

CROZONO

Herramienta de Detección e Investigación de Cibercrimen

Mg. Ing. Pablo Romanos

CLAI  **2017**
BUENOS AIRES **ARGENTINA**
XXII CONGRESO LATINOAMERICANO
DE AUDITORES INTERNOS

1, 2, 3 y 4 de octubre de 2017 | Buenos Aires | Argentina



Auditoría de Seguridad a Sistemas Informáticos

Penetration Test o Test de Intrusión:

Un Penetration Test, es una evaluación del estado de seguridad a nivel lógico de una infraestructura informática. Permite conocer las vulnerabilidades que un atacante podría aprovechar para acceder a una red y comprometer información sensible.

- **White Box (Externa/Interna):**

En una auditoría white box, el auditor dispone de información sobre la infraestructura del objetivo.

- **Black Box (Externa/Interna):**

El auditor no dispone de información sobre el objetivo, por lo que deberá obtener datos útiles por sus propios medios.



Herramientas Comúnmente Empleadas



Para realizar una auditoría externa o black box a una red WiFi se utilizan distintos programas en una notebook junto a una antena de largo alcance.

Origen de CROZONO



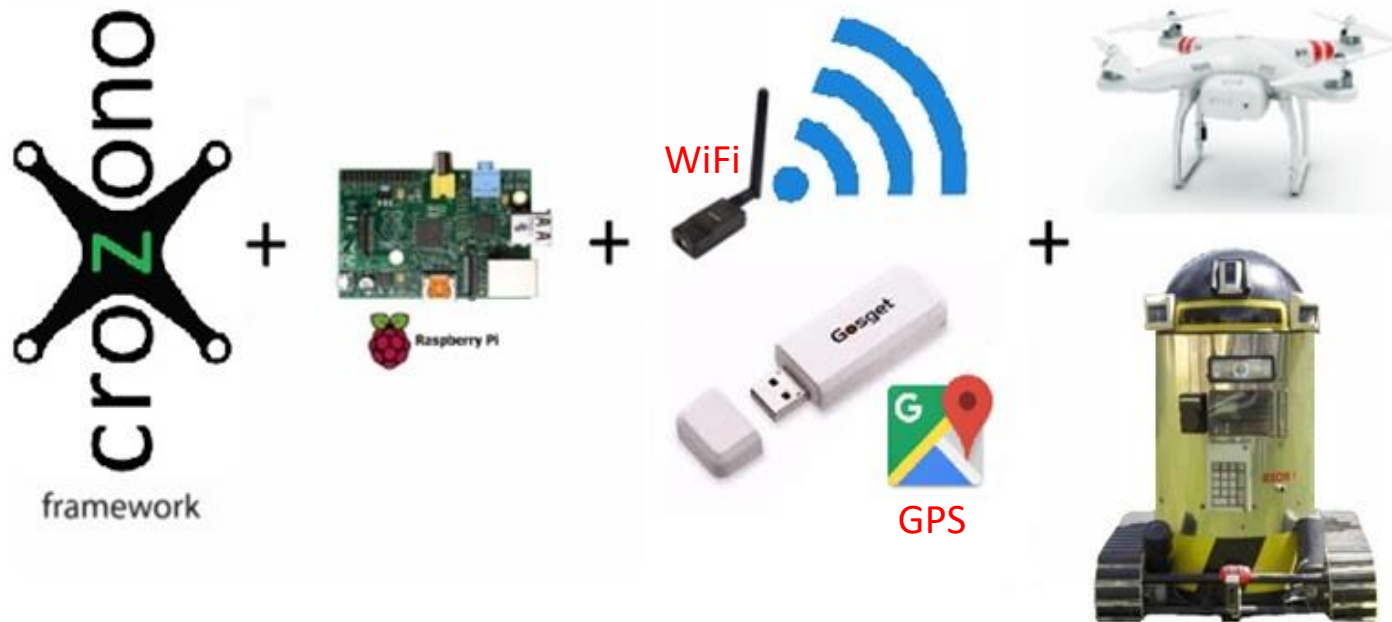
¿Es posible utilizar los últimos inventos tecnológicos para realizar *auditorías de seguridad a infraestructuras informáticas*?

¿Qué es CROZONO?

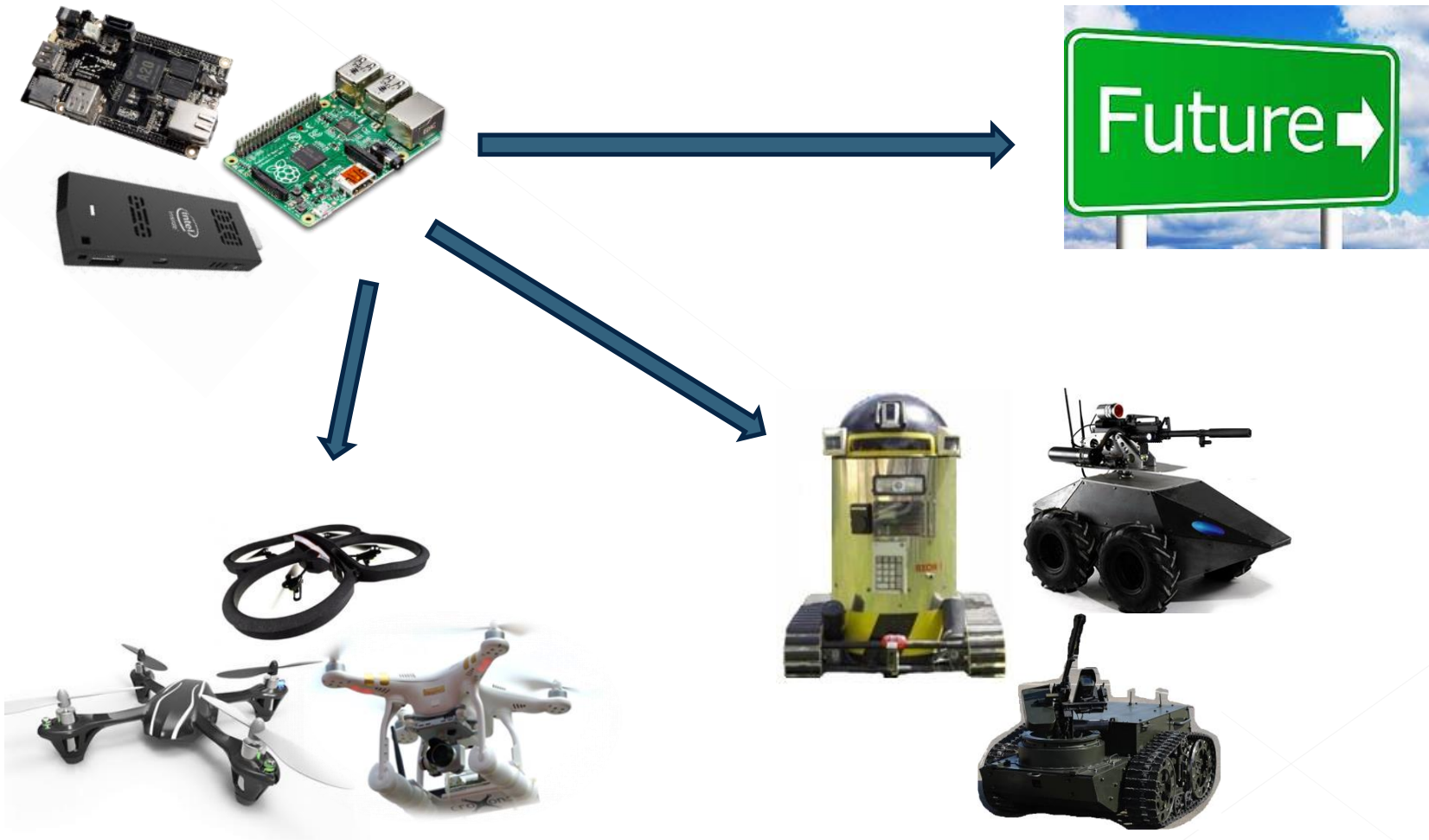
- Framework (software) open source programado en Python.
- Se ejecuta en sistemas GNU/Linux.
- Toma decisiones y NO se controla remotamente.
- Incorpora pruebas de seg. para redes Wlan y LAN.
- Es posible agregar nuevos módulos y parámetros.



Arquitectura de CROZONO



Aplicación en Drones & Robots



CROZONO: Invento Argentino

Alerta para empresas y usuarios particulares de Internet

Prueban que desde un drone se puede hackear una red Wi-Fi

Lo explicaron expertos

de la seguridad party, que se en el Konex.



Pericias. Especialistas y entusiastas ayer, en Ekoparty, probando errores en sistemas informáticos. MAURIPALMA

apoyado en un techo, la pregunta que se hicieron es "¿Cómo meterse a la red de una empresa, sin tecla-



Sheila Berta y Pablo Romanes. Exponen mañana en la cumbre hacke



El día que llegó el futuro. Una réplica del DeLorean, el auto del filme Volver al Futuro 2, desfiló ayer por las calles de Tokio. En la película transcurre el año 1985, y los protagonistas viajan al futuro adelantándose a su tiempo 30 años, exactamente el 21 de octubre de 2015.

Crozono (invento argentino) Un drone detecta fallas de seguridad

Los expertos argentinos en el robo de seguridad de la Policía Federal desarrollaron un software que, mediante el uso de un dron, prueba las fallas de seguridad que presentan las redes Wi-Fi.

Los especialistas de 30 años que se dedican a la promoción de los drones y sus usos tecnológicos, comenzaron a idear luego de haberse conocido durante clases en la Escuela Multimedial DuVino.

Los expertos utilizan un cuadricóptero Phantom 3 y con una tablet programan el punto por donde el dron debe pasar, y así lograr que el equipo se vaya desmenuzando y captando toda la información.



El invento argentino Crozono y su nombre de seguridad de la Policía Federal.

Hay hackers que usan su conocimiento para robar y otros lo usan para proteger.

El invento argentino Crozono y su nombre de seguridad de la Policía Federal.



De hackers a emprendedores

Primero se dedicaron a detectar la vulnerabilidad de diferentes sistemas. Y luego pasaron a encarar sus propios desarrollos como empresarios.

por HERNÁN MURJÁ

Desde el aire

CROZONO UTILIZA DRONES PARA DETECTAR LA VULNERABILIDAD DE REDES INFORMÁTICAS.

Sheila Berta y Pablo Romanes, fundadores de Crozono, una empresa que se dedica a detectar fallas de seguridad en redes Wi-Fi mediante el uso de drones. Los hermanos comenzaron a idear el proyecto en 2013, cuando se conocieron en la Escuela Multimedial DuVino.

Los expertos argentinos en el robo de seguridad de la Policía Federal desarrollaron un software que, mediante el uso de un dron, prueba las fallas de seguridad que presentan las redes Wi-Fi.

Los especialistas de 30 años que se dedican a la promoción de los drones y sus usos tecnológicos, comenzaron a idear luego de haberse conocido durante clases en la Escuela Multimedial DuVino.

Los expertos utilizan un cuadricóptero Phantom 3 y con una tablet programan el punto por donde el dron debe pasar, y así lograr que el equipo se vaya desmenuzando y captando toda la información.

La misión es parámetros académicos, los hicieron para investigar. Pero en realidad, tal vez, de un accidente en serio la verdad es que llegaron de hecho a presentar como producto objetivo en decir, que la policía utilizar el hecho de haberse informado a la policía, ya que cuando hacen un allanamiento y tienen que ir

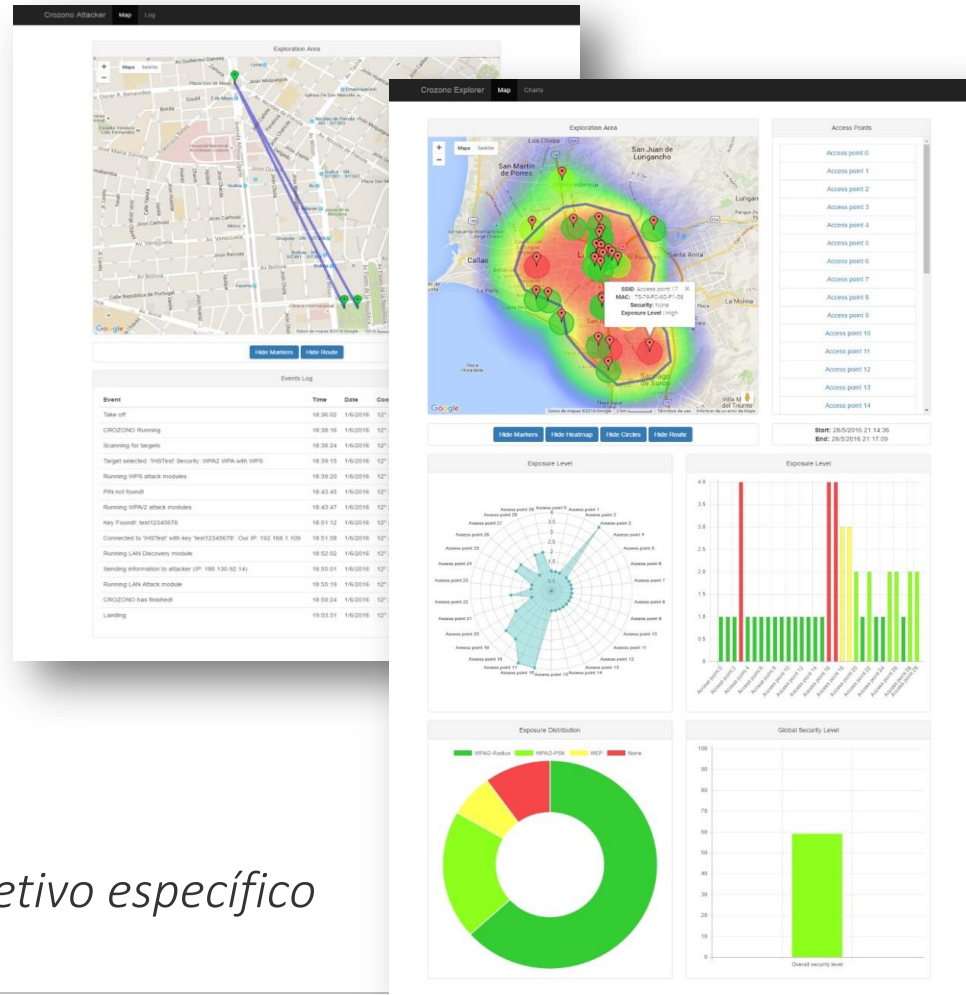
Hay hackers que usan el conocimiento para robar y hacer plata, y otros lo usan para proteger y ayudar a la Asociación como una persona que tiene mucho conocimiento técnico y tiempo para investigar, que en la fuerza es lo que se necesita para averiguar cómo funcionan las cosas", relatan.

Hay hackers que usan el conocimiento para robar y hacer plata, y otros lo usan para proteger y ayudar a la Asociación como una persona que tiene mucho conocimiento técnico y tiempo para investigar, que en la fuerza es lo que se necesita para averiguar cómo funcionan las cosas", relatan.

Versiones de CROZONO

Explorer

Relevamiento de información sobre un sector geográfico



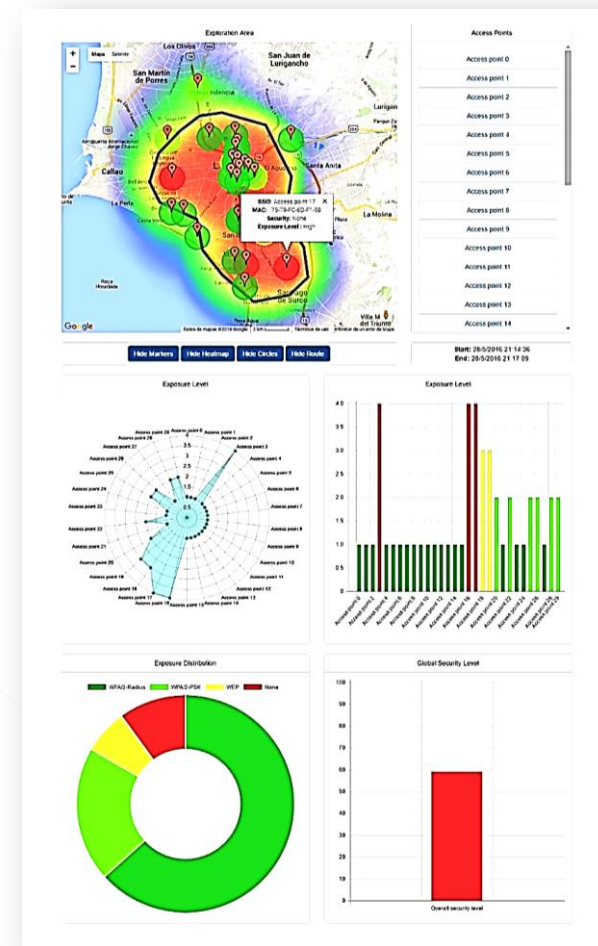
Attacker

Pruebas contra un objetivo específico

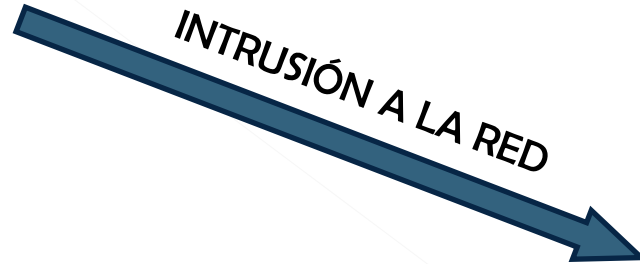
CROZONO Explorer

¿Qué buscar?

- ❑ C1 - Ubicación del AP dentro del área:
 - Alta, media o baja.
- ❑ C2 - Potencia del AP:
 - Alta, media o baja.
- ❑ C3 - Seguridad implementada:
 - WPA/2 Radius -> **Alta**
 - WPA/2 PSK -> **Media**
 - WEP -> **Baja**
 - None -> **Ninguna**



CROZONO Attacker



¿ALGÚN OBJETIVO EN ESTE EDIFICIO?

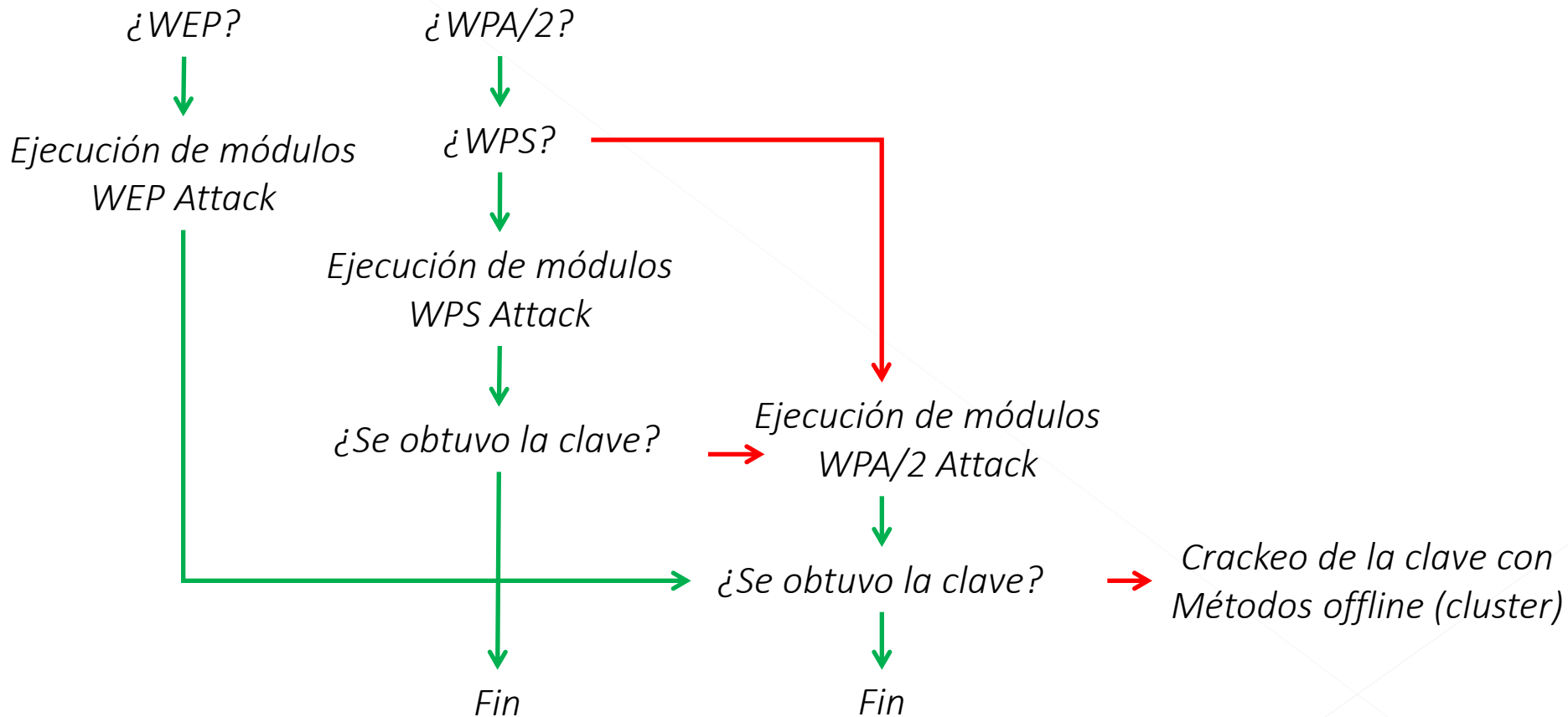
CROZONO Attacker (paso a paso)

- ❑ Paso 1: **Pentest** al punto de acceso **WiFi** objetivo (crackeo automático), “**rompiendo su seguridad**”.
- ❑ Paso 2: Una vez dentro de la red, **utiliza la conexión a Internet de la víctima** para conectarse al equipo del auditor (**conexión inversa**).
- ❑ Paso 3: Realiza un **descubrimiento** de la red ejecutando los módulos de “**LAN Discovery**” y **enviar el resultado** en tiempo real **al auditor**.
- ❑ Paso 4: Realiza un **pentest** ejecutando los módulos de “**LAN Attack**” (definidos previamente) y **enviar el resultado** en tiempo real **al auditor**.

The screenshot displays the Crozono Attacker interface. At the top, there's a 'Map' tab. Below it, a map shows an 'Exploration Area' with a blue line indicating a path between two points. Below the map is an 'Events Log' table with columns for Event, Time, Date, and Coordinates. The log contains the following entries:

Event	Time	Date	Coordinates
Take off	18:36:02	1/6/2016	12° 2' 29.9675' 77° 2' 12.007°
CROZONO Running	18:38:16	1/6/2016	12° 2' 47.0075' 77° 2' 33.947°
Scanning for targets	18:38:24	1/6/2016	12° 2' 47.0075' 77° 2' 33.947°
Target selected: 'WHSTest' Security: WPA2 WPA with WPS	18:39:19	1/6/2016	12° 2' 47.0075' 77° 2' 33.947°
Running WPS attack modules	18:39:20	1/6/2016	12° 2' 47.0075' 77° 2' 33.947°
PIN not found!	18:43:45	1/6/2016	12° 2' 47.0075' 77° 2' 33.947°
Running WPA2 attack modules	18:43:47	1/6/2016	12° 2' 47.0075' 77° 2' 33.947°
Key Found: test12345678	18:51:12	1/6/2016	12° 2' 47.0075' 77° 2' 33.947°
Connected to 'WHSTest' with key 'test12345678'. Our IP: 192.168.1.109	18:51:58	1/6/2016	12° 2' 47.0075' 77° 2' 33.947°
Running LAN Discovery module	18:52:02	1/6/2016	12° 2' 47.0075' 77° 2' 33.947°
Sending information to attacker (IP: 186.130.92.14)	18:55:01	1/6/2016	12° 2' 47.0075' 77° 2' 33.947°
Running LAN Attack module	18:55:19	1/6/2016	12° 2' 47.0075' 77° 2' 33.947°
CROZONO has finished!	18:59:24	1/6/2016	12° 2' 47.0075' 77° 2' 33.947°
Landing	19:03:31	1/6/2016	12° 2' 29.9475' 77° 2' 14.907°

Paso 1: Crackeo Automático WiFi



Paso 2: Conexión Inversa



AUDITOR

CONEXIÓN INVERSA



IP: 190.188.65.214:1337



TARGET

CROZONO se conecta a la red WiFi crackeada en el paso1, y utiliza ese enlace a Internet para realizar una conexión de forma inversa con el auditor.

Paso 3: Descubrimiento de la red local

```
[+] Hello! :)  
[+] Executing Nmap...  
  
Starting Nmap 6.00 ( http://nmap.org ) at 2015-12-08 19:37 ART  
Nmap scan report for Broadcom.Home (192.168.1.1)  
Host is up (0.0043s latency).  
Not shown: 995 closed ports  
PORT      STATE SERVICE      VERSION  
21/tcp    open  pwdgen       pwdgen  
23/tcp    open  telnet?        
80/tcp    open  http         micro_httpd  
139/tcp   open  netbios-ssn  Samba smbd 3.X (workgroup: WORKGROUP)  
445/tcp   open  netbios-ssn  Samba smbd 3.X (workgroup: WORKGROUP)
```

Ej: nmap -sV -O X.X.X.1-255

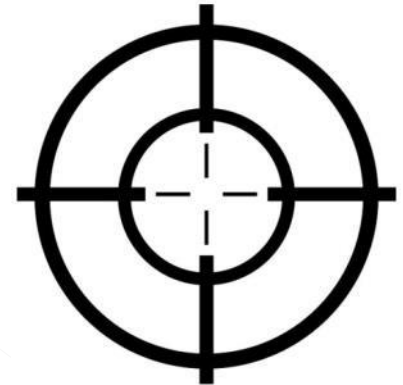
Paso 4: Ataque a la red local

Con el fin de ahorrar tiempo, CROZONO puede automatizar los siguientes ataques:

Sniffing-MITM: Man in the middle a un equipo de la red objetivo y envío de los datos capturados al auditor en tiempo real.

Evilgrade: Selección del plugin (interacción con el auditor). Man in the middle, DNS Spoof y Evilgrade contra un equipo de la red.

Metasploit: Terminal de Metasploit controlada remotamente por el auditor.



Ejecución de CROZONO Attacker sin parámetros

La ejecución de CROZONO sin parámetros conlleva la realización de los siguientes pasos:

- Configuración de hardware (modo monitor, falseo de MAC, etc.).
- Escaneo de las redes WiFi al alcance (1 minuto).
- Selección del target por cercanía y cantidad de paquetes capturados.
- Detección del tipo de seguridad (cifrado) de la red seleccionada.
- Crackeo de la red utilizando el ataque adecuado según el cifrado.
- Almacenamiento de la clave y/o captura de paquetes.

SIN PARAMETROS, NO se realizará conexión inversa, ni escaneo o pruebas sobre la red local interna.

Configuración de parámetros

The screenshot displays the 'CROZONO Assistant Software' window. At the top, there are menu items: 'Device', 'Templates', and 'Help'. The main area is titled 'Settings Panel' and is divided into three columns:

- Target:** Contains two input fields. The first is labeled 'WiFi AP's name (ESSID):' with the placeholder text '(Optionally)'. The second is labeled 'Password:' with the placeholder text '(Optionally)'. Below these fields is a green button labeled 'Load settings on attack device'.
- Attacker:** Contains two input fields. The first is labeled 'IP:' with the placeholder text '(Optionally)'. The second is labeled 'Port:' with the placeholder text '(Optionally)'. Below these fields is a green button labeled 'Load settings on attack device'.
- Attack modules:** Contains two dropdown menus. The first is labeled 'LAN discovery:' and has 'discovery_nmap_simple' selected. The second is labeled 'LAN Attack:' and has 'lan_sniffing_mitm_attac' selected.

Below the 'Settings Panel' is a 'Notifications' section, which is currently a solid black rectangle. To the right of the 'Settings Panel' is an 'Attack device management' section containing two green buttons: 'Extract data captured' and 'Check for updates'.

Uso en Fuerzas de Seguridad



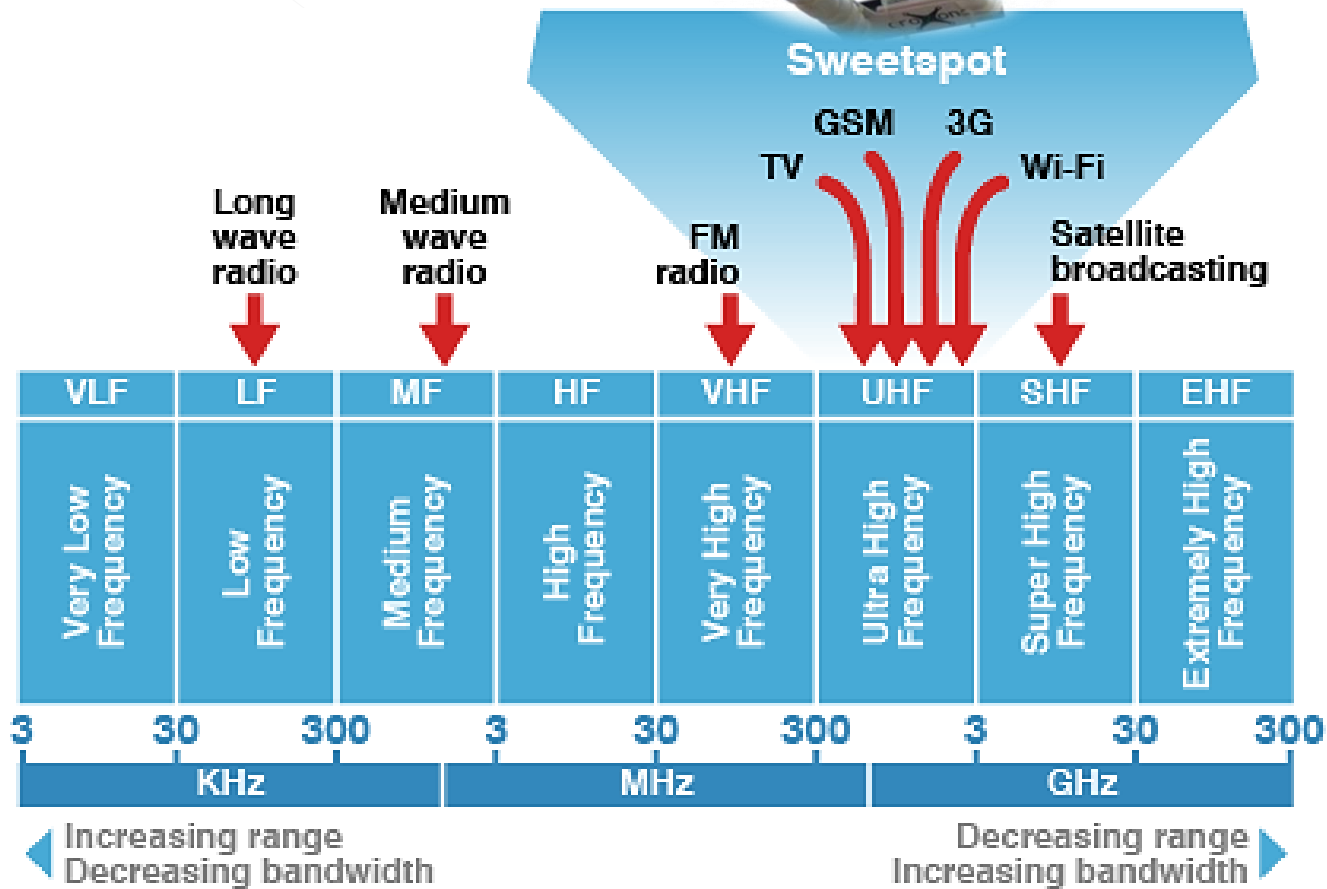
Testing de Infraestructuras Críticas



Video Demo



Próximos pasos...



Roadmap

2019

NEXT

2018

NEW

- Ataques a Cámaras IP
- -Análisis del Espectro Radioeléctrico

2017

- CROZONO Attacker
- Almacenamiento en Cloud
- CROZONO Explorer

2016

- CROZONO Professional (Versión Modular)
- Trazabilidad (Módulo GPS)

2015

- CROZONO Free (Script)

Muchas Gracias por su atención



www.crozono.com
info@crozono.com

Los invitamos a compartir sus comentarios en twitter e Instagram:

#CLAI2017 **#ProgresarCompartiendo**