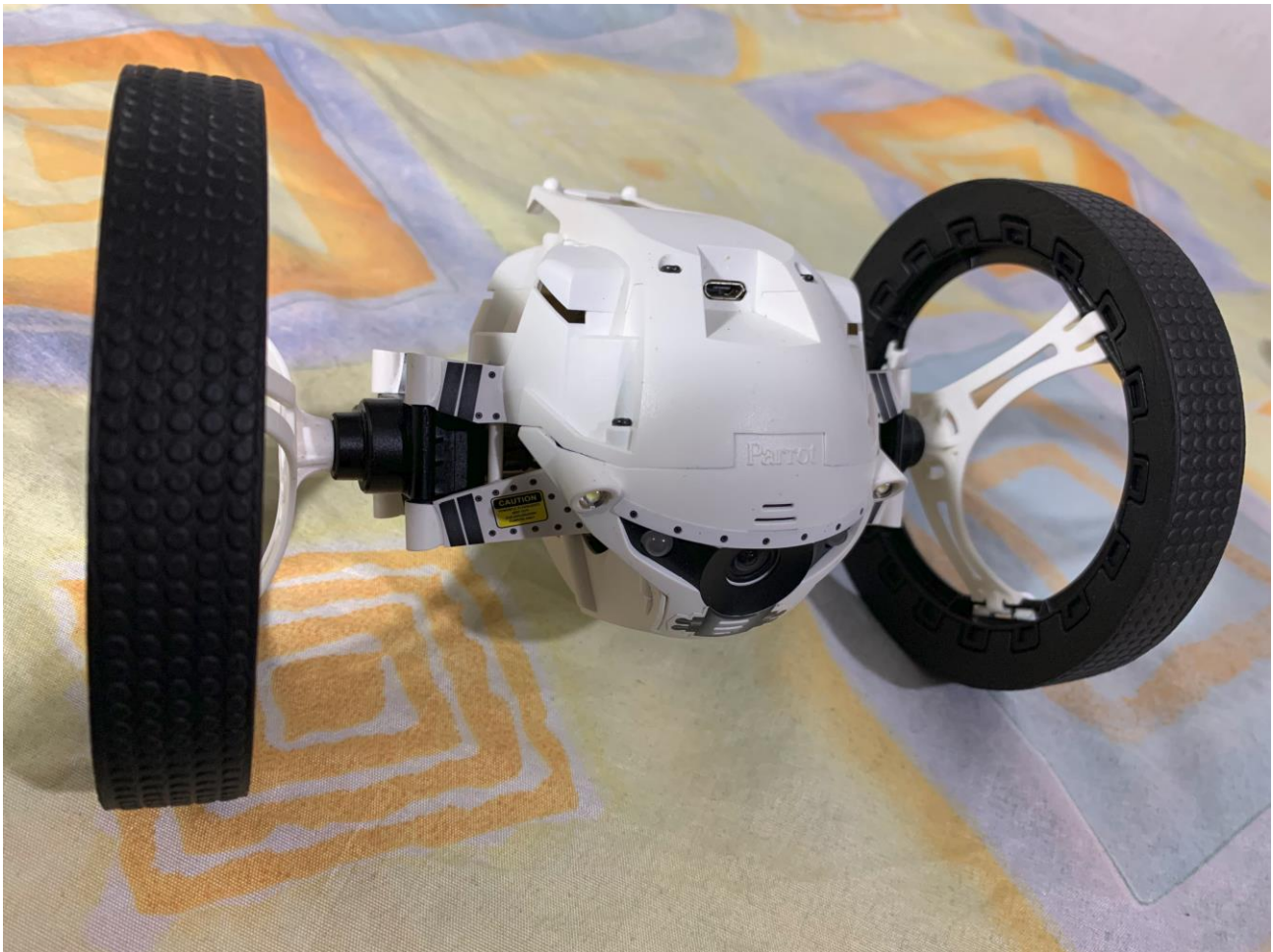


Reporte de investigación

El hackeo de drones se ha convertido en una preocupación creciente en el campo de la ciberseguridad, debido a las vulnerabilidades en sus mecanismos de transmisión de datos, especialmente aquellos basados en **tecnología WiFi y radiofrecuencia**.

El **Parrot Jumping Sumo** es un minidrón terrestre de la línea MiniDrones de Parrot, diseñado para realizar acrobacias, saltos y desplazamientos rápidos. A continuación, se detallan sus especificaciones técnicas:



Especificaciones Técnicas

- **Dimensiones:**
 - Con ruedas extendidas: 185 x 150 x 110 mm
 - Con ruedas retraídas: 143 x 150 x 110 mm
- **Peso:** 180 g
- **Velocidad máxima:** hasta 7 km/h (aproximadamente 2 m/s)
- **Alcance:** hasta 50 metros mediante conexión Wi-Fi directa
- **Modos de control:**
 - **Jumper:** salta hasta 80 cm de altura o longitud
 - **Kicker:** empuja objetos mediante un resorte incorporado
 - **Auto-balance:** mantiene el equilibrio automáticamente
- **Cámara:**
 - Resolución: 640 x 480 píxeles
 - Velocidad de captura: 15 fps
 - Transmisión en vivo a través de la aplicación
- **Conectividad:**
 - Wi-Fi de doble banda (2.4 GHz y 5 GHz)

- Puerto USB 2.0 para almacenamiento externo
- **Batería:**
 - Tipo: Li-Po de 3.7V y 550 mAh
 - Autonomía: aproximadamente 20 minutos
 - Tiempo de carga: entre 60 y 90 minutos
- **Control:**
 - Aplicación FreeFlight 3 compatible con iOS, Android y Windows
 - Permite programar secuencias de movimientos y acrobacias
- **Sensores:**
 - Giroscopio y acelerómetro integrados
- **Indicadores:**
 - Luces LED que indican el estado del dispositivo
- **Audio:**
 - Altavoz incorporado para emitir sonidos y expresar "emociones"

Contenido de la Caja

- 1 x Parrot Jumping Sumo (color blanco)
- 1 x Batería Li-Po
- 1 x Cable micro-USB
- 2 x Almohadillas de goma
- 3 x Stickers para personalización
- 1 x Guía rápida de inicio



Este minidrón es ideal para uso en interiores y superficies planas. Aunque puede utilizarse en exteriores, se recomienda evitar superficies húmedas o irregulares para preservar su

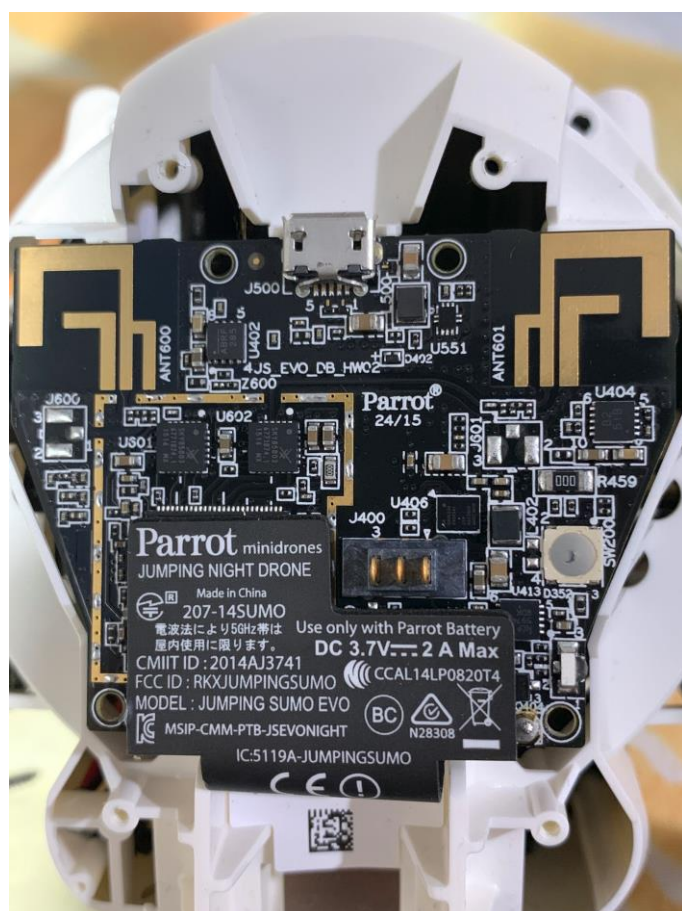
integridad. Su diseño robusto y funciones interactivas lo convierten en una opción entretenida para usuarios de todas las edades.

Ss

El SKY85803 es un módulo de front-end (FEM) de doble banda diseñado por Skyworks Solutions Inc. para aplicaciones WLAN compatibles con los estándares 802.11a/b/g/n/ac. Este circuito integra múltiples funciones esenciales para la transmisión y recepción de señales de radiofrecuencia en las bandas de 2.4 GHz y 5 GHz.

Función Principal

El SKY85803 actúa como un módulo de front-end para dispositivos WLAN, integrando amplificadores de potencia (PA), filtros de transmisión, interruptores de transmisión/recepción y diplexores. Su diseño compacto y altamente integrado permite mejorar el rendimiento de transmisión y recepción en dispositivos inalámbricos, facilitando la implementación de soluciones de conectividad Wi-Fi de alta velocidad.



Características Técnicas

Integración de componentes:

Amplificadores de potencia (PA) para 2.4 GHz y 5 GHz

Filtros de transmisión

Interruptores de transmisión/recepción

Diplexores

Puertos RF: Todos los puertos de RF están adaptados a 50 Ω

Detectores de potencia: Integrados para cada cadena de transmisión

Rendimiento de potencia de salida:

+21 dBm para 802.11b a 11 Mbps con ACPR de +35 dBc

+18 dBm @ 3.0% EVM para 802.11n 64 QAM en 2.4 GHz

+16 dBm @ 3.0% EVM para 802.11n 64 QAM en 5 GHz

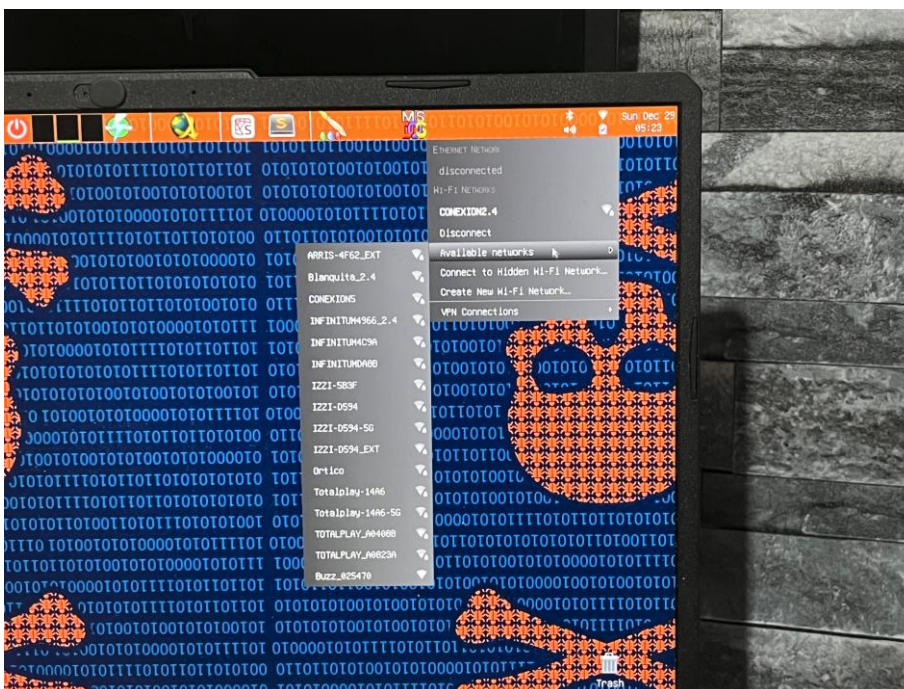
+16 dBm @ 1.8% EVM para 802.11ac 256 QAM en 2.4 GHz



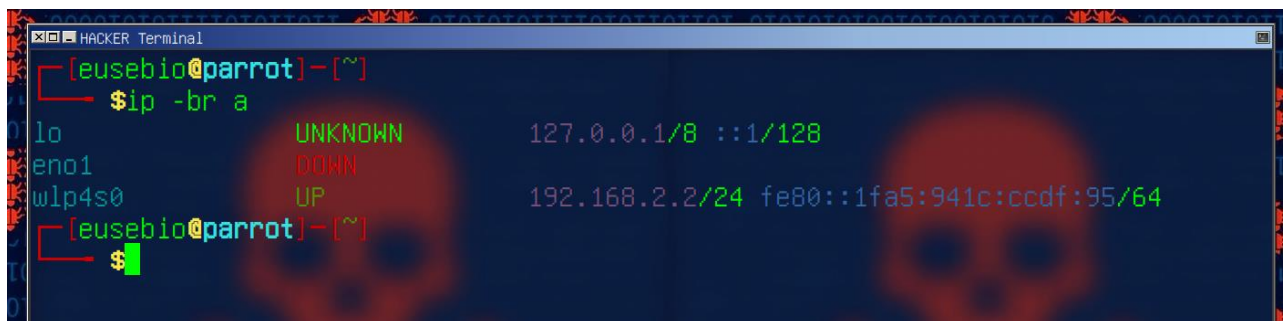
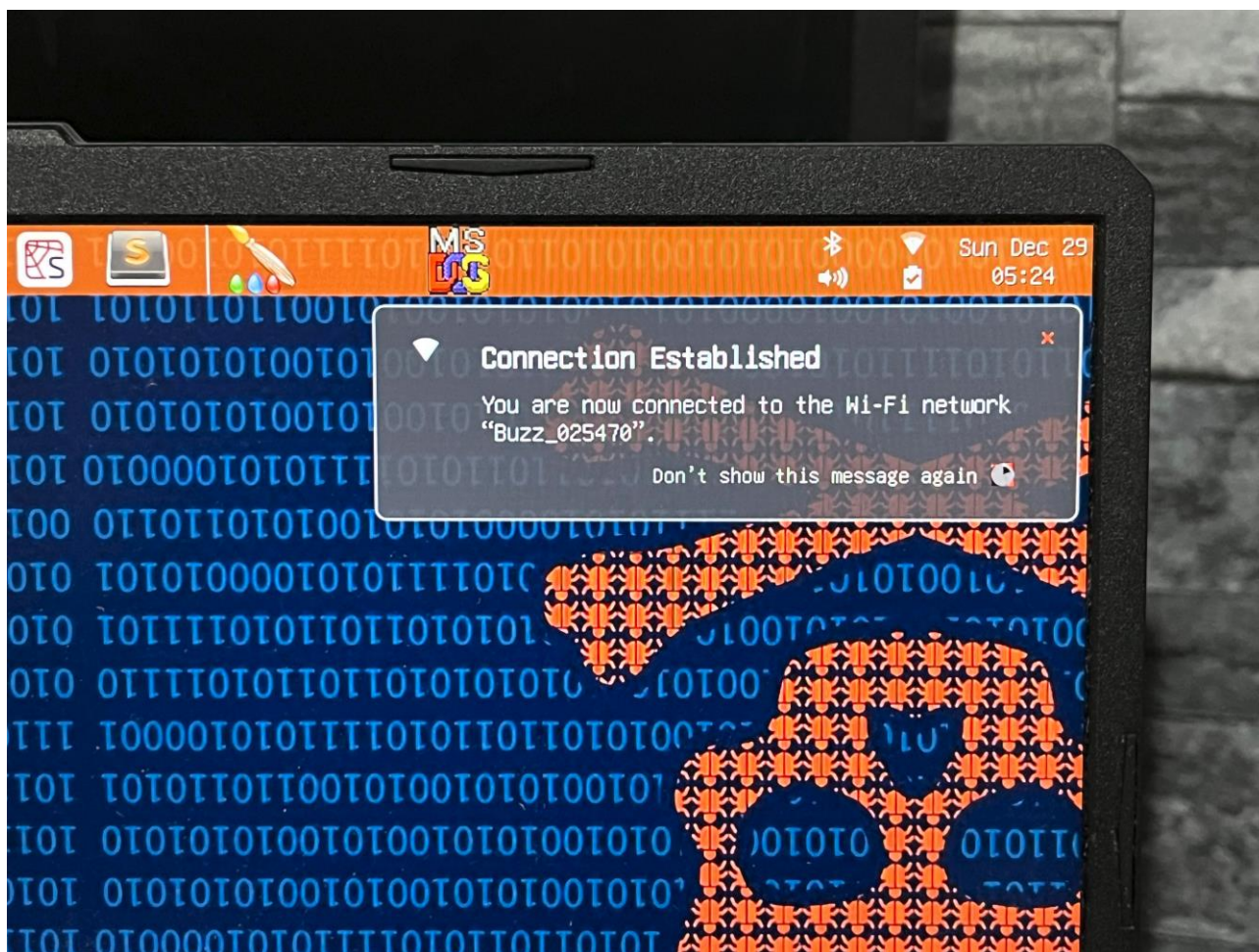
+13 dBm @ 1.8% EVM para 802.11ac
256 QAM en 5 GHz
Voltaje de operación: 3.3 V \pm 10%
Empaque: LGA de 24 pines, dimensiones de 4 x 4 mm
Cumplimiento de estándares: MSL3, 250 °C según JEDEC J-STD-020

Este módulo es ideal para integrarse en dispositivos que requieren conectividad Wi-Fi de alto rendimiento, como routers, puntos de acceso, laptops y otros equipos electrónicos que operan en las bandas de 2.4 GHz y 5 GHz. Su alto nivel de integración reduce la necesidad de componentes externos, simplificando el diseño y mejorando la eficiencia del sistema.

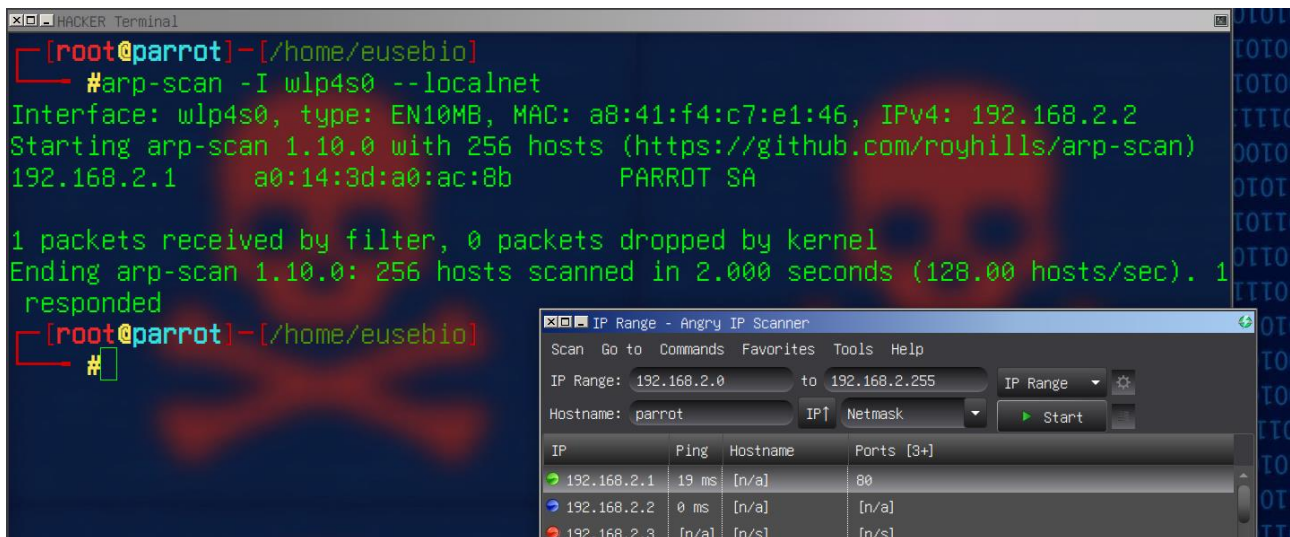
Los ataques *Man in the Middle* (MITM) representan una de las amenazas más significativas en las redes WLAN, ya que permiten a los ciberdelincuentes interceptar, alterar o incluso controlar las comunicaciones entre el dron AP y su operador dentro del rango del punto de acceso (**Access Point**). Estos ataques explotan las debilidades de las redes inalámbricas, poniendo en riesgo tanto la seguridad de los drones como la integridad de las operaciones aéreas. En este contexto, es esencial comprender cómo funcionan estos mecanismos de transmisión y las tácticas utilizadas para vulnerarlos, así como las estrategias para mitigar dichos riesgos.



En los últimos meses, he estado realizando pruebas de manera autodidacta con un dron de la marca Parrot, utilizando un enfoque de prueba y error. Este dron opera mediante la creación de una red Wi-Fi,



lo que permite la comunicación con el dispositivo a través de una aplicación móvil y facilita la realización de auditorías de seguridad, Durante el proceso, encontré relevante cómo se puede vulnerar la seguridad perimetral del dron, lo que permitiría el acceso remoto al mismo.



The screenshot shows a terminal window with the following output:

```
[root@parrot]-[/home/eusebio]
#arp-scan -I wlp4s0 --localnet
Interface: wlp4s0, type: EN10MB, MAC: a8:41:f4:c7:e1:46, IPv4: 192.168.2.2
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.2.1      a0:14:3d:a0:ac:8b      PARROT SA

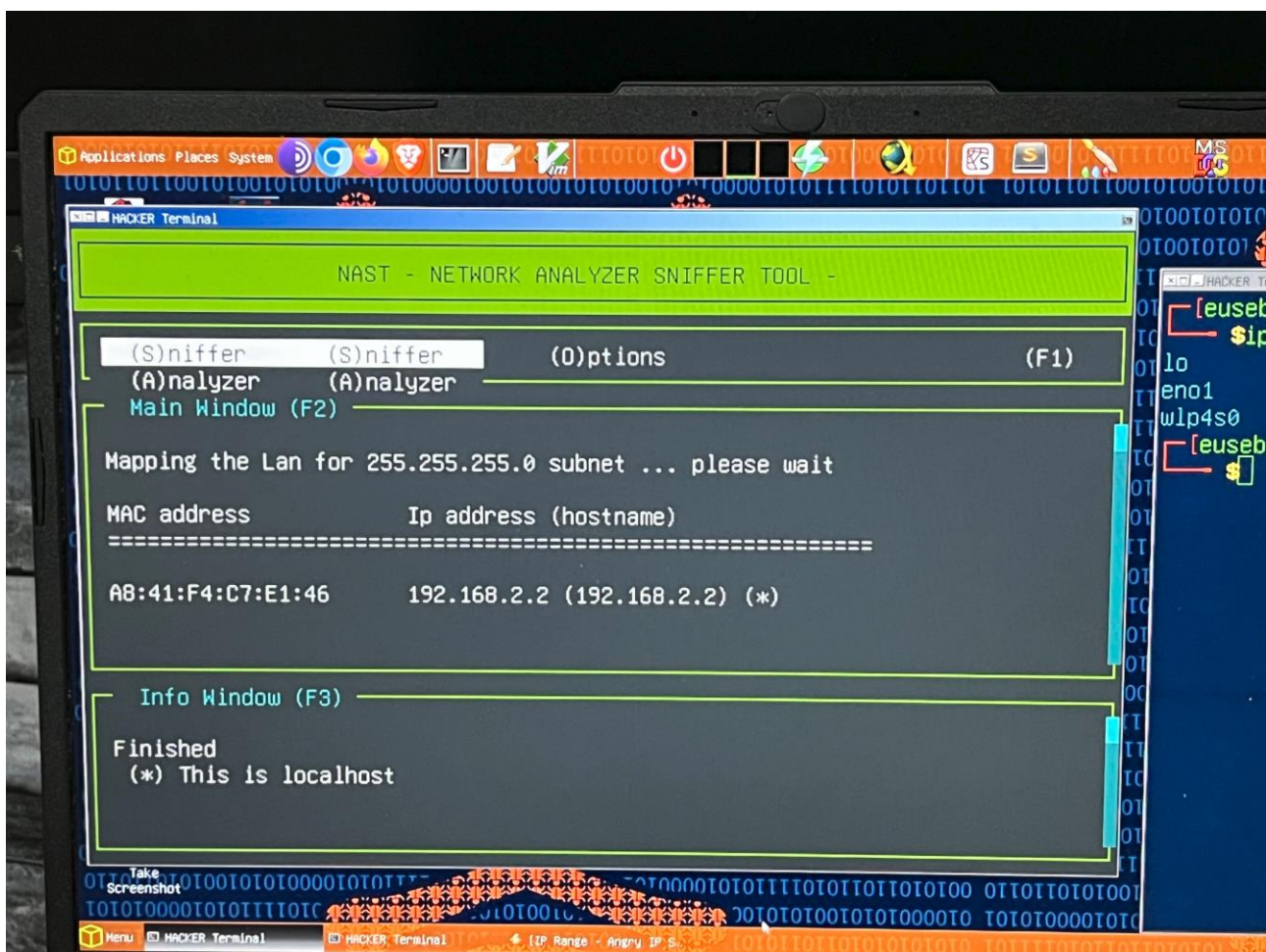
1 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.000 seconds (128.00 hosts/sec). 1
responded
[root@parrot]-[/home/eusebio]
#
```

Overlaid on the terminal is the 'Angry IP Scanner' window. It shows the IP Range set to 192.168.2.0 to 192.168.2.255, Hostname set to parrot, and a table of results:

IP	Ping	Hostname	Ports [3+]
192.168.2.1	19 ms	[n/a]	80
192.168.2.2	0 ms	[n/a]	[n/a]
192.168.2.3	[n/a]	[n/s]	[n/s]

Figura

Se realiza un escaneo arp-scan tomando de referencia el interfaz de red en el localnet obteniendo la direccion ip y la mac address del dispositivo parrot




```
[root@parrot]-[/home/eusebio]
#ping -c 5 192.168.2.1 -p 80
PATTERN: 0x80
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
64 bytes from 192.168.2.1: icmp_seq=1 ttl=64 time=7.37 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=64 time=7.50 ms
64 bytes from 192.168.2.1: icmp_seq=3 ttl=64 time=2.08 ms
64 bytes from 192.168.2.1: icmp_seq=4 ttl=64 time=7.41 ms
64 bytes from 192.168.2.1: icmp_seq=5 ttl=64 time=2.12 ms

--- 192.168.2.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 2.076/5.297/7.504/2.611 ms
```

Figura

realizo un barrido ping de la direccion ip y especificamente al puerto 80 si hay respuesta por parte del dron , la traza icmp arroja que se trata de un sistema linux ttl=64 al realizar un escaneo nmap obtengo los puertos abiertos:

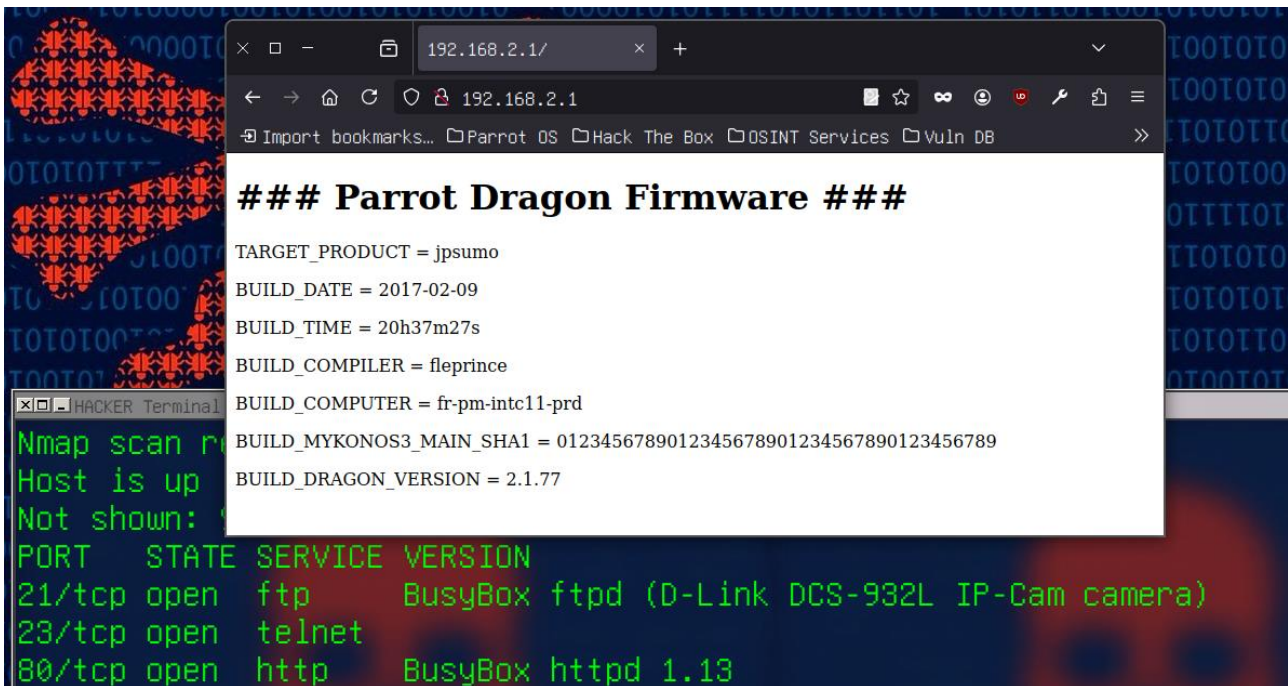
```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      BusyBox ftpd (D-Link DCS-932L IP-Cam camera)
23/tcp    open  telnet
80/tcp    open  http     BusyBox httpd 1.13
```

```
HACKER Terminal
[root@parrot]-[/home/eusebio]
#nmap -T4 -F -O 192.168.2.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-29 06:02 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.2.1
Host is up (0.0047s latency).
Not shown: 97 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
80/tcp    open  http
MAC Address: A0:14:3D:A0:AC:8B (Parrot SA)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.16 - 2.6.35 (embedded)
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.83 seconds
```

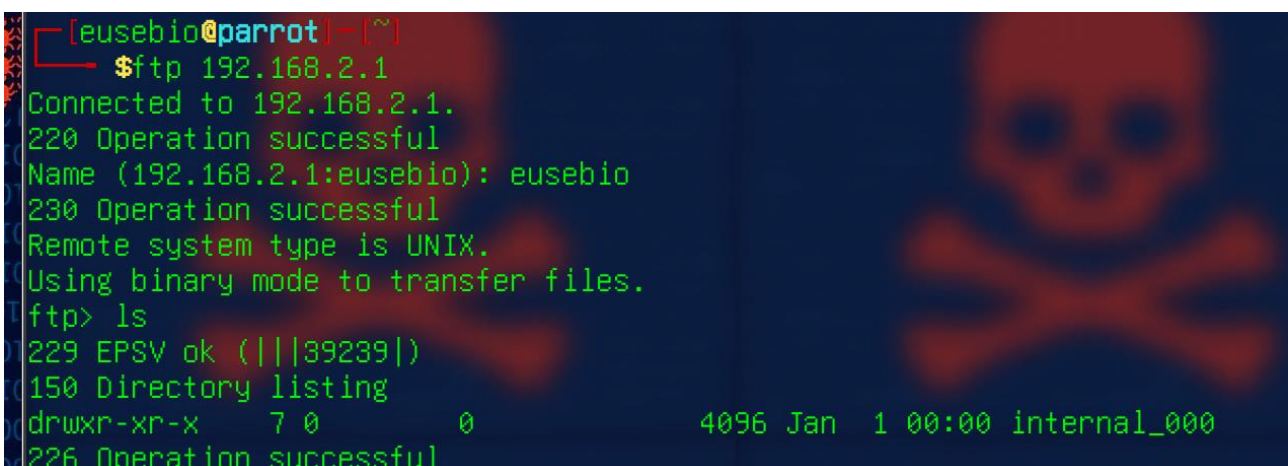
obtengo los datos clave: sistema operativo linux y kernel, distancia del hop en la red , el tipo de webcam.

```
MAC Address: A0:14:3D:A0:AC:8B (Parrot SA)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.16 - 2.6.35 (embedded)
Uptime guess: 0.002 days (since Sun Dec 29 06:05:06 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=200 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; Device: webcam; CPE: cpe:/h:dlink:dcs-932l, cpe:/o:linu
x:linux_kernel
```



Figura

El dron parrot ha levantado un servidor web accesible desde la direccion ip y el puerto 80



Figura

Obtengo fácil acceso vía conexión FTP: ¡ CONEXION ESTABLECIDA !