CURSO INTERNACIONAL A DISTANCIA DE SEGURIDAD INFORMATICA

MODULO 5

TECNICAS DE HACKING

VERSION DEMOSTRACION

Comentario de esta demostración:

El Curso de Seguridad Informática consta de 5 módulos. Los primeros 4 están en formato interactivo multimedia y el último en formato PDF.

El último módulo corresponde a esta demostración. El documento original consta de 81 páginas como puede observar en el índice al final.

Inscríbase o consulte en www.cordobatech.com.ar

Protocolo de Red TCP/IP

Introducción

La arquitectura TCP/IP esta hoy en día ampliamente difundida, a pesar de ser una arquitectura de facto, en lugar de ser uno de los estándares definidos por la ISO, IICC, etc...

Esta arquitectura se empezó a desarrollar como base de la ARPANET (red de comunicaciones militar del gobierno de los EE.UU), y con la expansión de la INTERNET se ha convertido en una de las arquitecturas de redes más difundida.

Antes de continuar, pasemos a ver la relación de esta arquitectura con respecto al modelo de referencia OSI (Open Systems Interconnection) de la ISO.

Así como el modelo de referencia OSI posee siete niveles (o capas), la arquitectura TCP/IP viene definida por 4 niveles : el **nivel de subred** [enlace y físico], el **nivel de interred** [Red, IP], **el protocolo proveedor de servicio** [Transporte, TCP o UDP] , y el **nivel de aplicación**.

Protocolo Internet (Internet Protocol - IP)

El protocolo IP es el principal del modelo OSI, así como parte integral del TCP/IP. Las tareas principales del IP son el direccionamiento de los datagramas de información y la administración del proceso de fragmentación de dichos datagramas.

El datagrama es la unidad de transferencia que el IP utiliza, algunas veces identificada en forma más específica como datagrama Internet o datagrama IP

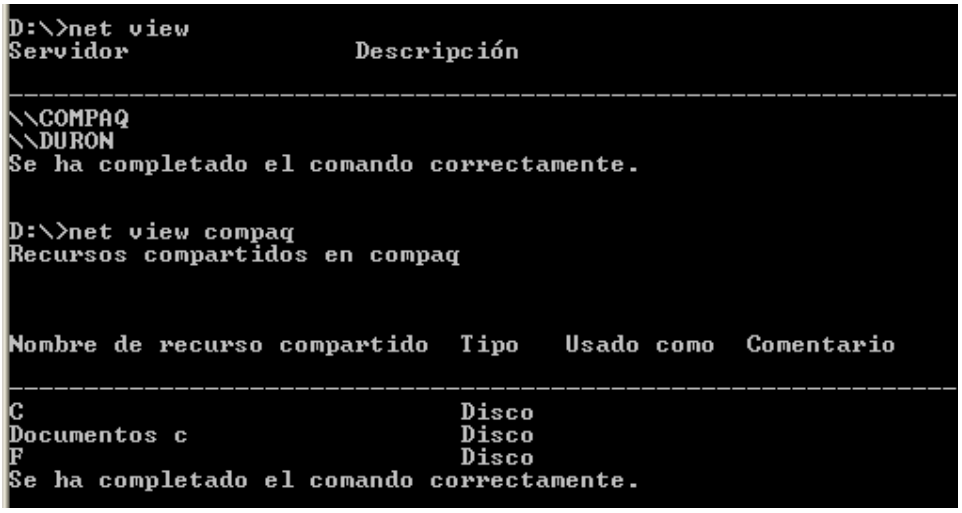
Las características de este protocolo son :
* NO ORIENTADO A CONEXIÓN
* Transmisión en unidades denominadas **datagramas**.
* Sin corrección de errores, ni control de congestión.
* No garantiza la entrega en secuencia.

.....demo.....

Comandos DOS

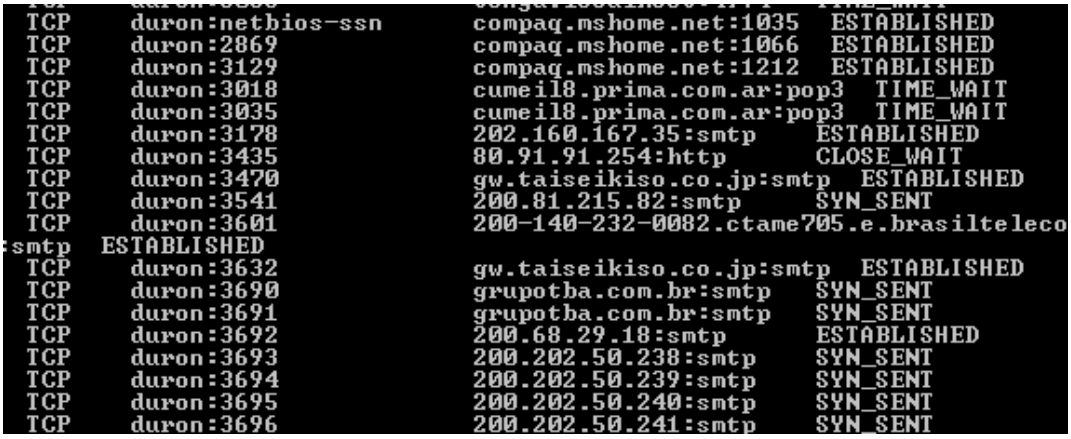
NET VIEW

Este comando nos permite visualizar los equipos accesibles y/o detalles de algunos de ellos.



NETSTAT –AN

Indica los puertos de comunicación, el estado y el tipo de conexión. En dirección local aparecerá nuestra IP y el numero del puerto, en dirección remoto la IP del equipo conectado, y en estado el estado (listening – preparado / established – conectado).



.....demo.....

Técnicas de Hacking

Ingeniería Social

La ingeniería social consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían; aunque a nadie le gusta ser manipulado, en algunos casos no es excesivamente perjudicial (por ejemplo un vendedor puede aplicar ingenieríaa social para conocer las necesidades de un cliente y ofrecer así mejor sus productos), si las intenciones de quien la pone en práctica no son buenas se convierte quizás el método de ataque más sencillo, menos peligroso para el atacante y por desgracia en uno de los más efectivos. Ese atacante puede aprovechar el desconocimiento de unas mínimas medidas de seguridad por parte de personas relacionadas de una u otra forma con el sistema para poder engañarlas en beneficio propio.

Por ejemplo, imaginemos que un usuario de Unix recibe el siguiente correo:

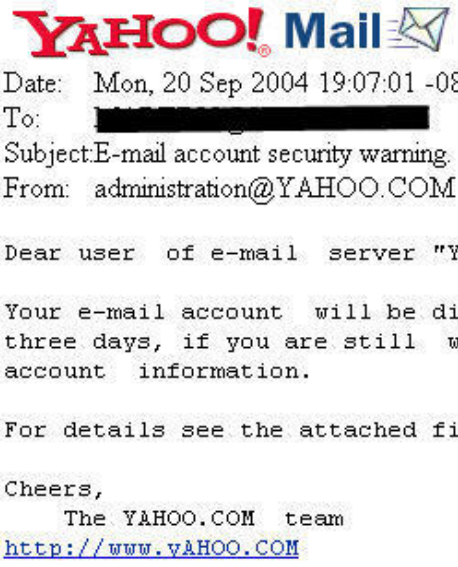
From: Super-User <root@sistema.com>
To: Usuario <user@sistema.com>
Subject: Cambio de clave
Hola,
Para realizar una serie de pruebas orientadas a conseguir un optimo funcionamiento de nuestro sistema, es necesario que cambie su clave mediante la orden 'passwd'. Hasta que reciba un nuevo aviso (aproximadamente en una semana), por favor, asigne a su contraseña el valor 'PEPITO' (en mayusculas).
Rogamos disculpe las molestias. Saludos,
Administrador

Si el usuario no sabe nada sobre seguridad, es muy probable que siga al pie de la letra las indicaciones de este e-mail; pero nadie le asegura que el correo no haya sido enviado por un atacante (es muy fácil camuflar el origen real de un mensaje), que consigue así un acceso al sistema: no tiene más que enviar un simple correo, sin complicarse buscando fallos en los sistemas operativos o la red, para poner en juego toda la seguridad. Sin saberlo, y encima pensando que lo hace por el bien común, el usuario está ayudando al pirata a romper todo el esquema de seguridad de nuestra máquina. Pero no siempre el atacante se aprovecha de la buena fe de los usuarios para lograr sus propósitos; tampoco es extraño que intente engañar al propio administrador del sistema.

Ejemplo de esto son:

- "Envienos un mail para confirmar los datos de su cuenta de Hotmail o caducará en 7 dias"
- Confirme sus datos en nuestra base de datos online para que ud. no tenga inconvenientes en el acceso a sus cuentas en nuestro banco. Estamos realizando estas operaciones debido a recientes ataques de hackers.
- Consiga una cuenta de 1gb de Google Gmail para toda la vida por sólo 20 dolares.
- Etc. Etc.

Conozca http://www.antiphishing.org/ para más detalles.



YAHOO! Mail

Date: Mon, 20 Sep 2004 19:07:01 -0800
To: [redacted]
Subject:E-mail account security warning.
From: administration@YAHOO.COM

Dear user of e-mail server "YAHOO.COM",

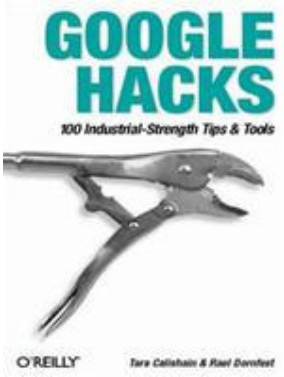
Your e-mail account will be disabled because of improper using in next three days, if you are still wishing to use it, please, resign your account information.

For details see the attached file.

Cheers,
The YAHOO.COM team
http://www.yAHOO.COM

.....demo.....

Google Hacking



Tema por demás interesante. Google se ha transformado en el buscador por excelencia. A diferencia de sus competidores, Google ha automatizado el proceso de indexación de la información a través de complejos algoritmos y a través de una importante y redundante red de más de 10.000 servidores propios donde "guarda" toda la información de internet, por eso la velocidad de respuesta.

El buscador ofrece muchas funciones como la traducción automática de sitios, imágenes, catálogos, etc. Estas herramientas tienen un gran potencial para el hacker experimentado. Para conocer brevemente las principales técnicas, acceda a las opciones de "Búsqueda Avanzada" de Google.

ATAQUES DE AUTENTIFICACIÓN

Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y password.

Spoofing-Looping

Spoofing puede traducirse como "hacerse pasar por otro" y el objetivo de esta técnica, justamente, es actuar en nombre de otros usuarios, usualmente para realizar tareas de Snooping o Tampering.
Una forma común de Spoofing es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él.
El intruso usualmente utiliza un sistema para obtener información e ingresar en otro, y luego utiliza este para entrar en otro, y así sucesivamente. Este proceso, llamado Looping, y tiene la finalidad de "evaporar" la identificación y la ubicación del atacante.

Virus

Un virus es un elemento de software destructivo que se adosa a diferentes soportes informáticos (diskettes, archvivos word, ejecutables, etc.). El virus tiene la capacidad de reproducirse e infectar otros programas y soportes. También producen daño cuando se activa su fase destructiva. La mejor defensa es utilizar software antivirus y mantenerlo actualizado.

Un ejemplo simple de mostrar es un macro virus, o sea un virus escrito en un documento de Office con una macro escrita en lenguaje Visual Basic para Aplicaciones. Este lenguaje permite escribir funciones o subrutinas con el mismo poder que un programa normal de Windows. Por ejemplo, un macro virus puede ejecutarse en la función AutoOpen de Word, copiarse en la plantilla Normal.dot e infectar todos los siguientes documentos de Word que se creen en ese sistema.

Algunos trazos de codigo VBA que se ha encontrado en macro-virus:

Virus FRIEND

```
Open “c:\autoexec.bat” for Append as #1
Print #1, “@echo off”
Print #1, “c:\dos\fast.com”
Close #1
```

Virus Galicia Kalidade

```
FijarAtributos “c:\io.sys”, 0
FijarAtributos “c:\msdos.sys”, 0
Kill “c:\io.sys”
Kill “c:\msdos.sys”
```

Virus ATOM

```
Sub Main
        On Error Goto KillError
        If Day(Now()) = 13 And Month(Now()) = 12 Then
                Kill “*.*”
        End If
KillError:
End Sub
```

Herramientas de Hacking

Microsoft Security Baseline Analyzer

http://www.microsoft.com/technet/security/tools/mbsahome.mspx

El Microsoft Security Baseline Analyzer (MSBA) es una herramienta que permite a los usuarios escanear una o más computadoras con Windows para encontrar problemas de seguridad comunes. MSBA analizará el sistema operativo y otros componentes como IIS, Windows Media Placer, MSXML y SQL Server, entre otros.

En el sistema operativo chequea la seguridad de Windows con ítems como el estatus de la cuenta "Invitado", el tipo de sistema de archivos, los archivos compartidos, los miembros del grupo Administradores, etc..

Tiene varios modos de análisis: Computadora única o Múltiples computadoras. También se puede analizar la red.

La versión 1.2.1 está disponible para UD. Verifique el CD o solicítelo a su tutor.

Para detalles técnicos consulte
http://www.microsoft.com/technet/security/tools/mbsawp.mspx

.....demo.....

Comentario de esta demostración:

El Curso de Seguridad Informática consta de 5 módulos. Los primeros 4 están en formato interactivo multimedia y el último en formato PDF.

El último módulo corresponde a esta demostración. El documento original consta de 81 páginas como pu

Inscríbase o consulte en www.cordobatech.com.ar

INDICE DE CONTENIDOS