V CONGRESO
SMART GRIDS
Madrid, 13 Diciembre 2018

SecureGrid

EL HACKING ÉTICO APLICADO A LA MEJORA DE LA SEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS DE LA RED ELÉCTRICA

Santiago De Diego, Iñaki Angulo

Investigador, Gestor de Proyectos

TECNALIA

SecureGrid

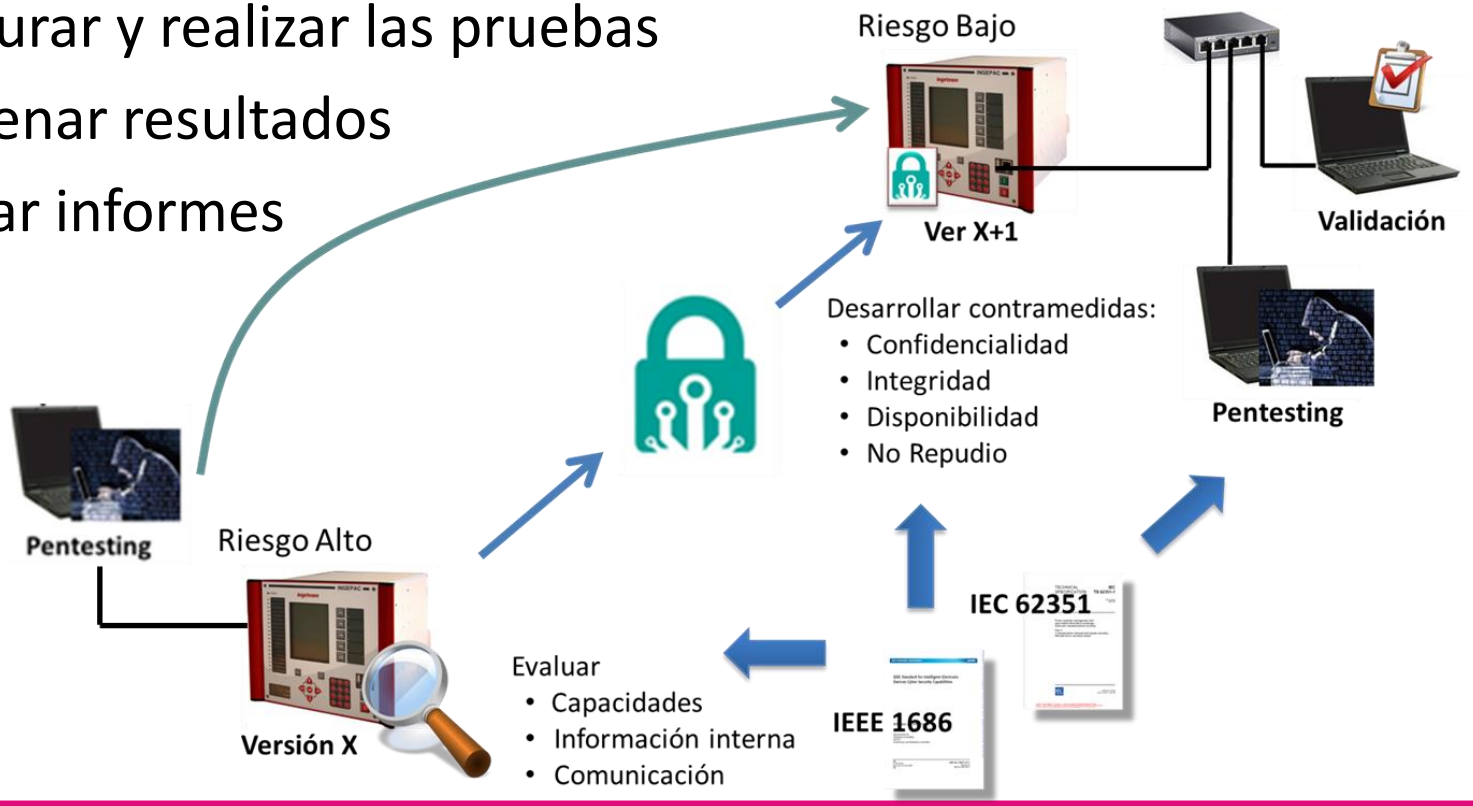
- Proyecto HAZITEK Estratégico (2016-2018)
- Presupuesto: ~ 4M€
- Desarrollar nueva tecnología que permita aumentar la seguridad de los IEDs en las instalaciones eléctricas.

ZIV arteche Ingeteam ORMAZABAL velatia

GE its LINKED TO Egile Cluster Energía BASQUE ENERGY CLUSTER tecnalia Inspiring Business

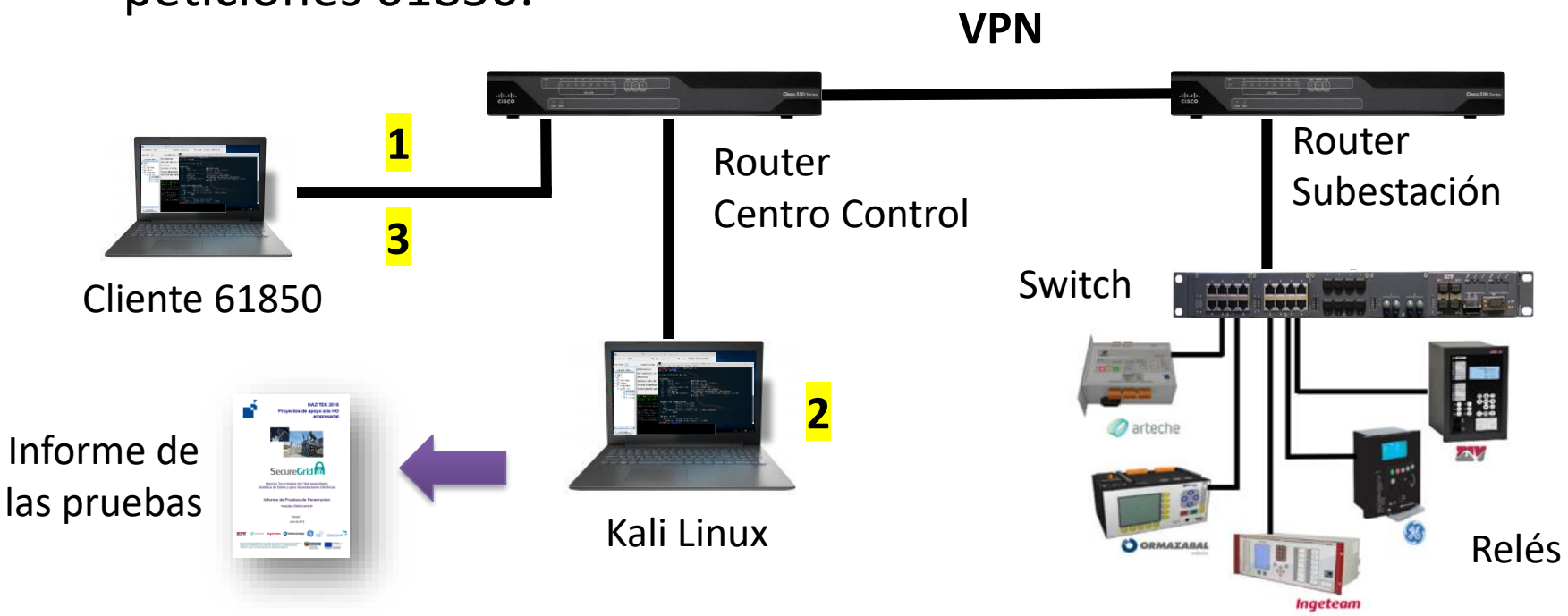
PENTESTING, ¿PARA QUÉ?

- Permite descubrir las vulnerabilidades utilizando herramientas propias de los hackers:
  - Configurar y realizar las pruebas
  - Almacenar resultados
  - Generar informes



EJEMPLO DOS

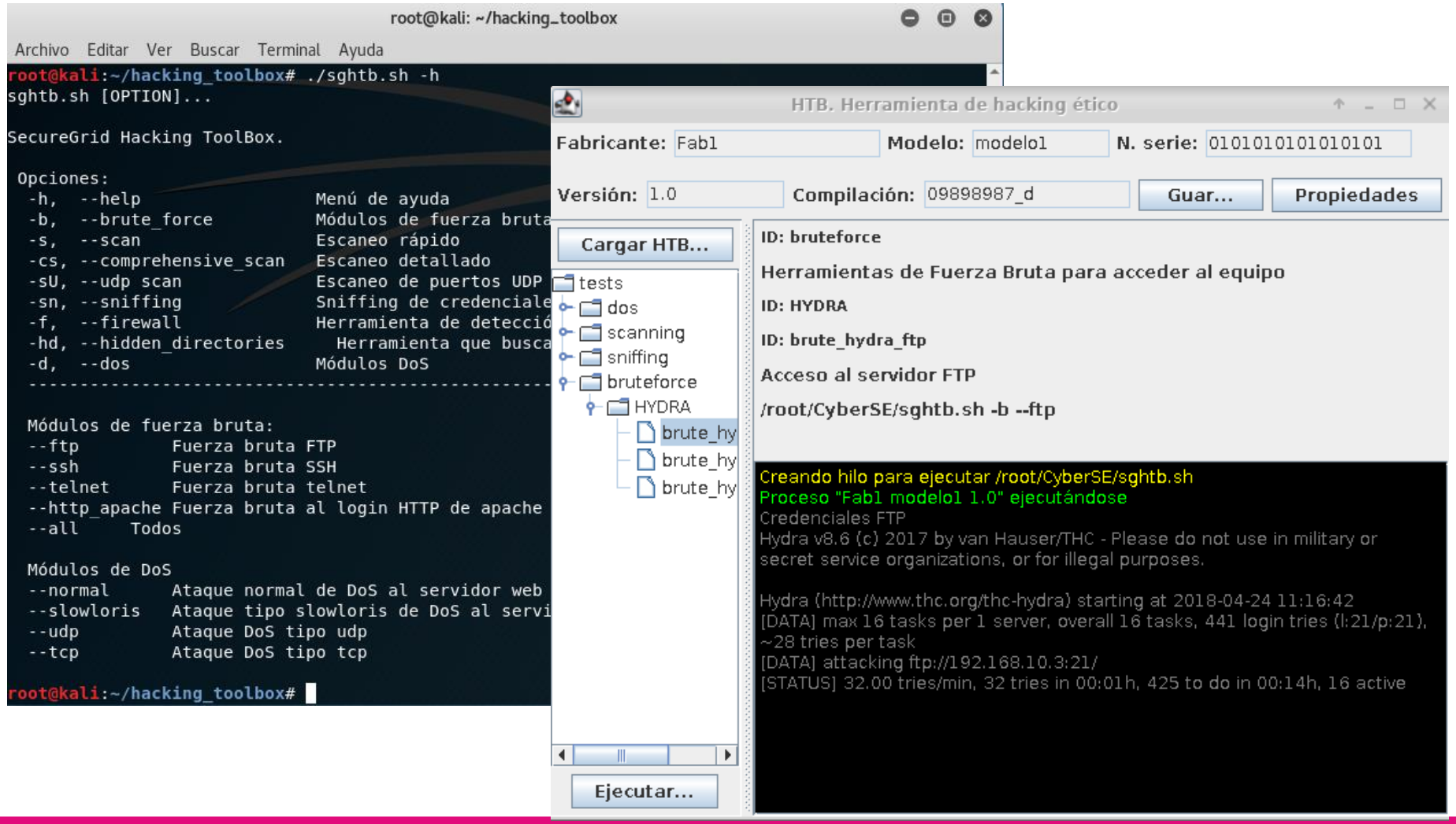
1. Lanzamos el cliente 61850
2. Lanzamos el ataque DoS
3. Comprobamos hasta cuando el equipo responde a las peticiones 61850.



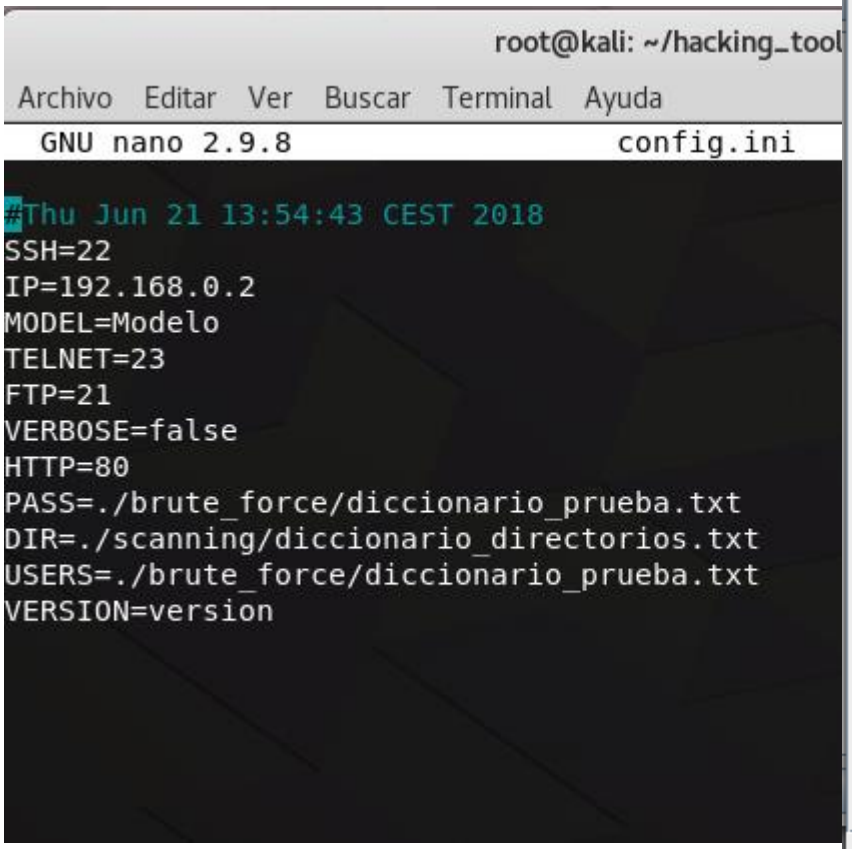
QUÉ PODEMOS DESCUBRIR

- Información de puertos y servicios
- Credenciales de acceso al dispositivo
- Resistencia ante diferentes ataques de denegación de servicio
- Si emplea protocolos seguros para su gestión
- Existencia de directorios web expuestos
- Existencia de un firewall de aplicación web
- Otros ataques ….

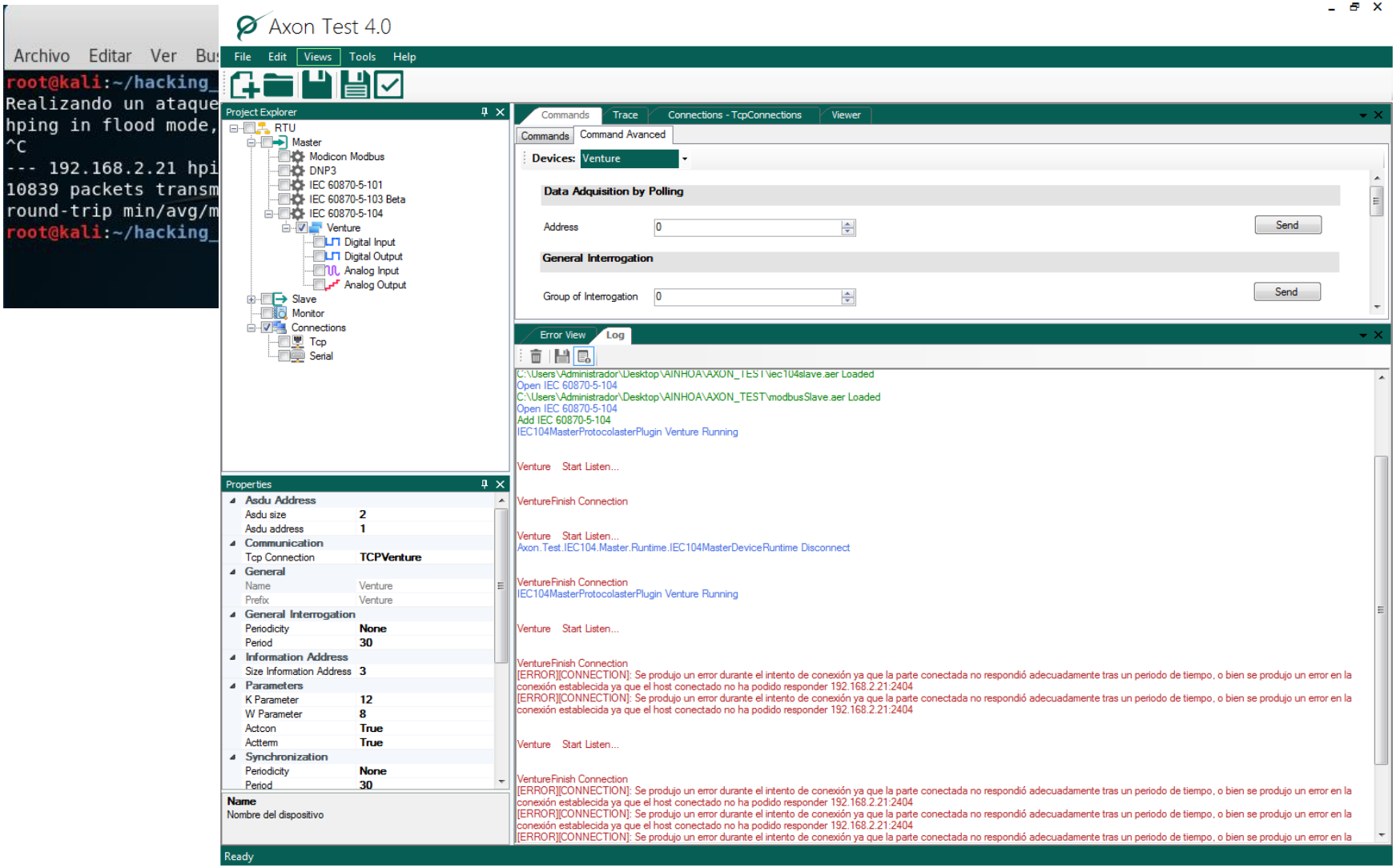
¿CÓMO FUNCIONA?



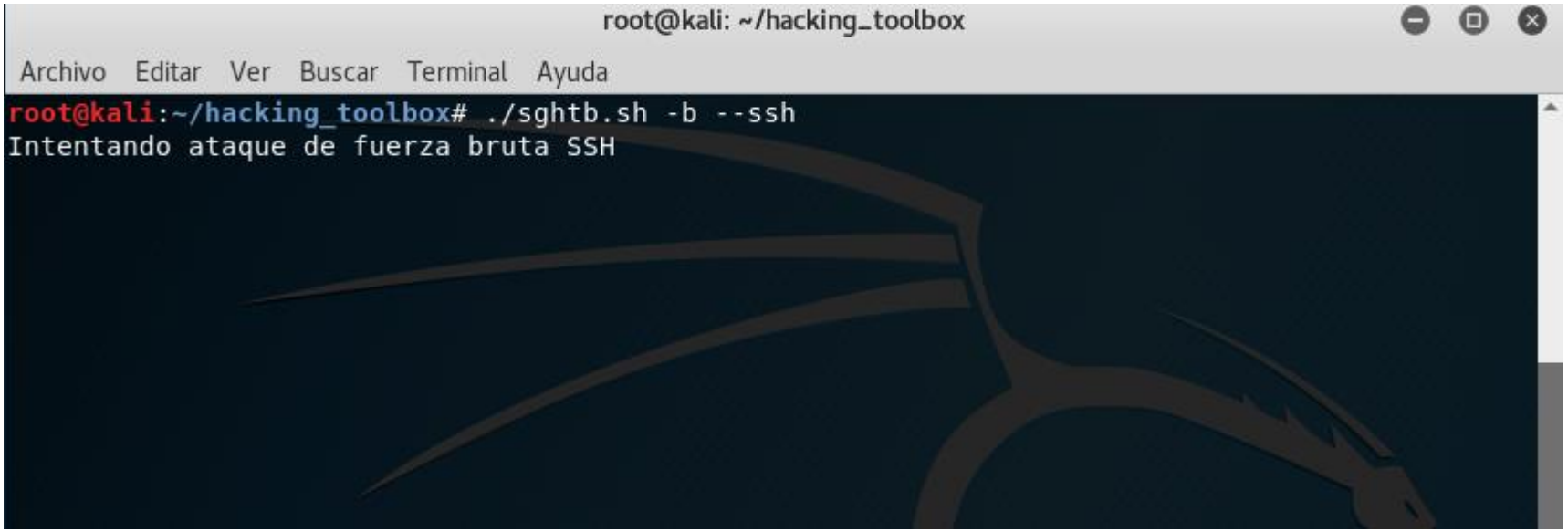
CONFIGURACIÓN



EJEMPLO DOS


Archivo Editar Ver Bus
root@kali:~/hacking_
Realizando un ataque
hping in flood mode,
^C
--- 192.168.2.21 hpi
10839 packets transm
round-trip min/avg/m
root@kali:~/hacking_
Axon Test 4.0
File Edit Views Tools Help
Project Explorer
RTU
Master
Modicon Modbus
DNP3
IEC 60870-5-101
IEC 60870-5-103 Beta
IEC 60870-5-104
Venture
Digital Input
Digital Output
Analog Input
Analog Output
Slave
Monitor
Connections
Tcp
Serial
Properties
Asdu Address
Asdu size 2
Asdu address 1
Communication
Tcp Connection TCPVenture
General
Name Venture
Prefix Venture
General Interrogation
Periodicity None
Period 30
Information Address
Size Information Address 3
Parameters
K Parameter 12
W Parameter 8
Actcon True
Actterm True
Synchronization
Periodicity None
Period 30
Name
Nombre del dispositivo
Commands
Trace
Connections - TcpConnections
Viewer
Commands
Command Avanced
Devices: Venture
Data Adquisition by Polling
Address 0
Send
General Interrogation
Group of Interrogation 0
Send
Error View
Log
C:\Users\Administrador\Desktop\AINHOA\AXON_TEST\iec104slave.aer Loaded
Open IEC 60870-5-104
C:\Users\Administrador\Desktop\AINHOA\AXON_TEST\modbusSlave.aer Loaded
Open IEC 60870-5-104
Add IEC 60870-5-104
IEC104MasterProtocolasterPlugin Venture Running
Venture Start Listen...
VentureFinish Connection
Venture Start Listen...
Axon.Test.IEC104.Master.Runtime.IEC104MasterDeviceRuntime Disconnect
VentureFinish Connection
IEC104MasterProtocolasterPlugin Venture Running
Venture Start Listen...
VentureFinish Connection
[ERROR][CONNECTION]: Se produjo un error durante el intento de conexión ya que la parte conectada no respondió adecuadamente tras un periodo de tiempo, o bien se produjo un error en la conexión establecida ya que el host conectado no ha podido responder 192.168.2.21:2404
[ERROR][CONNECTION]: Se produjo un error durante el intento de conexión ya que la parte conectada no respondió adecuadamente tras un periodo de tiempo, o bien se produjo un error en la conexión establecida ya que el host conectado no ha podido responder 192.168.2.21:2404
Venture Start Listen...
VentureFinish Connection
[ERROR][CONNECTION]: Se produjo un error durante el intento de conexión ya que la parte conectada no respondió adecuadamente tras un periodo de tiempo, o bien se produjo un error en la conexión establecida ya que el host conectado no ha podido responder 192.168.2.21:2404
[ERROR][CONNECTION]: Se produjo un error durante el intento de conexión ya que la parte conectada no respondió adecuadamente tras un periodo de tiempo, o bien se produjo un error en la conexión establecida ya que el host conectado no ha podido responder 192.168.2.21:2404
[ERROR][CONNECTION]: Se produjo un error durante el intento de conexión ya que la parte conectada no respondió adecuadamente tras un periodo de tiempo, o bien se produjo un error en la
Ready

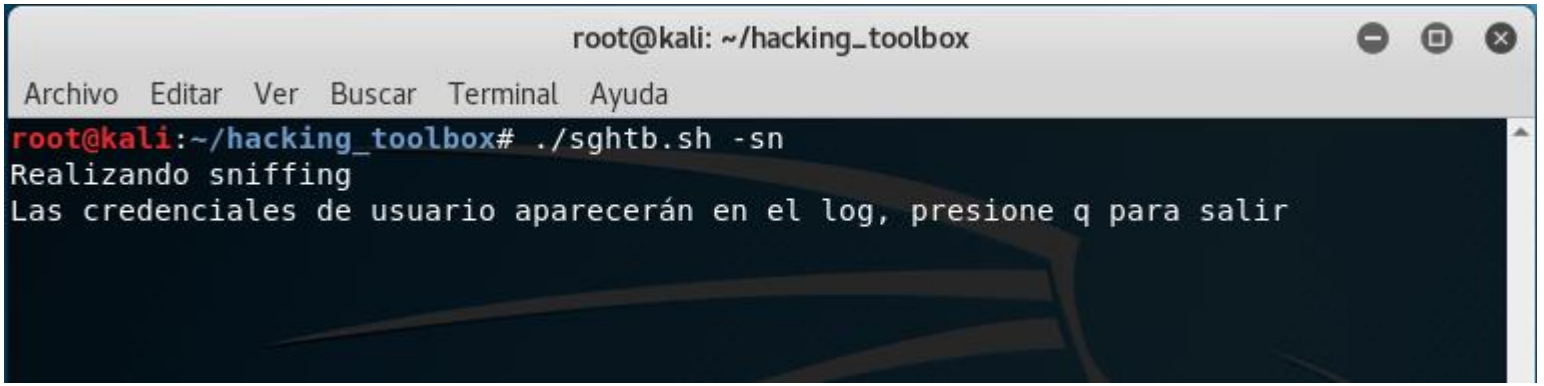
EJEMPLO FUERZA BRUTA

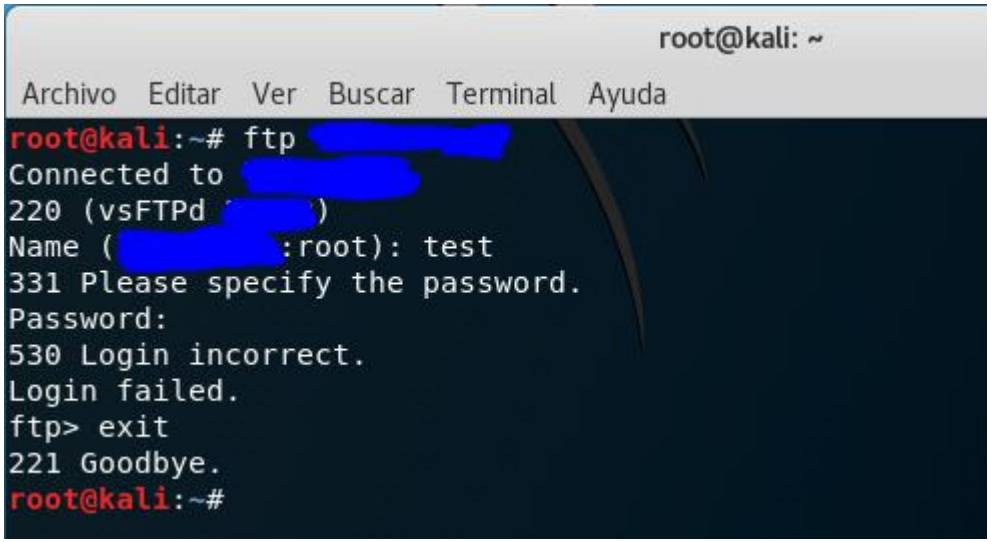


Comprobando el log que genera la herramienta:

```
[DATA] max 5 tasks per 1 server, overall 5 tasks, 484 login tries (l:22/p:0), ~22 tries per task
[DATA] attacking ssh://[redacted]:22/
[22][ssh] host: [redacted]   login: [redacted]   password: [redacted]
[STATUS] 173.00 tries/min, 173 tries in 00:00h, 0 to do in 01:00h, 311 active
[STATUS] 156.33 tries/min, 469 tries in 00:00h, 0 to do in 03:00h, 15 active
1 of 1 target successfully completed, 1 valid password found
```

CAPTURA DE CREDENCIALES



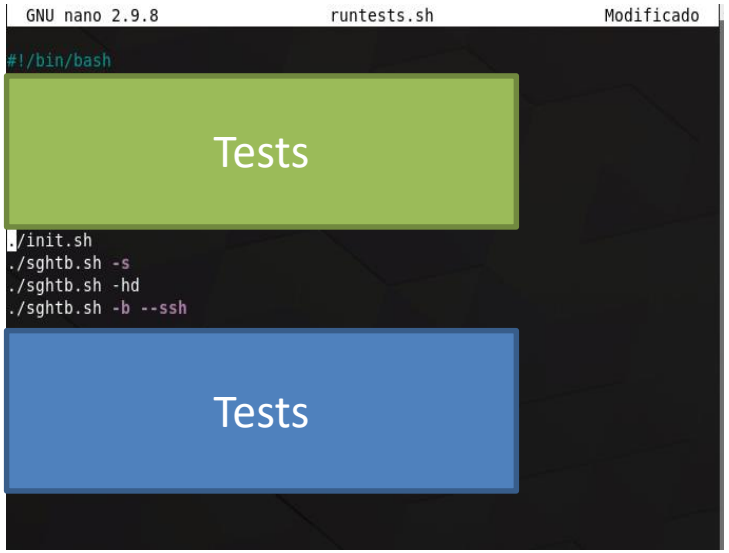


http: ***.***.***.*** -> USER: **** PASS: *****

CONCLUSIONES

- Utilización de este tipo de herramientas dentro del propio proceso de desarrollo
- Incorporar una métrica del grado de seguridad

Hacking Tool



V CONGRESO
SMART GRIDS
Madrid, 13 Diciembre 2018

DATOS DE CONTACTO:

santiago.dediego@tecnalia.com

inaki.angulo@tecnalia.com

SecureGrid

tecnalia Inspiring Business