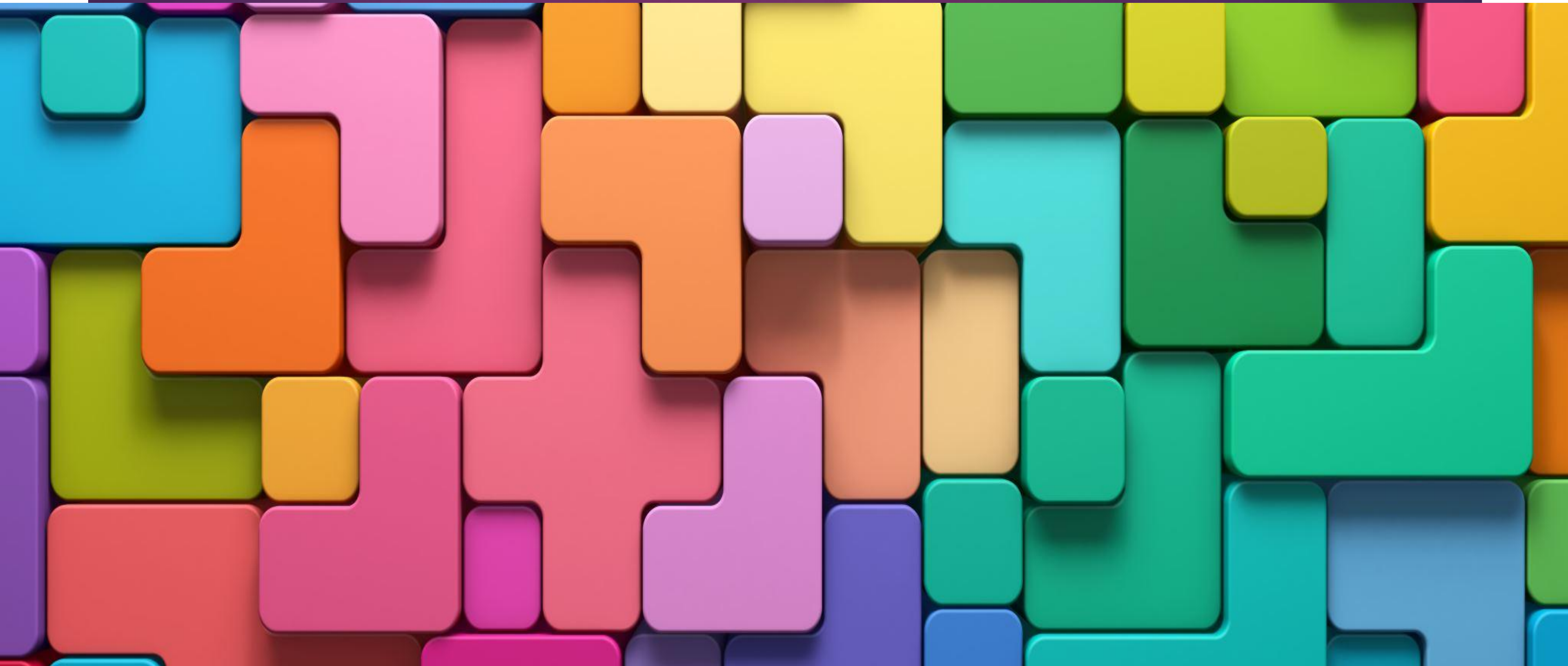
THE HONEYPOT

COWRIE RUNNING ON UBUNTU/PYTHON3

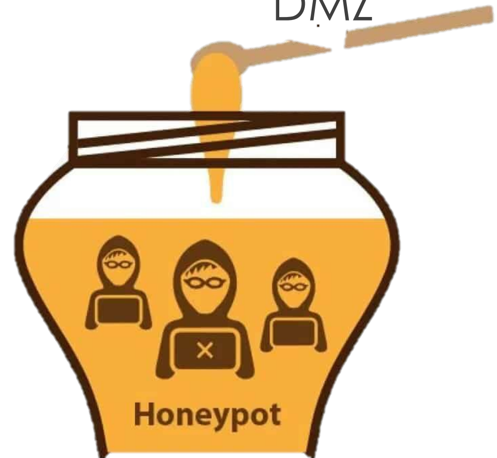
JOSHUA BRISSON, AARON MCCAMENT

CS 4910

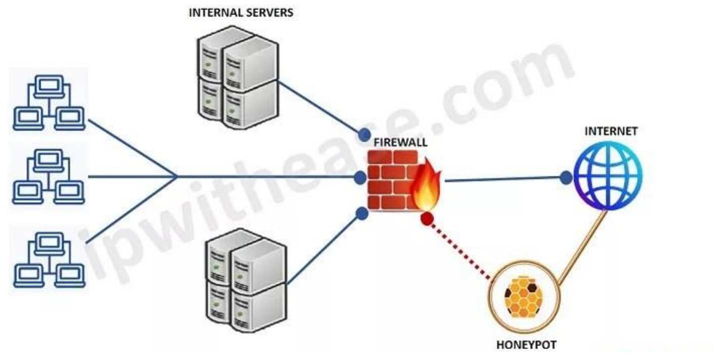


What is a honeypot?

- A fake system designed to attract malicious attackers
- Logs everything a user does (IMPORTANT!)
- Needs to be believable, so takes some effort to appear legit
- Needs to be safe to exploit, so run on a system in DMZ

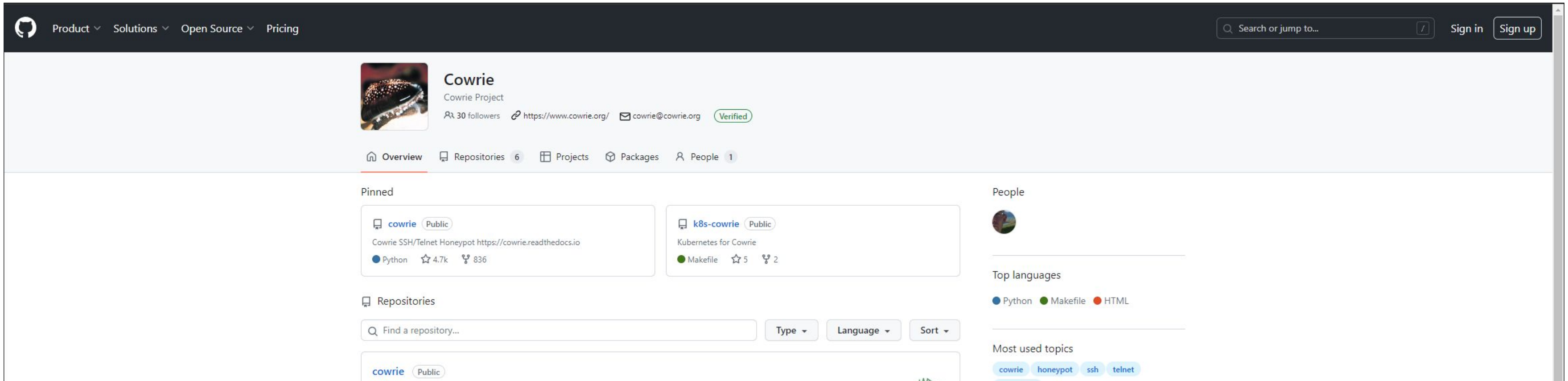


Honeypot Placed in-between Firewall & Internet



COWRIE: A Prime Example (because free and useful)

- For this project we used ‘cowrie’: https://github.com/cowrie/cowrie
- Python3 script, ran in a virtual environment, simulates an entire host system
- We ran on Ubuntu (ver 18+), via Oracle VM (AVOID CentOS! Need Python3.8+)



Cowrie
Cowrie Project
30 followers · https://www.cowrie.org/ · cowrie@cowrie.org · Verified

Pinned

cowrie Public
Cowrie SSH/Telnet Honeypot https://cowrie.readthedocs.io
Python ☆ 4.7k 836

k8s-cowrie Public
Kubernetes for Cowrie
Makefile ☆ 5 2

Repositories
Find a repository...

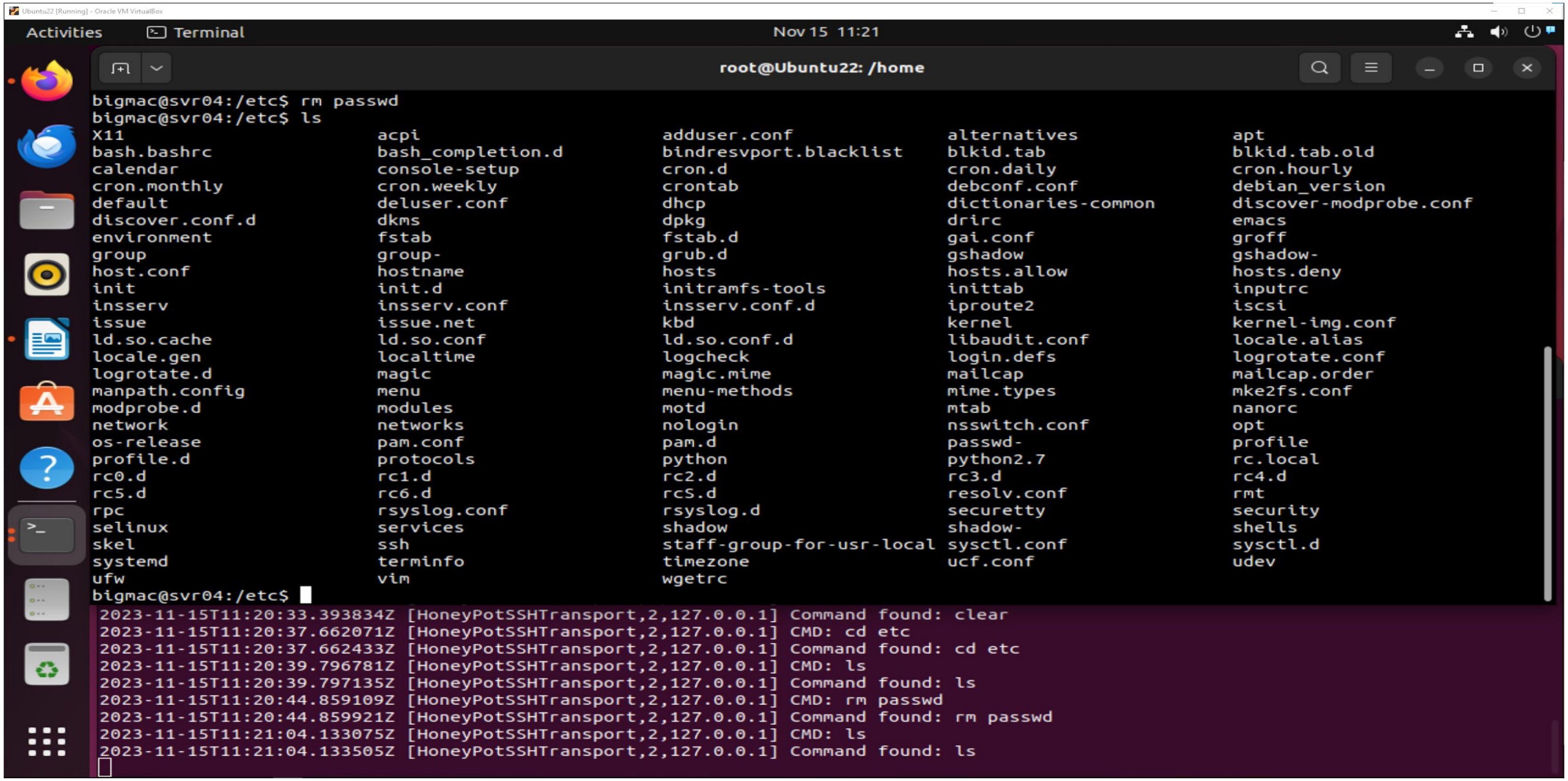
cowrie Public

People

Top languages
● Python ● Makefile ● HTML

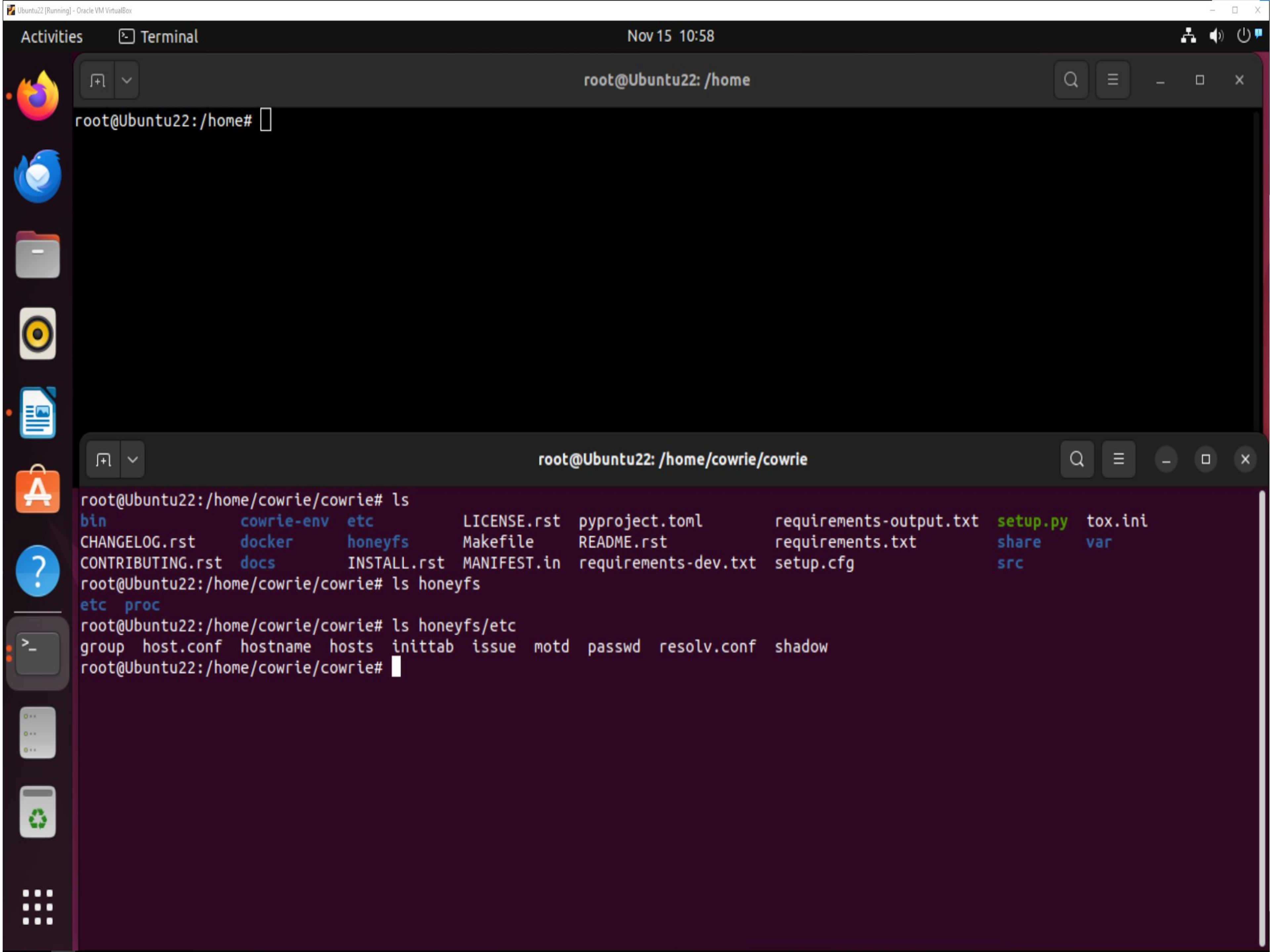
Most used topics
cowrie honeypot ssh telnet

The DEMO



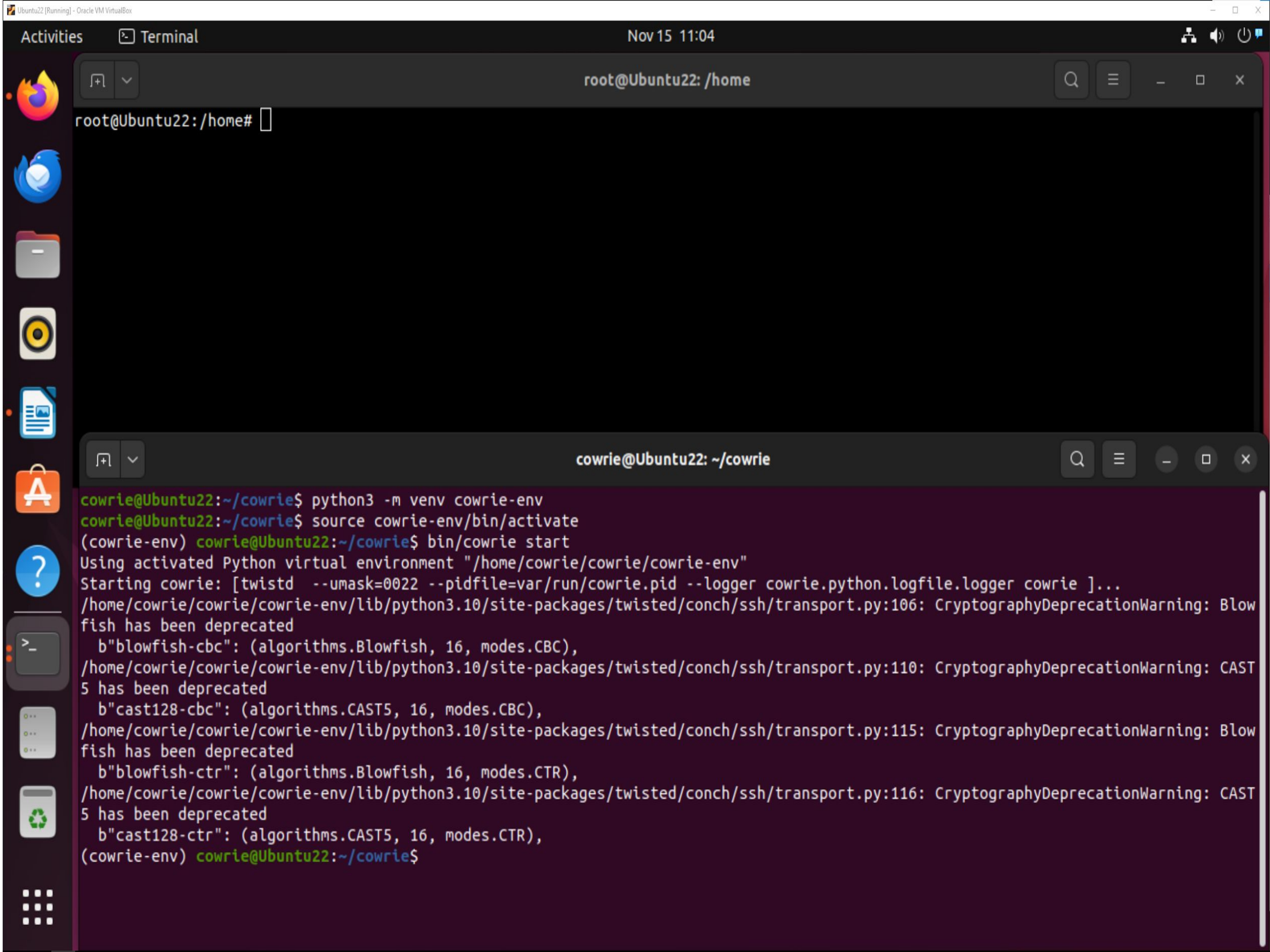
```
bigmac@svr04:/etc$ rm passwd
bigmac@svr04:/etc$ ls
X11                       acpi                      adduser.conf              alternatives              apt
bash.bashrc               bash_completion.d         bindresvport.blacklist    blkid.tab                 blkid.tab.old
calendar                  console-setup             cron.d                    cron.daily                cron.hourly
cron.monthly              cron.weekly               crontab                   debconf.conf              debian_version
default                   deluser.conf              dhcp                      dictionaries-common       discover-modprobe.conf
discover.conf.d           dkms                      dpkg                      drirc                     emacs
environment               fstab                     fstab.d                   gai.conf                  groff
group                     group-                    grub.d                    gshadow                   gshadow-
host.conf                 hostname                  hosts                     hosts.allow               hosts.deny
init                      init.d                    initramfs-tools           inittab                   inputrc
insserv                   insserv.conf              insserv.conf.d            iproute2                  iscsi
issue                     issue.net                 kbd                       kernel                    kernel-img.conf
ld.so.cache               ld.so.conf                ld.so.conf.d              libaudit.conf             locale.alias
locale.gen                localtime                 logcheck                  login.defs                logrotate.conf
logrotate.d               magic                     magic.mime                mailcap                   mailcap.order
manpath.config            menu                      menu-methods              mime.types                mke2fs.conf
modprobe.d                modules                   motd                      mtab                      nanorc
network                   networks                  nologin                   nsswitch.conf             opt
os-release                pam.conf                  pam.d                     passwd-                   profile
profile.d                 protocols                 python                    python2.7                 rc.local
rc0.d                     rc1.d                     rc2.d                     rc3.d                     rc4.d
rc5.d                     rc6.d                     rcS.d                     resolv.conf               rmt
rpc                       rsyslog.conf              rsyslog.d                 securetty                 security
selinux                   services                  shadow                    shadow-                   shells
skel                      ssh                       staff-group-for-usr-local sysctl.conf               sysctl.d
systemd                   terminfo                  timezone                  ucf.conf                  udev
ufw                       vim                       wgetrc
bigmac@svr04:/etc$
```

```
2023-11-15T11:20:33.393834Z [HoneyPotSSHTransport,2,127.0.0.1] Command found: clear
2023-11-15T11:20:37.662071Z [HoneyPotSSHTransport,2,127.0.0.1] CMD: cd etc
2023-11-15T11:20:37.662433Z [HoneyPotSSHTransport,2,127.0.0.1] Command found: cd etc
2023-11-15T11:20:39.796781Z [HoneyPotSSHTransport,2,127.0.0.1] CMD: ls
2023-11-15T11:20:39.797135Z [HoneyPotSSHTransport,2,127.0.0.1] Command found: ls
2023-11-15T11:20:44.859109Z [HoneyPotSSHTransport,2,127.0.0.1] CMD: rm passwd
2023-11-15T11:20:44.859921Z [HoneyPotSSHTransport,2,127.0.0.1] Command found: rm passwd
2023-11-15T11:21:04.133075Z [HoneyPotSSHTransport,2,127.0.0.1] CMD: ls
2023-11-15T11:21:04.133505Z [HoneyPotSSHTransport,2,127.0.0.1] Command found: ls
```


Ubuntu22 [Running] - Oracle VM VirtualBox
Activities
Terminal
Nov 15 10:58
root@Ubuntu22: /home
root@Ubuntu22: /home/cowrie/cowrie

```
root@Ubuntu22:/home#
```

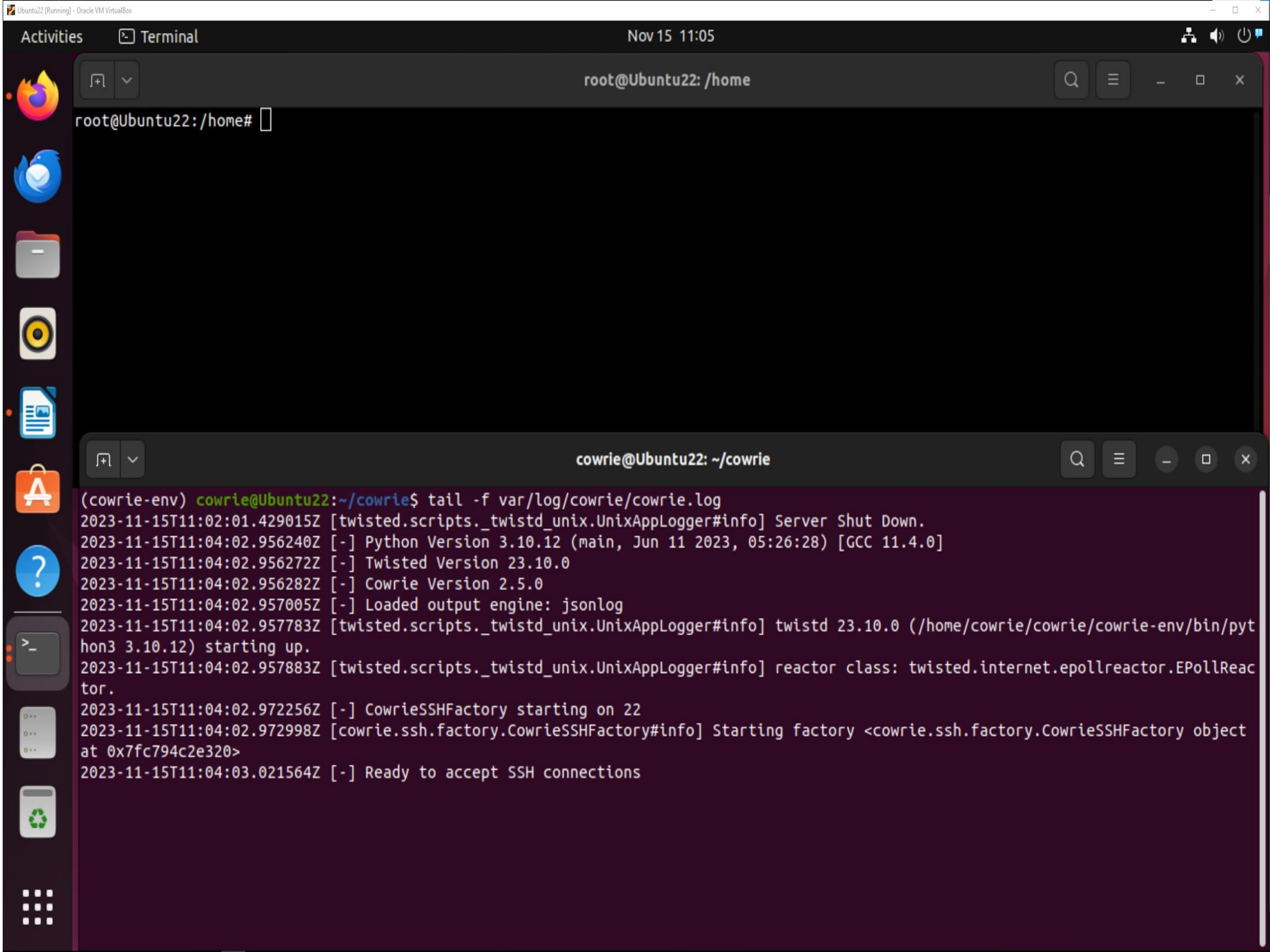
```
root@Ubuntu22:/home/cowrie/cowrie# ls
bin              cowrie-env  etc          LICENSE.rst  pyproject.toml          requirements-output.txt  setup.py  tox.ini
CHANGELOG.rst    docker      honeyfs      Makefile     README.rst              requirements.txt         share     var
CONTRIBUTING.rst docs        INSTALL.rst  MANIFEST.in  requirements-dev.txt    setup.cfg                src
root@Ubuntu22:/home/cowrie/cowrie# ls honeyfs
etc  proc
root@Ubuntu22:/home/cowrie/cowrie# ls honeyfs/etc
group  host.conf  hostname  hosts  inittab  issue  motd  passwd  resolv.conf  shadow
root@Ubuntu22:/home/cowrie/cowrie#
```



Ubuntu22 [Running] - Oracle VM VirtualBox
Activities
Terminal
Nov 15 11:04
root@Ubuntu22: /home
cowrie@Ubuntu22: ~/cowrie

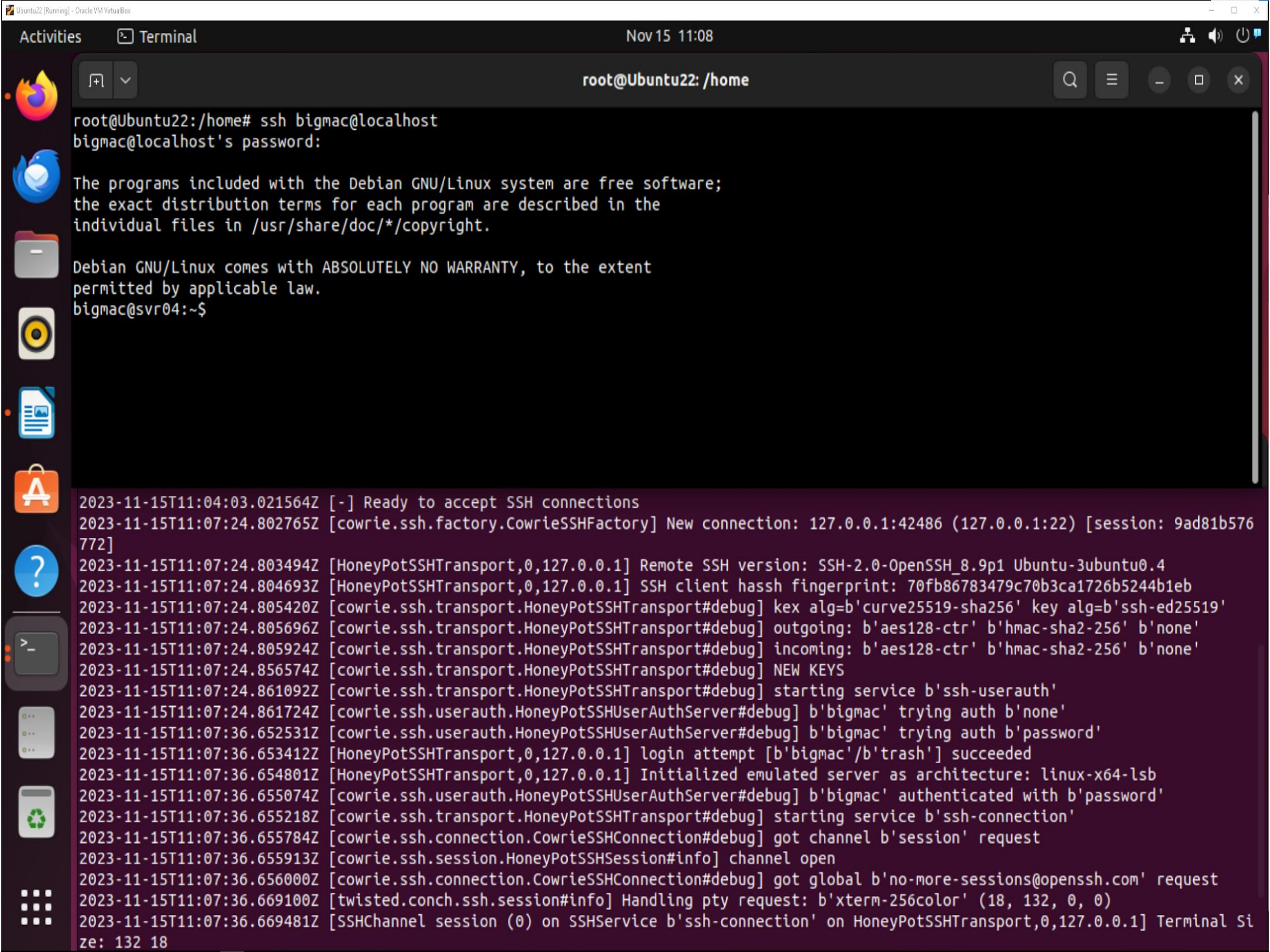
```
root@Ubuntu22:/home#
```

```
cowrie@Ubuntu22:~/cowrie$ python3 -m venv cowrie-env
cowrie@Ubuntu22:~/cowrie$ source cowrie-env/bin/activate
(cowrie-env) cowrie@Ubuntu22:~/cowrie$ bin/cowrie start
Using activated Python virtual environment "/home/cowrie/cowrie/cowrie-env"
Starting cowrie: [twistd  --umask=0022 --pidfile=var/run/cowrie.pid --logger cowrie.python.logfile.logger cowrie ]...
/home/cowrie/cowrie/cowrie-env/lib/python3.10/site-packages/twisted/conch/ssh/transport.py:106: CryptographyDeprecationWarning: Blowfish has been deprecated
  b"blowfish-cbc": (algorithms.Blowfish, 16, modes.CBC),
/home/cowrie/cowrie/cowrie-env/lib/python3.10/site-packages/twisted/conch/ssh/transport.py:110: CryptographyDeprecationWarning: CAST5 has been deprecated
  b"cast128-cbc": (algorithms.CAST5, 16, modes.CBC),
/home/cowrie/cowrie/cowrie-env/lib/python3.10/site-packages/twisted/conch/ssh/transport.py:115: CryptographyDeprecationWarning: Blowfish has been deprecated
  b"blowfish-ctr": (algorithms.Blowfish, 16, modes.CTR),
/home/cowrie/cowrie/cowrie-env/lib/python3.10/site-packages/twisted/conch/ssh/transport.py:116: CryptographyDeprecationWarning: CAST5 has been deprecated
  b"cast128-ctr": (algorithms.CAST5, 16, modes.CTR),
(cowrie-env) cowrie@Ubuntu22:~/cowrie$
```


Ubuntu22 [Running] - Oracle VM VirtualBox
Activities
Terminal
Nov 15 11:05
root@Ubuntu22: /home
cowrie@Ubuntu22: ~/cowrie

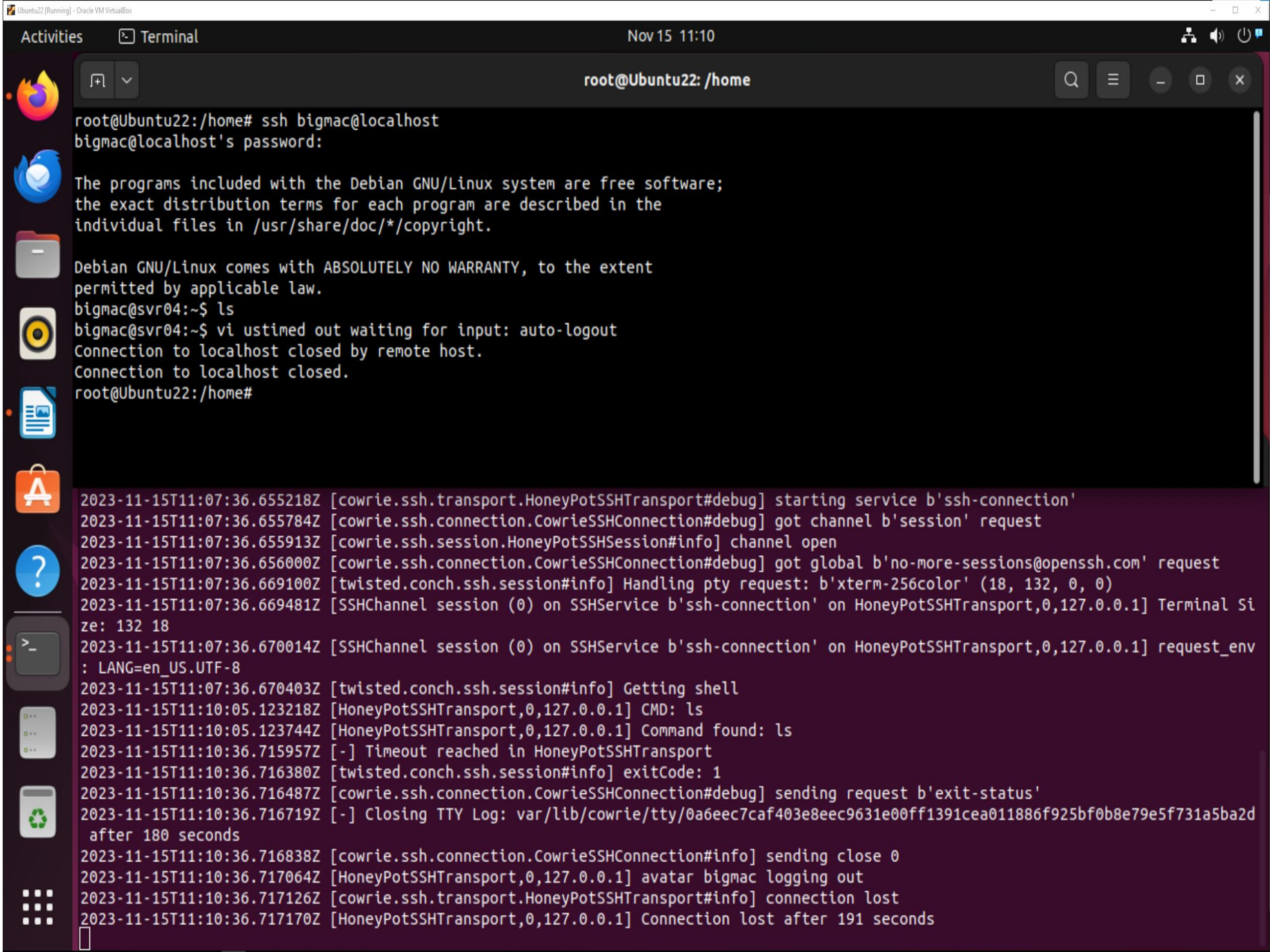
```
root@Ubuntu22:/home# 
```

```
(cowrie-env) cowrie@Ubuntu22:~/cowrie$ tail -f var/log/cowrie/cowrie.log
2023-11-15T11:02:01.429015Z [twisted.scripts._twistd_unix.UnixAppLogger#info] Server Shut Down.
2023-11-15T11:04:02.956240Z [-] Python Version 3.10.12 (main, Jun 11 2023, 05:26:28) [GCC 11.4.0]
2023-11-15T11:04:02.956272Z [-] Twisted Version 23.10.0
2023-11-15T11:04:02.956282Z [-] Cowrie Version 2.5.0
2023-11-15T11:04:02.957005Z [-] Loaded output engine: jsonlog
2023-11-15T11:04:02.957783Z [twisted.scripts._twistd_unix.UnixAppLogger#info] twistd 23.10.0 (/home/cowrie/cowrie/cowrie-env/bin/pyt
hon3 3.10.12) starting up.
2023-11-15T11:04:02.957883Z [twisted.scripts._twistd_unix.UnixAppLogger#info] reactor class: twisted.internet.epollreactor.EPollReac
tor.
2023-11-15T11:04:02.972256Z [-] CowrieSSHFactory starting on 22
2023-11-15T11:04:02.972998Z [cowrie.ssh.factory.CowrieSSHFactory#info] Starting factory <cowrie.ssh.factory.CowrieSSHFactory object
at 0x7fc794c2e320>
2023-11-15T11:04:03.021564Z [-] Ready to accept SSH connections
```



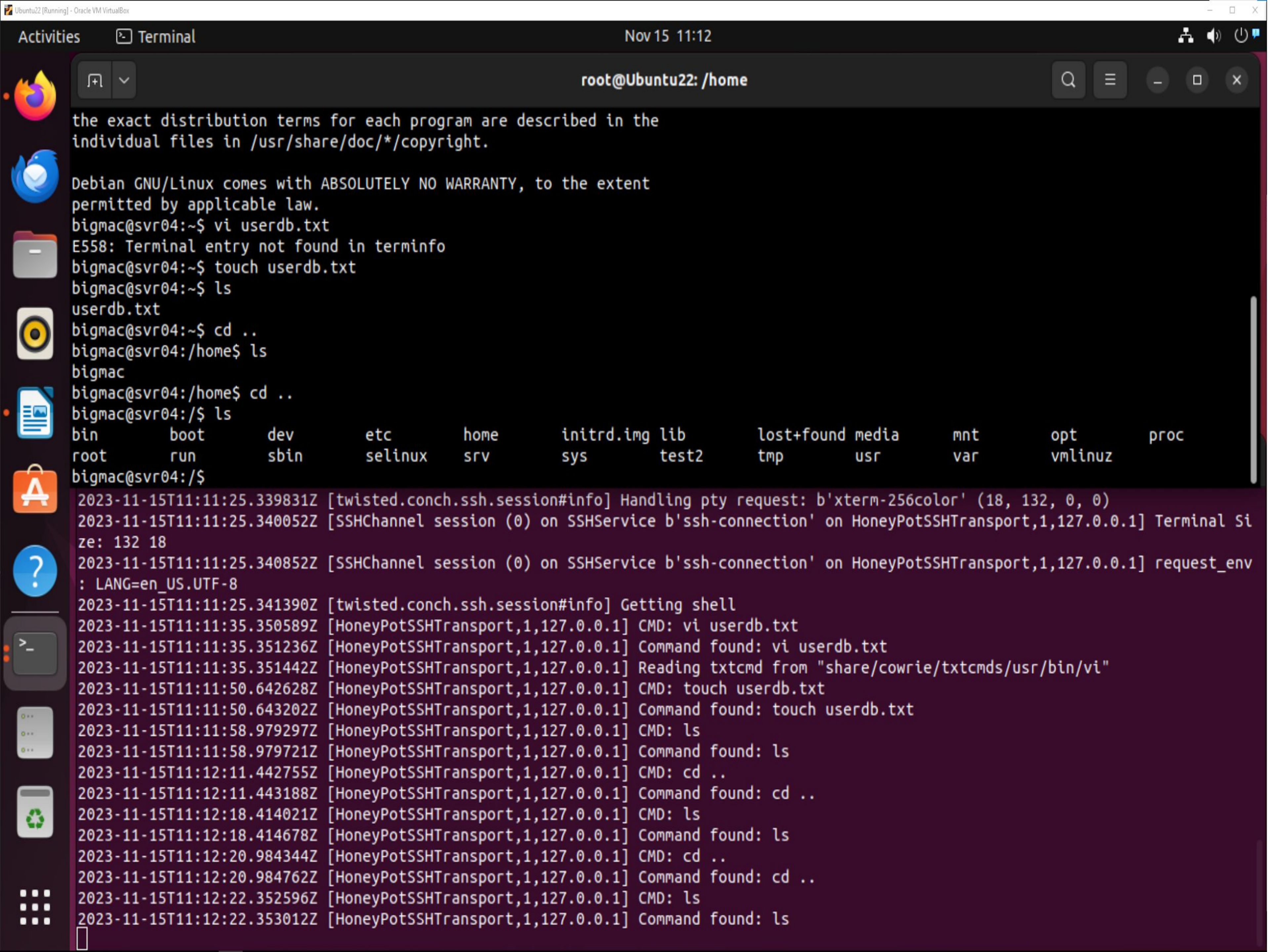
```
root@Ubuntu22:/home# ssh bigmac@localhost
bigmac@localhost's password:

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.
bigmac@svr04:~$
```

```
2023-11-15T11:04:03.021564Z [-] Ready to accept SSH connections
2023-11-15T11:07:24.802765Z [cowrie.ssh.factory.CowrieSSHFactory] New connection: 127.0.0.1:42486 (127.0.0.1:22) [session: 9ad81b576
772]
2023-11-15T11:07:24.803494Z [HoneyPotSSHTransport,0,127.0.0.1] Remote SSH version: SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.4
2023-11-15T11:07:24.804693Z [HoneyPotSSHTransport,0,127.0.0.1] SSH client hassh fingerprint: 70fb86783479c70b3ca1726b5244b1eb
2023-11-15T11:07:24.805420Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] kex alg=b'curve25519-sha256' key alg=b'ssh-ed25519'
2023-11-15T11:07:24.805696Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] outgoing: b'aes128-ctr' b'hmac-sha2-256' b'none'
2023-11-15T11:07:24.805924Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] incoming: b'aes128-ctr' b'hmac-sha2-256' b'none'
2023-11-15T11:07:24.856574Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] NEW KEYS
2023-11-15T11:07:24.861092Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-userauth'
2023-11-15T11:07:24.861724Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'bigmac' trying auth b'none'
2023-11-15T11:07:36.652531Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'bigmac' trying auth b'password'
2023-11-15T11:07:36.653412Z [HoneyPotSSHTransport,0,127.0.0.1] login attempt [b'bigmac'/b'trash'] succeeded
2023-11-15T11:07:36.654801Z [HoneyPotSSHTransport,0,127.0.0.1] Initialized emulated server as architecture: linux-x64-lsb
2023-11-15T11:07:36.655074Z [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'bigmac' authenticated with b'password'
2023-11-15T11:07:36.655218Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-connection'
2023-11-15T11:07:36.655784Z [cowrie.ssh.connection.CowrieSSHConnection#debug] got channel b'session' request
2023-11-15T11:07:36.655913Z [cowrie.ssh.session.HoneyPotSSHSession#info] channel open
2023-11-15T11:07:36.656000Z [cowrie.ssh.connection.CowrieSSHConnection#debug] got global b'no-more-sessions@openssh.com' request
2023-11-15T11:07:36.669100Z [twisted.conch.ssh.session#info] Handling pty request: b'xterm-256color' (18, 132, 0, 0)
2023-11-15T11:07:36.669481Z [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,0,127.0.0.1] Terminal Si
ze: 132 18
```



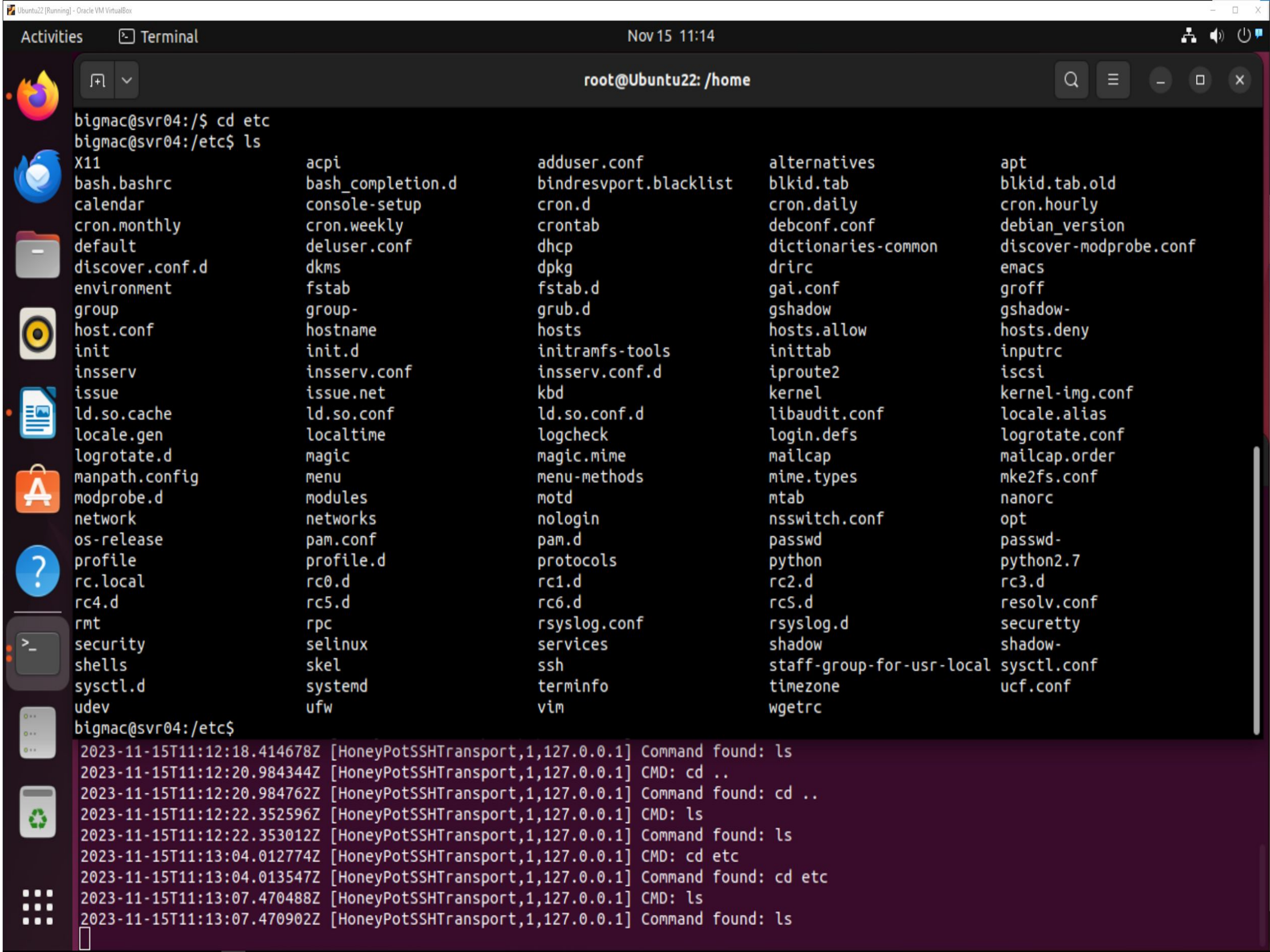
```
root@Ubuntu22:/home# ssh bigmac@localhost
bigmac@localhost's password:

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.
bigmac@svr04:~$ ls
bigmac@svr04:~$ vi ustimed out waiting for input: auto-logout
Connection to localhost closed by remote host.
Connection to localhost closed.
root@Ubuntu22:/home#
```

```
2023-11-15T11:07:36.655218Z [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-connection'
2023-11-15T11:07:36.655784Z [cowrie.ssh.connection.CowrieSSHConnection#debug] got channel b'session' request
2023-11-15T11:07:36.655913Z [cowrie.ssh.session.HoneyPotSSHSession#info] channel open
2023-11-15T11:07:36.656000Z [cowrie.ssh.connection.CowrieSSHConnection#debug] got global b'no-more-sessions@openssh.com' request
2023-11-15T11:07:36.669100Z [twisted.conch.ssh.session#info] Handling pty request: b'xterm-256color' (18, 132, 0, 0)
2023-11-15T11:07:36.669481Z [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,0,127.0.0.1] Terminal Si
ze: 132 18
2023-11-15T11:07:36.670014Z [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,0,127.0.0.1] request_env
: LANG=en_US.UTF-8
2023-11-15T11:07:36.670403Z [twisted.conch.ssh.session#info] Getting shell
2023-11-15T11:10:05.123218Z [HoneyPotSSHTransport,0,127.0.0.1] CMD: ls
2023-11-15T11:10:05.123744Z [HoneyPotSSHTransport,0,127.0.0.1] Command found: ls
2023-11-15T11:10:36.715957Z [-] Timeout reached in HoneyPotSSHTransport
2023-11-15T11:10:36.716380Z [twisted.conch.ssh.session#info] exitCode: 1
2023-11-15T11:10:36.716487Z [cowrie.ssh.connection.CowrieSSHConnection#debug] sending request b'exit-status'
2023-11-15T11:10:36.716719Z [-] Closing TTY Log: var/lib/cowrie/tty/0a6eec7caf403e8eec9631e00ff1391cea011886f925bf0b8e79e5f731a5ba2d
 after 180 seconds
2023-11-15T11:10:36.716838Z [cowrie.ssh.connection.CowrieSSHConnection#info] sending close 0
2023-11-15T11:10:36.717064Z [HoneyPotSSHTransport,0,127.0.0.1] avatar bigmac logging out
2023-11-15T11:10:36.717126Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2023-11-15T11:10:36.717170Z [HoneyPotSSHTransport,0,127.0.0.1] Connection lost after 191 seconds
```



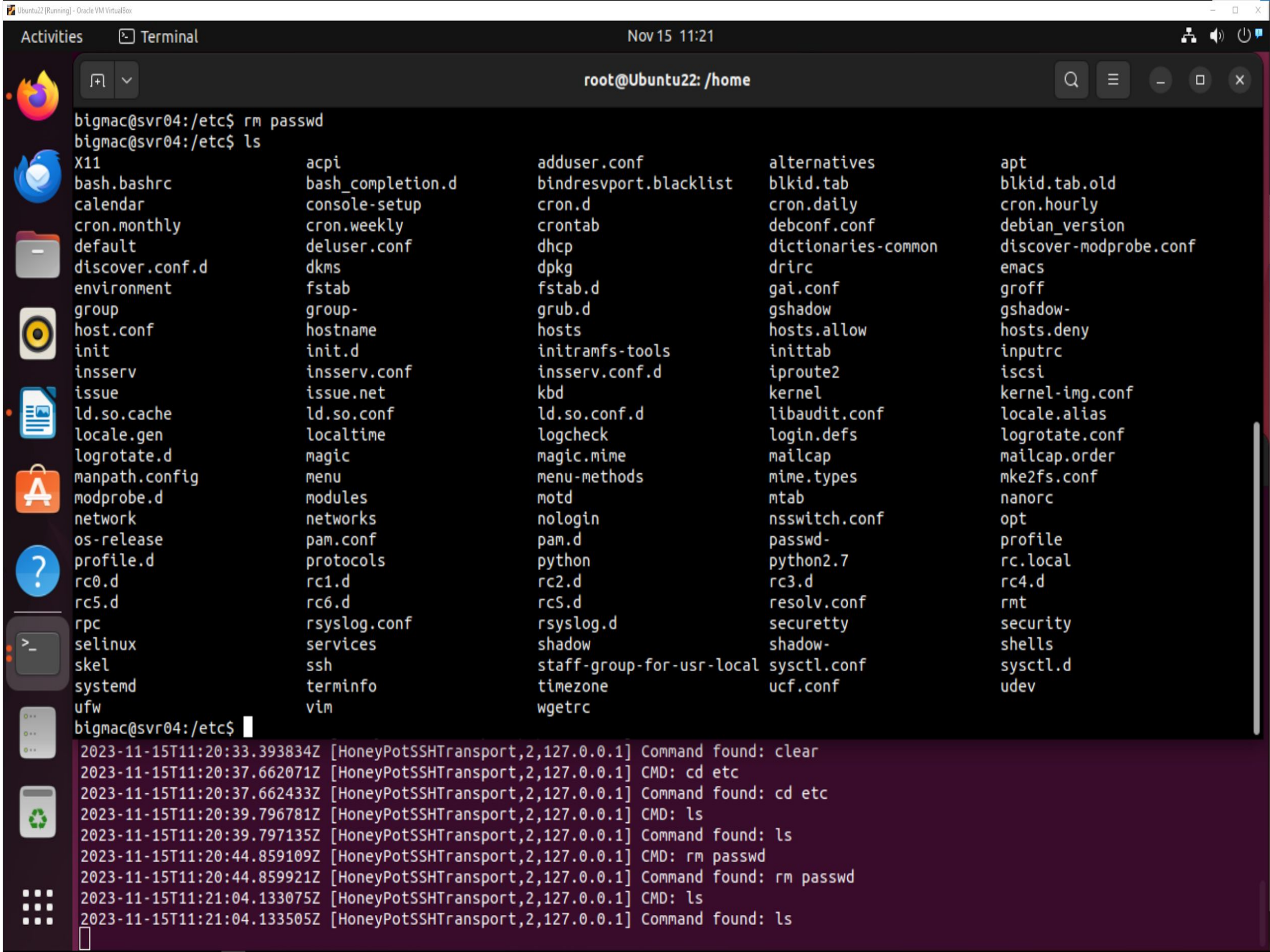
```
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
bigmac@svr04:~$ vi userdb.txt
E558: Terminal entry not found in terminfo
bigmac@svr04:~$ touch userdb.txt
bigmac@svr04:~$ ls
userdb.txt
bigmac@svr04:~$ cd ..
bigmac@svr04:/home$ ls
bigmac
bigmac@svr04:/home$ cd ..
bigmac@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
bigmac@svr04:/$
```

```
2023-11-15T11:11:25.339831Z [twisted.conch.ssh.session#info] Handling pty request: b'xterm-256color' (18, 132, 0, 0)
2023-11-15T11:11:25.340052Z [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,1,127.0.0.1] Terminal Si
ze: 132 18
2023-11-15T11:11:25.340852Z [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,1,127.0.0.1] request_env
: LANG=en_US.UTF-8
2023-11-15T11:11:25.341390Z [twisted.conch.ssh.session#info] Getting shell
2023-11-15T11:11:35.350589Z [HoneyPotSSHTransport,1,127.0.0.1] CMD: vi userdb.txt
2023-11-15T11:11:35.351236Z [HoneyPotSSHTransport,1,127.0.0.1] Command found: vi userdb.txt
2023-11-15T11:11:35.351442Z [HoneyPotSSHTransport,1,127.0.0.1] Reading txtcmd from "share/cowrie/txtcmds/usr/bin/vi"
2023-11-15T11:11:50.642628Z [HoneyPotSSHTransport,1,127.0.0.1] CMD: touch userdb.txt
2023-11-15T11:11:50.643202Z [HoneyPotSSHTransport,1,127.0.0.1] Command found: touch userdb.txt
2023-11-15T11:11:58.979297Z [HoneyPotSSHTransport,1,127.0.0.1] CMD: ls
2023-11-15T11:11:58.979721Z [HoneyPotSSHTransport,1,127.0.0.1] Command found: ls
2023-11-15T11:12:11.442755Z [HoneyPotSSHTransport,1,127.0.0.1] CMD: cd ..
2023-11-15T11:12:11.443188Z [HoneyPotSSHTransport,1,127.0.0.1] Command found: cd ..
2023-11-15T11:12:18.414021Z [HoneyPotSSHTransport,1,127.0.0.1] CMD: ls
2023-11-15T11:12:18.414678Z [HoneyPotSSHTransport,1,127.0.0.1] Command found: ls
2023-11-15T11:12:20.984344Z [HoneyPotSSHTransport,1,127.0.0.1] CMD: cd ..
2023-11-15T11:12:20.984762Z [HoneyPotSSHTransport,1,127.0.0.1] Command found: cd ..
2023-11-15T11:12:22.352596Z [HoneyPotSSHTransport,1,127.0.0.1] CMD: ls
2023-11-15T11:12:22.353012Z [HoneyPotSSHTransport,1,127.0.0.1] Command found: ls
```



```
bigmac@svr04:/$ cd etc
bigmac@svr04:/etc$ ls
X11                       acpi                      adduser.conf              alternatives              apt
bash.bashrc               bash_completion.d         bindresvport.blacklist    blkid.tab                 blkid.tab.old
calendar                  console-setup             cron.d                    cron.daily                cron.hourly
cron.monthly              cron.weekly               crontab                   debconf.conf              debian_version
default                   deluser.conf              dhcp                      dictionaries-common       discover-modprobe.conf
discover.conf.d           dkms                      dpkg                      drirc                     emacs
environment               fstab                     fstab.d                   gai.conf                  groff
group                     group-                    grub.d                    gshadow                   gshadow-
host.conf                 hostname                  hosts                     hosts.allow               hosts.deny
init                      init.d                    initramfs-tools           inittab                   inputrc
insserv                   insserv.conf              insserv.conf.d            iproute2                  iscsi
issue                     issue.net                 kbd                       kernel                    kernel-img.conf
ld.so.cache               ld.so.conf                ld.so.conf.d              libaudit.conf             locale.alias
locale.gen                localtime                 logcheck                  login.defs                logrotate.conf
logrotate.d               magic                     magic.mime                mailcap                   mailcap.order
manpath.config            menu                      menu-methods              mime.types                mke2fs.conf
modprobe.d                modules                   motd                      mtab                      nanorc
network                   networks                  nologin                   nsswitch.conf             opt
os-release                pam.conf                  pam.d                     passwd                    passwd-
profile                   profile.d                 protocols                 python                    python2.7
rc.local                  rc0.d                     rc1.d                     rc2.d                     rc3.d
rc4.d                     rc5.d                     rc6.d                     rcS.d                     resolv.conf
rmt                       rpc                       rsyslog.conf              rsyslog.d                 securetty
security                  selinux                   services                  shadow                    shadow-
shells                    skel                      ssh                       staff-group-for-usr-local sysctl.conf
sysctl.d                  systemd                   terminfo                  timezone                  ucf.conf
udev                      ufw                       vim                       wgetrc
bigmac@svr04:/etc$
```

~~~
2023-11-15T11:12:18.414678Z [HoneyPotSSHTransport,1,127.0.0.1] Command found: ls
2023-11-15T11:12:20.984344Z [HoneyPotSSHTransport,1,127.0.0.1] CMD: cd ..
2023-11-15T11:12:20.984762Z [HoneyPotSSHTransport,1,127.0.0.1] Command found: cd ..
2023-11-15T11:12:22.352596Z [HoneyPotSSHTransport,1,127.0.0.1] CMD: ls
2023-11-15T11:12:22.353012Z [HoneyPotSSHTransport,1,127.0.0.1] Command found: ls
2023-11-15T11:13:04.012774Z [HoneyPotSSHTransport,1,127.0.0.1] CMD: cd etc
2023-11-15T11:13:04.013547Z [HoneyPotSSHTransport,1,127.0.0.1] Command found: cd etc
2023-11-15T11:13:07.470488Z [HoneyPotSSHTransport,1,127.0.0.1] CMD: ls
2023-11-15T11:13:07.470902Z [HoneyPotSSHTransport,1,127.0.0.1] Command found: ls
```]]>
~~~

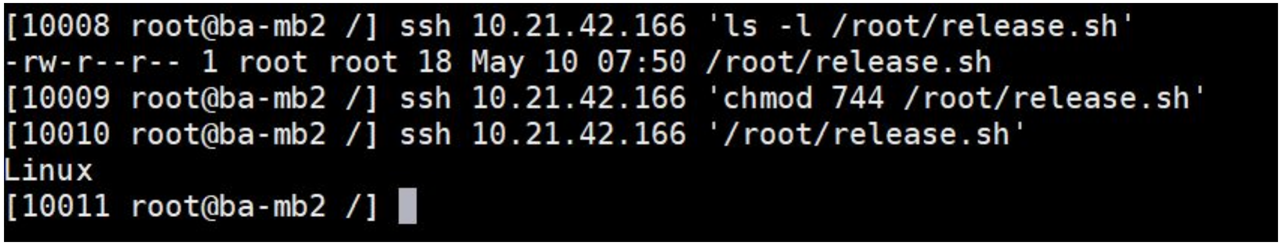


```
bigmac@svr04:/etc$ rm passwd
bigmac@svr04:/etc$ ls
X11                       acpi                      adduser.conf              alternatives              apt
bash.bashrc               bash_completion.d         bindresvport.blacklist    blkid.tab                 blkid.tab.old
calendar                  console-setup             cron.d                    cron.daily                cron.hourly
cron.monthly              cron.weekly               crontab                   debconf.conf              debian_version
default                   deluser.conf              dhcp                      dictionaries-common       discover-modprobe.conf
discover.conf.d           dkms                      dpkg                      drirc                     emacs
environment               fstab                     fstab.d                   gai.conf                  groff
group                     group-                    grub.d                    gshadow                   gshadow-
host.conf                 hostname                  hosts                     hosts.allow               hosts.deny
init                      init.d                    initramfs-tools           inittab                   inputrc
insserv                   insserv.conf              insserv.conf.d            iproute2                  iscsi
issue                     issue.net                 kbd                       kernel                    kernel-img.conf
ld.so.cache               ld.so.conf                ld.so.conf.d              libaudit.conf             locale.alias
locale.gen                localtime                 logcheck                  login.defs                logrotate.conf
logrotate.d               magic                     magic.mime                mailcap                   mailcap.order
manpath.config            menu                      menu-methods              mime.types                mke2fs.conf
modprobe.d                modules                   motd                      mtab                      nanorc
network                   networks                  nologin                   nsswitch.conf             opt
os-release                pam.conf                  pam.d                     passwd-                   profile
profile.d                 protocols                 python                    python2.7                 rc.local
rc0.d                     rc1.d                     rc2.d                     rc3.d                     rc4.d
rc5.d                     rc6.d                     rcS.d                     resolv.conf               rmt
rpc                       rsyslog.conf              rsyslog.d                 securetty                 security
selinux                   services                  shadow                    shadow-                   shells
skel                      ssh                       staff-group-for-usr-local sysctl.conf               sysctl.d
systemd                   terminfo                  timezone                  ucf.conf                  udev
ufw                       vim                       wgetrc
bigmac@svr04:/etc$
```

```
2023-11-15T11:20:33.393834Z [HoneyPotSSHTransport,2,127.0.0.1] Command found: clear
2023-11-15T11:20:37.662071Z [HoneyPotSSHTransport,2,127.0.0.1] CMD: cd etc
2023-11-15T11:20:37.662433Z [HoneyPotSSHTransport,2,127.0.0.1] Command found: cd etc
2023-11-15T11:20:39.796781Z [HoneyPotSSHTransport,2,127.0.0.1] CMD: ls
2023-11-15T11:20:39.797135Z [HoneyPotSSHTransport,2,127.0.0.1] Command found: ls
2023-11-15T11:20:44.859109Z [HoneyPotSSHTransport,2,127.0.0.1] CMD: rm passwd
2023-11-15T11:20:44.859921Z [HoneyPotSSHTransport,2,127.0.0.1] Command found: rm passwd
2023-11-15T11:21:04.133075Z [HoneyPotSSHTransport,2,127.0.0.1] CMD: ls
2023-11-15T11:21:04.133505Z [HoneyPotSSHTransport,2,127.0.0.1] Command found: ls
```

Additionally…

- Cowrie supports SFTP and SCP for file upload
- Supports SSH exec commands:



```
[10008 root@ba-mb2 /] ssh 10.21.42.166 'ls -l /root/release.sh'
-rw-r--r-- 1 root root 18 May 10 07:50 /root/release.sh
[10009 root@ba-mb2 /] ssh 10.21.42.166 'chmod 744 /root/release.sh'
[10010 root@ba-mb2 /] ssh 10.21.42.166 '/root/release.sh'
Linux
[10011 root@ba-mb2 /] █
```

- Forward SMTP connections to SMTP 'Spam Trap'
  (e.g. mailoney)
- JSON logging for easy processing in log management solutions

Honeypot -> Pineapple

- Malicious agents use honeypots too
- Create a ‘wi-fi pineapple’: fake wi-fi network to mimic a real one
  - Easily monitor / log traffic and user data
  - Ethical questionability (I’d use it on my kids)
  - Good for penetration testing (identify vulnerabilities in a network)

Issues

- Unable to enable log sorting and display
- Contact ISP due to conflicting terms of use
- Difficulties transferring to Raspberry Pi
- Enabling SSH hardening / SSH key setup

Conclusion

- Honeypots are a great way to monitor malicious activity
- Cost-effective, real data collection with few false positives
- Capture malicious activity, even if an attacker is using encryption
- Does not replace a standard IDS
- Zero attempts to access the honeypot means no data to analyze
- Can be resource extensive to setup properly