DEPLOYMENT OF A HONEYPOT SYSTEM FOR CYBER-ATTACK DETECTION

BY

NTEWO TOYO
20/SCI01/081

ALOBA SUAD
21/SCI01/075

SUPERVISOR:
Mr. FEMI SANYA

MAY, 2023

Outline

01

Background

The concept of honeypots has a rich history dating back decades and has gained significant attention in recent years. Originally articulated by Spitzner in 2002 as a security resource intentionally probed or attacked, honeypots, Honeypots can also be described as virtual decoys strategically placed to mimic real systems.

02

Problem Statement

Traditional security measures like Intrusion Detection Systems (IDS) and firewalls aim to detect abnormal activities, but they often struggle with high false alarm rates and lack sufficient detail in generated alerts for effective analysis. This limitation means that security teams may spend valuable time investigating false positives, diverting attention from genuine threats.

03

Aim & Objectives

This project Aims to design and implement a honeypot system for cyber-attack detection.

Objectives:

1. To Implement a honeypot system in a controlled environment (cloud server).
2. To analyse the data on attacker activities and footprints stored in the log.
3. Give valuable insights into the behaviors and methodologies of attackers from the analyzed log in (2) to enable more effective and efficient response.

03

Methodology

Our methodology entails a systematic approach across three key stages.

Firstly,

In Cloud Platform selection:

A comprehensive evaluation based on scalability, availability, performance, and compliance. This involves accessing factors like data center locations, network traffic and adherence to data sovereignty regulations, alongside evaluating support for virtual machines, containers, and networking capabilities.

After the platform selection, we proceed with the **Installation and Configuration** of honeypot software on cloud-hosted VMs or containers, tailoring configurations to simulate diverse services and protocols while implementing stringent security measures.

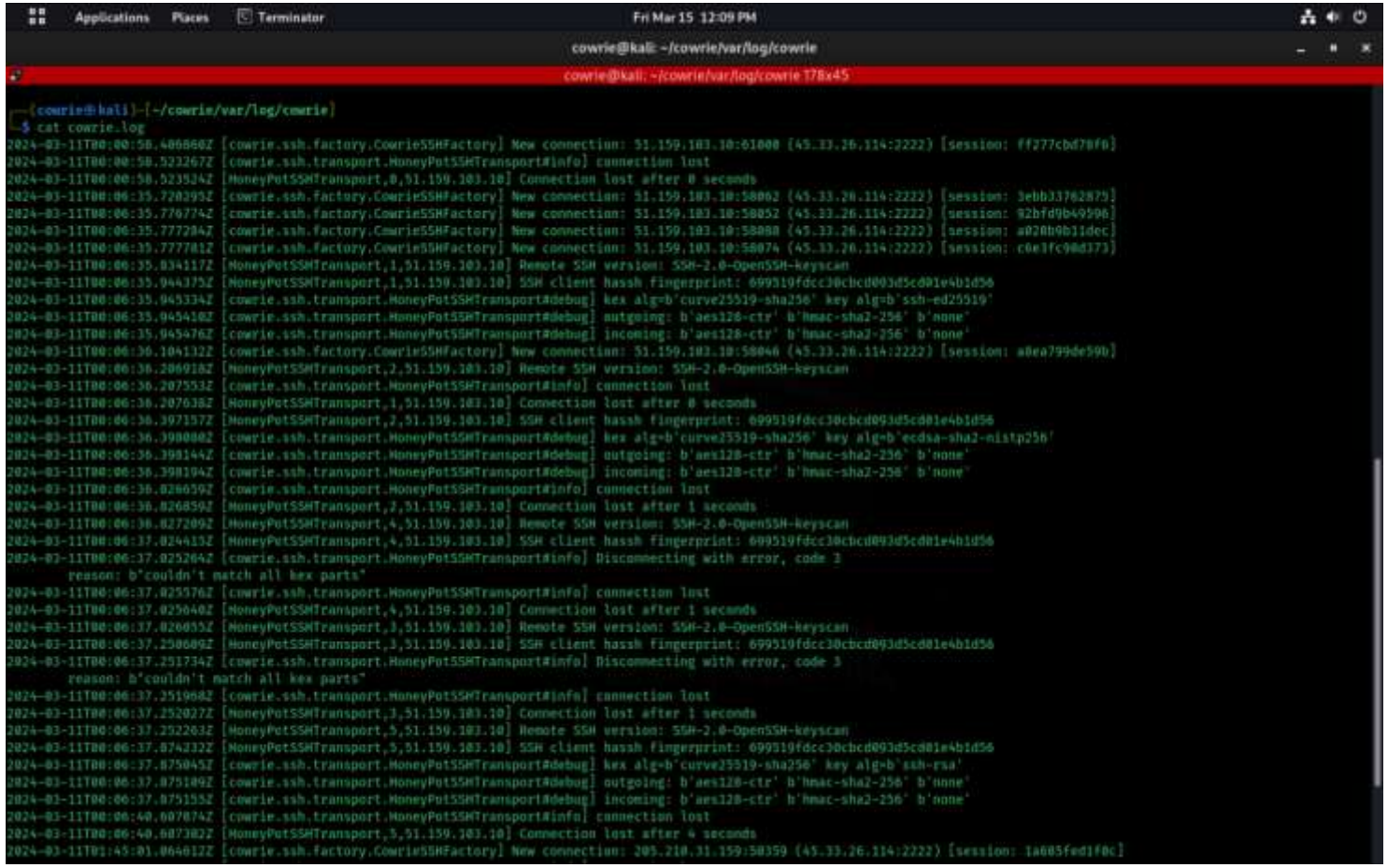
04

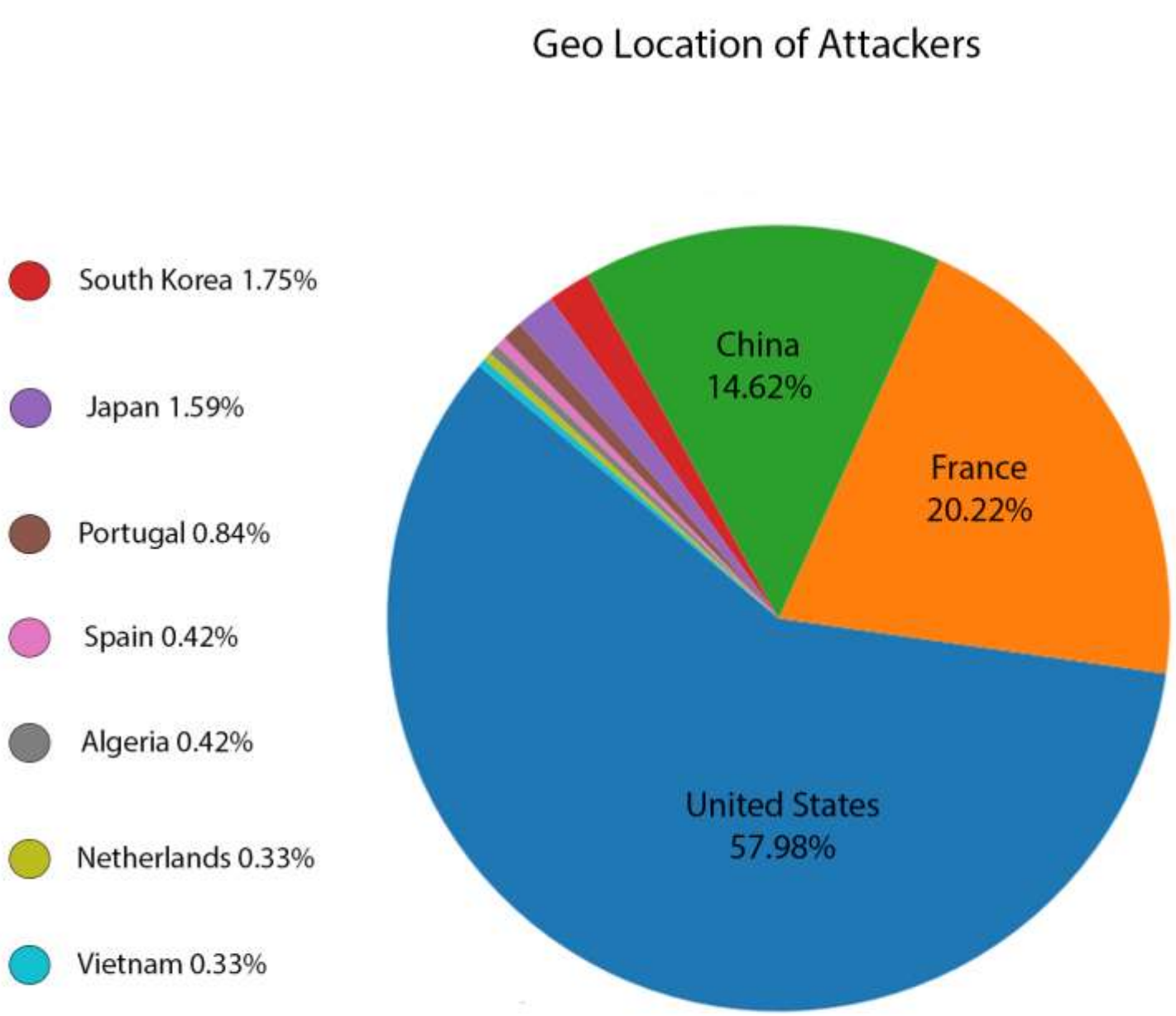
Literature Review

Paper	Method Detail	Mitigated attacks	Vulnerabilities/Limitations
(Kapczynski and Lawnik, 2019)	Using cyphers with adjusting key lengths	This system is built to withstand a variety of assaults, including plaintext, related-key, and side-channel attacks.	Execution space and time are greatly expanded.
(Aggarwal and Maurer, 2016)	Utilising the generic ring method for RSA factoring	RSA's reduction of factoring problems	Various attacks involving cryptoanalysis are feasible.
(Hwang et al, 2016)	Certificates are encrypted with pairless cryptography.	Defends against assaults by employing specific cypher messages	The design is vulnerable to Denial-of-Service assaults since it depends so heavily on bandwidth.

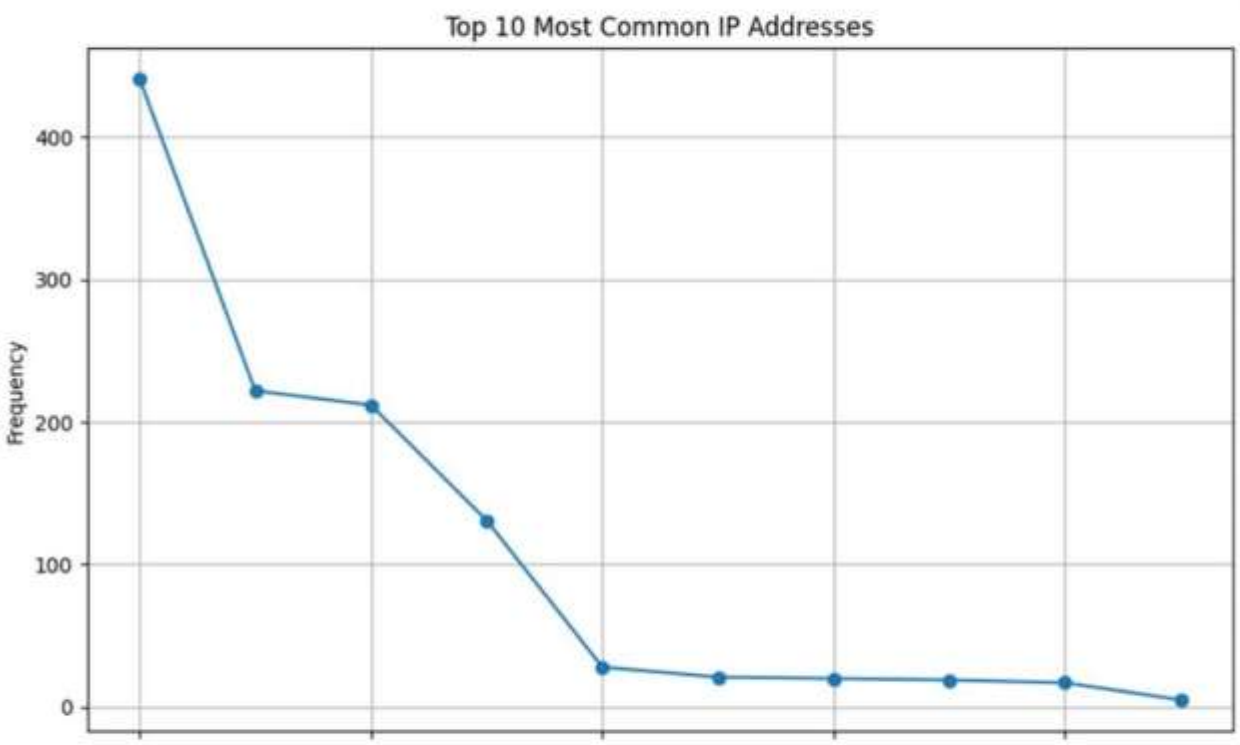
05

System Analysis





According to the system log data, the United States accounted for the highest proportion of attempted system accesses, comprising 57.98%. Following closely behind, France constituted 20.22%, with China contributing 14.62%. It's noteworthy that a significant portion of these access attempts originated from Asia and Europe, indicating a widespread presence of potential attackers across these regions



Top 10 Most Common IP Addresses

1. 154.27.68.195 (441)
2. 138.68.224.69 (222)
3. 51.15.17.105 (212)
4. 219.134.218.250 (131)
5. 51.83.75.133 (28)
6. 103.20.248.188 (21)
7. 13.125.39.155 (20)
8. 111.167.211.169 (19)
9. 122.131.191.170 (17)
10. 188.78.242.233 (5)

In the log data, specific IP addresses stand out for their persistent attempts to intrude. Notably, IP address 154.27.68.195 recorded the highest number of attempts, totaling 441. Following closely behind is 138.68.224.69, which made 222 attempts, trailed by 51.15.17.105 with 212 attempts, and 219.134.218.250 with 131 attempts. These repeated intrusion attempts from these IPs raiseconcerns about potential security vulnerabilities and the need for enhanced protective measures.

06

Data Analysis result summary

CATEGORY	DESCRIPTION	RESULT
Basic information	Shape of the dataset	1197 * 10
Basic information	Column names	id, ymd, time, session, from_ip_address, to_ip_address, username, password, success, country
Basic information	Data types of columns	Integer & Object
Summary Statistics	Number of records	1197
Counting Values	Counts of success values	Failed: 869, Successful: 328
Counting Values	Counts of country values	United States: 694, France: 242, China: 175, South Korea: 21
Missing Values	Missing values in each column	password: 3
Successful Logins	Successful logins by username	admin: 15, oracle: 28, root: 218, ubuntu: 17

REFERENCES

- **Akkaya, D., & Thalgott, F. (2010)**. Honeypots in network security.
- **Anicas, M. (2015)**. How to install Elasticsearch, logstash, and kibana (ELK Stack) on Ubuntu 14.04.
- **Dittrich, D. (2004)**. Creating and managing distributed honeynets using honeywalls. Draft. University of Washington.
- **Döring, C. (2005)**. Improving network security with honeypots. Darmstadt: University of Applied Sciences.
- **Hoque, M. S., & Bikas, M. A. (2012)**. An implementation of an intrusion detection system using a genetic algorithm. International Journal of Network Security & Its Applications (IJNSA).
- **Jaiganesh, V., Sumathi, D. P., & A.Vinitha. (2013)**. Classification algorithms in intrusion detection system: A survey. A Vinitha et al. Int. J. Computer Technology & Applications.

No Author listed. (https://www.honeyd.org/)

- **Ralph E.S Jr** (No date listed): How to build and use a honeypot.

Deception Toolkit, https://all.net/dtk/index.html fetched 5/02/2015

THANKS