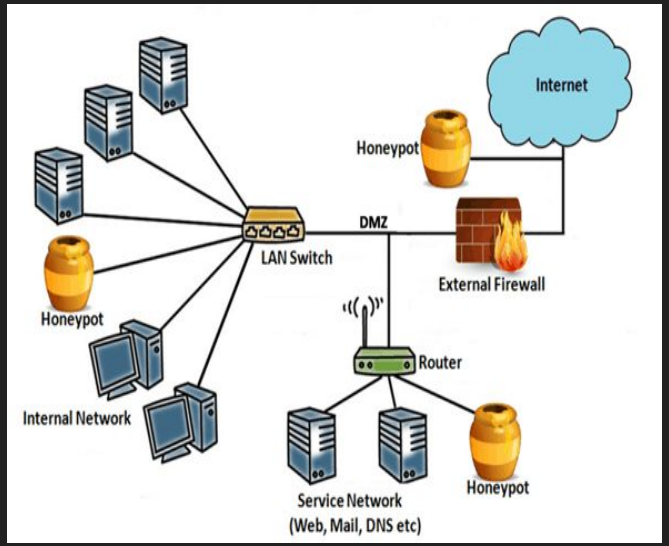
Capstone Project: Honey Pot

Sean, Rob, Jason, Chris

Overview of the Honey Pot

- What is a Honey Pot?
  - A tool that is used to study or detect malicious activity.
- What are the kinds of Honey Pots?
  - Two different kinds of Honey Pots:
    - Production
    - Research



Overview of TPot

- Automated Response and Data Collection
- Designed to simulate vulnerable web servers
  - Email, SQL, SSH, FTP, SMB protocols enabled
- Multi-HoneyPot project designed by T-Mobile
- User friendly dashboard and analytic tools
- Low Maintenance cost and effective design
- Additional built in tools:
  - T-Sec Radar
  - Cyberchef
  - Kibana
  - Spiderfoot

Home Cockpit CyberChef ES Head Kibana Spiderfoot

Dashboard / >T-Pot

Full screen Share Clone Edit Auto-refresh Last 24 hours

>_ *

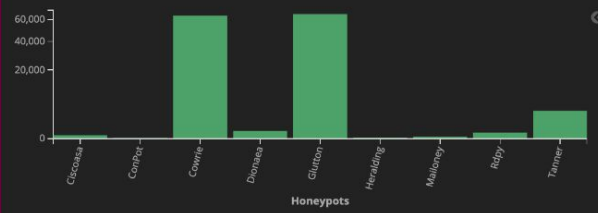
Options Update

Add a filter +

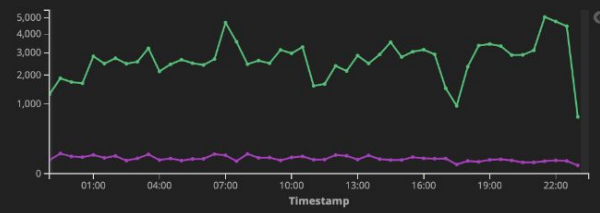
Honeypot Attacks - Top 10

65,727	64,025	3,281	249	152	50	16	5	3
Glutton - Attacks	Cowrie - Attacks	Tanner - Attacks	Dionaea - Attacks	Rdpy - Attacks	Ciscoasa - Attacks	Mailoney - Attacks	Heralding - Attacks	ConPot - Attacks

Honeypot Attacks Bar

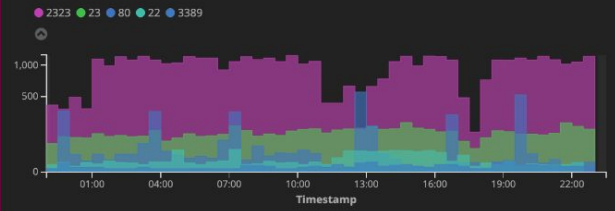


Honeypot Attacks Histogram

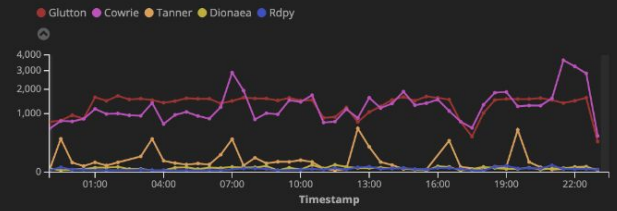


Honeypot Attack Map

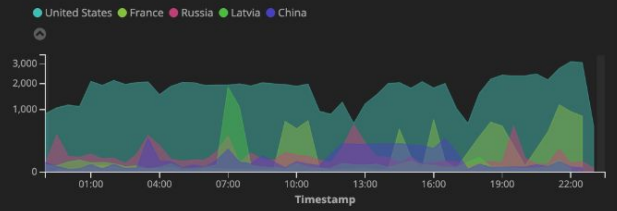
Attacks by Destination Port Histogram



Attacks by Honeypot Histogram

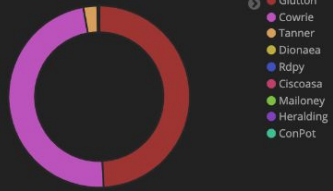


Attacks by Country Histogram

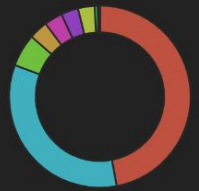


Attacker Src IP Reputation

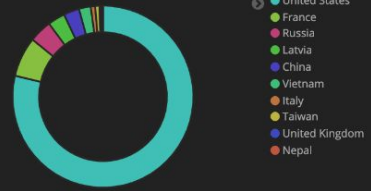
Attacks by Honeypot



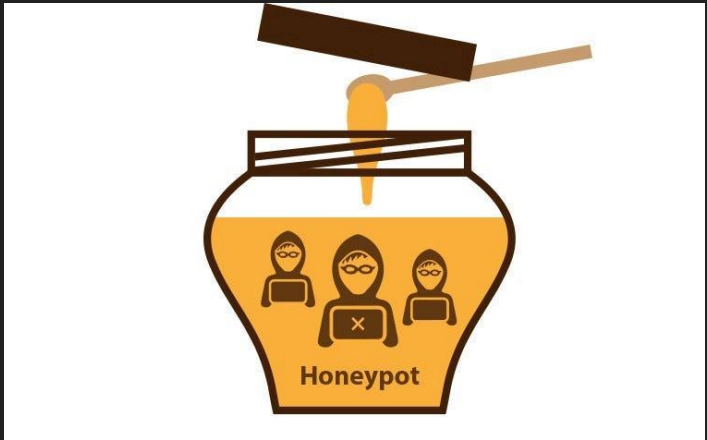
P0f OS Distribution



Attacks by Country



How the Project Comes Together



- Vultr Hosting
  - Cloud Platform hosting the linux server
- Debian 11 Server
  - Linux Based Server environment for honeypot
- T-Pot Software
  - Multiplatform software suit

How we set it up and how it works

- Collection of 20+ honeypots combined together in a cloud container
- Emulation
  - Emulates the behavior of a real network and services
- Attraction
  - Advertises itself on a public network where attackers might search for vulnerable devices
- Interaction
  - Captures and logs interactions including exploits and commands
- Analysis
  - Analyzes captured data to understand patterns and trends

Results & Outcomes (So Far)

- Initially, we expected that the result of this project would be attackers successfully accessing the fake data that is provided on our server.
  - Did this happen?
    - Yes, we have seen thousands of attackers successfully access our fake data throughout a variety of our honeypots.
- The attacks have been examined within the attack log dashboards for each individual honeypot, as well as the IP addresses and other data that was sent to them.

Results & Outcomes (So Far) Cont.

- Through access ports 1 through 64,000, it is expected that the attackers will be able to access the Honey Pot.
  - So far we have seen a large number of different common access ports that were used by attackers to attack our HoneyPots.
  - Some of the Most Common Ports We Have Seen:
    - 5900 - DDoS, Brute Force, Port Scanning
    - 19 - Trojan Attacks, Port Scanning, DoS
    - 1080 - Malware Attacks, DoS
    - 445 - SMB Exploits, Ransomware Attacks, DoS
    - 3306 - Brute Force, DDoS
    - 135 - DoS, Buffer Overflow Attacks, Malware Attacks
    - 27017 - Brute Force, Ransomware Attacks

What Data Do We Aim To Collect

We were Expecting to see Many Different Types of Attacks Captured on our HoneyPot

- Brute Force, Phishing, Port scanning, DDoS attacks, IOT Exploits, etc.
  - We saw all of these on our honeypots some with lots of hits and some with few hits

Why are we Collecting the Data?

- The data is the most important because it allows us to gain an understanding of how an attacker thinks and how they act
- Such as what are the common ports they attack through and what are the common ips that attack specific honey pots

Our future plans

We plan to gain a better understanding of the mind of an attacker through further data analysis and record what we find:

- Why the attackers choose a specific honeypot to attack
- Where the attacks are coming from and what that means overall

We plan on finishing collecting and analyzing data within the month then starting our writeup

Our final presentation will consist of the data we have gathered and what it means, what we have learned about honeypots and attackers, and the differences and similarities between a few of the honeypots and why they are getting different attacks from different places

Data we have collected

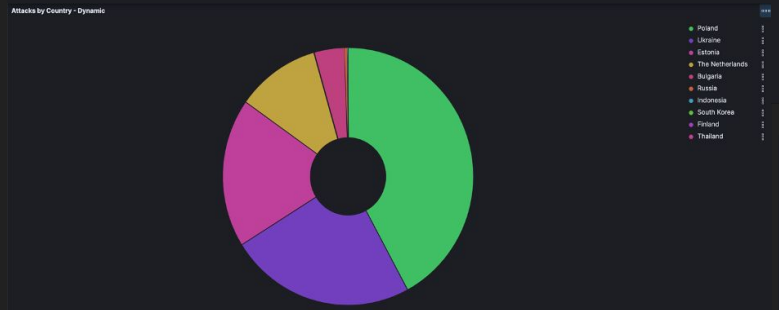
Mailoney

- A Low interaction SMTP honeypot
- Vulnerabilities such as **open_relay**, **postfix_creds**, or **schizo_open_relay**
- **Open_relay** Vulnerability is used by spammers to send illegal messages through an open server to make it harder to track the sender
- **Postfix_creds** can allows a bypass of email authentication allowing domain spoofing and further spamming

Mailoney eMails - Top 10

filters	eMail Address	Count
Sender	spameri@tiscali.it	153
Sender	test@vultrusercontent.com	16
Sender	info@usa.net	14
Sender	info.warren@berkshirehathaway.ngo	10
Sender	test@central.mercfresh.com	10
Sender	jgilliard853@gmail.com	8
Sender	rnrivanglasenberg8@gmail.com	6
Sender	w.u.o@outlook.com	6
Sender	westernunionmoneyt4@aol.com	6
Sender	westernunionmoneyt67@aol.com	6
Receiver	spameri@tiscali.it	75
Receiver	versionforlove@outlook.com	10
Receiver	info@usa.net	7
Receiver	innocentobio220@gmail.com	6
Receiver	sopuluobiora@yahoo.com	6

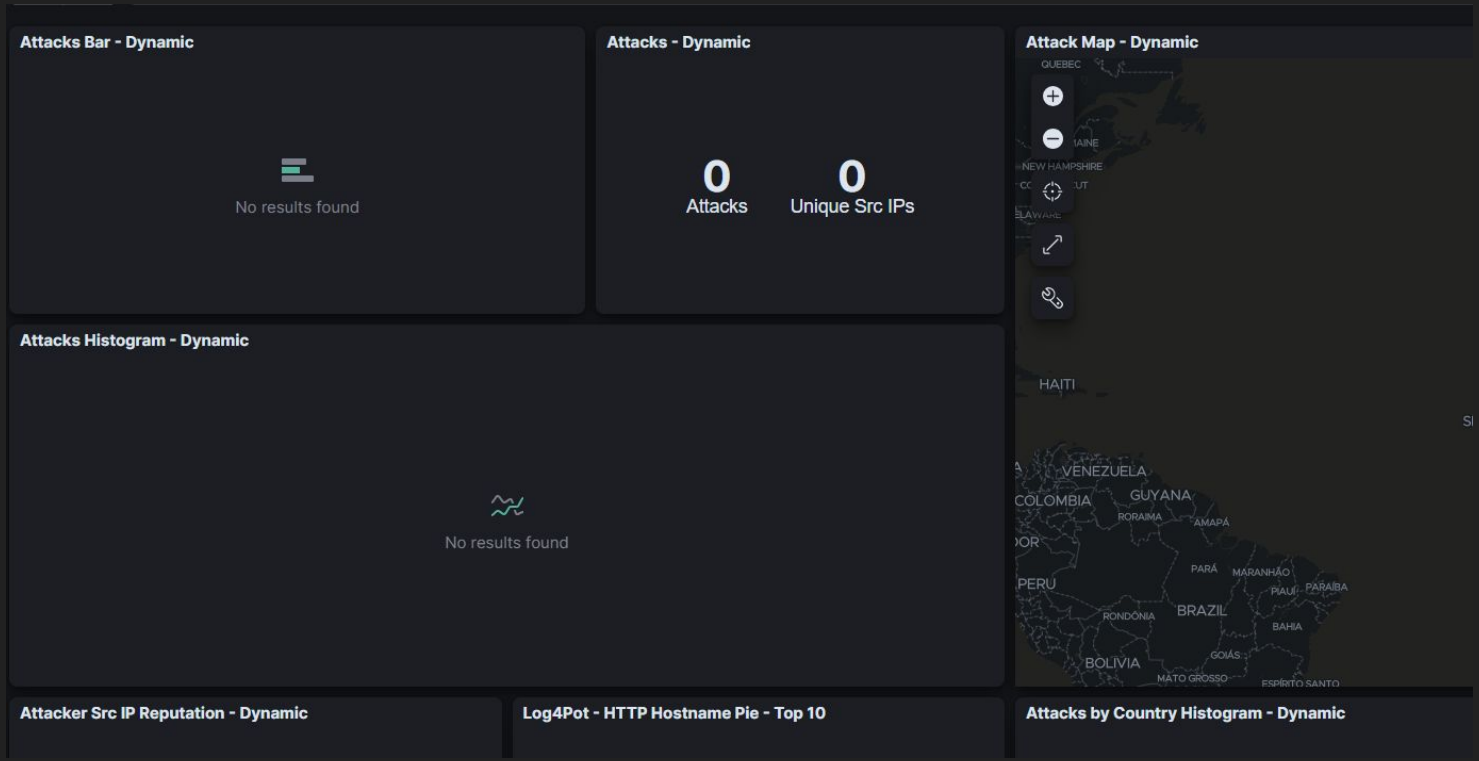
Heralding



Src IP - Top 10 - Dynamic

Source IP	Count
31.43.185.65	83,517
87.251.67....	40,908
87.251.67....	37,727
185.73.125...	35,609
185.73.124...	29,560
87.251.67....	23,786
80.66.88.145	22,806
87.251.67....	21,251
80.66.88.148	14,785
79.124.58....	13,090

Log4Pot


Attacks Bar - Dynamic
No results found
Attacks - Dynamic
0
Attacks
0
Unique Src IPs
Attack Map - Dynamic
QUEBEC
MAINE
NEW HAMPSHIRE
HAITI
VENEZUELA
COLOMBIA
GUYANA
RORAIMA
AMAPÁ
PERU
PARÁ
MARANHÃO
PIAUÍ
PARAÍBA
RONDÔNIA
BRAZIL
BAHIA
GOIÁS
BOLIVIA
MATO GROSSO
ESPÍRITO SANTO
Attacks Histogram - Dynamic
No results found
Attacker Src IP Reputation - Dynamic
Log4Pot - HTTP Hostname Pie - Top 10
Attacks by Country Histogram - Dynamic

Problems & Guard Rails

- With the assembly of 25+ honeypots, results may vary depending on the amount of attacks given to each honeypot
- Medpot; is a honeypot that attempts to replicate a HL7 / FHIR honeypot
- Although Healthcare data breaches are a hotspot for attackers, our honey pot did not meet the sufficient requirements to attract attackers
- There have been times where we didn't have enough storage for all of the data saved on tpot so it wouldn't give us access
- There was so much data on some honeypots that it started to automatically delete saved data from past months

Works Cited

https://jgmsoftware.co.uk/2020/05/24/deploying-a-honeypot-onto-aws/

https://www.secjuice.com/adventuring-with-an-ssh-honeypot/

https://docs.rapid7.com/insightidr/aws-honeypots/

https://blog.devgenius.io/creating-a-research-honeypot-on-aws-b0ded134729a

https://docs.rapid7.com/insightidr/aws-honeypots

https://security.packt.com/honeypot/