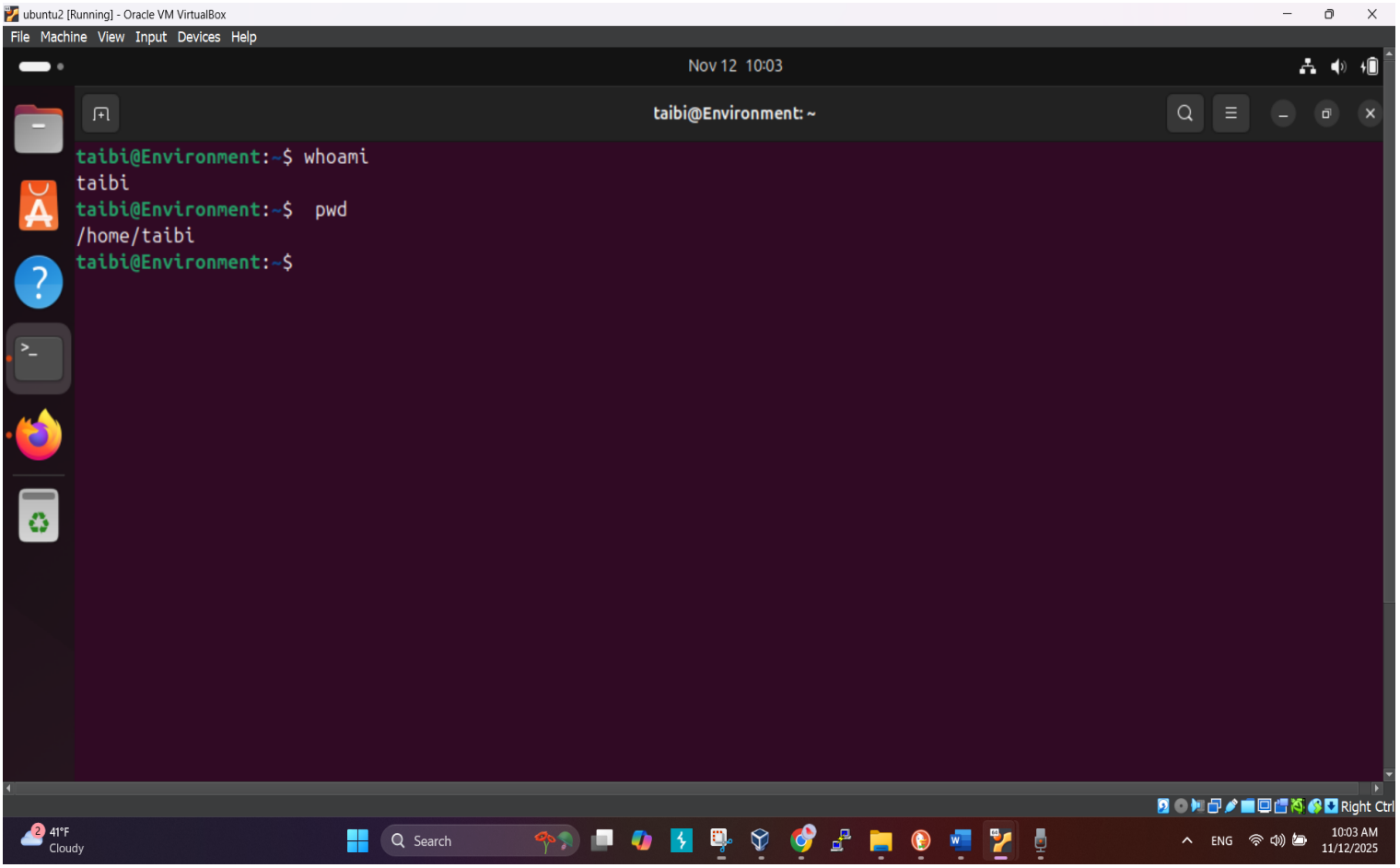
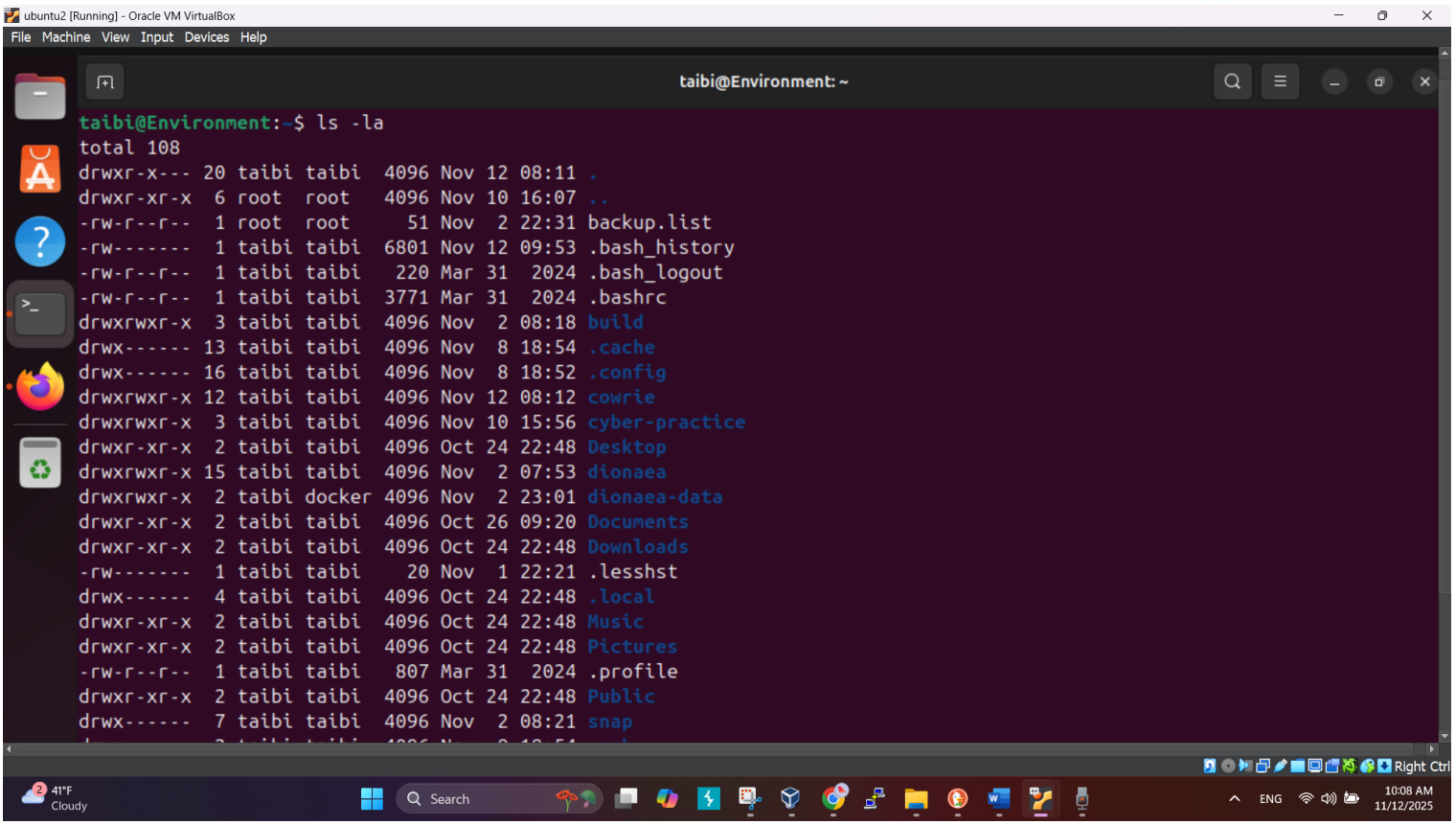
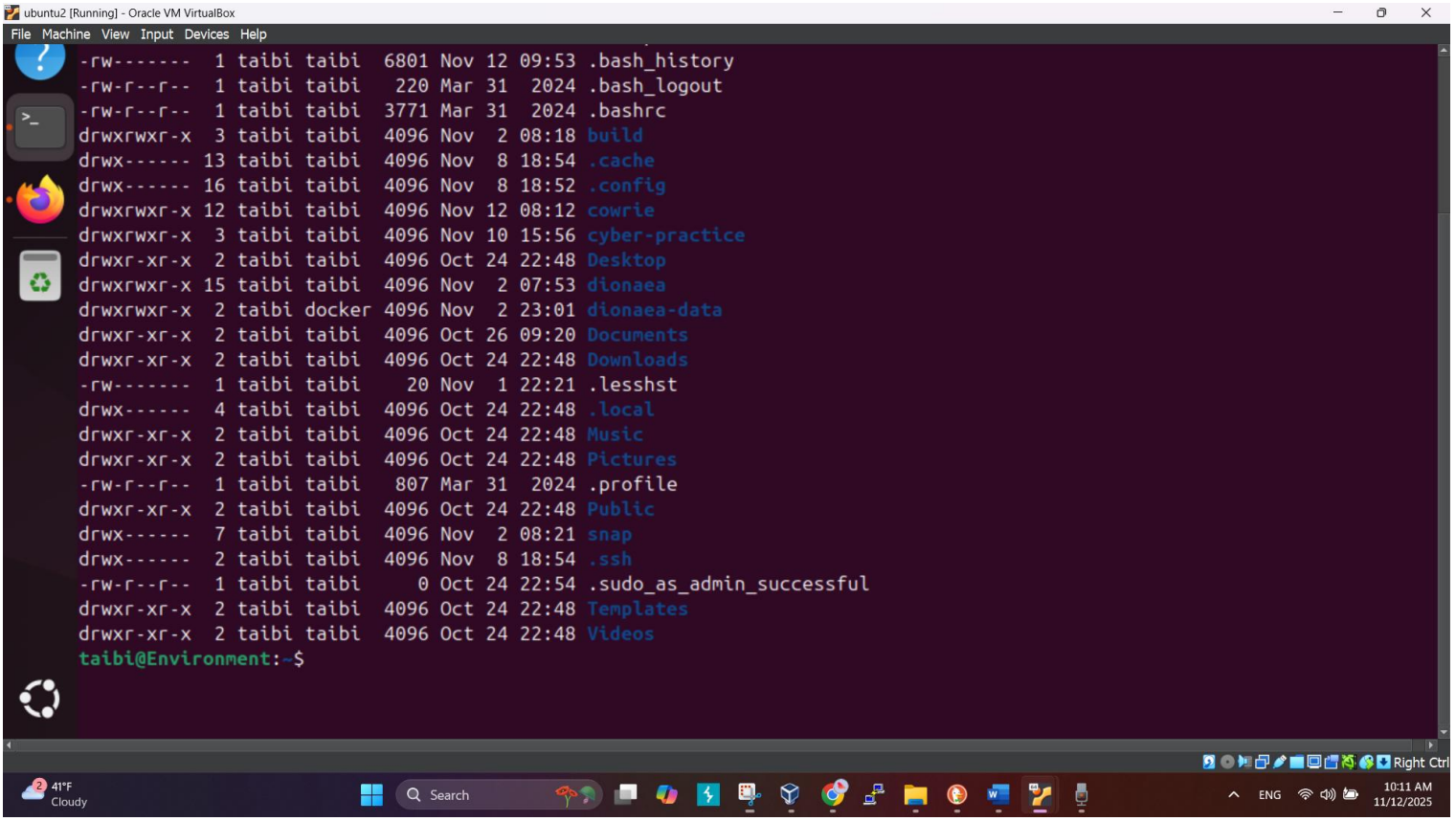
Honeypot-Log-View.png

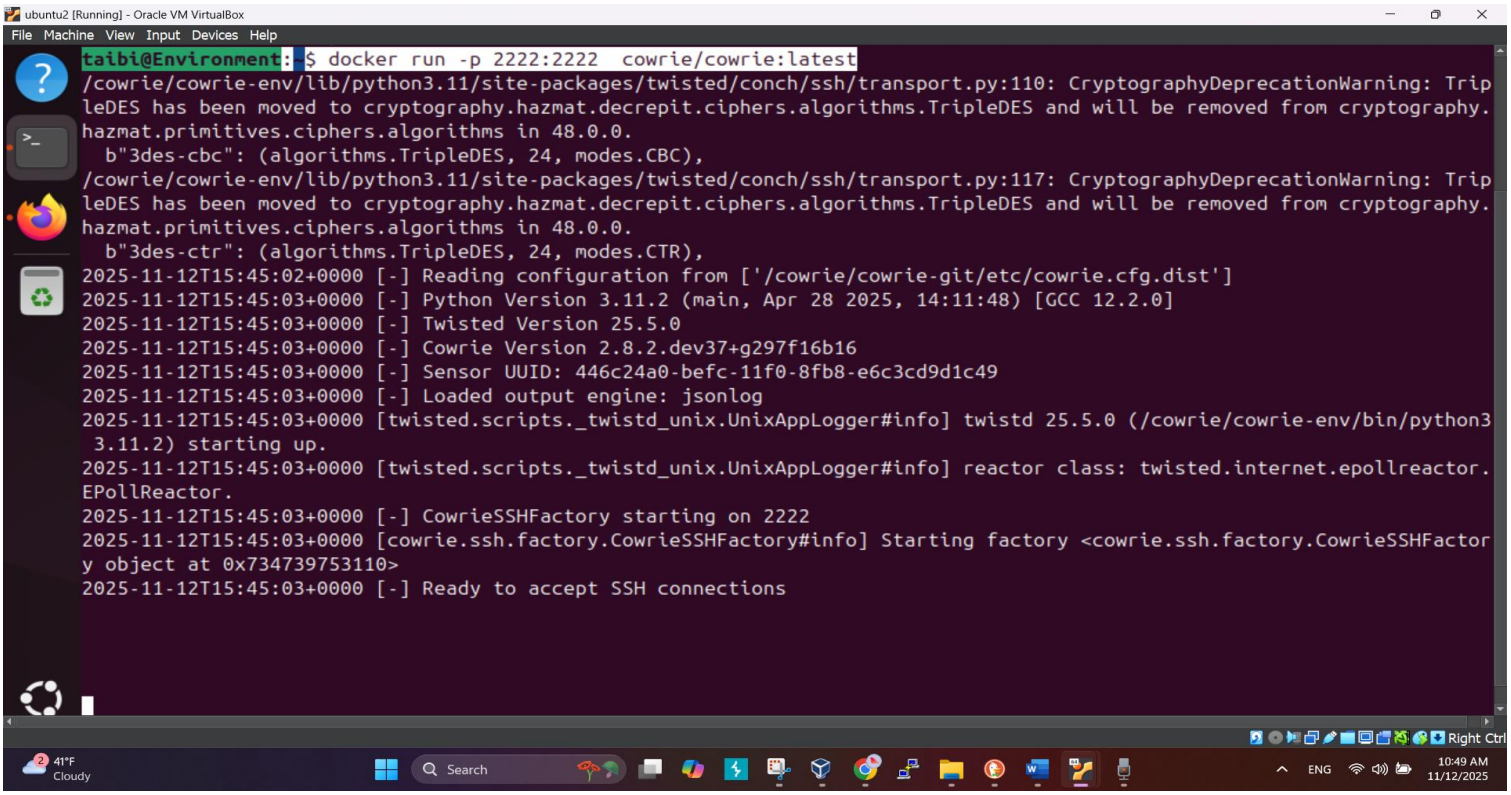


Cowrie-Installation-Directories.png

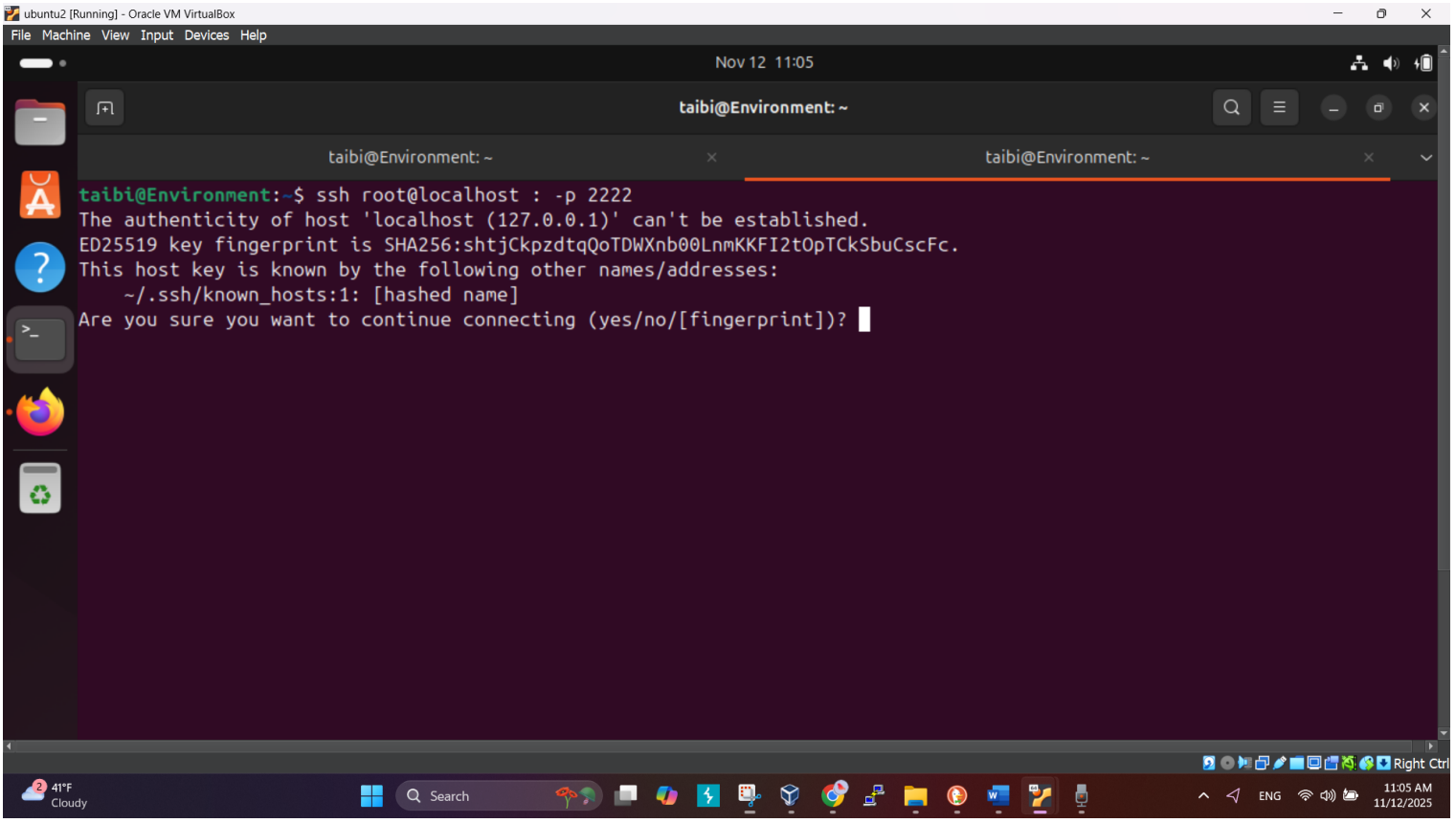


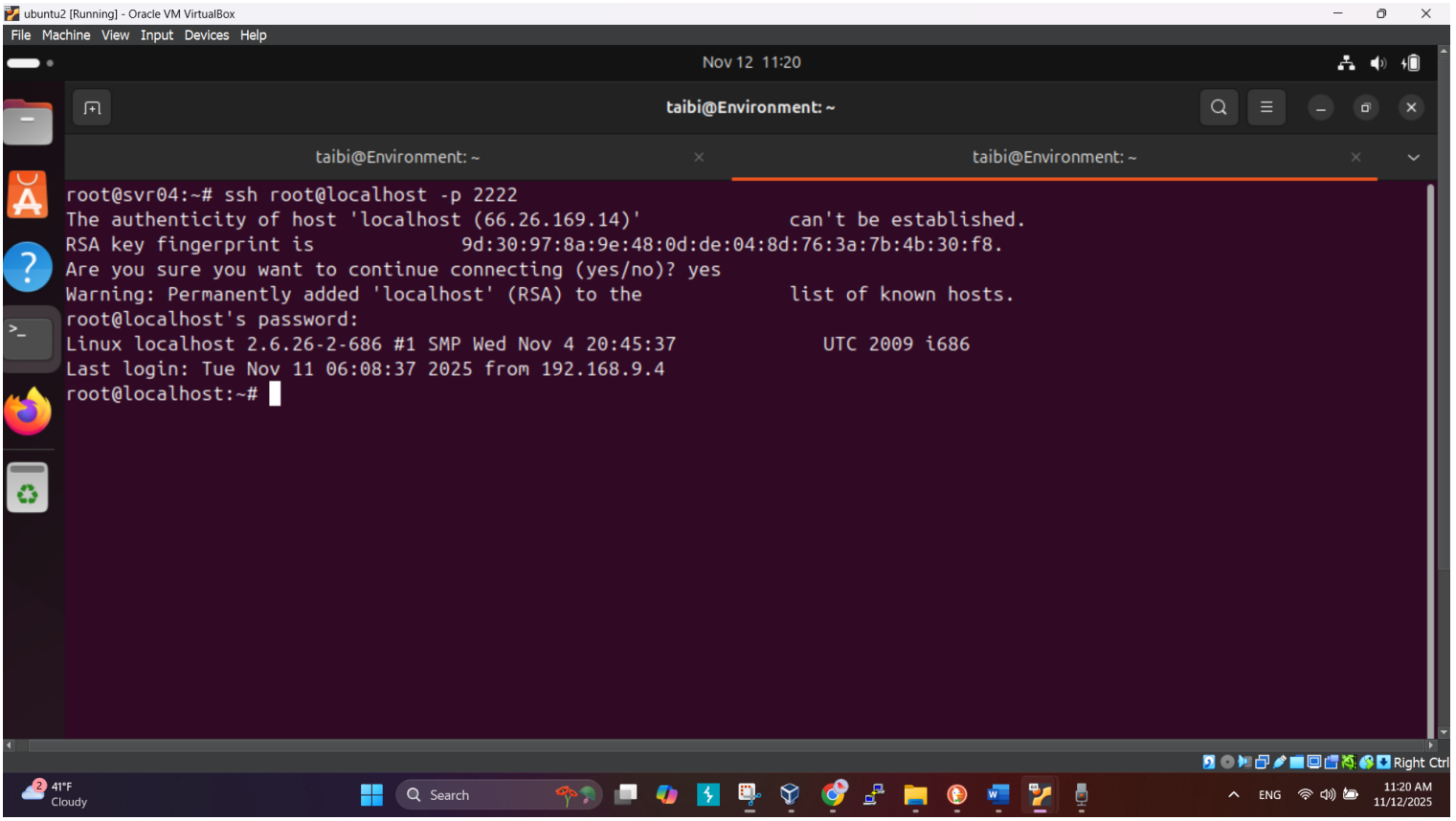


Docker-Setup-Configuration.png

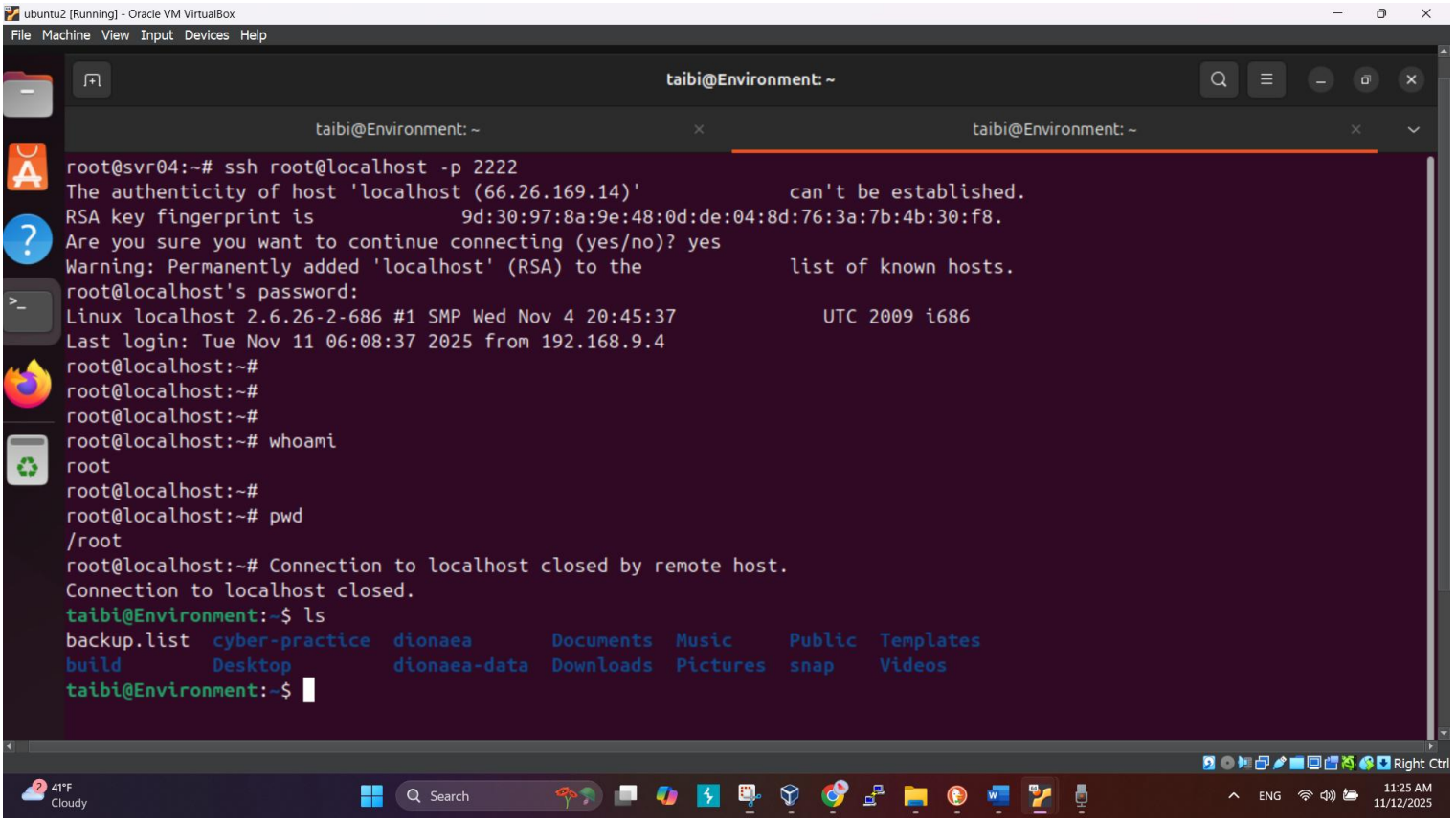


Honeypot Authentication Flow

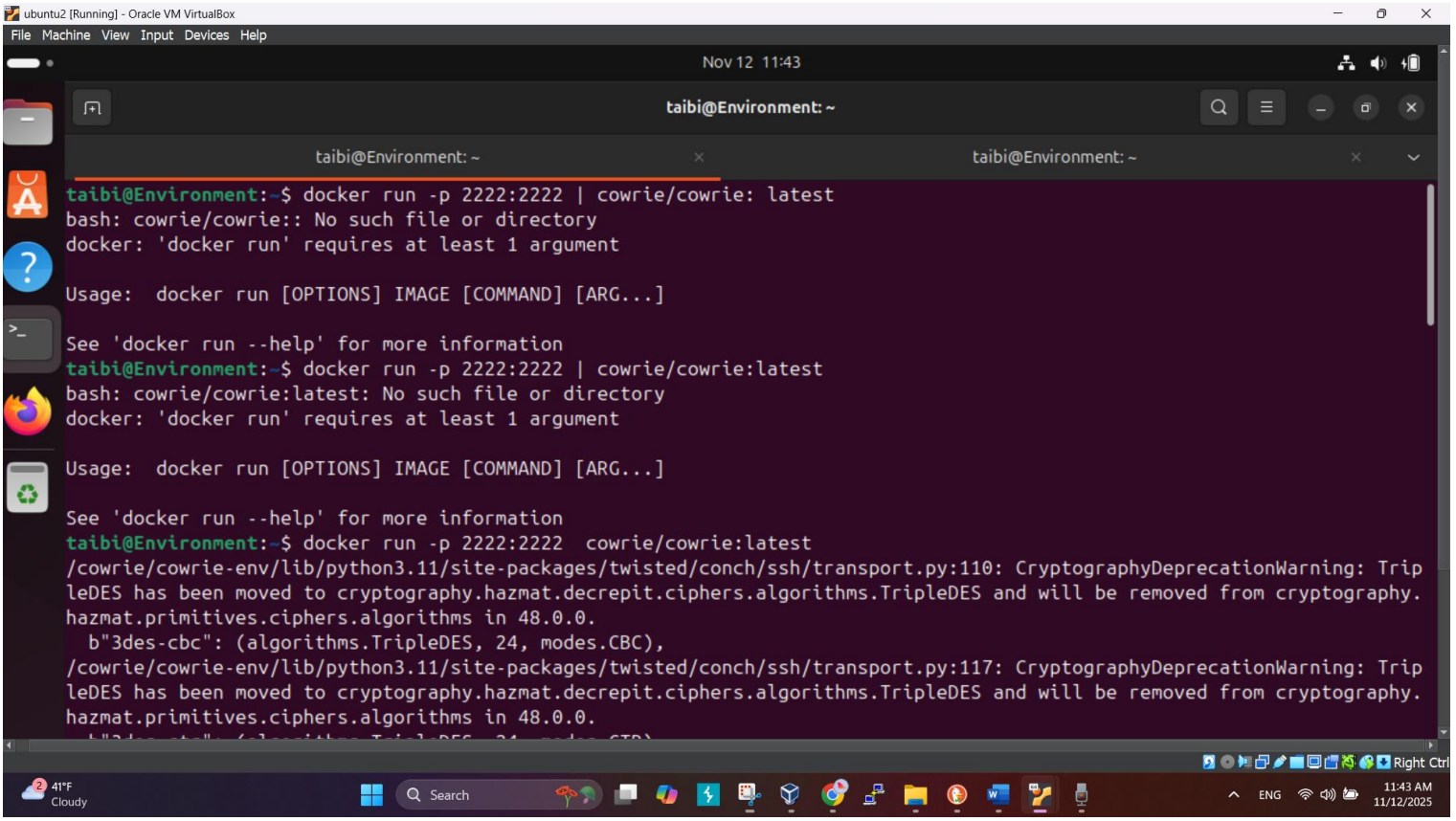




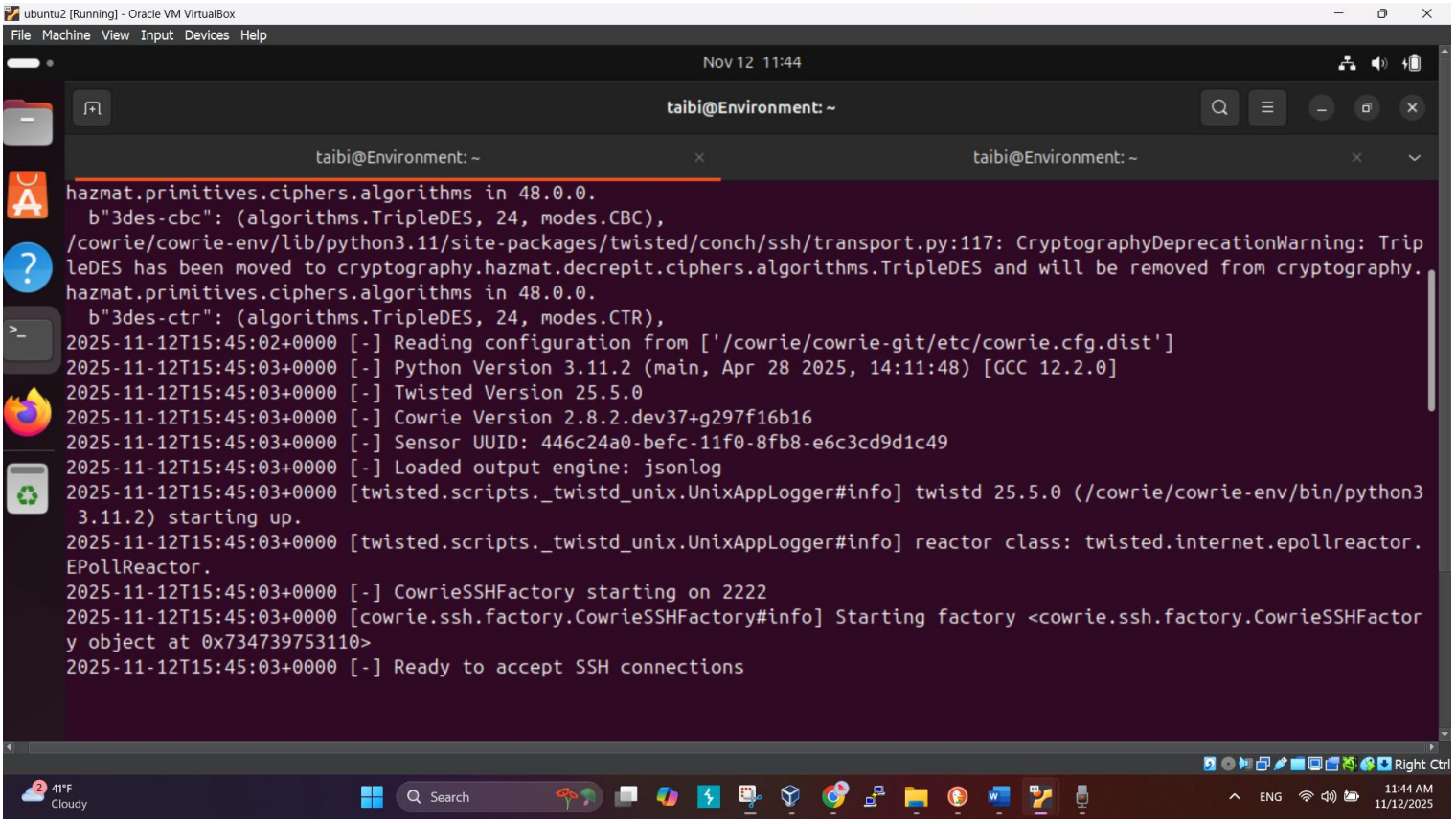
Attack session recording



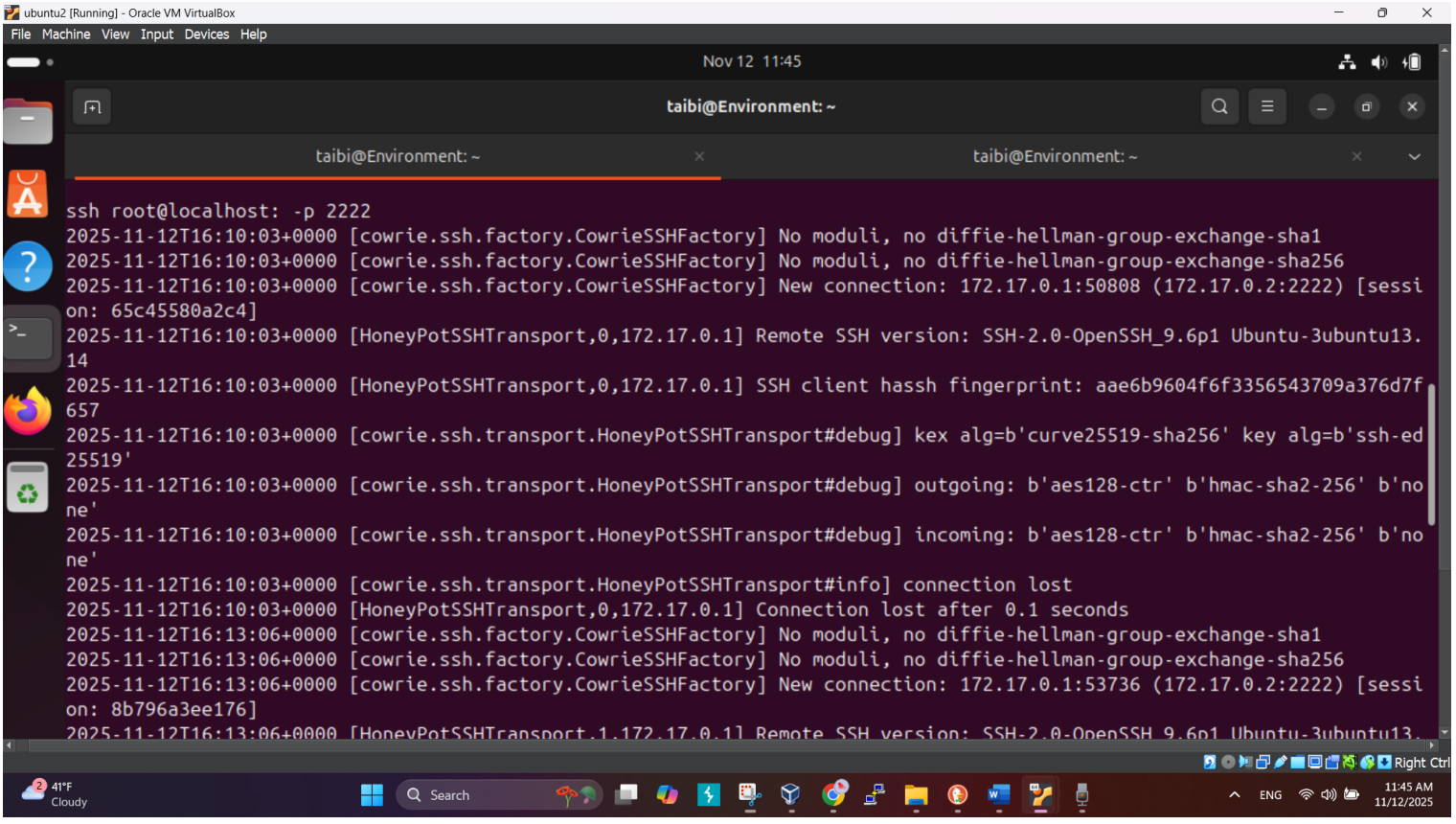
Honeypot-Log-View.png

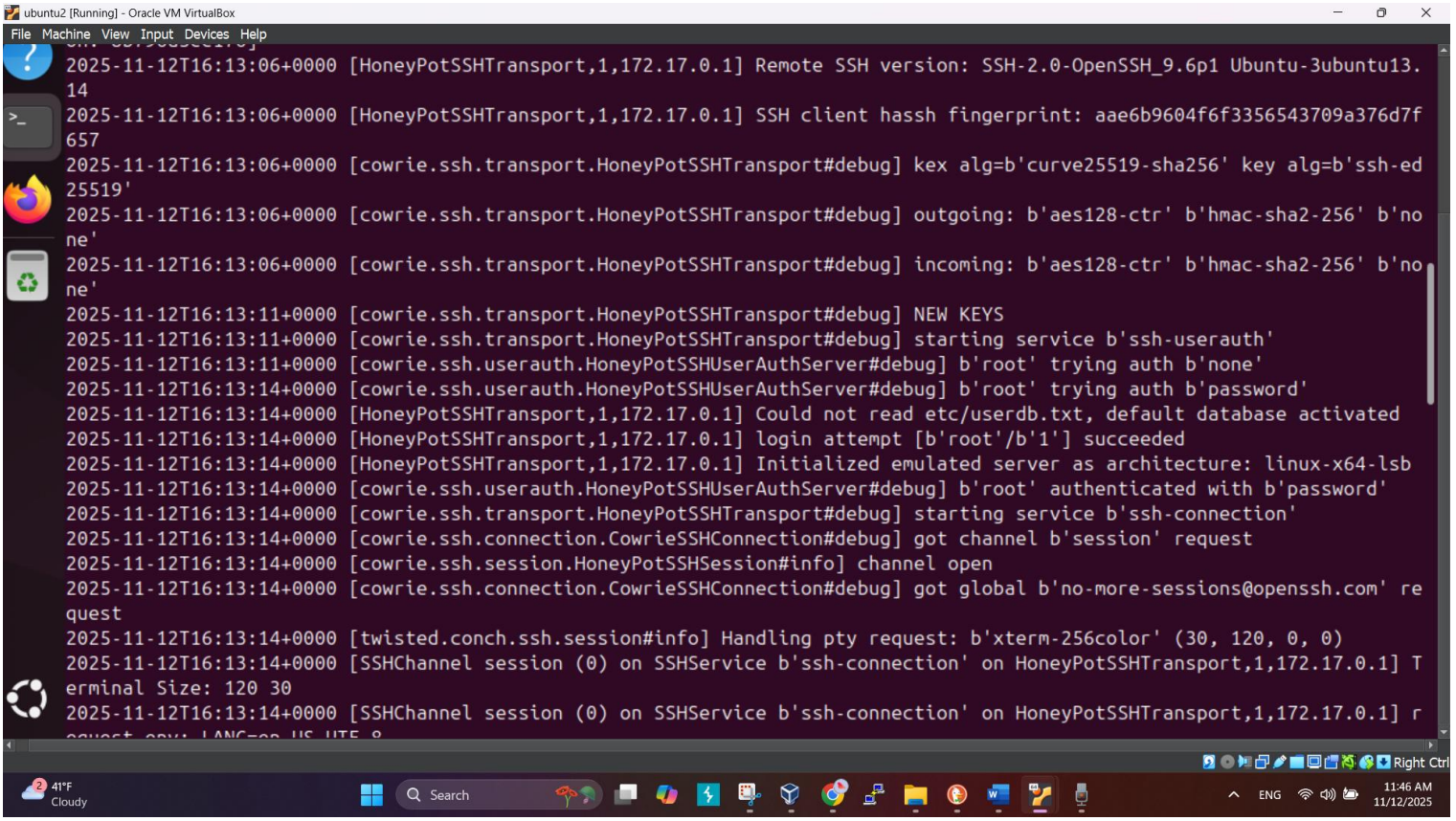


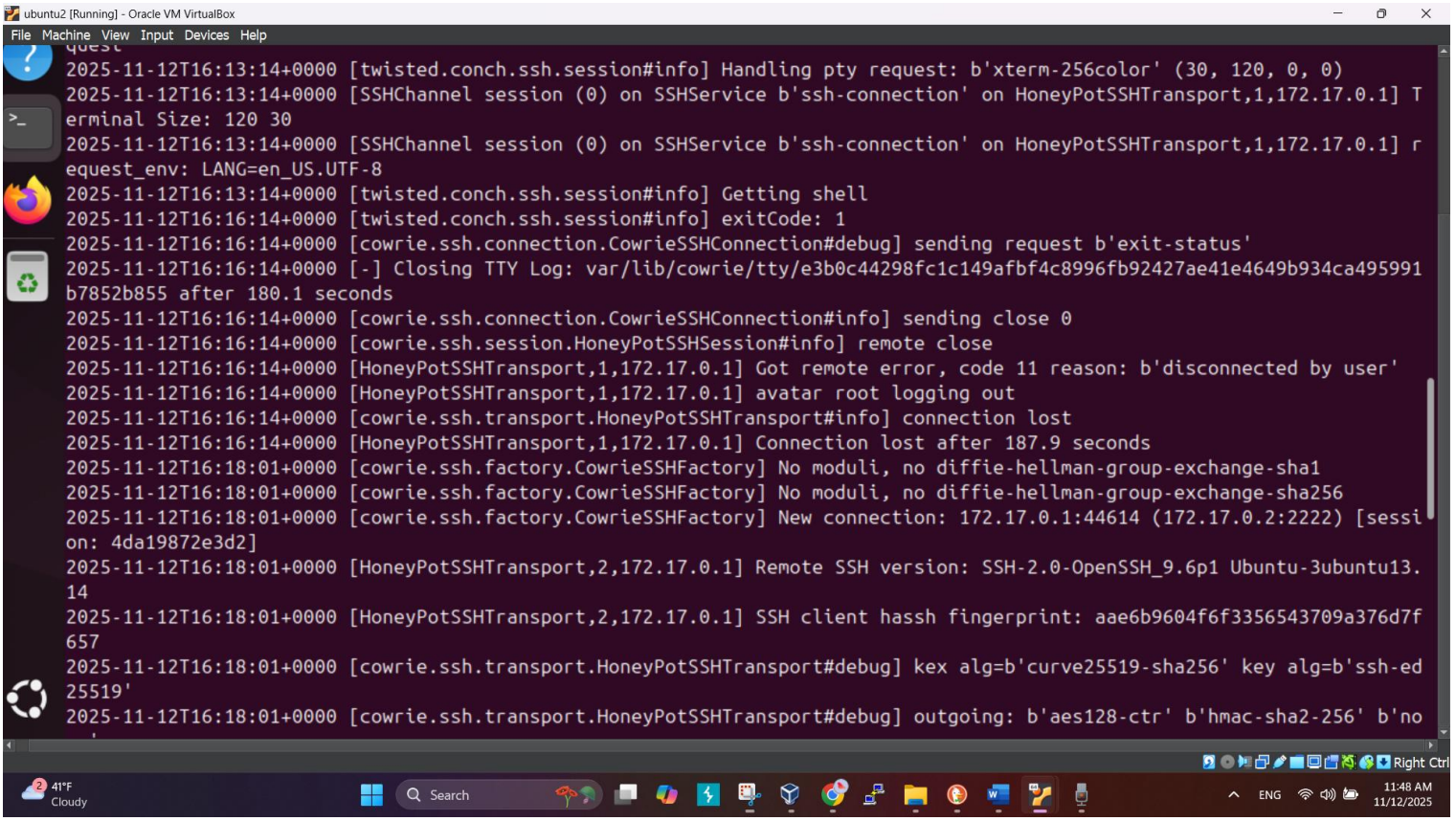
Continuation

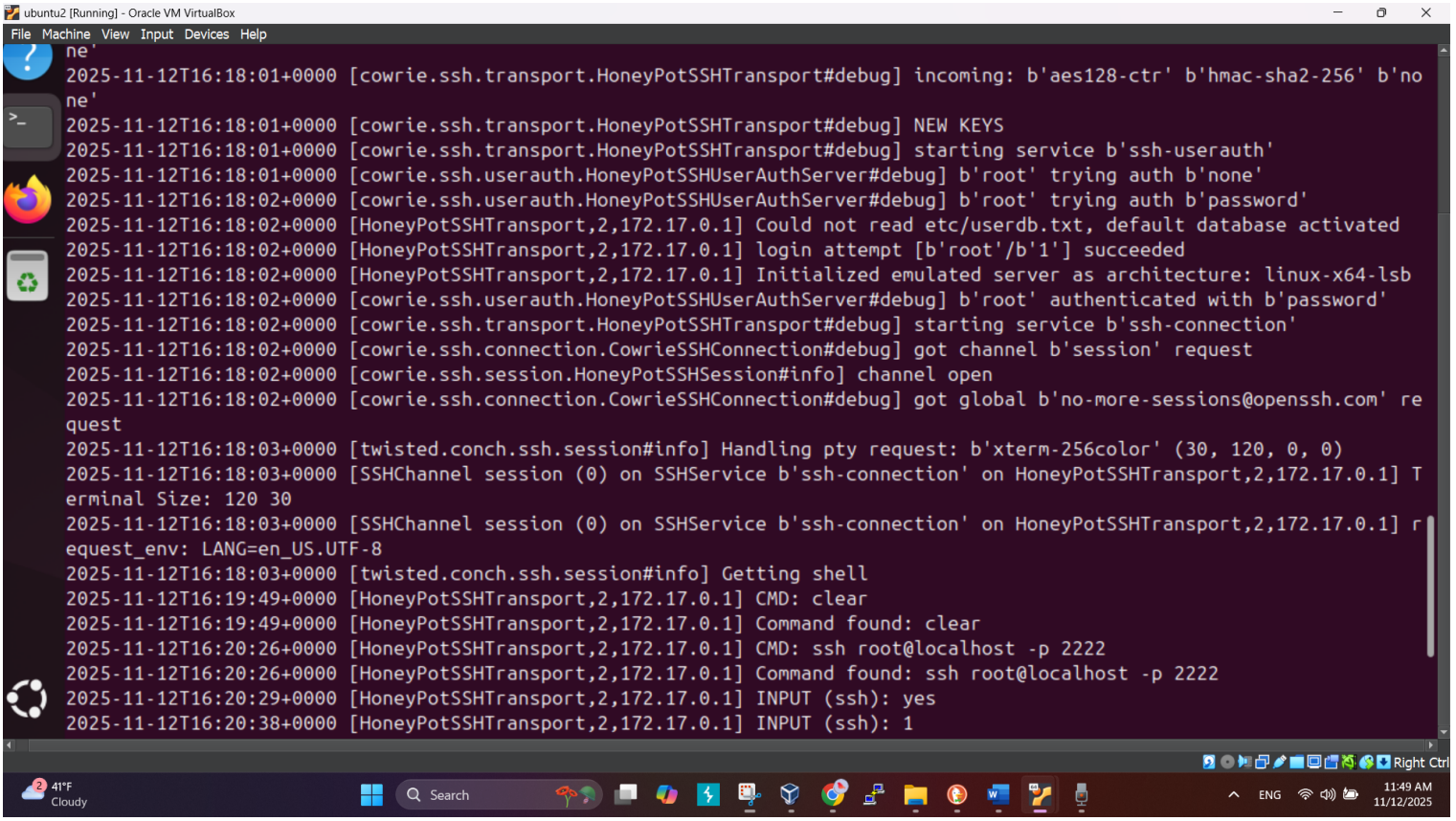


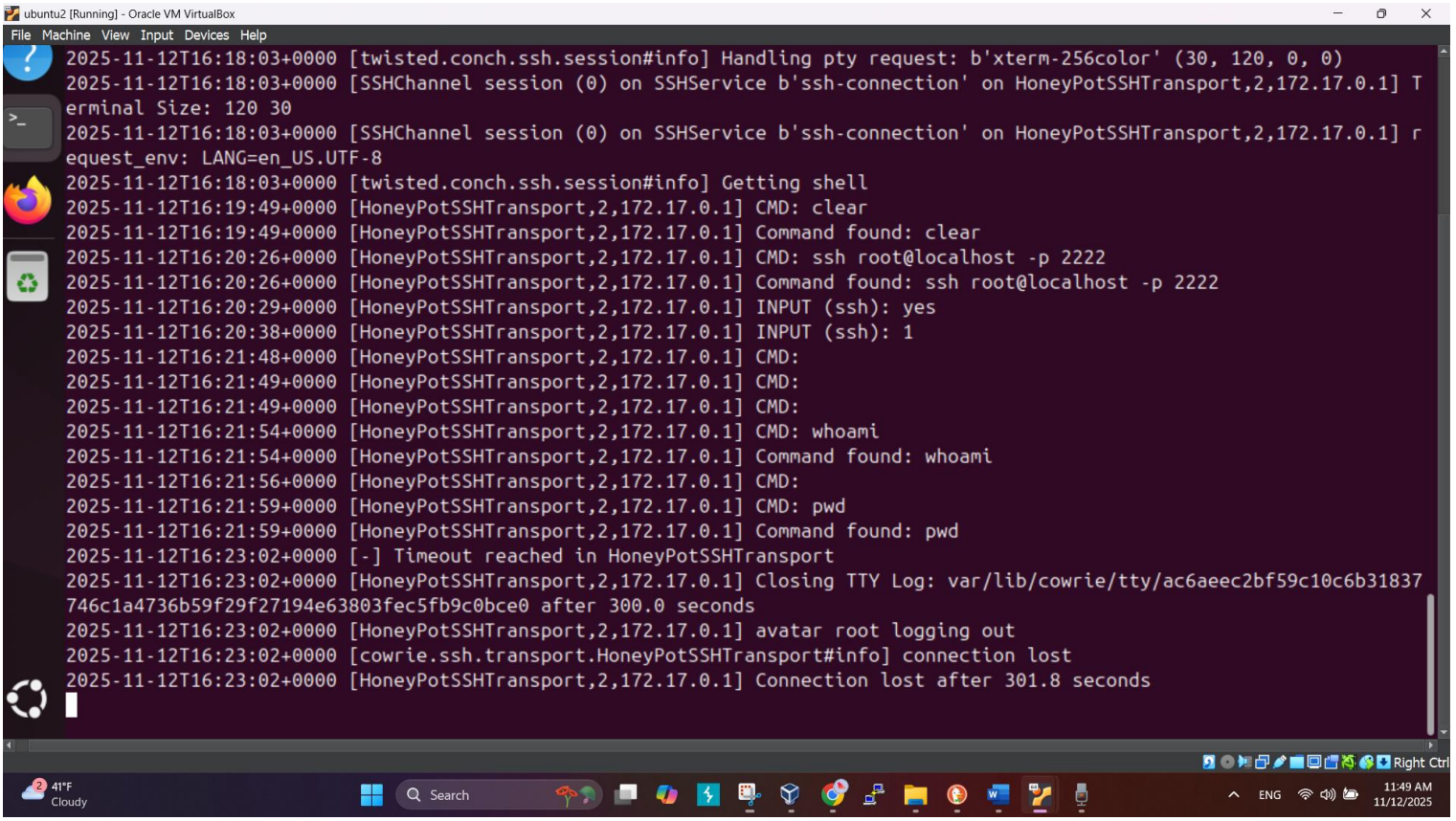
Continuation




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: aae6b9604f6f3356543709a376d7f657
2025-11-12T16:13:06+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] kex alg=b'curve25519-sha256' key alg=b'ssh-ed25519'
2025-11-12T16:13:06+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] outgoing: b'aes128-ctr' b'hmac-sha2-256' b'none'
2025-11-12T16:13:06+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] incoming: b'aes128-ctr' b'hmac-sha2-256' b'none'
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' request
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] Terminal 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
Right Ctrl
41°F Cloudy
Search
ENG
11:46 AM 11/12/2025


ubuntu2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
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] Terminal Size: 120 30
2025-11-12T16:13:14+0000 [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,1,172.17.0.1] request_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/e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855 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) [session: 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: aae6b9604f6f3356543709a376d7f657
2025-11-12T16:18:01+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] kex alg=b'curve25519-sha256' key alg=b'ssh-ed25519'
2025-11-12T16:18:01+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] outgoing: b'aes128-ctr' b'hmac-sha2-256' b'no
Right Ctrl
41°F Cloudy
Search
ENG
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'none'
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.HoneyPotSSHSession#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
Right Ctrl
41°F Cloudy
Search
ENG
11:49 AM 11/12/2025


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/ac6aeec2bf59c10c6b31837746c1a4736b59f29f27194e63803fec5fb9c0bce0 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
Right Ctrl
41°F Cloudy
Search
ENG
11:49 AM 11/12/2025

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.