Honeypot Lab 2 – Cowrie Log Analysis (APRICOT 2020)

1. Access the running docker instance

- cd /home/apnic/docker-cowrie
- sudo docker-compose exec cowrie bash

note: you should see something like this "root@2e2fdf7f9e1e:/#"

2. Go to the log directory

- cd /opt/cowrie/var/log/cowrie
- ls -lah

Note: by default the logs are in text and json format. Note cowrie.log and cowrie.json

3. We are going to use *jq* for viewing the json-formatted logs
apt install jq

4. Check the contents of cowrie.json
jq . cowrie.json | less

Note: observe the relevant fields & values to understand what is going to the honeypot

5. What are successful username/password combinations
jq 'select(.eventid=="cowrie.login.success")' cowrie.json | less

6. Follow a session – pick a **session id** (from the command above)
jq 'select(.session =="insert_session_number_here")' cowrie.json| less

Example (please select your own session number!)
cat cowrie.json | jq 'select(.session =="f89e0dfcb40c")' | less

Can you identify information related to:
a. Source IP address (source of attack)
b. Username and Password used to login 'successfully' in the honeypot
d. Any other interesting information

7. What are the commands inputted by attackers?
jq 'select(.eventid =="cowrie.command.input")' cowrie.json | less

8. What are the files that have been successfully downloaded on the honeypot?

jq 'select(.eventid =="cowrie.session.file_download")' cowrie.json | less

9. Can we identify some indicators to search further?
Hint:
shashum:
url:
domain/ip_address hosting file:
source of attack:

10. Can we find out what the file is related to?
Hint: search the hash (shasum) on https://www.virustotal.com

11. When done with the exercise exit docker.

Appendix

1. jq manual https://stedolan.github.io/jq/manual/