Honeypot LAB #1 ((APRICOT 2020))

Objective: Install a ssh/telnet honeypot (Cowrie) on Linux. The honeypot will connect to the APNIC Honeynet Project backend.

Requirement: SSH client on Linux/Mac or Putty (Windows)

1. Log into your Linux server based on credentials provided by the trainer

   Username: apnic
   Password:
   Hostname:
   Port: 3843

   Example on Linux/Mac:

   ssh apnic@hostname -p 3843 -v

2. Record IP address of your server
   a. ifconfig -a

3. Download docker-cowrie-install.sh from the training repository
   a. wget https://durian.fsck.my/chn-cowrie-lab.sh

4. Change permission of the file
   a. chmod 755 chn-cowrie-lab.sh

5. Run the script
   a. ./chn-cowrie-lab.sh

6. Change directory to docker-cowrie.
   a. cd docker-cowrie

7. Check if docker image is running
   a. sudo docker-compose ps

Testing your honeypot

From the linux server or your computer.

Note: Your management port is 3843. Telnet and SSH services are emulated on port 22 & 23 respectively.

1. ssh to your honeypot (port 22)
    a. username: root and password: <anything>

2. telnet to your honeypot (port 23) *
    a. username: root and password: <anything>
    use telnet / cowrie

3. Try different combinations of password for root to log-in

4. What can you do in the honeypot?
    a. Can you download a file?
    b. Can you add user
    c. Can you ping another host?

Investigating Cowrie

To access the logs and files captured by Cowrie, we have to get shell on our cowrie docker image

1. Execute bash on Cowrie docker image
    a. sudo docker-compose exec cowrie bash

2. Cowrie is installed in /opt/cowrie
    a. cd /opt/cowrie
    b. ls

3. Are there any connections yet to SSH and Telnet Port?
    a. Install iftop in docker (apt-get iftop)
    b. iftop

4. Check out the configuration files in /opt/cowrie/etc/
    a. Username & passwords
    b. Hostname & settings

5. Check out the log files
    a. cd /opt/cowrie/var/log/cowrie

6. Check out files downloaded on the honeypot. Run the following commands
    a. cd /opt/cowrie/var/lib/cowrie/downloads

    b. ls -lt

    c. file *

    i. note: filename is already hash/fingerprint of the actual filename

7. Search hash of Linux Executable on the Internet (from file * command)

8. Look into content of bash script (from file * command search for Bourne-Again Shell Script *)