Blue Team Wireless

Madrid. Feb 2026

@vulnexsl
@simonroses

VULNEX

¿YO?

- **Simón Roses Femerling**

- Licenciado en Informática (Suffolk University), Postgrado E-Commerce (Harvard University) y Executive MBA (IE Business School)
- Fundador & CEO, VULNEX www.vulnex.com
- Blog: www.simonroses.com
-  @simonroses | @vulnexsl
- Ex: Microsoft, PwC, @Stake
- Beca del DARPA Cyber Fast Track (CFT) para investigar sobre seguridad en el ciclo de desarrollo de software

  http://www.simonroses.com/es/2014/06/mi-visita-al-pentagono/
- Ponente: Black Hat, DEFCON, RSA, HITB, OWASP, AppSec USA, SOURCE, DeepSec, TECHNET, Mundo Hacker Day
- CEH, CISSP, CSSLP & OSWP

GRACIAS

- Hackplayers / hc0n
- Vosotros!!

OBJETIVOS DEL TALLER

- Seguridad WIFI
  - Defensa
- Tendencias
- Que no cubre:
  - Linux
  - Wireless Ofensivo
  - Wireshark

REPOSITORIO DEL TALLER

- Material seguridad sobre WIFI
- https://github.com/vulnex/BlueTeamWireless

TIPOS DE SEGURIDAD WIFI

- Open -> Sin contraseña, sin cifrado. Inseguro.
- WEP -> Obsoleto. Cuestión de minutos en romper.
- WPA -> Mejor cifrado. En desuso.
- WPA2 -> El mas común hoy en día
- WPA/2 Enterprise -> WIFI corporativa
- WPA3 -> Nuevo estándar (2018)

CERTIFICADOS

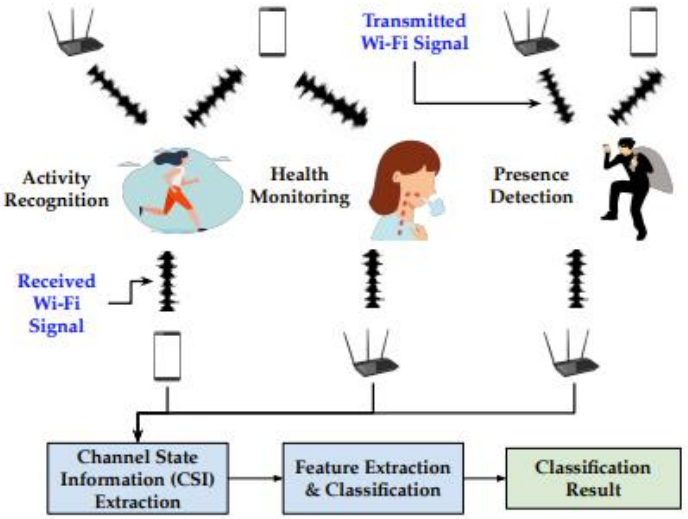
- Offensive Security Wireless Professional (OSWP) https://www.offensive-security.com/wifu-oswp/
- GIAC Assessing and Auditing Wireless Networks (GAWN) - SEC617 https://www.giac.org/certifications/assessing-auditing-wireless-networks-gawn/
- Certified Wireless Security Professional (CWSP) https://www.cwnp.com/certifications/cwsp#:~:text=The%20CWSP%20certification%20is%20a,with%20a%2080%25%20or%20higher.
- PentesterAcademy
- CWP Certification https://github.com/v1s1t0r1sh3r3/airgeddon/wiki/CWP%20Certification

FRECUENCIAS Y CANALES

- 2.4 GHz : 11 Canales (14 total, como en Japón)
  - 2.4 GHz = 802.11 b / g / n / ax
- 5 GHz : 45 Canales
  - 5 GHz = 802.11 a / h / j / n / ac / ax
- 6 Ghz: 1-233 Canales
  - 6 GHz = 802.11 ax
- WIFI 0, 1, 2, 3, 4, 5, 6, 6E, 7 & 8 https://en.wikipedia.org/wiki/Wi-Fi

WI-FI-802.11BF

- "Wi-Fi 7" o "Wi-Fi sensorial" (Wi-Fi Sensing o SENS)
- Septiembre de 2024



- https://arxiv.org/abs/2103.14918

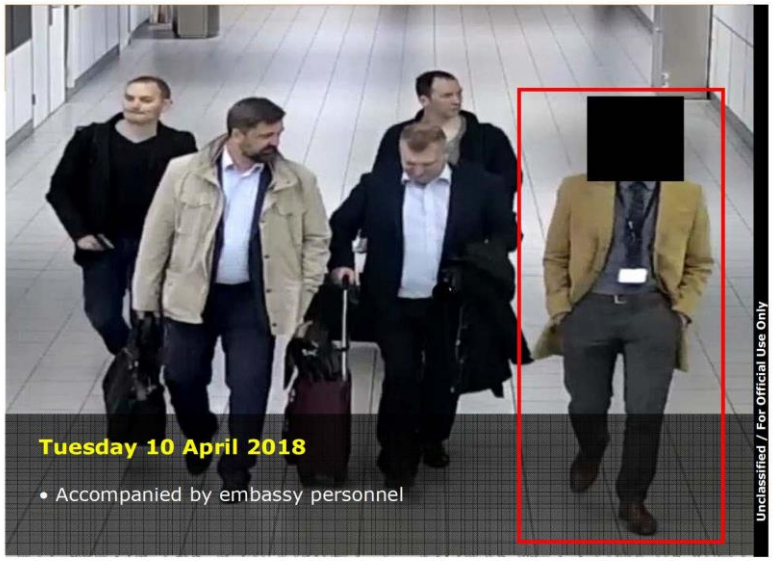
CASO REAL: ALBERT GONZALEZ

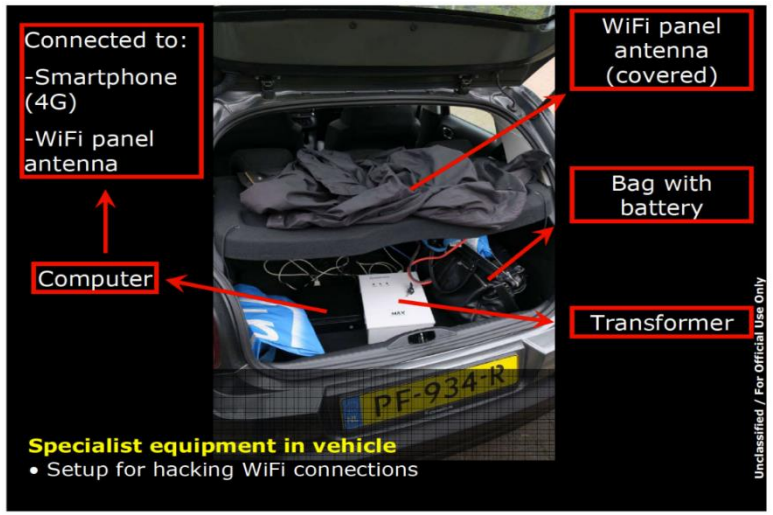
- Robo más de 130 millones tarjetas: TJX, Heartland Payment Systems, 7-Eleven, Hannaford, BJ's, Boston Market, DSW, y OfficeMax
- TJX: ataque inicial mediante WIFI (2005-2006)
- TJX gasto millones en recuperarse de la intrusión
- https://es.wikipedia.org/wiki/Albert_Gonz%C3%A1lez

CASO REAL: GRU RUSIA VS OPCW

- The Organization for the Prohibition of Chemical Weapons (OPCW)

- https://info.publicintelligence.net/NL-MoD-RussianOperationOPCW.pdf





1. BLUE TEAM: ¿QUÉ VIGILAN?

- Redes: Muchos
- WIFI: Algunos
- Bluetooth: Pocos
- Radio: ¿?

1. HOLA MITRE ATT&CK

- T1011 - Exfiltration Over Other Network Medium https://attack.mitre.org/techniques/T1011/

- "the exfiltration may occur, for example, over a WiFi connection, modem, cellular data connection, Bluetooth, or another radio frequency (RF) channel."

RED TEAM WIFI

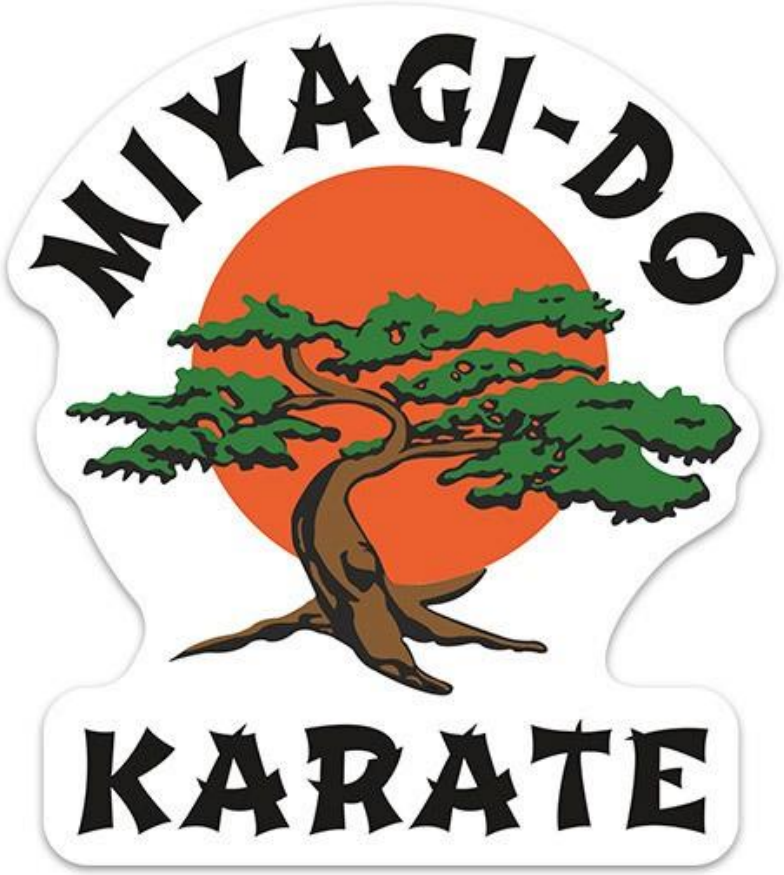
@vulnexsl
@simonroses

VULNEX

HOY NO…

- ☺

BLUE TEAM WIFI



OBJETIVOS DE APRENDIZAJE

- Al finalizar este taller, serás capaz de:

- ✅ Configurar Kismet como IDS inalámbrico
- ✅ Desplegar Nzyme para monitorización WiFi
- ✅ Detectar ataques de desautenticación
- ✅ Identificar evil twins / puntos de acceso falsos
- ✅ Configurar alertas personalizadas
- ✅ Responder a incidentes inalámbricos

WIRELESS BLUE TEAM

- ¿Tenemos capacidad de monitorización?
- ¿Qué tenemos en nuestro perímetro?
- Ataques
  - Rogue AP
  - Deauth
  - Etc.

ENTORNO LABORATORIO I

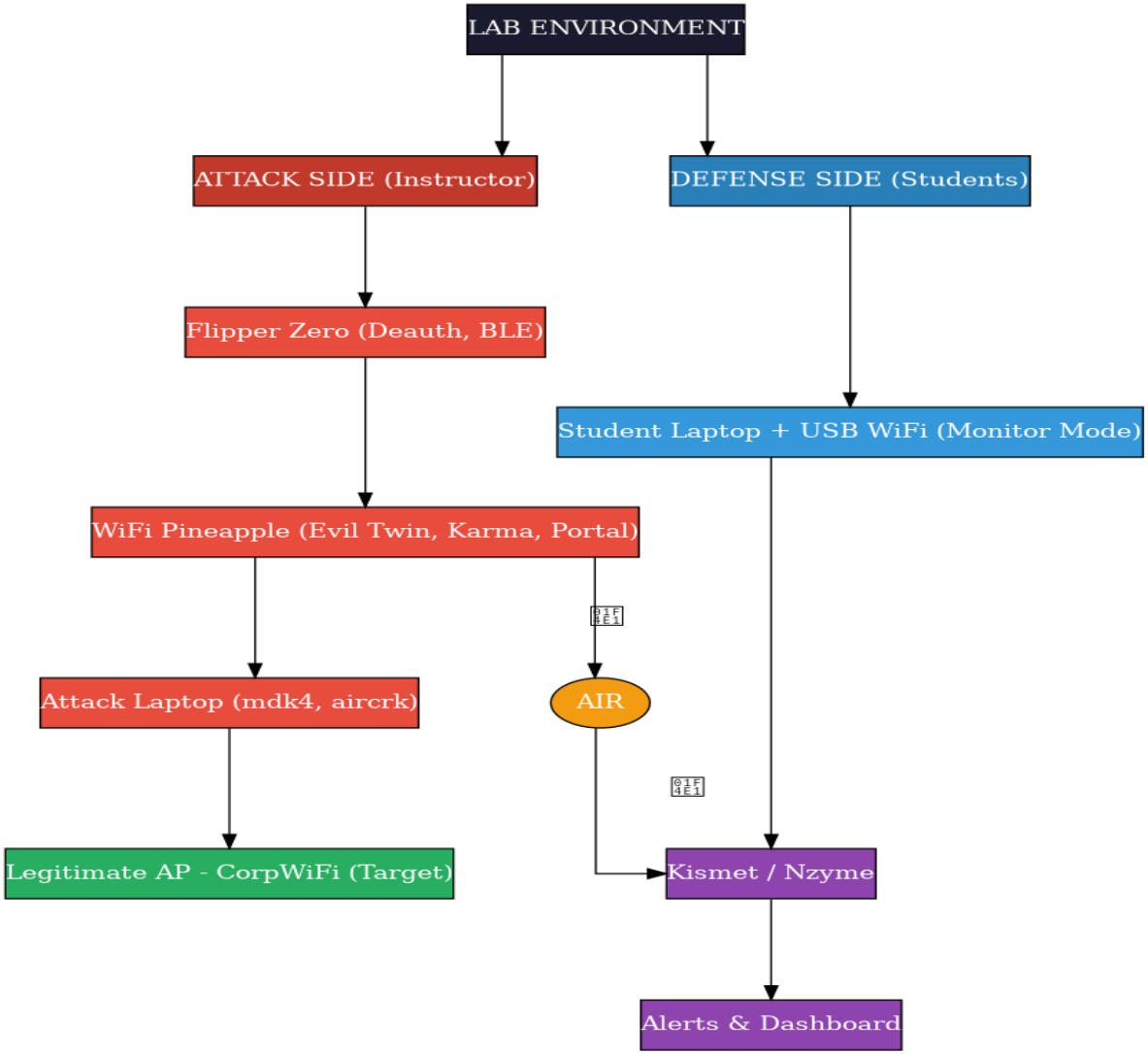
- Atacante (Instructor)

- Ataques Wifi
- Flipper Zero
- WIFI Pineapple
- Pwngotchi

- Estudiante

- Portatil
- Adaptador WIFI (Monitor)
- Kismet
- Nzyme

ENTORNO LABORATORIO II



VERIFICACIÓN RÁPIDA DE CONFIGURACIÓN

```
# Verifica tu adaptador WiFi
iwconfig

# Habilita el modo monitor
sudo ip link set wlan1 down
sudo iw wlan1 set monitor control
sudo ip link set wlan1 up

# o aircrack tools
sudo airmon-ng start wlan1


# Verifica
iwconfig wlan1

# Debería mostrar: Mode:Monitor
```

POR QUÉ LAS REDES INALÁMBRICAS SON VULNERABLES

- El problema fundamental:
  -  Las ondas de radio no se detienen en las paredes
  - Cualquiera en el rango puede capturar tráfico
  - Los frames de gestión están **sin cifrar**
  - Fácil suplantar dispositivos
  - No se requiere acceso físico

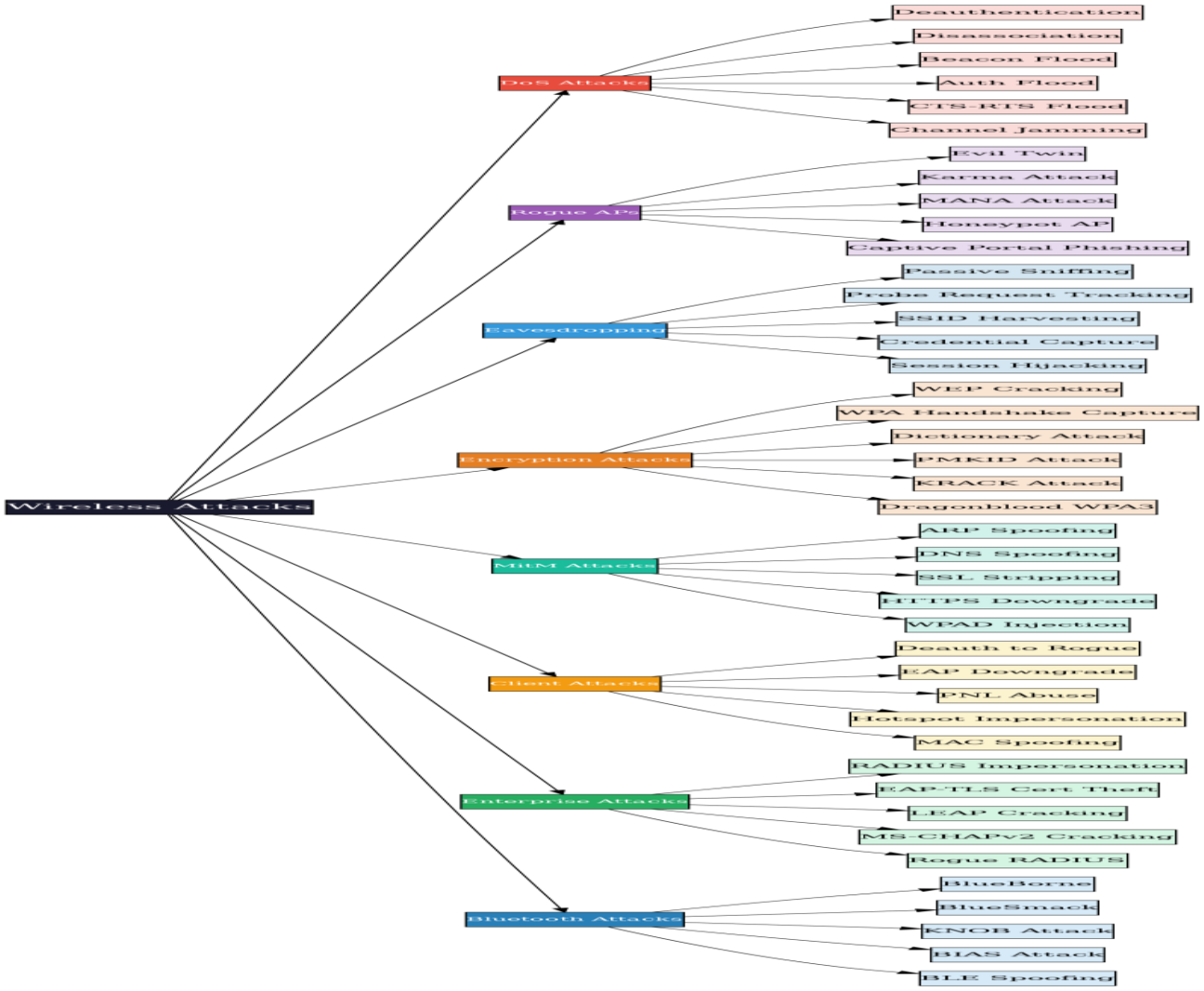
TIPOS FRAMES 802.11

Tipo	Propósito	¿Protegido?
Gestión	Auth, Assoc, Beacon, Deauth	❌ No*
Control	ACK, RTS, CTS	❌ No
Datos	Tráfico real	✅ Sí (WPA2/3)

HERRAMIENTAS DE LOS ATACANTES

Herramienta	Plataforma	Ataques
WiFi Pineapple	Hardware	Evil twin, Karma
Flipper Zero	Hardware	Deauth, BLE
Aircrack-ng	Software	Crack WPA, deauth
mdk4	Software	DoS, inundación beacon
Bettercap	Software	MitM, sniffing
airgeddon	Software	Muchos, automatizados

CATEGORÍAS DE ATAQUES



@vulnexsl
@simonroses

VULNEX

DENEGACIÓN DE SERVICIO (DOS)

- **Ataques**: - Inundación de desautenticación - Ataque de disociación - Inundación de beacons - Interferencia de canal
- **Impacto**: Red no disponible
- **Detección**: Anomalías en la tasa de frames

PUNTOS DE ACCESO FALSOS

- **Ataques**: - Evil Twin - Karma / MANA - Honeypot AP - Phishing con portal cautivo
- **Impacto**: Robo de credenciales, MitM
- **Detección**: Discrepancia BSSID/SSID

ESPIONAJE

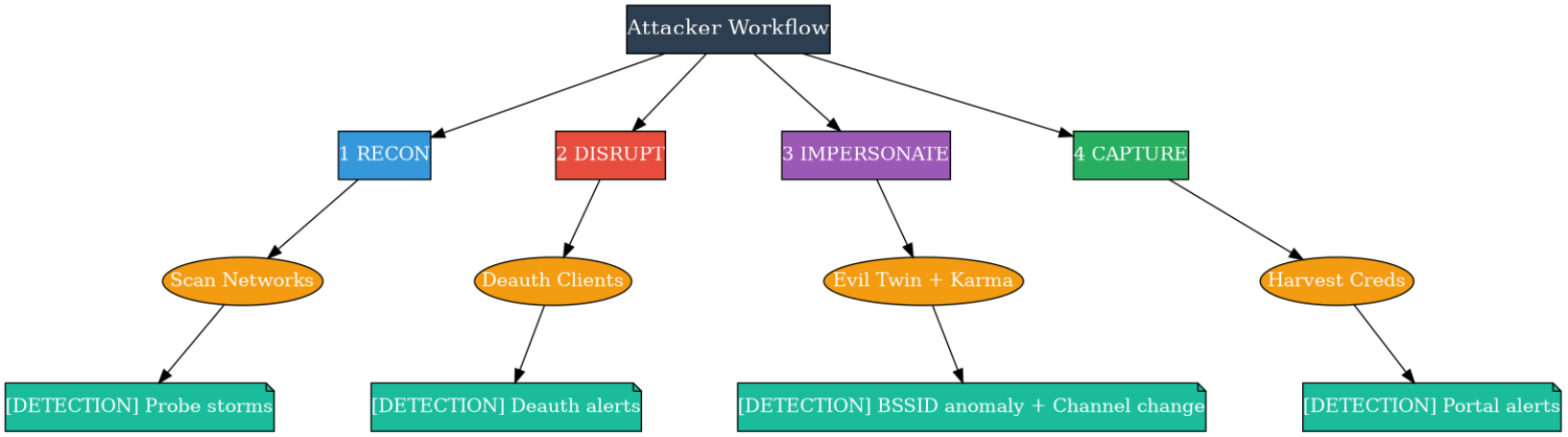
- **Ataques**: - Sniffing pasivo - Rastreo de probe requests - Recolección de SSIDs - Captura de credenciales
- **Impacto**: Violación de privacidad, recopilación de inteligencia
- **Detección**: Comportamiento inusual de probes

ATAQUES DE CIFRADO

- **Ataques**: - Cracking de WEP - Captura de handshake WPA - Ataque PMKID - KRACK, Dragonblood
- **Impacto**: Compromiso de red
- **Detección**: Fuerza bruta WPS, handshakes inusuales

SEQUENCIA DE ATAQUE

1. **RECONOCIMIENTO** → Escanear redes
2. **INTERRUPCIÓN** → Desautenticar clientes
3. **SUPLANTACIÓN** → Evil twin
4. **CAPTURA** → Cosechar credenciales



ESTRATEGIA DE DEFENSA

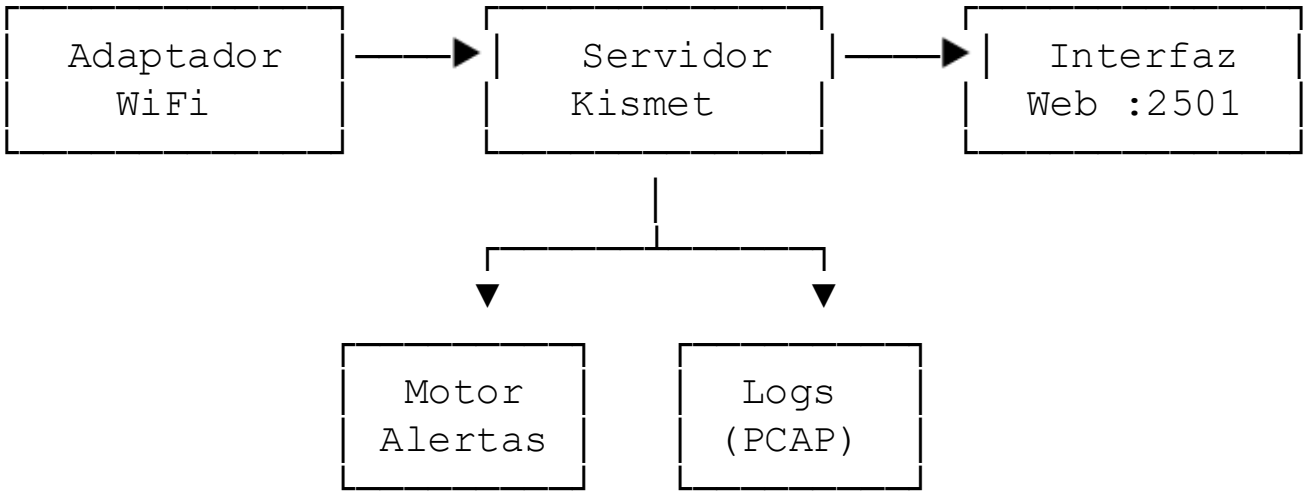
1. **Detectar** → Kismet, Nzyme (enfoque de hoy)
2. **Prevenir** → 802.11w, WPA3, 802.1X
3. **Responder** → Localizar, eliminar, documentar
4. **Mejorar** → Entrenamiento de usuarios, políticas

KISMET

¿QUÉ ES KISMET?

- Herramienta de detección inalámbrica de código abierto
- Sniffer pasivo y captura de paquetes
- IDS inalámbrico (WIDS)
- Soporta: WiFi, Bluetooth, Zigbee, y más
- Interfaz web
- API REST para integración
- https://www.kismetwireless.net

ARQUITECTURA DE KISMET



INICIAR KISMET

```
# Inicio básico
kismet -c wlan1

# Interfaz Web
http://localhost:2501

# Primera ejecución: Crear
usuario admin
```

INTERFAZ WEB DE KISMET

Pestaña	Propósito
Devices	Todos los APs + clientes descubiertos
SSIDs	Nombres de red vistos
Alerts	Alertas de seguridad ⚠
Datasources	Interfaces de captura
Packets	Estadísticas en vivo

INFORMACIÓN DEL DISPOSITIVO

- Para cada dispositivo descubierto:
  - Dirección MAC + Fabricante (OUI)
  - SSID (si es AP)
  - Canal
  - Cifrado (Abierto/WPA2/WPA3)
  - Intensidad de Señal (RSSI)
  - Primera/Última Vez Visto
  - Clientes Asociados

ALERTAS DE KISMET I

- Dos Tipos:
  - **Fingerprint** - Patrones de ataque conocidos
  - **Tendencia/Stateful** - Anomalías de comportamiento

ALERTAS DE KISMET II

Alerta	Tipo	Detecta
DEAUTHFLOOD	Tendencia	DoS de Deauth
APSPOOF	Fingerprint	Evil Twin
CRYPTODROP	Tendencia	Degradación de cifrado
KARMAOUI	Fingerprint	Ataque Karma (00:13:37)
WPSBRUTE	Tendencia	Fuerza bruta WPS
CHANCHANGE	Tendencia	Canal del AP cambió

CONFIGURAR ALERTAS

- **Archivo de configuración:**

/etc/kismet/kismet_site.conf

```
# Formato:
alert=NOMBRE,tasa/tiempo,ráfaga
alert=DEAUTHFLOOD,10/min,5/sec
alert=APSPOOF,5/min,1/sec

# Definir APs legítimos
apspoof=CorpWiFi:ssid="CorpWiFi",
validmacs="AA:BB:CC:DD:EE:FF"
```

CONFIGURACIÓN DE APSPOOF

- **Lista blanca de tus APs legítimos:**

```
# Coincidencia exacta de MAC
apspoof=Corp:ssid="CorpWiFi",validmacs="AA:BB:CC:D
D:EE:FF"

# Múltiples MACs
apspoof=Corp:ssid="CorpWiFi",validmacs="AA:BB:CC:D
D:EE:FF,AA:BB:CC:DD:EE:00"

# Máscara MAC (coincidencia OUI)
apspoof=Corp:ssid="CorpWiFi",validmacs="AA:BB:CC:0
0:00:00/FF:FF:FF:00:00:00”
```

¡Cualquier otra MAC anunciando “CorpWiFi” = ALERTA!

API DE KISMET

```
# Obtener todos los dispositivos
curl
http://localhost:2501/devices/all_d
evices.json

# Obtener alertas
curl
http://localhost:2501/alerts/all_al
erts.json

# Usar para integración con SIEM
```

LAB 1: CONFIGURACIÓN DE KISMET

- **Ejercicio Práctico**

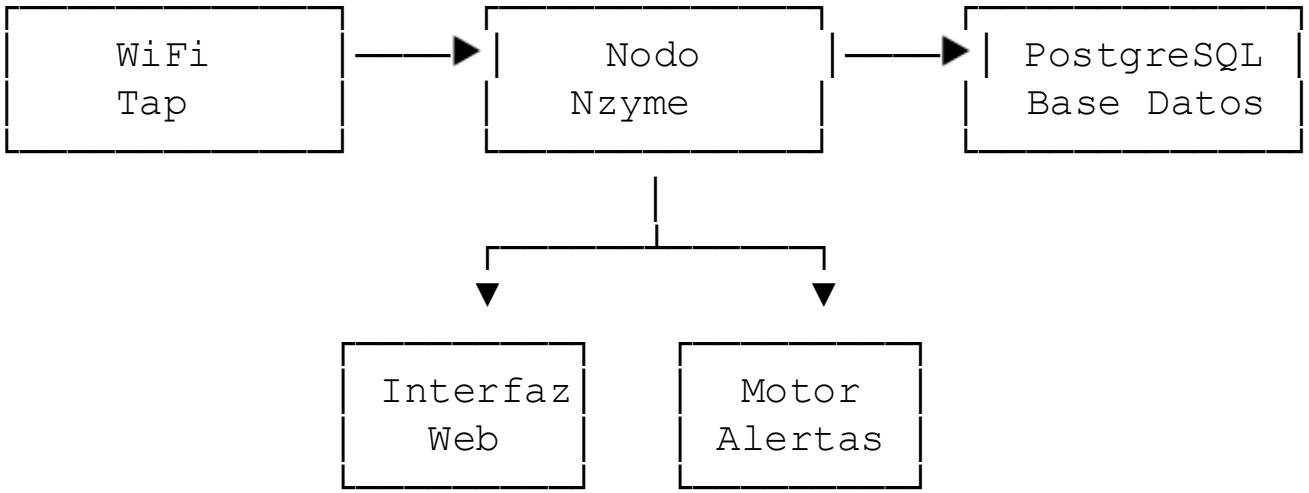
1. Inicia Kismet con tu adaptador
2. Accede a la interfaz web
3. Verifica que la captura funciona
4. Encuentra “CorpWiFi” en la lista de dispositivos
5. Revisa la pestaña de Alertas
    1. Ver: *LAB1-kismet-setup.md*

NZYME

¿QUÉ ES NZYME?

- Sistema de Defensa WiFI
- Monitorización inalámbrica en tiempo real
- Detección de evil twins
- Detección de ataques de desautenticación
- Panel web moderno
- Alertas e informes de cumplimiento
-  https://www.nzyme.org

ARQUITECTURA DE NZYME



CONCEPTOS CLAVE DE NZYME

- **Redes Monitorizadas**: - SSIDs que posees/gestionas - BSSIDs esperados (direcciones MAC) - Canales esperados - Seguridad esperada

- **Trampas (Traps)**: - Reglas de detección - Se activan con anomalías

TRAMPAS

Trampa	Detecta
`unexpected_bssid`	Evil twin (nueva MAC para SSID conocido)
`unexpected_channel`	AP en canal incorrecto
`unexpected_security`	Discrepancia de cifrado
`deauth_monitor`	Inundación de deauth
`unknown_ssid`	AP falso

TRAMPAS - CONFIGURAR REDES

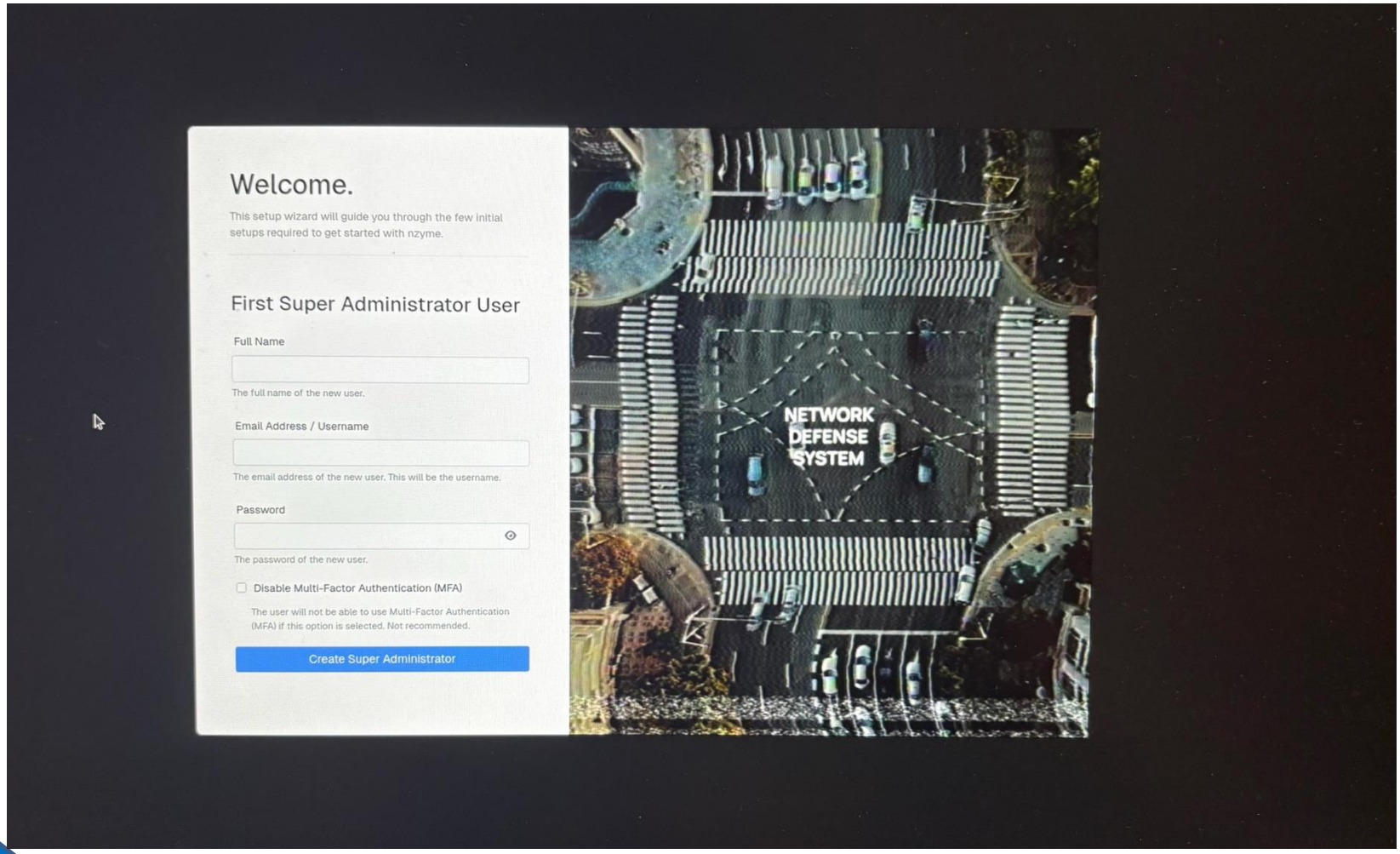
```
dot11.networks = [
   {
      ssid = "CorpWiFi"
      bssids = ["AA:BB:CC:DD:EE:FF"]
      channels = [6]
      security = ["WPA2-PSK"]
   }
]
```

- Cualquier cosa fuera de esta definición = sospechoso

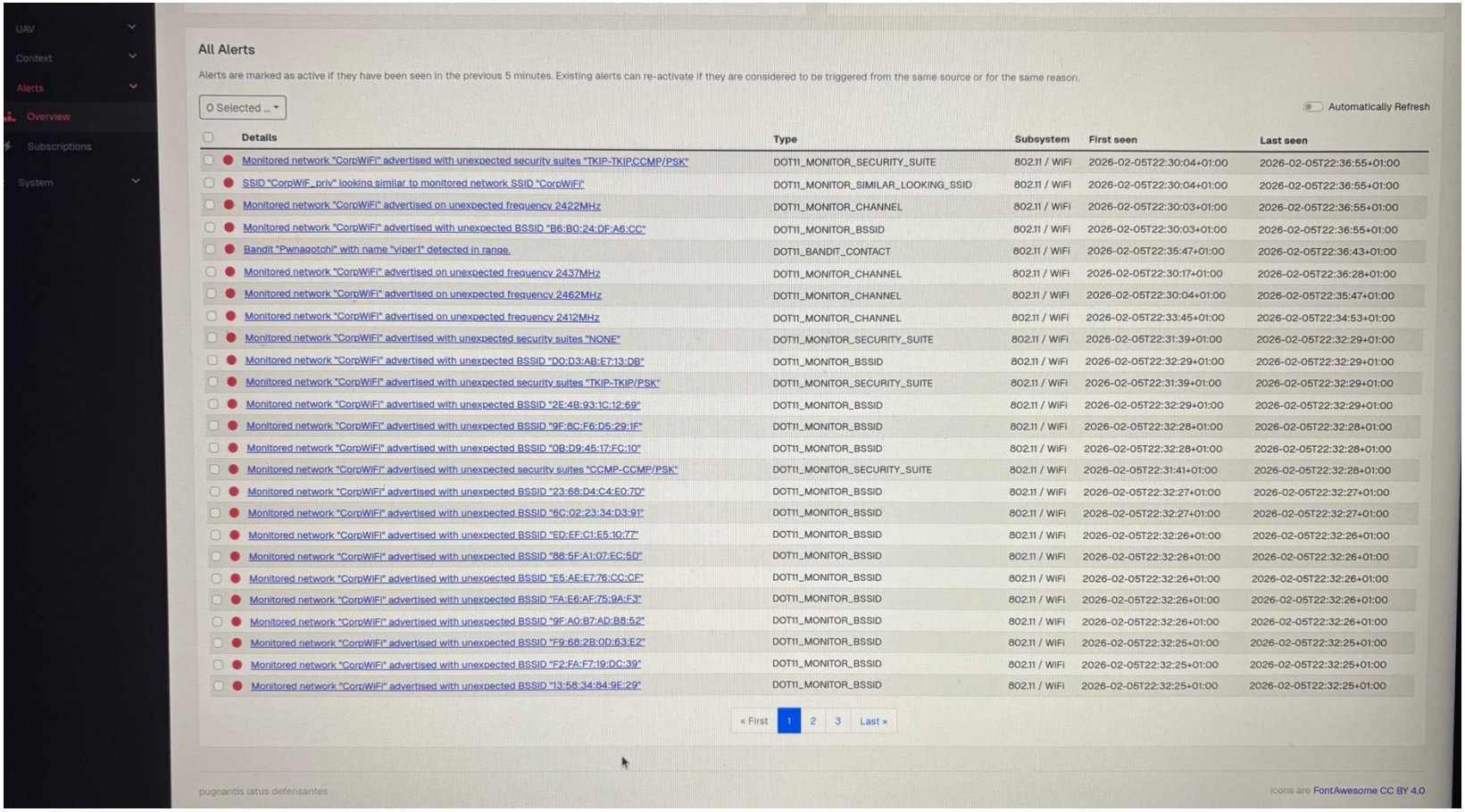
PANEL DE NZYME

- **Secciones Clave:**
  - Overview - Salud del sistema
  - Networks - SSIDs monitorizados
  - Alerts - Eventos de detección
  - Taps - Interfaces de captura
  - Compliance - Informes

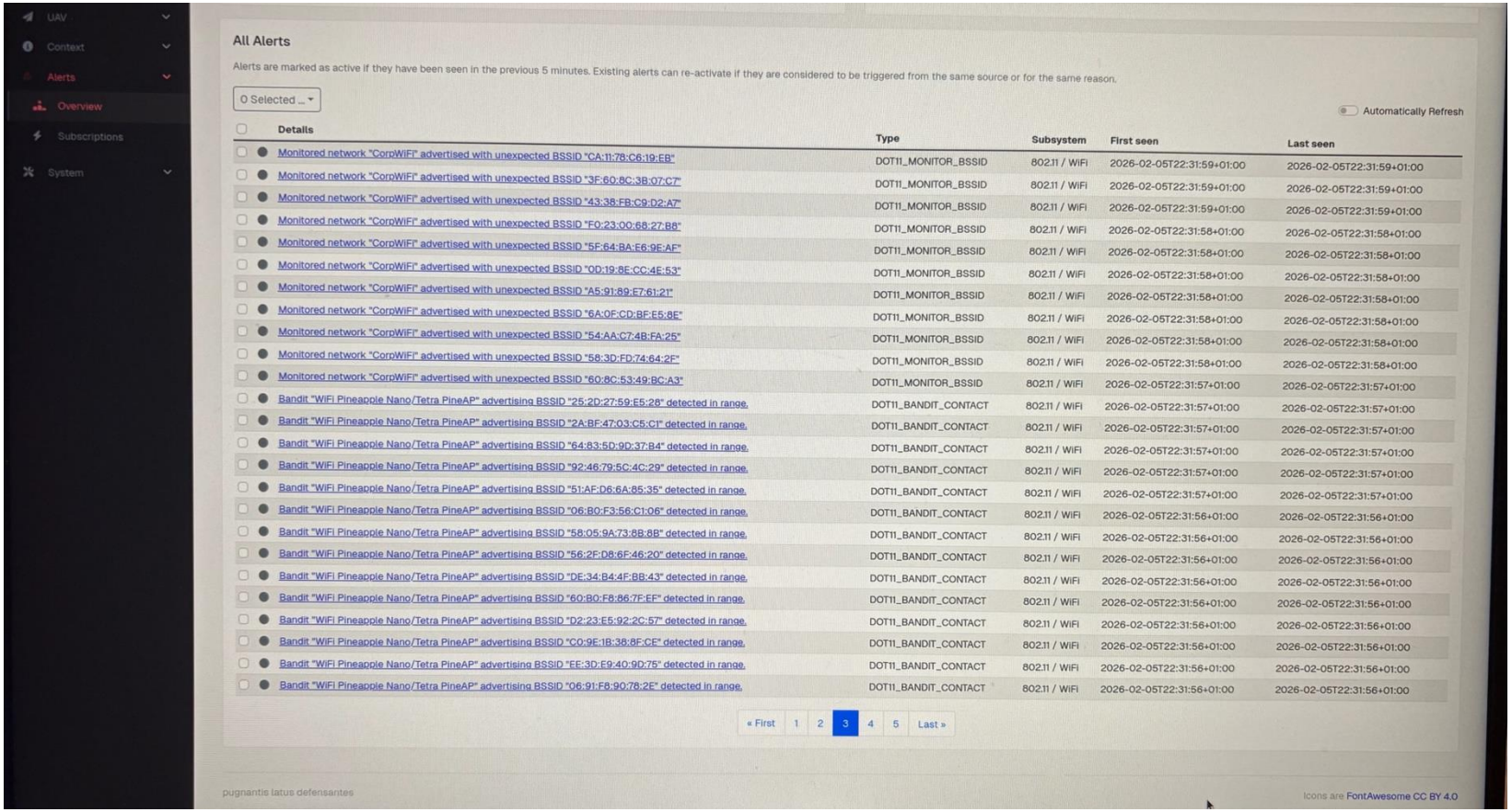
NZYME LOGIN


Welcome.
This setup wizard will guide you through the few initial setups required to get started with nzyme.
First Super Administrator User
Full Name
The full name of the new user.
Email Address / Username
The email address of the new user. This will be the username.
Password
The password of the new user.
Disable Multi-Factor Authentication (MFA)
The user will not be able to use Multi-Factor Authentication (MFA) if this option is selected. Not recommended.
Create Super Administrator
NETWORK
DEFENSE
SYSTEM

NZYME ALERTS I



NZYME ALERTS II



LAB 2: CONFIGURACIÓN DE NZYME

- **Ejercicio Práctico**

1. Verifica que Nzyme está corriendo
2. Accede al panel
3. Configura red monitorizada
4. Habilitas trampas de detección
5. Prueba que la captura funciona
    1. Ver: *LAB2-nzyme-setup.md*

KIMSET + NZYME

- **¡Usa ambos! Se complementan.**

Característica	Kismet	Nzyme
Enfoque	Herramienta inalámbrica general	Defensa/IDS WiFi
UI	Web (funcional)	Web (moderna)
Alertas	Básicas	Avanzadas
Lista Blanca de Redes	Configuración manual	Basada en UI
Cumplimiento	Limitado	PCI, NIST, CIS
Despliegue	Nodo único	Distribuido

LABORATORIOS PRÁCTICOS DE DETECCIÓN

Lab	Ataque	Herramienta
LAB 3	Desautenticación	mdk4 / aireplay-ng
LAB 4	Evil Twin	WiFi Pineapple
LAB 5	AP Falso	hostapd

TU TRABAJO

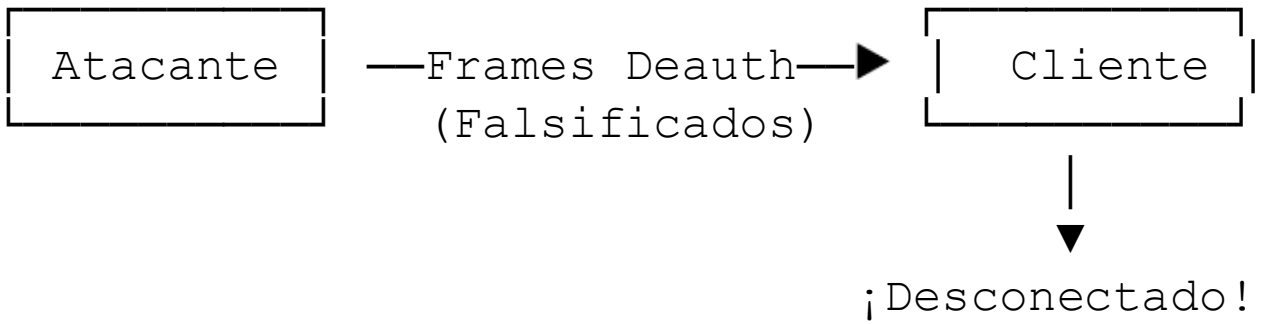
- **¡Detectarlos todos!**

LAB 3: DETECCIÓN DE DEAUTH

- **Ejercicio Práctico**

1. **Ataque**: El instructor envía inundación de deauth
2. **Detectar con Kismet**: - Observa la pestaña Alertas - Busca DEAUTHFLOOD
3. **Detectar con Nzyme**: - Observa el panel de Alertas - Busca DEAUTH_FLOOD
    1. Ver: *LAB3-detect-deauth.md*

ATAQUE DE DEAUTH EXPLICADO



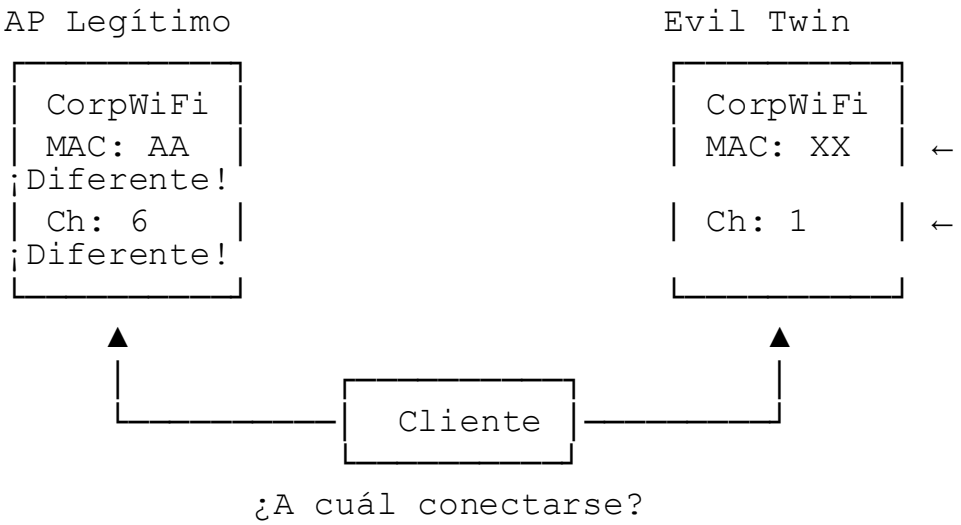
- **Por qué funciona:** - Frames de gestión sin cifrar - Cliente confía en deauth del “AP” - No se requiere autenticación

LAB 4: DETECCIÓN DE EVIL TWIN

- **Ejercicio Práctico**

1. **Ataque**: El instructor crea un "CorpWiFi" falso
2. **Detectar con Kismet**: - Busca APSPOOF - Compara BSSIDs en la pestaña Dispositivos
3. **Detectar con Nzyme**: - Busca UNEXPECTED_BSSID - Verifica sección Redes
    1. Ver: *LAB4-detect-evil-twin.md*

ATAQUE EVIL TWIN EXPLICADO



LAB 5: DETECCIÓN DE AP FALSO

- **Ejercicio Práctico**

1. **Ataque**: El instructor despliega un AP no autorizado
2. **Detectar con Kismet**: - Nuevo dispositivo en la pestaña Dispositivos - Verificar contra inventario
3. **Detectar con Nzyme**: - Busca UNKNOWN_SSID - Verifica redes no monitorizadas
    1. Ver: *LAB5-detect-rogue-ap.md*

LOCALIZAR ATACANTES

- Usa la intensidad de señal (RSSI):

RSSI	Distancia
-30 dBm	Muy cerca (misma habitación)
-50 dBm	Cerca
-70 dBm	Media
-90 dBm	Lejos

- **Técnica**: ¡Camina hacia señal más fuerte!

ALERTAS

Ataque	Alerta Kismet	Alerta Nzyme
Deauth	DEAUTHFLOOD	DEAUTH_FLOOD
Evil Twin	APSPOOF	UNEXPECTED_BSSID
AP Falso	DEVICEFOUND	UNKNOWN_SSID
Karma	KARMAOUI	UNEXPECTED_BSSID
WPS Brute	WPSBRUTE	-

LO QUE HEMOS CUBIERTO

- Temas:

- ✅ Panorama de ataques inalámbricos
- ✅ Vulnerabilidades 802.11
- ✅ Configuración de Kismet
- ✅ Despliegue de Nzyme
- ✅ Detección de ataques de desautenticación
- ✅ Detección de evil twins
- ✅ Detección de APs falsos
- ✅ Fundamentos de respuesta a incidentes

CONTRAMEDIDAS

- **Técnicas**: - Habilitar 802.11w (MFP) - Desplegar WPA3 - Usar 802.1X/EAP-TLS - Monitorización continua

- **Operacionales**: - Auditorías inalámbricas regulares - Inventario de activos - Plan de respuesta a incidentes - Entrenamiento de concienciación de usuarios

PRÓXIMOS PASOS

1. **Desplegar** Kismet/Nzyme en tu entorno
2. **Inventariar** todos los APs legítimos
3. **Configurar** alertas para tus SSIDs
4. **Integrar** con SIEM si está disponible
5. **Probar** regularmente con ataques controlados
6. **Entrenar** a tu equipo

RECURSOS

- https://book.hacktricks.xyz/generic-methodologies-and-resources/pentesting-wifi
- https://foxglovesecurity.com/2016/02/24/when-whales-fly-building-a-wireless-pentest-environment-using-docker/

Q&A

- ¡Gracias!
- ¡Cervezas y copas son bienvenidas!
- 𝕏 @simonroses
- 𝕏 @vulnexsl

- www.vulnex.com
- www.simonroses.com
- https://github.com/vulnex/BlueTeamWireless