

Problem Description

General Context

In today's cybersecurity landscape, organizations face a growing number of cyberattacks targeting their infrastructures, systems, and data. These attacks, motivated by various reasons such as data theft, service disruption, or sabotage, jeopardize the core principles of information security: confidentiality, integrity, and availability (CIA triad). Ensuring that data is accessible only to authorized users, remains unaltered without authorization, and is available when needed is crucial for the operational continuity of any organization.

Although traditional tools like firewalls and intrusion detection systems (IDS) play a significant role, their scope can be limited. These solutions tend to focus on blocking known threats or reacting to ongoing attacks without providing a deeper understanding of attackers' tactics, techniques, and procedures (TTPs).

In this context, honeypots and Security Information and Event Management (SIEM) platforms play a key role. Honeypots not only act as decoys to attract attackers but also allow for studying their behavior in a controlled environment, offering valuable insights to anticipate future attacks. On the other hand, SIEM systems collect, analyze, and correlate event data in real-time from multiple network sources, providing a comprehensive view of threats and ensuring continuous infrastructure monitoring.

By combining these technologies, organizations can strengthen their defenses, improving both detection and incident response while protecting the core pillars of the CIA triad against an ever-evolving threat landscape.

Theoretical Framework

1. Cybersecurity and Cyber Threats

Technology has transformed the way of living in most societies, drastically improving the quality of life. However, the use of digital technology can sometimes backfire against the user, whether a person, a company, or even a government. As the internet increases human interaction and enhances social relationships, it becomes a double-edged sword since cyberspace has no boundaries and can facilitate illegal activities. (Raufo, Tsado & Ben-Edet, 2021) Cybersecurity encompasses a set of practices, technologies, and controls designed to protect systems and data from unauthorized access, attacks, and damage.

Types of threats include:

- **Brute force attacks:** Automated attempts to discover access

credentials.

- **Exploits:** Use of known vulnerabilities to compromise a system.
- **Malware:** Malicious software designed to harm or compromise devices.

The detection and analysis of these threats are essential components for mitigating risks and minimizing the impact of security incidents.

2. Honeypots: Concept and Classification

A honeypot is a cybersecurity system designed to simulate real vulnerabilities and attract attackers. Honeypots have three main functionalities: (1) Detection, (2) Prevention, and (3) Research. (Javadpour et al., 2024)

They are classified as:

- **Low-Interaction Honeypots:** Simulate basic services and are safer but provide limited data.
- **High-Interaction Honeypots:** Simulate full systems, offering richer data but posing greater risks if compromised.

Honeypots allow:

- Identifying emerging attack vectors.
- Analyzing attackers' tactics and tools.
- Diverting threats away from real systems.

3. Log Analysis and Data Collection

Logs are records generated by the honeypot that document every interaction. Their analysis allows:

- Identifying patterns in attack attempts.
- Recognizing suspicious IP addresses.
- Classifying attack techniques, such as command injections or port scanning.

4. Selected Tools

In this project, the following tools were used:

- **VMware Workstation Pro:** For network configuration.
- **syslog-ng:** To store logs of attempted access by attackers.
- Services: **HTTP** (with its respective webpage and login), **SSH**, and **FTP**.



The attacker will use Hydra to discover the (intentionally weak) password, SSH, and FTP to compromise the machine.

Project Objectives

General Purpose of the Project

This project is conducted to provide a controlled and secure environment for studying attack attempts targeting simulated services. It aims to identify patterns, methods, and tools used by attackers, offering a better understanding of current threats and helping organizations and professionals strengthen their cybersecurity defenses.

- **Why is this project being conducted?**

To identify and analyze attack tactics, improve security strategies, and generate knowledge about emerging threats.

What problem does it aim to solve?

The lack of proactive tools that allow for collecting detailed data on attack attempts in real time and understanding the behavior of attackers.

General Objective

Design, implement, and deploy a honeypot that allows for detecting, recording, and analyzing attack attempts.

Specific Objectives

1. Configure a secure and functional honeypot environment.
2. Record and collect data from attack attempts.
3. Analyze the collected data.

Project Methodology

The methodology of this project focused on the design, implementation, and analysis of a honeypot as a tool for detecting and studying cyberattacks. This process required the integration of various tools and techniques to simulate a realistic network environment that would attract attackers. The methodological strategy ensures that the objectives set are achieved in a structured, precise, and replicable manner.

1. Methodological Approach

The approach followed in this project is experimental and analytical, as a controlled environment was designed and configured to capture information about potential attack attempts. The process involves three main phases:

- **Planning:** The honeypot architecture is designed, considering the essential elements to simulate a realistic environment (internal network, fake services, and attacker network).
- **Implementation:** The technological elements are configured, including the honeypot, simulated services (HTTP, FTP, SSH), and the IDS/EDR system for data collection and analysis.
- **Data Collection and Analysis:** The collected data is processed to identify attack patterns, evaluate vulnerabilities, and draw useful conclusions to strengthen the security of real networks.
- **Evaluation and Presentation:** Results are analyzed and conclusions are drawn.

2. Procedures and Techniques

• Planning the Environment

- **Identification of Necessary Components:** Honeypot (SSH, FTP, and HTTP services), internal network, and attacker network.
- **Definition of IP Addresses and Subnets for Simulation:** 172.16.0.0/24 for the internal network, including the honeypot, and 192.168.1.0/24 for the attacker network.

2. Honeypot Configuration:

- Use of tools like SSH, FTP, and a simulated HTTP server.
- Configuration of detailed logs to record connection attempts, fake credentials, and executed commands.

3. Simulation of the Attacker Network:

- Implementation of the host machine representing the attackers, equipped with tools such as Nmap and Hydra to perform controlled attack tests.

4. Implementation of the Log Collection System:

- Integration with a log analysis server (syslog-ng).

5. Data Capture and Analysis:

● Log Collection from Each Honeypot Component

- Use of analysis tools to identify patterns in attack attempts.

1. Detailed Architecture Design

The diagram describes a segmented network architecture using virtual machines in VMware and a Honeypot as a decoy (see diagram):

1. Honeypot (NAT “published”):

- Configured in a public network with rules allowing external access (through NAT), but traffic to private servers is restricted. The honeypot is set up to attract attackers.

2. Production Server (vnet “private”):

- Real and management servers are in a private network, isolated from direct external traffic. Firewall iptables commands protect this network by blocking unwanted connections.

3. Management Server (IT ADMIN vnet “private”):

- Simulates the origin of cyberattacks.
- The attacker machine (192.168.1.210) runs tools like Nmap to interact with the honeypot.

1. 1. Log System:

- Monitors all traffic between the networks and logs suspicious events for analysis.

This design allows for simulating a realistic environment where attackers interact with fake services, generating valuable data for analysis.

2. Justification

The methodology applied ensures that the specific objectives of the project are achieved in a structured and effective manner.

- The separation into networks (internal, honeypot, and attacker) replicates a typical business environment, making it easier to identify vulnerabilities and analyze attack patterns.
- Simulating an attacker provides a realistic context to assess the effectiveness of the honeypot.
- Analyzing the collected data will help identify common attack methods and security recommendations applicable to real networks.

1. Timeline

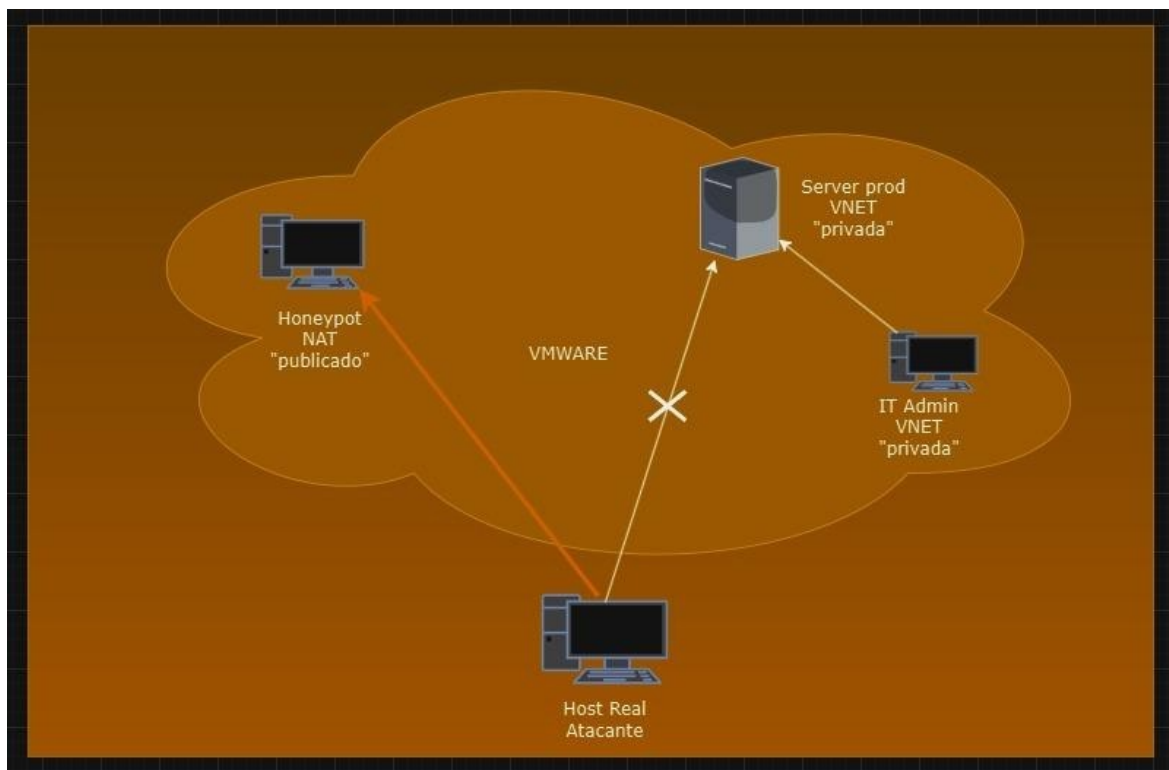
Fase	Actividad	Duración estimada	Descripción
Preparation	Environment Configuration	1 day	Installation of OS (Linux). Basic network configuration. System and necessary dependencies update.
Honeypot	Implementation	1 day	Configure SSH service. Implement FTP service. Create a fake web server for HTTP honeypot.
Internal Network	Configuration of Internal Services	1 day	Implement a basic internal web server. Adjust firewall to protect the internal network.
IDS and logs system	Installation y configuration	1 day	Configure log system to monitor traffic on both subnets. Create custom rules. Verify logs and alerts.
Attacker network	Installation of Testing Tools	1 day	Configure machines with Nmap, Hydra, and the necessary tools. Prepare attack scripts to test vulnerabilities.
tests	Validation of All Components	1 day	Simulate attacks from the attacker network. Review honeypot logs to validate detections.
Documentation	Generate Final Reports	1 day	Summarize configurations. Present results of security tests.

The services offered in the honeypot were:

- **HTTP (Hypertext Transfer Protocol):** It is the protocol that allows web browsers to communicate with servers to display web pages. In short, it is the foundation of the web.
- **FTP (File Transfer Protocol):** It is used to transfer files between a computer (client) and a server. In other words, it is used for uploading and downloading files.

- **SSH (Secure Shell):** It is a protocol that allows secure remote access and control of another computer. It is like a remote command line, but with encryption to protect the communication.

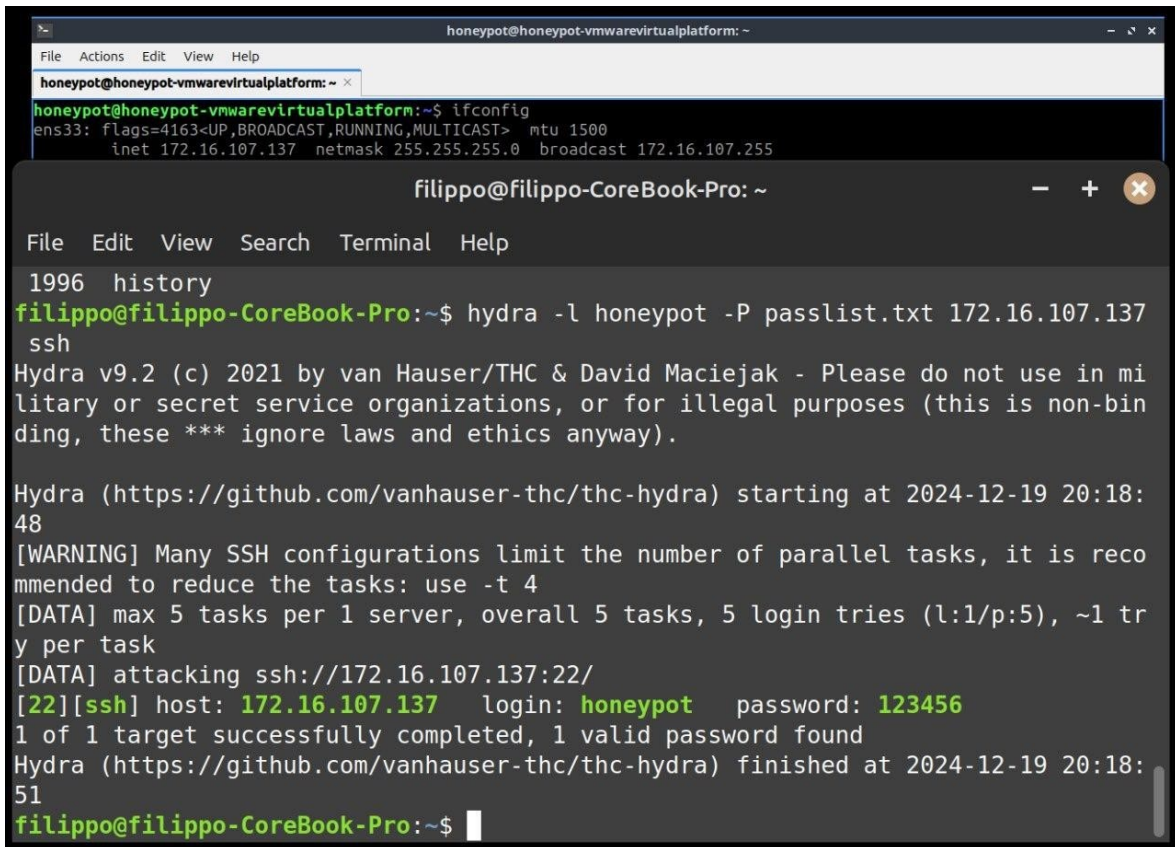
Configuration



Own Image: ZFA Honeypot Topology

It can be seen that there are two private network segments, while the honeypot is public, meaning that the services are exposed for the attacker to access. However, the attacker cannot access the server, which in turn allows connections with the IT Admin.

Results



The image shows two terminal windows. The top window, titled 'honeypot@honeypot-vmwarevirtualplatform: ~', displays the output of the 'ifconfig' command for the 'ens33' interface, showing an IP address of 172.16.107.137. The bottom window, titled 'filippo@filippo-CoreBook-Pro: ~', shows the execution of a Hydra brute force attack. The command used is 'hydra -l honeypot -P passlist.txt 172.16.107.137 ssh'. The output indicates that the attack was successful, finding the password '123456' for the 'honeypot' user on the target host.

```
honeypot@honeypot-vmwarevirtualplatform: ~  
File Actions Edit View Help  
honeypot@honeypot-vmwarevirtualplatform: ~  
honeypot@honeypot-vmwarevirtualplatform:~$ ifconfig  
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet 172.16.107.137 netmask 255.255.255.0 broadcast 172.16.107.255  
  
filippo@filippo-CoreBook-Pro: ~  
File Edit View Search Terminal Help  
1996 history  
filippo@filippo-CoreBook-Pro:~$ hydra -l honeypot -P passlist.txt 172.16.107.137  
ssh  
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in mi  
litary or secret service organizations, or for illegal purposes (this is non-bin  
ding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-19 20:18:  
48  
[WARNING] Many SSH configurations limit the number of parallel tasks, it is reco  
mmended to reduce the tasks: use -t 4  
[DATA] max 5 tasks per 1 server, overall 5 tasks, 5 login tries (l:1/p:5), ~1 tr  
y per task  
[DATA] attacking ssh://172.16.107.137:22/  
[22][ssh] host: 172.16.107.137 login: honeypot password: 123456  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-12-19 20:18:  
51  
filippo@filippo-CoreBook-Pro:~$
```

Own Source: Brute Force Attack to Discover SSH Password

Attacker AS/N - Top 10 - Dynamic			Src IP - Top 10 - Dynamic		Cowrie Input - Top 10	
AS	ASN	Count	Source IP	Count	Command Line Input	Count
3462	Data Communic	38,632	183.91.160.89	1,854	shell	3,534
14061	DIGITALOCEAN	3,746	117.50.213.252	1,723	system	3,534
4134	Chinanet	3,358	116.193.222.195	1,281	enable	1,767
210644	Aeza Internatio	2,658	103.100.159.215	1,252	sh	1,767
138968	rainbow networ	2,489	47.239.233.10	1,249	ping ;sh	1,754
8075	MICROSOFT-CO	2,487	123.205.121.86	1,248	/bin/busybox wget --he	1,666
131127	GLOBAL TECHN	1,854	103.119.3.35	1,246	cat /proc/mounts grep	1,666
4808	China Unicom B	1,836	134.209.31.107	1,246	cat /proc/mounts grep	1,666
136052	PT Cloud Hostir	1,714	20.127.141.235	1,246	echo -e \x67\x61\x79\x	1,666
16276	OVH SAS	1,593	45.150.32.168	1,246	for i in	1,666

Own Source: IP addresses and internet providers of cybercriminals, and the most commonly used commands once the machine is compromised.

Conclusions

It is undeniable that cybersecurity is one of the fields with the most ongoing development, advancing alongside the growth of other technologies. Day by day, cyberattacks increase dramatically, and it is essential to implement and update prevention, detection, and response systems.

Honeypots set a trend and serve as an effective tool to enhance cybersecurity in many organizations. With these, the primary focus is on studying the behavior of cybercriminals, and therefore, appropriate measures are taken based on the observed behaviors. This helps to safeguard the organization's real systems or services to prevent disruptions, errors, and abrupt leaks caused by cybercrime that could jeopardize business continuity.

References

Abiodun Raufu, Lucy Tsado, Emmanuel Ben-Edet. International Journal of Law, Crime and Justice, Volume 64, 2021, 100454, ISSN 1756-0616, <https://doi.org/10.1016/j.ijlcrj.2020.100454>.
(<https://www.sciencedirect.com/science/article/pii/S1756061620304894>)

Amir Javadpour, Forough Ja'fari, Tarik Taleb, Mohammad Shojafar, Chafika Benzaïd. A comprehensive survey on cyber deception techniques to improve honeypot performance. Computers & Security, Volume 140, 2024, 103792, ISSN

0167-4048.<https://doi.org/10.1016/j.cose.2024.103792>.
(<https://www.sciencedirect.com/science/article/pii/S0167404824000932>)

Niclas Ilg, Paul Duplys, Dominik Sisejkovic, Michael Menth. A survey of contemporary open-source honeypots, frameworks, and tools. Journal of Network and Computer Applications, Volume 220, 2023, 103737, ISSN 1084-8045. <https://doi.org/10.1016/j.jnca.2023.103737>.
(<https://www.sciencedirect.com/science/article/pii/S108480452300156X>)