



V CONGRESO
SMART GRIDS

Madrid, 13 Diciembre 2018



**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

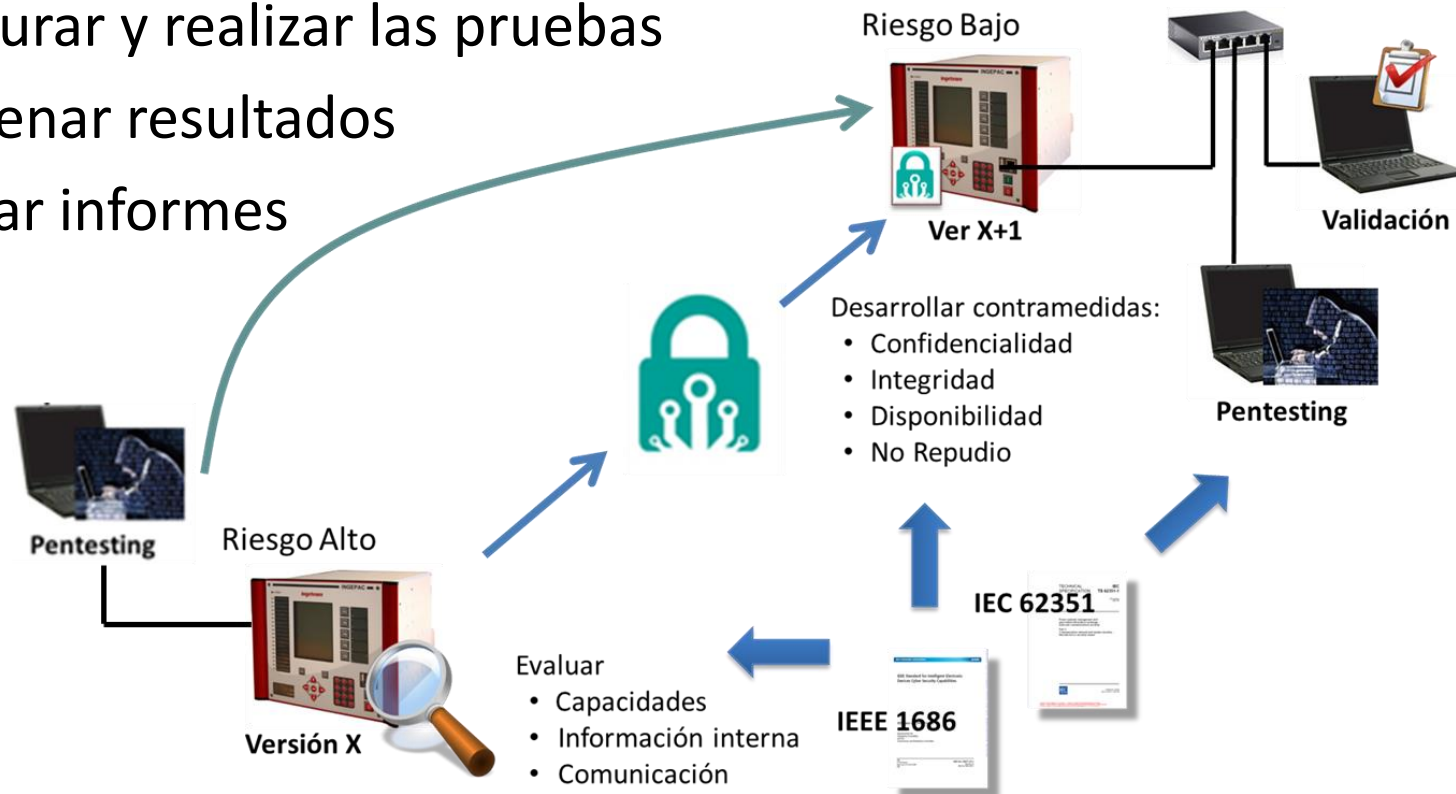
SecureGrid

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



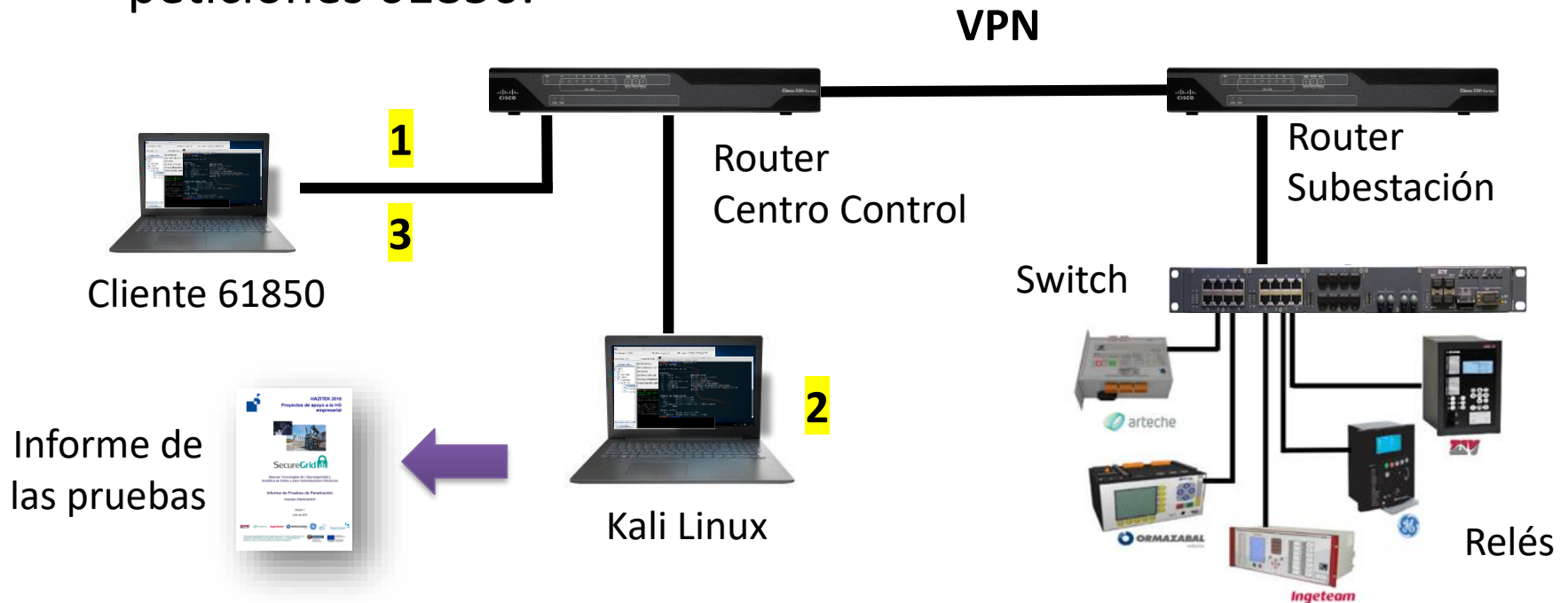
PENTESTING, ¿PARA QUÉ?

- 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?

The image shows a Kali Linux terminal window and the HTB (Herramienta de hacking ético) GUI. The terminal window displays the output of the command `./sghtb.sh -h`, showing various options and modules. The HTB GUI is a graphical interface for running the tool, with fields for manufacturer, model, and serial number, and buttons for loading and executing HTB files. A file browser shows the directory structure, with `brute_hy` selected. A terminal window within the GUI shows the execution of `/root/CyberSE/sghtb.sh -b --ftp`, displaying the output of the Hydra tool.

```
root@kali: ~/hacking_toolbox
Archivo Editar Ver Buscar Terminal Ayuda
root@kali:~/hacking_toolbox# ./sghtb.sh -h
sghtb.sh [OPTION]...

SecureGrid Hacking ToolBox.

Opciones:
-h, --help           Menú de ayuda
-b, --brute_force   Módulos de fuerza bruta
-s, --scan          Escaneo rápido
-cs, --comprehensive_scan Escaneo detallado
-sU, --udp_scan     Escaneo de puertos UDP
-sn, --sniffing     Sniffing de credenciales
-f, --firewall      Herramienta de detección
-hd, --hidden_directories Herramienta que busca
-d, --dos           Módulos DoS

-----

Módulos de fuerza bruta:
--ftp      Fuerza bruta FTP
--ssh      Fuerza bruta SSH
--telnet   Fuerza bruta telnet
--http_apache Fuerza bruta al login HTTP de apache
--all      Todos

Módulos de DoS
--normal   Ataque normal de DoS al servidor web
--slowloris Ataque tipo slowloris de DoS al servi
--udp      Ataque DoS tipo udp
--tcp      Ataque DoS tipo tcp

root@kali:~/hacking_toolbox#
```

HTB. Herramienta de hacking ético

Fabricante: Fab1 Modelo: modelo1 N. serie: 0101010101010101

Versión: 1.0 Compilación: 09898987_d Guar... Propiedades

Cargar HTB...

tests

- dos
- scanning
- sniffing
- bruteforce
 - HYDRA
 - brute_hy
 - brute_hy
 - brute_hy

CONFIGURACIÓN

```
root@kali: ~/hacking_tool
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.9.8 config.ini
Thu Jun 21 13:54:43 CEST 2018
SSH=22
IP=192.168.0.2
MODEL=Modelo
TELNET=23
FTP=21
VERBOSE=false
HTTP=80
PASS=./brute_force/diccionario_prueba.txt
DIR=./scanning/diccionario_directorios.txt
USERS=./brute_force/diccionario_prueba.txt
VERSION=version
```

Variables de Entorno

FTP	<input type="text" value="21"/>
PASS	<input type="text" value="ario_prueba.txt"/> ...
TELNET	<input type="text" value="23"/>
IP	<input type="text" value="192.168.0.2"/>
VERSION	<input type="text" value="version"/>
SSH	<input type="text" value="22"/>
HTTP	<input type="text" value="80"/>
VERBOSE	<input type="text" value="false"/>
MODEL	<input type="text" value="Modelo"/>
USERS	<input type="text" value="ario_prueba.txt"/> ...
DIR	<input type="text" value="o_directorios.txt"/> ...

Cancelar Aceptar

EJEMPLO DOS

The image displays the Axon Test 4.0 software interface. On the left, a terminal window shows a script for a DDoS attack: `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`. The main interface shows a project tree with a Master RTU containing Modicon Modbus, DNP3, and IEC 60870-5-101/103/104 protocols, and a Slave Monitor with Digital and Analog I/O. The Properties window shows configuration for the Slave: Asdu Address (2), Asdu size (1), Communication (TCPVenture), General (Name: Venture, Prefix: Venture), General Interrogation (Periodicity: None, Period: 30), Information Address (Size: 3), Parameters (K: 12, W: 8, Actcon: True, Acttem: True), and Synchronization (Periodicity: None, Period: 30). The Command Advanced window shows 'Data Adquisition by Polling' and 'General Interrogation' sections with 'Address' and 'Group of Interrogation' fields set to 0. The Error View Log shows messages for loading slave and modbus plugins, and multiple 'Venture Start Listen...' and 'VentureFinish Connection' events, with several red error messages: `[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`.

EJEMPLO FUERZA BRUTA

```
root@kali: ~/hacking_toolbox
Archivo Editar Ver Buscar Terminal Ayuda
root@kali:~/hacking_toolbox# ./sghtb.sh -b --ssh
Intentando ataque de fuerza bruta SSH
```

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

```
root@kali: ~/hacking_toolbox
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@kali:~/hacking_toolbox# ./sghtb.sh -sn
Realizando sniffing
Las credenciales de usuario aparecerán en el log, presione q para salir
```

```
root@kali: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@kali:~# ftp [redacted]
Connected to [redacted]
220 (vsFTPd [redacted])
Name ([redacted]:root): test
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
ftp> exit
221 Goodbye.
root@kali:~#
```

*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

```
GNU nano 2.9.8          runtests.sh          Modificado
#!/bin/bash

Tests

/init.sh
./sghtb.sh -s
./sghtb.sh -hd
./sghtb.sh -b --ssh

Tests
```



V CONGRESO **SMART GRIDS**

Madrid, 13 Diciembre 2018

DATOS DE CONTACTO:

santiago.dediego@tecnalia.com

inaki.angulo@tecnalia.com

