Honeypot Deployment and Cyber Analysis Using T-Pot

Mauricio Spadoni

Department of Computer Science and Information Systems

University of North Georgia

CYBR 4950

Professor Yong Wei

May 6th, 2025

Abstract

This capstone project focuses on the deployment of a honeypot system using the T-Pot framework to detect and analyze real-world cyber threats. The study aims to create a secure, isolated, and effective honeypot environment that captures attacker behavior and malicious activities. Technologies including Docker, Elasticsearch, Kibana, and SpiderFoot were utilized to support data collection, visualization, and intelligence gathering. The project emphasizes hands-on experience in server setup, Linux command-line proficiency, and security operations, contributing to enhanced cybersecurity defense skills.

Introduction

As cyber threats grow in complexity and volume, security professionals must proactively understand attacker behavior and exploit tactics. Honeypots, as decoy systems designed to attract and monitor malicious actors, provide valuable insights into these threats (Spitzner, 2003). This project explores the deployment of a multi-sensor honeypot using the T-Pot framework, an integrated platform developed by Deutsche Telekom that combines various honeypot sensors and security tools into a Docker-based architecture.

The objective of this capstone is to simulate a real-world cyber defense scenario, allowing in-depth monitoring and analysis of attack attempts targeting SSH, Telnet, and HTTP services. The experience gained through server configuration, command-line operations, Docker orchestration, and network monitoring tools forms a vital part of a senior cybersecurity student's skillset.

Project Scope and Objectives

The primary goals of this project are:

1. To deploy a secure and isolated T-Pot honeypot environment on a cloud-based server.
2. To simulate and capture common attack vectors, such as brute force attempts and reconnaissance.
3. To analyze collected data using ELK (Elasticsearch, Logstash, Kibana) and OSINT tools like SpiderFoot.
4. To document attacker behavior, identify threat patterns, and provide actionable insights.

The honeypot is specifically configured to emulate services frequently targeted by attackers, including SSH (port 22), Telnet (port 23), and web services (port 80/443). By studying these vectors, the project contributes to a practical understanding of how attackers operate and how organizations can better defend against them.

Methodology

Server Deployment and Setup

A virtual private server was provisioned via DigitalOcean, running Debian 11 with a minimum of 4 CPU cores, 16 GB RAM, and 256 GB SSD storage. Secure Shell (SSH) access was established using cryptographic keys, and the server was hardened to minimize exposure.

T-Pot Framework Installation

T-Pot was selected due to its robust integration of multiple honeypot sensors such as Cowrie, Dionaea, and Honeytrap, along with pre-configured monitoring and analytics tools. The installation was done using the official T-Pot ISO, and Docker was used to manage its containerized services efficiently.

Linux Command-Line Proficiency

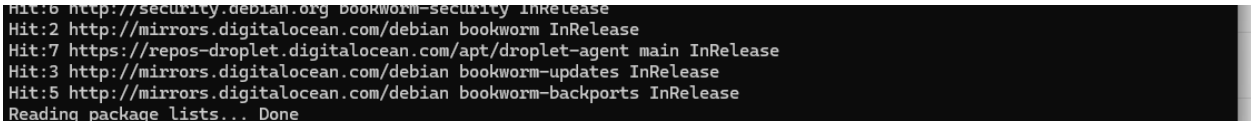
All installation and configuration processes were executed via the Linux command line. Tasks included managing system updates, configuring network interfaces, creating user accounts, and setting up logging tools. This experience significantly improved my comfort and capability with Linux-based systems.

Docker Orchestration

As T-Pot relies heavily on Docker, learning container orchestration was essential. I managed individual honeypot containers, examined logs, and ensured seamless interaction between services such as Kibana and Elasticsearch. Troubleshooting Docker and network issues formed a critical component of the learning curve.

Network Isolation and Security Controls

Using VirtualBox in the planning phase allowed the creation of a secure lab environment. Later, in the production environment, firewall rules and isolated VLANs ensured the honeypot could attract traffic without risking lateral movement into secure networks.



Data Collection and Analysis

Over the course of deployment, the honeypot recorded over 151,000 attack attempts. Cowrie was the most targeted sensor with 70,000+ hits, followed by Honeytrap and Dionaea. The most common attack vectors included brute-force SSH logins, unauthorized HTTP access, and malware propagation.

Analysis via Kibana dashboards revealed frequent usernames like "root," "admin," and "ubuntu," and passwords like "123456" and "admin." Attack sources were geographically diverse, with the U.S., China, and the Netherlands among the top origin countries.

SpiderFoot provided valuable intelligence by scanning attacker IPs, domains, and WHOIS records, helping identify potentially compromised infrastructure and actors.

Challenges and Solutions

- Selecting the Right Framework: Initial tests of multiple honeypots highlighted differences in capabilities. T-Pot was chosen for its integrated and extensible design.

- Network Configuration: Ensuring proper isolation required deep understanding of virtual network adapters and firewall rules.

- Tool Compatibility: Integration of Splunk and Wireshark posed challenges in virtual environments. Issues were mitigated by adjusting dependencies and opting for native T-Pot tools.

Results and Key Findings

- High volume of SSH-based brute force attacks confirmed the popularity of this attack vector.
- Attackers consistently used default credentials, indicating reliance on low-effort compromise strategies.
- Real-time dashboards and visualizations allowed rapid assessment of threat intensity and geography.
- The use of SpiderFoot complemented the ELK stack by offering threat intelligence from open sources.

Conclusion

This project successfully demonstrated the feasibility and value of deploying a honeypot using T-Pot. As a senior cybersecurity student, the hands-on experience deepened my technical expertise in server setup, command-line operations, Docker management, and threat intelligence analysis. It provided a practical foundation for future roles in security operations and threat hunting.

Future improvements include integrating Splunk for enhanced correlation, automating alerts with TheHive and Cortex, and expanding intelligence gathering with platforms like Maltego.

References

Spitzner, L. (2003). *Honeypots: Tracking Hackers*. Addison-Wesley.

Deutsche Telekom Security GmbH. (2023). *T-Pot: The All-In-One Multi Honeypot Platform*. https://github.com/telekom-security/tpotce

Elastic. (2023). *The Elastic Stack*. https://www.elastic.co/what-is/elk-stack

SpiderFoot. (2023). *Automated OSINT Tool*. https://www.spiderfoot.net/

Docker Inc. (2023). *What is Docker?*. https://www.docker.com/resources/what-container/