

# High-interaction honeypots

DALIBOR DOŠA



# Čo je honeypot?

Definícia:

- Honeypot je simulovaný systém, ktorý slúži na prilákanie útočníkov.
- Cieľom je zaznamenávať ich správanie a analyzovať použité techniky útoku.

Typy honeypotov:

- **Low-interaction:** Obmedzené funkcie, nižšie riziko kompromitácie.
- **High-interaction:** Realistická simulácia, vyššia úroveň interakcie.

# Návrh riešenia

Azure Virtual Network (VNet)

Honeypot subnet



Cowrie



T-Pot



MongoDB-  
HoneyProxy



IoT  
honeypot

# Cowrie



A medium to high interaction SSH and Telnet honeypot



Designed to log brute force attacks and shell interaction



Simulates a Unix system to attract attackers

# T-Pot

- An all-in-one honeypot platform
- Combines multiple honeypot technologies
- Features a web interface for monitoring
- Provides comprehensive threat intelligence gathering





SPECIALIZED HONEYPOT  
FOR MONGODB ATTACKS



MONITORS UNAUTHORIZED  
ACCESS ATTEMPTS



LOGS DATABASE  
EXPLOITATION ATTEMPTS

# MongoDB-HoneyProxy



SIMULATES INTERNET  
OF THINGS DEVICES



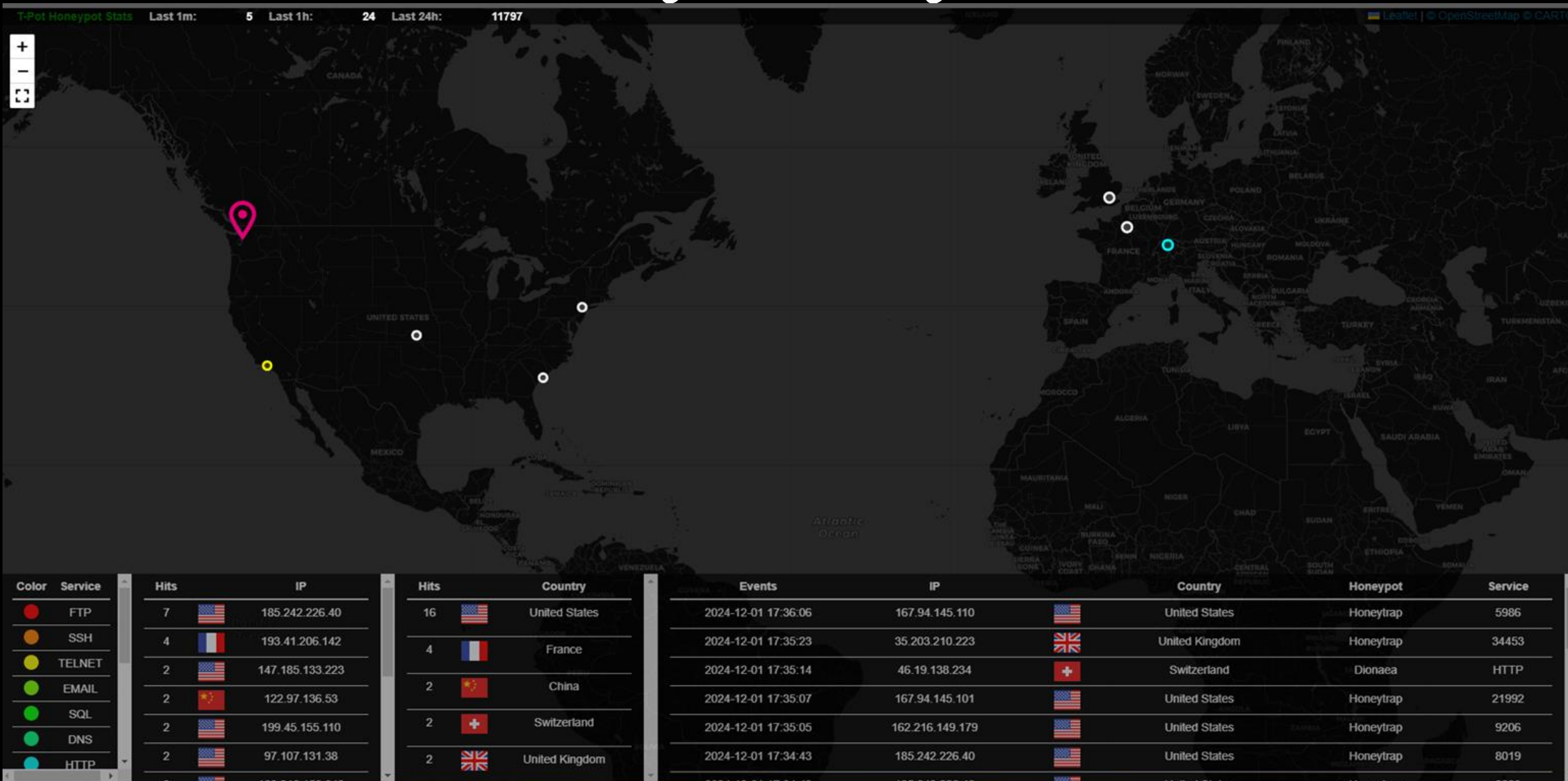
CAPTURES IOT-SPECIFIC  
ATTACK PATTERNS



MONITORS BOTNET  
INFECTION ATTEMPTS

# IoT Honeypot

# Výsledky



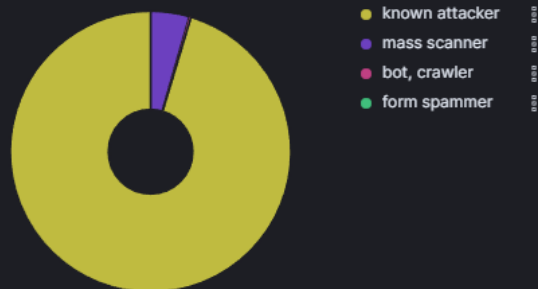


# Výsledky

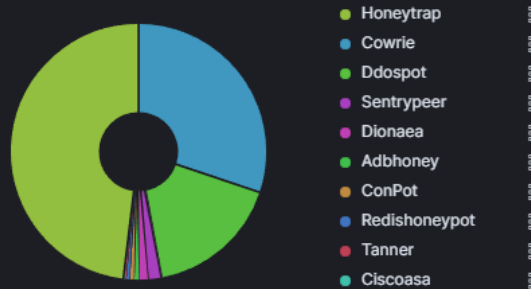


# Výsledky

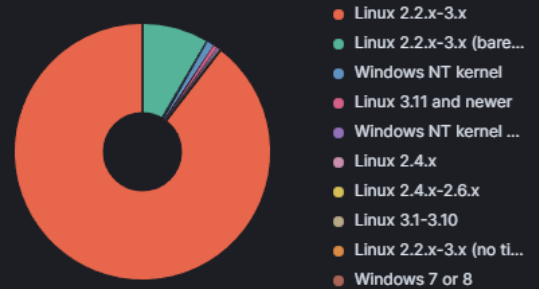
Attacker Src IP Reputation



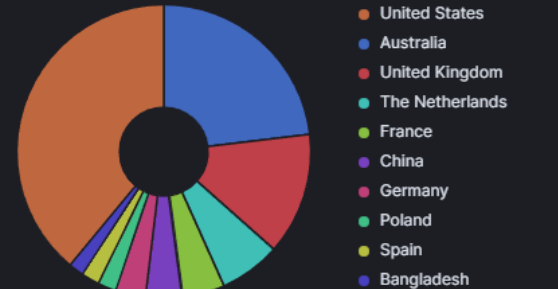
Attacks by Honeypot



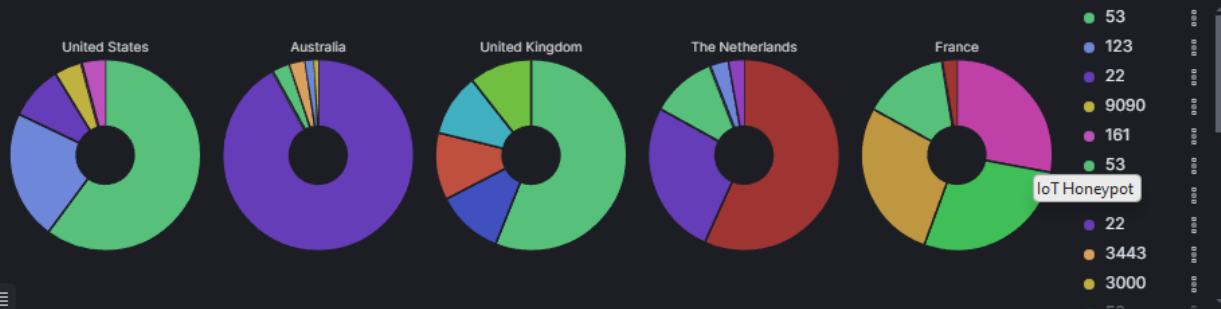
Pof OS Distribution



Attacks by Country



Attacks by Country and Port



Suricata Alert Category Histogram



# Výsledky

Attacker AS/N - Top 10			Attacker Source IP - Top 10		Suricata CVE - Top 10		Suricata Alert Signature - Top 10		
AS	ASN	Count	Source IP	Count	CVE ID	Count	ID	Description	Count of records
396982	GOOGLE-CLOUD-PL	3,383	209.38.91.62	2,360	CVE-2002-0013 CV	40	2210051	SURICATA STREAM Packet with broke	32,720
14061	DIGITALOCEAN-ASN	2,631	45.148.10.46	377	CVE-2002-0013 CV	31	2402000	ET DROP Dshield Block Listed Source	2,815
48090	Pptechnology Limited	377	202.4.115.172	180	CVE-2020-11899	12	2100384	GPL ICMP PING	1,119
20473	AS-VULTR	239	134.209.168.99	175	CVE-2001-0414	4	2006408	ET INFO HTTP Request on Unusual P	1,110
216167	Skoali SAS	234	37.148.204.83	164	CVE-2019-11500 C	3	2024766	ET EXPLOIT [PTsecurity] DoublePulsa	1,090
211298	Driftnet Ltd	231	40.74.252.77	78	CVE-2014-8361 CV	2	2009582	ET SCAN NMAP -sS window 1024	422
135377	UCLOUD INFORMATIK	200	194.165.17.11	77	CVE-1999-0183	1	2023753	ET SCAN MS Terminal Server Traffic	371
8075	MICROSOFT-CORP-M	192	193.41.206.156	63	CVE-1999-0517	1	2027759	ET DNS Query for .co TLD	317
214340	Eduardo Denis Tanas	184	34.76.133.13	62	CVE-2009-2765	1	2400007	ET DROP Spamhaus DROP Listed Trai	239
23956	AmberIT Limited	180	193.41.206.142	60	CVE-2013-7471 CV	1	2210041	SURICATA STREAM RST recv but no s	236
Rows per page: 10			Rows per page: 10		Rows per page: 10		Rows per page: 10		



```
{
  "eventid": "cowrie.session.closed", "duration": "1.8101587295532227", "message": "Connection lost after 1 seconds", "sensor": "bit", "timestamp": "2024-11-24T00:26:02.771994Z", "src_ip": "206.189.146.57", "session": "7db2b3ab17fd"}
{"eventid": "cowrie.session.connect", "src_ip": "167.94.145.105", "src_port": 47848, "dst_ip": "10.0.0.4", "dst_port": 2222, "session": "4f43d5d94bfd", "protocol": "ssh", "message": "New connection: 167.94.145.105:47848 (10.0.0.4:2222) [session: 4f43d5d94bfd]", "sensor": "bit", "timestamp": "2024-11-24T00:37:35.984789Z"}
{"eventid": "cowrie.client.version", "version": "SSH-2.0-Go", "message": "Remote SSH version: SSH-2.0-Go", "sensor": "bit", "timestamp": "2024-11-24T00:37:35.985773Z", "src_ip": "167.94.145.105", "session": "4f43d5d94bfd"}
{"eventid": "cowrie.client.kex", "hash": "873a5fb5fedc2d4f8638ebde4abc6cfc", "hashAlgorithms": "curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha256,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,arcfour256,arcfour128,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,arcfour256,arcfour128,aes128-cbc,hmac-sha2-256,hmac-sha1,hmac-sha1-96;none", "keyAlgs": "ssh-rsa-cert-v01@openssh.com,ssh-dss-cert-v01@openssh.com,ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,ssh-ed25519-cert-v01@openssh.com,ssh-rsa-cert-v01@openssh.com,ssh-dss-cert-v01@openssh.com,ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,ssh-ed25519-cert-v01@openssh.com,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-rsa,ssh-dss,ssh-ed25519,ssh-rsa-cert-v01@openssh.com,ssh-dss-cert-v01@openssh.com,ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,ssh-ed25519-cert-v01@openssh.com,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-rsa,ssh-dss,ssh-ed25519", "encCS": "aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,arcfour256,arcfour128,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,arcfour256,arcfour128,aes128-cbc", "macCS": "hmac-sha2-256,hmac-sha1,hmac-sha1-96", "compCS": "none", "langCS": "", "message": "SSH client hash fingerprint: 873a5fb5fedc2d4f8638ebde4abc6cfc", "sensor": "bit", "timestamp": "2024-11-24T00:37:36.142230Z", "src_ip": "167.94.145.105", "session": "4f43d5d94bfd"}
{"eventid": "cowrie.session.closed", "duration": "15.343737125396729", "message": "Connection lost after 15 seconds", "sensor": "bit", "timestamp": "2024-11-24T00:37:51.329353Z", "src_ip": "167.94.145.105", "session": "4f43d5d94bfd"}
{"eventid": "cowrie.session.connect", "src_ip": "198.235.24.120", "src_port": 56353, "dst_ip": "10.0.0.4", "dst_port": 2222, "session": "e13341a4f135", "protocol": "ssh", "message": "New connection: 198.235.24.120:56353 (10.0.0.4:2222) [session: e13341a4f135]", "sensor": "bit", "timestamp": "2024-11-24T00:49:45.783003Z"}
{"eventid": "cowrie.session.closed", "duration": "0.1515789031982422", "message": "Connection lost after 0 seconds", "sensor": "bit", "timestamp": "2024-11-24T00:49:45.935309Z", "src_ip": "198.235.24.120", "session": "e13341a4f135"}
{"eventid": "cowrie.session.connect", "src_ip": "45.148.10.46", "src_port": 56356, "dst_ip": "10.0.0.4", "dst_port": 2222, "session": "48440a3f27d8", "protocol": "ssh", "message": "New connection: 45.148.10.46:56356 (10.0.0.4:2222) [session: 48440a3f27d8]", "sensor": "bit", "timestamp": "2024-11-24T00:53:18.126112Z"}
{"eventid": "cowrie.client.version", "version": "SSH-2.0-Go", "message": "Remote SSH version: SSH-2.0-Go", "sensor": "bit", "timestamp": "2024-11-24T00:53:18.161495Z", "src_ip": "45.148.10.46", "session": "48440a3f27d8"}
{"eventid": "cowrie.client.kex", "hash": "0a07365cc01fa9fc82608ba4019af499", "hashAlgorithms": "curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group14-sha256,diffie-hellman-group14-sha1,ext-info-c,kex-strict-c-v00@openssh.com,aes128-gcm@openssh.com,aes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1,hmac-sha1-96;none", "keyAlgs": "curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group14-sha256,diffie-hellman-group14-sha1,ext-info-c,kex-strict-c-v00@openssh.com", "keyAlgs": "rsa-sha2-256-cert-v01@openssh.com,rsa-sha2-512-cert-v01@openssh.com,ssh-rsa-cert-v01@openssh.com,ssh-dss-cert-v01@openssh.com,ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,ssh-ed25519-cert-v01@openssh.com,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,rsa-sha2-256,rsa-sha2-512,ssh-rsa,ssh-dss,ssh-ed25519", "encCS": "aes128-gcm@openssh.com,aes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr", "macCS": "hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1,hmac-sha1-96", "compCS": "none", "langCS": "", "message": "SSH client hash fingerprint: 0a07365cc01fa9fc82608ba4019af499", "sensor": "bit", "timestamp": "2024-11-24T00:53:18.273688Z", "src_ip": "45.148.10.46", "session": "48440a3f27d8"}
{"eventid": "cowrie.login.failed", "username": "root", "password": "123456", "message": "Login attempt [root/123456] failed", "sensor": "bit", "timestamp": "2024-11-24T00:53:18.883785Z", "src_ip": "45.148.10.46", "session": "48440a3f27d8"}
{"eventid": "cowrie.session.closed", "duration": "1.9237816333770752", "message": "Connection lost after 1 seconds", "sensor": "bit", "timestamp": "2024-11-24T00:53:20.050673Z", "src_ip": "45.148.10.46", "session": "48440a3f27d8"}
{"eventid": "cowrie.session.connect", "src_ip": "45.148.10.46", "src_port": 56364, "dst_ip": "10.0.0.4", "dst_port": 2222, "session": "fe74e4273962", "protocol": "ssh", "message": "New connection: 45.148.10.46:56364 (10.0.0.4:2222) [session: fe74e4273962]", "sensor": "bit", "timestamp": "2024-11-24T00:53:20.228862Z"}
{"eventid": "cowrie.client.version", "version": "SSH-2.0-Go", "message": "Remote SSH version: SSH-2.0-Go", "sensor": "bit", "timestamp": "2024-11-24T00:53:20.246418Z", "src_ip": "45.148.10.46", "session": "fe74e4273962"}
{"eventid": "cowrie.client.kex", "hash": "0a07365cc01fa9fc82608ba4019af499", "hashAlgorithms": "curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group14-sha256,diffie-hellman-group14-sha1,ext-info-c,kex-strict-c-v00@openssh.com,aes128-gcm@openssh.com,aes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1,hmac-sha1-96;none", "keyAlgs": "curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group14-sha256,diffie-hellman-group14-sha1,ext-info-c,kex-strict-c-v00@openssh.com", "keyAlgs": "rsa-sha2-256-cert-v01@openssh.com,rsa-sha2-512-cert-v01@openssh.com,ssh-rsa-cert-v01@openssh.com,ssh-dss-cert-v01@openssh.com,ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,ssh-ed25519-cert-v01@openssh.com,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,rsa-sha2-256,rsa-sha2-512,ssh-rsa,ssh-dss,ssh-ed25519", "encCS": "aes12
```

# Výsledky honeything a Mongoddb

FAIL



