Reporte Técnico de Auditoría Wi-Fi – RootNet Coffee

Sebastian Bulla Matallana / Hacking ëtico

1. Objetivo de la Auditoría

Evaluar la seguridad de las redes Wi-Fi del café RootNet Coffee para identificar vulnerabilidades, realizar pruebas controladas y proponer medidas correctivas que garanticen la privacidad de los usuarios y la continuidad del negocio.

2. Plan de Trabajo

Fase A – Análisis Inicial

1. **Conectarse desde una máquina virtual** con **Kali Linux**.
2. Configurar el adaptador inalámbrico en **modo monitor** para escuchar todo el tráfico de red.
3. Identificar las redes disponibles (SSID, canal, nivel de señal) con herramientas como:
    - **Vistumbler** (Windows)
    - **Airmon-ng / Airodump-ng** (Kali Linux)

Fase B – Escaneo y Descubrimiento

1. **Ejecutar Nmap**
    - Objetivo: detectar dispositivos conectados, puertos abiertos y servicios activos.

    Comando base:

    - nmap -sS -sV -O 192.168.0.0/24
2. **Usar Kismet**
    - Monitorear actividad inalámbrica y detectar posibles puntos de acceso no autorizados (rogue APs).
3. **Comparar Router vs Access Point**
    - Determinar si los equipos del cliente están configurados correctamente o presentan fallos de aislamiento de tráfico entre clientes.

Fase C – Captura y Análisis de Paquetes

1. **Usar Wireshark**
    - Analizar tráfico para identificar protocolos inseguros (HTTP, FTP, Telnet).
    - Detectar posibles fugas de información o intentos de conexión sospechosos.
2. **Aircrack-ng Suite**
    - Verificar el nivel de cifrado (WEP, WPA, WPA2 o WPA3).
    - Intentar romper contraseñas débiles de manera **controlada y ética** con autorización del cliente.

Fase D – Validación de Seguridad

1. **Probar el firewall actual**
    - Identificar si filtra correctamente paquetes entrantes/salientes.
    - Ver si detecta y bloquea ataques simples (ej. ping flood con hping3 -S --flood 192.168.0.1).
2. **Flipper Zero (opcional)**
    - Revisar exposición de señales inalámbricas adicionales (RFID, Bluetooth, IR).

3. Recomendaciones Técnicas

Área	Recomendación
Segmentación de red	Separar red de **clientes**, **administradores** y **dispositivos IoT** mediante VLANs.
Firewall	Implementar o actualizar un **firewall perimetral** que registre y bloquee conexiones sospechosas.
Equipos obsoletos	Sustituir el **router Cisco Linksys viejo** por un modelo con soporte **WPA3** y actualizaciones de firmware.
Contraseñas y cifrado	Usar contraseñas robustas y protocolos **WPA2-Enterprise o WPA3**. Evitar WEP o WPA antiguo.
Monitoreo continuo	Instalar herramientas de detección de intrusos (IDS/IPS) como **Snort** o **Zeek**.
Pruebas periódicas	Realizar auditorías trimestrales con **Kali Linux** y herramientas complementarias.

4. Conclusiones

La auditoría permitirá:

- Identificar vulnerabilidades de configuración, cifrado y segmentación.
- Probar de forma controlada la exposición de las redes Wi-Fi.
- Reforzar la infraestructura de RootNet Coffee para garantizar un entorno seguro y eficiente tanto para clientes como para empleados.