**Honeypot & Canary Token Monitoring**

**Importance for Cybersecurity Analysts:**

Knowing how to deploy honeypots and Canary Tokens successfully is a strategic skill as well as a technical one. These deception tools enable analysts to outsmart attackers; now reconnaissance not only triggers alarms but also alerts them to potential threats. Additionally, they provide early warning indicators that a possible breach is in progress. Uncover threat behavior from within, which ordinary defenses might now recognize. Generate real attacker data to help analysts learn how threat actors operate. Help showcase actual hands-on analyst work, such as setting up systems, examining logs, and active defense. Thus, contributing to the ability to speak confidently about causes for the need of deception tools, this demonstrates initiative and ability to tackle advanced threat hunting.

**Honeypot Walkthrough**

**Step 1: Set Up a Kali Linux Virtual Machine**

1. **Download and install Kali Linux**:
   * If you don’t already have Kali Linux, download it from the official Kali Linux website and set it up in your preferred environment (VMware, VirtualBox, or a cloud service).
2. **Start your Kali Linux VM**:

A screenshot of a computer

AI-generated content may be incorrect.

1. Ensure your VM is up and running before proceeding with the Cowrie honeypot setup.

**Step 2: Install Cowrie**

1. **Install required dependencies**:

* Run the following command to install necessary packages:
* sudo apt-get update && sudo apt-get install git python3-virtualenv -y

1. **Clone the Cowrie repository**:
   * Clone the official Cowrie repository to your system by running:
   * git clone <https://github.com/cowrie/cowrie.git>

A computer screen shot of a computer code

AI-generated content may be incorrect.

**Step 3: Set Up Python Virtual Environment**

1. **Navigate to the Cowrie directory**:
   * Enter the Cowrie directory by running:

A screen shot of a computer

AI-generated content may be incorrect.

cd cowrie

1. **Create a Python virtual environment**:

* Set up a virtual environment for Cowrie using: A computer screen shot of a program

  AI-generated content may be incorrect.
* virtualenv -p python3 cowrie-env

1. **Activate the virtual environment**:

* Activate it by running:
* source cowrie-env/bin/activate

**Step 4: Install Required Python Packages**

1. **Install dependencies**:

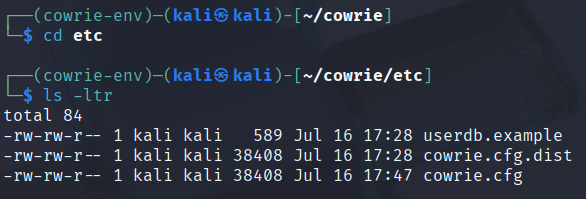
* Install all the necessary Python packages by running: A screen shot of a computer

  AI-generated content may be incorrect.A screen shot of a computer

  AI-generated content may be incorrect.
* pip install -r requirements.txt

**Step 5: Configure Cowrie**

1. **Copy the default configuration file**:

* Copy the default configuration file to create your own:
* cp etc/cowrie.cfg.dist etc/cowrie.cfg

1. **Modify the configuration (optional)**:

* By default, Cowrie listens on port 2222. If you want to change it to the standard SSH port (22), open the configuration file in a text editor and modify the port setting:
* nano etc/cowrie.cfg
* Find the line that says listen\_endpoints and change the port number to 22.

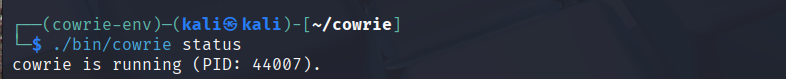
**Step 6: Start the Cowrie Honeypot**

1. **Run the honeypot**:
   * Start Cowrie by running the following **command:** cowrie start

A computer screen shot of a computer code

AI-generated content may be incorrect.

1. **Verify Cowrie is running**:

* Confirm Cowrie is running by checking the status with: 
* cowrie status

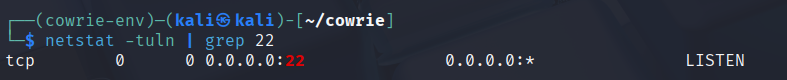
**Step 7: Check if Cowrie is Listening on the Correct Port**

1. **Verify port configuration**:

* Check if Cowrie is listening on the correct port by running:
* netstat -tuln | grep 2222
* If you changed the port to 22, update the command to check that port.

**Step 8: Simulate an Attacker Connecting to the Honeypot**

1. **Connect to the honeypot**:

* Use the SSH command to connect to your honeypot:
* ssh username@localhost -p 2222
* Replace the port number with 22 if you changed the configuration. This is what an attacker would see when they attempt to connect. 

**Step 9: View Attack Logs**

1. **Navigate to the log directory**:

* Cowrie logs all attacker actions. You can view these logs by navigating to the following directory:
* cd var/log/cowrie A computer screen shot of a code

  AI-generated content may be incorrect.

1. **Tail the log file**:

* To view the log of commands the attacker has attempted to run, use the tail command:
* tail -f cowrie.log

**Step 10: Analyze Attack Data**

1. **Review logged commands**: A screen shot of a computer screen

   AI-generated content may be incorrect.
   * Observe the commands attackers tried to run on your honeypot. These insights can be useful for understanding attack patterns and malicious behaviors.

**Step 11: Stop the Honeypot**

1. **Stop Cowrie**:

* Once you're done, you can stop the honeypot using the following command: A computer screen shot of white text

  AI-generated content may be incorrect.
* cowrie stop

**Canary Token Simple Breakdown**A screenshot of a computer

AI-generated content may be incorrect.

* Navigate to the Canary Tokens website: <https://canarytokens.org/nest/>
* Select the token you wish to configure and set up
  + We chose an Excel file in the video
* Choose the email address where you would like the notification to be sent.
* Download the Canary token
* Create your Honey Pot Scenario
  + Rename the Excel file a name that would trick a malicious into believing it could be contain sensitive information
  + Place it in a folder that is relevant to the file name
  + Place some fake data inside the file
* Test executing the file and confirm you have received the notification email to the nominated email address
* The email will include the following details:
  + Source IP of the person who accessed the file
  + User agent
  + Timestamp

**What I Learned in this project 🏆**

* **Understanding Deception Tools:**
  + Learning the concept and importance of deception in cybersecurity to detect and monitor attackers by creating fake assets.
  + Gaining knowledge on how Canary Tokens and honeypots can alert defenders about malicious activity without alerting the attackers.
* **Creating Canary Tokens:**
  + Setting up **Canary Tokens**, which can be embedded in files, URLs, or network resources.
  + Configuring tokens to trigger alerts when interacted with by unauthorized users (e.g., accessing a fake document or visiting a hidden URL).
* **Monitoring and Alerting with Canary Tokens:**
  + Analyzing the alert details, such as the time, source IP address, and method of access, to identify potential security incidents.
  + Using these alerts to detect early signs of insider threats, network reconnaissance, or external attacks.
* **Setting Up a Honeypot:**
  + Installing and configuring a honeypot on your network using **Cowrie**.
  + Creating a vulnerable but isolated system or service that mimics real production environments, enticing attackers to engage with it.
* **Advanced Threat Detection:**
  + Ability to detect advanced threats and APTs using deception tools.
* **Reporting and Documentation:**
  + Documenting the entire process of setting up Canary Tokens and honeypots Ability to detect advanced threats and APTs using deception tools.
* **Reporting and Documentation:**
  + Documenting the entire process of setting up Canary Tokens and honeypots