Azure

Azure Honeypot Project Documentation

Project Overview

Project Purpose

- To install and deploy a Honeypot on Microsoft Azure Virtual Machine and monitor and analyze potential cyber threats and attack patterns
- To collect real-world attack data for analysis of current threat landscapes

Target Audience

- Potential employers and recruiters evaluating your cybersecurity skills
- IT hiring managers reviewing your technical capabilities
- Security professionals assessing your understanding of threat analysis

Implementation Timeline

- Project Start Date: January 28, 2025
- Completion Date: January 31, 2025

Technical Architecture

Infrastructure Components

Virtual Network Configuration

- Single Virtual Network hosting the honeypot VM
- Isolated environment within Azure cloud
- NSG controls all inbound and outbound traffic

Virtual Machine Specifications

- Operating System: Linux (Ubuntu 24.04)
- VM Size: Standard D4s v3

- vCPUs: 4
- RAM: 16 GiB
- Network Bandwidth: 4,000 Mbps
- VM Generation: V2
- VM Architecture: x64
- Agent Version: 2.12.0.2
- Disk Controller: SCSI
- Security Features:
  - Security Type: Trusted Launch
  - Secure Boot: Enabled
  - vTPM: Enabled
- Storage:
  - Temporary storage (SSD): 32 GiB
  - Maximum data disks: 8
  - Maximum IOPS: 8,000
  - Maximum throughput: 128 MB/second
- Region: East US (Zone 1)

Security Controls

Authentication Methods

- Azure Portal browser-based connection with username and password authentication
- SSH access is enabled through open port configuration

Network Security Groups (NSG) Configuration

Inbound Rules

- Rule 300: SSH
  - Port: 22
  - Protocol: TCP
  - Source/Destination: Any
  - Action: Allow
- Rule 310: AllowAnyCustom1-65535Inbound
  - Ports: 1-65,535
  - Protocol: Any
  - Source/Destination: Any
  - Action: Allow
- Rule 65000: AllowVnetInBound
  - Protocol: Any
  - Source: VirtualNetwork
  - Destination: VirtualNetwork
  - Action: Allow
- Rule 65001: AllowAzureLoadBalancerInBound

    - Protocol: Any
    - Source: AzureLoadBalancer
    - Destination: Any
    - Action: Allow
- Rule 65500: DenyAllInBound
    - Protocol: Any
    - Source/Destination: Any
    - Action: Deny

Outbound Rules

- Rule 65000: AllowVnetOutBound
    - Protocol: Any
    - Source: VirtualNetwork
    - Destination: VirtualNetwork
    - Action: Allow
- Rule 65001: AllowInternetOutBound
    - Protocol: Any
    - Source: Any
    - Destination: Internet
    - Action: Allow
- Rule 65500: DenyAllOutBound
    - Protocol: Any
    - Source/Destination: Any
    - Action: Deny

Azure Security Center Integration

- Identity: Disabled
- Microsoft Defender for Cloud: Disabled (No security alerts detected)

Monitoring and Logging Setup

- Not configured at this time

Honeypot Configuration 🍯

Honeypots Deployed

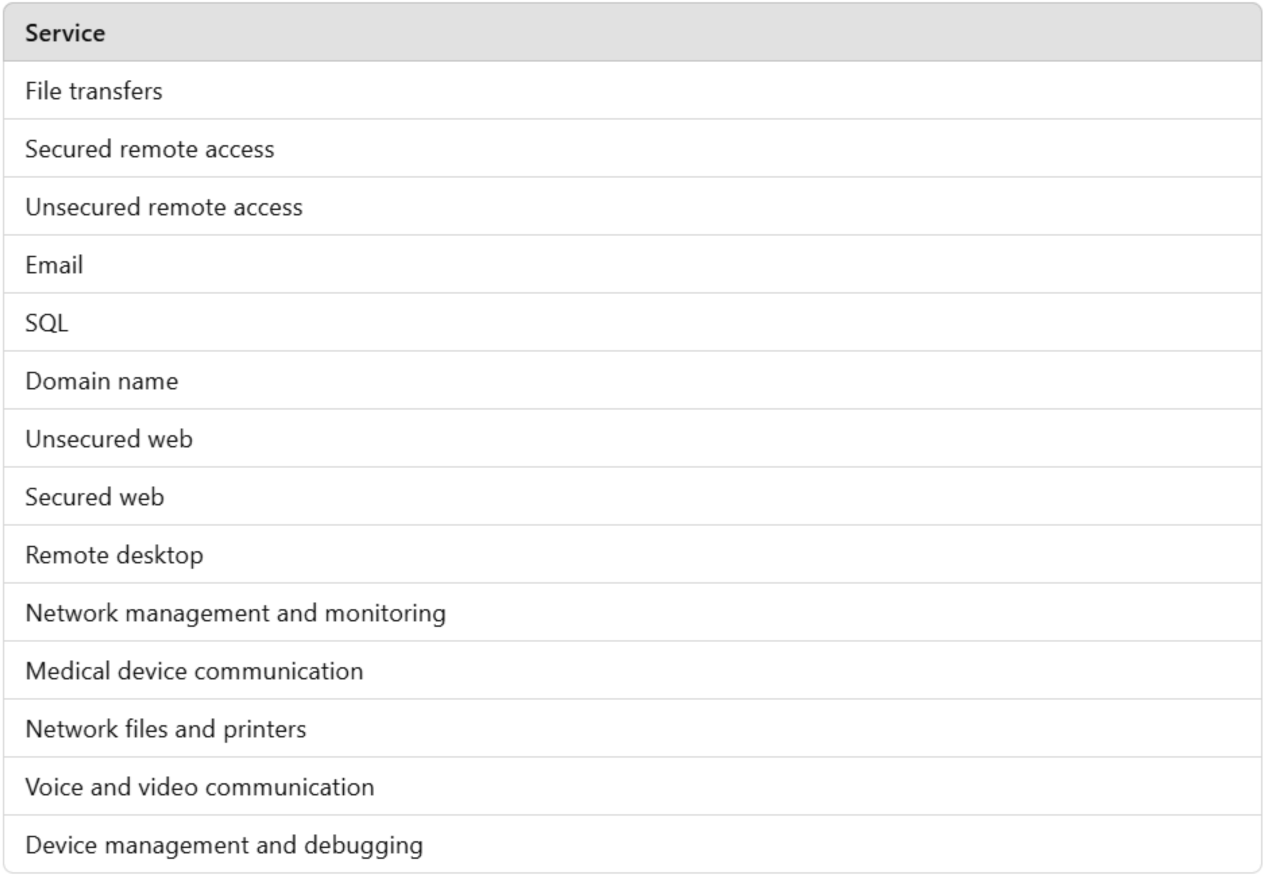
- T-pot offers a wide variety of configured honeypots.

- Docker images for the following honeypots:

    - *adbhoney, beelzebub, ciscoasa, citrixhoneypot, conpot, cowrie, ddospot, dicompot, dionaea, elasticpot, endlessh, galah, go-pot, glutton, h0neytr4p, hellpot, heralding, honeyaml, honeypots, honeytrap, ipphoney, log4pot, mailoney, medpot, miniprint, redishoneypot, sentrypeer, snare, tanner, wordpot.*

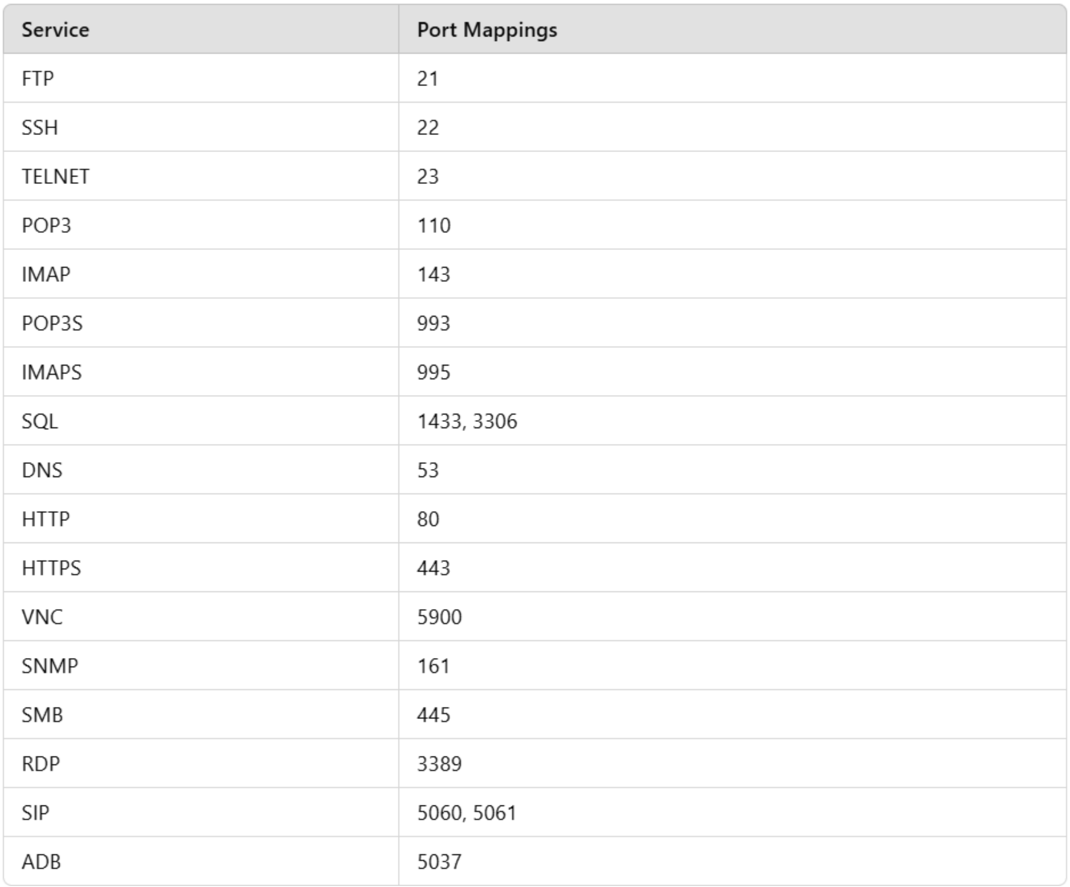
Emulated Services

List of exposed services



Service
File transfers
Secured remote access
Unsecured remote access
Email
SQL
Domain name
Unsecured web
Secured web
Remote desktop
Network management and monitoring
Medical device communication
Network files and printers
Voice and video communication
Device management and debugging

Port Mappings



Service	Port Mappings
FTP	21
SSH	22
TELNET	23
POP3	110
IMAP	143
POP3S	993
IMAPS	995
SQL	1433, 3306
DNS	53
HTTP	80
HTTPS	443
VNC	5900
SNMP	161
SMB	445
RDP	3389
SIP	5060, 5061
ADB	5037

Tools Used

- **Autoheal**: Automatically restarts containers with failed health checks, ensuring continuous operation of honeypots.
- **CyberChef**: A versatile web application for encryption, encoding, compression, and data analysis tasks.
- **Elastic Stack**: Provides visually appealing dashboards for analyzing and visualizing events captured by T-Pot.

- **Elasticvue**: A web-based front-end for browsing and interacting with Elasticsearch clusters.
- **Fatt**: A Pyshark-based script for extracting network metadata and fingerprints from PCAP files and live network traffic.
- **T-Pot Attack Map**: A visually engaging and animated attack map showcasing honeypot activity.
- **P0f**: A passive traffic fingerprinting tool for identifying characteristics of incoming connections.
- **Spiderfoot**: An open-source intelligence (OSINT) automation tool for gathering data about attackers.
- **Suricata**: A powerful Network Security Monitoring engine for real-time analysis and intrusion detection.

Deception Techniques

- LLM-Based Honeypots simulate human interactions to engage attackers realistically and gain valuable insights into attacker behavior and tactics.
- Service emulation of email clients and open ports to web services especially telnet and remote desktop services attract threat actors in attempts to gain remote access and remote execution techniques. In turn, this allows monitoring of specific techniques used by attackers to enhance and refine security measures and improve the honeypot's effectiveness.
- T-pot handled credentials management, ensuring realistic interactions and maintaining collected data integrity.

Monitoring and Data Collection

Log Analytics Setup

Alert Configuration

- I have no custom alert configurations, notification methods, or escalation procedures implemented due to T-pot's automatically configured monitoring and analysis features.

Data collection rules

- Rules are preconfigured by T-pot and collect logs that are deployed to Elesticvue, Kibana, and Attack Map.

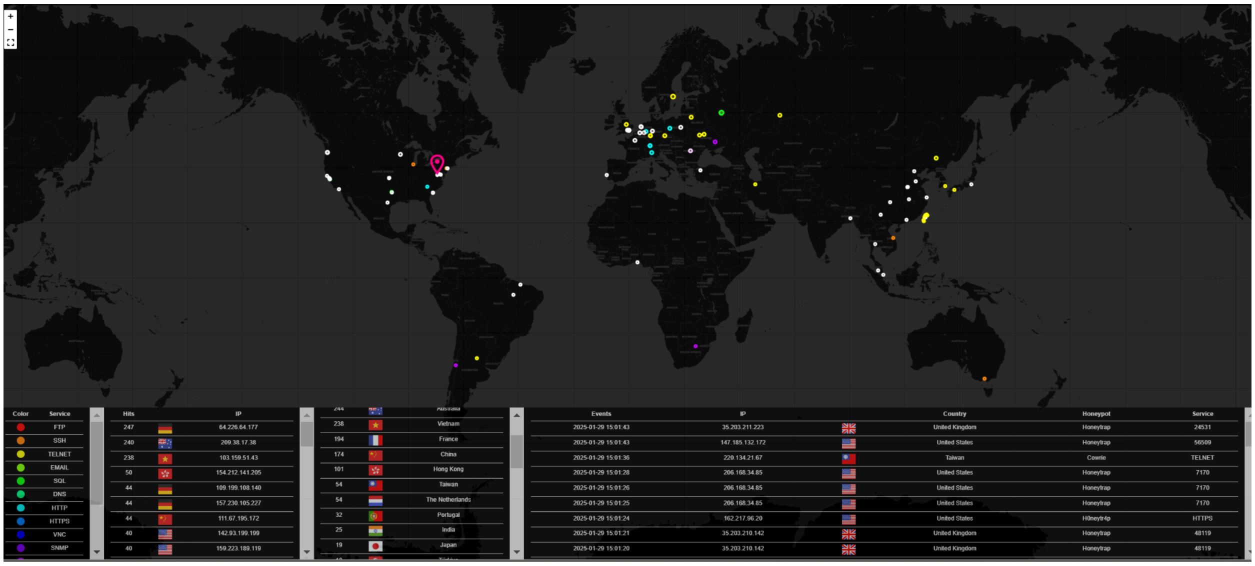
Retention policies

- No retention policies were configured as the preconfigured T-pot deployment manages data storage automatically.

- **Elasticvue**
  - T-pot interface is directly linked to Elasticvue. Log analytics and workspace configuration are automatically configured for log collection.
  - Elasticvue provides resource monitoring for CPU, RAM, HEAP, and disk usage performance metrics.
  - Elasticvue's Shards help manage data distribution efficiently across nodes ensuring optimal honeypot performance by keeping data well-distributed and efficiently managed.

- **Kibana**
  - As shown in the screenshot below (*Kibana dashboards 1 & 2*), Kibana's dashboards are used to visualize data in specific ways to allow ease of data analysis. Dashboard layout helps identify trends, patterns, and anomalies.

- **Dashboards Configuration**
  - **Honeypot Attackers Bar:** Displays the frequency of attacks on each deployed honeypot.
  - **Honeypot Histograms:** Displays timeline of attacks including the number of attacks and unique source IPs. Also, attacks by destination ports, honeypots, and countries. Additionally, features Suricota alert categories.
  - **Attack map -** Visual tool that displays real-time attack data. Including time recorded events of the attacker's country of origin, IP addresses, protocols, and services used. See Attack Map Figure Below.



Color	Service
🔴	FTP
🟠	SSH
🟡	TELNET
🟢	EMAIL
🟢	SQL
🟢	DNS
🔵	HTTP
🔵	HTTPS
🔵	VNC
🟣	SNMP

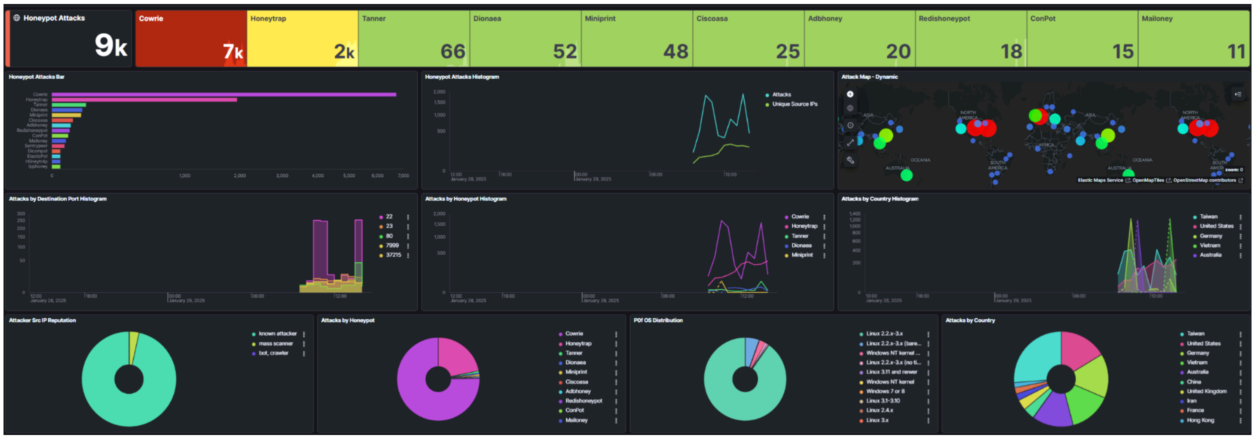
Hits		IP
247	🇩🇪	64.226.64.177
240	🇦🇺	209.38.17.38
238	🇻🇳	103.159.51.43
50	🇭🇰	154.212.141.205
44	🇩🇪	109.199.108.140
44	🇩🇪	157.230.105.227
44	🇨🇳	111.67.195.172
40	🇺🇸	142.93.199.199
40	🇺🇸	159.223.189.119

244	🇦🇺	Australia
238	🇻🇳	Vietnam
194	🇫🇷	France
174	🇨🇳	China
101	🇭🇰	Hong Kong
54	🇹🇼	Taiwan
54	🇳🇱	The Netherlands
32	🇵🇹	Portugal
25	🇮🇳	India
19	🇯🇵	Japan

Events	IP		Country	Honeypot	Service
2025-01-29 15:01:43	35.203.211.223	🇬🇧	United Kingdom	Honeytrap	24531
2025-01-29 15:01:43	147.185.132.172	🇺🇸	United States	Honeytrap	56509
2025-01-29 15:01:36	220.134.21.67	🇹🇼	Taiwan	Cowrie	TELNET
2025-01-29 15:01:28	206.168.34.85	🇺🇸	United States	Honeytrap	7170
2025-01-29 15:01:26	206.168.34.85	🇺🇸	United States	Honeytrap	7170
2025-01-29 15:01:25	206.168.34.85	🇺🇸	United States	Honeytrap	7170
2025-01-29 15:01:24	162.217.96.20	🇺🇸	United States	H0neytr4p	HTTPS
2025-01-29 15:01:21	35.203.210.142	🇬🇧	United Kingdom	Honeytrap	48119
2025-01-29 15:01:20	35.203.210.142	🇬🇧	United Kingdom	Honeytrap	48119

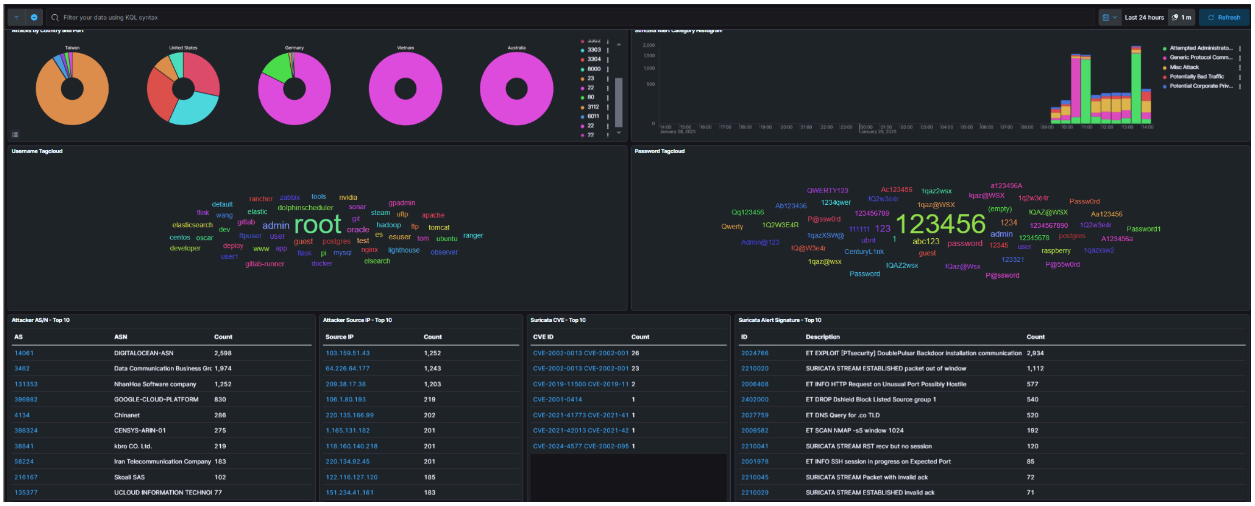
Attack Map

- ○ **Pie Charts**: Compiled data of attacker source IP reputation, attacks by honeypot, country, and ports. Also, includes passive OS fingerprinting operating system distribution.
- ○ **Tagcloud information**: Provides a visual summary of credentials used during the honeypot attacks. See Tagcloud Usernames & Passwords figures below.
- ○ **Top 10:** Insights to the attacker's autonomous system number (ASN) networks' internet service providers (ISP). Also, highlighting the attacker's source IP, Suricata's common vulnerabilities and exposures (CVE), and alert signatures.



Honeypot Attacks	Cowrie	Honeytrap	Tanner	Dionaea	Miniprint	Ciscoasa	Adbhoney	Redishoneypot	ConPot	Mailoney
9k	7k	2k	66	52	48	25	20	18	15	11

Kibana Dashboards 1



Attacker AS/N - Top 10

AS	ASN	Count
14061	DIGITALOCEAN-ASN	2,598
3462	Data Communication Business Grc	1,974
131353	NhanHoa Software company	1,252
396982	GOOGLE-CLOUD-PLATFORM	830
4134	Chinanet	286
398324	CENSYS-ARIN-01	275
38841	kbro CO. Ltd.	219
58224	Iran Telecommunication Company	183
216167	Skoali SAS	102
135377	UCLOUD INFORMATION TECHNOI	77

Attacker Source IP - Top 10

Source IP	Count
103.159.51.43	1,252
64.226.64.177	1,243
209.38.17.38	1,203
106.1.80.193	219
220.135.166.99	202
1.165.131.182	201
118.160.140.218	201
220.134.92.45	201
122.116.127.120	185
151.234.41.161	183

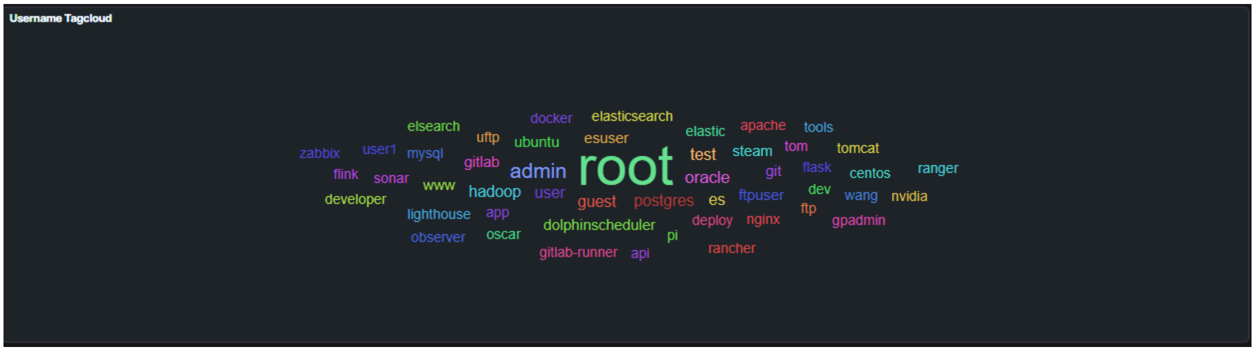
Suricata CVE - Top 10

CVE ID	Count
CVE-2002-0013 CVE-2002-001	26
CVE-2002-0013 CVE-2002-001	23
CVE-2019-11500 CVE-2019-11	2
CVE-2001-0414	1
CVE-2021-41773 CVE-2021-41	1
CVE-2021-42013 CVE-2021-42	1
CVE-2024-4577 CVE-2002-095	1

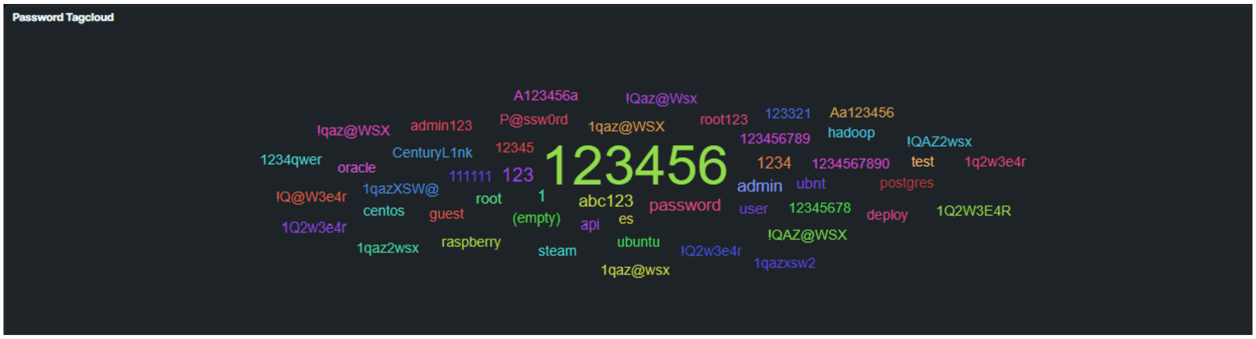
Suricata Alert Signature - Top 10

ID	Description	Count
2024766	ET EXPLOIT [PTsecurity] DoublePulsar Backdoor installation communication	2,934
2210020	SURICATA STREAM ESTABLISHED packet out of window	1,112
2006408	ET INFO HTTP Request on Unusual Port Possibly Hostile	577
2402000	ET DROP Dshield Block Listed Source group 1	540
2027759	ET DNS Query for .co TLD	520
2009582	ET SCAN NMAP -sS window 1024	192
2210041	SURICATA STREAM RST recv but no session	120
2001978	ET INFO SSH session in progress on Expected Port	85
2210045	SURICATA STREAM Packet with invalid ack	72
2210029	SURICATA STREAM ESTABLISHED invalid ack	71

Kibana Dashboards 2



Tagcloud Usernames



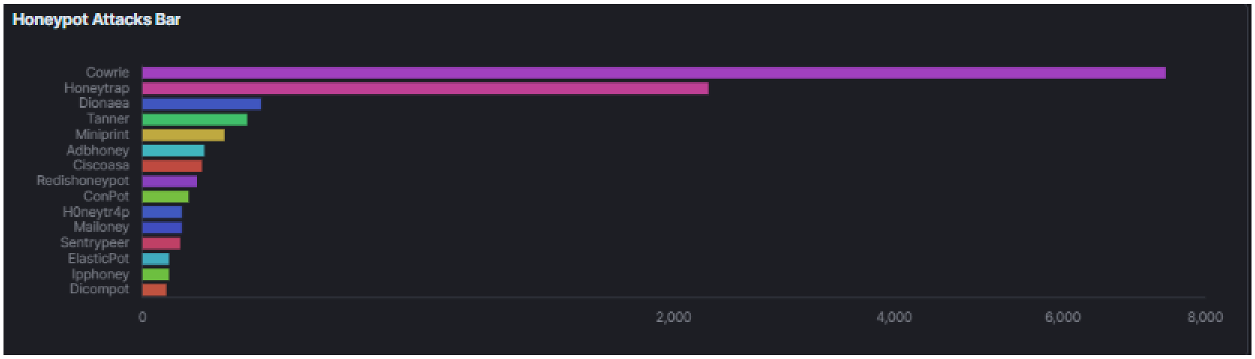
Tagcloud Passwords

Analysis

Key Findings

- **Total number of attacks recorded**
  - 10k attacks in total

        - 7k Cowrie
        - 3k Honeytrap
        - 100 Doinaea
        - 70 Tanner
        - 48 Miniprint
        - 27 Adbhoney
        - 25 Ciscoasa
        - 21 Redishhoneypot
        - 15 ConPot
        - 11 H0neytr4p



Attack frequencies

- **Most common attack vectors**
    - ET EXPLOIT [PTsecurity] DoublePulsar Backdoor installation communication (2,934)
        - Most frequent attacks observed.
        - Targeting Microsoft Windows is often delivered through the EternalBlue exploit and is best known for its recent use in deploying the WannaCry ransomware (Wanna Decryptor 2.0).
        - DoublePulsar attacks have been proven difficult to prevent and detect indicating sophisticated attack attempts.

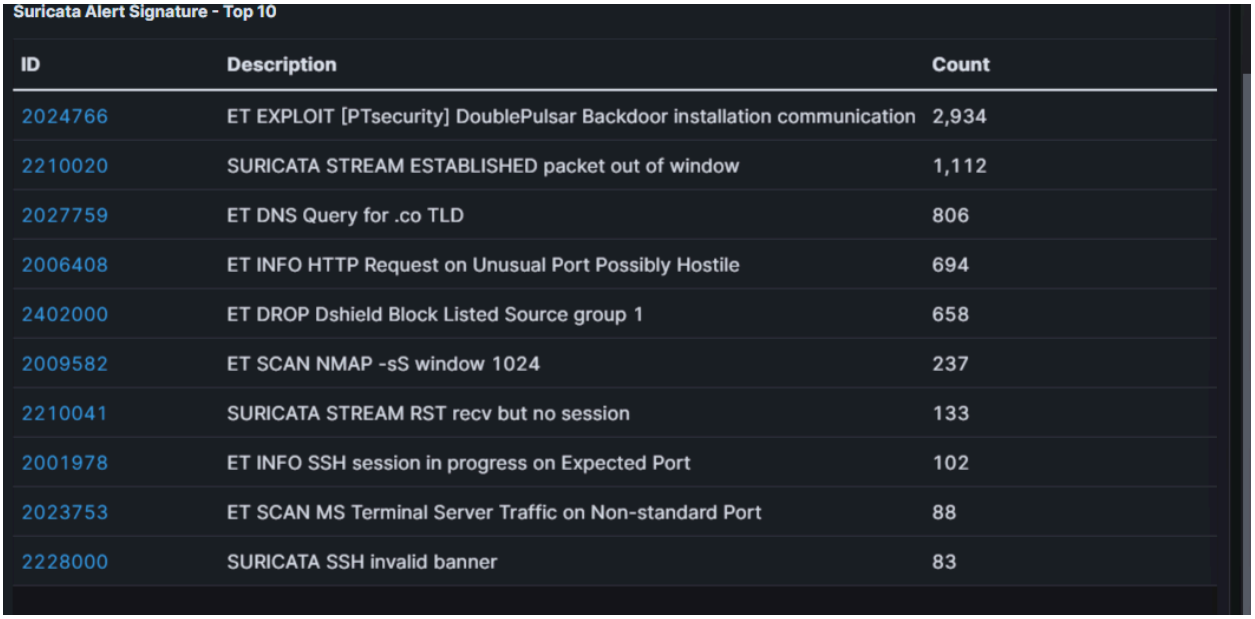
    - SURICATA STREAM ESTABLISHED packet out of window(1,112)
        - The second most frequent attack detected.
        - Indicates TCP sequence manipulation where packets arrive outside the expected TCP window sequence.
        - These anomalies suggest advanced attack techniques including:
            - TCP session hijacking attempts.
            - Man-in-the-middle attack vectors.
            - Network evasion techniques.
            - Security control bypassing efforts.
            - The high frequency of these alerts (1,112) demonstrates sophisticated threat actors utilizing advanced network manipulation rather than simple scanning tools.

    - ET DNS Query for .co TLD (806)
        -

        - The third most frequent attack observed.
        - Suspicious DNS Queries.
        - Possible command and control (C2) communications.
        - Domain generation algorithms (DGAs) looking for active C2 servers.
        - To assess if the DNS queries are malicious, analyze the specific domain being queried, look for patterns in timing and frequency, identify the query sources, and check for correlations with other suspicious activities.

    - ET INFO HTTP Request on Unusual Port Possibly Hostile.
        - The fourth most frequent attack observed.
        - HTTP traffic is being detected on non-standard ports (ports other than 80/443).
        - This could indicate:
            - Port scanning attempts.
            - Attackers looking for web services on uncommon ports.
            - Attempts to bypass security controls.
            - Malware communication attempts.

    - ET DROP Dshield Block Listed Source group 1
        - The fifth most frequent attack observed.
        - Receiving traffic from an IP address that has been reported for malicious activity by multiple sources in the DShield community.



Suricata Alert Signature - Top 10

ID	Description	Count
2024766	ET EXPLOIT [PTsecurity] DoublePulsar Backdoor installation communication	2,934
2210020	SURICATA STREAM ESTABLISHED packet out of window	1,112
2027759	ET DNS Query for .co TLD	806
2006408	ET INFO HTTP Request on Unusual Port Possibly Hostile	694
2402000	ET DROP Dshield Block Listed Source group 1	658
2009582	ET SCAN NMAP -sS window 1024	237
2210041	SURICATA STREAM RST recv but no session	133
2001978	ET INFO SSH session in progress on Expected Port	102
2023753	ET SCAN MS Terminal Server Traffic on Non-standard Port	88
2228000	SURICATA SSH invalid banner	83

Top 10 Suricata Alert Signatures

- **Notable attack patterns**

    - Geographic distribution of threats
    - Taiwan (~35% of total attacks)
    - United States (~25% of total attacks)

  - Germany (~15% of total attacks)
  - Vietnam (~10% of total attacks)
  - Australia (~5% of total attacks)
  - Others (~10% of total attacks)

- **Top Attempted Usernames:**
  - “root" appears most prominent
  - "admin"
  - "default"
  - Other system-level usernames

- **Common Password Patterns**
  - Numerical sequences (like "123456")
  - Simple passwords
  - Default credentials

- **Top Attacker ASNs**
  - DIGITALOCEAN-ASN
  - Data Communication Business Group
  - GOOGLE-CLOUD-PLATFORM
  - Others listed with specific counts

Technical Challenges & Solutions

- **Challenge 1: Authentication Access Issues**
  - Challenge: Encountered difficulty accessing T-Pot interface due to credential authentication problems
  - Solution: Resolved by utilizing Azure Portal's VM password reset functionality under the Support + troubleshooting section, which allowed successful system access and continuation of honeypot monitoring
- **Challenge 2: Data Preservation Limitations**
  - Challenge: Unable to create VM snapshots to preserve attack data findings for later analysis
  - Solution: Implemented an alternative approach by resetting T-Pot and conducting a new one-hour data collection period to generate fresh attack data for analysis. This provided current threat landscape information while demonstrating the rapid attraction of malicious actors to the honeypot

Skills Demonstrated

Technical Skills:

- Cloud Infrastructure (Azure VM & NSG Configuration)
- Security Information & Event Management (Kibana)
- Linux System Administration
- Network Protocol Analysis
- Virtual Machine Management

Security Skills:

- Honeypot Deployment & Management
- Threat Detection & Analysis
- Attack Vector Identification
- Security Monitoring
- Network Security Implementation

Documentation Skills:

- Technical Report Writing
- Attack Pattern Analysis Documentation
- Security Control Documentation
- Data Visualization Interpretation