AWS T-Pot Honeypot Lab Read Me

**Summary:**

For this project I will be running a Debian 11 EC2 instance on AWS and hosting Telekom-Security’s T-Pot honeypot from August 20th-August 26th 2024. I will then look at the data collected by the honeypots and do reports for each day and a final one at the end of the lab that aggregates all the data collected. My goal for this lab is to get more hands-on experience with AWS, common cybersecurity tools, and report writing. Thank you for looking!

**What is AWS?**

Amazon Web Services(AWS) is a subsidiary of Amazon that allows users, companies, and governments to access cloud resources on demand with a pay-as-you-go basis. For this lab I will be leveraging their Elastic Cloud Compute(EC2) resources to host a Debian 11 virtual machine. This cost about $4/day for the size tier of the VM that I chose.

**What is a Honeypot?**

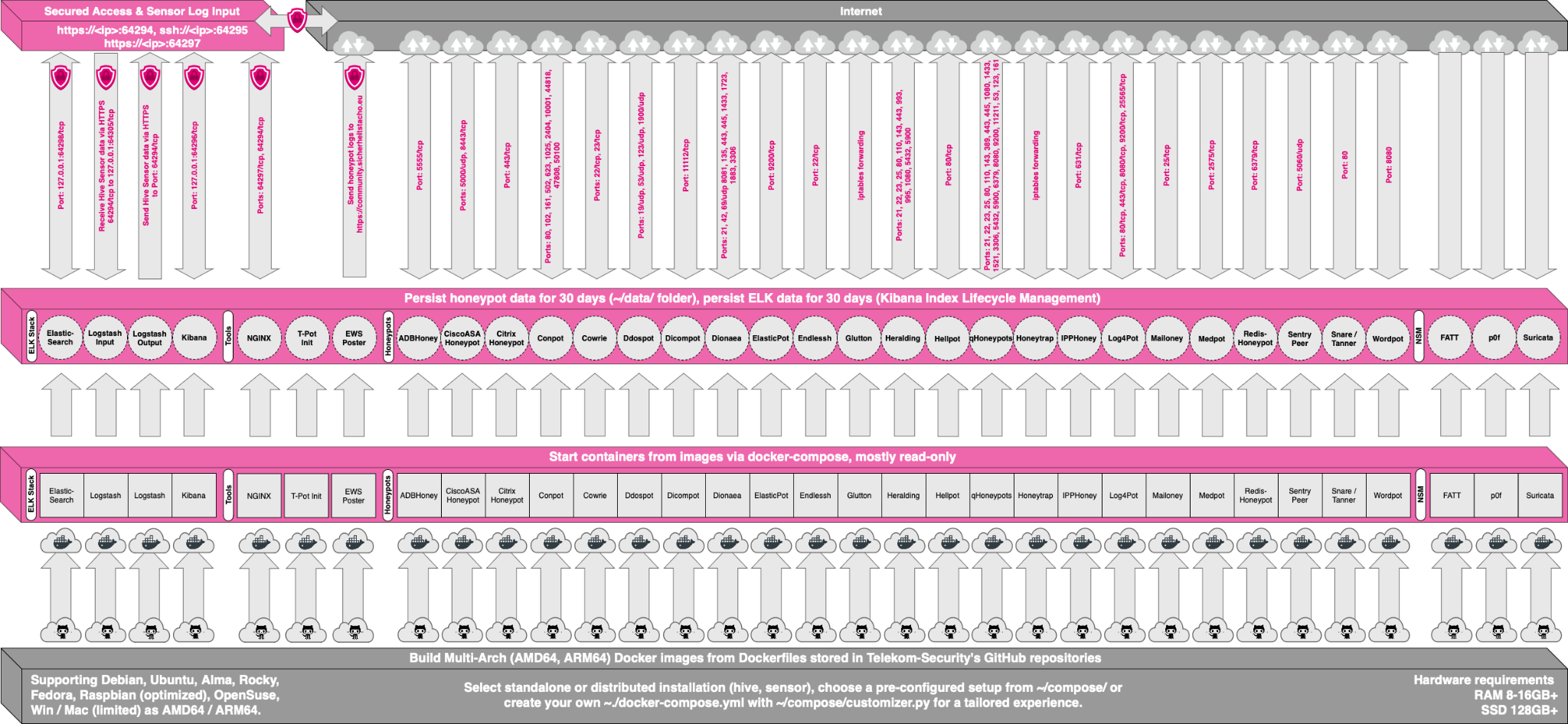
A honeypot is a cybersecurity tool that mimics vulnerable systems that are attractive to attackers. Honeypots are used to collect information about attackers such as their Tactics, Techniques, and Procedures(TTPs) and give cyber security professionals insights into how to counteract these attackers.

**What is T-Pot?**

T-Pot is an all in one tool developed by Telekom-Security that supports 20+ honeypots, visualizations using the ElasticStack, and other security tools. The honeypots used in the lab are the following:

* Honeytrap: a honeypot that emulates various types of network services and protocols, such as SSH, Telnet, FTP, HTTP, SMTP, and more. Can be configured to listen on multiple ports and simulate authentic behavior of various services to attract and trap attackers.
* Dionaea: a honeypot that emulates a vulnerable Windows environment designed to capture malware and attack payloads. Uses Python as its scripting language, supports IPv6 and TLS, uses libemu to detect shellcode, and collects hash values of collected files for later analysis.
* Cowire: a SSH and Telnet honeypot designed to emulate a system and provide a shell environment that captures the attacker’s actions on the system. This includes things like tools, techniques, credentials, and commands.
* Redishoneypot: a honeypot designed to emulate Redis servers and databases. Can collect the attacker’s IP address and commands used during connection attempts
* ADB Honeypot: a honeypot designed to emulate an ADB-enabled Android device and log unauthorized access attempts
* Snare/Tanner: a honeypot designed to emulate Windows systems and services that can capture attackers IP addresses, commands issued, tools, techniques, and procedures to identify patterns and send the collected data to security professionals.
* Ciscoasa: a honeypot designed to emulate Cisco Adaptive Security Appliances and software to track attacks targeting Cisco ASA devices.
* Citrix Honeypot: a honeypot designed to emulate a vulnerable Citrix environment.
* Mailoney: a honeypot designed to emulate a vulnerable mail server.
* Conpot: a honeypot designed to emulate SCADA protocols and industrial control systems.
* Elasticpot: this is a honeypot that simulates a vulnerable ElasticSearch server that is open to the internet.
* Dicompot: a honeypot that is designed to simulate a Digital Imaging and Communications in Medicine(DICOM) server.
* Sentrypeer: an open source VoIP fraud detection tool that tracks the IP addresses of attackers making calls to a SIP server.
* Heralding: a simple honeypot that is designed to log credentials of login attempts across multiple protocols.

**Network Topology of T-Pot**

****