ACME Anvils
Denver Colorado
SOC Team
October 26, 2023

Internal Honeypot

OVERVIEW

It has been brought to our attention that ACME Anvils is in need of a solution to detect and deflect attacks on the company's environment. It is our job as the SOC Team here at ACME Anvils to provide such a solution in a detailed report describing exactly how to implement a plan to resolve the issue at hand.

GOALS

1. Suggest a possible honeypot to detect and defend against attacks to the company's network.
2. Include details in the plan such as tools needed, cost, and procedure.

COWRIE

Cowrie is a medium to high interaction SSH and Telnet honeypot designed to log brute force attacks and the shell interaction performed by the attacker. In medium interaction mode (shell) it emulates a UNIX system in Python, and in high interaction mode (proxy) it functions as an SSH and telnet proxy to observe attacker behavior to another system. Cowrie is free to use and very simple to set up on your network. It can be downloaded as a zip file and started through docker on your system. Cowrie can also be customized by the user to modify banners, create a pickle file system, add custom files an attacker can access, etc. Cowrie should be run in a demilitarized zone since it can lead to a higher possibility of attacks on other services that may have security flaws. Keeping this in mind, we should ensure that wherever we install this honeypot is not being used as a live machine for any other services.

FEATURES

Run as an emulated shell (default):

- Fake file system with the ability to add/remove files. A full fake file system resembling a Debian 5.0 installation is included.
- Possibility of adding fake file contents so the attacker can cat files such as /etc/passwd.
- Cowrie saves files downloaded with wget/curl or uploaded with SFTP and scp for later inspection.

Proxy SSH and Telnet to another system:

- Run as a pure telnet and SSH proxy with monitoring.
- Let Cowrie manage a pool of QEMU emulated servers to provide the systems to login to.

For both settings:

- Session logs are stored in an UML Compatible format for easy replay with the bin/playlog utility.
- SFTP and SCP support for file upload.
- Support for SSH exec commands.
- Logging of direct-tcp connection attempts (ssh proxying).
- Forward SMTP connections to SMTP Honeypot.
- JSON logging for easy processing in log management solutions.

REQUIREMENTS

- Python 3.8+
- Python-virtualenv

PROCEDURE

- Change the port you'll use to administer the server.
    - Cowrie will be listening for SSH connections on port 22. You’ll want to configure the SSH service to listen on a different port for you to connect to and administer the server.
- Install and configure Cowrie
    - Download updated package lists.
    - Install Cowrie’s dependencies.
- Create a new python virtual environment for Cowrie.
- Activate the new virtual environment.
- Generate a key for the Cowrie instance.
- Make a copy of the config file for your new cowrie instance.
    - Set the hostname in the configuration file to a server name of your choice.
    - Change the listening port for incoming SSH connections to port 22.
- Enable authbind in Cowrie’s start.sh file.
- Start Cowrie.
- Test connectivity to the Cowrie Honeypot.
    - Execute some commands for Cowrie to log.
- Review the Cowrie log file.
    - Connect to your server (not the Cowrie instance) and review the log file.
    - The attacker's IP address will be shown along with commands acted out by the attacker to reveal their intentions.