Las 8 Mejores Herramientas De Seguridad Y Hacking

Hoy les presentamos 8 de las mejores herramientas de seguridad y hacking las cuales son extremadamente útiles en la obtención y explotación de redes y sistemas de información. Estas herramientas están diseñadas de tal manera que se puede recopilar la información necesaria para asegurar o explotar un computador o una red completa. Todas estos programas son muy utilizados por los piratas informáticos y analistas de seguridad. Así que sigua leyendo para conocer los 8 mejores herramientas de hacking.

En general, todas estas herramientas que describiremos a continuación son herramientas de seguridad y hacking. Estas se utilizan para fines tanto legales como ilegales, y por lo tanto, la mayoría de las personas piensan que estas herramientas son solo utilizadas por hackers maliciosas (algo totalmente fuera de la realidad), cuando en realidad están diseñadas para ayudar a los administradores y profesionales de seguridad a asegurar las redes y los sistemas de información.

Nmap

Nmap ("Network Mapper") es una herramienta gratuita de código abierto para la exploración de la red o la auditoría de seguridad. Fue diseñado para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. Nmap utiliza paquetes IP para determinar qué hosts están disponibles en la red, qué servicios (nombre de la aplicación y la versión) estos equipos ofrecen, qué sistemas operativos (y versiones del sistema operativo) se están ejecutando, qué tipo de filtros de paquetes o cortafuegos están en uso, y docenas de otras características. Nmap se ejecuta en la mayoría de los ordenadores y la consola y versiones gráficas están disponibles. Nmap es libre y de código abierto.

Nessus

Nessus es el escáner de vulnerabilidades más popular y es utilizado en más de 75.000 organizaciones en todo el mundo. Muchas organizaciones alrededor del mundo están dando cuenta de los importantes ahorros de costes que estas reciben mediante el uso de Nessus como herramienta de auditoría de sistemas de información para la búsqueda de fallas críticas de seguridad.

John the Ripper

John the Ripper es esencialmente una herramienta de descifrado de contraseñas que se desarrolló para sistemas tipo UNIX. También sus desarrolladores han extendido su apoyo a los sistemas Windows y MAC.

El software es utilizado por muchos usuarios para probar la fortaleza de la contraseña elegida. Obviamente, esta herramienta también puede ser usada para descifrar las contraseñas y entrar en un sistema. Es compatible tanto con ataque de diccionario (probando todas las palabras en el diccionario, de ahí que nunca se debe elegir una palabra que se ha encontrado en el diccionario) y ataque de fuerza bruta (en este caso todas las posibles combinaciones son juzgados – por lo tanto, si usted elige una contraseña que es alfanumérico y largo plazo, será difícil romperlo).

Nikto

Nikto es un software de código abierto (GPL) para escanear vulnerabilidades en los servidores web. Esta herramienta tiene el potencial de detectar más de 3200 archivos potencialmente peligrosos / CGIs, versiones sobre más de 625 servidores, y los problemas específicos de la versión de más de 230 servidores. Los elementos de exploración y plugins pueden ser actualizado automáticamente (si se desea).

Wireshark

Wireshark es un programa analizador de protocolos de red o sniffer, que le permite capturar y navegar de forma interactiva por los contenidos de los paquetes capturados en la red. El objetivo del proyecto fue crear un analizador de calidad comercial para Unix. Funciona muy bien en Linux y Windows (con una interfaz gráfica de usuario), fácil de utilizar y puede reconstruir flujos TCP / IP y VoIP!

Putty

PuTTY es una implementación libre de Telnet y SSH para Win32 y Unix, junto con un emulador de terminal xterm.

NetStumbler

NetStumbler es una herramienta de detección de redes inalámbricas para Windows. NetStumbler es una herramienta para Windows que permite detectar redes de área local (WLAN), usando 802.11b, 802.11ay 802.11g.

Algunos de los usos de esta herramienta son:

- Verificar que su red esta configurada de la manera segura.
- Buscar lugares con baja cobertura en su WLAN.
- Detectar otras redes que puedan estar causando interferencias en la red.
- Detectar AP no autorizados “rogue” en su lugar de trabajo.
- Ayudar a apuntar antenas direccionales para enlaces de larga distancia WLAN.

El equivalente de NetStumbler para Linux se llama Kismet.

Metasploit

El Proyecto Metasploit es un proyecto de seguridad informática que proporciona información sobre las vulnerabilidades, ayuda en las pruebas de penetración y en la ejecución de la explotación de vulnerabilidades de seguridad. Metasploit representa un conjunto de herramientas que ayuda a los profesionales de seguridad y hacker a llevar a cabo ataques informáticos de manera sistematizada y automatizada.

Su más conocido sub-proyecto es el marco de código abierto Metasploit, una herramienta para el desarrollo y ejecución de código de explotación en contra de un equipo o sistema de información destino remoto. Otros importantes sub-proyectos son la base de datos Opcode, archivo shellcode, e investigaciones de seguridad.