IJEEE: Indonesian Journal of Electrical Engineering and Electronics
| Vol. 2| No. 1 | Pages 22 - 27
[January] [2025]

KF Sensor-Based Honeypot against Hacker Attacks using Kali Linux on a Laptop

Ahmad Fauzan Ritonga , Albert Ronald Wijoyo , Naufal Syafiq , Rafi Dzikra, and Firza Ilham Pratama

Department of Electrical Engineering, Universitas Pembangunan Nasional Veteran Jakarta
2210314020@mahasiswa.upnvj.ac.id

Received July 15, 2024 **|** Revised January 16, 2025 **|** Accepted January 16, 2025

ABSTRACT

This research analyzes the effectiveness of using KF Sensor-based honeypots in detecting and mitigating hacker attacks using Kali Linux on a laptop. A honeypot is a security system designed to attract and study cyber attacks by deceiving attackers into believing they have accessed a vulnerable system. KF Sensor, as a type of honeypot, serves as bait to monitor malicious activities and collect attack data. This research employs an experimental method by configuring KF Sensor on a laptop targeted by attacks from Kali Linux. The results show that KF Sensor is effective in detecting various types of attacks, such as port scanning, brute force attacks, and exploit attempts. The data collected by KF Sensor provides valuable insights into the techniques and strategies used by attackers, as well as aids in strengthening overall system security. This study concludes that implementing a KF Sensor-based honeypot is a proactive and beneficial step in enhancing network security and protecting systems from cyber threats.

***Keywords**: honeypot, KF sensor, kali linux*

1. INTRODUCTION

In today's digital era, network security threats are becoming increasingly complex and sophisticated. Organizations worldwide face a wide range of cyberattacks, including malware, phishing, and Distributed Denial of Service (DDoS) attacks. To address these threats, various security strategies have been developed, one of which is the use of honeypots.

A honeypot is a tool or system designed to attract and monitor attacker activities (Wafi, 2016). Unlike traditional security systems that focus on preventing and detecting attacks, a honeypot proactively lures attackers into interacting with it. By creating an environment that appears attractive and vulnerable to attackers, honeypots can collect valuable information about attackers' techniques, tactics, and motives.

This approach enables network administrators to gain deep insights into existing threats without risking their primary systems. Data gathered from honeypots can be used to enhance defensive measures, develop new attack signatures, and strengthen overall network security policies.

This paper explores the concept of honeypots, their types, and the benefits and challenges associated with their implementation in network security environments. By understanding the roles and functions of honeypots, organizations can better prepare to face cyber threats and protect their digital assets more effectively (Aminanto, 2019.

Network security systems need to be fortified against DDoS attacks. DDoS attacks can cause disruptions leading to system failures, operational shutdowns, erroneous requests, and even damage to server hardware. Therefore, a system capable of protecting computer servers from such attacks is essential, as the impact of DDoS attacks can be highly detrimental to servers (Angella, 2016).

One solution that can be implemented is the use of honeypots. A honeypot is a system intentionally designed to attract and be accessible to crackers, making all traffic directed at the honeypot identifiable as suspicious activity. Honeypots can assist network administrators in detecting malicious traffic and taking necessary measures to protect the system.

The primary objectives of implementing honeypots in network security encompass several key aspects. First, honeypots aim to detect cyberattacks at an early stage, providing security teams with time to respond before further damage occurs. Second, they gather detailed data about attacks, which can be analyzed to understand the latest trends and techniques used by attackers. Additionally, honeypots function to divert attacks away from the main system, test the effectiveness of existing security systems, and provide forensic evidence that can be used in investigations and legal proceedings (Sulaksono, 2020).

Thus, honeypots are a critical tool in the network security ecosystem, offering an additional layer of protection and in-depth insights into cyber threats. Their implementation not only aids in detecting and mitigating attacks but also enhances the awareness and capabilities of security teams in addressing the ever-evolving threat landscape.

The implementation of honeypot systems requires additional applications such as Kali Linux and Oracle VM VirtualBox. Kali Linux is used to simulate network attacks, while Oracle VM VirtualBox is used to run the Kali Linux application itself (Gatra, 2019).

2. METODHOLOGY

This study employs a quantitative method with an experimental design to compare the number of open ports between two conditions: without a honeypot and with a KF Sensor-based honeypot on Windows and MacOS devices. A honeypot is a security system designed to attract and study cyberattacks by deceiving attackers into believing they have accessed a vulnerable system. KF Sensor, as a type of honeypot, acts as bait to monitor malicious activity and collect attack data.

The research objects consist of two laptops, one running Windows and the other MacOS, configured both with and without the KF Sensor-based honeypot. The research procedure begins with the installation and configuration of KF Sensor on both laptops, creating an environment that appears vulnerable to attract attackers. Subsequently, attacks are simulated using Kali Linux, an operating system used for penetration testing and network security. Kali

Linux is equipped with various tools enabling users to conduct different types of attacks, such as port scanning and brute force attacks.

Scanning is conducted in two phases: first without the honeypot, and then with the honeypot. Data collected include the number of open ports and the types of attacks detected by the KF Sensor on both operating systems. The data are analyzed quantitatively to compare the effectiveness of the honeypot in detecting attacks on Windows and MacOS, with statistical analysis conducted to determine significant differences between the two conditions.

This research method also considers ethical standards by ensuring the privacy protection of research subjects and adhering to good scientific writing practices. Consequently, this study aims to provide insights into the use of honeypots in enhancing network security across different operating systems and to offer valuable data for the development of improved security measures.

3. RESULTS AND DISCUSSIONS

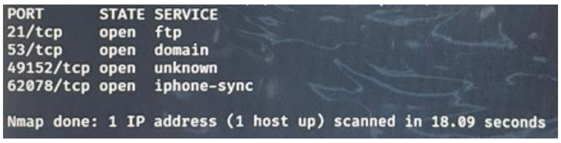
3.1. Detection of Open Port Without Honeypot (WINDOWS)

In the first phase of the study, we used Kali Linux to perform a port scan on the target laptop without utilizing the KF Sensor-based honeypot. The scan results revealed that only 4 ports were open on the laptop. The scanning process was conducted using commonly used port scanning tools, such as the command:
`nmap -sS 192.168.1.10`

The detailed scan in Figure 1 is as follows:

Target IP: 192.168.1.10
Open Ports:
- Port 21 (FTP)
- Port 53 (Domain)
- Port 49152 (Unknown)
- Port 62078 (iPhone-Sync)

These results indicate that the target laptop only has standard ports open, which are typically used for web services and remote access.



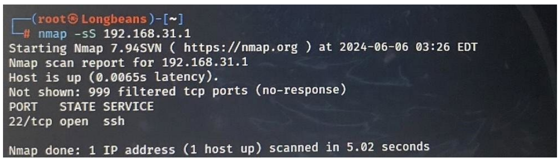
```
PORT       STATE SERVICE
21/tcp     open  ftp
53/tcp     open  domain
49152/tcp open  unknown
62078/tcp open  iphone-sync

Nmap done: 1 IP address (1 host up) scanned in 18.09 seconds
```

Figure 1. Port without HoneyPot (WINDOWS)

3.2. Detection of Open Port with KF Sensor-Based Honeypot (MAC OS)

At this stage, we continued to use Kali Linux as the port scanning tool on the target device without utilizing the KF Sensor-based honeypot.

The scan results in Figure 2 showed that the MacOS device could not be scanned via Kali Linux. This was due to the high-level security measures already in place within MacOS, which prevented us from obtaining any port information on the device (no response).



```
┌──(root㉿Longbeans)-[~]
└─# nmap -sS 192.168.31.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-06 03:26 EDT
Nmap scan report for 192.168.31.1
Host is up (0.0065s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 5.02 seconds
```

Figure 2. Port without HoneyPot (MAC OS)

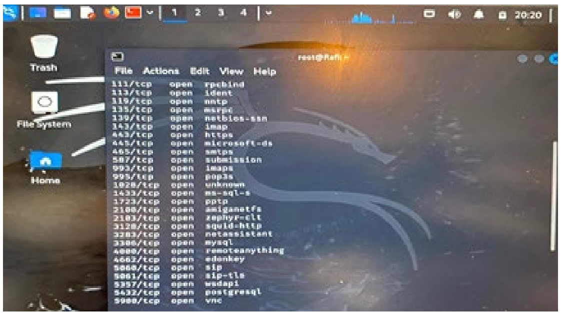
3.3. Detection of Open Port with KF Sensor-Based Honeypot (WINDOWS)

In the third phase, we activated the KF Sensor-based honeypot on the target laptop and conducted another port scan using Kali Linux. The honeypot was designed to simulate the appearance of many open services and ports to attract and study potential attacker activities.

The scan results in Figure 3 were significantly different from the previous scans. Kali Linux reported thousands of open ports on the target laptop. Below are some of the scan results:

Target IP: 192.168.1.10
Open Ports (Sample):
- Port 21 (FTP)
- Port 53 (Domain)
- Port 49152 (Unknown)
- Port 862078 (iPhone-Sync)
- Port 1000–2365 (Various fake services activated by the honeypot)

In total, more than 2,000 open ports were detected, spanning almost the entire possible range of ports.



```
111/tcp   open  rpcbind
113/tcp   open  ident
119/tcp   open  nntp
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
143/tcp   open  imap
443/tcp   open  https
445/tcp   open  microsoft-ds
465/tcp   open  smtps
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
1028/tcp  open  unknown
1433/tcp  open  ms-sql-s
1723/tcp  open  pptp
2100/tcp  open  amiganetfs
2103/tcp  open  zephyr-clt
3128/tcp  open  squid-http
3283/tcp  open  netassistant
3306/tcp  open  mysql
4000/tcp  open  remoteanything
4662/tcp  open  edonkey
5060/tcp  open  sip
5061/tcp  open  sip-tls
5357/tcp  open  wsdapi
5432/tcp  open  postgresql
5900/tcp  open  vnc
```

Figure 3. Display Port with HoneyPot (Windows)

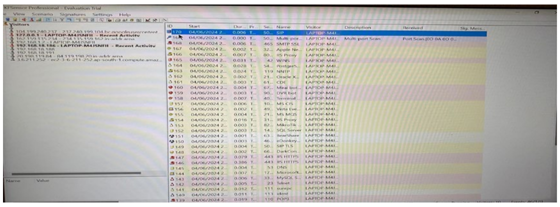
3.4. Comparative Analysis

The results from the two scanning phases revealed a significant difference in the number of detected open ports. When the KF Sensor-based honeypot was activated, the scan results showed thousands of open ports, compared to only 4 ports detected during the scan without the honeypot. This indicates that the honeypot is effective in creating the illusion of a larger and more complex network, which can mislead attackers.

Figure 4 shows display port on KF sensor.

Comparison of Open Ports:

- Without Honeypot: 4 ports
- With Honeypot: >1000 ports



Visitors

- 104.199.240.237 - 237.240.199.104.bc.googleusercontent...
- **127.0.0.1 - LAPTOP-M4JSNFII - Recent Activity**
- 162.159.135.234 - 234.135.159.162.in-addr.arpa
- 192.168.1.2 - LAPTOP-M4JSNFII
- **192.168.18.186 - LAPTOP-M4JSNFII - Recent Activity**
- 192.168.18.188
- 192.168.18.191
- 20.198.119.84 - 84.119.198.20.in-addr.arpa
- 3.6.211.252 - ec2-3-6-211-252.ap-south-1.compute.amaz...

ID	Start	Dur...	Pr...	Se...	Name	Visitor	Description	Received	Sig. Mess...
170	04/06/2024 2...	0.006	T...	50...	SIP	LAPTOP-M4J...			
169	04/06/2024 2...	0.000	T...	50...	Multi-por...	LAPTOP-M4J...	Multi-port Scan	Port Scan.[0D 0A 0D 0...	
168	04/06/2024 2...	0.006	T...	465	SMTP SSL	LAPTOP-M4J...			
167	04/06/2024 2...	0.002	T...	32...	Apple Ne...	LAPTOP-M4J...			
166	04/06/2024 2...	0.007	T...	80...	IIS Proxy	LAPTOP-M4J...			
165	04/06/2024 2...	0.031	T...	42	WINS	LAPTOP-M4J...			
164	04/06/2024 2...	0.028	T...	54...	PostgreS...	LAPTOP-M4J...			
163	04/06/2024 2...	0.024	T...	119	NNTP	LAPTOP-M4J...			
162	04/06/2024 2...	0.002	T...	21...	Oracle X...	LAPTOP-M4J...			
161	04/06/2024 2...	0.003	T...	61...	CDE	LAPTOP-M4J...			
160	04/06/2024 2...	0.004	T...	67...	Mirai bot...	LAPTOP-M4J...			
159	04/06/2024 2...	0.003	T...	90...	DVR bot	LAPTOP-M4J...			
158	04/06/2024 2...	0.007	T...	40...	Terminal ...	LAPTOP-M4J...			
157	04/06/2024 2...	0.006	T...	10...	MS CIS	LAPTOP-M4J...			
156	04/06/2024 2...	0.002	T...	49...	Vista Eve...	LAPTOP-M4J...			
155	04/06/2024 2...	0.004	T...	21...	MS MQS	LAPTOP-M4J...			
154	04/06/2024 2...	0.016	T...	31...	IIS Proxy	LAPTOP-M4J...			
153	04/06/2024 2...	0.003	T...	82...	MikroTik ...	LAPTOP-M4J...			
152	04/06/2024 2...	0.003	T...	14...	SQL Server	LAPTOP-M4J...			
151	04/06/2024 2...	0.001	T...	63...	BearShare	LAPTOP-M4J...			
150	04/06/2024 2...	0.003	T...	46...	eDonkey...	LAPTOP-M4J...			
149	04/06/2024 2...	0.004	T...	50...	SIP TLS	LAPTOP-M4J...			
148	04/06/2024 2...	0.002	T...	66...	DarkCon...	LAPTOP-M4J...			
147	04/06/2024 2...	0.079	T...	443	IIS HTTPS	LAPTOP-M4J...			
146	04/06/2024 2...	0.386	T...	443	IIS HTTPS	LAPTOP-M4J...			
145	04/06/2024 2...	0.004	T...	53	DNS	LAPTOP-M4J...			
144	04/06/2024 2...	0.007	T...	17...	Microsoft...	LAPTOP-M4J...			
143	04/06/2024 2...	0.006	T...	33...	MySQL S...	LAPTOP-M4J...			
142	04/06/2024 2...	0.005	T...	23	Telnet	LAPTOP-M4J...			
141	04/06/2024 2...	0.012	T...	111	sunrpc	LAPTOP-M4J...			
140	04/06/2024 2...	0.011	T...	113	ident	LAPTOP-M4J...			
139	04/06/2024 2...	0.019	T...	110	POP3	LAPTOP-M4J...			

Figure 4. Display port on KF Sensor

4. CONCLUSIONS

This study demonstrates that user awareness of cyber threats can be measured through phishing attack simulations, and that the KF Sensor-based honeypot is effective in creating the illusion of a more complex network to mislead attackers. These findings can be used to enhance cybersecurity education strategies and strengthen network defenses within the Faculty of Engineering at UPN Veteran Jakarta.

Data collected from phishing email simulations show varying levels of user awareness of cyber threats. Responses to phishing emails reveal differences in response time and participant success in identifying phishing threats. This highlights the effectiveness of existing cybersecurity education methods in addressing phishing threats.

The significant difference in the number of detected open ports shows that the KF Sensor-based honeypot can effectively deceive attackers by creating the illusion of multiple active services, thereby enhancing network security.

LIST OF REFERENCES

H. Wafi (2016). Implementasi Sistem Keamanan Honeypot dengan Modern Honey Network pada Jaringan Wireless.

A. Aminanto and W. Sulistyo (2019). Simulasi Sistem Keamanan Jaringan Komputer Berbasis IPS Snort dan Honeypot Artilery. *Aiti*. vol. 16, pp. 135-150.

P. Angella (2016). Implementasi Honeypot untuk Mendeteksi Serangan Distributed Denial of Service (DDoS). Universitas Kristen Satya Wacana.

W. A. Sulaksono and C. E. Suharyanto (2020). Implementasi Honeypot Sebagai Sistem Keamanan Jaringan Pada Virtual Private Server. *Infotekjar*. vol. 5, no. 1.

Gatra, H., Hendrarini, N., & Sularsa, A. (2019). Implementasi Honeypot Pada Web Server Air Traffic Control (ATC) Menggunakan KFSensor. *eProceedings of Applied Science*.

Suartana, A. (2016). Analisis Dan Implementasi Honeypot Dalam Mendeteksi Serangan Distributed Denial-Of-Services (DDOS) Pada Jaringan Wireless. *INTEGER: Journal of Information Technology*.

Supriyono, A., & Widiasari, W. (2021). Analisis Celah Keamanan Website Menggunakan Tools WEBPWN3R di Kali Linux. *Universitas PGRI Madiun*.