

# 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.

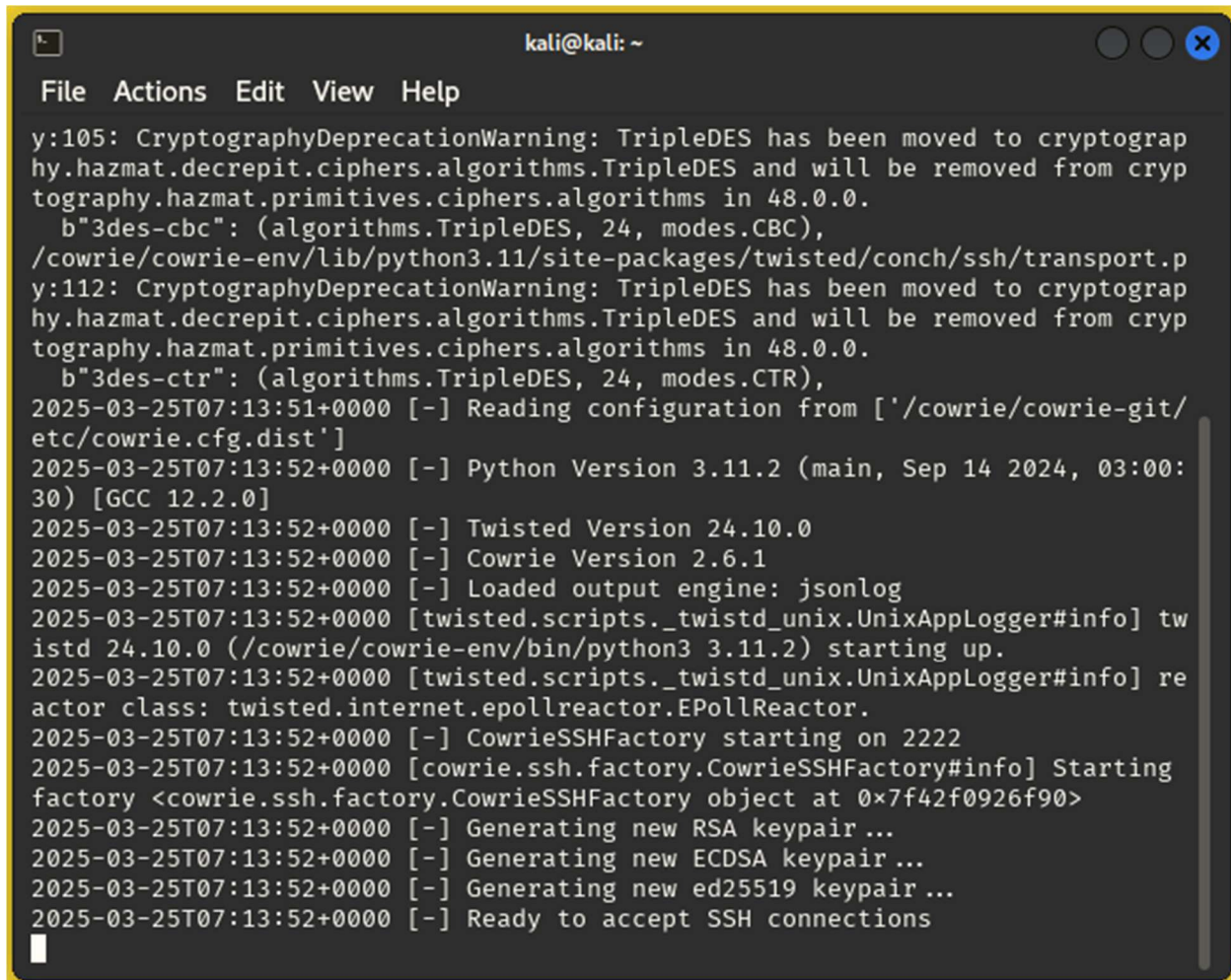
## Demonstration

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`



```
kali@kali: ~  
File Actions Edit View Help  
y:105: CryptographyDeprecationWarning: TripleDES has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed from cryptography.hazmat.primitives.ciphers.algorithms in 48.0.0.  
  b"3des-cbc": (algorithms.TripleDES, 24, modes.CBC),  
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.p  
y:112: CryptographyDeprecationWarning: TripleDES has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed from cryptography.hazmat.primitives.ciphers.algorithms in 48.0.0.  
  b"3des-ctr": (algorithms.TripleDES, 24, modes.CTR),  
2025-03-25T07:13:51+0000 [-] Reading configuration from ['/cowrie/cowrie-git/etc/cowrie.cfg.dist']  
2025-03-25T07:13:52+0000 [-] Python Version 3.11.2 (main, Sep 14 2024, 03:00:30) [GCC 12.2.0]  
2025-03-25T07:13:52+0000 [-] Twisted Version 24.10.0  
2025-03-25T07:13:52+0000 [-] Cowrie Version 2.6.1  
2025-03-25T07:13:52+0000 [-] Loaded output engine: jsonlog  
2025-03-25T07:13:52+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] twistd 24.10.0 (/cowrie/cowrie-env/bin/python3 3.11.2) starting up.  
2025-03-25T07:13:52+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] reactor class: twisted.internet.epollreactor.EPollReactor.  
2025-03-25T07:13:52+0000 [-] CowrieSSHFactory starting on 2222  
2025-03-25T07:13:52+0000 [cowrie.ssh.factory.CowrieSSHFactory#info] Starting factory <cowrie.ssh.factory.CowrieSSHFactory object at 0x7f42f0926f90>  
2025-03-25T07:13:52+0000 [-] Generating new RSA keypair ...  
2025-03-25T07:13:52+0000 [-] Generating new ECDSA keypair ...  
2025-03-25T07:13:52+0000 [-] Generating new ed25519 keypair ...  
2025-03-25T07:13:52+0000 [-] Ready to accept SSH connections
```

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>`

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
└─$ nmap -p 2222 -sV 192.168.52.133  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-25 03:20 EDT  
Nmap scan report for 192.168.52.133  
Host is up (0.00060s latency).  
  
PORT      STATE SERVICE VERSION  
2222/tcp  open  ssh      OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)  
MAC Address: 00:0C:29:62:8D:78 (VMware)  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds  
  
(kali@kali)-[~]  
└─$ █
```

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>`

```
kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
└─$ ssh -p 2222 root@192.168.52.133
The authenticity of host '[192.168.52.133]:2222 ([192.168.52.133]:2222)' can't
be established.
ED25519 key fingerprint is SHA256:n3EIsviH/cDhtHSU620dciSDJPd9jWADrvrz02c6cnc
.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.52.133]:2222' (ED25519) to the list of k
nown hosts.
root@192.168.52.133's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@svr04:~# ls
root@svr04:~# cd /
root@svr04:/# ls
bin          boot        dev          etc          home         initrd.img  lib
lost+found  media      mnt          opt          proc         root        run
sbin        selinux    srv          sys          test2       tmp         usr
var         vmlinuz
root@svr04:/# █
```

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

```
kali@kali: ~
File Actions Edit View Help
2025-03-25T07:31:59+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'none'
2025-03-25T07:32:02+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'password'
2025-03-25T07:32:02+0000 [HoneyPotSSHTransport,1,192.168.52.134] Could not read etc/userdb.txt, default database activated
2025-03-25T07:32:02+0000 [HoneyPotSSHTransport,1,192.168.52.134] login attempt [b'root'/b'bobthe'] succeeded
2025-03-25T07:32:02+0000 [HoneyPotSSHTransport,1,192.168.52.134] Initialized emulated server as architecture: linux-x64-lsb
2025-03-25T07:32:02+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' authenticated with b'password'
2025-03-25T07:32:02+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-connection'
2025-03-25T07:32:02+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got channel b'session' request
2025-03-25T07:32:02+0000 [cowrie.ssh.session.HoneyPotSSHSession#info] channel open
2025-03-25T07:32:02+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got global b'no-more-sessions@openssh.com' request
2025-03-25T07:32:02+0000 [twisted.conch.ssh.session#info] Handling pty request: b'xterm-256color' (28, 77, 0, 0)
2025-03-25T07:32:02+0000 [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,1,192.168.52.134] Terminal Size: 77 28
2025-03-25T07:32:02+0000 [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,1,192.168.52.134] request_env: LANG=en_US.UTF-8
2025-03-25T07:32:02+0000 [twisted.conch.ssh.session#info] Getting shell
```

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.

```
kali@kali: ~
File Actions Edit View Help
2025-03-25T07:32:02+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' authenticated with b'password'
2025-03-25T07:32:02+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-connection'
2025-03-25T07:32:02+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got channel b'session' request
2025-03-25T07:32:02+0000 [cowrie.ssh.session.HoneyPotSSHSession#info] channel open
2025-03-25T07:32:02+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got global b'no-more-sessions@openssh.com' request
2025-03-25T07:32:02+0000 [twisted.conch.ssh.session#info] Handling pty request: b'xterm-256color' (28, 77, 0, 0)
2025-03-25T07:32:02+0000 [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,1,192.168.52.134] Terminal Size: 77 28
2025-03-25T07:32:02+0000 [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,1,192.168.52.134] request_env: LANG=en_US.UTF-8
2025-03-25T07:32:02+0000 [twisted.conch.ssh.session#info] Getting shell
2025-03-25T07:34:10+0000 [HoneyPotSSHTransport,1,192.168.52.134] CMD: cd /
2025-03-25T07:34:10+0000 [HoneyPotSSHTransport,1,192.168.52.134] Command found: cd /
2025-03-25T07:34:14+0000 [HoneyPotSSHTransport,1,192.168.52.134] CMD: ls
2025-03-25T07:34:14+0000 [HoneyPotSSHTransport,1,192.168.52.134] Command found: ls
2025-03-25T07:34:42+0000 [HoneyPotSSHTransport,1,192.168.52.134] CMD: cat /etc/passwd
2025-03-25T07:34:42+0000 [HoneyPotSSHTransport,1,192.168.52.134] Command found: cat /etc/passwd
```

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/>