Honeypot Deployment & Analysis with T-Pot

This capstone explores honeypot deployment using T-Pot for cybersecurity threat detection.

M **by Mauricio Spadoni**

What Is a Honeypot?

Definition

Decoy system designed to attract and analyze attacker behavior.

Purpose

Detect, delay, and study cyber attacks deeply.

Types

- Low-interaction (e.g., Cowrie)
- High-interaction

Introduction to T-Pot

All-in-One Platform

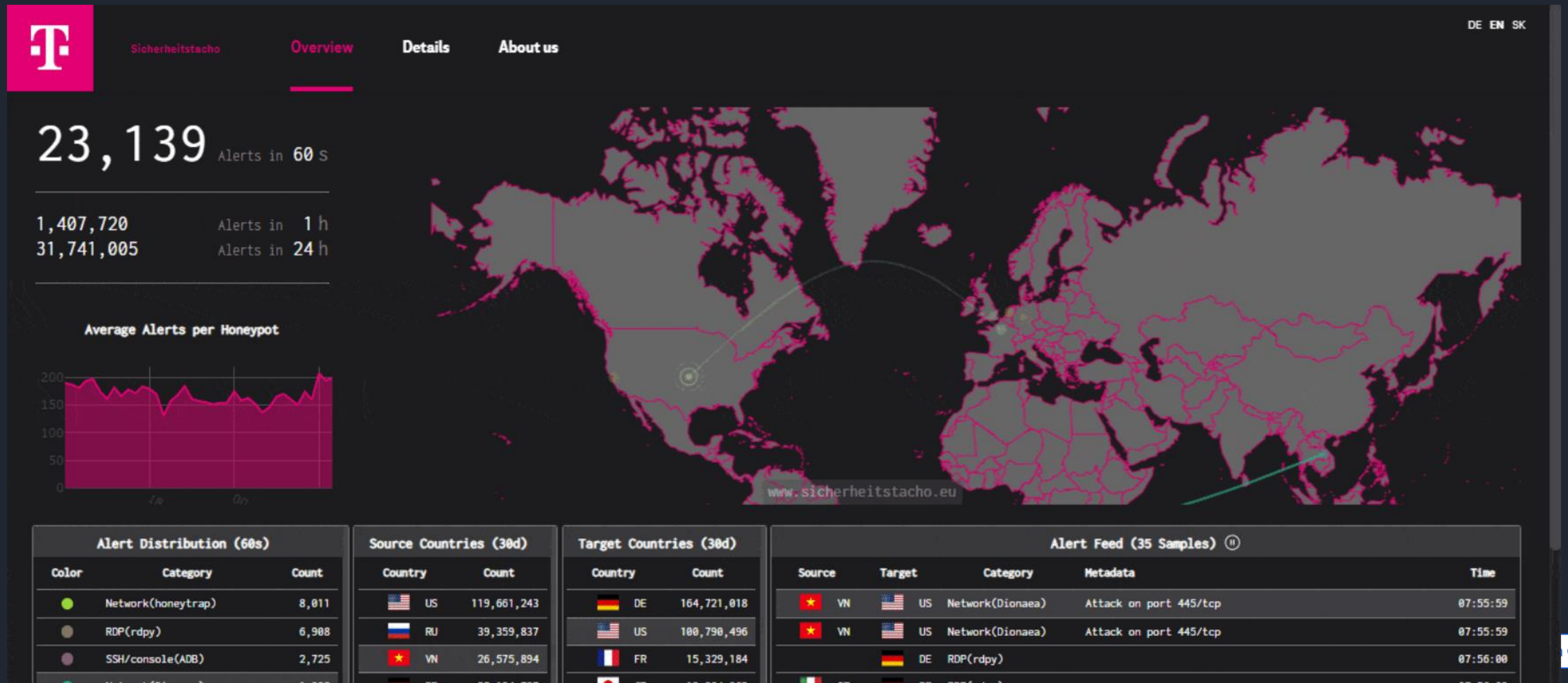
From Deutsche Telekom, integrates multiple honeypots and analytics.

Core Components

Combines sensors with ELK stack: Elastic, Logstash, Kibana.

Use Case

Detect threats and analyze malicious traffic patterns.



Architecture of T-Pot

Container-Based

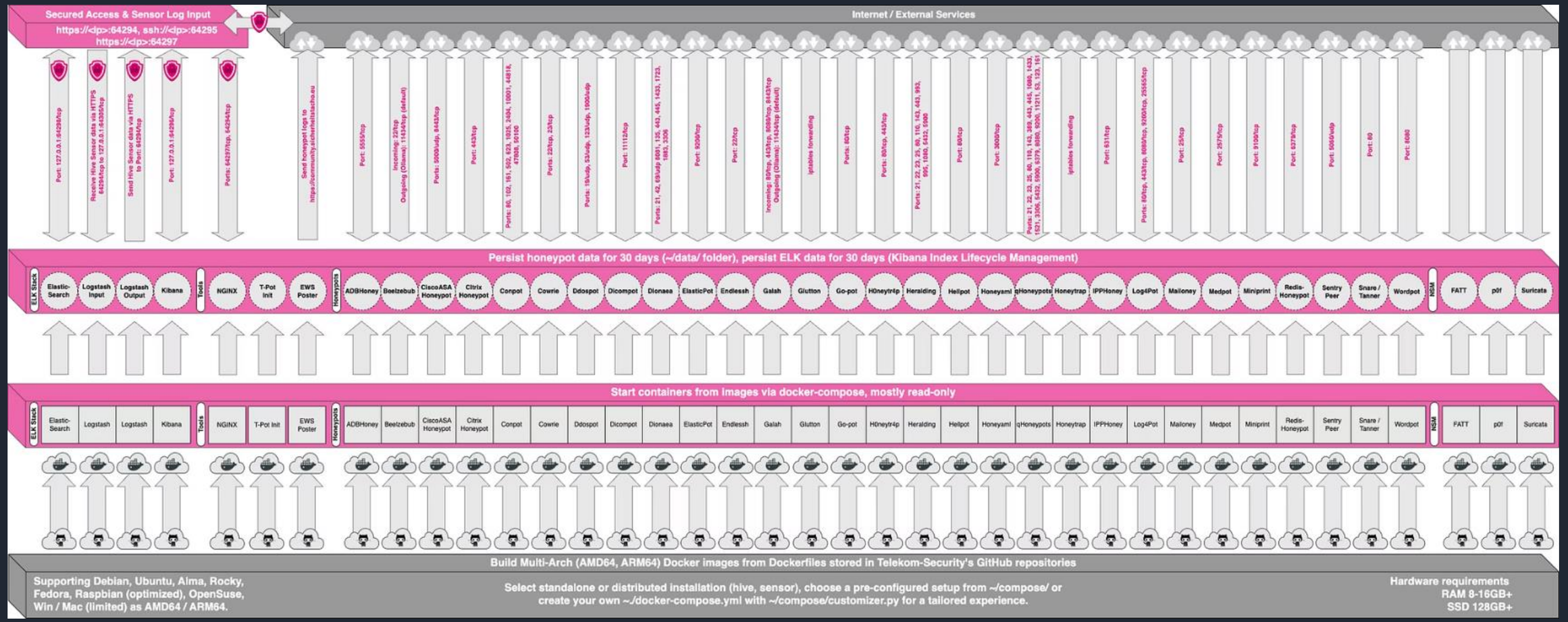
Utilizes Docker to isolate honeypot components efficiently.

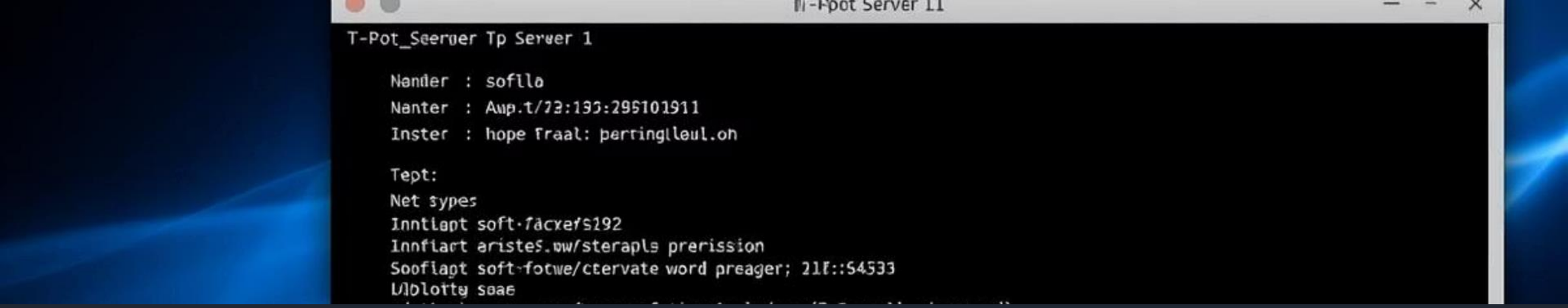
Key Components

- Cowrie
- Dionaea
- Spiderfoot
- Attack Map

Network Ports

- 22 (SSH)
- 23 (Telnet)
- 80/443 (HTTP/S traps)





Deployment Process

Setup Server

Deployed Debian server on DigitalOcean cloud platform.

Install T-Pot

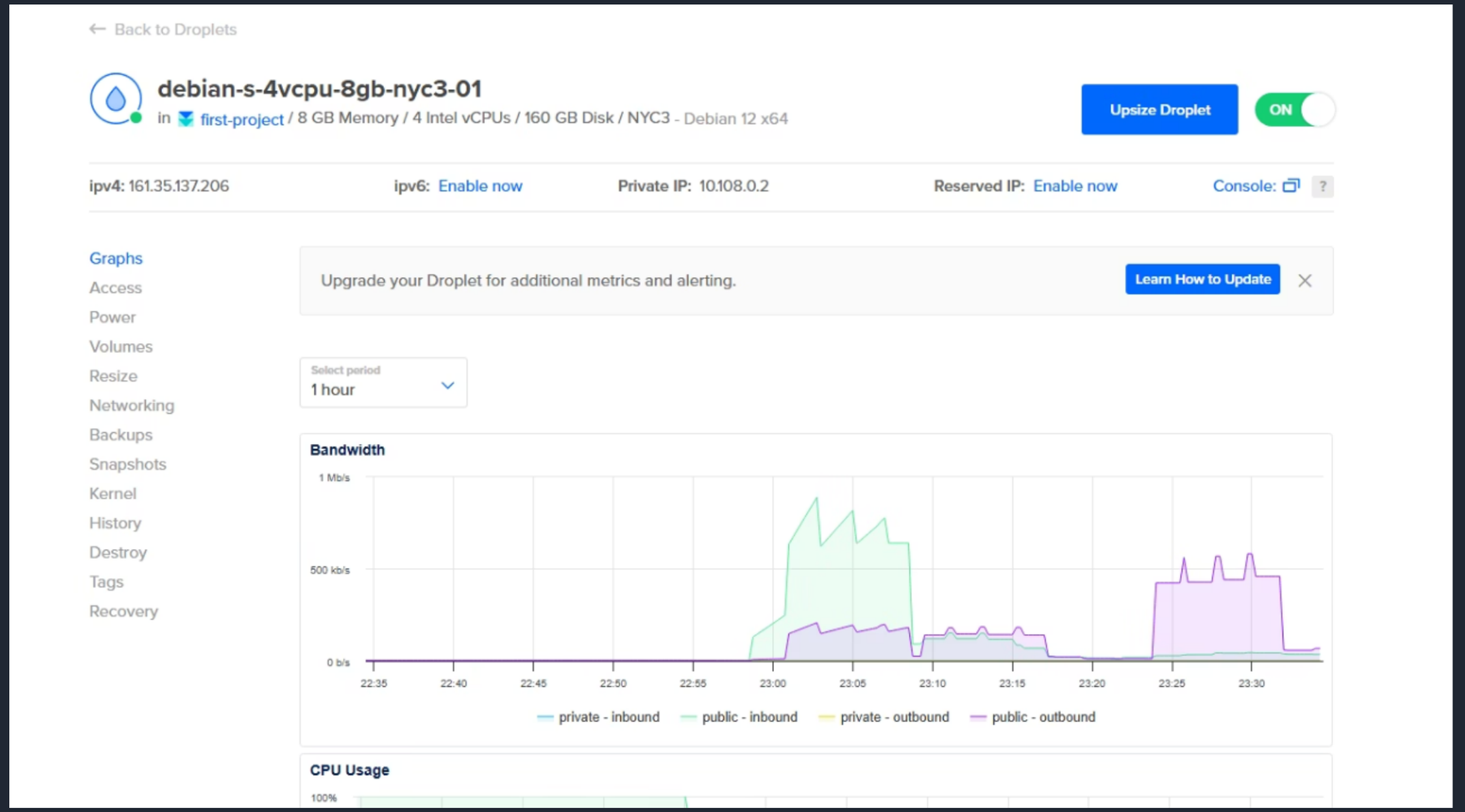
Installed with Hive for enhanced alert and case management.

Migrate Components

Upgraded from Cowrie-only to full T-Pot multi-honeypot setup.

Troubleshoot

Resolved Docker and network configuration challenges.



Cloud Setup

Debian server on DigitalOcean

Requirements

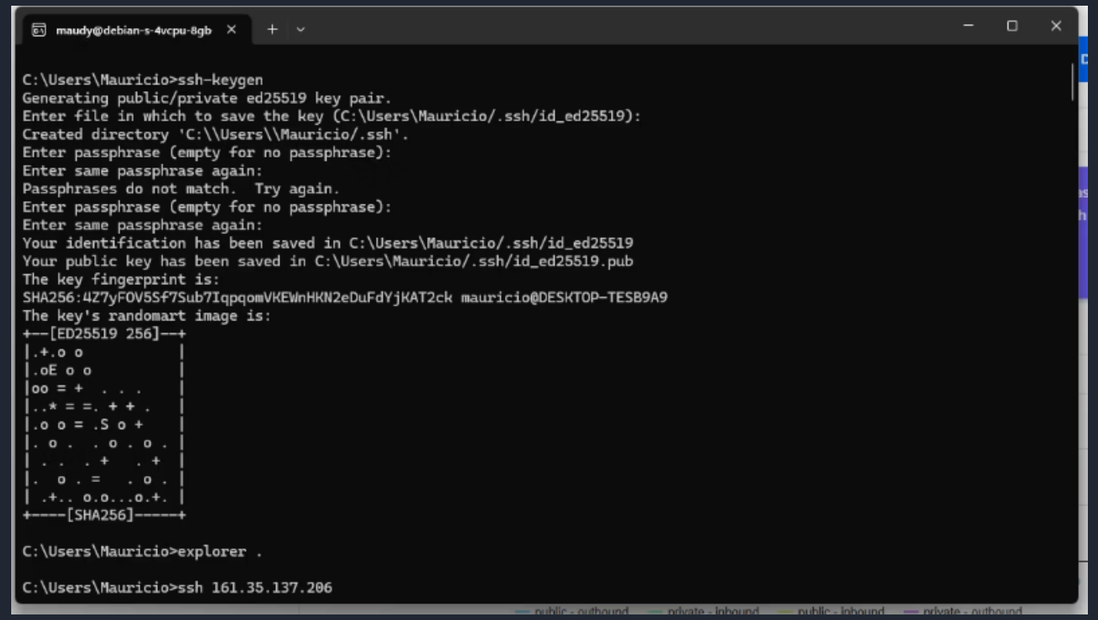
- Debian 11, 4+ cores, 16 GB RAM, 256 GB SSD
- Internet and root access

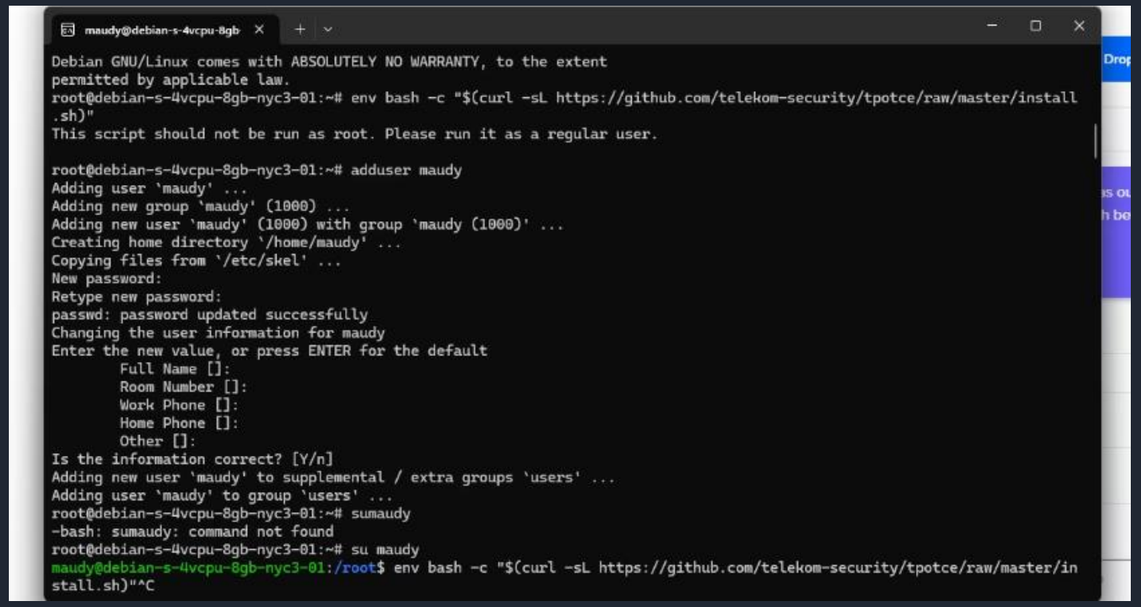
Tools

Docker, Hive for case management

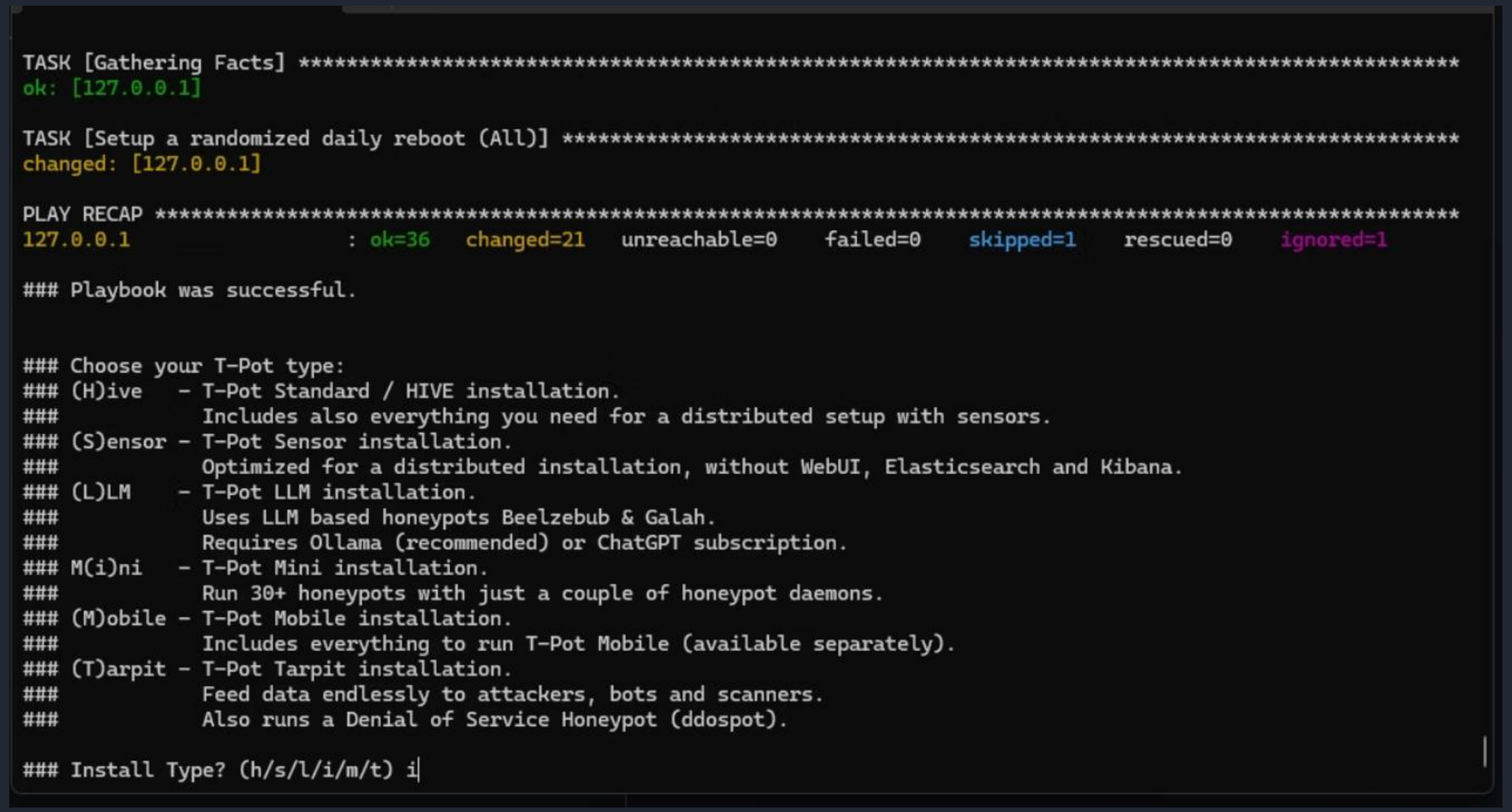
Challenges

Networking and Docker troubleshooting

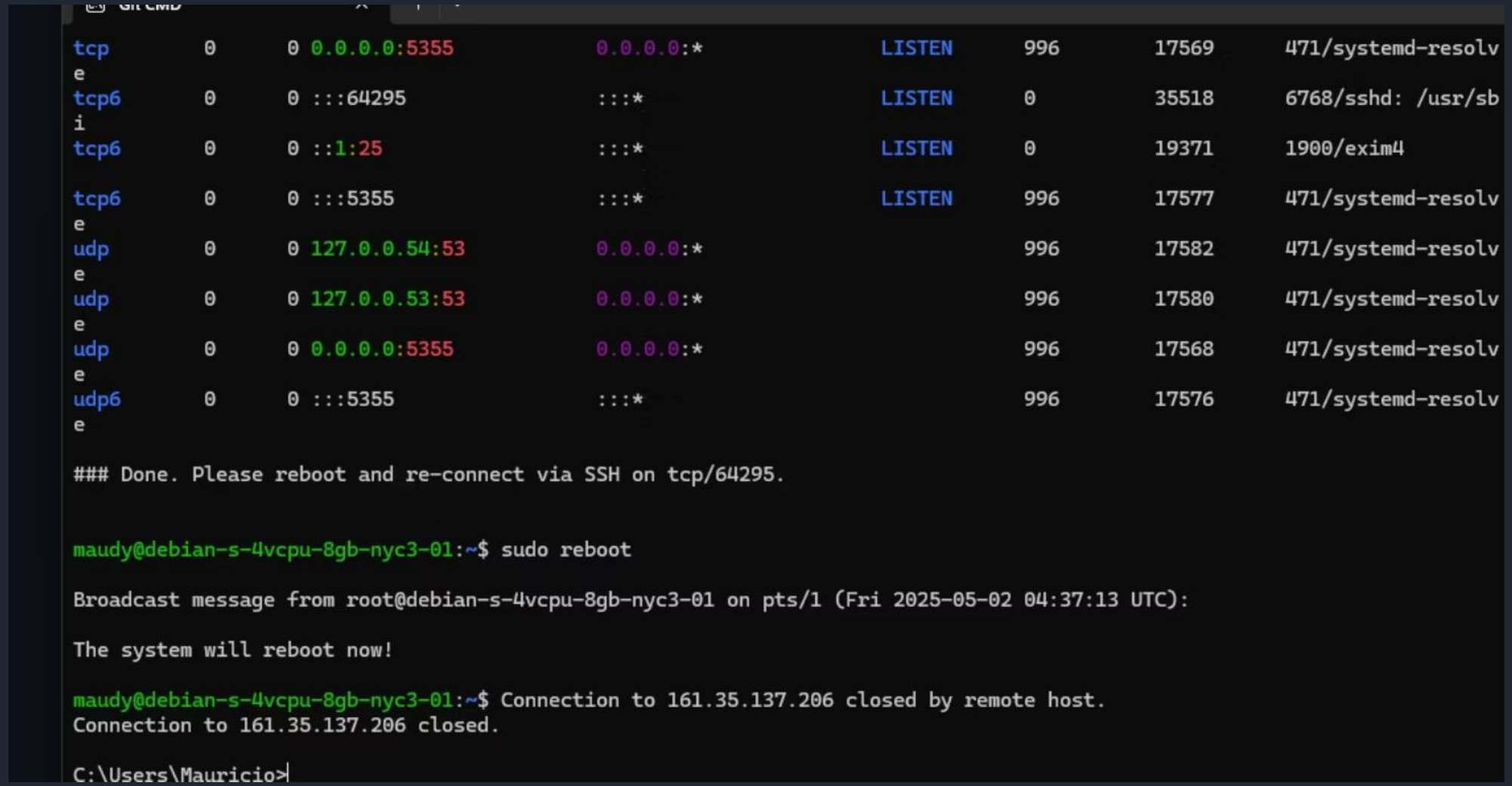




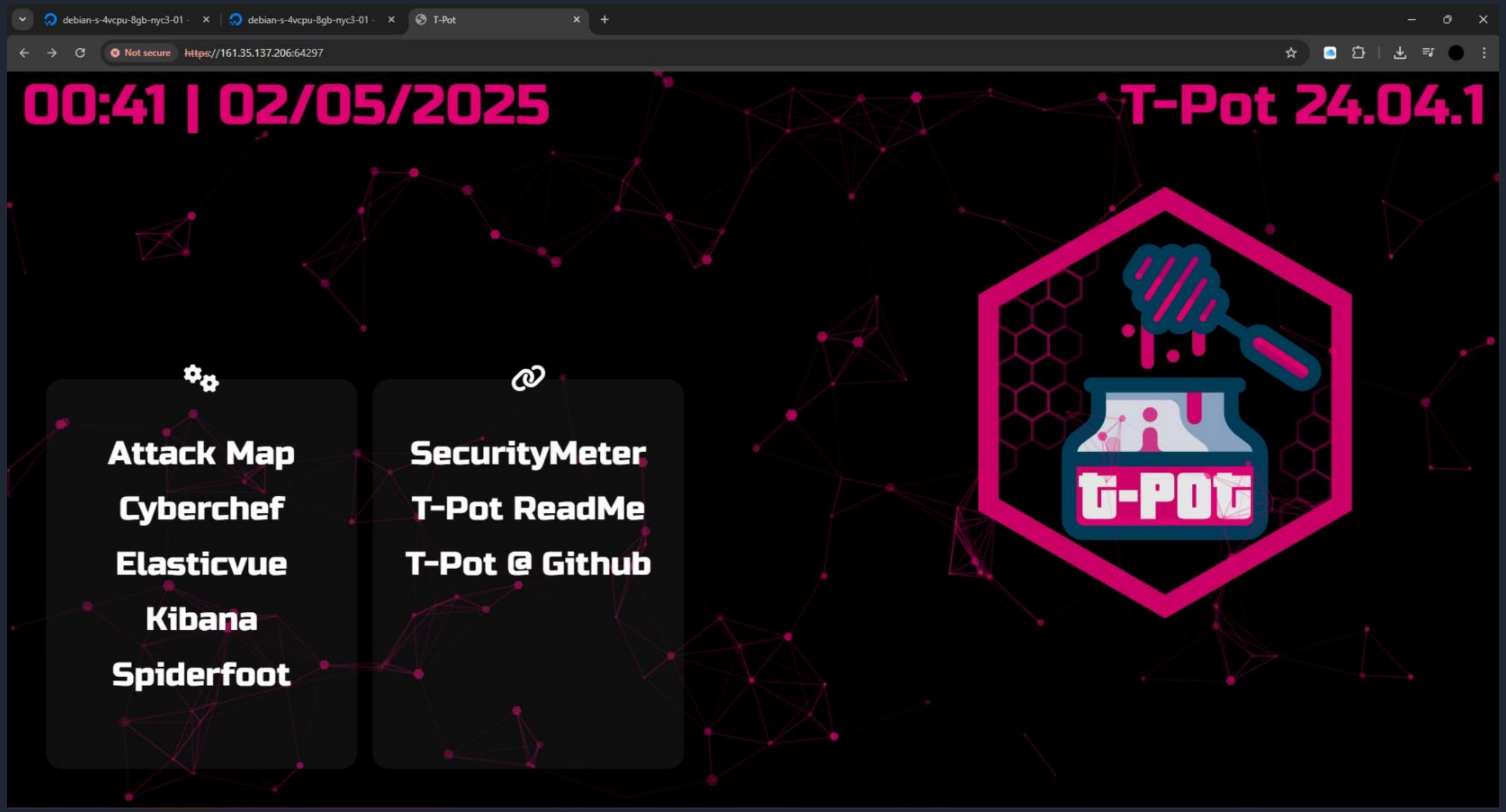
- Setting up SSH Key and adding user access to WebUI



- Installing Hive T-Pot after initially installing Mini due to ability to access Elastic Search, Kibana, and other Dashboard Metrics.



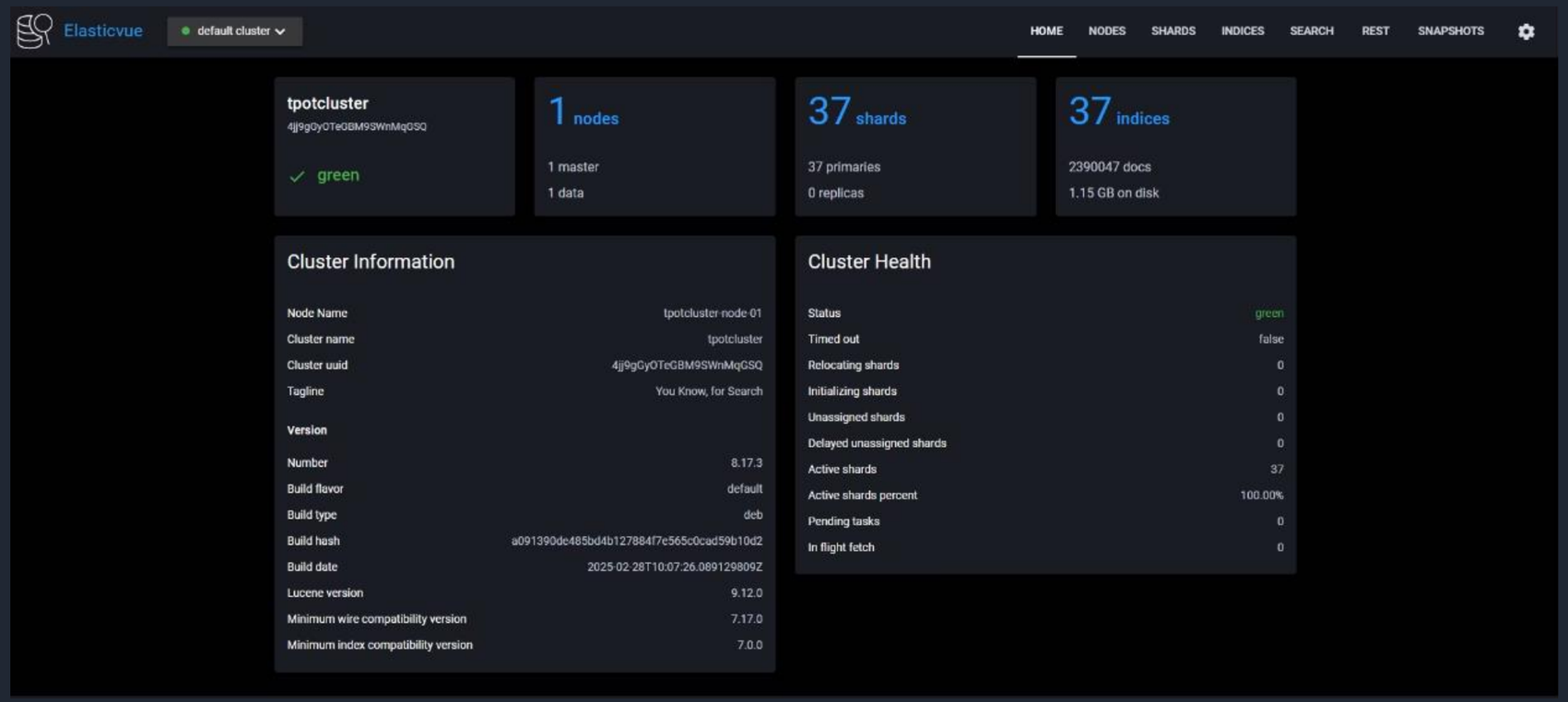
Rebooting Server after installation



Honeypot Overview & Attack Volume

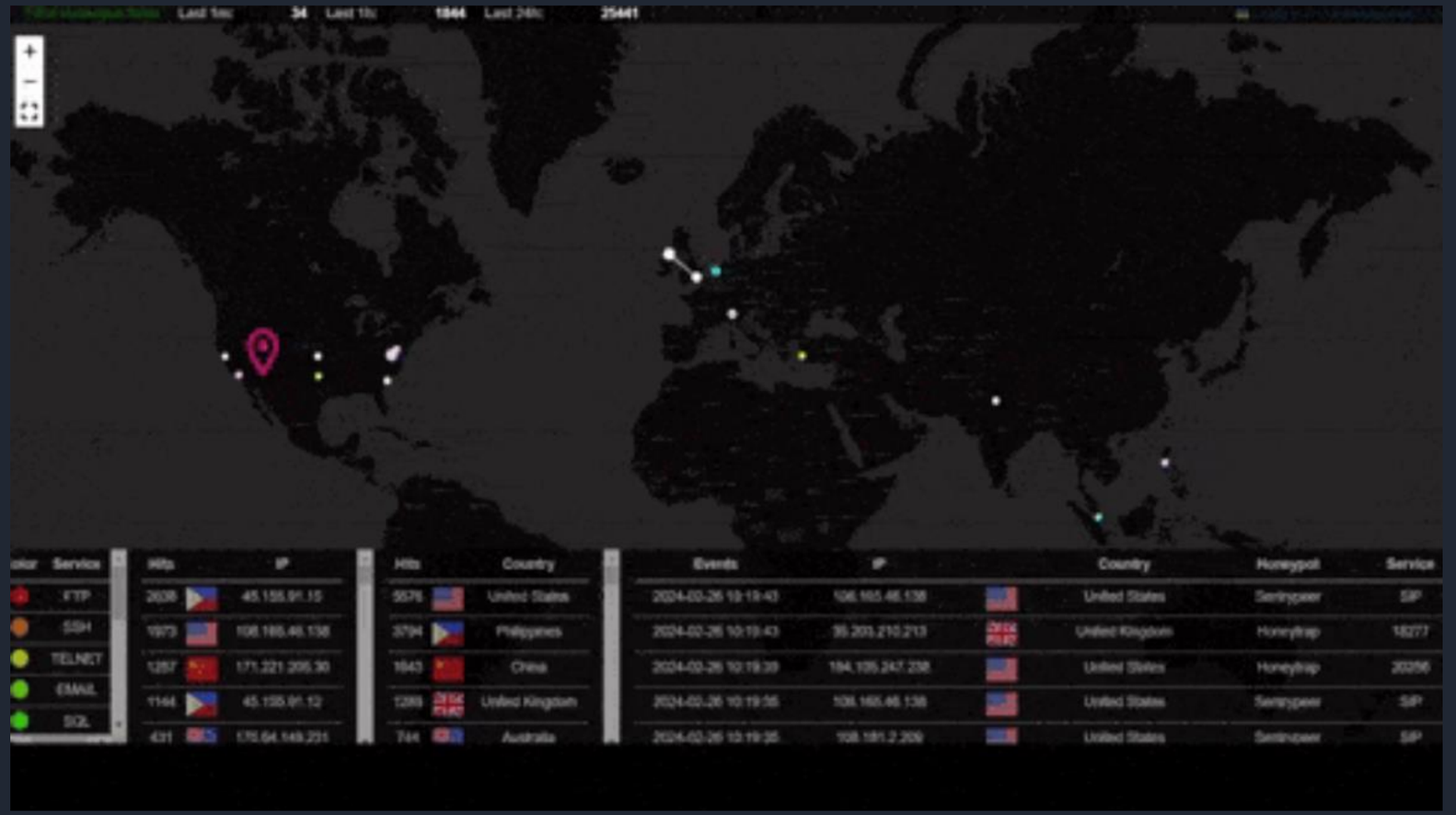
- **Total Attacks Logged**: 151,000+
- **Top Honeypots by Volume**:
  - **Cowrie**: 70,000+ attacks
  - **Honeytrap**: 37,000+ attacks
  - **Dionaea**: 20,000+ attacks
- Multiple attack vectors captured across SSH, Telnet, and other protocols

- **Top Source Countries**: USA 46%, Netherlands 12%, China 9%
- **Frequent Destination Ports**: 5060(non encrypted signaling traffic), 445 Server Message Blocking to share files and printers over TCP/IP, 22 SSH to connect to device and issue commands
- **Common Username Tags**: Root(2911), ubuntu(514), Administrator(514), 345gs5662d34(242), sa(207)
- **Top Password Tags**: 123456(1063), 123(246), 3245gs5662d34(242)



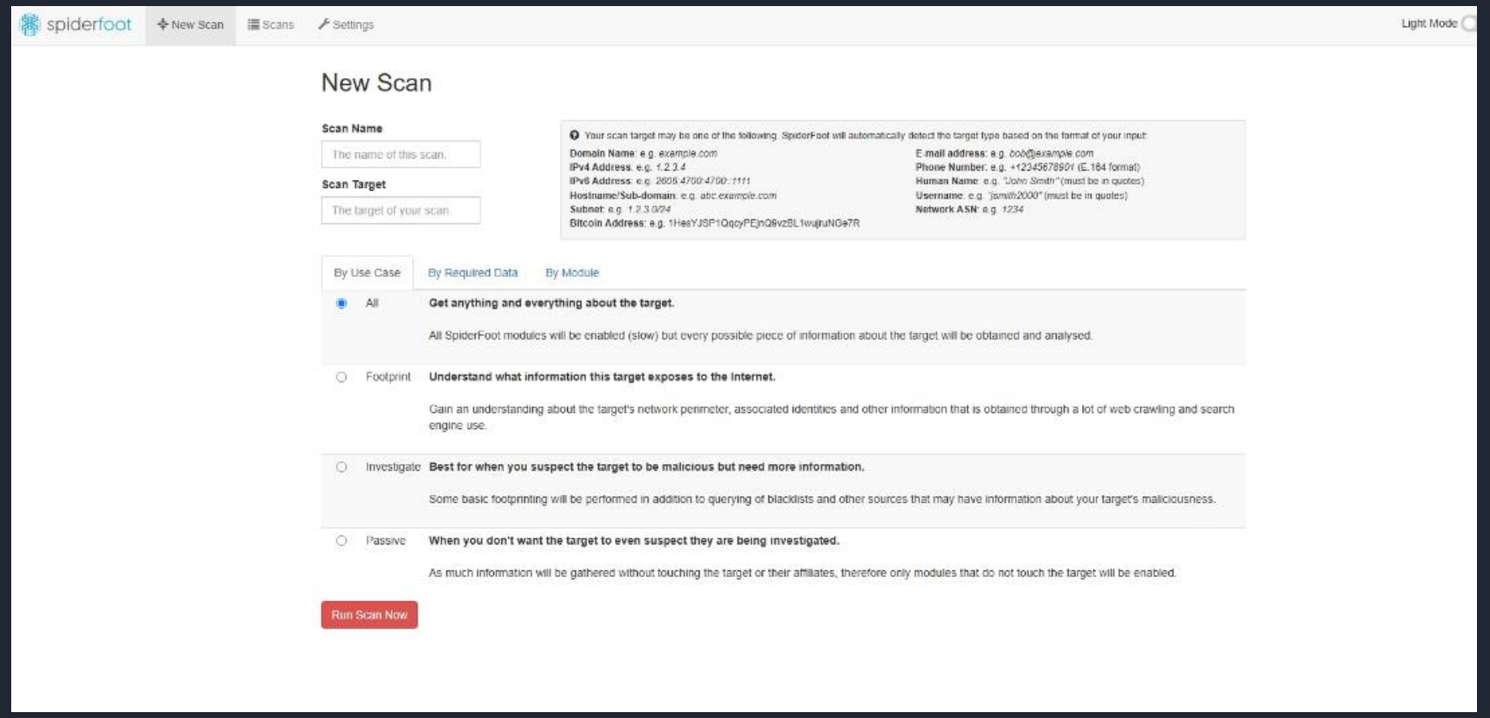
Elasticvue – T-Pot Cluster Insights

- Lightweight web GUI to explore Elasticsearch data from T-Pot
- View cluster health, node status, and storage usage
- Browse and query honeypot logs (Cowrie, Dionaea, Honeytrap, etc.)
- Inspect attack data: source IPs, ports, protocols, credentials, malware
- Filter logs by time, honeypot type, geolocation, ASN, and more
- Useful for quick threat analysis and data validation without Kibana



T-Pot Attack Map Overview

- **Real-Time Visualization** of global honeypot attacks
- Displays attacker geolocation based on source IPs
- Shows target ports, protocols, and affected honeypot sensors
- Highlights top attacking countries and IP addresses
- Visual clustering of attacks by intensity and region
- Useful for identifying trends, hotspots, and threat origins



SpiderFoot Overview

- **Automated OSINT (Open Source Intelligence) Tool** for threat intelligence gathering
- **Monitors** various data sources like IPs, domains, ASN, WHOIS, and social media
- **Comprehensive Scans** for vulnerabilities, leaks, and footprints of a target
- Provides detailed **reports** on attack surface and security risks
- Supports **multiple data sources**: Shodan, DNS, WHOIS, Pastebin, and more
- **Customizable** with modules to suit specific intelligence needs
- **Visualization** of findings through graphs and maps for easy analysis
- Used for profiling threat actors, identifying exposed assets, and proactive defense

Analytics with T-Pot (ELK Stack)

Kibana

Visualizes logs via interactive dashboards.

Elasticsearch

Indexes and stores honeypot event data efficiently.

Attack Map

Real-time global visualization of attack sources.

Spiderfoot

Automates Open Source Intelligence (OSINT) collection.

What I Learned

Linux CLI

Enhanced proficiency in the command line environment.

Docker Orchestration

Managed containerized honeypot components effectively.

Log Analysis

Used SIEM principles for attack pattern detection.

Troubleshooting

Diagnosed and fixed deployment and network issues.

Key Findings

Common Attack Ports

Targeted ports: 22, 23, 80, 443, 445.

Traffic Sources

Attacks originated from diverse global IP addresses.

Attack Types

- Brute force attempts
- Default credential use
- Network scanning activities

Future Improvements

Enhance Integration

Leverage Splunk or Security Onion platforms for deeper analysis.

Automate Alerts

Use TheHive and Cortex for real-time alerting.

Expand OSINT

Integrate Spiderfoot with Maltego for rich intelligence.

Use Threat Feeds

Incorporate MISP and OTX for updated threat intel.

Conclusion

Summary

Successfully deployed T-Pot and analyzed honeypot data.

Learning Outcome

Hands-on experience in cyber defense and threat analysis.

Next Steps

Build advanced operational security and OSINT skills.