Cloud-Native Honeypot Analysis Report

Project: High-Interaction TPOT Deployment on DigitalOcean

Brandon
Cloud Security Analyst

October 30, 2025

Abstract

This report documents the deployment, configuration, and initial threat analysis of a high-interaction, open-source honeypot environment using **TPOT (The Honeypot Project)**. The system was provisioned on a DigitalOcean Droplet and quickly began capturing real-time malicious traffic. Initial observations show a high volume of attacks targeting the default SSH port, with a significant portion of adversarial scanning originating from major cloud hosting providers. The collected telemetry demonstrates the efficacy of using cloud-native honeypots for high-fidelity threat intelligence gathering and analysis via the integrated Elastic Stack (Kibana).

1 Executive Summary

The objective was successfully met by establishing a secure, external-facing TPOT HIVE deployment. The system immediately attracted opportunistic threat actors, validating the hypothesis that exposed cloud infrastructure is rapidly scanned and targeted. Key findings highlight the prevalence of brute-force SSH attacks and the use of legitimate cloud infrastructure by attackers.

- **Deployment Status: SUCCESS**. TPOT HIVE successfully deployed on DigitalOcean (Droplet IP: 129.212.188.183).
- **Primary Threat Vector:** Automated brute-forcing against the default SSH port (via the Cowrie honeypot).
- **Key Insight:** Out of 38 initial attacks, **89**% (34) targeted the SSH service, confirming its status as the most exposed and frequently targeted service on the public internet.
- **Risk Observation:** Attackers are heavily leveraging major cloud infrastructure (Google Cloud, Alibaba US) for scanning, masking their true origin.

2 Deployment and System Hardening

The lab began with the provisioning of a Linux server and subsequent security hardening, a critical step before deploying any public-facing service.

2.1 Cloud Provisioning and Initial Setup. The Droplet, named `tzmnc-web-server1`, was provisioned using Ubuntu 24.04 LTS. Initial access was confirmed via SSH client and immediate steps were taken for system hygiene.

1. System packages were fully updated and patched using `apt-get update && apt-get upgrade -y`.
2. A non-root user, `martin`, was created and granted `sudo` privileges to adhere to the principle of least privilege.

2.2 TPOT Installation and Security Configuration. The TPOT Community Edition repository was cloned and installed with the HIVE configuration to include the full Elastic Stack for superior analysis.

3. The primary setup script, `./install.sh`, was initiated.
4. **Critical Hardening:** The default SSH port was automatically changed to `64295` for added security, successfully confirmed upon reconnection after a system reboot.

3 Threat Intelligence and Attack Analysis

Upon deployment and a short period of operation, the TPOT system successfully collected and aggregated threat data into the Kibana SIEM dashboard.

3.1 Honeypot Activity Summary. The initial dataset clearly demonstrates that opportunistic attackers prioritize easily accessible, high-value services. Out of 38 distinct attacks, the distribution across the honeypots was heavily skewed.

Honeypot (Service)	Purpose	Attack Count
Cowrie (SSH)	Simulate SSH/Telnet server	**34**
Dionaea (FTP/SMB)	Capture malware/exploits	2
Conpot (SCADA)	Simulate ICS environments	1
Elastic Potter (ElasticSearch)	Simulate API exposure	1

3.2 Adversarial Infrastructure Analysis. Detailed analysis via the Kibana dashboard identified key characteristics of the attacking infrastructure.

A1. **Geographic Origin:** The global attack map showed a diverse range of sources, with a prominent pin in the **United States** acting as a top source location.

A2. **Source ASN/ISP:** The Attacker ASN panel revealed top attacks originating from known, large-scale cloud providers, specifically `GOOGLE-CLOUD-PLATFORM` and `Alibaba US Technology`. This indicates that attackers are likely renting or compromising cloud infrastructure to conduct large-scale scanning operations.

A3. **Attack Pattern (Suricata):** Intrusion Detection System (Suricata) alerts highlighted aggressive, automated scanning. Alerts such as `"STREAM Packet with broken ack"` and `"TLS invalid record type"` are consistent with tools designed for rapid service probing and reconnaissance, not human interaction.

4 Conclusion and Future Policy Recommendations

The Cloud-Native Honeypot Lab provided high-fidelity, actionable threat intelligence demonstrating the immediate risks associated with deploying services on public cloud IP space.

- ✓ **Validated Tools:** The combination of TPOT and the Elastic Stack proved effective for real-time aggregation and visualization of raw attack telemetry.
- ✓ **Confirmed Threat Model:** The data confirms that automated scanners predominantly target default, exposed services (SSH) and utilize cloud-hosting infrastructure to facilitate large-scale, anonymous scanning.

Policy Recommendations. The following recommendations are derived directly from the threat intelligence collected during the lab:

- → **Mandate Port Changes:** All production services must immediately change default ports (e.g., SSH from 22 to a random high port) to drastically reduce exposure to automated scanning.
- → **Implement Geofencing/Rate Limiting:** Use firewall rules to block traffic originating from high-risk Autonomous System Numbers (ASNs) like generic cloud platforms unless a business need is justified.
- → **Strengthen Brute-Force Detection:** Increase monitoring sensitivity for login failures on remaining default-port services (e.g., FTP) to detect high-frequency attacks observed by the honeypots.