Software para test de seguridad
Fundamentos de Redes

SOFÍA ALMEIDA BRUNO
FERNANDO DE LA HOZ MORENO
Universidad de Granada
28 de noviembre de 2017

Índice

1. Introducción

Los test de seguridad son un conjunto de herramientas que se utilizan para evaluar el nivel de seguridad de un sistema. El conjunto de herramientas de seguridad es muy amplio, ya que recoge aspectos muy diferentes de la seguridad una no sustituye a otra, son complementarias.

1.1. Kali Linux

Kali Linux es un sistema operativo, basado en Debian, orientado a la realización de pruebas de penetración y auditorías de seguridad. Es un entorno de desarrollo seguro, esto quiere decir que solo un pequeño grupo de personas puede acceder e interactuar con los paquetes del sistema. Kali tiene más de 300 herramientas de pruebas de seguridad agrupadas según su función: recopilar información, análisis de vulnerabilidades, aplicaciones web, evaluación de bases de datos, ataques a contraseñas, ataques wireless, ingeniería inversa, herramientas de explotación, sniffing, mantener el acceso.

En esta exposición nos centraremos en cinco herramientas ampliamente utilizadas y que tienen diferentes objetivos. En esta exposición pretendemos dar una visión global del ámbito de la seguridad, en lugar de centrarnos en una única herramienta.

2. John the Ripper

John the Ripper es una aplicación de descifrado de claves (password craking), es una de las herramientas más populares para test de contraseñas porque reúne diferentes técnicas para desencriptar contraseñas. El objetivo es que el administrador evalúe la seguridad de las contraseñas elegidas por los usuarios para previnirlos si son débiles.

Puede utilizarse para varios formatos de encriptación de contraseñas incluyendo muchos tipos de encriptación hash los cuales se encuentran mayormente en varias versiones Unix y Windows.

¿Cómo funciona?

En primer lugar, se proporciona un archivo con las contraseñas encriptadas. Por ejemplo, en los sistemas Unix se obtienen de los archivos /etc/passwd y /etc/shadow. Se puede personalizar el tipo de ataque pero el más común suele ser el ataque por diccionario. Un archivo (wordlist) en el que hay una

lista de palabras de un diccionario o contraseñas reales ya encontradas o combinaciones y alteraciones de las mismas. Las palabras se encriptan y se comparan con el hash del archivo de contraseñas, devolviendo las coincidencias.

El ataque por diccionario es más efectivo, pero si no tiene éxito, podemos intentar el ataque por fuerza bruta, que consiste en comprobar todas las posibilidades.

3. Aircrack-ng

Aircrack-ng es una herramienta que analiza los paquetes de una red inalámbrica con seguridad tipo 802.11 WEP Y WPA/WPA2-PSK para hallar la clave de encriptación de estos. A partir de los paquetes capturados, hace un análisis estadístico con un algoritmo bastante complejo matemáticamente para determinar byte por byte la clave de encriptación, dando una tabla con los key-bytes más probables ordenados por su probabilidad. Cuanto más paquetes capturemos, mejor será el análisis estadístico realizado y mayor será la probabilidad de acertar la clave.

4. Wireshark

Como ya sabemos, Wireshark es una analizador de protocolos de red, permite inspeccionar lo que ocurre en la red con mucha profundidad. Aunque normalmente se utiliza para analizar y gestionar la red, tiene una gran utilidad en el campo de la seguridad.

Una funcionalidad es el análisis dinámico de software malicioso. Se procede a infectar un sistema en un entorno controlado y se analiza el tráfico que genera en la red, esto es de gran utilidad puesto que podemos detectar patrones de envío de mensajes de este malware y así localizarlos en otras redes.

Otra funcionalidad es, cuando descubrimos a un agente extraño utilizando nuestra red, analizar el tráfico que este genera en la red para revelar sus intenciones.

5. Nmap

Nmap es una herramienta para exploración de redes y auditorías de seguridad. Una de sus utilidades más importantes es el llamado "host discovery", descubrimiento de sistemas. Cuando uno reconoce una red es importante reducir el rango de direcciones de la red a una lista de direcciones de equipos activos. De cara a una auditoría de seguridad se tiene que disponer de esta información pues estos equipos son los que van a ser punto de mira de posibles ataques y es importante saber cuales son. Nmap realiza esta técnica enviando combinaciones arbitrarias de sondas (paquetes) TCP SYN, TCP ACK, UDP e ICMP (como ping) a un conjunto de direcciones a un puerto concreto. Si se recibe respuesta de una dirección IP se sabrá que el sistema con esa IP está disponible y responde.

Otra utilidad importante de Nmap es el análisis de puertos de un equipo. Los atacantes y las personas que realizan pruebas de intrusión saben que cada puerto abierto (una aplicación acepta conexiones TCP o paquetes UDP en este puerto) es un vector de ataque, por lo que los administradores intentan cerrarlos, o protegerlos con firewalls, pero sin que los usuarios legítimos pierdan acceso al servicio. Esta técnica consiste en el envío de paquetes de diferente tipo (TCP SYN, TCP ACK, UDP, ICMP, ...) y análisis de la respuesta del puerto para así determinar el estado del puerto. Por ejemplo, se envía un paquete SYN como si se fuera a abrir una conexión real a un puerto. Si se recibe como respuesta un paquete SYN/ACK esto indica que el puerto está en escucha (abierto), mientras que si se recibe RST indica que no hay nadie escuchando el puerto (cerrado). Si no hay respuesta se marca el puerto como filtrado pues un firewall está filtrando los paquetes enviados a este puerto. Nmap también nos ofrece otras funcionalidades como puede ser ver los servicios y qué versión de estos ofrecen los equipos, determinar el sistema operativo que utilizan, qué firewall utilizan, etc.

Imágenes de wireshark viendo el tráfico generado por nmap.

6. Metaesploit

Metaesploit es un proyecto de seguridad informática que proporciona información acerca de vulnerabilidades de seguridad y resulta muy útil durante los test de penetración. El proyecto más conocido es Metaesploit Framework, una herramienta para desarrollar y ejecutar exploits contra una

máquina remota. Un exploit es un fragmento de software, datos o secuencia de comandos cuyo objetivo es forzar un fallo no previsto en un servicio. Una vez forzado este fallo, utilizamos otra herramienta denominada payload. Los payload son programas cuya finalidad es aprovechar el fallo (bug) forzado por el exploit. Por ejemplo, abrir una shell en la máquina remota desde nuestro ordenador.

7. Pros y contras

7.1. Pros

- Evalúa la seguridad del sistema.
- Permite encontrar funcionalidades no deseadas de los programas.
- Útiles para administración y gestión de redes.

7.2. Contras

- Estas mismas herramientas se pueden utilizar con fines maliciosos.
- Nunca estaremos completamente asegurados, hay rutas de ataque que puedes no haber tenido en cuenta.

8. Bibliografía

- http://www.openwall.com/john/doc/
- https://en.wikipedia.org/wiki/John_the_Ripper
- https://nmap.org/man/es
- https://www.aircrack-ng.org/doku.php?id=aircrack-ng
- https://en.wikipedia.org/wiki/Metasploit_Project