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

IAIA
FLAI
FUNDACIÓN LATINOAMERICANA DE AUDITORES INTERNOS

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.

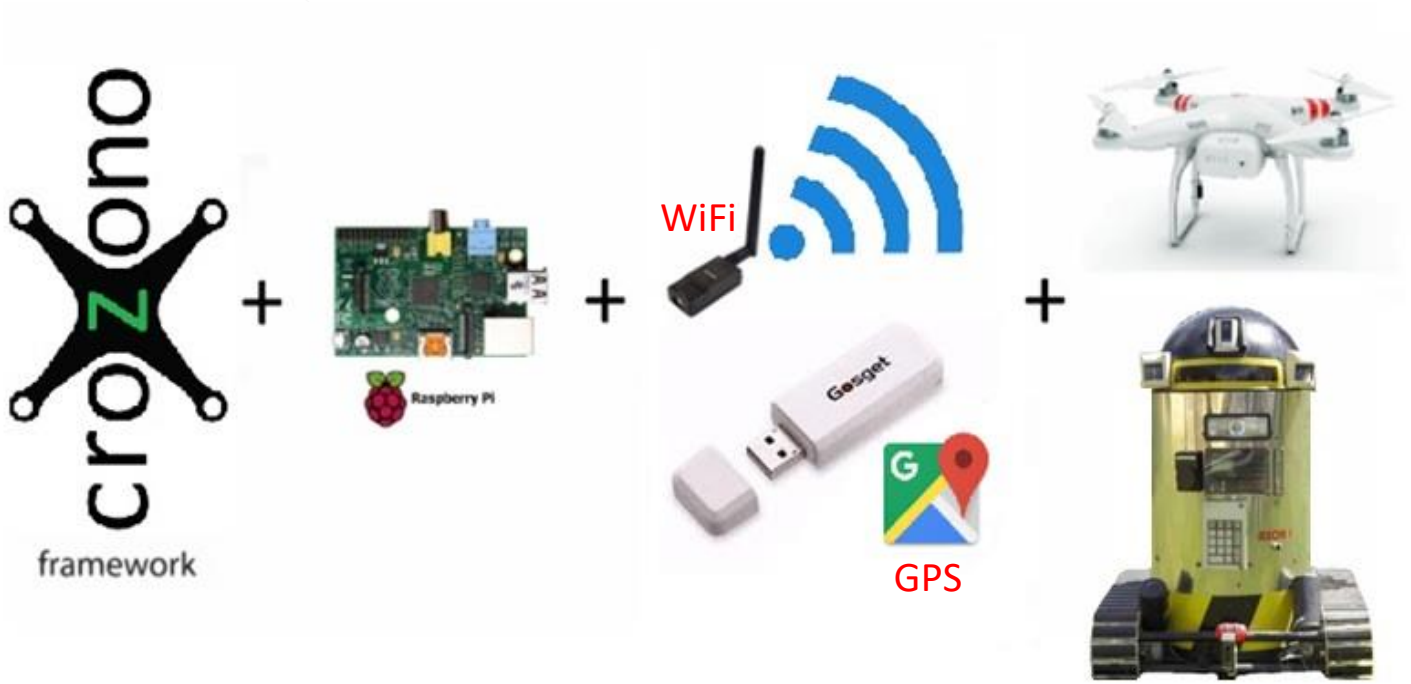
Origen de CROZONO

¿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
seguridad
party, que se
en el Konex.

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

Sheila Berta y Pablo Romanos. Exponen mañana en la cumbre hacki

El día que llegó el futuro

Una réplica del DeLorean, el auto del filme Volver el Futuro 2, des filó ayer por las calles de Tokio. En la película transcurría el año 1985, y los protagonistas viajaban al futuro adelantándose a su tiempo 30 años, exactamente al 21 de octubre de 2015.

Crozono (invento argentino)

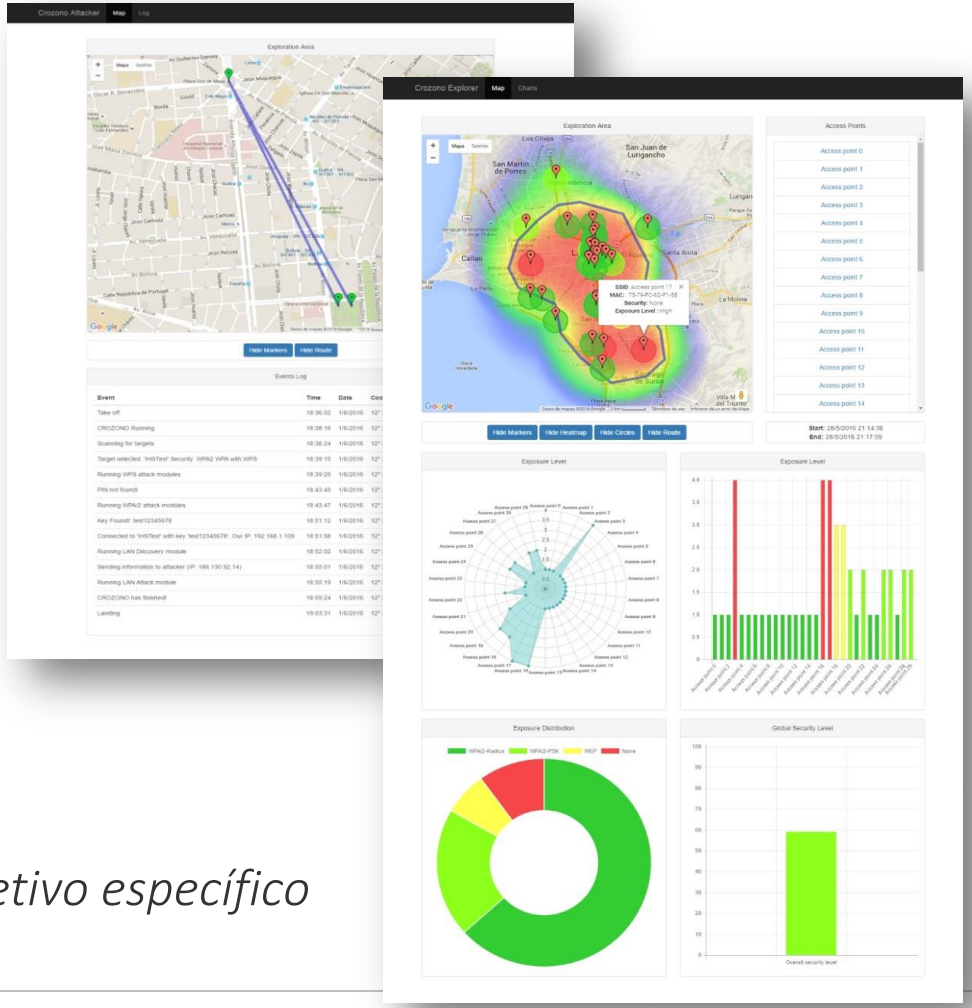
Un dron detecta fallas de seguridad

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

Versiones de CROZONO

Explorer

Relevamiento de información sobre un sector geográfico



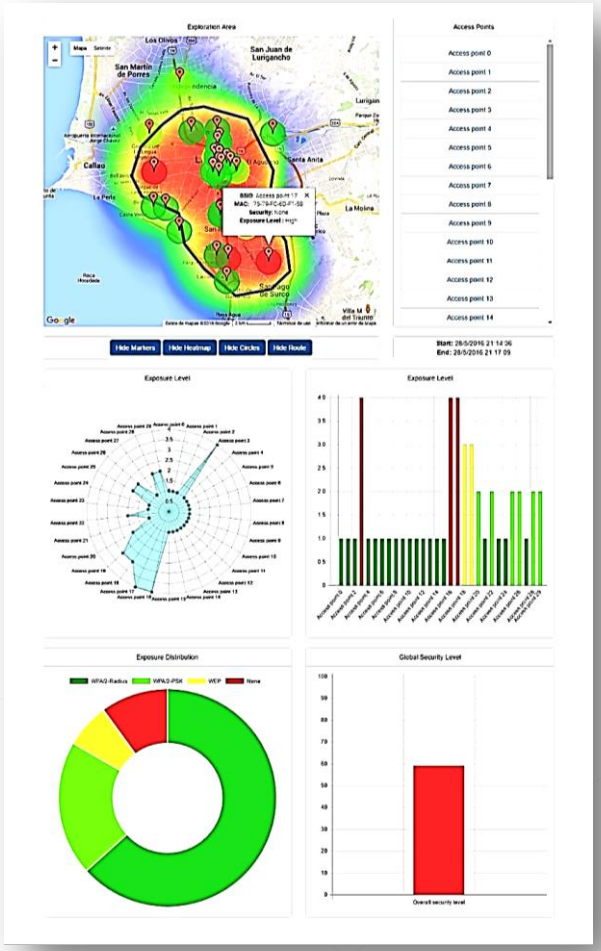
Attacker

Pruebas contra un objetivo específico

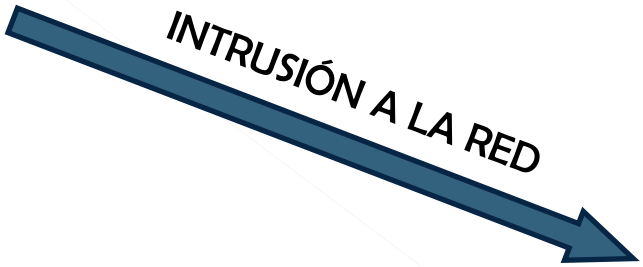
CROZONO Explorer

¿Qué buscar?

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



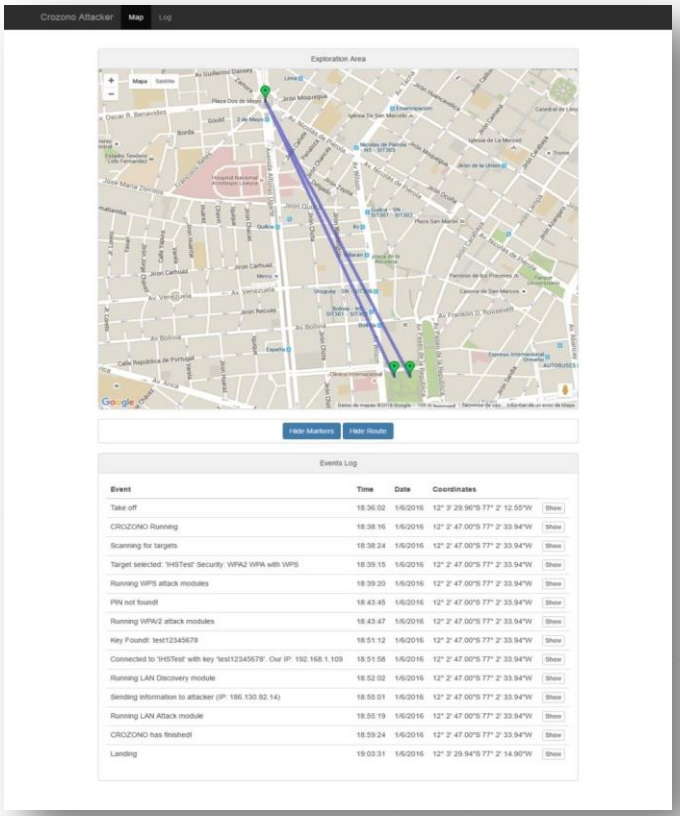
CROZONO Attacker



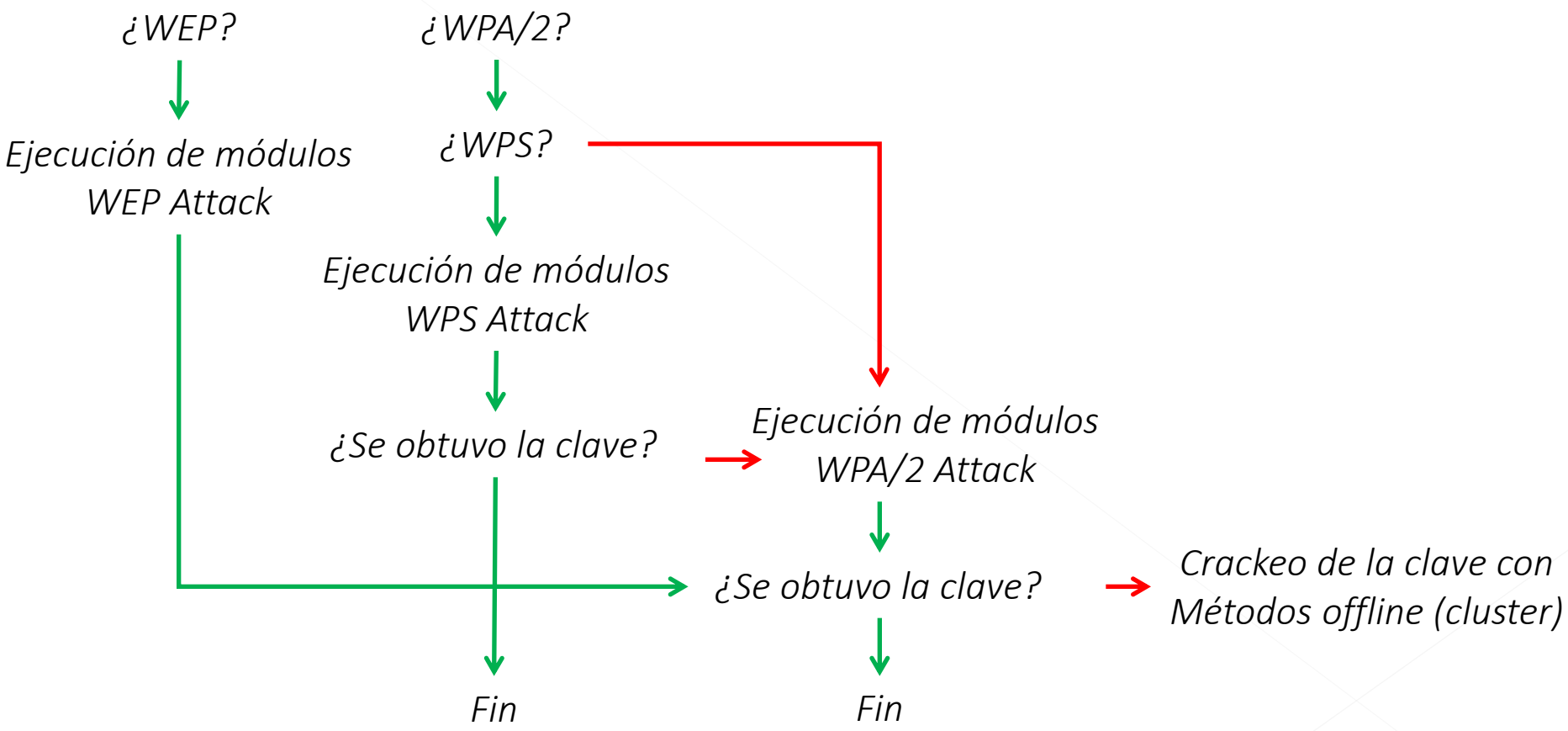
¿ALGÚN OBJETIVO EN ESTE EDIFICIO?

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.



Paso 1: Crackeo Automático WiFi



Paso 2: Conexión Inversa

CONEXIÓN INVERSA

IP: 190.188.65.214:1337

AUDITOR

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

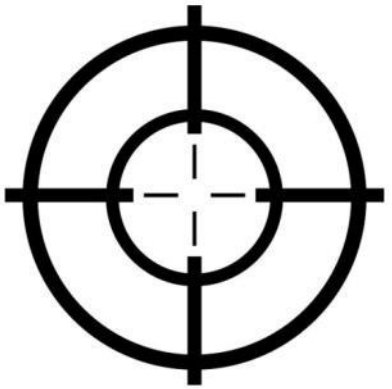
Paso 4: Ataque a la red local

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.



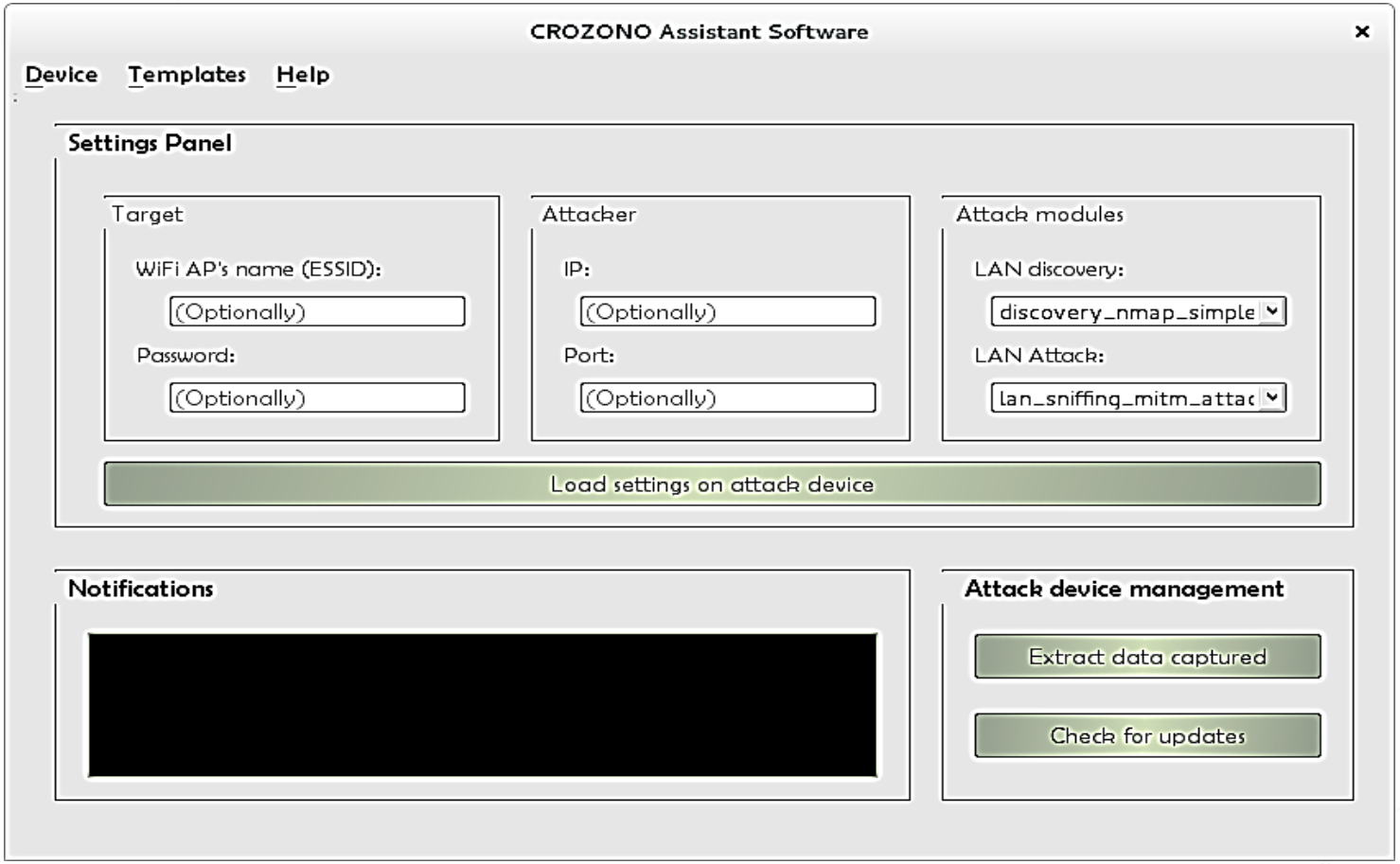
Ejecución de CROZONO Attacker
sin parámetros

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

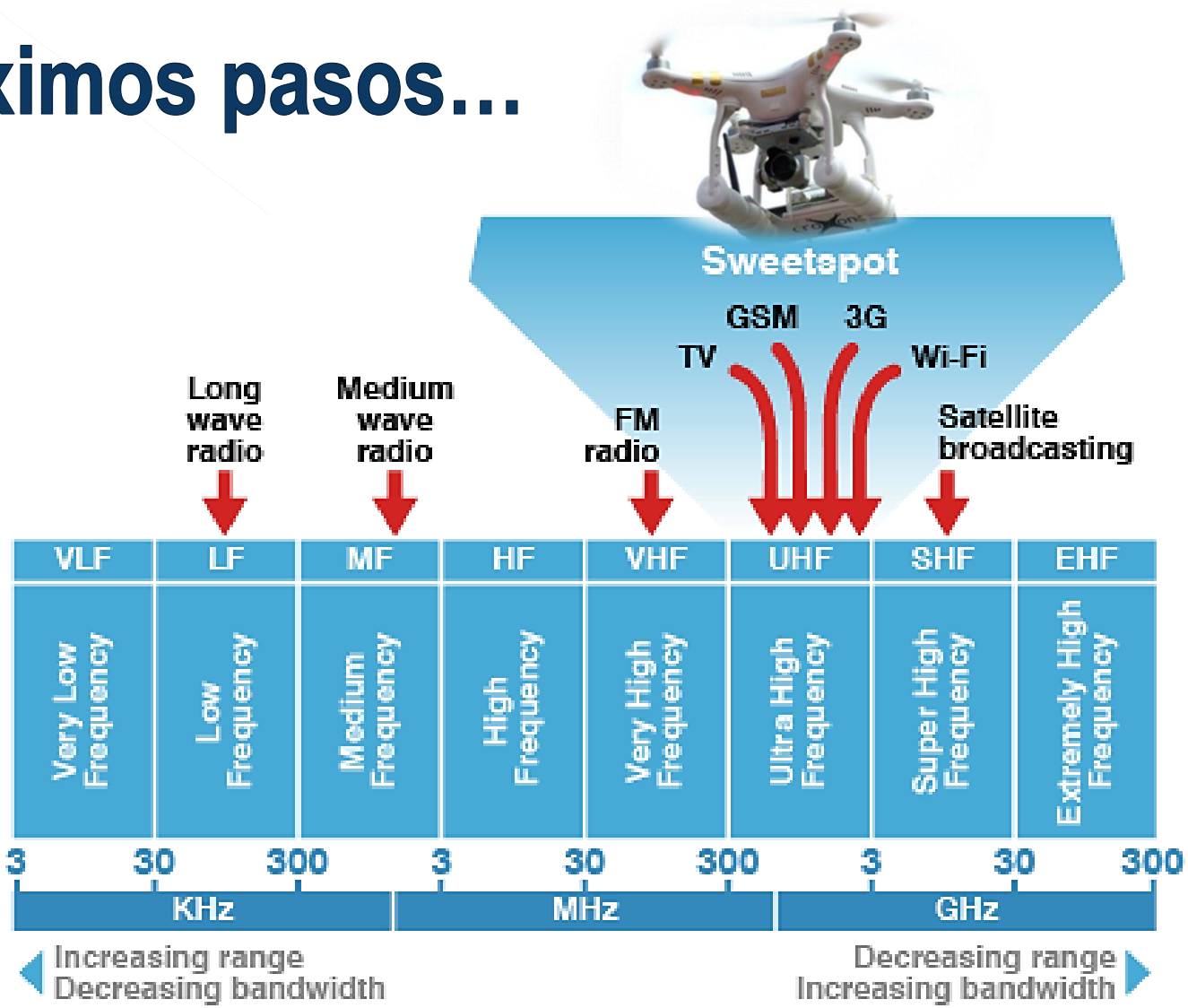


Uso en Fuerzas de Seguridad

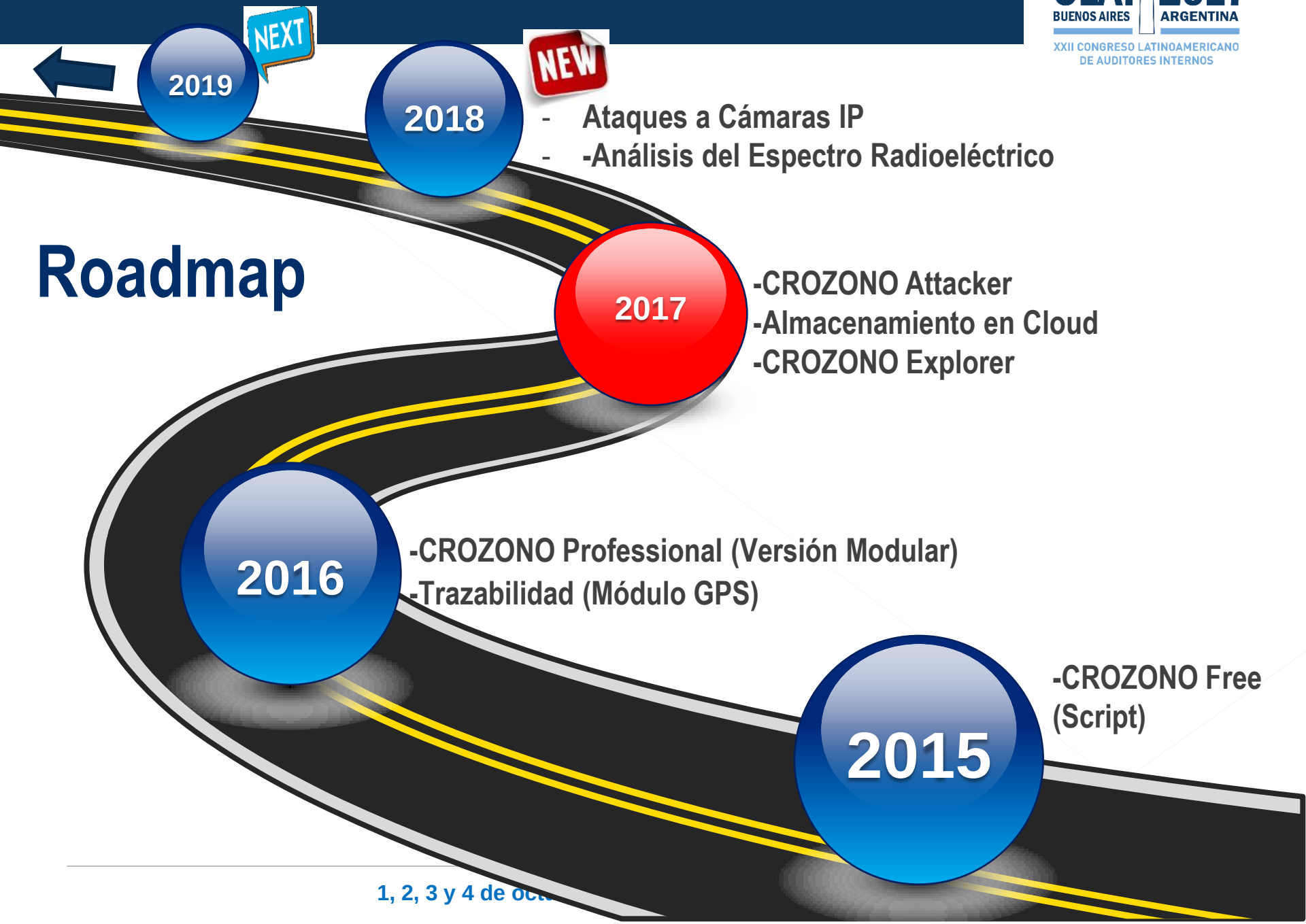
Testing de Infraestructuras Críticas

Video Demo

Próximos pasos…



Roadmap


NEXT
2019
NEW
2018
- 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)

CLAI 2017
BUENOS AIRES ARGENTINA
XXII CONGRESO LATINOAMERICANO DE AUDITORES INTERNOS

Muchas Gracias por su atención

www.crozono.com
info@crozono.com

Los invitamos a compartir sus comentarios en twitter e Instagram:

#CLAI2017 **#ProgresarCompartiendo**