Wireless 802.11 “El Otro Lado”

\
Ezequiel Sallis CISSP/CEH/MBCI
esallis(AT)root-secure.com
Root-Secure Director

Introducción:

Mucho se ha hablado de los riesgos asociados a las tecnologías inalámbricas 802.11, pero de un tiempo a esta parte las técnicas de ataque parecen haber incorporado dentro de sus objetivos al usuario final, algo que no sorprende si analizamos la tendencia de los ataques de los últimos tiempos.

Asistiendo a Defcon 16 en Agosto de 2008, la sala se lleno de exclamaciones cuando uno de los creadores de Aircrak-ng (Una de las suites de análisis de redes inalámbricas 802.11 mas reconocidas) anunciaba las novedosas funcionalidades de su herramienta, las cuales tenían por objetivo “el otro lado” de la infraestructura 802.11, es decir, el usuario final. De ahí en más proliferaron otras tantas herramientas y scripts en su gran mayoría basadas en “Karma”, la primer herramienta que implemento el concepto aproximadamente en el 2005.

Es verdad, lo se, quizá aun redoblan los tambores por las tradicionales técnicas de ataque a las redes 802.11. Como olvidar los ya conocidos ataques a las debilidades de WEP, o bien a WPA/WP2 y los ataques de diccionario, si aun se ven grandes cantidades de redes inalámbricas vulnerables a estos, pero bueno quizá también, sea hora de mirar mas allá de estos y ver donde irán a asestar el próximo golpe

De qué estamos hablando entonces?

Imaginemos por un momento la siguiente situación: un usuario enciende su ordenador en el aeropuerto o en un bar, con el objetivo de leer algunos documentos de trabajo que debe presentar en su próxima reunión. Claro está, estos documentos están en su equipo y el usuario no tiene necesidad alguna de establecer ninguna conexión, ahora bien, sucede que en ese mismo aeropuerto o bar se encuentra alguien con malas intenciones, por lo que para poder extraer algo de información sensible de equipos de usuarios desprevenidos, levanta un punto de acceso inalámbrico desde su portátil buscando que mediante la debilidad de conexión automática a redes inalámbricas preferidas, presentes por defecto en la mayoría de los sistemas operativos, este usuario se conecte a el punto de acceso ofrecido, el final de la historia no es difícil de adivinar verdad?

Veamos a continuación con más detalle algunas de la técnicas más comunes.

Un mundo de apariencias:

Sinceramente hay varios nombres asociados a diferentes variantes de este ataque

- Karma Attack
- Katmasploit Attack
- Radius WPE Attack
- Otros

Pero hay una característica que las une a todas y es la de que si de aparentar se trata, estas técnicas no dejan ningún detalle suelto.

En una de las técnicas, el atacante levanta un punto de acceso y brinda a través del mismo los siguientes servicios:

- DHCP
- DNS
- HTTP
- SMB
- POP3
- IMAP
- SMTP

de manera que todo aquel que se conecte al punto de acceso obtenga una dirección IP para que luego, toda petición de servicios asociada a los arriba detallados, sea interceptada por el DNS falso, que claro está, resolverá como dirección al atacante. Por lo que cualquier tipo de credenciales que se intercambie en texto plano, como así también cookies de sesión de los sitios mas populares (Linked-In, Facebook, Gmail, Yahoo Mail y otros) quedarán en manos del atacante en un abrir y cerrar de ojos.

Adicionalmente en esta técnica se combina la utilización de técnicas de explotación tradicionales, las cuales intentan explotar debilidades comunes en el navegador del usuario, para intentar lograr tener acceso remoto y ejecutar código arbitrario.

Otras técnicas en cambio, intentan engañar al usuario haciendo que una vez que este se conecte al punto de acceso inalámbrico falso sea redirigido a un portal cautivo en el cual se le indica, mediante algún ardid, que descargue un ejecutable, que dará acceso a la ejecución con los permisos del usuario a código arbitrario y de manera remota por parte del atacante.

Algunas variantes de las técnicas mencionadas son menos activas, por lo que sólo realizan una ataque de man in the middle, brindándole al usuario acceso real a Internet a cambio del monitoreo total del trafico que este produzca.

Por ultimo, existen técnicas similares orientadas a atacar los controles de acceso de robustas implementaciones corporativas de infraestructuras inalámbricas, las cuales también se basan en debilidades del lado del cliente. Por ejemplo, sabemos que la implementación de WPA Enterprise envuelve una serie de controles bastante robustos e interesantes, los cuales abarcan fuertes algoritmos de cifrado, certificados digitales y demás. Pero no todos conocemos que en la implementación pueden producirse pequeños errores de configuración que harían caer el control de acceso a niveles no deseables.

Conclusión:

Lo arriba expuesto no es más que una descripción acotada de prácticas habituales utilizadas hoy en día para el acceso no autorizado a información sensible, las cuales, como habrán podido ver, explotan tanto aspectos técnicos cómo características predecibles del comportamiento del factor humano asociado a la tecnología.

Es importante entender una vez más que las debilidades explotadas no son nuevas, sino que lo nuevo es la manera de llevarlas a la practica de una forma creativa.