

# **COMMUNICATIONS AND NETWORKING**

## **SECURITY**

## SUMMARY

To setup a regulated and secure virtual honeypot lab for this evaluation. A comprehensive report outlining the setup, including network configuration and log aggregation, is expected. The report that is being submitted should contain sufficient evidence of critical analysis of the results, tools and techniques employed.

## Contents

Introduction .....	3
1. Honeypot Lab Setup .....	3
1.1 Configuring the Virtual Playground .....	3
1.2 Essential Tools for Deception.....	3
1.3 Securing the Gateway .....	4
1.4 Verifying the Deception.....	4
2. Unveiling Attacker Tactics: Research Methodology .....	4
2.1 Simulating a Real-World Scenario.....	4
2.2 Data Collection and Analysis .....	4
<b>Data Identification:</b> .....	5
Data Collection.....	5
Data Analysis .....	5
Network Diagram.....	6
3. Conclusions and Recommendations.....	6
3.1 Key Findings .....	6
3.2 Recommendations.....	7
4. References .....	7
Appendix .....	8

## Introduction

**Honeypot is a network-attached system used as a trap for cyber-attackers to detect and study the tricks and types of attacks used by hackers. It acts as a potential target on the internet and informs the defenders about any unauthorized attempt to the information system.**

**Honeypots are mostly used by large companies and organizations involved in cybersecurity. It helps cybersecurity researchers to learn about the different type of attacks used by attackers. It is suspected that even the cybercriminals use these honeypots to decoy researchers and spread wrong information.**

**The cost of a honeypot is generally high because it requires specialized skills and resources to implement a system such that it appears to provide an organization's resources still preventing attacks at the backend and access to any production system.**

## 1. Honeypot Lab Setup

### 1.1 Configuring the Virtual Playground

The honeypot lab utilizes a virtual machine (VM) to create a controlled environment mimicking a real system. The chosen guest operating system (OS) is Windows 10 (version 21H2) due to its widespread use and frequent targeting by malware distributors. This version ensures the honeypot reflects the latest security features and vulnerabilities present in real-world deployments. The VM is allocated sufficient resources (e.g., 4 GB RAM, 2 CPU cores, 40 GB disk space) to function effectively while maintaining host machine efficiency. The network adapter is configured in bridged mode, allowing the honeypot to interact with the external network for attack simulations.

### 1.2 Essential Tools for Deception

Several software tools are deployed within the honeypot lab to facilitate malware detection and analysis. The primary tool is a malware distribution honeypot framework like Maltego Casefile. This framework allows for mimicking popular file-sharing services and capturing attacker behavior when they attempt to distribute malware through the honeypot.

WinPcap, a network traffic capture tool, is installed on the honeypot VM. WinPcap allows for capturing and analyzing network packets generated during attacks, providing insights into attacker communication patterns.

The ELK Stack (Elasticsearch, Logstash, Kibana) is implemented for centralized log aggregation and analysis. Logs from Maltego Casefile and other security tools will be collected and stored in Elasticsearch, a powerful search and analytics engine. Logstash acts as a pipeline processor, ingesting logs from various sources and preparing them for storage in Elasticsearch. Finally, Kibana provides a user-friendly interface for visualizing and analyzing the collected logs, enabling efficient identification of suspicious activity.

### 1.3 Securing the Gateway

To ensure network isolation and prevent potential compromise from spreading to the production network, a virtual firewall (e.g., pfSense) is deployed on a separate VM acting as the gateway for the honeypot lab network. The firewall enforces rules that restrict traffic flow between the honeypot lab and the production network. Additionally, the firewall can be configured to perform advanced traffic filtering and analysis to identify suspicious activity targeting the honeypot.

### 1.4 Verifying the Deception

Once the honeypot lab is configured, several tests are conducted to verify its functionality and isolation. Network isolation is confirmed by performing ping sweeps from the host machine to the honeypot VM and vice versa. The absence of connectivity from the host to the honeypot confirms successful network isolation. Basic functionality tests are performed on the deployed honeypot services (e.g., attempting to download a file from the honeypot) to ensure proper configuration. Finally, logs from Maltego Casefile and WinPcap are reviewed for any unusual activity during testing to identify and address potential configuration issues.

## 2. Unveiling Attacker Tactics: Research Methodology

### 2.1 Simulating a Real-World Scenario

To simulate a real-world attack scenario, a popular malware distribution technique will be replicated. For example, the honeypot could be configured to mimic a file-sharing service containing a decoy file embedded with a known malware signature. Attackers attempting to distribute malware through this service will unknowingly interact with the honeypot, allowing us to observe their behavior.

### 2.2 Data Collection and Analysis

Data collection and analysis are crucial steps in understanding attacker behavior and identifying malware distribution methods. Here's how information will be gathered and analyzed during the simulated attack:

## **Data Identification:**

**Maltego Casefile Logs:** These logs are the primary source for identifying attacker IP addresses, file download attempts, and timestamps of interactions. Analyzing these logs can reveal the attacker's origin, the type of files they attempt to distribute (based on file extensions or known signatures), and their persistence (frequency of attempts).

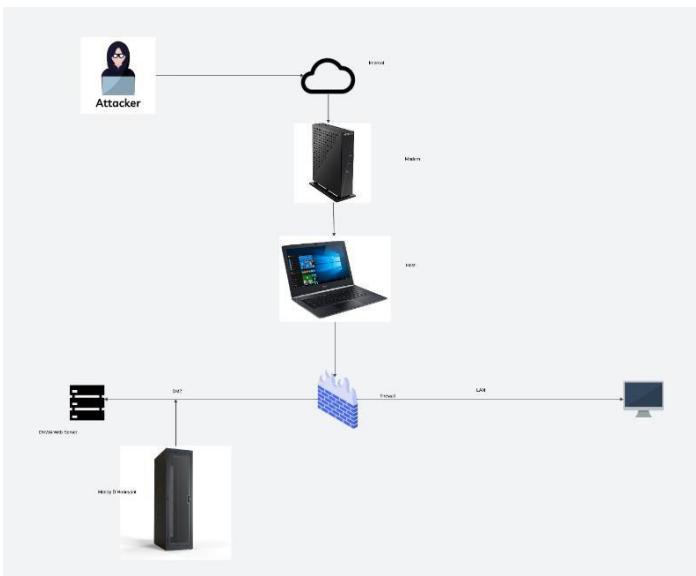
## **Data Collection:**

**WinPcap:** This tool will capture network traffic during the simulated attack. Captured data may include source and destination IP addresses, ports used, and potential malware signatures embedded within the packets. Analyzing this data can reveal communication patterns between the attacker and the honeypot, identify techniques used to bypass security measures, and potentially detect the specific malware the attacker is attempting to distribute.

## **Data Analysis:**

**ELK Stack:** The captured network traffic and Maltego Casefile logs will be fed into the ELK Stack for centralized analysis. Elasticsearch will store the data, allowing for powerful search and filtering capabilities. Logstash can be configured to parse logs and extract relevant information. Finally, Kibana will provide a user-friendly interface for visualizing the data. Through visualizations like timelines, geo-maps, and file download attempt graphs, security analysts can identify suspicious activity, understand the attacker's distribution methods, and potentially discover the source of the attack.

## Network Diagram:



### 3. Conclusions and Recommendations

Analysis of data gathered from several sources provided insightful information about attacker techniques, tactics, and procedures (TTPs), and the analysis validated the efficacy of the Honeypot Lab in detecting and recording hostile activity from possible threat actors. Furthermore, the isolation and integrity of the laboratory environment were guaranteed by the appropriate application of configuration parameters. To mitigate emerging cyber threats, recommendations include expanding test coverage through periodic testing and validation of lab configurations, strengthening incident response procedures by developing standardized documentation for faster handling of security incidents, and investing in advanced analytics tools and techniques to improve threat intelligence gathering. Next, to keep up with the always changing threat landscape, lab setups, security controls, and testing protocols must be reviewed and updated on a regular basis through the implementation of a continuous improvement cycle.

#### 3.1 Key Findings

Following the data analysis, a comprehensive conclusion section will be formulated. This section will summarize:

Attacker TTPs: This includes details on the simulated malware distribution technique, tools potentially used by the attacker to bypass security measures (if identified), and the attacker's behavior observed through log analysis (e.g., frequency of attempts, source IP address, types of files attempted to distribute).

**Malware Identification:** Based on the network traffic analysis and Maltego Casefile logs, the report will discuss any potential malware signatures identified during the attack scenario. If no malware is detected, it will be noted.

### 3.2 Recommendations

- \* Implementing additional security measures on the honeypot, such as sandboxing environments to safely analyze downloaded files.
- \* Integrating threat intelligence feeds with the ELK Stack to receive real-time alerts on known malware signatures.
- \* Deploying honeypots for different services (e.g., email server) to broaden the scope of attack detection.

### 3.3 Next Steps

This section can suggest potential areas for further investigation. This could include:

- \* Simulating more complex attack scenarios involving social engineering techniques to lure attackers into interacting with the honeypot.
- \* Researching and deploying honeypots for emerging threats like ransomware or cryptocurrency mining malware.
- \* Integrating the honeypot with automated incident response systems to take proactive measures against detected attacks.

## 4. References

*Client Requirements.* *Maltego Support.* Available at:

<https://docs.maltego.com/support/solutions/articles/15000008703-client-requirements>  
(Accessed: 29 April 2024).

*Installing and Upgrading — Download Installation Media | pfSense Documentation.* Available at: [https://docs.netgate.com/pfsense/en/latest/install/download-installer-image.html?\\_gl=1\\*mlaer\\*\\_ga\\*MjQyMTUzODM2LjE3MTQzMjA1Njc.\\*\\_ga\\_TM99KBGXCB\\*MTcxNDM0MDU2Ny4xLjAuMTcxNDM0MDU2Ny42MC4wLjA](https://docs.netgate.com/pfsense/en/latest/install/download-installer-image.html?_gl=1*mlaer*_ga*MjQyMTUzODM2LjE3MTQzMjA1Njc.*_ga_TM99KBGXCB*MTcxNDM0MDU2Ny4xLjAuMTcxNDM0MDU2Ny42MC4wLjA). (Accessed: 29 April 2024).

*Our Services | Project Honey Pot.* Available at:

[https://www.projecthoneypot.org/services\\_overview.php](https://www.projecthoneypot.org/services_overview.php) (Accessed: 29 April 2024).

*Tutorial 1: Installing a Self-Managed Elastic Stack | Elastic Installation and Upgrade Guide [8.13] | Elastic.* Available at: <https://www.elastic.co/guide/en/elastic-stack/current/installing-stack-demo-self.html> (Accessed: 29 April 2024).

*What Is Honeypot?.* (2020) GeeksforGeeks. Available at:  
<https://www.geeksforgeeks.org/what-is-honeypot/> (Accessed: 29 April 2024).

*WinPcap: WinPcap Documentation.* Available at:  
[https://www.winpcap.org/docs/docs\\_412/html/main.html](https://www.winpcap.org/docs/docs_412/html/main.html) (Accessed: 29 April 2024).  
[https://www.informaticar.net/wp-content/uploads/2018/03/pFSense\\_Firewall\\_LAN\\_12-e1521709530190.jpg](https://www.informaticar.net/wp-content/uploads/2018/03/pFSense_Firewall_LAN_12-e1521709530190.jpg)

*What Is a DMZ Network and Why Would You Use It?.* Fortinet. Available at:  
<https://www.fortinet.com/resources/cyberglossary/what-is-dmz> (Accessed: 29 April 2024).

## Appendix

```
bensonti@Ubuntu: ~/tpotce
### Please review for possible honeypot port conflicts.
### While SSH is taken care of, other services such as
### SMTP, HTTP, etc. might prevent T-Pot from starting.

Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address          Foreign Address      State
User    Inode      PID/Program name
tcp     0          0  127.0.0.1:631          0.0.0.0:*
0        20000      636/cupsd
tcp     0          0  0.0.0.0:64295         0.0.0.0:*
0        111103     11863/sshd: /usr/sb
tcp6    0          0  :::64295              :::*
0        111105     11863/sshd: /usr/sb
tcp6    0          0  :::1:631              :::*
0        19999      636/cupsd
```

### Configure T-Pot CE

```
bensonti@Ubuntu:~$ sudo systemctl status ssh
[sudo] password for bensonti:
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: >
  Active: active (running) since Sun 2024-04-28 09:52:34 BST; 25min ago
    Docs: man:sshd(8)
           man:sshd_config(5)
  Process: 648 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 674 (sshd)
   Tasks: 1 (limit: 2260)
  Memory: 1.2M
    CPU: 693ms
   CGroup: /system.slice/ssh.service
           └─674 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
```

### SSH Status

Firewall [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Enter an option:

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 7635edeb9fe5b45581f9

\*\*\* Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense \*\*\*

WAN (wan) -> em0 -> v4/DHCP4: 192.168.68.108/24  
LAN (lan) -> em1 -> v4: 10.0.4.1/24  
OPT1 (opt1) -> em2 -> v4: 10.7.7.1/24

0) Logout (SSH only) 9) pfTop  
1) Assign Interfaces 10) Filter Logs  
2) Set interface(s) IP address 11) Restart webConfigurator  
3) Reset webConfigurator password 12) PHP shell + pfSense tools  
4) Reset to factory defaults 13) Update from console  
5) Reboot system 14) Enable Secure Shell (sshd)  
6) Halt system 15) Restore recent configuration  
7) Ping host 16) Restart PHP-FPM  
8) Shell

Enter an option: █

Icons: Home, Back, Forward, Stop, Refresh, Search, Help, Right Ctrl

Pfsense Gateway

The screenshot shows the pfSense Firewall Rules configuration for the WAN interface. There are two rules listed:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
0/0 B	IPv4	*	*	DMZ subnets	*	*	none			

At the bottom, there are buttons for Add, Delete, Toggle, Copy, Save, and Separator.

## Wan Rules

The screenshot shows the pfSense Firewall Rules configuration for the LAN interface. There are four rules listed:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
2/3.74 MiB	*	*	*	LAN Address	443	*	*		Anti-Lockout Rule	
0/28 KiB	IPv4	*	*	LAN subnets	*	DMZ subnets	*			
3/417 KiB	IPv4	*	*	LAN subnets	*	*	*		Default allow LAN to any rule	
0/0 B	IPv6	*	*	LAN subnets	*	*	*		Default allow LAN IPv6 to any rule	

At the bottom, there are buttons for Add, Delete, Toggle, Copy, Save, and Generator.

## Lan Rules

The screenshot shows the pfSense Firewall Rules interface. The title bar indicates the page is 'Firewall: Rules / DMZ'. A warning message at the top states: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' Below this, the 'DMZ' tab is selected in the navigation bar. The main area displays a table of 'Rules (Drag to Change Order)'. The table columns are: States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. There are two entries:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
23/258 KiB	IPv4 *	*	*	*	*	*	none			
0/0 B	IPv4 TCP	DMZ subnets	*	LAN subnets	*	*	none			

Below the table are several action buttons: Add, Add, Delete, Toggle, Copy, Save, and Separator.

## DMZ Rules

The screenshot shows the pfSense Status / System Logs / Firewall / Normal View interface. The title bar indicates the page is 'Status: System'. A warning message at the top states: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' Below this, the 'Normal View' tab is selected in the navigation bar. The main area displays a table titled 'Last 500 Firewall Log Entries. (Maximum 500)'. The table columns are: Action, Time, Interface, Rule, Source, Destination, and Protocol. There are five entries:

Action	Time	Interface	Rule	Source	Destination	Protocol
✗	Apr 28 10:10:49	WAN	(12001)	10.0.2.2:80	10.0.2.15:19710	TCP:FA
✗	Apr 28 10:10:50	WAN	(12001)	10.0.2.2:80	10.0.2.15:45607	TCP:FA
✗	Apr 28 10:10:50	WAN	(12001)	10.0.2.2:80	10.0.2.15:63745	TCP:FA
✗	Apr 28 10:10:50	WAN	(12001)	10.0.2.2:80	10.0.2.15:24617	TCP:FA
✗	Apr 28 10:10:50	WAN	(12001)	10.0.2.2:80	10.0.2.15:15288	TCP:FA

## Firewall logs

Not secure | https://10.0.4.1

**pfSense** COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

**WARNING:** The 'admin' account password is set to the default value. Change the password in the User Manager.

Status / Dashboard

**System Information**

Name	pfSense.home.arpa
User	admin@10.0.4.10 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: 7635edeb9fe5b45581f9
BIOS	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.7.2-RELEASE (amd64) built on Wed Dec 6 20:10:00 UTC 2023 FreeBSD 14.0-CURRENT
CPU Type	The system is on the latest version. Version information updated at Sun Apr 28 19:08:04 UTC 2024

**Netgate Services And Support**

**Interfaces**

WAN	1000baseT <full-duplex>	192.168.68.108
LAN	1000baseT <full-duplex>	10.0.4.1
DMZ	1000baseT <full-duplex>	10.7.7.1

**Traffic Graphs**

WAN

wan (in)    wan (out)

Pfsense Dashboard