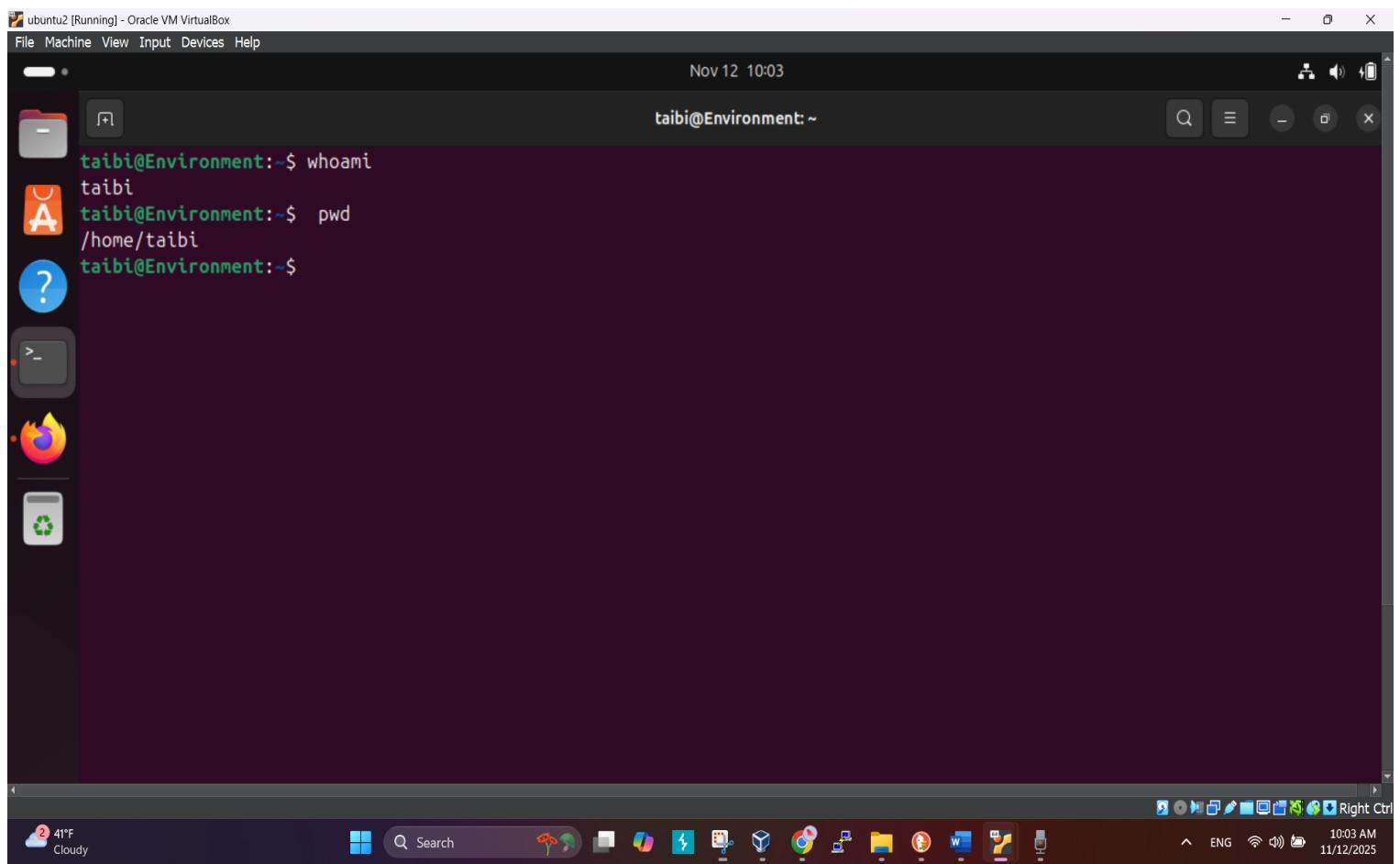
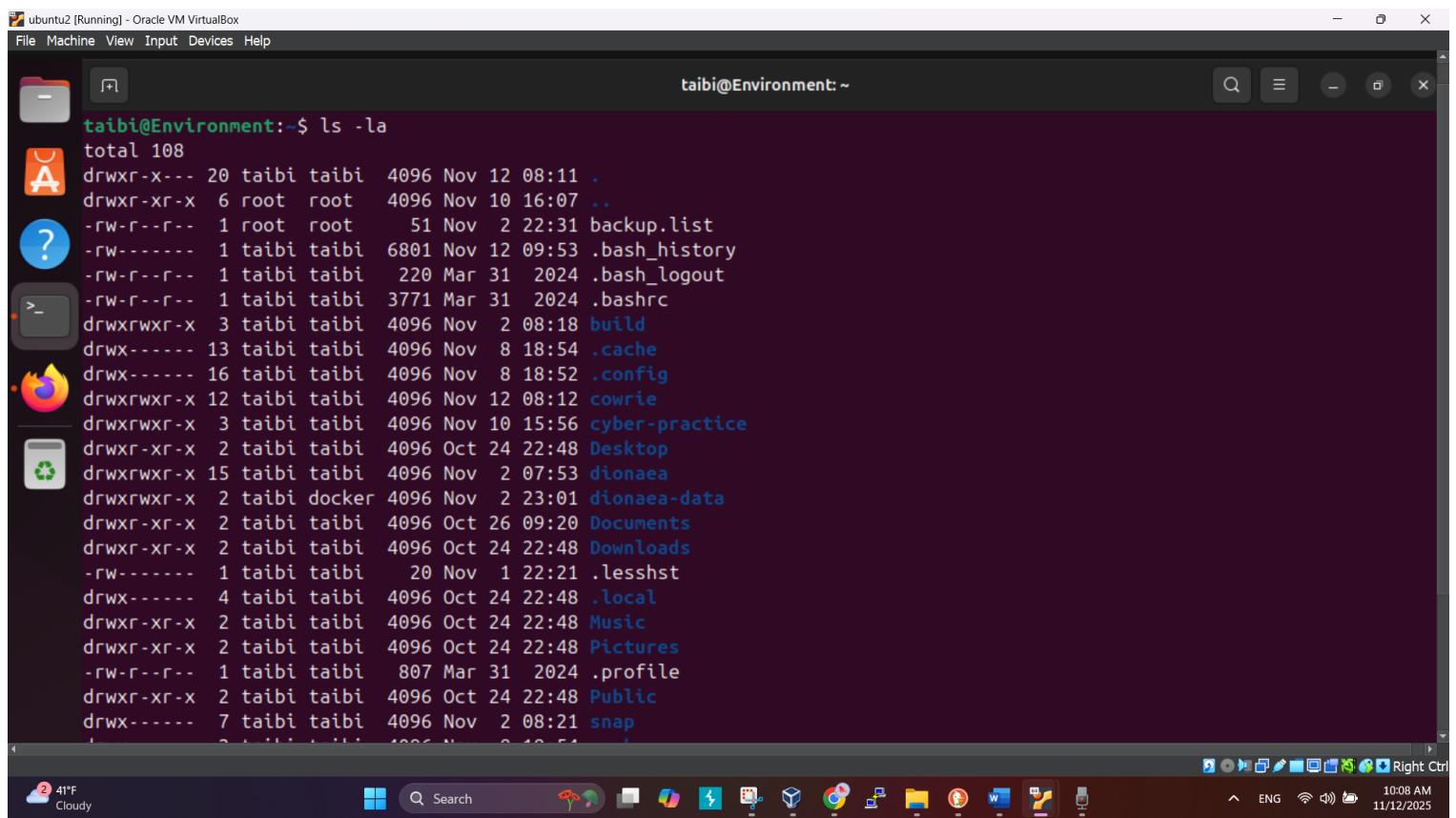


Honeypot-Log-View.png



Cowrie-Installation-Directories.png



Ubuntu2 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
? -rw----- 1 taibi taibi 6801 Nov 12 09:53 .bash_history
>_ -rw-r--r-- 1 taibi taibi 220 Mar 31 2024 .bash_logout
? -rw-r--r-- 1 taibi taibi 3771 Mar 31 2024 .bashrc
drwxrwxr-x 3 taibi taibi 4096 Nov 2 08:18 build
drwx----- 13 taibi taibi 4096 Nov 8 18:54 .cache
drwx----- 16 taibi taibi 4096 Nov 8 18:52 .config
drwxrwxr-x 12 taibi taibi 4096 Nov 12 08:12 cowrie
drwxrwxr-x 3 taibi taibi 4096 Nov 10 15:56 cyber-practice
drwxr-xr-x 2 taibi taibi 4096 Oct 24 22:48 Desktop
drwxrwxr-x 15 taibi taibi 4096 Nov 2 07:53 dionaea
drwxrwxr-x 2 taibi docker 4096 Nov 2 23:01 dionaea-data
drwxr-xr-x 2 taibi taibi 4096 Oct 26 09:20 Documents
drwxr-xr-x 2 taibi taibi 4096 Oct 24 22:48 Downloads
-rw----- 1 taibi taibi 20 Nov 1 22:21 .lessht
drwx----- 4 taibi taibi 4096 Oct 24 22:48 .local
drwxr-xr-x 2 taibi taibi 4096 Oct 24 22:48 Music
drwxr-xr-x 2 taibi taibi 4096 Oct 24 22:48 Pictures
-rw-r--r-- 1 taibi taibi 807 Mar 31 2024 .profile
drwxr-xr-x 2 taibi taibi 4096 Oct 24 22:48 Public
drwx----- 7 taibi taibi 4096 Nov 2 08:21 snap
drwx----- 2 taibi taibi 4096 Nov 8 18:54 .ssh
-rw-r--r-- 1 taibi taibi 0 Oct 24 22:54 .sudo_as_admin_successful
drwxr-xr-x 2 taibi taibi 4096 Oct 24 22:48 Templates
drwxr-xr-x 2 taibi taibi 4096 Oct 24 22:48 Videos
taibi@Environment:~$
```

Cloudy 41°F Search

Right Ctrl

ENG 10:49 AM 11/12/2025

Docker-Setup-Configuration.png

Ubuntu2 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
? taibi@Environment: ~ $ docker run -p 2222:2222 cowrie/cowrie:latest
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:110: 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.py:117: 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),
2025-11-12T15:45:02+0000 [-] Reading configuration from ['/cowrie/cowrie-git/etc/cowrie.cfg.dist']
2025-11-12T15:45:03+0000 [-] Python Version 3.11.2 (main, Apr 28 2025, 14:11:48) [GCC 12.2.0]
2025-11-12T15:45:03+0000 [-] Twisted Version 25.5.0
2025-11-12T15:45:03+0000 [-] Cowrie Version 2.8.2.dev37+g297f16b16
2025-11-12T15:45:03+0000 [-] Sensor UUID: 446c24a0-befc-11f0-8fb8-e6c3cd9d1c49
2025-11-12T15:45:03+0000 [-] Loaded output engine: jsonlog
2025-11-12T15:45:03+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] twistd 25.5.0 (/cowrie/cowrie-env/bin/python3 3.11.2) starting up.
2025-11-12T15:45:03+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] reactor class: twisted.internet.epollreactor.EPollReactor.
2025-11-12T15:45:03+0000 [-] CowrieSSHFactory starting on 2222
2025-11-12T15:45:03+0000 [cowrie.ssh.factory.CowrieSSHFactory#info] Starting factory <cowrie.ssh.factory.CowrieSSHFactory object at 0x734739753110>
2025-11-12T15:45:03+0000 [-] Ready to accept SSH connections
```

Cloudy 41°F Search

Right Ctrl

ENG 10:49 AM 11/12/2025

Honeypot Authentication Flow

A screenshot of a Linux desktop environment (Ubuntu 22.04 LTS) running in Oracle VM VirtualBox. The terminal window shows the command `ssh root@localhost : -p 2222` being run. The system is prompting for confirmation to proceed due to the host's fingerprint not being known. The desktop interface includes a dock with various application icons and a system tray at the bottom.

```
taibi@Environment:~$ ssh root@localhost : -p 2222
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ED25519 key fingerprint is SHA256:shtjCkpzdtqQoTDWXnb00LnmKKFI2t0pTCkSbuCscFc.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? 
```

A screenshot of a Linux desktop environment (Ubuntu 22.04 LTS) running in Oracle VM VirtualBox. The terminal window shows the command `ssh root@localhost -p 2222` being run. The system is prompting for confirmation to proceed due to the host's fingerprint not being known. The desktop interface includes a dock with various application icons and a system tray at the bottom.

```
root@svr04:~# ssh root@localhost -p 2222
The authenticity of host 'localhost (66.26.169.14)' can't be established.
RSA key fingerprint is 9d:30:97:8a:9e:48:0d:de:04:8d:76:3a:7b:4b:30:f8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (RSA) to the list of known hosts.
root@localhost's password:
Linux localhost 2.6.26-2-686 #1 SMP Wed Nov 4 20:45:37 UTC 2009 i686
Last login: Tue Nov 11 06:08:37 2025 from 192.168.9.4
root@localhost:~# 
```

Attack session recording

The screenshot shows a terminal window titled "ubuntu2 [Running] - Oracle VM VirtualBox". The terminal has two tabs: "taibi@Environment:~" and "taibi@Environment:~". The left tab is active and displays the following command and output:

```
root@svr04:~# ssh root@localhost -p 2222
The authenticity of host 'localhost (66.26.169.14)' can't be established.
RSA key fingerprint is 9d:30:97:8a:9e:48:0d:de:04:8d:76:3a:7b:4b:30:f8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (RSA) to the list of known hosts.
root@localhost's password:
Linux localhost 2.6.26-2-686 #1 SMP Wed Nov 4 20:45:37 UTC 2009 i686
Last login: Tue Nov 11 06:08:37 2025 from 192.168.9.4
root@localhost:~#
root@localhost:~#
root@localhost:~#
root@localhost:~# whoami
root
root@localhost:~#
root@localhost:~# pwd
/root
root@localhost:~# Connection to localhost closed by remote host.
Connection to localhost closed.
taibi@Environment:~$ ls
backup.list  cyber-practice  dionaea      Documents  Music    Public  Templates
build        Desktop         dionaea-data  Downloads  Pictures  snap    Videos
taibi@Environment:~$
```

The right tab is also titled "taibi@Environment:~". The desktop environment includes icons for a file manager, terminal, browser, and file explorer. The taskbar at the bottom shows various application icons and system status.

Honeypot-Log-View.png

The screenshot shows a terminal window titled "ubuntu2 [Running] - Oracle VM VirtualBox". The terminal has two tabs: "taibi@Environment:~" and "taibi@Environment:~". The left tab is active and displays the following commands and errors:

```
taibi@Environment:~$ docker run -p 2222:2222 | cowrie/cowrie: latest
bash: cowrie/cowrie:: No such file or directory
docker: 'docker run' requires at least 1 argument
Usage: docker run [OPTIONS] IMAGE [COMMAND] [ARG...]
See 'docker run --help' for more information
taibi@Environment:~$ docker run -p 2222:2222 | cowrie/cowrie:latest
bash: cowrie/cowrie:latest: No such file or directory
docker: 'docker run' requires at least 1 argument
Usage: docker run [OPTIONS] IMAGE [COMMAND] [ARG...]
See 'docker run --help' for more information
taibi@Environment:~$ docker run -p 2222:2222 cowrie/cowrie:latest
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:110: 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.py:117: 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)
```

The right tab is also titled "taibi@Environment:~". The desktop environment includes icons for a file manager, terminal, browser, and file explorer. The taskbar at the bottom shows various application icons and system status.

Continuation

A screenshot of a Linux desktop environment (Ubuntu 22.04 LTS) running in Oracle VM VirtualBox. The terminal window shows log output from the Cowrie SSH honeypot. The logs detail the setup of the Cowrie SSH factory, including the configuration of ciphers and modes, the loading of the jsonlog output engine, and the start of the reactor. The reactor begins accepting SSH connections on port 2222.

```
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.py:117: 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),
2025-11-12T15:45:02+0000 [-] Reading configuration from ['/cowrie/cowrie-git/etc/cowrie.cfg.dist']
2025-11-12T15:45:03+0000 [-] Python Version 3.11.2 (main, Apr 28 2025, 14:11:48) [GCC 12.2.0]
2025-11-12T15:45:03+0000 [-] Twisted Version 25.5.0
2025-11-12T15:45:03+0000 [-] Cowrie Version 2.8.2.dev37+g297f16b16
2025-11-12T15:45:03+0000 [-] Sensor UUID: 446c24a0-befc-11f0-8fb8-e6c3cd9d1c49
2025-11-12T15:45:03+0000 [-] Loaded output engine: jsonlog
2025-11-12T15:45:03+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] twistd 25.5.0 (/cowrie/cowrie-env/bin/python3 3.11.2) starting up.
2025-11-12T15:45:03+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] reactor class: twisted.internet.epollreactor.EPollReactor.
2025-11-12T15:45:03+0000 [-] CowrieSSHFactory starting on 2222
2025-11-12T15:45:03+0000 [cowrie.ssh.factory.CowrieSSHFactory#info] Starting factory <cowrie.ssh.factory.CowrieSSHFactory object at 0x734739753110>
2025-11-12T15:45:03+0000 [-] Ready to accept SSH connections
```

Continuation

A continuation of the previous terminal session, showing further log output from the Cowrie SSH honeypot. It details a new connection attempt from an IP address 172.17.0.1. The logs show the client's SSH version (SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.14), its SSH client hash fingerprint, and the chosen encryption key exchange algorithm (curve25519-sha256). The logs also indicate the connection was lost after 0.1 seconds due to a timeout.

```
ssh root@localhost: -p 2222
2025-11-12T16:10:03+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2025-11-12T16:10:03+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2025-11-12T16:10:03+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 172.17.0.1:50808 (172.17.0.2:2222) [session: 65c45580a2c4]
2025-11-12T16:10:03+0000 [HoneyPotSSHTransport,0,172.17.0.1] Remote SSH version: SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.14
2025-11-12T16:10:03+0000 [HoneyPotSSHTransport,0,172.17.0.1] SSH client hash fingerprint: aae6b9604f6f3356543709a376d7f657
2025-11-12T16:10:03+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] kex alg=b'curve25519-sha256' key alg=b'ssh-ed25519'
2025-11-12T16:10:03+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] outgoing: b'aes128-ctr' b'hmac-sha2-256' b'none'
2025-11-12T16:10:03+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] incoming: b'aes128-ctr' b'hmac-sha2-256' b'none'
2025-11-12T16:10:03+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2025-11-12T16:10:03+0000 [HoneyPotSSHTransport,0,172.17.0.1] Connection lost after 0.1 seconds
2025-11-12T16:13:06+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2025-11-12T16:13:06+0000 [cowrie.ssh.factory.CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2025-11-12T16:13:06+0000 [cowrie.ssh.factory.CowrieSSHFactory] New connection: 172.17.0.1:53736 (172.17.0.2:2222) [session: 8b796a3ee176]
2025-11-12T16:13:06+0000 [HoneyPotSSHTransport,1,172.17.0.1] Remote SSH version: SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.14
```

```
Ubuntu2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
! 2025-11-12T16:13:06+0000 [HoneyPotSSHTransport,1,172.17.0.1] Remote SSH version: SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.
14
2025-11-12T16:13:06+0000 [HoneyPotSSHTransport,1,172.17.0.1] SSH client hassh fingerprint: aae6b9604f6f3356543709a376d7f
657
2025-11-12T16:13:06+0000 [cowrie ssh transport HoneyPotSSHTransport#debug] kex alg=b'curve25519-sha256' key alg=b'ssh-ed
25519'
2025-11-12T16:13:06+0000 [cowrie ssh transport HoneyPotSSHTransport#debug] outgoing: b'aes128-ctr' b'hmac-sha2-256' b'no
ne'
2025-11-12T16:13:06+0000 [cowrie ssh transport HoneyPotSSHTransport#debug] incoming: b'aes128-ctr' b'hmac-sha2-256' b'no
ne'
2025-11-12T16:13:11+0000 [cowrie ssh transport HoneyPotSSHTransport#debug] NEW KEYS
2025-11-12T16:13:11+0000 [cowrie ssh transport HoneyPotSSHTransport#debug] starting service b'ssh-userauth'
2025-11-12T16:13:11+0000 [cowrie ssh userauth HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'none'
2025-11-12T16:13:14+0000 [cowrie ssh userauth HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'password'
2025-11-12T16:13:14+0000 [HoneyPotSSHTransport,1,172.17.0.1] Could not read etc/userdb.txt, default database activated
2025-11-12T16:13:14+0000 [HoneyPotSSHTransport,1,172.17.0.1] login attempt [b'root'/b'1'] succeeded
2025-11-12T16:13:14+0000 [HoneyPotSSHTransport,1,172.17.0.1] Initialized emulated server as architecture: linux-x64-lsb
2025-11-12T16:13:14+0000 [cowrie ssh userauth HoneyPotSSHUserAuthServer#debug] b'root' authenticated with b'password'
2025-11-12T16:13:14+0000 [cowrie ssh transport HoneyPotSSHTransport#debug] starting service b'ssh-connection'
2025-11-12T16:13:14+0000 [cowrie ssh connection CowrieSSHConnection#debug] got channel b'session' request
2025-11-12T16:13:14+0000 [cowrie ssh session HoneyPotSSHSession#info] channel open
2025-11-12T16:13:14+0000 [cowrie ssh connection CowrieSSHConnection#debug] got global b'no-more-sessions@openssh.com' re
quest
2025-11-12T16:13:14+0000 [twisted.conch.ssh.session#info] Handling pty request: b'xterm-256color' (30, 120, 0, 0)
2025-11-12T16:13:14+0000 [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,1,172.17.0.1] T
erminal Size: 120 30
2025-11-12T16:13:14+0000 [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,1,172.17.0.1] r
equest_env: LANG=en_US.UTF-8
Cloudy 41°F
Right Ctrl
11:46 AM
11/12/2025
```

```
Ubuntu2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
! quest
2025-11-12T16:13:14+0000 [twisted.conch.ssh.session#info] Handling pty request: b'xterm-256color' (30, 120, 0, 0)
2025-11-12T16:13:14+0000 [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,1,172.17.0.1] T
erminal Size: 120 30
2025-11-12T16:13:14+0000 [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,1,172.17.0.1] r
equest_env: LANG=en_US.UTF-8
2025-11-12T16:13:14+0000 [twisted.conch.ssh.session#info] Getting shell
2025-11-12T16:16:14+0000 [twisted.conch.ssh.session#info] exitCode: 1
2025-11-12T16:16:14+0000 [cowrie ssh connection CowrieSSHConnection#debug] sending request b'exit-status'
2025-11-12T16:16:14+0000 [-] Closing TTY Log: var/lib/cowrie/tty/e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991
b7852b855 after 180.1 seconds
2025-11-12T16:16:14+0000 [cowrie ssh connection CowrieSSHConnection#info] sending close 0
2025-11-12T16:16:14+0000 [cowrie ssh session HoneyPotSSHSession#info] remote close
2025-11-12T16:16:14+0000 [HoneyPotSSHTransport,1,172.17.0.1] Got remote error, code 11 reason: b'disconnected by user'
2025-11-12T16:16:14+0000 [HoneyPotSSHTransport,1,172.17.0.1] avatar root logging out
2025-11-12T16:16:14+0000 [cowrie ssh transport HoneyPotSSHTransport#info] connection lost
2025-11-12T16:16:14+0000 [HoneyPotSSHTransport,1,172.17.0.1] Connection lost after 187.9 seconds
2025-11-12T16:18:01+0000 [cowrie ssh factory CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha1
2025-11-12T16:18:01+0000 [cowrie ssh factory CowrieSSHFactory] No moduli, no diffie-hellman-group-exchange-sha256
2025-11-12T16:18:01+0000 [cowrie ssh factory CowrieSSHFactory] New connection: 172.17.0.1:44614 (172.17.0.2:2222) [sessi
on: 4da19872e3d2]
2025-11-12T16:18:01+0000 [HoneyPotSSHTransport,2,172.17.0.1] Remote SSH version: SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.
14
2025-11-12T16:18:01+0000 [HoneyPotSSHTransport,2,172.17.0.1] SSH client hassh fingerprint: aae6b9604f6f3356543709a376d7f
657
2025-11-12T16:18:01+0000 [cowrie ssh transport HoneyPotSSHTransport#debug] kex alg=b'curve25519-sha256' key alg=b'ssh-ed
25519'
2025-11-12T16:18:01+0000 [cowrie ssh transport HoneyPotSSHTransport#debug] outgoing: b'aes128-ctr' b'hmac-sha2-256' b'no
ne'
Cloudy 41°F
Right Ctrl
11:48 AM
11/12/2025
```

```
Ubuntu2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
ne'
2025-11-12T16:18:01+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] incoming: b'aes128-ctr' b'hmac-sha2-256' b'no
ne'
2025-11-12T16:18:01+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] NEW KEYS
2025-11-12T16:18:01+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-userauth'
2025-11-12T16:18:01+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'none'
2025-11-12T16:18:02+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'password'
2025-11-12T16:18:02+0000 [HoneyPotSSHTransport,2,172.17.0.1] Could not read etc/userdb.txt, default database activated
2025-11-12T16:18:02+0000 [HoneyPotSSHTransport,2,172.17.0.1] login attempt [b'root'/b'1'] succeeded
2025-11-12T16:18:02+0000 [HoneyPotSSHTransport,2,172.17.0.1] Initialized emulated server as architecture: linux-x64-lsb
2025-11-12T16:18:02+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' authenticated with b'password'
2025-11-12T16:18:02+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-connection'
2025-11-12T16:18:02+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got channel b'session' request
2025-11-12T16:18:02+0000 [cowrie.ssh.session.HoneyPotSSHSessions#info] channel open
2025-11-12T16:18:02+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got global b'no-more-sessions@openssh.com' request
2025-11-12T16:18:03+0000 [twisted.conch.ssh.session#info] Handling pty request: b'xterm-256color' (30, 120, 0, 0)
2025-11-12T16:18:03+0000 [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,2,172.17.0.1] Terminal Size: 120 30
2025-11-12T16:18:03+0000 [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,2,172.17.0.1] request_env: LANG=en_US.UTF-8
2025-11-12T16:18:03+0000 [twisted.conch.ssh.session#info] Getting shell
2025-11-12T16:19:49+0000 [HoneyPotSSHTransport,2,172.17.0.1] CMD: clear
2025-11-12T16:19:49+0000 [HoneyPotSSHTransport,2,172.17.0.1] Command found: clear
2025-11-12T16:20:26+0000 [HoneyPotSSHTransport,2,172.17.0.1] CMD: ssh root@localhost -p 2222
2025-11-12T16:20:26+0000 [HoneyPotSSHTransport,2,172.17.0.1] Command found: ssh root@localhost -p 2222
2025-11-12T16:20:29+0000 [HoneyPotSSHTransport,2,172.17.0.1] INPUT (ssh): yes
2025-11-12T16:20:38+0000 [HoneyPotSSHTransport,2,172.17.0.1] INPUT (ssh): 1
2025-11-12T16:20:38+0000 [HoneyPotSSHTransport,2,172.17.0.1] INPUT (ssh): 1
```

```
Ubuntu2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
?
2025-11-12T16:18:03+0000 [twisted.conch.ssh.session#info] Handling pty request: b'xterm-256color' (30, 120, 0, 0)
2025-11-12T16:18:03+0000 [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,2,172.17.0.1] Terminal Size: 120 30
2025-11-12T16:18:03+0000 [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,2,172.17.0.1] request_env: LANG=en_US.UTF-8
2025-11-12T16:18:03+0000 [twisted.conch.ssh.session#info] Getting shell
2025-11-12T16:19:49+0000 [HoneyPotSSHTransport,2,172.17.0.1] CMD: clear
2025-11-12T16:19:49+0000 [HoneyPotSSHTransport,2,172.17.0.1] Command found: clear
2025-11-12T16:20:26+0000 [HoneyPotSSHTransport,2,172.17.0.1] CMD: ssh root@localhost -p 2222
2025-11-12T16:20:26+0000 [HoneyPotSSHTransport,2,172.17.0.1] Command found: ssh root@localhost -p 2222
2025-11-12T16:20:29+0000 [HoneyPotSSHTransport,2,172.17.0.1] INPUT (ssh): yes
2025-11-12T16:20:38+0000 [HoneyPotSSHTransport,2,172.17.0.1] INPUT (ssh): 1
2025-11-12T16:21:48+0000 [HoneyPotSSHTransport,2,172.17.0.1] CMD:
2025-11-12T16:21:49+0000 [HoneyPotSSHTransport,2,172.17.0.1] CMD:
2025-11-12T16:21:49+0000 [HoneyPotSSHTransport,2,172.17.0.1] CMD:
2025-11-12T16:21:54+0000 [HoneyPotSSHTransport,2,172.17.0.1] CMD: whoami
2025-11-12T16:21:54+0000 [HoneyPotSSHTransport,2,172.17.0.1] Command found: whoami
2025-11-12T16:21:56+0000 [HoneyPotSSHTransport,2,172.17.0.1] CMD:
2025-11-12T16:21:59+0000 [HoneyPotSSHTransport,2,172.17.0.1] CMD: pwd
2025-11-12T16:21:59+0000 [HoneyPotSSHTransport,2,172.17.0.1] Command found: pwd
2025-11-12T16:23:02+0000 [-] Timeout reached in HoneyPotSSHTransport
2025-11-12T16:23:02+0000 [HoneyPotSSHTransport,2,172.17.0.1] Closing TTY Log: var/lib/cowrie/tty/ac6aec2bf59c10c6b31837746c1a4736b59f29f27194e63803fec5fb9c0bce0 after 300.0 seconds
2025-11-12T16:23:02+0000 [HoneyPotSSHTransport,2,172.17.0.1] avatar root logging out
2025-11-12T16:23:02+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2025-11-12T16:23:02+0000 [HoneyPotSSHTransport,2,172.17.0.1] Connection lost after 301.8 seconds
```

Project Reflection

Mission Accomplished!

This project started as a simple idea "I want to understand how honeypots work" and turned into a hands-on learning experience that taught me more than I expected. From struggling with Docker commands to successfully capturing my own "attack" data, every step was a lesson in cybersecurity.

Beyond the Technical

What surprised me most wasn't just the technical setup, but how much I learned about the mindset of security:

Patience: Some things take a few tries to get right

Curiosity: Each error message was a chance to learn something new

Persistence: The satisfaction of seeing "Ready to accept SSH connections" after troubleshooting

Security Awareness: Now I look at servers differently, thinking about what attackers might see

The Real Value

The screenshots and logs in this document aren't just proof that the honeypot worked, they're snapshots of genuine learning. The wrong commands, the syntax errors, the "aha!" moments when things finally clicked that's where the real growth happened.

Where This Leads

This project isn't an end point, but a starting line. Now I'm curious about:

What would real attackers do differently?

How can I make the honeypot even more convincing?

What other security tools can I explore?

Sometimes the best lessons come not from getting everything perfect, but from the journey of figuring it out. This honeypot project was exactly that a journey worth taking.