Laboratorio de seguridad

Escaneo de puertos en la configuración de sistemas

Hoy llevaremos a la práctica los test de seguridad que venimos describiendo en las notas anteriores. Comenzaremos por lo básico, para que estas guías sean útiles para todos y luego iremos avanzando en metodologías más avanzadas.

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

En notas anteriores habíamos dicho que uno de los factores más importantes de la implementación, en lo que a seguridad de la información refiere, es el chequeo de los puertos que dejamos abiertos en el sistema. Indudablemente, todo sistema deberá tener puertos abiertos para la trasmisión/recepción de datos, sin importar qué tipo de implementación estemos realizando, sea ésta de CCTV, alarma, control de acceso u otro tipo. Lo importante en este punto es que queden abiertos solo los puertos necesarios para que la instalación sea más segura. Aquellos que no sean necesarios, deben ser cerrados.

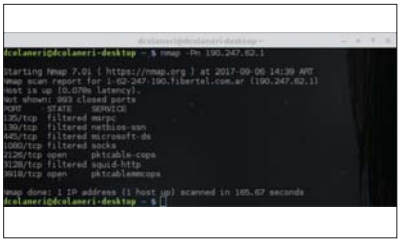
Más allá de esto, habíamos recomendado jamás dejar usuarios y claves por defecto: estos accesos deben ser configurados a mano y quitando todas las etiquetas de códigos QR de los dispositivos. Si bien muchos pensarán que abrir puertos en los routers es peligroso, es un riesgo que podemos auditar y controlar con más precisión

Volviendo al inicio de esta nota, desde la configuración mediante el software que nos sea provisto por el fabricante, podremos deshabilitar servicios y por ende cerrar puertos. Por ejemplo, cuando el acceso web no sea necesario debemos desactivarlo, ya sea que el sistema permita HTTP o HTTPS (puertos 80 y 443 respectivamente).

Luego de realizar las configuraciones correspondientes, deberemos testear que los puertos realmente estén cerrados y también verificar que nuestro equipo no tenga puertos abiertos que el fabricante no nos haya notificado. Para esto usaremos un escáner de puertos. Hay muchos, pero para este laboratorio nos enfocaremos en el más utilizado: NMAP.

NMAP es un escáner gratuito y tiene soporte para Windows, Linux, por consola o con interfaz gráfica. Aquí trabajaré desde una consola de Linux pero la metodología es la misma en todos los sistemas.

El uso de NMAP es muy simple: con "nmap –h" nos dará las opciones posibles por si quieren investigar, aunque vamos a centrarnos en lo que nosotros usaremos, para ello debemos ingresar : "nmap –Pn –p 1-65000 IP-A-AUDITAR". Aquí lo que hacemos es decirle a NMAP que mire todos los puertos, del 1 al 65000, sin hacer un ping previo usando "–Pn" (útil si el sistema no responde paquetes ICMP) de la IP que coloquemos. Este tipo de test completo es para realizar en la misma LAN y no desde fuera de la misma, dado el tiempo que demora.



En la imagen anterior vemos un ejemplo de NMAP sin especificar puertos, por lo que solo testea los más conocidos. En la misma podemos observar que identifica si los puertos son UPD o TCP, el nombre del servicio, si es conocido, y el estado del mismo. Este ejemplo demuestra que se testeó un equipo Windows.

Los estados que veremos son OPEN para puertos abierto, CLOSED para puertos cerrados y FILTERED para puertos que están abiertos pero con una política DROP, que significa que "rebote" toda conexión que no sea como el puerto de espera.

Todos los puertos abiertos son interesantes, pero haremos hincapié en 22 SSH, 23 TELNET, 25 SMTP, 80 HTTP y 443 HTTPS.

En la próxima nota veremos por qué y usaremos un framework para auditar nuestra implementación. Más precisamente Metasploit, que incorpora, entre otras cosas, herramientas para explorar fallos y una específica para sistemas de CCTV, llamada "cctv_dvr_login", que nos da acceso de administración al sistema con solo un comando, si este no está bien configurado. Les dejo una captura hasta la próxima nota. ■