Institut Riset dan Publikasi Indonesia (IRPI)
MALCOM: Indonesian Journal of Machine Learning and Computer Science
Journal Homepage: https://journal.irpi.or.id/index.php/malcom
Vol. 4 Iss. 3 July 2024, pp: 771-776
ISSN(P): 2797-2313 | ISSN(E): 2775-8575

Network Security Analysis on The Internet Facility (Wifi) UIN Syarif Hidayatullah Jakarta Against Packet Sniffing Attacks

A. Nurul Anwar

Department of Informatics Engineering, 1Faculty of Computer Science,
Pamulang University, Indonesia

Email: dosen02523@unpam.ac.id

Received Feb 8th 2024; Revised Apr 2nd 2024; Accepted Apr 22th 2024
Corresponding Author: A. Nurul Anwar

Abstract

In an increasingly digital era, network security has become very important to protect sensitive data from cyber attacks. One common attack is a packet sniffing attack, where hackers can capture and snoop on data packets sent over a WiFi network. This research aims to analyze the level of network security in internet facilities (WiFi) at UIN Syarif Hidayatullah Jakarta against packet sniffing attacks. The methods used include surveys, observations and technical analysis of existing network infrastructure. The research results show that although UIN Syarif Hidayatullah Jakarta has implemented several network security measures, there are still gaps that can be exploited by packet sniffing attacks. Factors such as the use of vulnerable network protocols and lack of use of data encryption are the main causes of network vulnerability to these attacks. Recommendations include the implementation of additional security measures such as the use of more secure protocols, implementation of strong data encryption, as well as user training and awareness to minimize the risk of packet sniffing attacks. In this way, it is hoped that internet facilities (WiFi) at UIN Syarif Hidayatullah Jakarta can be safer and protected from potentially detrimental cyber attacks.

Keyword: COBIT 4.1, GAP, Information Technology, Maturity Level, Monitor dan Evaluate

1. INTRODUCTION

At this time the issue of network security has become very important and deserves attention, networks connected to the internet are basically unsafe and can always be exploited by hackers, both wired LAN and wireless LAN networks. When data is sent, it will pass through several terminals to reach its destination, meaning it will give other irresponsible users the opportunity to intercept or change the data. In developing the design, the security system for networks connected to the Internet must be planned and understood well in order to effectively protect the resources in the network and minimize attacks by hackers.

Ettercap is a packet sniffer tool used to analyze network protocols and audit network security. It has the ability to block traffic on LAN networks, steal passwords, and perform active eavesdropping on common protocols. Meanwhile, Netstumbler is a WiFi hacking tool that is used to detect and identify open wireless signals that have infiltrated the network.

Forms of security exploitation generally use various techniques, therefore a security system is needed that is able to overcome these forms of exploitation. This paper discusses how to exploit a system and its techniques with the object used being the security system at the internet facility (WIFI) at UIN Syarif Hidayatullah Jakarta. It is hoped that with this paper readers will be able to know and understand how to secure a network. Some research on network security includes Evaluation of Institution X's Website Security Through Penetration Testing Using the ISSAF Framework [1]. Network Security on VPN Servers Using L2TP and IPSec Protocols [2]. Data Center Network Security using Performance Comparison of Canonical and Folded Clos Tree Topologies [3]. Monitoring Network Security on Ubuntu Servers from DDoS Attacks Using Snort IDS[4]. Wireless lan network security with the use of web proxy [5]. Network Security Using Port Blocking and Port Knocking Methods on Mikrotik RB-941 [6].

Computer network security from phishing threats to online banking services [7]. Network security using switch port security [8]. Protective measures on network or information system security [9]. Network Security in the era of big data [10]. Sniffing and spoofing in computer security [11]. Packet Sniffing and sniffing detection [12]. Analysis of firewalls as bandwidth limiters and network security using pfsense [13]. Network security analysis simulation at the GCS in the UCAV to support the Indonesian defense area [14]. Network security analysis using virtual private network in vocational school [15]. Network security analysis on the web from sniffing attacks using experimental methods [16]. Design of wireless communication base station monitoring system based on artificial intelligence and network security [17]. The normative enactment of international cybersecurity Capacity building assistance: a comparative analysis on Japanese and south korean practices [18]. Prediction of ecological security network in Northeast China based on landscape ecological risk [19]. Network Security Intrusion Detection Methods Combining Optimization Algorithms and Neural Networks [20].

2. MATERIAL AND METHOD

In this study, the research material is based on the basic theory of computer network security taken from various literature such as books, articles in softcopy and hardcopy form. The specifications for the tools used in the research are as follows:

1. Hardware and operating system requirements.
   a. Compaq CQ40 laptop, 2.10 Ghz dual-core processor, 2 GB memory.
   b. LAN Card 10/100BASE-T Ethernet LAN.
   c. Wireless Network Card Broadcom 802.11b/g WLAN.
   d. Windows 7 Ultimate operating system.
   e. Ubuntu 11.10 Linux operating system.

2. Software requirements.
   a. Ettercap-NG-0.7.3 software (for Packet sniffing attacks).
   b. Netstumbler software version 0.4.0 (to see the presence of WiFi)

In explaining a problem, the framework of thought or research flow is presented to facilitate understanding of the research. This method is presented in the research flow diagram. In Figure 1 it starts with collecting materials and collecting data. Where after collecting materials and data, configuration preparations are carried out for both software and hardware. Preparation for the attack is carried out as a further step. If it is successful, data analysis will be carried out, but if it is not successful, it will be studied further with preparations for another attack. After analyzing the data, conclusions can be drawn from the situation regarding the attack.

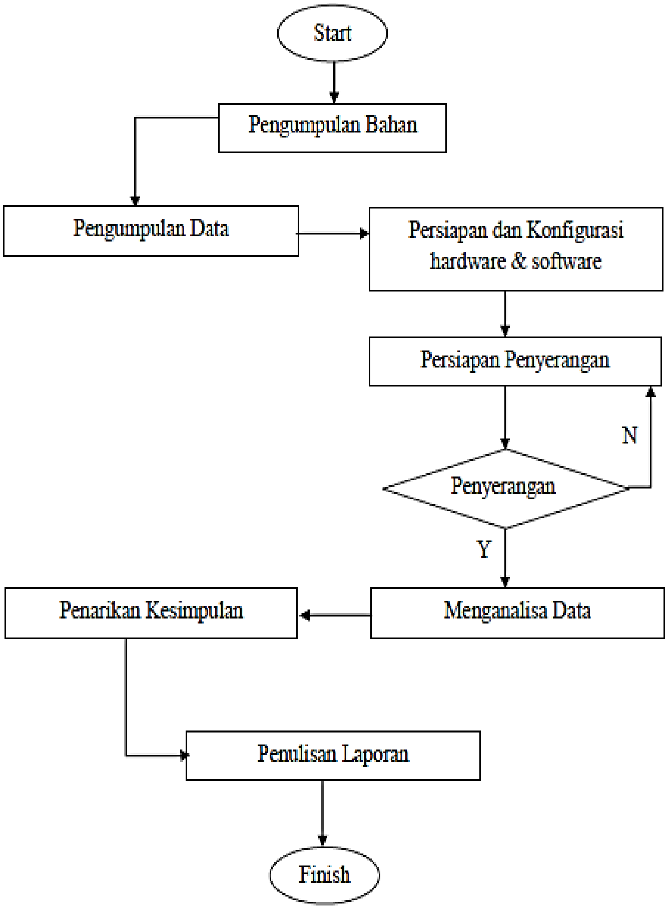


Figure 1. Research Flowchart

3. RESULTS AND DISCUSSION

3.1. Install the Netstumbler software on Windows 7

At this stage, installation is carried out first. The first step is to install the Netstumbler software on Windows 7. The second step is to double click on the netstumblerinstaller_0_4_0.exe file for installation, then follow the next instructions by clicking i agree, next and install until finished. Configure the network device connected to the laptop on netstumbler by clicking on the device option, as in Figure 2.

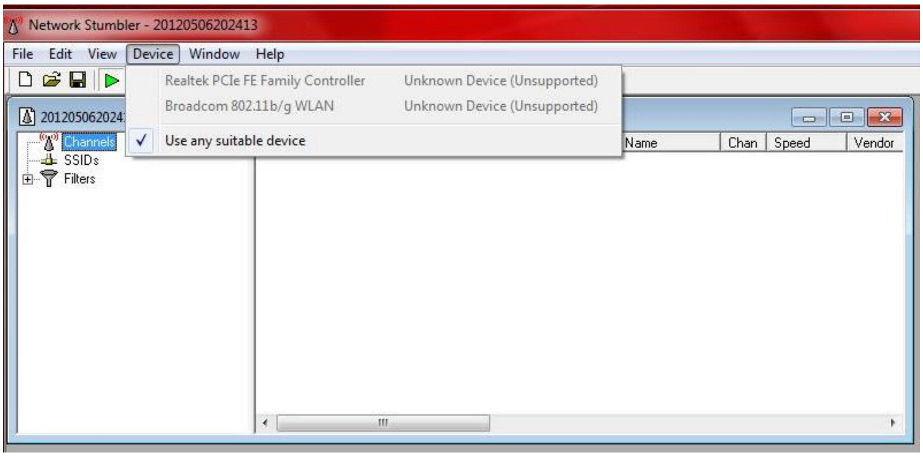

Network Stumbler - 20120506202413
File
Edit
View
Device
Window
Help
Realtek PCIe FE Family Controller
Unknown Device (Unsupported)
Broadcom 802.11b/g WLAN
Unknown Device (Unsupported)
✓ Use any suitable device
20120506202413
Channels
SSIDs
Filters
Name
Chan
Speed
Vendor

Figure 2. Network adapter device configuration in Netslumber software

After looking at Figure .2. It turns out that the network adapter device connected to the author's laptop does not support it, because the netstumbler software can only run perfectly on Windows XP and cannot run perfectly on Windows 7. Then the author replaced it with inSSIDer software as an alternative to the netstumbler software for Windows 7**.**

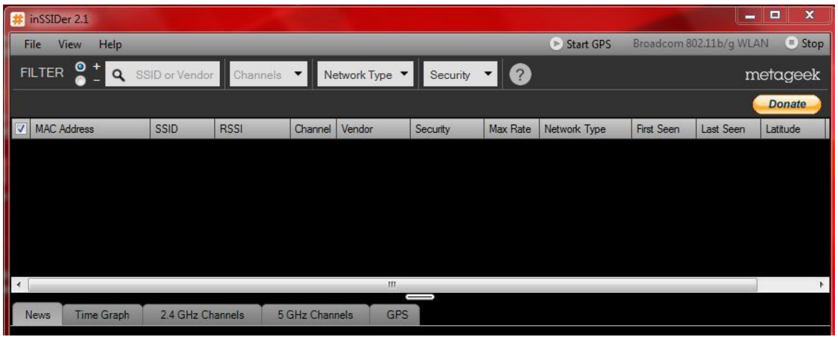


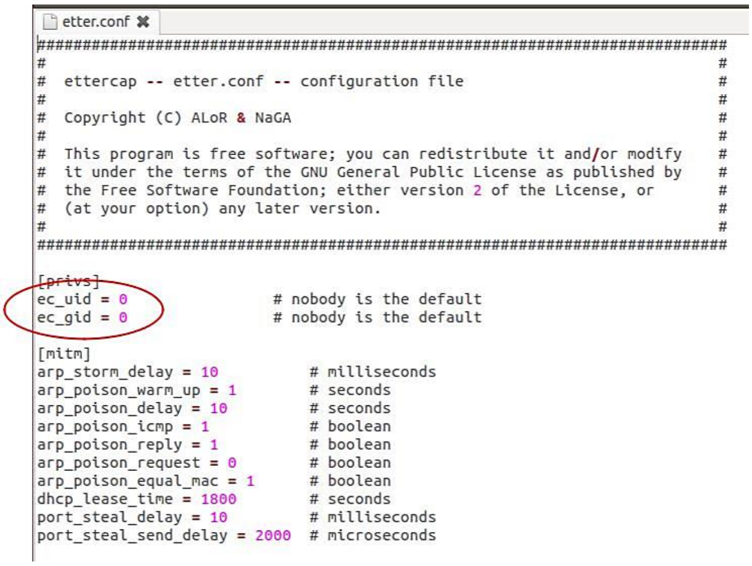
Figure 3. Appearance of inSSIDer software on Windows 7

3.2. Installing Ettercap software on Ubuntu 11.10

First, update the index package first via the terminal with the command: sudo apt-get update. Then install ettercap-gtk deb package with the command: sudo apt-get install ettercap-gtk. Figure 4 is setting the etter.conf file with the command # sudo gedit /etc/etter.conf

Figure 4. Display of Ettercap software on Ubuntu 11.10.

Then change the contents of the etter.conf file to configure the ettercap software so that it can run properly on a secure SSL connection.



```
##############################################################################
#                                                                            #
#  ettercap -- etter.conf -- configuration file                              #
#                                                                            #
#  Copyright (C) ALoR & NaGA                                                 #
#                                                                            #
#  This program is free software; you can redistribute it and/or modify      #
#  it under the terms of the GNU General Public License as published by      #
#  the Free Software Foundation; either version 2 of the License, or         #
#  (at your option) any later version.                                       #
#                                                                            #
##############################################################################

[privs]
ec_uid = 0                # nobody is the default
ec_gid = 0                # nobody is the default

[mitm]
arp_storm_delay = 10          # milliseconds
arp_poison_warm_up = 1        # seconds
arp_poison_delay = 10         # seconds
arp_poison_icmp = 1           # boolean
arp_poison_reply = 1          # boolean
arp_poison_request = 0        # boolean
arp_poison_equal_mac = 1      # boolean
dhcp_lease_time = 1800        # seconds
port_steal_delay = 10         # milliseconds
port_steal_send_delay = 2000  # microseconds
```

Figure 5. Etter.conf file configuration display 1.

Figure 5. above is an ettercap configuration which aims to be able to carry out tasks as attacking software cleanly or without other users knowing, by changing the privs section to 0.

```
# if you use iptables:
redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp
--dport %port -j REDIRECT --to-port %rport"
redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp
--dport %port -j REDIRECT --to-port %rport"
```

The command above is an ettercap configuration which aims to carry out the attack so that it can run well on a secure SSL and https network connection, so the author must ensure that the redir_command_on script in etter.conf is active.

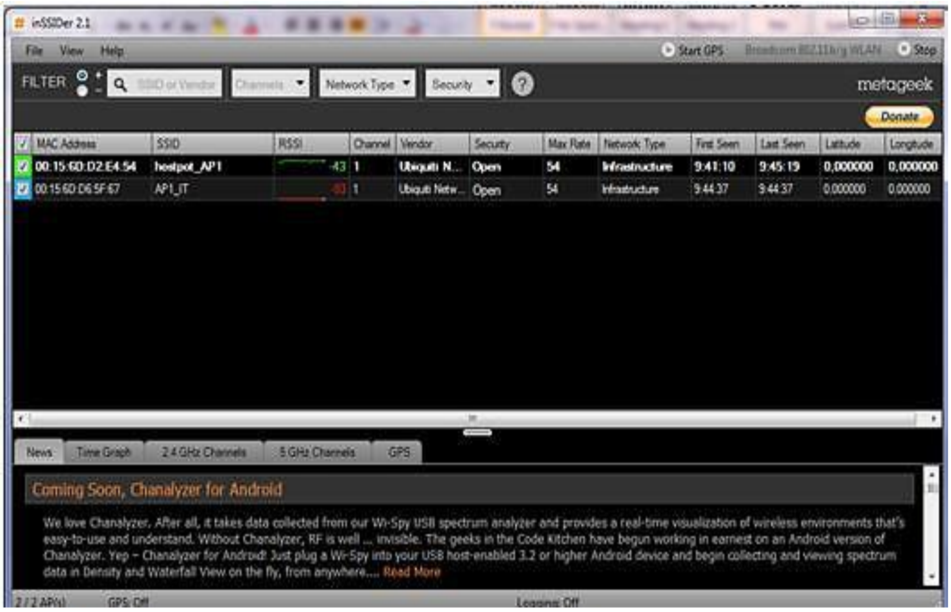
1. Security Testing Techniques
   Security testing aims to gain awareness of security issues in wired and wireless networks (wireless LAN). The author tries to identify the existence and security used by the target WiFi using inSSIDer software. After knowing the existence and security used by the target WiFi, the author logs in to get a connection with the target WiFi.
   Security testing steps, after getting a connection with the target WiFi, the author tries to carry out a Packet Sniffing attack on WiFi and cable networks using Ettercap software, the attack will be successful if data transfer is not protected by security such as SSL, IPSec, WEP, WPA and WPA2. Because the data obtained is encrypted.

2. Stages of attack
   Identifying Wifi security using inSSIDer software. The author runs inSSIDer software on Windows 7 and will automatically display information about the existence of WiFi complete with SSID name, MAC address, RSSI, vendor, channel used, network type and security or security used, can be seen in figure 6.

   Packet Sniffing uses ettercap software on WiFi and cable networks

   The steps taken are:
   The author's first step is to activate the ettercap software via the terminal with a command

```
# sudo ettercap -gtk
```



☑	MAC Address	SSID	RSSI	Channel	Vendor	Security	Max Rate	Network Type	First Seen	Last Seen	Latitude	Longitude
☑	00:15:6D:D2:E4:54	hestpot_AP1	-43	1	Ubiquiti N...	Open	54	Infrastructure	9:41:10	9:45:19	0,000000	0,000000
☑	00:15:6D:D6:5F:67	AP1_IT	[illegible]	1	Ubiquiti Netw...	Open	54	Infrastructure	9:44:37	9:44:37	0,000000	0,000000

Coming Soon, Chanalyzer for Android

We love Chanalyzer. After all, it takes data collected from our Wi-Spy USB spectrum analyzer and provides a real-time visualization of wireless environments that's easy-to-use and understand. Without Chanalyzer, RF is well ... invisible. The geeks in the Code Kitchen have begun working in earnest on an Android version of Chanalyzer. Yep – Chanalyzer for Android! Just plug a Wi-Spy into your USB host-enabled 3.2 or higher Android device and begin collecting and viewing spectrum data in Density and Waterfall View on the fly, from anywhere.... Read More

2 / 2 AP(s) GPS: Off Logging: Off

Figure 6. Display of inSSIDer software when identifying WiFi.

4. CONCLUSION

The conclusion of "Network Security Analysis of Internet Facilities (WiFi) at UIN Syarif Hidayatullah Jakarta against Packet Sniffing Attacks" is the identification of WiFi-based internet facilities at UIN Syarif Hidayatullah Jakarta as vulnerable to packet sniffing attacks. This threat is one of the main threats in the context of network security which can cause theft of sensitive user data. Apart from that, there is a vulnerability in the WiFi network infrastructure at UIN Syarif Hidayatullah Jakarta against packet sniffing attacks. It was found that weaknesses in network configuration and use of weak security protocols increased the risk of attacks. So packet sniffing attacks can have serious impacts, including theft of sensitive user information such as passwords, personal data and financial information. This can result in financial losses and damage the institution's reputation. In this case, protecting WiFi networks requires a holistic approach, including improving network security infrastructure, implementing strong encryption protocols, and user awareness of good security practices. Additionally, it is recommended that UIN Syarif Hidayatullah Jakarta improve their network security measures. This includes updating software regularly, encrypting data traffic, strengthening security policies, and providing training to users on network security threats and safe practices. In this way, UIN Syarif Hidayatullah Jakarta can improve their network security and protect sensitive user information from threats that may arise.

REFERENCES

[1] I. G. Ary, S. Sanjaya, G. Made, A. Sasmita, D. Made, and S. Arsa, “Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF,” vol. 8, no. 2, pp. 113–124, 2020.

[2] S. Keamanan, “Jurnal KomtekInfo Perancangan Implementasi VPN Server Menggunakan Protokol L2TP,” vol. 8, no. 3, pp. 6–8, 2021, doi: 10.35134/komtekinfo.v8i3.128.

[3] E. S. Negara and M. Ulfa, “Perbandingan Kinerja Topologi Canonical Dan Folded Clos Tree Pada Jaringan Data Center,” vol. 01, no. 01, pp. 25–38, 2020.

[4] L. F. Nainggolan, N. F. Saragih, and F. G. N. Larosa, “Monitoring Keamanan Jaringan Pada Server Ubuntu Dari Serangan DDoS Menggunakan Snort IDS,” vol. 2, no. 2, pp. 1–10, 2022.

[5] J. K. Informatika, “PEMANFAATAN WEB PROXY SEBAGAI PENGOPTIMAL KEAMANAN,” vol. VIII, no. 1, pp. 34–39, 2020.

[6] P. Blocking and K. Pada, “Implementasi Keamanan Jaringan Menggunakan Metode,” vol. 19, no. 1, pp. 1–8, 2020, doi: 10.36054/jict-ikmi.v19i1.119.

[7] A. Muftiadi, T. Putri, M. Agustina, and M. Evi, “Studi kasus keamanan jaringan komputer : analisis ancaman phising terhadap layanan online banking,” vol. 1, no. 2, pp. 60–65, 2022.

[8] T. Jaringan and K. Al Fikri, “InfoTekJar : Jurnal Nasional Informatika dan Keamanan Jaringan Menggunakan Switch Port Security,” vol. 2, 2021.

[9] J. Pendidikan, I. Unistek, and A. Bustami, “Ancaman , Serangan dan Tindakan Perlindungan pada Keamanan Jaringan atau Sistem Informasi : Systematic Review,” 2020.

[10] M. Informatika and P. L. P. I. Bandung, “KEAMANAN JARINGAN KOMPUTER PADA ERA BIG DATA,” vol. 02, pp. 14–20, 2020.

[11] S. Ra, A. Pranata, R. Zulanggara, and N. Halimah, "Sniffing and Spoofing in Computer Security," vol. 2, no. 6, pp. 869–874, 2023.

[12] R. Tuli, "Packet Sniffing and Sniffing Detection," vol. 16, no. 1, pp. 22–32, 2020.

[13] A. Wirjawan, H. Iskandar, R. Hidayat, and I. Y. Wulandari, "Analisis firewall sebagai bandwidth limiter dan network security menggunakan pfsense," vol. 16, no. 1, pp. 19–32, 2023.

[14] B. P. Zen, A. Zafia, I. Nofi, and Y. Putro, "JURNAL RESTI Network Security Analysis Simulation at the GCS in the UCAV to support the Indonesian Defense Area," vol. 5, no. 158, pp. 824–831, 2022.

[15] A. H. Yosi Nofita Sari, Dedy Irfan, "Network Security Analysis Using Virtual Private Network in Vocational School," vol. 9, no. 3, pp. 582–590, 2022.

[16] Y. Hae and W. Sulistyo, "Analisis Keamanan Jaringan Pada Web Dari Serangan Sniffing Dengan Metode Eksperimen," vol. 8, no. 4, pp. 2095–2105, 2021.

[17] X. Liu, "Design of Wireless Communication Base Station Monitoring system Based on Artificial Intelligence and Network Security System," *Procedia Comput. Sci.*, vol. 228, pp. 1254–1261, 2023, doi: 10.1016/j.procs.2023.11.097.

[18] A. Bimantara, "The Normative Enactment of International Cybersecurity Capacity Building Assistance : A Comparative Analysis on Japanese and South Korean Practices," vol. 24, no. 1, 2022, doi: 10.7454/global.v24i1.684.

[19] L. Sui, Z. Yan, K. Li, C. Wang, Y. Shi, and Y. Du, "Prediction of ecological security network in Northeast China based on landscape ecological risk," *Ecol. Indic.*, vol. 160, no. January, p. 111783, 2024, doi: 10.1016/j.ecolind.2024.111783.

[20] L. Xia and X. Xia, "^ Network Security Intrusion Detection Methods Combining Optimization Algorithms and Neural Networks," *Procedia Comput. Sci.*, vol. 228, pp. 582–592, 2023, doi: 10.1016/j.procs.2023.11.067.