was no longer available.

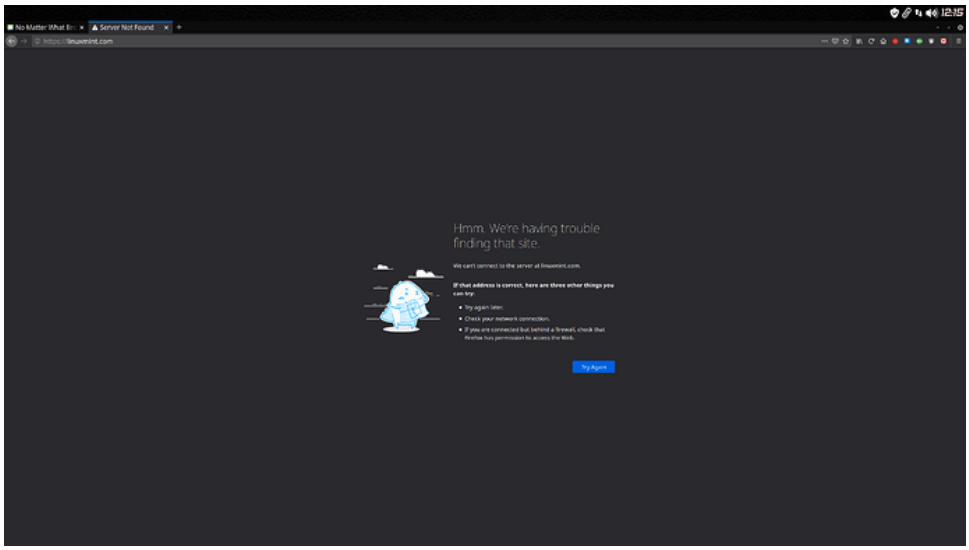

Figure 4: Internet access testing

Testing Report Using the PTES Method

Here is the presentation of the results from all stages of the penetration testing conducted by the author using the PTES method on the wireless network of the Setia Mekar Village Office in the Tambun Utara District, Bekasi Regency.

Table 3: Results of Testing with PTES

Type of Attack	The data needed	Testing Standards	Tools	Testing Status
Cracking The Encryption	Handshake, wordlist, SSID target	Crack password wifi	Aircrack-ng	Failed Failed Failed Failed Failed Success Success
Bypassing Mac Address	List of connected MAC addresses	Changing the MAC Address to access the network	Macchanger	Success Success Success Success Success Success Success
ARP Spoofing	List of connected devices	Disconnecting the network (offline)	Murder Death Kill 3 (MDK3)	Success Success Success Success Success Success Success

CONCLUSION

Based on the penetration testing conducted, the wireless network security system at the Setia Mekar Village Office is quite secure as it has implemented WPA2-PSK encryption. However, it is still vulnerable to attacks, as the encryption security can still be exploited using brute force techniques to find the password based on the handshake packets and the wordlist that has been created. Network configuration and topology need several improvements, such as in the attack testing phase using techniques like Bypassing MAC Address and ARP Spoofing. This testing has been successful in seven trials. It is necessary to improve the configuration of the wireless network security system and the topology used to avoid wireless network attacks such as cracking the encryption, Bypassing MAC Authentication, or ARP Spoofing.

REFERENCE

Adiguna, M. A., & Widagdo, B. W. (2022). *Analisis Keamanan Jaringan Wpa2-Psk Menggunakan Metode Penetration Testing (Studi Kasus : Router Tp-Link Mercusys Mw302r)*.

Astuti, I. K. (n.d.). *Jaringan Komputer*.

Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. *Prosiding Seminar Nasional Sains*

Teknologi Dan Inovasi Indonesia (SENASTINDO), *3*, 223–234. https://doi.org/10.54706/senastindo.v3.2021.141

Dasmen, R. N., Rasmila, R., Widodo, T. L., Kundari, K., & Farizky, M. T. (2023). PENGUJIAN PENETRASI PADA WEBSITE ELEARNING2.BINADARMA.AC.ID DENGAN METODE PTES (PENETRATION TESTING EXECUTION STANDARD). *Jurnal Komputer Dan Informatika*, *11*(1), 91–95. https://doi.org/10.35508/jicon.v11i1.9809

Edi Surya Negara. (2014). *Implementasi Management Network Security pada Laboratorium Cisco Universitas Bina Darma*.

Efendi, R., Wahyono, T., & Widiasari, I. R. (2024). Uji kerentanan keamanan pada aplikasi berbasis web menggunakan metode Vulnerability Assessment. *AITI: Jurnal Teknologi Informasi*, *21*(Maret), 44–57.

Galang Saputra, S., & Parga Zen, B. (2023). Analisis Keamanan Jaringan Wireless menggunakan Metode Penetration Testing Execution Standard (PTES). *JURNAL SISTEM INFORMASI GALUH*, *1*(2), 2023. https://ojs.unigal.ac.id/index.php/jsig/index

Gondohanindijo, J. (2012). *Sistem Keamanan Jaringan NIRKABEL*.

Jumadi, P., Parenreng, M., Wahid, A., & Yusmalasari, S. A. (2022). *PENGANTAR JARINGAN KOMUNIKASI NIRKABEL CV. ZT CORPORA*.

Maliq Ibrahim, A., Defisa, T., Bayu Seta, H., & Wayan Widi, I. P. (2022). Analisis Keamanan Sistem pada Website Perusahaan CV. Kazar Teknologi Indonesia dengan Metode Vulnerability Assesment and Penetration Testing (VAPT). In *Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA) Jakarta-Indonesia*.

Isnawati, I., & Ali, H. (2024). Pengaruh Pendidikan, Informasi dan Komunikasi terhadap Internet of Things. *JURNAL MANAJEMEN PENDIDIKAN DAN ILMU SOSIAL*, *5*(3), 312-319.

Mangalindung, G. H., & Ali, H. (2023). Pengaruh Teknologi Informasi, Kualitas Informasi dan Dukungan Manajemen Puncak terhadap Sistem Informasi Keuangan. *Jurnal Manajemen dan Pemasaran Digital*, *1*(4), 232-238.

Sabarini, N. E., & Ali, H. (2024). Pengaruh Teknologi Informasi, Pemanfaatan Blog dan Database terhadap Sistem Informasi. *JURNAL MANAJEMEN PENDIDIKAN DAN ILMU SOSIAL*, *5*(3), 383-389.

Primawanti, E. P., & Ali, H. (2022). Pengaruh Teknologi Informasi, Sistem Informasi Berbasis Web Dan Knowledge Management Terhadap Kinerja Karyawan (Literature Review Executive Support Sistem (Ess) for Business). *Jurnal Ekonomi Manajemen Sistem Informasi*, *3*(3), 267-285.

Hamdani, E., & Ali, H. (2023). Pengaruh Keamanan Informasi, Teknologi Informasi dan Network terhadap Security of Information. *Jurnal Siber Multi Disiplin*, *1*(3), 109-116.

Salsabilla, P. J., & Ali, H. (2024). Pengaruh Teknologi Informasi, Kreativitas, dan Kualitas Produk terhadap Strategi Bersaing Perusahaan. *Jurnal Siber Multi Disiplin*, *2*(1), 18-26.

Wahono, S., & Ali, H. (2023). Determinasi Kinerja Karyawan: Komunikasi, Technology Acceptance dan Pengambilan Keputusan (Literature Review Executive Support Sistem For Business). *Jurnal Ekonomi Manajemen Sistem Informasi*, *4*(3), 614-621.

Muhajirin, A., Poernamasasi, I. O., Rony, Z. T., & Ali, H. (2024). Pengaruh Kompetensi, Budaya Kerja, dan Teknologi Informasi di Era Endemi pada Kinerja Guru pada SMK XYZ. *Jurnal Ekonomi Manajemen Sistem Informasi*, *5*(3), 250-256.

Prayoga, L., & Ali, H. (2023). Tren Terkini dalam Rekrutmen dan Retensi Bakat Berkualitas. *Jurnal Siber Multi Disiplin*, *1*(2), 87-92.

Amalia, D. N., & Ali, H. (2023). Pemanfaatan Laporan Keuangan, Software dan Brainware Terhadap Pengambilan Keputusan Manajemen. *Jurnal Ekonomi Manajemen Sistem Informasi*, *5*(1), 64-71.