Guía para evitar un escaneo de puertos

Escrito por David García Martín 24 octubre, 2010 a las 13:00

redes | 6 Comentarios

Es práctica común entre los piratas informáticos escanear puertos para encontrar vulnerabilidades que aprovechar.

En este manual os explicamos unas nociones mínimas para estar seguros frente a esos escaneos.

Otro manual que publicaremos próximamente se encargará de explicar cómo hacer un escaneo de puertos.

Son 8 pequeños puntos que nos ayudarán a establecer un punto seguro en cualquier servidor o aplicación con acceso a la red.

1. Abre exclusivamente los puertos necesarios.

Un atacante buscará escanear probablemente con un robot y por fuerza bruta. Eso quiere decir que no sirve eso de "esto quien lo va a atacar si tardaría 10 horas": los inicios de los ataques están automatizados.

2. Utiliza puertos que no sean un estándar

Cuando un atacante recoge información de un sistema, intentará seguramente hacerlo por puertos estándar es decir: el 1521 para Oracle, o el 8081 para un artifactory de Maven. En estos casos, sería ideal (aunque ello no constituye una seguridad por si misma) utilizar puertos no estándar que dificulten un poco al posible pirata informático.

3. Si no usas el puerto, ¿para qué lo quieres abierto?

Esta asertación parece una trivialidad pero no lo es en absoluto: la mayoría de administradores de sistemas, en sus inicios profesionales, olvidan cerrar o silenciar aquellos puertos que no se están usando. La diferencia entre cerrar y silenciar es que al cerrarlos, el puerto ofrecerá información de que está cerrado si está silenciado, no revelerá información de su estado.

4. Proteger el acceso a aquello que deba ser restringido y a sus conexiones.

Si se necesita ofrecer un servicio a algún usuario o empresa, pero es un servicio susceptible de ser atacado, debe ser protegido con sistemas de autentificación adecuados. Un claro ejemplo a evitar es o era, no se si estará corregido, el sistema de autentificación de Tuenti: por el puerto 80 sin encriptar.

Yo propongo como alternativa por ejemplo un SSL.

5. Usar métodos preventivos: Cortafuegos e IDS

Este punto es absolutamente imprescindible. Cuando se tiene un servicio público, éste debe tener sistemas preventivos que reaccionen de forma inteligente a los ataques. Es en este punto donde los IDS y los firewalls actúan. Un IDS reacciona de forma programada ajustándose a unas reglas definidas por el usuario, que además pueden ser dinámicas. El uso del firewall es sobradamente conocido y existen alternativas software y hardware bastante buenas.

Si además de esto, utilizas redundancia, es decir, dos Cortafuegos, por ejemplo, mejor que mejor.

6. Ocultar información.

Si un atacante necesita información para atacar nuestro sistema, parece lógico que le ofrezcamos la menor información posible. Ya hemos visto el silenciado de puertos; ahora vamos a explicar algunos detalles que muchos administradores de sistemas novatos desconocen:

Desactivar los banners de información de cualquier servicio. Cuando realizas una prueba, por ejemplo un SQL injection, es posible que la traza de error diga algo como "Apace Http 5.6.4" (versiones inventadas). Esa traza da idea del servicio que estamos usando y el posible atacante tiene un punto para comenzar a investigar. Aunque se puede silenciar para que no se envíe nada, lo ideal sería dar pistas falsas; devolver un servicio falso es mi opción recomendada: se puede falsificar la huella de la pila TCP/IP para engañar a los sistemas de detección de fingerprint, con lo cual los atacantes escogerían un punto de entrada equivocado e inútil.

7. Tener el software actualizado

Este punto es imprescindible y de sobra conocido por todos: un software antiguo contendrá errores y fallos de vulnerabilidad que cualquier script kiddie puede aprovechar para tumbarlo, secuestrarlo y otras lindezas.

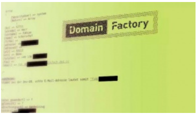
8. Y por último: investigación sobre las últimas mejoras en seguridad.

No hay que perder de vista que la seguridad y sus atacantes mejoran constantemente. Uno de los puntos fuertes de un profesional de la seguridad es estar informado de las últimas novedades. Por ejemplo, aunque es un tema que nunca he tocado personalmente, es ofrecer un servicio sin ningún puerto abierto: no es imposibe, se pueden configurar reglas para, en determinados casos, abrir el puerto y proporcionar el servicio.

Comparte: Share 4 | Tweet 0 | Google + 0 | Share 0

CONTINÚA LEYENDO

No te fíes de tu GPS; piratas informáticos los utilizan para llevarte donde ellos quieren



¿Tienes alguna web o dominio en DomainFactory? Cambia todos tus datos tras esta brecha de seguridad

Actualiza el Kernel de Ubuntu para protegerte de estas graves vulnerabilidades

WPA3
Wi-Fi Security

El estándar WPA3 para Wi-Fi es lanzado oficialmente: estas son las características que tienes que conocer

Microsoft Edge

Microsoft Edge permite que terceros accedan a tus archivos; actualiza cuanto antes

SPECTRERSB

SpectreRSB: una nueva vulnerabilidad, basada en Spectre, que afecta a todas las CPUs modernas

6 Comentarios Redeszone 1 Acceder

Recomendar Compartir Ordenar por los más antiguos

Únete a la conversación...

INICIAR SESIÓN CON O REGISTRARSE CON DISQUS ?

Nombre

Anonymous • hace 8 años
¿no eran 10?, nos han hackeado los 2 últimos puntos... :-p
Responder • Compartir ›

Sergio De Luz ➦ Anonymous • hace 8 años
Una pequeña errata...gracias por el aviso! Ya está corregido.
Responder • Compartir ›

Anonymous ➦ Sergio De Luz • hace 8 años
Se te ha pasado justo encima del primer punto: "Son 10 pequeños puntos que nos ayudarán a establecer...."
Responder • Compartir ›

Sergio De Luz ➦ Anonymous • hace 8 años
Corregido, creo que ya está todo :D
Responder • Compartir ›

Solido • hace 8 años
Interesante :)
Responder • Compartir ›

ethiel ➦ Solido • hace 8 años
Se agradece el comentario, solido. :D
Responder • Compartir ›

TAMBIÉN EN **REDESZONE**

Skype ya permite grabar llamadas, algo que demandaban los usuarios
1 comentario • hace 11 días
Shouko Nishimiya — llega 5 años tarde xd

Microsoft agrega antivirus a Office, pero ¿es suficiente?
4 comentarios • hace 3 días
Javier Antillaque — Más basura , y el problema es usar Windows y sus productos que ahora necesitan más …

¿Por qué se ha desactivado la sandbox Bubblewrap de GNOME?
2 comentarios • hace 15 días
fredii_145 — En resumen la desactivaron quizá en otros y en ubuntu confirmado porque les dio la gana.

Miles de routers MikroTik hackeados para reenviar tu tráfico de red a …
2 comentarios • hace 12 días
Martin Zarate — Yo tuve uno de mis clientes comprometidos con este ataque. Tome captura de toda la config que …

Suscríbete | Añade Disqus a tu sitio web | Política de privacidad de Disqus | DISQUS

¿Te gusta RedesZone?
Ayúdanos desactivando adblock en nuestra web
Te explicamos como filtrarlo Aquí

» FABRICANTES

- Alfa Network
- ASUS
- ASUSTOR
- Beelink
- Cisco Linksys
- Comtrend
- D-Link
- devolo
- dodocool
- Edimax
- Foscam
- FRITZ!
- HP
- Huawei
- Kaiboer
- NETGEAR
- Nextcloud
- Orange
- Popcorn Hour
- QNAP
- Salicru
- Sitecom
- SpotCam
- Synology
- Tenda
- Thecus
- TP-Link
- TRENDnet
- Western Digital
- Xiaomi
- Zaapa
- ZTE
- ZyXEL

» ÚLTIMOS ANÁLISIS

D-Link DCS-8000LH — Valoración RZ 9

ASUS 4G-AC68U AC1900 — Valoración RZ 9

Edimax Office 1-2-3 AC1300 Wave2 PoE — Valoración RZ 9

TP-Link EAP225 AC1350 Wave2 PoE — Valoración RZ 9

D-Link COVR-P2502 AV2 1300 AC1200 — Valoración RZ 8

ASUS Lyra Trio MAP-AC1750 — Valoración RZ 9

Beelink BT3 Pro — Valoración RZ 8

NETGEAR GC110P — Valoración RZ 10

TP-Link LB130 — Valoración RZ 10

NETGEAR Orbi RBK23 AC2200 — Valoración RZ 9

RedesZone
G+ Seguir

» TUTORIALES DE AYUDA

- Android
- Bugtraq
- Chromecast
- Curso de Redes
- Curso HTML y CSS
- Curso Java online
- FreeNAS
- GNU/Linux
- IPFire
- IPsec
- Latch
- Mac OS X
- Raspberry Pi
- Redes
- Seguridad Informática
- Descarga Software
- Whatsapp
- Windows
- Movistar FTTH

» FIRMWARES

- Firmware Comtrend
- Firmware DD-WRT
- Firmware Tomato RAF
- Firmwares Zyxel