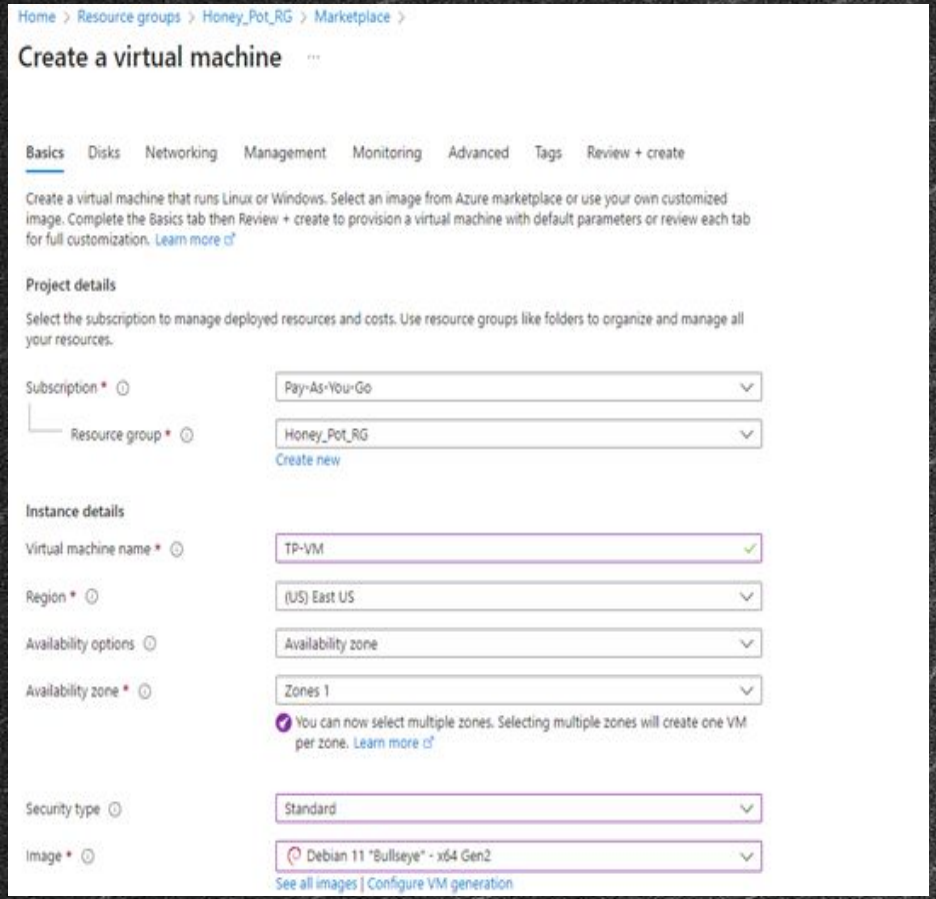
HoneyPot

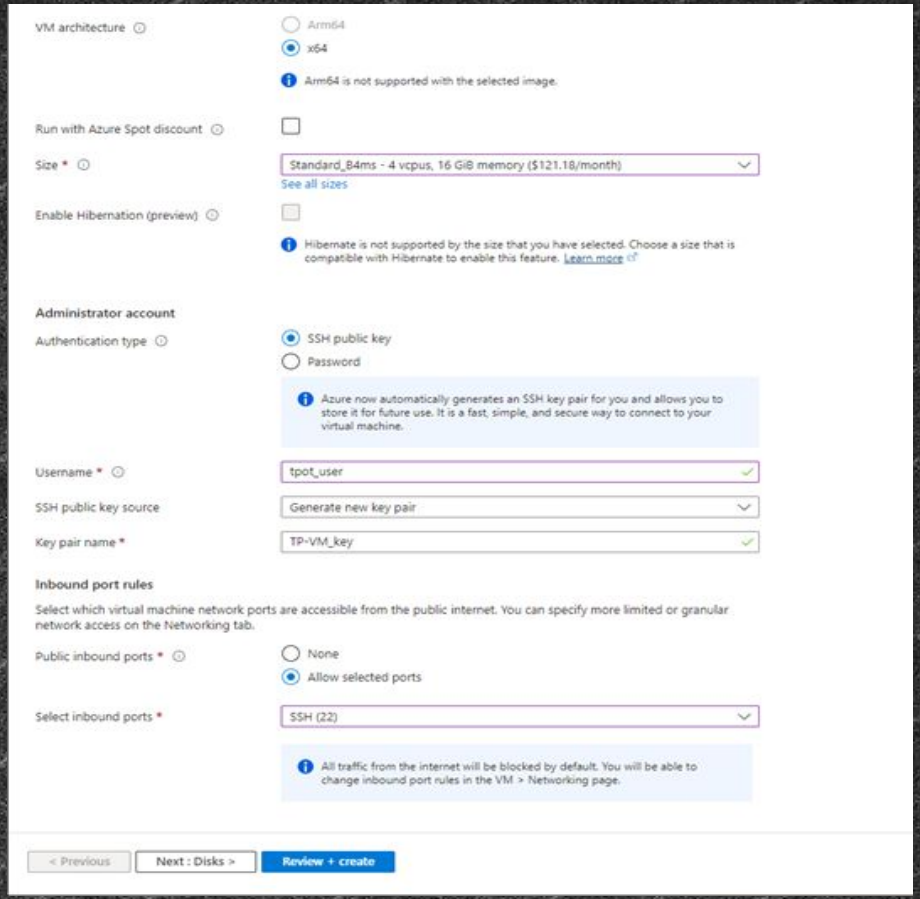
Security Tech Solutions, LLC

Intro to HoneyPot

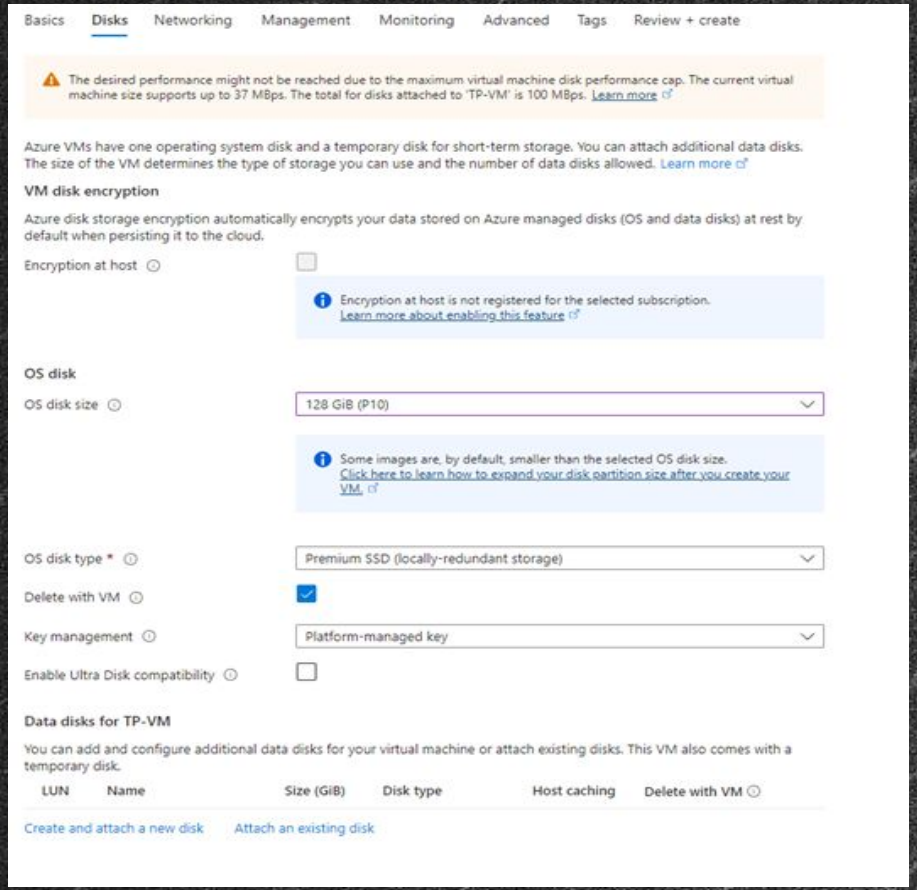
- **What is a honeypot?**
  - A cyber trap or decoy designed to look like a legitimate part of a system, network, or other digital environment
- **How do they operate?**
  - Research vs Production
  - Use security vulnerabilities to lure in attackers
- **Benefits of using a honeypot**
  - Detection of malicious activity
  - Diversion of malicious traffic
  - Data collection

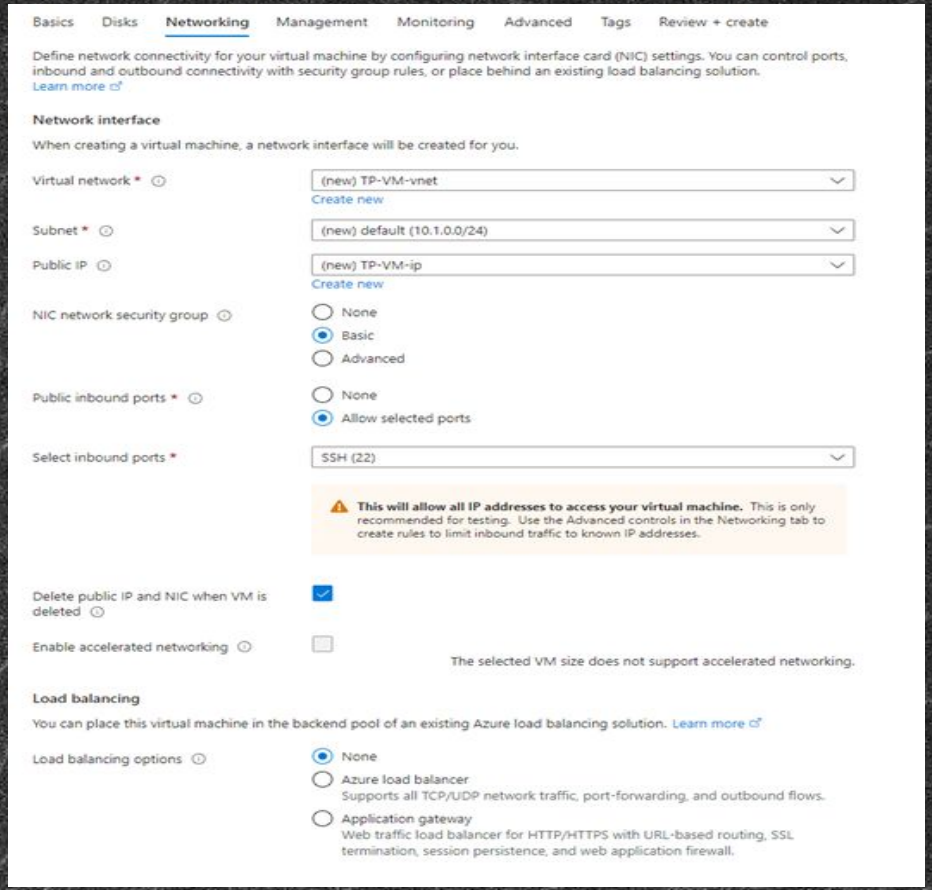
Deployment to Azure



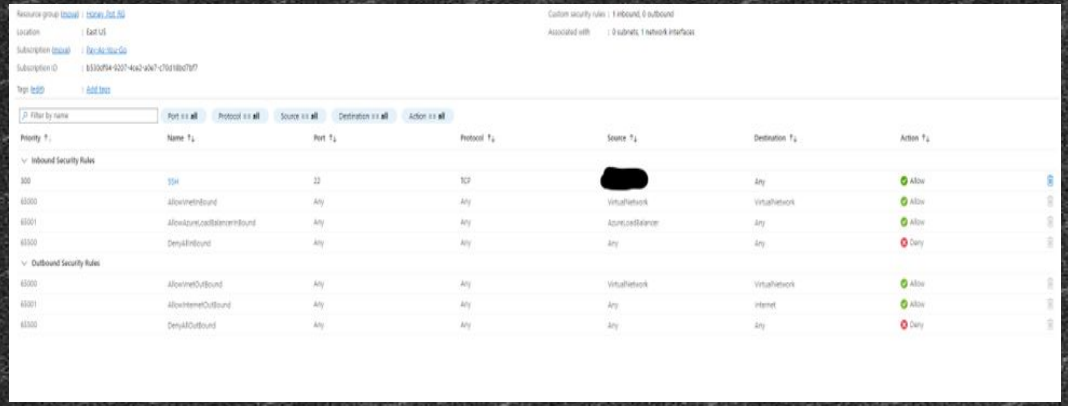


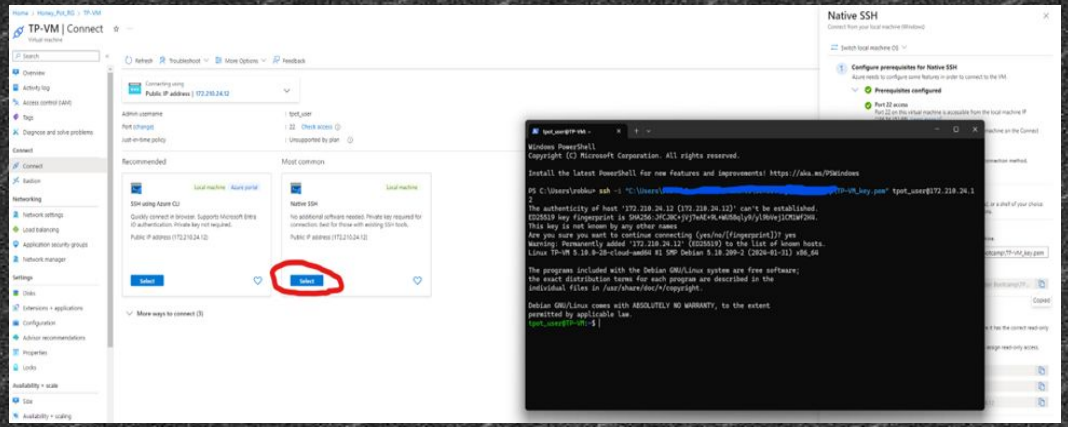
Disk and Networking





Net_Sec Group and Preparing for Install

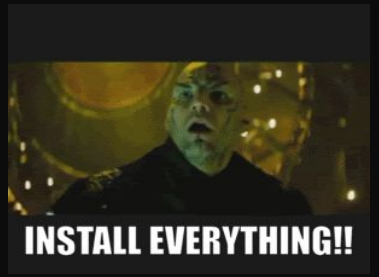




Physical Network install

tpot_user@TP-VM: ~/tpotce

```
tpot_user@TP-VM:~$ git clone https://github.com/telekom-security/tpotce
Cloning into 'tpotce'...
remote: Enumerating objects: 15864, done.
remote: Counting objects: 100% (998/998), done.
remote: Compressing objects: 100% (502/502), done.
remote: Total 15864 (delta 483), reused 961 (delta 461), pack-reused 14866
Receiving objects: 100% (15864/15864), 278.39 MiB | 57.64 MiB/s, done.
Resolving deltas: 100% (8749/8749), done.
tpot_user@TP-VM:~$ cd tpotce
tpot_user@TP-VM:~/tpotce$ sudo ./makeiso.sh
```

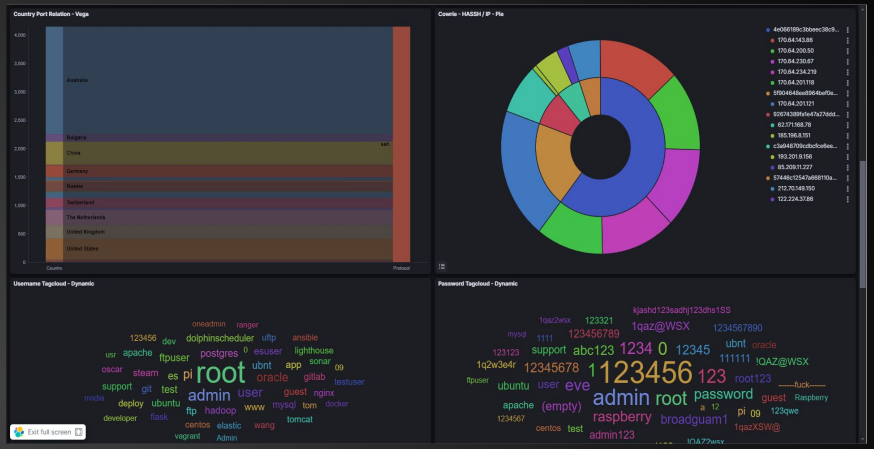


User Install Method

```
tpot_user@TP-VM:~/tpotce$ git clone https://github.com/telekom-security/tpotce
Cloning into 'tpotce'...
remote: Enumerating objects: 15864, done.
remote: Counting objects: 100% (998/998), done.
remote: Compressing objects: 100% (503/503), done.
remote: Total 15864 (delta 483), reused 960 (delta 460), pack-reused 14866
Receiving objects: 100% (15864/15864), 278.39 MiB | 54.86 MiB/s, done.
Resolving deltas: 100% (8749/8749), done.
tpot_user@TP-VM:~/tpotce$ cd tpotce/iso/installer/
tpot_user@TP-VM:~/tpotce/tpotce/iso/installer$ sudo ./install.sh --type=user
```

(If you have Debian already Installed)

Elasticvue/Kibana



Attacker AS/N - Top 10 - Dynamic

AS	ASN	Count
14061	DIGITALOCEAN-ASN	11,136
206264	Amarutu Technology Ltd	1,180
51167	Contabo GmbH	891
51852	Private Layer INC	821
4766	Korea Telecom	762
45090	Shenzhen Tencent Computer Systems Company ...	659
204428	SS-Net	631
49505	OOO Network of data-centers Selectel	484
4134	Chinanet	313
57523	Chang Way Technologies Co. Limited	298

Src IP - Top 10 - Dynamic

Source IP	Count
170.64.201.121	2,328
170.64.143.86	1,570
170.64.200.50	1,432
170.64.230.67	1,426
170.64.234.219	1,423
170.64.201.118	1,286
183.81.169.238	1,180
161.35.165.241	1,148
62.171.168.78	891
179.43.180.106	821

Cowrie Input - Top 10

Command Line Input	Count
apt install sudo curl -y	58
apt update	58
./oinasf	43
./oinasf; dd if=/proc/self/exe bs=22 count=1 || while read i; do echo ...	43
while read i	43
uname -s -v -n -r -m	30
uname -a	27
/ip cloud print	20
cat /proc/cpuinfo	9
echo Hi | cat -n	9

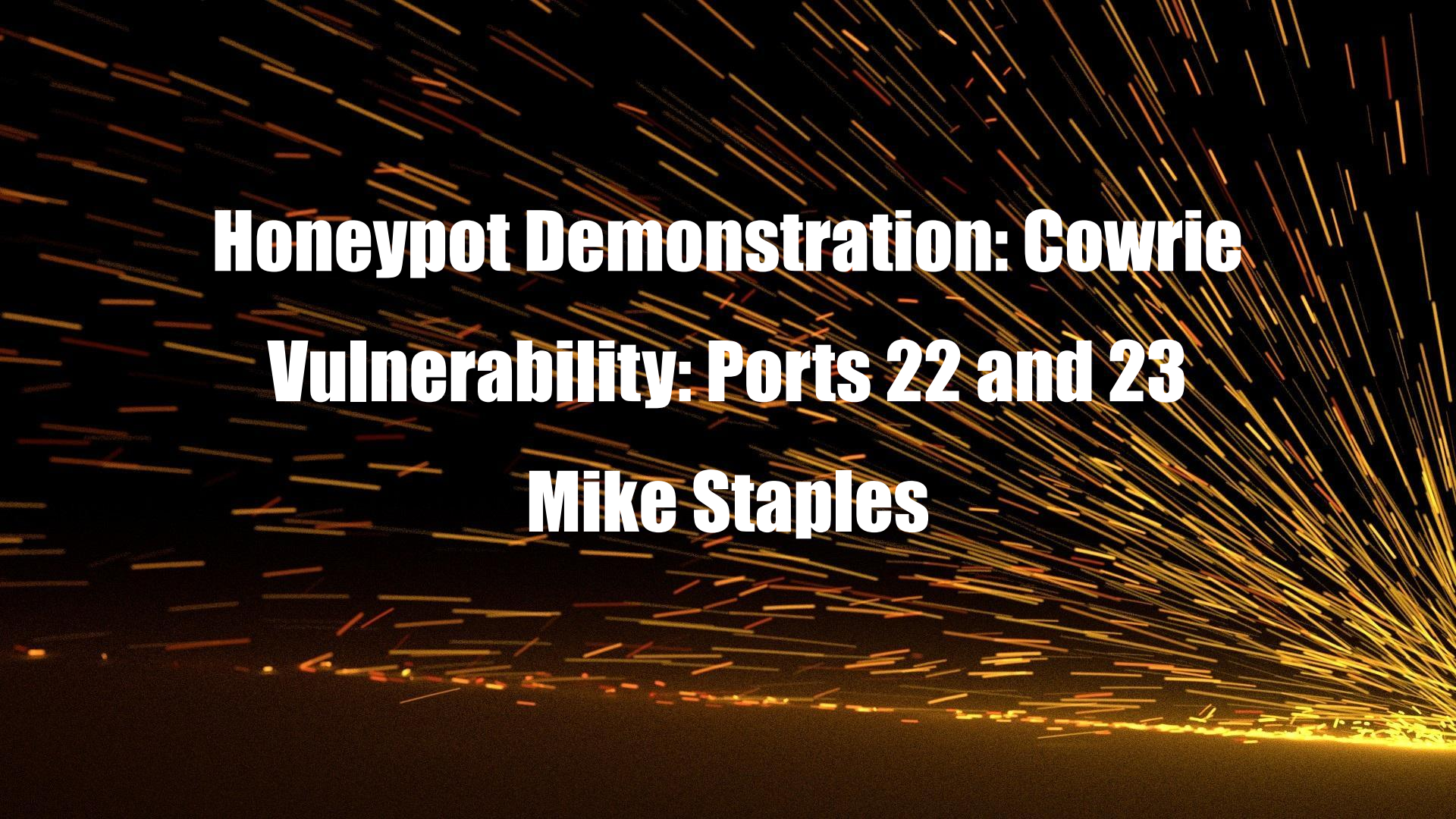
Cowrie - Top URI Downloads

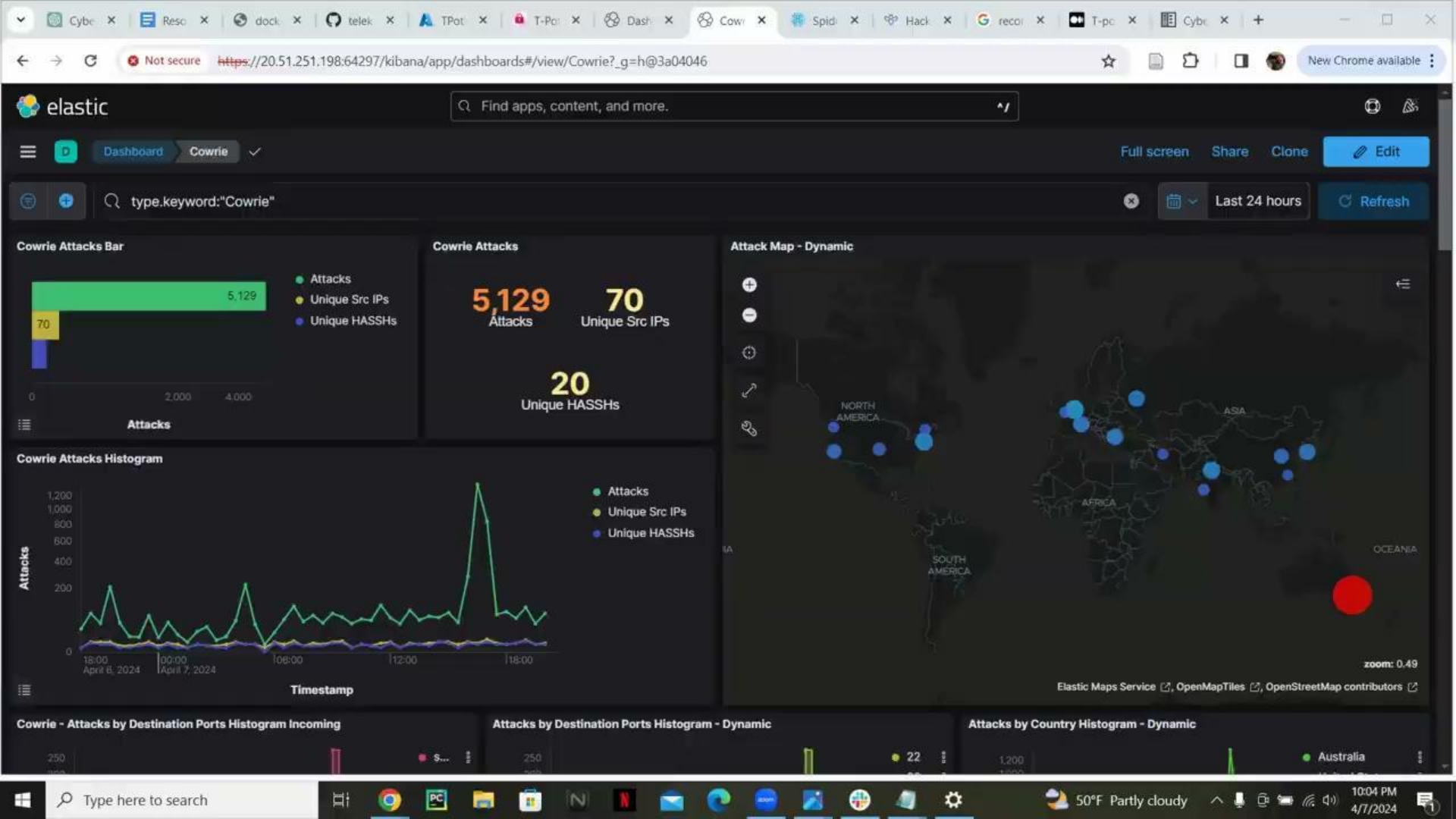
Filename	T-Pot Path (/data/cowrie/downloads)	Count
http://103.163.214.97/sh	dl/18e0f574bf11bc5e7de8c95b83c187649b2d87d74651e59d9c2aad53ac7bb...	4

Cowrie - Top Downloads

Filename	T-Pot Path (/data/cowrie/downloads)	Count
sshd	dl/94f2e4d8d4436874785cd14e6e6d403507b8750852f7f2040352069a75da4c00	1
sshd	dl/ca48a4225ffd98afb2f389f421403a741d005652f435a2a6a4ccc63dd08f8a7e	1

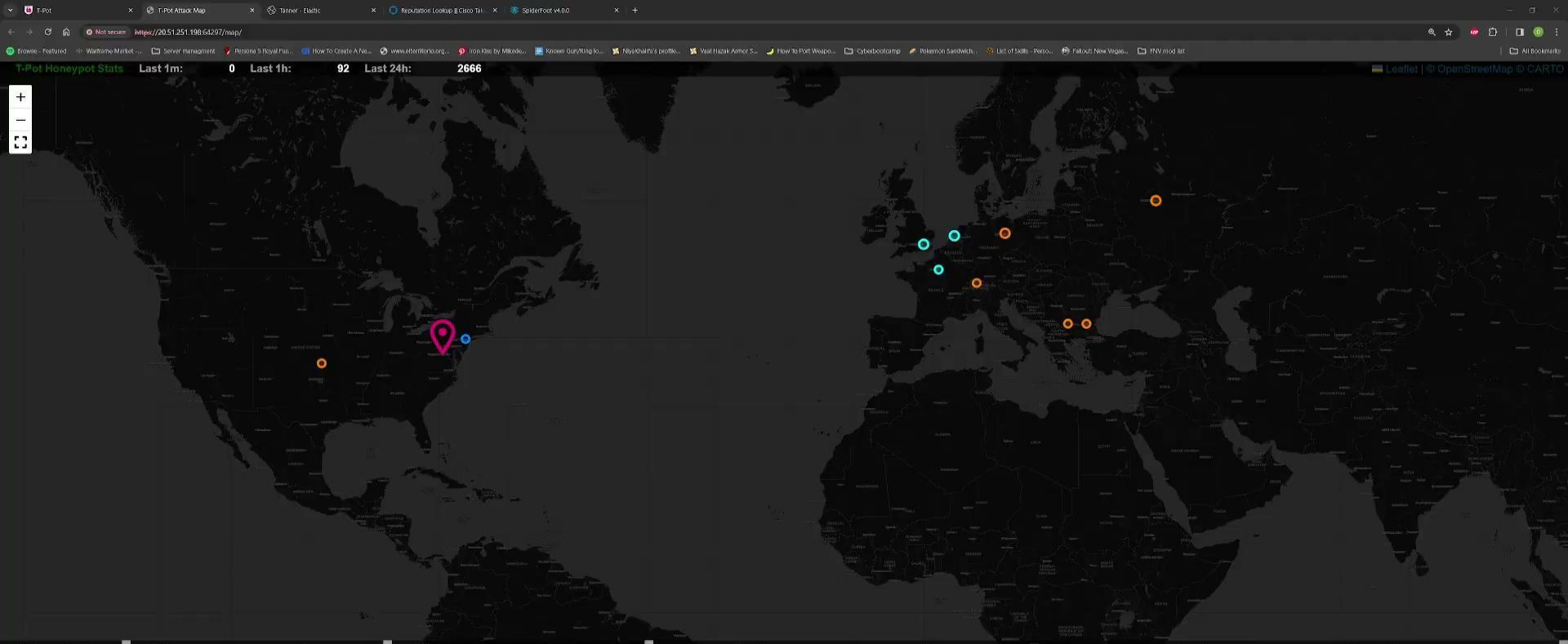
Exit full screen


Honeypot Demonstration: Cowrie
Vulnerability: Ports 22 and 23
Mike Staples


elastic
Find apps, content, and more.
Dashboard
Cowrie
Full screen
Share
Clone
Edit
type.keyword:"Cowrie"
Last 24 hours
Refresh
Cowrie Attacks Bar
5,129
70
Attacks
Unique Src IPs
Unique HASSHs
0
2,000
4,000
Attacks
Cowrie Attacks
5,129
Attacks
70
Unique Src IPs
20
Unique HASSHs
Attack Map - Dynamic
NORTH AMERICA
SOUTH AMERICA
AFRICA
ASIA
OCEANIA
zoom: 0.49
Elastic Maps Service, OpenMapTiles, OpenStreetMap contributors
Cowrie Attacks Histogram
1,200
1,000
800
600
400
200
0
Attacks
18:00
April 6, 2024
00:00
April 7, 2024
06:00
12:00
18:00
Timestamp
Attacks
Unique Src IPs
Unique HASSHs
Cowrie - Attacks by Destination Ports Histogram Incoming
Attacks by Destination Ports Histogram - Dynamic
22
Attacks by Country Histogram - Dynamic
Australia
Not secure
https://20.51.251.198:64297/kibana/app/dashboards#/view/Cowrie?_g=h@3a04046
New Chrome available
Type here to search
50°F Partly cloudy
10:04 PM
4/7/2024

Honeypot Demonstration: Tanner Vulnerability: HTTP

Nathan Almeida



Color	Service
	FTP
	SSH
	TELNET
	EMAIL
	SQL
	DNS
	HTTP
	HTTPS

Hits	IP
43	36.139.89.106
41	209.38.144.48
20	112.168.248.149
8	212.70.149.150
7	54.37.79.75
7	23.90.225.204
6	193.201.9.156

Hits	Country
51	United States
44	China
23	South Korea
13	France
9	Bulgaria
9	Russia
5	Switzerland

Events	IP	Country	Honeypot	Service
2024-04-08 18:00:35	220.82.146.218	South Korea	Cowrie	SSH
2024-04-08 17:56:56	209.38.144.48	United States	Cowrie	SSH
2024-04-08 17:51:06	209.38.144.48	United States	Cowrie	SSH
2024-04-08 17:46:13	91.92.251.164	Bulgaria	Cowrie	SSH
2024-04-08 17:45:15	209.38.144.48	United States	Cowrie	SSH
2024-04-08 17:39:54	54.37.79.75	France	Tanner	HTTP
2024-04-08 17:39:54	54.37.79.75	France	Tanner	HTTP

Legal/Ethical Implications

- **Entrapment**
  - Despite the controversy, Honeypots are not a form of entrapment
  - Honeypots don’t induce anyone
- **Privacy**
  - Federal Wiretap Act
  - Exemption under Service Provider Protection
- **Liability**
  - Liability implies you could be sued if your honeypot is used to harm others.
  - Civil issue

Resources

T-Pot/tpotce

https://github.com/telekom-security/tpotce?tab=readme-ov-file#ssh-and-cockpit