La seguridad informática es algo que nos preocupa a todos en mayor o menor medida. Ya comenté en publicaciones anteriores que esta preocupación mal llevada nos obsesionará a cada click que realicemos en nuestro día a día, haciendo a algunos casi volver al papel y lápiz. Aunque sí que es verdad que, sin esta obsesión, la seguridad informática no estaría donde está hoy, y muchos proyectos hoy muy populares ni se hubiesen llegado a plantear.

De algunos de estos proyectos de seguridad os vamos a hablar hoy. Aplicaciones dedicadas, distribuciones con funcionalidades de seguridad, software basado en web (sin necesidad de descargar e instalar nada), espero al menos abarcar un poco de todo esto y poder brindaros la ocasión de dároslas a conocer y que probéis algunas de ellas, que la verdad sea dicha, las hay de lo más interesantes.

¡Empezamos!

10 - Nikto .

Este **escáner de servidores web** realizará pruebas exhaustivas contra (qué sorpresa...) servidores web, teniendo en cuenta diversos factores como las versiones no actualizadas de aplicaciones, problemas específicos de cada versión encontrada, elementos

de configuración del servidor, identificará los sistemas instalados y los analizará… Todo esto contrastando con más de 6400 archivos de su base de datos, así como con más de 1200 servidores con los que contrastar las versiones del software instalado. Sus **herramientas de análisis, así como sus plugins se actualizan con frecuencia y de forma automática,** por lo que no tendremos que estar pendientes de contar con tal o cual versión del programa, siempre tendremos la última disponible.

09 - Cain and Abel .

Nos encontramos ante la única aplicación **sólo disponible para Windows** de este listado. Esta herramienta de recuperación de contraseñas cuenta con una enorme cantidad de utilidades. **Podremos recuperar passwords** mediante 'inhalación' de la red (snnifers), mediante ataques por diccionario, fuerza bruta, criptoanálisis o mediante el uso de algunos exploits. Además, podremos grabar conversaciones VoIP, decodificar contraseñas devueltas por algunas webs, revelar cuadros de contraseñas (los típicos que aparecen como asteriscos), obtener contraseñas de la caché del sistema, etc… También nos permite **analizar los protocolos de enrutamiento del sistema,** un extra añadido a todo lo anterior.

08 - Netcat .

Esta herramienta está diseñada para que o bien sea utilizada por otras aplicaciones o scripts, o bien ser una utilidad back-end fácil de manejar y en la que se pueda confiar. **Nos permitirá leer y escribir datos mediante conexiones TCP/UDP** al mismo tiempo que nos permite **crear casi cualquier tipo de conexión** que podamos necesitar (por ejemplo, conexión a un puerto determinado para aceptar conexiones entrantes). También nos es útil como herramienta de depuración o exploración de red.

A pesar de su popularidad, fue discontinuada en 1995, llegando a ser difícil encontrar una copia del código fuente. Pero ahí está la comunidad Linux (concretamente el proyecto Nmap) para actualizar una herramienta tan útil, dando como resultado **Ncat,** un re implementación moderna con soporte para SSL, IPv6, SOCKS y otros protocolos aún inexistentes por aquellas fechas.

07 - Sqlmap .

Esta herramienta para 'pen-testing' (pruebas de accesibilidad a sistemas) **automatizará el proceso de detección y explotación de los errores de inyección SQL** y se hace cargo de los servidores de base de datos en back-end. Cuenta con una amplia gama de funciones, como por ejemplo acceder al sistema de archivos del servidor vulnerado y ejecutar comandos desde nuestro equipo fuera de su red, o el hecho de poder obtener el fingerprint (huella dactilar en su más estricta traducción) o clave de acceso a una base de datos para poder acceder a los datos contenidos en dicha base.

06 - Aircrack .

Esta suite de **herramientas para cifrado WEP y WPA** (compatible con 802.11 a/b/g), implementa los algoritmos de 'crackeo' más populares para recuperar las claves de nuestras redes inalámbricas. Esta suite cuenta con más de una docena de aplicaciones muy discretas como **airodump** (captor de paquetes de una red), **aireplay** (inyección de paquetes a una red), **aircrack** (apertura de grietas en WPA-PSK y estáticas en las WEP) y **airdecap** (descifrador archivos capturados en WEP y WPA).

05 - Snort .

Este software de **detección de intrusiones de red, así como de prevención de accesos** no autorizados al sistema, se destaca en el análisis de tráfico y registro de paquetes en redes IP. Mediante análisis de protocolos, búsqueda de contenidos y varios pre-procesados, **Snort es capaz de detener y alertarnos de los miles de gusanos, troyanos, intentos de vulnerar nuestro firewall,** además de ponernos sobre aviso en caso de que estén escaneando alguno de nuestros puertos u otros

comportamientos sospechosos. También **cuenta con una interfaz web** para la gestión de alertas llamada **BASE** (Basic Analysis and Security Engine).

Esta aplicación es Open Source y totalmente gratuita, aunque la compañía desarrolladora también cuenta con versiones comerciales verificadas y certificadas por VRT, y en absoluto caras si comparamos con otros precios que aparecen en esta publicación; 499$.

04 - Kali Linux (anteriormente conocida como BackTrack).

De sobra ya conocida por aquellos que se muevan en el mundo de las distribuciones Linux o en el de la seguridad informática. Esta distribución en Live-CD (cd de arranque con opción a instalable) nos ofrece un **amplio catálogo de herramientas de seguridad y forenses,** proporcionándonos un entorno de desarrollo, pruebas e implementación de lo más completo. Otra característica de Kali-Linux es la **modularidad** , que es básicamente que podemos crearnos una distribución que se adecue a nuestras necesidades, eligiendo los paquetes que vayamos a usar y prescindiendo de otras tantas funcionalidades que no Además de la personalización de la paquetería de la distribución, el hecho de contar con un escritorio como Gnome, hará fácil que **podamos personalizar también los menús, iconos, apariencia, etc.** … pudiendo contar con una distribución que podemos usar a diario y como herramienta de mantenimiento de la seguridad de nuestra red.

03 - Nessus .

Uno de los escáneres de vulnerabilidades más popular y efectivo es Nessus. Más de **46000 plugins componen su extenso repertorio,** con el que podremos poner a prueba sobradamente cualquier entorno que se nos ponga por delante. **Autentificaciones, accesos remotos, accesos locales, control de privilegios y escalado de los mismos, análisis de arquitecturas cliente-servidor,** además de contar con una interfaz web avanzada y con un entorno propio para desarrollar nuestros propios plugins.

Principalmente ideado para sistemas UNIX (aunque aplicable a cualquier plataforma que encontremos hoy día), al igual que Metasploit comenzó siendo de código abierto hasta que

en 2005 se privatizó y retiró las versiones gratuitas en 2008. Lo podemos adquirir a día de hoy por unos 1200$ al año, aunque la comunidad Linux como siempre está ahí para demostrarnos una vez más que el Open Source es omnipresente y **un grupo de usuarios aún desarrollan una versión de Nessus bajo el nombre de OpenVAS.**

02 - Metasploit .

En su lanzamiento en 2004, **Meta sploit revolucionó el mundo de la seguridad.** Nos encontramos ante lo que era un software de código abierto fundamentalmente diseñado **para el desarrollo avanzado de aplicaciones y sistemas, y para el uso y pruebas de código de explotación en entornos controlados.** El popular modelo de análisis a través de **payloads, codificadores, generadores no-op y otros muchos exploits integrables** en diversos programas, han hecho que Metasploit se encuentre siempre a la vanguardia de las opciones más sonadas de entre el software para análisis de seguridad. Entre su repertorio de 'extras' encontramos cientos de exploits que podremos usar o editar para crear los nuestros propios, lo cual es más recomendable que aventurarse a descargar otros scripts o shellcode's de cualquier foro, blog, web, que no sabemos qué puede tener detrás, recordad que el mundo de la seguridad existe por el escepticismo de muchos internautas, nunca viene mal un poco de esa desconfianza en según qué ocasiones.

Algo muy interesante que nos ofrece Metasploit, es un entorno Linux contrastadamente INseguro, que podremos usar para probar todas las 'bondades' de Metasploit en un entorno controlado en lugar de tener que desplegar un servidor únicamente para este fin, o probarlo contra nuestro servidor en activo (únicamente recomendable si sabemos lo que nos hacemos y conocemos mínimamente qué resultado obtendremos).

Comentar también que Metasploit era un software totalmente Open Source, pero en 2009 la compañía **Rapid7** la adquirió y comenzaron a surgir variantes comerciales. Aunque como siempre en este mundo del Software Libre, **gracias a la comunidad seguimos teniendo una versión gratuita, aunque limitada.** Para aquellos que estén interesados en comprar las licencias, comentar que estas se encuentran a un precio de entre 3000$ y 15000$ en función de las funciones que necesitemos.

01 - Wireshark .

Conocido anteriormente como **Ethereal** (hasta que en 2006 perdió los derechos sobre dicho nombre por una disputa con otra marca de similar denominación), se trata de una magnífica **herramienta de código abierto** que nos proporcionará un análisis exhaustivo de nuestra red. Wireshark cuenta con multitud de características interesantes, como el hecho de poder **realizar el análisis sobre una red existente, sobre un mapeado o un archivo existente en disco.** Además, incluye un amplísimo diccionario para aplicar filtros a la navegación, así como la **posibilidad de reconstruir una sesión TCP al completo mediante el flujo de datos analizado,** pudiendo así rastrear la navegación que se genera desde nuestra red.

Es **compatible con cientos de protocolos** y podemos encontrar esta aplicación disponible en varias plataformas como Windows, Linux o Mac OS. Esperamos que toda esta información os sea de ayuda y os anime a probar alguna de estas aplicaciones. **Recordad suscribiros** para estar al día de los artículos, webinars y noticias más relevantes, y no dejéis de echar un vistazo al catálogo de cursos de Openwebinars.net.