Honeypot Demonstration Lesson Plan

Christopher Bingham

Introduction

A honeypot is a cybersecurity tool designed to distract and monitor attackers. It is a system that is safely isolated from the real network but designed to appear as if it were legitimately in use. It intentionally contains vulnerabilities, so that it is an attractive target. When accessed by an attacker, the honeypot will keep detailed logs of all activity. Cybersecurity professionals will then analyze these logs to identify information about the attacker.

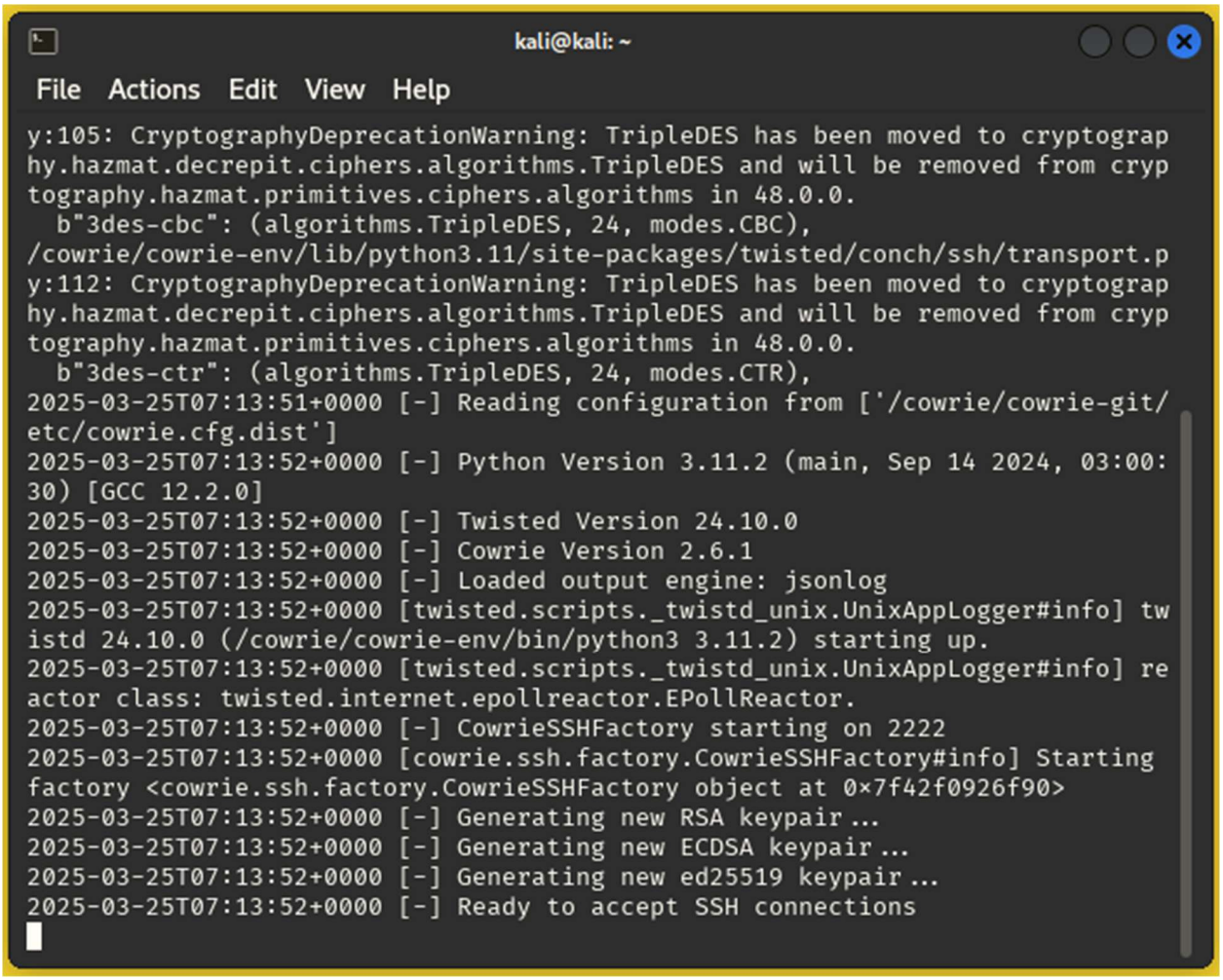
Demonstration

These instructions will walk you through a demonstration of setting up and using a simple honeypot. An attacker will be able to gain fake SSH access and then the honeypot will log their actions. You will be using VMware, Kali Virtual Machines, and Cowrie.

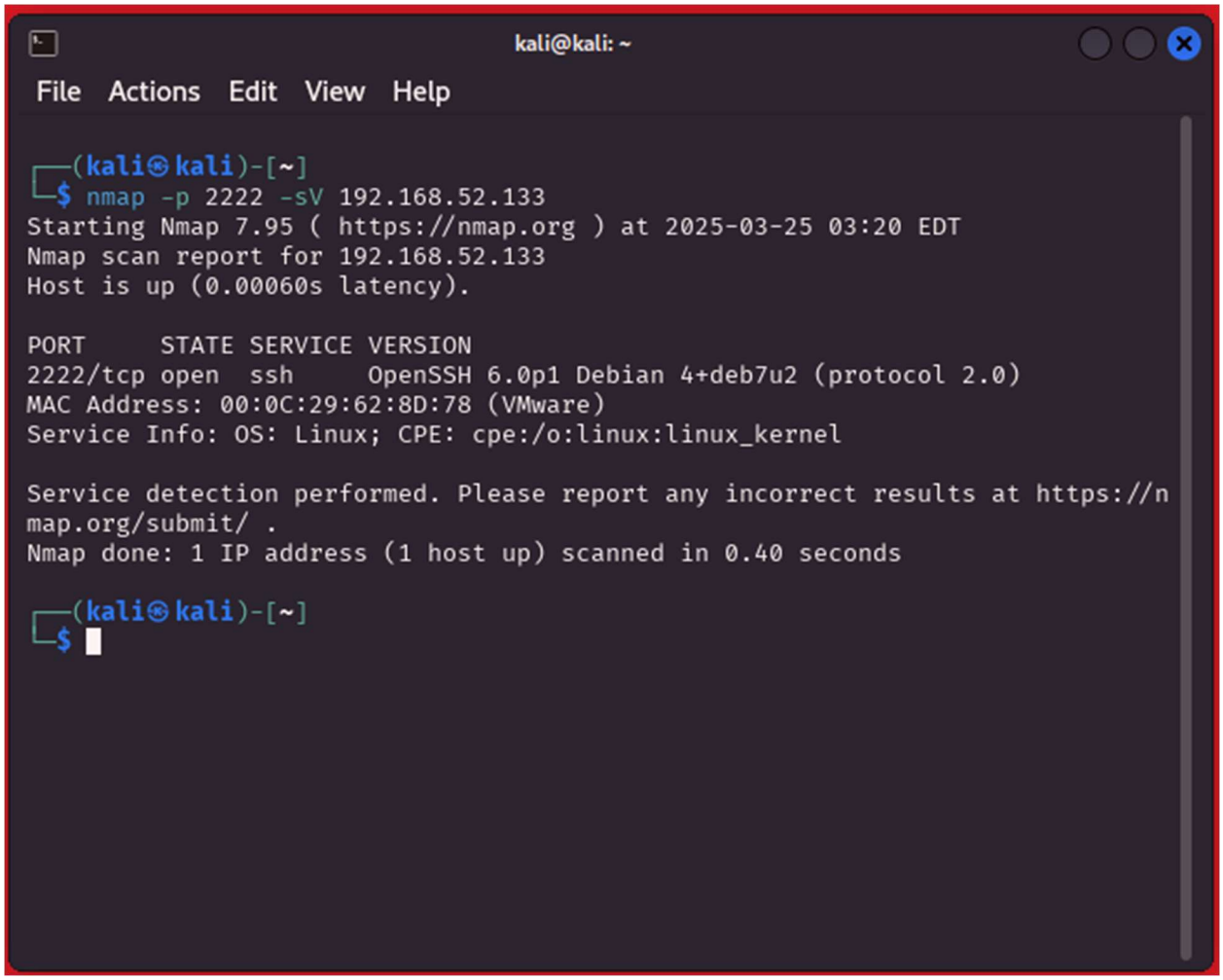
Note: For safety make sure to do these activities on an isolated network. For example, once you have pulled Cowrie you could put your two VMs on a virtual network with no internet access.

1. Download VMware Workstation or Fusion
    a. https://www.vmware.com/products/desktop-hypervisor/workstation-and-fusion
2. Download a pre-made Kali VM for VMware
    a. https://www.kali.org/get-kali/#kali-virtual-machines
3. Unzip the download and make a second copy. Be sure to rename the folders so you can keep track of the machines. One will be our attack box and the other will be the honeypot.
4. Open the .vmx file for each VM and rename the VMs.
5. Start each machine. If it asks, tell it you copied the machine.
    a. The username and password for these machines is “kali.”
6. On the honeypot machine run the following commands to install and start docker. The status command will tell you if you have succeeded.
    a. sudo apt update
    b. sudo apt install docker.io
    c. sudo systemctl start docker
    d. sudo systemctl status docker

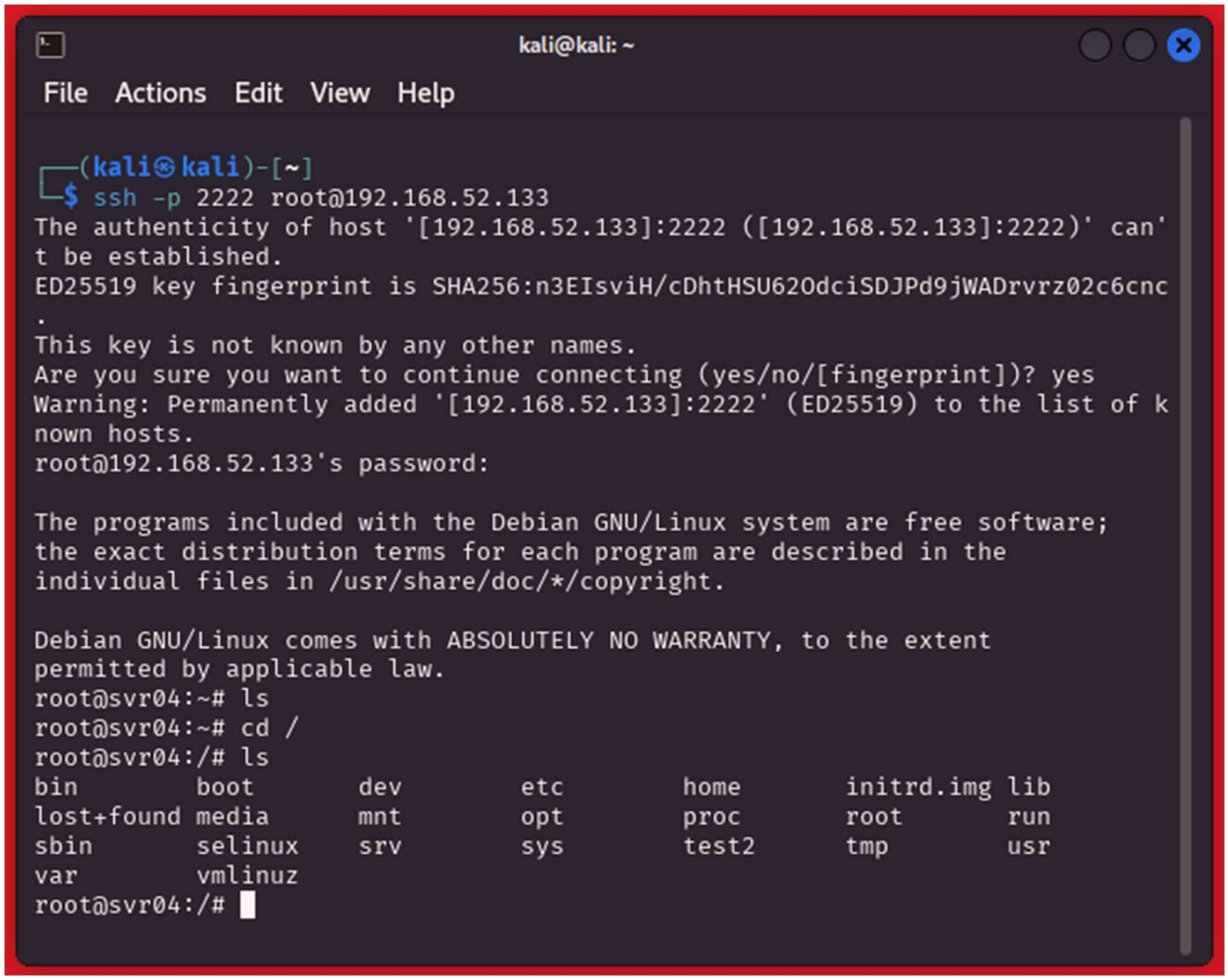
7. On the honeypot machine run the following commands to download and run the Cowrie honeypot software. If successful, the bottom line will say “Ready to accept SSH connections.”
    a. sudo docker pull cowrie/cowrie
    b. sudo docker run -p 2222:2222 cowrie/cowrie:latest



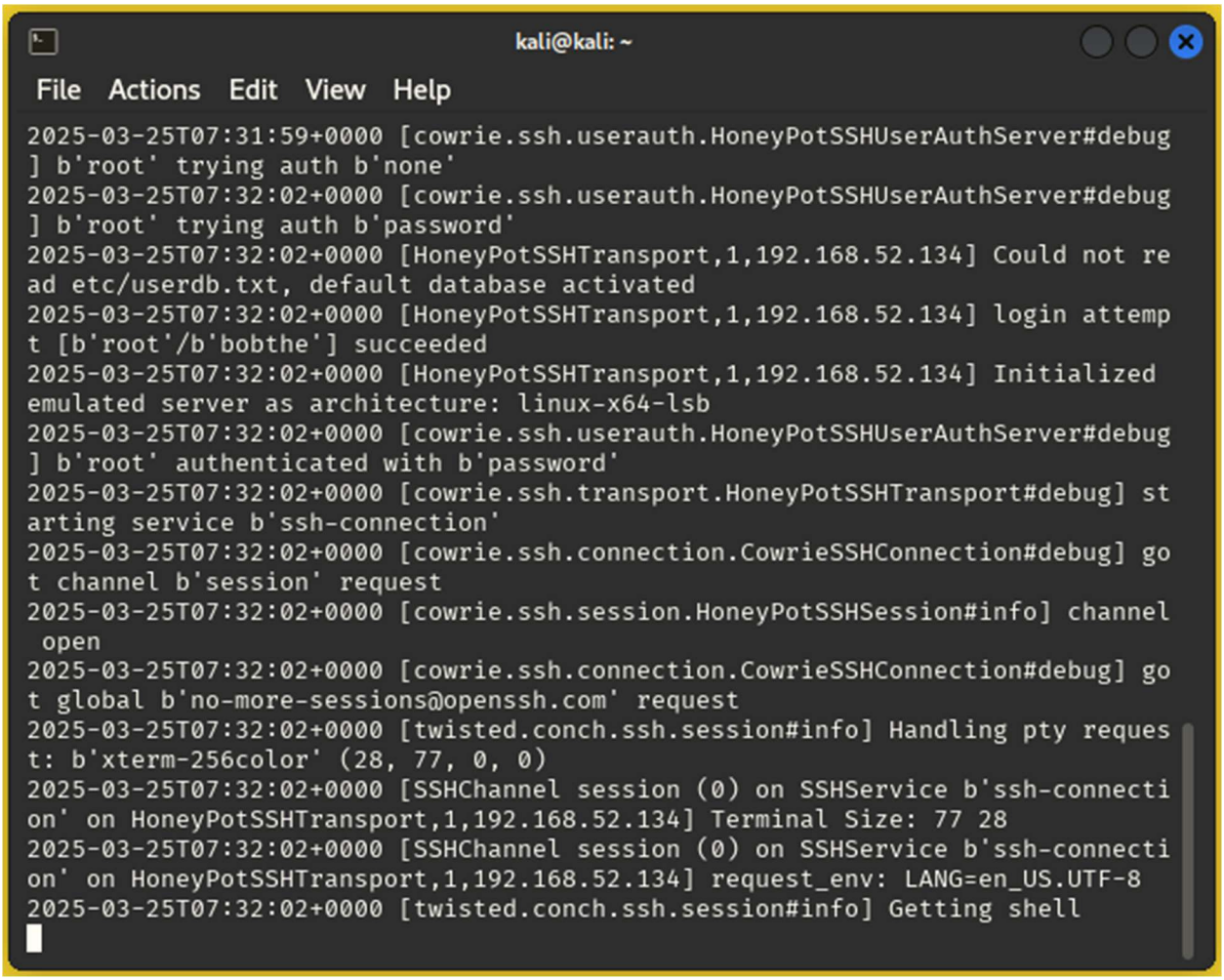
8. In another terminal on the honeypot machine run the following command and take note of the IP address.
    a. ip a
9. On the attack machine run the following command. You should see that port 2222/tcp is open for OpenSSH.
    a. nmap -p 2222 -sV <honeypot_ip>



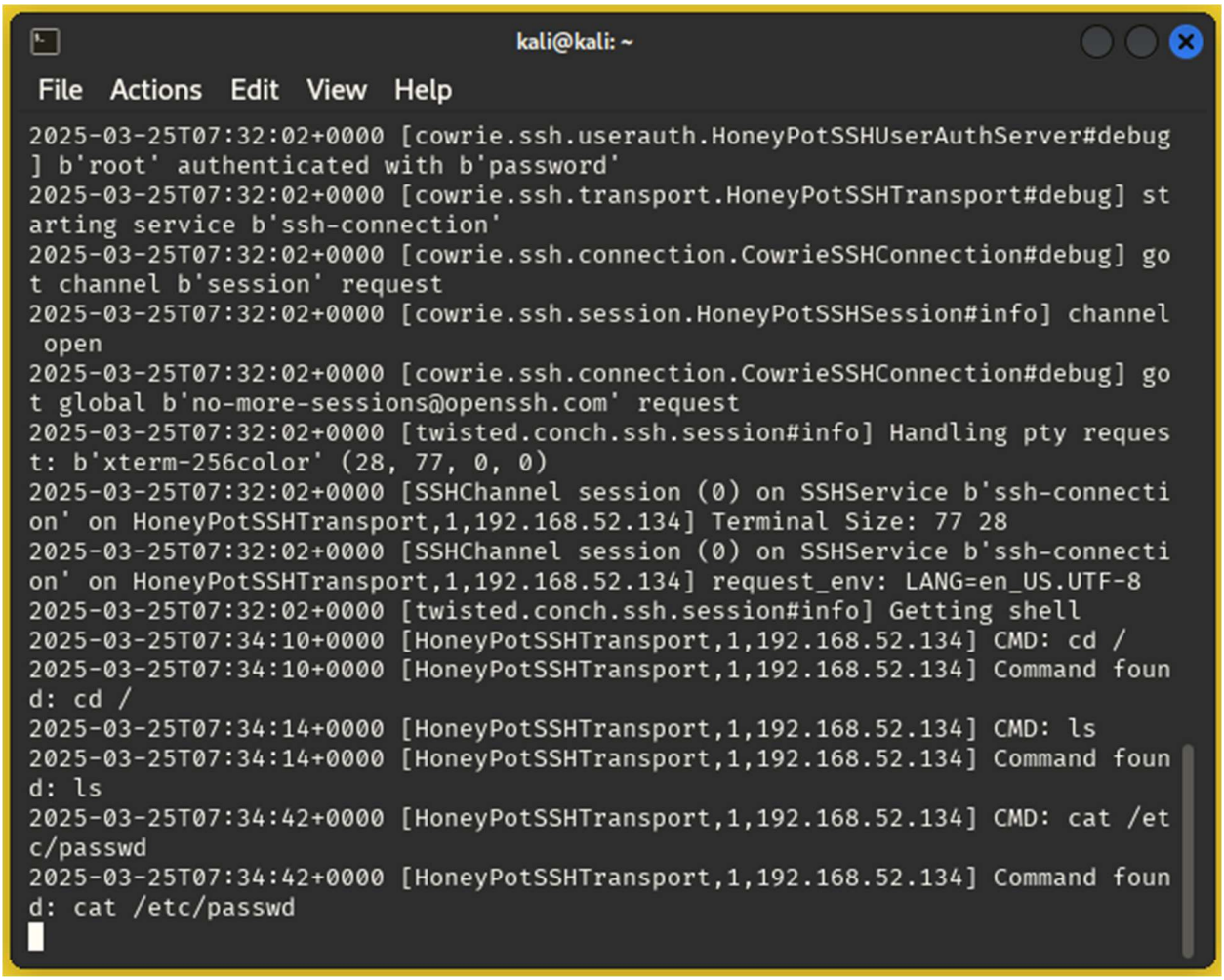
10. On the attack machine run the following command to gain SSH access as root. Any password will work.
    a. ssh -p 2222 root@<honeypot_ip>



11. Now look back at the honeypot. You will see logs about the attack machine SSHing in.



12. Now play around from the attack machine. For example, cat out a file. On the honeypot logs you will see everything the attacker does.



13. Have a discussion about the following questions:
    a. How could the information in the logs be useful to a defender?
    b. What might be some risks of setting up a honeypot?
    c. What other services besides SSH would be useful in a honeypot setup?
    d. How could you make a honeypot more convincing to a skilled attacker?
14. Bonus: Cowrie has several configuration options. For example, you can add files into the fake ssh server. You could pretend to be a certain type of business and add files that look realistic.

Resources

- https://www.crowdstrike.com/en-us/cybersecurity-101/exposure-management/honeypots/
- https://medium.com/threatpunter/how-to-setup-cowrie-an-ssh-honeypot-535a68832e4c

- https://github.com/cowrie/cowrie
- https://youtu.be/o3thhfKN6iQ
- https://www.geeksforgeeks.org/what-is-honeypot/
- https://www.perplexity.ai/