DEPLOYMENT OF T-POT IN CLOUD

MSC in Applied Cybersecurity

Assignment – 1

Submitted by:

RAMA KRISHNA KAMBHAMPATY (B00168197)

Professor:

MARK LANE

TECHNOLOGICAL UNIVERSITY OF DUBLIN

BLANCHARDSTOWN

1. ABSTRACT

This assignment digs into the examination of honeypot data acquired via the TPOT (The Pot of Gold at the End of the Rainbow) framework from October 9, 2023 to the present. The honeypot detected a concerning increase in cyber attacks, which fell into three major categories: Ddospot, Cowrie, and Dionaea. Ddospot attacks totaled 2,491,639, demonstrating a prevalent Denial-of-Service assault environment, with Brazil and the United States appearing as major contributors. Cowrie attacks, which mostly exploited SSH weaknesses, demonstrated the vulnerability of popular credentials like "root" and weak passwords like "123456," with China being a major source. Dionaea attacks targeted online application vulnerabilities and originated mostly in Vietnam and the United States. The time analysis found that attacks peaked on October 19, 2023, which was ascribed to a distributed denial-of-service (DDoS) attack.

The findings highlight the vital need of knowing and combating various cyber dangers. Enhancing DDoS mitigation techniques, implementing advanced SSH security measures, raising awareness about secure coding practices for online applications, establishing real-time threat information sharing channels, and integrating behavioral analysis tools are among the recommendations for future development. As cyber threats grow, an adaptive and coordinated defense plan is required to properly secure digital infrastructure. This abstract presents a succinct overview of the TPOT honeypot data analysis, providing useful insights into future cyber dangers and recommending proactive cybersecurity solutions.

1. INTRODUCTION

HONEYPOTS:

Honeypots are a form of security mechanism that attracts and deceives intruders. They are often used to gather data about attackers, such as their tactics, tools, and targets. Honeypots can also be used to redirect or prevent assaults on important systems. Honeypots can have a modest or high engagement level [1]. Honeypots with low involvement just listen for and log connections. High-interaction honeypots may more realistically replicate genuine systems and communicate with attackers. The TPOT Honeypot is an advanced cybersecurity tool developed to detect, analyze, and prevent cyber threats in real time. It is simple to set up and utilize. It has a web interface for controlling the honeypot and viewing logs.

A honeypot serves as an early warning system, setting up a sensitive target and analyzing cyber attackers' strategies to gain insights into potential dangers before they break into the network. Data from encounters with opposing parties provides valuable knowledge for cybersecurity experts.

The TPOT honeypot is capable of detecting a wide variety of attacks, including:

SSH assaults: TPOT can identify SSH attacks like brute-force, credential stuffing, and privilege escalation.

HTTP assaults: HTTP attacks like as SQL injection, cross-site scripting, and command injection can be detected by TPOT.

RDP assaults: TPOT can identify RDP attacks like brute-force, credential stuffing, and privilege escalation.

Other sorts of assaults: TPOT can identify malware, phishing, and botnet attacks, among others.

TPOT is a powerful technique for increasing network security. TPOT can be used to acquire information on attackers and their methods, as well as to prevent or deflect attacks.

2. METHODOLOGY AND DESIGN

This discusses the design and implementation of our honeypot experiment. It describes the cloud service used to deploy the honeypot, how we designed and deployed the honeypot.

A. GOOGLE CLOUD PLATFORM:

The Honeypot is deployed in a cloud service environment, so that we can have most control over the honeypot. The Google Cloud Platform was found to be an ideal service, as it did not discourage security applications such as honeypots and was priced well for the services we would use.

Google Cloud Platform offers Google Compute Engine, a service designed for the deployment of virtual machines in the cloud. TPOT Honeypot, designed to simulate vulnerable systems and services, leverages the flexibility and power of Compute Engine to construct customized virtual instances. This capability enables security professionals to simulate a wide range of situations, increasing the honeypot's attraction to potential attackers and enabling more precise threat assessments.

Google Cloud Platform allows users to dynamically adjust computing resources. This ensures that TPOT Honeypot will be able to deal with fluctuations in network activity and growing security threats. In addition, users are able to reproduce authentic environments and increase the effectiveness of honeypots in detecting and evaluating a large number of potential threats by allowing them to customize VM instances. GCP's VPC offers TPOT Honeypot for security in isolated network situations, enhancing network isolation and enabling controlled communication, thereby providing a safe environment for threat research.

GCP enhances TPOT Honeypot deployments with robust monitoring and security services, including real-time insights, cloud logging, and integration with GCP's security services like Identity and Access Management and Cloud Security Command Center, enhancing overall security posture.

B. T-POT:

T-Pot is a honeypot deployment platform. TPOT uses Docker to facilitate the deployment and management of its honeypots[2][3]. Docker, a containerization platform, enables TPOT to encapsulate each honeypot within a lightweight and isolated container. This containerization offers a consistent and reproducible environment across several computers, allowing TPOT honeypots to be deployed in a variety of scenarios with ease.

Docker offers TPOT honeypots with a level of isolation, protecting the host system from any compromises within the honeypot environment. This security feature is critical for protecting the whole system's integrity, especially in cases when the honeypot may be attacked. The Docker container enables TPOT to concurrently deploy multiple Honeypot instances, which covers different network segments in an efficient manner.

T-Pot offers docker images to various honeypots such as Cowrie, Dicompot, Dionaea, Conpot, Elasticpot, medpot and several other honeypots along with the tools like Kibana, T-Pot Attack Map, Cockpit, Cyberchef, Elastic Stack, Spiderfoot.

Kibana is a powerful open-source data visualization software that can be used to analyze and visualize TPOT honeypot logs and data. Kibana has a number of features that make it excellent for honeypot analysis, such as:

Dashboard Creation: Kibana allows you to design custom dashboards that display the information that is most important to you. Visualizations of attack data, patterns in attacker activity, and the overall efficacy of your honeypot deployment can all be included.

Data exploration and filtering: Kibana has a number of filters and exploration tools that allow you to drill down into the data and uncover specific patterns and trends. This can assist you in identifying new attack pathways, tracking attacker progress, and understanding the motivations of various attacker groups.

Alerting and notification: Kibana can be set to deliver alerts and notifications when specific events occur, such as a new attack or suspicious activity. This allows you to respond to assaults more quickly and prevent them from causing damage.

Visualize honeypot traffic: Kibana can be used to view honeypot traffic, such as the number of connections, the sorts of connections, and the attackers' originating IP addresses. This data can assist you in identifying trends in attacker behavior and evaluating the success of your honeypot deployment.

Track attack patterns: Kibana can be used to track attack patterns such as attack kinds, tools and strategies used by attackers, and attack targets. This data can assist you in identifying new attack techniques and developing preventive measures.

Analyze attacker behavior: Kibana can be used to examine attacker behavior, such as motivations, strategies, and techniques. This data can help you enhance your honeypot deployment and gain a better understanding of the threat.

3. IMPLEMENTATION

This section goes into additional details about how our T-Pot honeypot was deployed in the Google Cloud Platform, configuration of the virtual machine and its deployment.

A. CONFIGURATION:

The Google Cloud Platform (GCP) provides virtual machines to deploy the honeypot. In GCP, firstly the virtual instances were created using pre-installed Debian-11-Bullseye. This instance is named as Tpot2. This virtual instance is deployed in the northeast Asia location which is Seoul, Korea.

This virtual instance is configured with Intel Broadwell CPU configuration. We used 4 dedicated processors with 8 Gigabytes of Random Access Memory (RAM) and 128 Gigabytes of Solid-State Drive (SSD) for main storage[4]. The RAM of 8GB is also upgraded to 16 Gigabytes an additional disk of 100 Gigabytes and is installed and attached dynamically as the machine configuration needed to be altered because of the network traffic and the alerts. A single public IPV4 address is assigned to the virtual instance. To facilitate analysis, no IPV6 connectivity was enabled on the droplets. GCP's VPC network allows to configure the firewall ruleset for the honeypot, which allows access from the outside world.

B. DEPLOYMENT:

After the configuration of the virtual instance, we start the process of deployment of the T-Pot honeypot into the real world. The minimum configuration requirement of the virtual machine is 4 Gigabytes of Random Access Memory and 128 Gigabytes of the Storage.

Firstly, after the configuration of the virtual machine, use the IP address to connect to the virtual machine running on the cloud to install and configure T-Pot in it. Once, connected to the cloud, we need to install and configure the honeypot.

Installing T-Pot

The following commands are used to install the T-Pot[5]. They are:

sudo su – (to acquire root previleges)

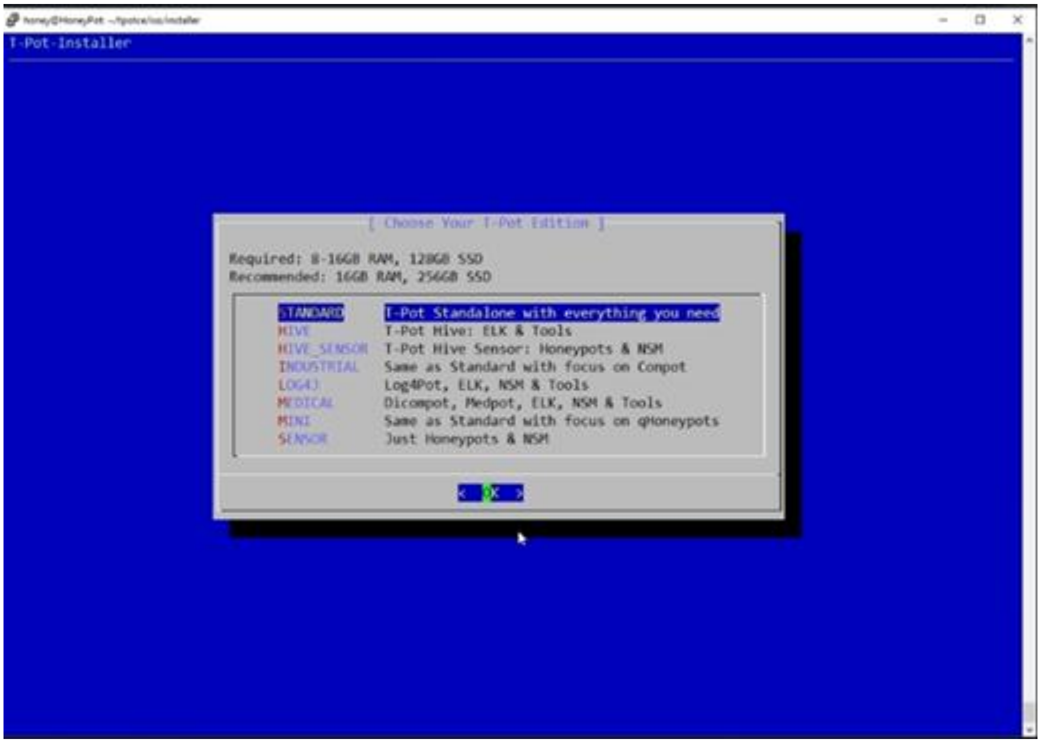
apt-get update && apt-get upgrade -y

apt install git -y

git clone https://github.com/telekom-security/tpotce.git

cd tpotce ./install.sh --type=user

After executing the last command, you will get a pop-up as the below screen



```
T-Pot-Installer

[ Choose Your T-Pot Edition ]

Required: 8-16GB RAM, 128GB SSD
Recommended: 16GB RAM, 256GB SSD

    STANDARD       T-Pot Standalone with everything you need
    HIVE           T-Pot Hive: ELK & Tools
    HIVE_SENSOR    T-Pot Hive Sensor: Honeypots & NSM
    INDUSTRIAL     Same as Standard with focus on Conpot
    LOG4J          Log4Pot, ELK, NSM & Tools
    MEDICAL        Dicompot, Medpot, ELK, NSM & Tools
    MINI           Same as Standard with focus on qHoneypots
    SENSOR         Just Honeypots & NSM

                       < OK >
```

Select the Standard Version and press OK.

At the next step, Enter the Username and Password that are required to access the web interface of T-Pot. After this, the virtual machine will be rebooted. Upon the successful reboot, the T-Pot will be installed.

Accessing the T-Pot

Type " https://Public_IP_of_VM:64297" to access the T-Pot web interface, as the T-Pot service runs on port 64297. Then, to login to the online page, enter the T-Pot's Username and Password. Kibana, which is used to analyze data, create alerts and notifications, and visualize data in the form of bar graphs, pie charts, and so on, is available on the T-Pot website.

C. PROBLEMS ENCOUNTERED:

First:

The T-Pot was not installed successfully at the first attempt as it displayed an Abort Error during the installation.

```
Aborting. Debian-Kinetic is not supported.
```

And it was rectified by adding a new command in the installation [6].

```
myLSB_STABLE_SUPPORTED=”kinetic”
```

Second:

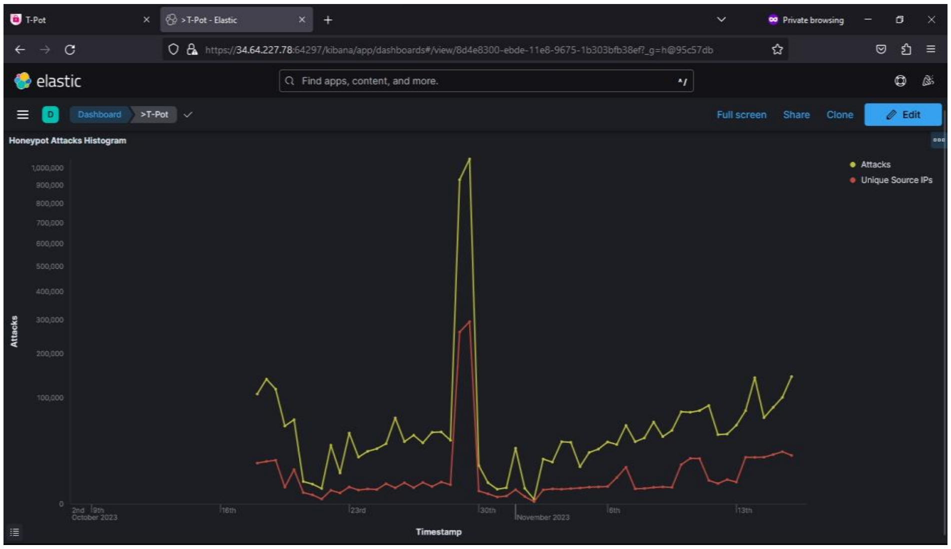
The initial configuration of the virtual machine was not sufficient for the network traffic that is encounted and the configuration was needed to upgraded to 4 dedicated processors and the RAM and the SSD was also need to be upgraded for the T-Pot to run without any performance issues. The continuous monitoring of the T-Pot helped to carefully analyse the errors and performance issues that were encountered in the operation.

4. ANALYSIS & RESULTS

The T-Pot honeypot ran from October 9, 2023 and the most common attacks that were detected by the T-Pot honeypot are as follows:

1. Ddospot Attacks (2,491,639 total)
2. Cowrie Attacks (1,030,375 total)
3. Dionaea Attacks (566,383 total)

Because each of these attacks is aimed to target a different type of vulnerability, it is critical to understand what each one is and how to resist it. The Ddospot attacks are Denial-Of-Service assaults that try to overload a server with traffic. As a result, legitimate users may find the server unusable. Cowrie attacks are SSH honeypot attacks that try to exploit SSH flaws. These attacks have the potential to steal user credentials or acquire system access. Dionaea attacks are honeypot online application attacks that try to exploit web application vulnerabilities. These assaults have the potential to steal information or deface websites.

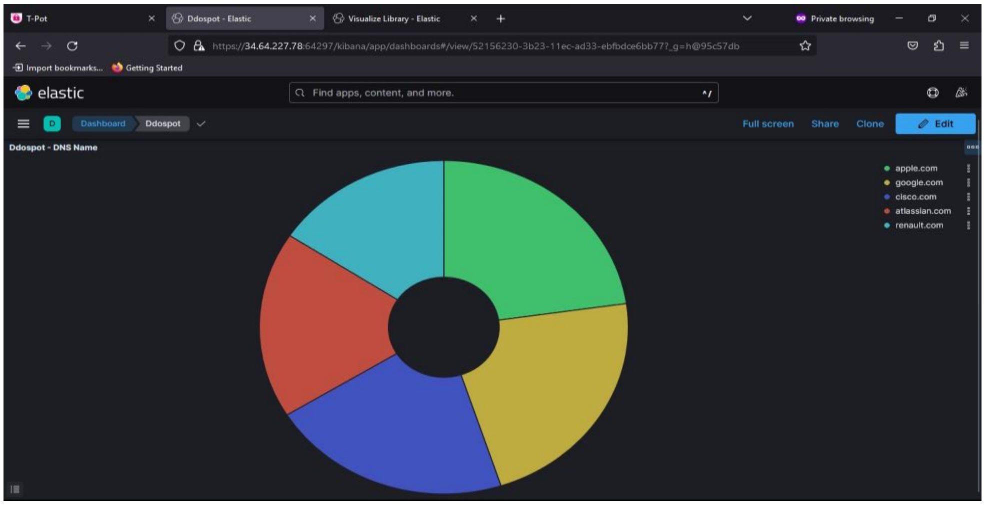


https://34.64.227.78:64297/kibana/app/dashboards#/view/8d4e8300-ebde-11e8-9675-1b303bfb38ef?_g=h@95c57db

According to the graph, the number of honeypot attacks has been increasing over time. There were around 800,000 honeypot attacks on November 2nd, 2023. The graph also shows that there was a peak in the number of honeypot attacks on October 19th, 2023. This peak was caused by a distributed denial-of-service (DDoS) attack.

DDOSPOT ATTACKS

There are a total of 2,491,639 attacks and 721,460 attacks are of unique source IP's. The most surge in the number of attacks were recorded on 29th October, 2023 and at that period there is also a surge in the mnumber of ip address but not as quickly as the number of attacks. The most number of attacks were recorded from Brazil (866,222) attacks and the second most attacks are from the united states. Around 53% of the attacks are from the known source ip address and 27% attacks are from bots or crawleres.



It shows the top five DNS(port 53) names that were targeted by attackers during the reporting period. The top five DNS names are: apple.com; google.com; cisco.com; atlassian.com ; renault.com.

The IP addresses that are recorded the most are 103.168.154.110(326) and 103.168.154.199(326). The said ip address are from yichen international building materials industry co. ltd. The most number recorded for the ddospot request packet is with destination port 123 and the count is 139,875.

COWRIE ATTACKS

The percentage of attacks that cowrie got on each port is SSH (92%)(port 22), Telnet (8%). Most of the attacks are from China (36%), United States (20%), Singapore (14%). The most used username was **“root”,** with around “58,405” hits and **“admin”** with around “5,569” hits. The password that was most used is **“123456”** with around 8,396 times.

The IP addresses that got most hits is 223.166.61.146 from China with a count of 16,434 hits with China Unicom Shanghai Network (AS - 17621). Around 58, 406 attacks out of 1,030,375 used the username “root” and the above ip address is also one of those.

The command that is most widely used is **“cd ~; chattr -ia .ssh; lockr -ia .ssh”** and the IP address “159.89.170.231” used this command for over 10 times from the Tencent Building, Kejizhongyi Avenue

Around 5000 attacks were used using this command and almost most of the attacks were recorded from China itself.

DIONAEA ATTACKS

The country that recorded most attacks is Vietnam(23%) and united states(22%). The 94% of Dionaea attacks are from known attacker and the remaining 6% are from mass scanner. The top hit Dionaea protocol is **“smdb”** with around 83% and the second is epmapper with around 13%. The Attacks by destination port recorded most from the 445 and 135 ports. With are around 84% and 13%.

The most used Dionaea is “accept” with 98% records. The interesting part is that 100% of Dionaea attacks are with TCP protocol. The most used username is root and sa with the count of 2491 and 865. The most used password are (empty) and 12345678 with count of 6663 and 54.

The IP addresses that recorded the most hits are 154.22.124.27 with the count of 44,609 and 154.22.154.56 with the count of 21,336 and both theses are from the San Jose,United States.

5. CONCLUSION

The data gathered from the TPOT honeypot deployment on October 9, 2023, demonstrates an alarming trend in the increasing frequency and diversity of cyber-attacks. Understanding the characteristics of these attacks is critical for designing effective defense methods. The three principal attack categories identified—Ddospot, Cowrie, and Dionaea—each target different vulnerabilities, emphasizing the importance of a diversified protection strategy.

Ddospot Attacks: The increase in Ddospot attacks, which totaled 2,491,639 and had 721,460 distinct source IPs, demonstrates the popularity of Denial-of-Service attacks. Brazil and the United States emerged as the primary sources, accounting for 53% of all attacks. The targeted DNS names, which include Apple, Google, and Cisco, indicate a broad impact. Future defenses should prioritize DDoS mitigation technologies and global collaboration to combat such pervasive attacks.

Cowrie attacks: Cowrie attacks generally exploit SSH weaknesses, with China playing a significant role (36%). Common credentials such as "root" and weak passwords such as "123456" are regularly attacked. The common use of the command "cd; chattr -ia.ssh; lockr -ia.ssh" indicates attempts to compromise SSH setups. Future initiatives should focus on improving SSH security, implementing stricter authentication protocols, and promoting password hygiene awareness.

Dionaea Attacks: Dionaea attacks, which primarily originate in Vietnam (23%) and the United States (22%), target online application vulnerabilities. The widespread use of the Dionaea protocol "accept" shows attempts to exploit service acceptance. Because TCP is the sole protocol, it is critical to pay close attention to TCP security precautions. It is critical to strengthen password policies and raise awareness about default and insecure credentials.

Recommendations for Future Work:

Enhanced DDoS Mitigation: Given the prevalence of DDoS attacks, future research should concentrate on improving DDoS mitigation solutions. Collaboration between organizations and regions can improve the collective defense against large-scale attacks.

Implementing advanced SSH security measures, such as two-factor authentication and stricter access rules, can greatly lower the danger of unwanted access to counter Cowrie assaults.

Because Dionaea attacks typically target web application weaknesses, future work should focus on raising knowledge about secure coding techniques and the significance of frequent security assessments for web applications.

6. REFERENCES

[1] "Collection and analysis of attack data based on honeypots deployed on the Internet" E.Alata, M.Dacier.

[2] https://github.com/telekom-security/tpotce#running-in-a-vm by Telecom-Security.

[3] "Honeypot Implementation in Cloud Environment" Stefan Machmeier, Heidelberg University

[4] "DEPLOYING AND ANALYZING CONTAINERIZED HONEYPOTS IN THE CLOUD WITH T-POT" by Alexander D. Washofsky, 2021.

[5] **https://www.youtube.com/watch?v=vJb_dgd7cHY&t=1892s**

[6] **https://www.youtube.com/watch?v=fq5TJd97EeM&t=1227s**