Writeups SUGUS CTF 2024 - Retos Patrocinados

Fundación Cidaut



CTF SUGUS 2024
”Unexpected Visitor”

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

Uno de los vigilantes de Fundación Cidaut ha corroborado un intento de robo en uno de las almacenes de prototipos, tras saltar la alarma de una de las barreras micro-ondas de las instalaciones y revisar una de las puertas de entrada ha podido confirmar un intento de forzar la cerradura. Sin embargo tras revisar las cámaras de seguridad no ha podido identificar ningún evento sospechoso. Hace tiempo que nuestro guarda desconfía de la instalación de cámaras IP y no confía en que los gatos del Parque Tecnológico como actores forzadores de cerraduras.

Nos han encargado un Pentesting de Infraestructura en Red y Servicios internos que encubre auditoría del circuito de cámaras, y nos han dejado como muestra una cámara IP de marca 'DLink' desplegadas en el almacén de prototipos. (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 212.183.202.230:82
- Estación de Trabajo de Auditoría
  1. La propia estación de trabajo de la persona que resuelve el reto

4 Notas del Autor

Se trata de un reto más de explotación de cámaras IP, destacar que estás técnicas son especialmente útiles en redes internas que dispongan de circuito de cámaras cerrados, también es frecuente encontrarlas en redes domesticas y en ambos casos directamente conectadas a rotures Wi-Fi por proveedores de seguridad con escasa segmentación.

La amplia interconexión de dispositivos ha motivado a conectarlas desde el inicio de su existencia directamente a Internet, solo a veces detrás de diferentes barreras de autenticación, aplicativos específicos, proxys web, actualmente pueden aparecer conectadas a ”Nodos IoT”, o integradas en algún ”BMS” (Building Management System). En naturaleza y a efectos prácticos sigue siendo la misma tecnolgía con otro nombre.

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.

Conclusiones:

- Identificado el modelo de la cámara ”DLink” en el elemento ”Basic Realm” ***DCS-932L***
- Identificado el Servidor Web Embebido en el elemento ”http-server-header” ***GoAhead-Webs***

Linea de nmap:

```
└─$ sudo nmap -Pn -p82 -sVC 212.183.202.230
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-21 17:03 CET
Nmap scan report for 212.183.202.230.static.user.ono.com (212.183.202.230)
Host is up (0.068s latency).

PORT   STATE SERVICE VERSION
82/tcp open  http    GoAhead WebServer
| http-title: Document Error: Unauthorized
|_Requested resource was http://212.183.202.230.static.user.ono.com:82/home.htm
|_http-server-header: GoAhead-Webs
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=DCS-932L

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.18 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/82
  - (-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:

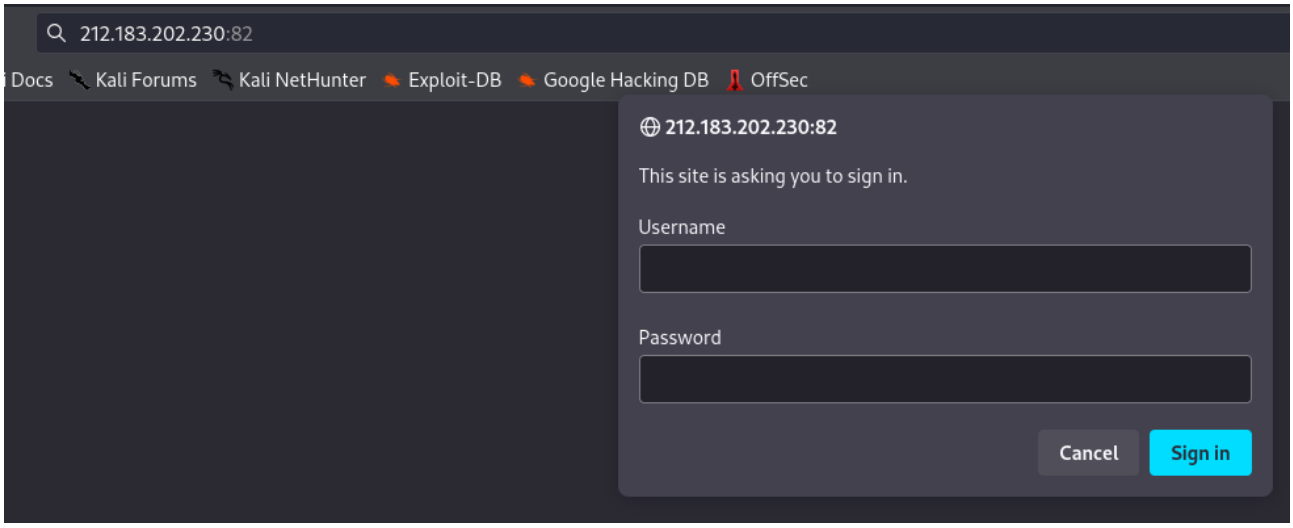


Figure 2: Simple HTTP Authentication

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.

En el caso de las cámaras ”DLink” nos encontramos que disponen de múltiples exploits, esto se debe a que fueron cámaras adoptadas por empresas de seguridad y existió mucha motivación por comprender estos dispositivos.

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

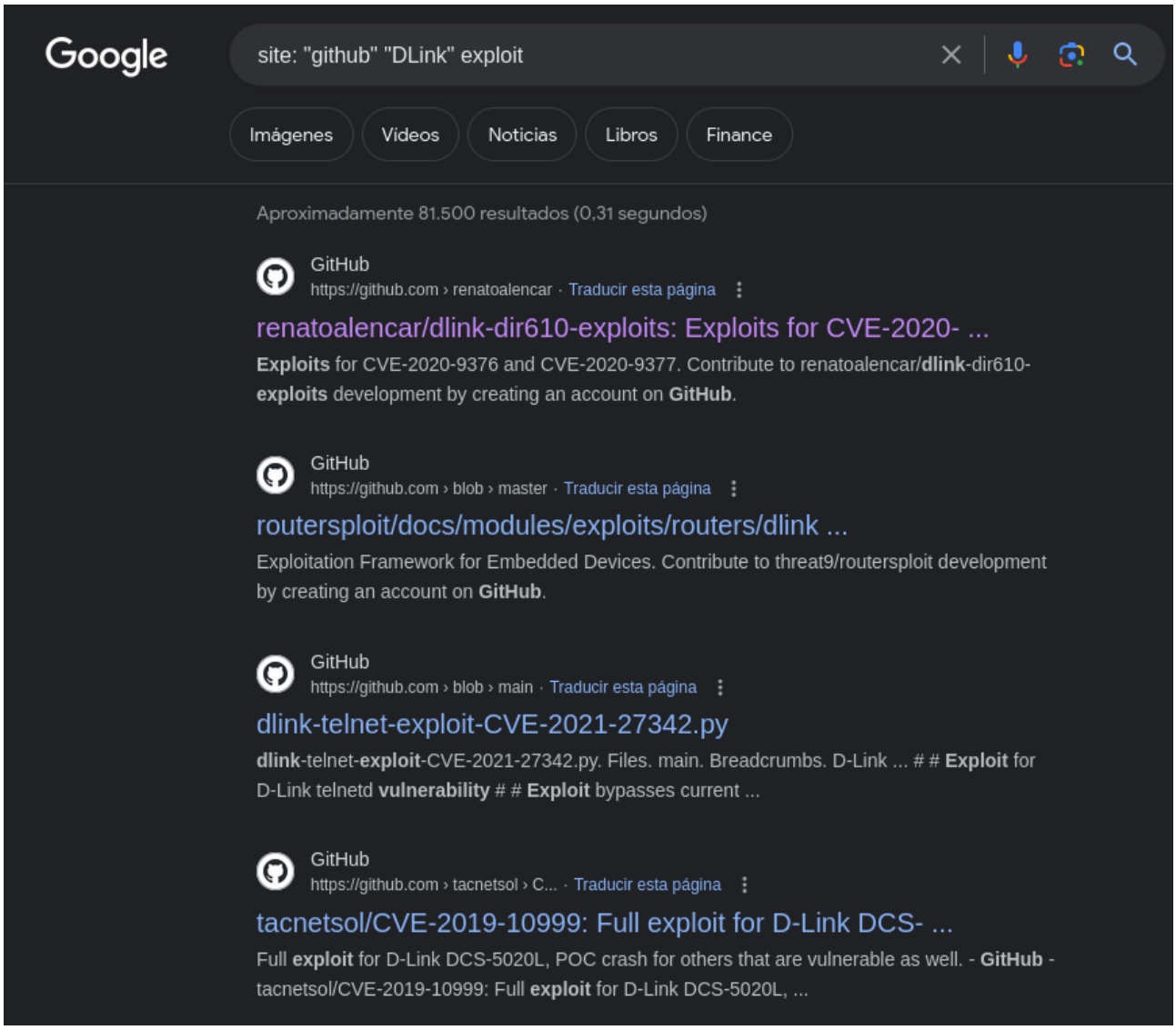


Figure 3: Búsqueda Abierta 1

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 4: 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

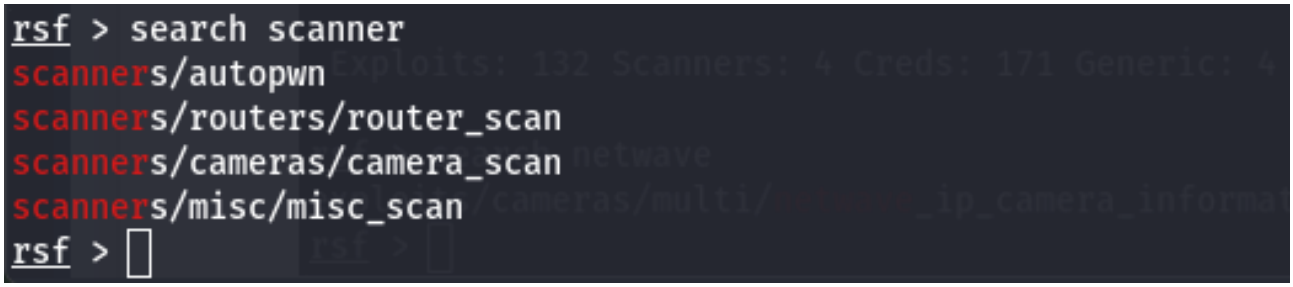


Figure 5: RouterSploit: Scanners Disponibles

Router Sploit: Configuracion Exploit

```
rsf (D-Link DCS Cameras Authentication Bypass) > show options

Target options:

   Name       Current settings     Description
   ----       ----------------     -----------
   ssl        false                SSL enabled: true/false
   target                          Target IPv4 or IPv6 address
   port       8080                 Target HTTP port


Module options:

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

Figure 6: RouterSploit: Configuración de un Exploit

Router Sploit: Configuración Exploit

```
rsf (D-Link DCS Cameras Authentication Bypass) > set target 212.183.202.230
[+] target => 212.183.202.230
rsf (D-Link DCS Cameras Authentication Bypass) > set port 82
[+] port => 82
rsf (D-Link DCS Cameras Authentication Bypass) >
```

Figure 7: RouterSploit: Configurar el Exploit

Router Sploit: Resultados del Exploit

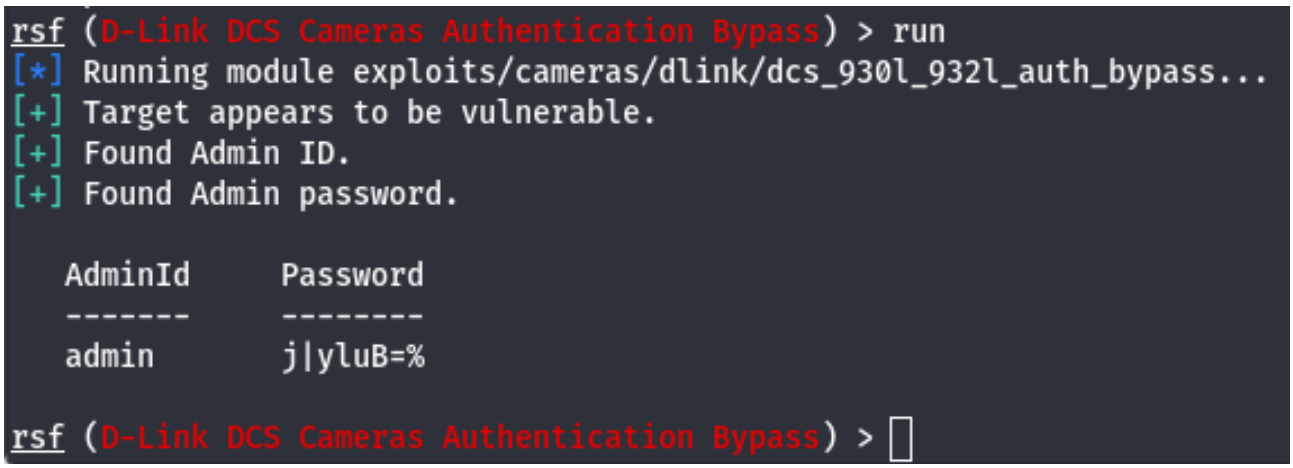


Figure 8: RouterSploit: Resultados del Exploit

Resultados:

- Username: admin
- Password: j|yluB=%

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

Tras acceder a la cámara por la interfaz Web la misma se encuentra directamente enfocando a la Flag y debe introducirse tal y como se visualiza.

Imagen de la Flag: Resultados del Exploit



Figure 9: Cámara Enfocando la Flag

Resultado:

- Flag: `SUGUS{THE_DARK_SITE_33}`

7 Soluciones Alternativas

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

```
GET http://212.183.202.230:82/dlink.css?cidx=1.022011-10-14 HTTP/1.1
host: 212.183.202.230:82
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/css,*/*;q=0.1
Accept-Language: en-US,en;q=0.5
Referer: https://212.183.202.230:82/wizard.htm
Authorization: Basic YWRtaW46anx5bHVCPSU=
Connection: keep-alive
Sec-Fetch-Dest: style
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
If-Modified-Since: Sat Jan  1 00:00:04 2011
```

Figure 10: RouterSploit: Autenticación con el servicio

Explotación Binaria: La autenticación y la aplicación acuden a rutas fijas del del Servidor Web embebido GoAhead, los firmwares pueden ser encontrados públicamente y des-compilados en busca de los binarios del servidor web, pudiéndose desarrollar exploits RCE contra la cámara. `https://www.embedthis.com/goahead/`