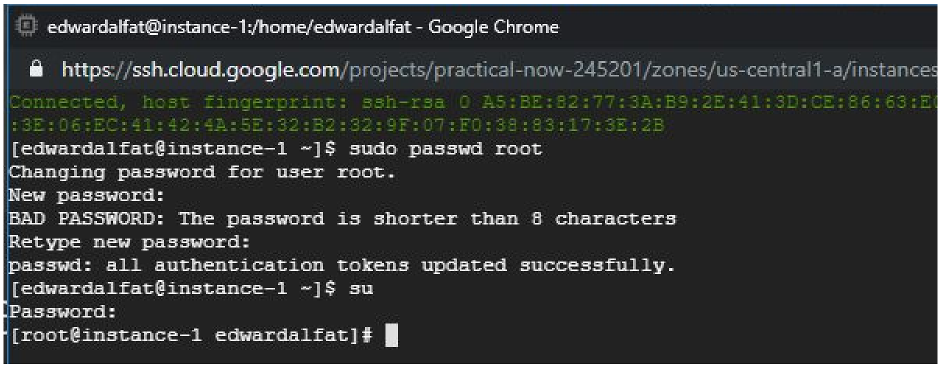
Honeypot - SSH Honeypot dengan cowrie

Apa itu honeypot?
Honeypot adalah security resource/sebuah sistem yang yang sengaja dibuat untuk menjadi target serangan hacker. Tujuannya untuk melihat pola, teknik dan aktifitas serangannya.

1. Persiapan

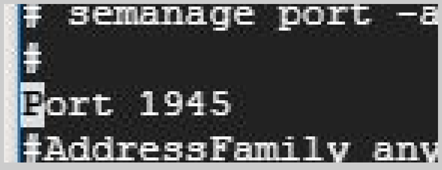
1. **Buat + beri password user root**
   sudo passwd root
   su (masuk ke root)


edwardalfat@instance-1:/home/edwardalfat - Google Chrome
https://ssh.cloud.google.com/projects/practical-now-245201/zones/us-central1-a/instances

```
Connected, host fingerprint: ssh-rsa 0 A5:BE:82:77:3A:B9:2E:41:3D:CE:86:63:E
:3E:06:EC:41:42:4A:5E:32:B2:32:9F:07:F0:38:83:17:3E:2B
[edwardalfat@instance-1 ~]$ sudo passwd root
Changing password for user root.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[edwardalfat@instance-1 ~]$ su
Password:
[root@instance-1 edwardalfat]#
```

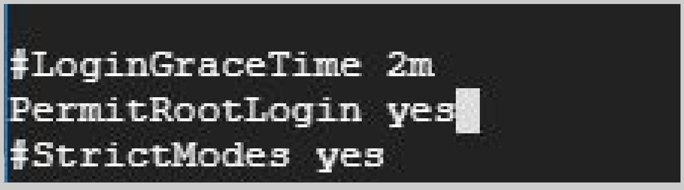
2. **Edit konfigurasi ssh memperbolehkan user root + password authentication**
   nano /etc/ssh/sshd_config

   Ubah port default ssh. Kali ini saya ganti ke **1945**



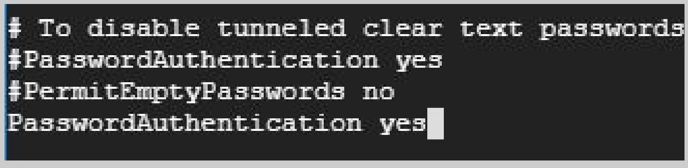
```
# semanage port -a
#
Port 1945
#AddressFamily any
```

PermitRootLogin ubah menjadi **yes**



```
#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
```

PasswordAuthentication ubah menjadi **yes**



```
# To disable tunneled clear text passwords
#PasswordAuthentication yes
#PermitEmptyPasswords no
PasswordAuthentication yes
```

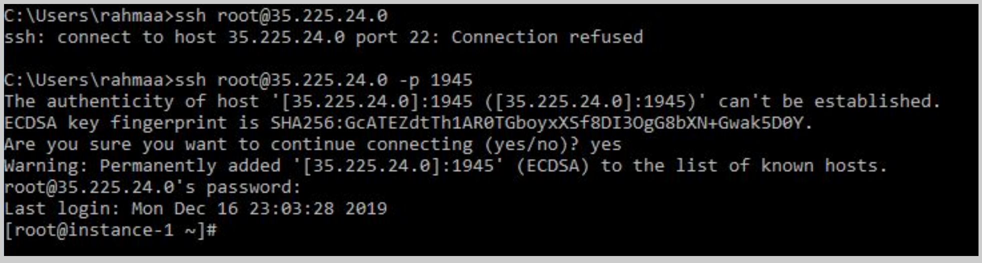
3. **Setelah konfigurasi tersimpan, ketikkan perintah berikut**
   semanage port -a -t ssh_port_t -p tcp 1945

4. **Menambah rule firewall**
   firewall-cmd --add-port 1945/tcp --permanent
   firewall-cmd --reload

5. **Restart service ssh**
   service sshd restart

6. **Selanjutnya kita testing remote SSH di client (Windows). Buka CMD/Putty > remote centos server.**
   ssh root@ipcentos (testing remote dengan default port 22 - harusnya tidak bisa → connection refused)

   ssh root@ipcentos -p 1945 (harusnya bisa)

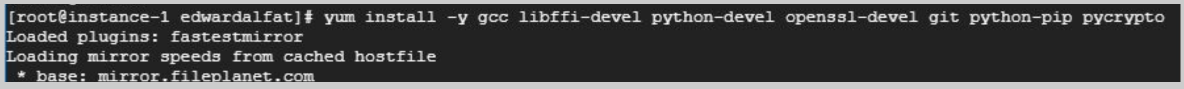


```
C:\Users\rahmaa>ssh root@35.225.24.0
ssh: connect to host 35.225.24.0 port 22: Connection refused

C:\Users\rahmaa>ssh root@35.225.24.0 -p 1945
The authenticity of host '[35.225.24.0]:1945 ([35.225.24.0]:1945)' can't be established.
ECDSA key fingerprint is SHA256:GcATEZdtTh1AR0TGboyxXSf8DI3OgG8bXN+Gwak5D0Y.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[35.225.24.0]:1945' (ECDSA) to the list of known hosts.
root@35.225.24.0's password:
Last login: Mon Dec 16 23:03:28 2019
[root@instance-1 ~]#
```

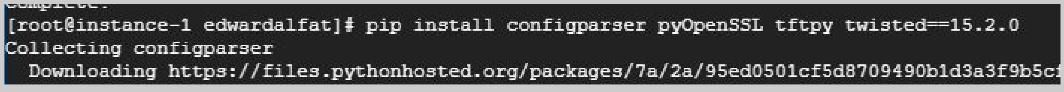
7. **Update repo**
   yum install -y epel-release

8. **Install beberapa package centos + python package**
   yum install -y gcc libffi-devel python-devel openssl-devel git python-pip pycrypto



```
[root@instance-1 edwardalfat]# yum install -y gcc libffi-devel python-devel openssl-devel git python-pip pycrypto
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirror.fileplanet.com
```

pip install configparser pyOpenSSL tftpy twisted==15.2.0



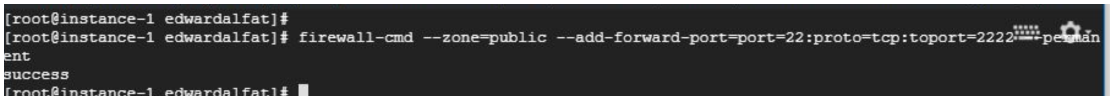
```
Complete.
[root@instance-1 edwardalfat]# pip install configparser pyOpenSSL tftpy twisted==15.2.0
Collecting configparser
  Downloading https://files.pythonhosted.org/packages/7a/2a/95ed0501cf5d8709490b1d3a3f9b5c
```

2. Setup cowrie honeypot

1. Menambah rule firewall

   firewall-cmd --add-port 2222/tcp --permanent

   firewall-cmd --reload

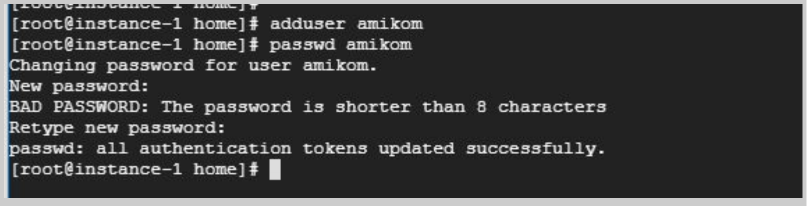


```
[root@instance-1 edwardalfat]#
[root@instance-1 edwardalfat]# firewall-cmd --zone=public --add-forward-port=port=22:proto=tcp:toport=2222 --perman
ent
success
[root@instance-1 edwardalfat]#
```

2. Membuat user ‘amikom’ + set password

   adduser amikom

   passwd amikom



```
[root@instance-1 home]#
[root@instance-1 home]# adduser amikom
[root@instance-1 home]# passwd amikom
Changing password for user amikom.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@instance-1 home]#
```

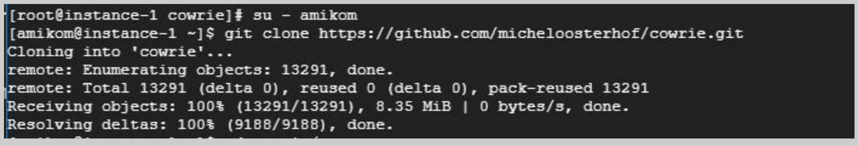
3. Menambah akses sudo user amikom

   usermod -aG wheel amikom

4. Masuk ke user amikom + download cowrie

   su - amikom

   git clone https://github.com/micheloosterhof/cowrie.git

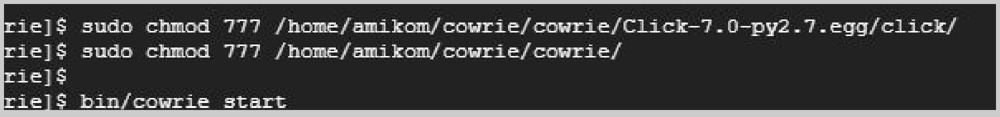


```
[root@instance-1 cowrie]# su - amikom
[amikom@instance-1 ~]$ git clone https://github.com/micheloosterhof/cowrie.git
Cloning into 'cowrie'...
remote: Enumerating objects: 13291, done.
remote: Total 13291 (delta 0), reused 0 (delta 0), pack-reused 13291
Receiving objects: 100% (13291/13291), 8.35 MiB | 0 bytes/s, done.
Resolving deltas: 100% (9188/9188), done.
```

5. Memberi hak akses penuh direktori cowrie

   sudo chmod 777 /home/amikom/cowrie/cowrie/Click-7.0-py2.7.egg/click/

   sudo chmod 777 /home/amikom/cowrie/cowrie/



```
rie]$ sudo chmod 777 /home/amikom/cowrie/cowrie/Click-7.0-py2.7.egg/click/
rie]$ sudo chmod 777 /home/amikom/cowrie/cowrie/
rie]$
rie]$ bin/cowrie start
```

6. Install virtualenv + install beberapa package tambahan

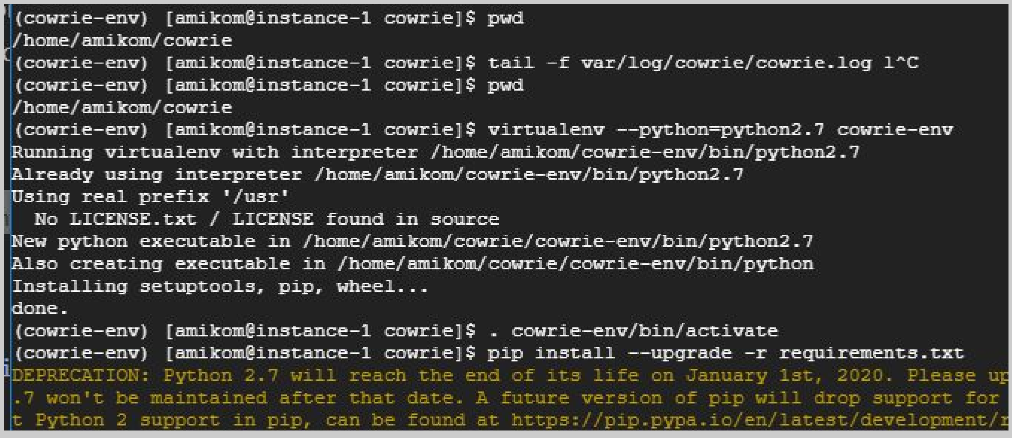
   cd cowrie

   sudo pip install virtualenv

   virtualenv --python=python2.7 cowrie-env

   . cowrie-env/bin/activate

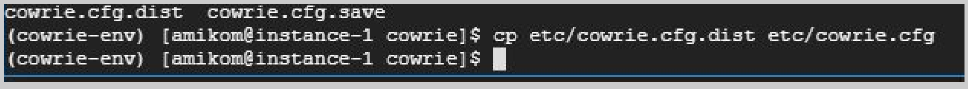
   pip install --upgrade -r requirements.txt



```
(cowrie-env) [amikom@instance-1 cowrie]$ pwd
/home/amikom/cowrie
(cowrie-env) [amikom@instance-1 cowrie]$ tail -f var/log/cowrie/cowrie.log 1^C
(cowrie-env) [amikom@instance-1 cowrie]$ pwd
/home/amikom/cowrie
(cowrie-env) [amikom@instance-1 cowrie]$ virtualenv --python=python2.7 cowrie-env
Running virtualenv with interpreter /home/amikom/cowrie-env/bin/python2.7
Already using interpreter /home/amikom/cowrie-env/bin/python2.7
Using real prefix '/usr'
  No LICENSE.txt / LICENSE found in source
New python executable in /home/amikom/cowrie/cowrie-env/bin/python2.7
Also creating executable in /home/amikom/cowrie/cowrie-env/bin/python
Installing setuptools, pip, wheel...
done.
(cowrie-env) [amikom@instance-1 cowrie]$ . cowrie-env/bin/activate
(cowrie-env) [amikom@instance-1 cowrie]$ pip install --upgrade -r requirements.txt
DEPRECATION: Python 2.7 will reach the end of its life on January 1st, 2020. Please up
.7 won't be maintained after that date. A future version of pip will drop support for
t Python 2 support in pip, can be found at https://pip.pypa.io/en/latest/development/r
```

7. Copy + rename default konfigurasi cowrie

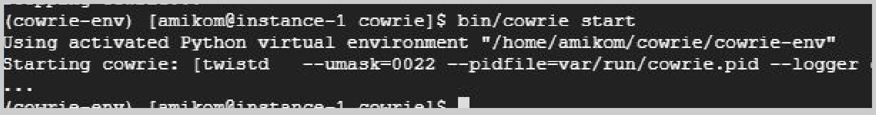
   cp etc/cowrie.cfg.dist etc/cowrie.cfg



```
cowrie.cfg.dist  cowrie.cfg.save
(cowrie-env) [amikom@instance-1 cowrie]$ cp etc/cowrie.cfg.dist etc/cowrie.cfg
(cowrie-env) [amikom@instance-1 cowrie]$ 
```

8. Untuk menjalankan honeypot cowrie

   bin/cowrie start



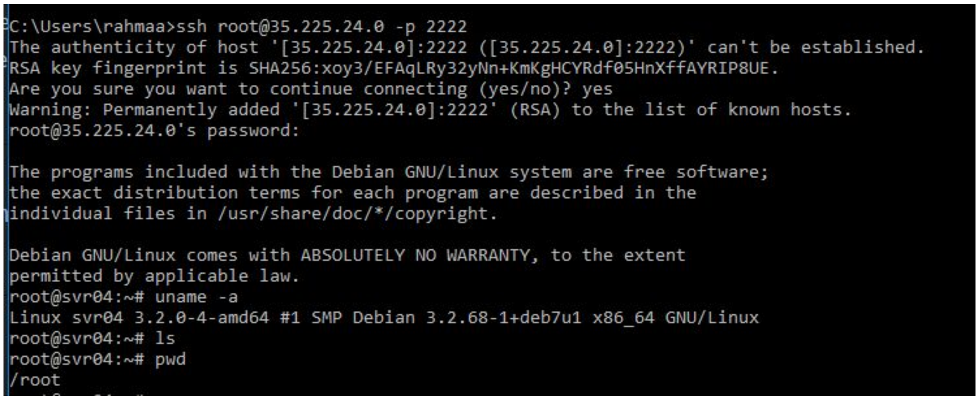
```
(cowrie-env) [amikom@instance-1 cowrie]$ bin/cowrie start
Using activated Python virtual environment "/home/amikom/cowrie/cowrie-env"
Starting cowrie: [twistd   --umask=0022 --pidfile=var/run/cowrie.pid --logger 
...
(cowrie-env) [amikom@instance-1 cowrie]$ 
```

3. Testing & Melihat Log Serangan

1. Karena traffik port 22 belum saya bikin rule untuk dibelokkan ke port 2222. Testing koneksi ssh tetap perlu menambahkan opsi -p 2222

   ```
   ssh root@ipcentos -p 2222
   ```

   Maka akan masuk ke shell/terminal tipuan honeypot

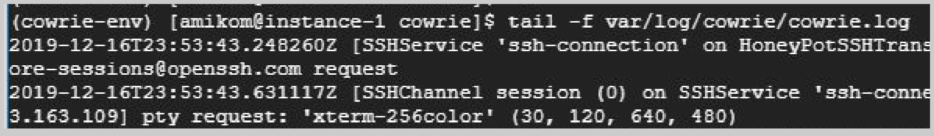
   ```
   C:\Users\rahmaa>ssh root@35.225.24.0 -p 2222
   The authenticity of host '[35.225.24.0]:2222 ([35.225.24.0]:2222)' can't be established.
   RSA key fingerprint is SHA256:xoy3/EFAqLRy32yNn+KmKgHCYRdf05HnXffAYRIP8UE.
   Are you sure you want to continue connecting (yes/no)? yes
   Warning: Permanently added '[35.225.24.0]:2222' (RSA) to the list of known hosts.
   root@35.225.24.0'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:~# uname -a
   Linux svr04 3.2.0-4-amd64 #1 SMP Debian 3.2.68-1+deb7u1 x86_64 GNU/Linux
   root@svr04:~# ls
   root@svr04:~# pwd
   /root
   ```

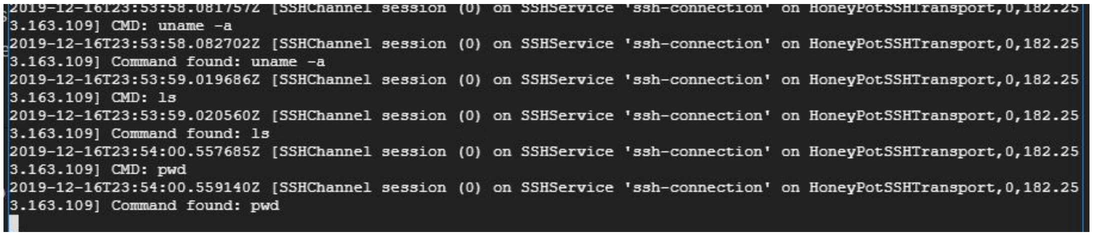
2. Untuk melihat log serangan honeypot

   ```
   tail -f var/log/cowrie/cowrie.log
   ```

   ```
   (cowrie-env) [amikom@instance-1 cowrie]$ tail -f var/log/cowrie/cowrie.log
   2019-12-16T23:53:43.248260Z [SSHService 'ssh-connection' on HoneyPotSSHTrans
   ore-sessions@openssh.com request
   2019-12-16T23:53:43.631117Z [SSHChannel session (0) on SSHService 'ssh-conne
   3.163.109] pty request: 'xterm-256color' (30, 120, 640, 480)
   ```

3. Log serangan :

   ```
   2019-12-16T23:53:58.081757Z [SSHChannel session (0) on SSHService 'ssh-connection' on HoneyPotSSHTransport,0,182.25
   3.163.109] CMD: uname -a
   2019-12-16T23:53:58.082702Z [SSHChannel session (0) on SSHService 'ssh-connection' on HoneyPotSSHTransport,0,182.25
   3.163.109] Command found: uname -a
   2019-12-16T23:53:59.019686Z [SSHChannel session (0) on SSHService 'ssh-connection' on HoneyPotSSHTransport,0,182.25
   3.163.109] CMD: ls
   2019-12-16T23:53:59.020560Z [SSHChannel session (0) on SSHService 'ssh-connection' on HoneyPotSSHTransport,0,182.25
   3.163.109] Command found: ls
   2019-12-16T23:54:00.557685Z [SSHChannel session (0) on SSHService 'ssh-connection' on HoneyPotSSHTransport,0,182.25
   3.163.109] CMD: pwd
   2019-12-16T23:54:00.559140Z [SSHChannel session (0) on SSHService 'ssh-connection' on HoneyPotSSHTransport,0,182.25
   3.163.109] Command found: pwd
   ```

4. Agar honeypot ssh ini beneran terlihat real. Belokkan traffik default port ssh/22 ke port cowrie

   ```
   firewall-cmd --add-masquerade --permanent

   firewall-cmd --add-forward-port=port=22:proto=tcp:toport=2222
   --permanent
   ```

```
firewall-cmd --reload
```