

sep

Dirección General de Institutos Tecnológicos

INSTITUTO TECNOLÓGICO
de tehuacán

seit



SEGURIDAD

- 1) TIPOS DE ATAQUES EN REDES LAN Y WAN
- 2) SEGURIDAD EN LA AUTHENTICACION Y SESIONES
- 3) INTRUSIONES EN LA RED (PREVENCION/CORRECCION)
- 4) EVITAR DUPLICAR IP Y DETECCION DE MAQUINAS MEDIANTE EL REGISTRO DE MAC'S

MATERIA: ADMINISTRACION DE REDES

PROFESOR: VAZQUEZ GUZMAN FRANCISCO

ALUMNA (S):

ANSELMO HERNANDEZ EDITH

MÉNDEZ SALAZAR DIANA PATRICIA



ING. EN SISTEMAS COMPUTACIONALES

TEHUACAN, PUE., A 21 DE MAYO DE 2010

TIPOS DE ATAQUES EN REDES LAN Y WAN

- **ATAQUES DE ESCANEEO:**

Los ataques de escaneo se realizan para la recopilación de información sobre posibles puertas de acceso a la red. Consisten en recopilar la información de que puertos están escuchando en la red para posteriormente acceder a los recursos a través de ellos.

>Ataques de escaneo TCP:

El protocolo TCP/IP utiliza puertos virtuales para realizar el envío y recepción de los datos por la red adoptando la estrategia cliente/servidor, escucha permanente por determinados puertos para recibir los datos que se van a transmitir de un equipo a otro. Los puertos pueden estar....

Escuchando Listening: si la respuesta es SYN/ACK.

Cerrados Closed: si la respuesta es RST/ACK.

Los ataques que se producen TCP se basan en el uso de los flags que el protocolo incorpora para regular la comunicación.

Los flags o banderas son bits de control para establecer, mantener y terminar una conexión, por ello pasan desapercibidos y los filtros que a veces no pueden determinar con que finalidad han sido lanzados.

Para establecer la comunicación se utilizan tres banderas de control o flags:

SYN, ACK, FIN.

Cuando un cliente quiere enviar datos a un servidor primero debe establecer la conexión siguiendo un proceso inicial que se denomina el saludo de tres vías. Este saludo es el que posibilita que ambos establezcan una conexión.

Hay dos tipos de ataques:

Ataque TCP SYN scanning (objetivo averiguar puertos abiertos):

Basándose en lo anterior, el servidor escucha permanentemente todas las peticiones que le llegan por la red a un número de puerto determinado que permanece abierto.

Se envía una solicitud de conexión enviándole un segmento SYN (Synchronize Sequence Number).



Se espera a que el servidor devuelva el estado del puerto



Inmediatamente al comprobar que el puerto esta abierto se envía un RST para finalizar la conexión dejando esta a medias, por eso se denomina ataque de media-apertura, y ya tenemos la información que estábamos buscando.



Para evitar este tipo de ataques se recomienda tener activo algún sistema de monitorización de redes como un Firewall o algún tipo de filtro que detecte paquetes SYN aunque no es 100% efectivo ya que cualquier comunicación se establece de esta forma y es difícil detectar el escaneo.

Ataque TCP FIN scanning (Stealth Port Scanning)

El protocolo TCP establece que:

Si el puerto esta abierto y recibe un paquete FIN con el bit RST activado lo ignora.

-Si esta cerrado responde con un RST.

-Se utiliza para burlar los dispositivos de filtrado y bloqueo de la red como los firewalls que detectan ataques SYN:

Cuando enviamos un paquete FIN a un puerto cerrado



la respuesta es un paquete con RST activo que confirma el puerto cerrado



y si el puerto esta abierto ignorará esta petición.

>Ataque por Fragmentación:

Como su nombre indica, consiste en fragmentar los paquetes de ataques SYN y FIN para que los filtros de la red no puedan detectarlos.

Es poco efectivo ya que genera tal cantidad de pequeños paquetes que son enviados a la víctima, que pueden llegar a bloquear tanto los recursos del atacante como saturar las colas de los posibles filtros de la red (firewalls).

>Snnifing:

El ataque Snnifing se considera un ataque pasivo, porque realmente sólo recopila y almacena la información que circula por la red.

Estas herramientas se pueden instalar tanto en quipos de la red como en equipos de comunicaciones de la red.

>Snooping:

Este tipo de ataque también es pasivo, también escucha en la red todo el trafico, pero a diferencia del anterior, este ataque permite acceder a datos e incluso descargar los mismos para una manipulación posterior.

- **ATAQUES DE AUTENTIFICACIÓN**

Los ataques de autenticación consisten en introducirse en un sistema suplantando la identidad de un usuario o del propio administrador. O bien se aprovecha una sesión establecida por el usuario, o bien con los datos obtenidos de los ataques de escaneo.

>Spoofing – looping:

El spoofing-looping es una combinación de ataque de suplantación de identidad y borrado de huellas.

El atacante accede al sistema suplantando la identidad de algún usuario preferentemente el administrador con la información que se obtuvo del ataque de escaneo, y después va saltando por la red, aprovechando las relaciones de confianza entre las redes.

En cada nueva red accesible el atacante realiza de nuevo escaneo para acceder como usuario legitimo y en conjunto desde el origen al destino pueden existir muchas estaciones, esto genera muchos problemas a la hora de rastrear, tanto legislativos porque al saltar de un equipo a otro podemos cambiar de país con sus correspondientes normas legislativas como el despliegue humano que conlleva, el rastreo.

>DNS spoofing

Los DNS son servidores distribuidos por la red que ejecutan servicios de traducción de direcciones ip numéricas a nombres.

DNS spoofing se refiere a un servidor que está recibiendo información de un host no autorizado para prestar este servicio con fines maliciosos, como la redirección hacia paginas incorrectas al acceder a la web.

>WEB spoofing

En este ataque lo que se suplanta es un sitio web por completo.

La finalidad de este ataque es la recopilación de todo tipo de información que se puede recoger de los usuarios de la página.

>ARP spoofing

Una de las soluciones para evitar el sniffing en una red es segmentarla usando un switch. Esto mejora los efectos de este tipo de ataques pero da paso a otros aprovechando las vulnerabilidades del switch.

>IP splicing-Hijacking

Son ataques de apropiación de identidad. Se producen en sesiones ya establecidas, el atacante espera a recibir la información del ingreso del usuario en el sistema y se apropia de su identidad para acceder.

Para protegerse de este tipo de ataques se utilizan las sesiones seguras en las que los datos van cifrados, por ejemplo usando el protocolo SSH de cifrado.

- **ATAQUES DE MODIFICACIÓN-DAÑO**

Este tipo de ataques son los más peligrosos porque actúan sobre los datos o los programas instalados, modificando o borrando los archivos.

Estos ataques necesitan primero de los anteriores para obtener la información necesaria de la red y normalmente es el objetivo final de un intruso.

> Tampering o Data Diddling

Con este tipo de ataques se puede hacer mucho daño a entidades como bancos, ya que al acceder al sistema, si se han conseguido los permisos oportunos, deja libre al atacante para crear por ejemplo cuentas falsas o modificar las existentes y desviar dinero de una a otra.

El uso de virus en sistemas, también es considerado como un ataque de modificación o daño, por ejemplo los troyanos ocultos en programas que efectúan operaciones de modificación y borrado sin el control del usuario que los está usando.

> Borrado de huellas:

El atacante cuando accede a un sistema lo hace aprovechando las vulnerabilidades que este tiene, estas acciones se pueden ver reflejadas en los logs del sistema, monitores de red o si nuestra red posee un firewall en los logs del firewall.

Es importante una vez realizado el ataque saber borrar las huellas que son todas aquellas operaciones que se han realizado en el sistema durante el acceso indebido.

Estas operaciones se almacenan en el sistema en diferentes archivos denominados logs

Estos logs deben ser debidamente manipulados para que el administrador no descubra por donde se accedió y que se instalo o modifiko y así corregir la vulnerabilidad. O rastrear el acceso.

> Ataques activeX

ActiveX es un conjunto de elementos desarrollados por Microsoft para darle al entorno Web un aspecto más vivo y dinámico.

Para prevenir las vulnerabilidades ActiveX utiliza certificados y firmas digitales, con entidad certificadora. Aceptando un el control ActiveX , estamos dando capacidad suficiente al control para ejecutarse sin restricciones.

La forma de actuar de estos controles dañinos se basa en la manipulación de algunos exploradores haciendo que no se solicite la confirmación a través de la entidad certificadora a la hora de descargarse un control.

>Ataques por vulnerabilidades

Las vulnerabilidades son puntos débiles de nuestros sistemas que son aprovechados para acceder y realizar alguna acción maliciosa.

Entre los ataques más conocidos destacaremos:

>>Ataques de "Ingeniería social":

Estos ataques son los más efectivos si el atacante tiene habilidad para convencer al usuario de realizar acciones para revelar login y password que serán usados posteriormente por el atacante. Los datos solicitados se usaran posteriormente para acceder al sistema remotamente.

>>Trashing o ataques de monitorización:

Este ataque consiste en monitorizar el sistema para descubrir posibles agujeros de seguridad que serán explotados posteriormente.

La única manera de mantenerse en la medida de lo posible a salvo de este tipo de ataque, es tener el sistema lo mas actualizado posible instalando los parches suministrados por el fabricante del software, y nunca revelar datos del sistema si no se conoce la fuente que los está solicitando.

- **ATAQUES DE PUERTAS TRASERAS BACKDOORS**

Estos ataques son los mas desconocidos, pero no por ello los menos dañinos y habitualmente utilizados. Una puerta trasera en si es un programa que permite remotamente acceder a un sistema con total libertad de movimientos, es un acceso a un sistema o programa de tal manera que para el usuario es transparente.

Las puertas traseras se pueden producir por dos causas:

- Cuando un programador desarrolla una aplicación y establece que puertas traseras para acceder al programa más rápidamente en la fase de pruebas.
- Por error o por fallos que se producen posteriormente.
- Una puerta trasera no es peligrosa en si, pero si es cierto que es una entrada al sistema no controlada y esto si es peligroso para la seguridad e integridad.

>Exploits:

Los exploits aprovechan las vulnerabilidades de los programas instalados para introducirse en el sistema. Existen multitud de exploits a la carta para explotar los errores del software instalado. Normalmente son programillas que están escritos en lenguajes de bajo nivel como C.

> Obtención de passwords Cracking:

Consiste en obtener las claves de acceso a los equipos a través de herramientas que realizan todas las combinaciones posibles, hasta dar con la correcta. Este tipo de ataques son conocidos como ataques por fuerza bruta.

Poner passwords demasiado evidentes, o no cambiar nunca la palabra de paso hace más sencillo este tipo de ataque.

>Uso de diccionarios:

Se denomina así a un tipo de programas capaces de probar multitud de claves hasta encontrar la correcta. Estos ataques se pueden realizar por varios computadores simultáneamente procesando datos. Hasta dar con la clave buscada.

SEGURIDAD EN LA AUTHENTICACION Y SESIONES

AUTENTICACIÓN MÁS SEGURA CON UNA SOLUCIÓN DE CONTRASEÑA DE UN SOLO USO

Una contraseña estática tradicional se cambia únicamente cuando es necesario: cuando ha expirado o cuando el usuario la ha olvidado y necesita restablecerla. Puesto que las contraseñas se guardan en la memoria caché de los discos duros de los equipos y se almacenan en los servidores, están expuestas a un riesgo potencial de manipulación.

Esto supone un verdadero riesgo para los equipos portátiles puesto que pueden ser robados con facilidad.

A diferencia de una contraseña estática, una contraseña de un solo uso cambia cada vez que el usuario inicia sesión. Las contraseñas se generan de una de estas dos maneras: como contraseñas de sincronización temporal o como contraseñas de sincronización de contador.

Ambos enfoques requieren normalmente que el usuario lleve consigo un pequeño dispositivo de hardware (a menudo un keychain) que se sincroniza con el servidor y ambos usan, con frecuencia, algún algoritmo para generar la contraseña.

AUTENTICACIÓN PASSPORT

El proveedor de autenticación Passport es un servicio de autenticación centralizado proporcionado por Microsoft que ofrece un único inicio de sesión y servicios de perfil principales para los sitios miembros. Passport es un servicio de autenticación basado en formularios.

Cuando los sitios miembros se registran en Passport, este servicio le concede una clave específica del sitio. El servidor de inicio de sesión de Passport utiliza esta clave para cifrar y descifrar cadenas pasadas entre él y el sitio miembro.

Ventajas

- >Admite un único inicio de sesión a través de varios dominios.
- >Es compatible con todos los exploradores.

Desventaja

- >Supone una dependencia externa para el proceso de autenticación.

AUTENTICACIÓN KERBEROS

Kerberos es un protocolo de autenticación de redes de ordenador que permite a dos computadores en una red insegura demostrar su identidad mutuamente de manera segura.

Sus diseñadores se concentraron primeramente en un modelo de cliente-servidor, y brinda autenticación mutua: tanto cliente como servidor verifican la identidad uno del otro. Los mensajes de autenticación están protegidos para evitar eavesdropping y ataques de Replay.

Kerberos se basa en criptografía de clave simétrica y requiere un tercero de confianza. Además, existen extensiones del protocolo para poder utilizar criptografía de clave asimétrica.

AUTENTICACIÓN NTLM

En un entorno de red, NTLM se utiliza como protocolo de autenticación para las transacciones entre dos equipos en los que al menos uno de ellos ejecuta Windows NT 4.0 o una versión anterior. Las redes con esta configuración se denominan de modo mixto, que es la configuración predeterminada en la familia de servidores Windows Server 2003.

Por ejemplo, en las siguientes configuraciones se utilizaría NTLM como mecanismo de autenticación:

- Un cliente con Windows 2000 o Windows XP Professional que se autentica en un controlador de dominio de Windows NT 4.0.
- Un cliente con Windows NT 4.0 Workstation que se autentica en un controlador de dominio de Windows 2000 o Windows Server 2003.
- Un cliente con Windows NT 4.0 Workstation que se autentica en un controlador de dominio de Windows NT 4.0.
- Usuarios de un dominio de Windows NT 4.0 que se autentican en un dominio de Windows 2000 o un dominio en el que se ejecuta algún miembro de la familia Windows Server 2003.
- Un cliente que ejecute Windows 95, Windows 98 o Windows Millennium Edition que se autentique en cualquier controlador de dominio.

Además, NTLM es el protocolo de autenticación para equipos que no forman parte de un dominio, como los servidores independientes y los grupos de trabajo.

SESIONES SEGURAS Y METADATOS

Cuando se establece una sesión segura y la propiedad `RequireCancellation` está establecida como `false`, Windows Communication Foundation (WCF) envía una aserción `mssp:MustNotSendCancel` como parte de los metadatos en el documento de Lenguaje de descripción de servicios web (WSDL) para el extremo del servicio. La aserción `mssp:MustNotSendCancel` informa a los clientes de que el servicio no responde a las solicitudes para cancelar la sesión segura. Cuando la propiedad `RequireCancellation` está establecida como `true`, WCF no emite una aserción `mssp:MustNotSendCancel` en el documento WSDL. Se espera que los clientes envíen una solicitud de cancelación al servicio cuando dejen de necesitar la sesión segura. Cuando se genera un cliente con ServiceModel Metadata Utility Tool (Svcutil.exe), el código de cliente reacciona adecuadamente a la presencia o ausencia de la aserción `mssp:MustNotSendCancel`.

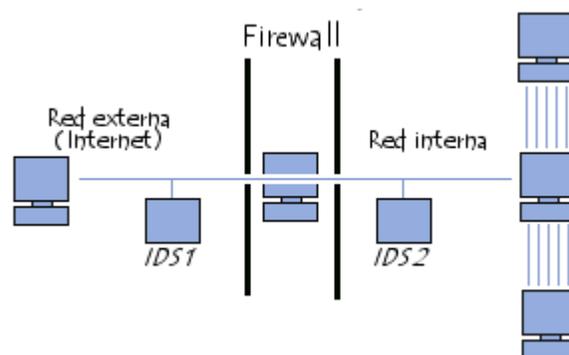
INTRUSIONES EN LA RED (PREVENCIÓN Y CORRECCIÓN)

El término **IDS** (*Sistema de detección de intrusiones*) hace referencia a un mecanismo que, sigilosamente, escucha el tráfico en la red para detectar actividades anormales o sospechosas, y de este modo, reducir el riesgo de intrusión.

Existen dos claras familias importantes de IDS:

- El grupo **N-IDS** (*Sistema de detección de intrusiones de red*), que garantiza la seguridad dentro de la red.
- El grupo **H-IDS** (*Sistema de detección de intrusiones en el host*), que garantiza la seguridad en el host.

Un N-IDS necesita un hardware exclusivo. Éste forma un sistema que puede verificar paquetes de información que viajan por una o más líneas de la red para descubrir si se ha producido alguna actividad maliciosa o anormal. El N-IDS pone uno o más de los adaptadores de red exclusivos del sistema en modo promiscuo. Éste es una especie de modo "invisible" en el que no tienen dirección IP. Tampoco tienen una serie de protocolos asignados. Es común encontrar diversos IDS en diferentes partes de la red. Por lo general, se colocan sondas fuera de la red para estudiar los posibles ataques, así como también se colocan sondas internas para analizar solicitudes que hayan pasado a través del firewall o que se han realizado desde dentro.



El H-IDS se encuentra en un host particular. Por lo tanto, su software cubre una amplia gama de sistemas operativos como Windows, Solaris, Linux, HP-UX, Aix, etc. El H-IDS actúa como un daemon o servicio estándar en el sistema de un host. Tradicionalmente, el H-IDS analiza la información particular almacenada en registros (como registros de sistema, mensajes, lastlogs y wtmp) y también captura paquetes de la red que se introducen/salen del host para poder verificar las señales de intrusión (como ataques por denegación de servicio, puertas traseras, troyanos, intentos de acceso no autorizado, ejecución de códigos malignos o ataques de desbordamiento de búfer).

Técnicas de detección

El tráfico en la red (en todo caso, en Internet) generalmente está compuesto por datagramas de IP. Un N-IDS puede capturar paquetes mientras estos viajan a través de las conexiones físicas a las que está sujeto. Un N-IDS contiene una lista TCP/IP que se asemeja a los datagramas de IP y a las conexiones TCP. Puede aplicar las siguientes técnicas para detectar intrusiones:

1. **Verificación de la lista de protocolos:** Algunas formas de intrusión, como "*Ping de la muerte*" y "*escaneo silencioso TCP*" utilizan violaciones de los protocolos IP, TCP, UDP e ICMP para atacar un equipo. Una simple verificación del protocolo puede revelar paquetes no válidos e indicar esta táctica comúnmente utilizada.
2. **Verificación de los protocolos de la capa de aplicación:** Algunas formas de intrusión emplean comportamientos de protocolos no válidos, como "WinNuke", que utiliza datos NetBIOS no válidos (al agregar datos fuera de la banda). Para detectar eficazmente estas intrusiones, un N-IDS debe haber implementado una amplia variedad de protocolos de la capa de aplicación, como NetBIOS, TCP/IP, etc.

Esta técnica es rápida (el N-IDS no necesita examinar la base de datos de firmas en su totalidad para secuencias de bytes particulares) y es también más eficiente, ya que elimina algunas falsas alarmas. Por ejemplo, al analizar protocolos, N-IDS puede diferenciar un "Back Orifice PING" (bajo peligro) de un "Back Orifice COMPROMISE" (alto peligro).

3. **Reconocimiento de ataques de "comparación de patrones"**: Esta técnica de reconocimiento de intrusión es el método más antiguo de análisis N-IDS y todavía es de uso frecuente.

Consiste en la identificación de una intrusión al examinar un paquete y reconocer, dentro de una serie de bytes, la secuencia que corresponde a una firma específica. Por ejemplo, al buscar la cadena de caracteres "cgi-bin/phf", se muestra un intento de sacar provecho de un defecto del script CGI "phf". Este método también se utiliza como complemento de los filtros en direcciones IP, en destinatarios utilizados por conexiones y puertos de origen y/o destino. Este método de reconocimiento también se puede refinar si se combina con una sucesión o combinación de indicadores TCP.

Esta táctica está difundida por los grupos N-IDS "Network Grep", que se basan en la captura de paquetes originales dentro de una conexión supervisada y en su posterior comparación al utilizar un analizador de "expresiones regulares". Éste intentará hacer coincidir las secuencias en la base de firmas byte por byte con el contenido del paquete capturado.

La ventaja principal de esta técnica radica en la facilidad de actualización y también en la gran cantidad de firmas que se encuentran en la base N-IDS. Sin embargo, cantidad no siempre significa calidad. Por ejemplo, los 8 bytes "CE63D1D2 16E713CF", cuando se colocan al inicio de una transferencia de datos UDP, indican un tráfico Back Orifice con una contraseña predeterminada. Aunque el 80% de las intrusiones utilicen la contraseña predeterminada, el 20% utilizarán contraseñas personalizadas y no serán necesariamente reconocidas por el N-IDS. Por ejemplo, si la contraseña se cambia a "evadir", la serie de bytes se convertirá en "8E42A52C 0666BC4A", lo que automáticamente la protegerá de que el N-IDS la capture. Además, la técnica inevitablemente conducirá a un gran número de falsas alarmas y falsos positivos.

Existen otros métodos para detectar e informar sobre intrusiones, como el método Pattern Matching Stateful, y/o para controlar el tráfico peligroso o anormal en la red.

En conclusión, un perfecto N-IDS es un sistema que utiliza las mejores partes de todas las técnicas mencionadas anteriormente.

Qué hacen los IDS

Los principales métodos utilizados por N-IDS para informar y bloquear intrusiones son:

- **Reconfiguración de dispositivos externos (firewalls o ACL en routers):** Comando enviado por el N-IDS a un dispositivo externo (como un filtro de paquetes o un firewall) para que se reconfigure inmediatamente y así poder bloquear una intrusión. Esta reconfiguración es posible a través del envío de datos que expliquen la alerta (en el encabezado del paquete).
- **Envío de una trampa SNMP a un hipervisor externo:** Envío de una alerta (y detalles de los datos involucrados) en forma de un datagrama SNMP a una consola externa como HP Open View Tivoli, Cabletron, Spectrum, etc.
- **Envío de un correo electrónico a uno o más usuarios:** Envío de un correo electrónico a uno o más buzones de correo para informar sobre una intrusión seria.
- **Registro del ataque:** Se guardan los detalles de la alerta en una base de datos central, incluyendo información como el registro de fecha, la dirección IP del intruso, la dirección IP del destino, el protocolo utilizado y la carga útil.
- **Almacenamiento de paquetes sospechosos:** Se guardan todos los paquetes originales capturados y/o los paquetes que dispararon la alerta.
- **Apertura de una aplicación:** Se lanza un programa externo que realice una acción específica (envío de un mensaje de texto SMS o la emisión de una alarma sonora).
- **Envío de un "ResetKill":** Se construye un paquete de alerta TCP para forzar la finalización de una conexión (sólo válido para técnicas de intrusión que utilizan el protocolo de transporte TCP).
- **Notificación visual de una alerta:** Se muestra una alerta en una o más de las consolas de administración.

Desafíos de IDS

En la prensa especializada, cada vez resuena más el término **IPS** (*Sistema de prevención de intrusiones*) que viene a sustituir al IDS "tradicional" o para hacer una distinción entre ellos.

El IPS es un sistema de prevención/protección para defenderse de las intrusiones y no sólo para reconocerlas e informar sobre ellas, como hacen la mayoría de los IDS. Existen dos características principales que distinguen a un IDS (de red) de un IPS (de red):

- El IPS se sitúa en línea dentro de la red IPS y no sólo escucha pasivamente a la red como un IDS (tradicionalmente colocado como un rastreador de puertos en la red).
- Un IPS tiene la habilidad de bloquear inmediatamente las intrusiones, sin importar el protocolo de transporte utilizado y sin reconfigurar un dispositivo externo. Esto significa que el IPS puede filtrar y bloquear paquetes en modo nativo (al utilizar técnicas como la caída de una conexión, la caída de paquetes ofensivos o el bloqueo de un intruso).

EVITAR INTRUSIONES EN LA RED

Para poder evitar las intrusiones en la red podemos hacer lo siguiente:

Las funciones que deberán ser deshabilitadas son:

1. Panel de Control -> Herramientas Administrativas -> Administración de Equipos -> Servicios y Aplicaciones -> Servicios -> Servicio de Informe de Errores. El servicio estará habilitado, proceder a deshabilitarlo.

2. Panel de Control -> Herramientas Administrativas -> Administración de Equipos -> Servicios y Aplicaciones -> Servicios -> Actualizaciones automáticas. El servicio estará habilitado, proceder a deshabilitarlo.

3. Mi PC -> Propiedades -> Opciones Avanzadas -> Inicio y Recuperación. Proceder a desactivar los 3 botones de Errores del Sistema.

4. Desactivar el escritorio remoto: Mi PC -> Propiedades -> Opciones Avanzadas -> Acceso Remoto. Desactivar el botón de Asistencia Remota. Siguiendo estos pasos se evitará que las acciones o la información del usuario quede a merced de los intrusos que deseen aprovecharse del desconocimiento de las funciones del nuevo sistema operativo de Microsoft.

Desactivar en propiedades de red “clientes de redes de Microsoft” y “compartir impresoras y archivos de redes de Microsoft” solo si no usa la red local el win xp lleva un pequeño firewall y esta desactivado por defecto practico para paquetes icmp pero no es configurable tan solo se añaden servicios para puertos específicos. Pero no permite crear reglas.

Para activarlo busca en > “propiedades de conexiones de red”> opciones avanzadas> habilita la casilla que dice “proteger mi equipo y mi red limitando o impidiendo el acceso desde internet” si tienes un servidor web o ftp acordarse de abrir los puertos en las opciones de configuración también se puede añadir un puerto en concreto para deshabilitar el netbios (sobre tcp/ip) ir a “propiedades de red” en la pestaña general de ahí seleccionar (poner azul) el campo “protocolo internet (tcp/ip)” darle en propiedades saldrá otra ventana .

En la pestaña general ir a “opciones avanzadas” en la pestaña wins deshabilitar net bios sobre (tcp/ip) y dar aceptar a todo con esto deshabilitamos los puertos tcp 139 udp 137 y 138 “Una vulnerabilidad presente en cualquier instalación por defecto de Windows XP, puede ocasionar que mediante un ataque de negación de servicio, cualquier ordenador con este sistema operativo conectado a Internet, pueda agotar el 100% de sus recursos en menos de 20 segundos, ocasionando su cuelgue Por defecto el puerto TCP/UPD 445 en Windows XP se recomienda cerrarlo con un firewall por ejemplo el Zone Alarm, podría ser suficiente, o al menos disminuir el riesgo de cuelgue. ”

Algo también importante es hacer un Windows update y bajar las actualizaciones críticas disponibles ya que en estas se encuentran parches necesarios para la seguridad ir a panel de control>herramientas administrativas>servicios >administración de ayuda de escritorio remoto (dar doble clic ahí y deshabilitarla panel de control>herramientas administrativas>servicios >ayuda sobre netbios (sobre tcp/ip) deshabilitarla panel de control>herramientas administrativas>servicios >enrutamiento y acceso remoto deshabilitarla panel de control>herramientas administrativas>servicios >registro remoto deshabilitarlo

Truco

Las funciones que deben ser deshabilitadas son:

1. Panel de Control -> Herramientas Administrativas -> Administración de Equipos -> Servicios y Aplicaciones -> Servicios -> Servicio de Informe de Errores. El servicio estará habilitado, proceder a deshabilitarlo.

2. Panel de Control -> Herramientas Administrativas -> Administración de Equipos -> Servicios y Aplicaciones -> Servicios -> Actualizaciones automáticas. El servicio estar? habilitado, proceder a deshabilitarlo.

3. Mi PC -> Propiedades -> Opciones Avanzadas -> Inicio y Recuperación. Proceder a desactivar los 3 botones de Errores del Sistema.

4. Desactivar el escritorio remoto: Mi PC -> Propiedades -> Opciones Avanzadas -> Acceso Remoto.

Desactivar el botón de Asistencia Remota.

Siguiendo estos pasos se evitar que las acciones o la información del usuario quede a merced de los intrusos que deseen aprovecharse del desconocimiento de las funciones del nuevo sistema operativo de Microsoft.

Desactivar en propiedades de red "clientes de redes de Microsoft" y "compartir impresoras y archivos de redes de Microsoft" solo si no usa la red local

El sistema operativo Windows xp lleva un pequeño firewall y esta desactivado por defecto practico para paquetes icmp pero no es configurable tan solo se añaden servicios para puertos específicos, pero no permite crear reglas.

Para activarlo busca en > "propiedades de conexiones de red"> opciones avanzadas> habilita la casilla que dice "proteger mi equipo y mi red limitando o impidiendo el acceso desde internet"

Si tienes un servidor web o ftp acordarse de abrir los puertos en las opciones de configuración también se puede añadir un puerto en concreto para deshabilitar el netbios (sobre tcp/ip) ir a "propiedades de red" en la pestaña general de ahí seleccionar (poner azul) el campo "protocolo internet (tcp/ip)" darle en propiedades saldrá otra ventana. En la pestaña general ir a "opciones avanzadas" en la pestaña wins deshabilitar net bios sobre (tcp/ip) y dar aceptar a todo con esto deshabilitamos los puertos tcp 139 udp 137 y 138

EVITAR DUPLICAR IP Y DETENCIÓN DE MAQUINAS MEDIANTE EL REGISTRO DE MAC'S

Muchos de nosotros tenemos redes conectadas con routers o Hubs, especialmente aquellos con un Cyber Café / Chat. Puede existir un problema, que al encender todas tus maquinas, o agregar una maquina a la red, Windows te presenta un error cual te dice que hay un conflicto de IP o nombres en la red. Esto ocurre al encender la computadora, la tarjeta de RED se comunica con tu router, hub o switch y pide un IP. Quizás antes de apagar las PCs, computadora #1 tenía el IP 192.166.0.1 y ahora computadora #3 quiere ese mismo IP ya que inició primero que computadora #1, entonces ahí está el conflicto. Si no entienden lo que digo, el router, hub o switch asigna IPs dependiendo de quién lo pida primero. Si ya hay dos computadoras conectadas: Computadora #1 192.166.0.1 y Computadora #2 192.166.0.2, pues la tercera computadora será 192.168.0.3 etc. Estos IPs son ejemplos, los tuyos pueden ser diferentes. Este problema ocurre mucho también en Redes inalámbricas.

Evitando un IP duplicado

Este proceso es un poco más complicado y tenemos que modificar los IPs de cada computadora manualmente. Para logra este paso, necesitamos completar los siguientes pasos:

Obteniendo información de tu red - Vamos a necesitar lo siguiente:

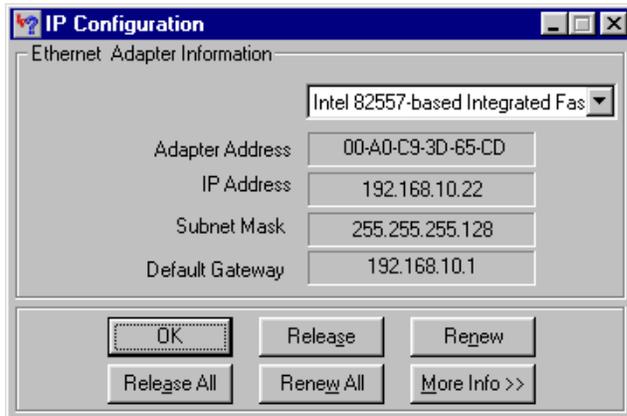
Subnet mask

Default Gateway

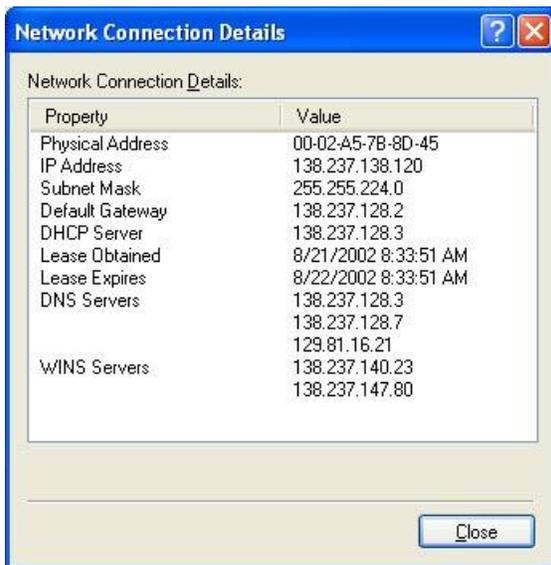
DNS Servers

Obteniendo esta información será diferente dependiendo de que windows tengas. En windows 98 puedes usar winipcfg, puedes ejecutarlo haciendo clic en el botón inicio,

después ejecutar/run y digitar winipcfg. Puedes hacer clic en More info >> para obtener más información sobre tu red.



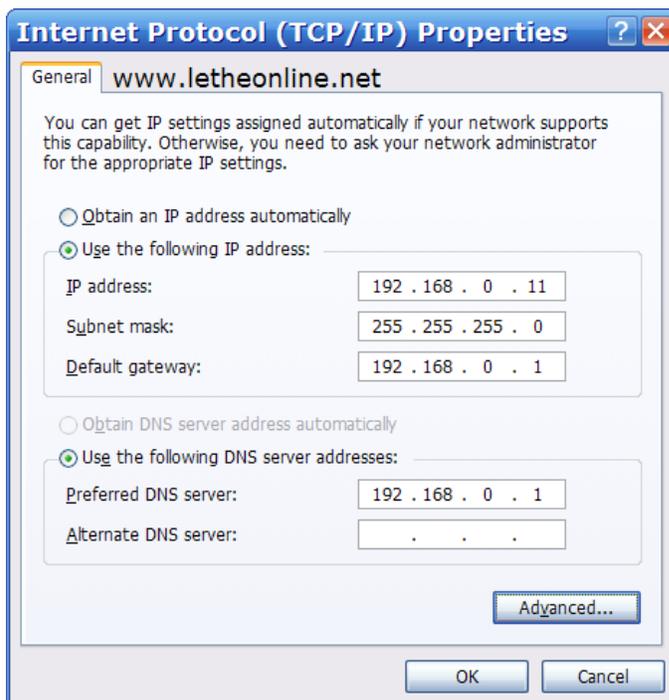
También puedes ejecutar una ventana de dos y digitar IPCONFIG, para más información, IPCONFIG /ALL. En otros Windows, como Windows XP y 2000, puedes ir a las propiedades de la conexión en Mis sitios de red.



Editando la información manualmente

Ahora necesitas conseguir las propiedades del protocolo TCP/IP. Ve al panel de control y haz doble clic en redes. En Windows XP o 2000 tendrás que buscar la conexión y hacer clic con el botón derecho sobre ella y eliges propiedades. Lo mismo en Windows 98, en la caja de propiedades, al ver el protocolo TCP/IP, lo eliges y haces clic en el botón

propiedades. Verás algo como la siguiente caja. Lo que queremos es poder llenar la información manualmente, y si vemos "obtener IP automáticamente" queremos cambiar a la opción cual nos deja digitar la información. Llena la información como ves aquí. Para evitar un conflicto de IP, las computadoras cuales tu estas seguro que siempre estarán conectadas, ponle un IP alto. Por ejemplo los IPs normales son como 192.168.0.3, ponle algo como 192.168.0.10 o 192.168.0.11. De esta manera, al conectar otra computadora, será asignado IPs bajos automáticamente, así como 192.168.0.3 y no causará conflicto. Finalmente, digitamos los DNS servers en la caja debajo.



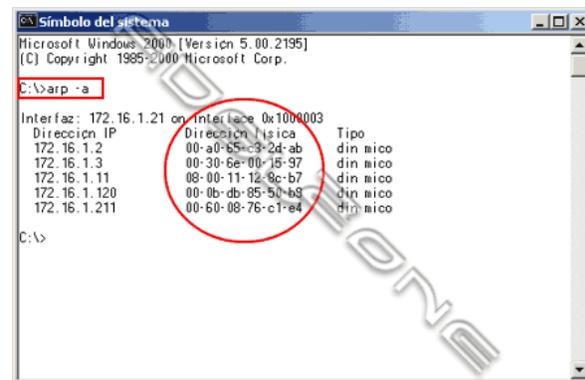
Retornando la configuración

Este paso no es necesario, lo pongo para evitar otro problema si van a cambiar de proveedor de internet, o mover una de las computadoras con IP fijo. Tienes que poner la opción de IP en obtener IP automáticamente, de esta manera la tarjeta de RED no tendrá un IP fijo y va a permitir que otro router o hub (cuál puede ser configurado diferente) le pueda asignar un IP diferente y la conexión a internet funcione.

Denegar acceso por su Mac's address

Vamos a ver consiste en crear un filtro que nos permita denegar el acceso a internet a 2 PC's de nuestra red, pero en lugar de evitarlo por su dirección IP, vamos a hacerlo mediante su direcciones MAC. De esta forma nos aseguramos que aunque cambien de IP el acceso a internet se le niegue igualmente.

Primero debemos de conocer la MAC; una forma sencilla es hacer ping al PC o PC's que nos interese (si es que no ha habido tráfico de paquetes anteriormente entre el nuestro y el otro), y a continuación en MS-DOS ejecutamos el comando **arp -a**, y a nos indica las direcciones físicas de cada equipo:



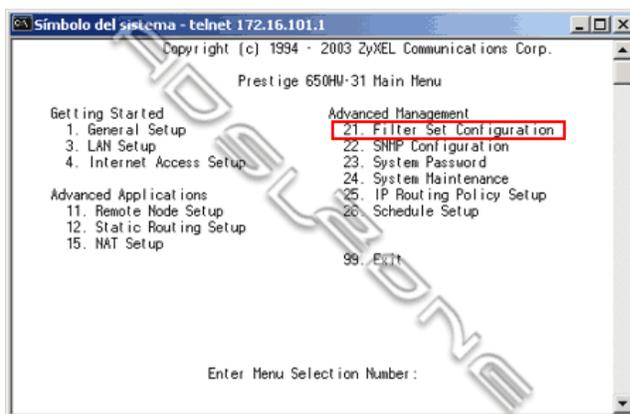
```
Microsoft Windows [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>arp -a

Interfaz: 172.16.1.21 on Interface 0x1000003
Direccion IP      Direccion Fisica      Tipo
172.16.1.2       00-a0-65-c3-2d-ab     din mico
172.16.1.3       00-30-6e-00-15-97     din mico
172.16.1.11      08-00-11-12-8c-b7     din mico
172.16.1.120     00-0b-db-85-50-b3     din mico
172.16.1.211     00-60-08-76-c1-e4     din mico

C:\>
```

Como en ejemplos anteriores accedemos al router mediante TELNET en una sesión MS-DOS. Para ello vamos a la opción **21 Filter Set Configuration** del menú principal, en la que configuraremos los filtros.



```
Microsoft Windows [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>telnet 172.16.101.1

Copyright (c) 1994 - 2003 ZyXEL Communications Corp.

Prestige 650HN-31 Main Menu

Getting Started
1. General Setup
3. LAN Setup
4. Internet Access Setup

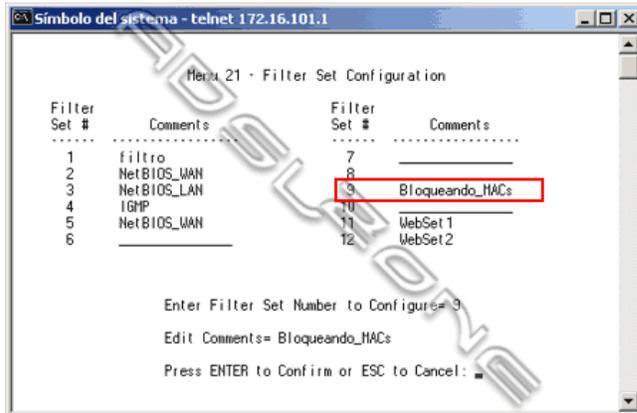
Advanced Applications
11. Remote Node Setup
12. Static Routing Setup
15. NAT Setup

Advanced Management
21. Filter Set Configuration
22. SNMP Configuration
23. System Password
24. System Maintenance
25. IP Routing Policy Setup
26. Schedule Setup

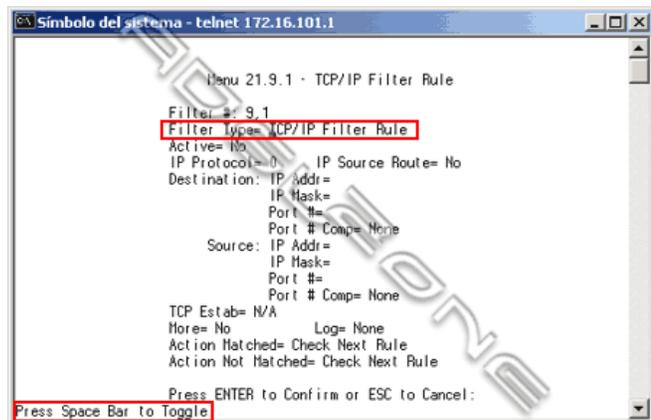
99. Exit

Enter Menu Selection Number :
```

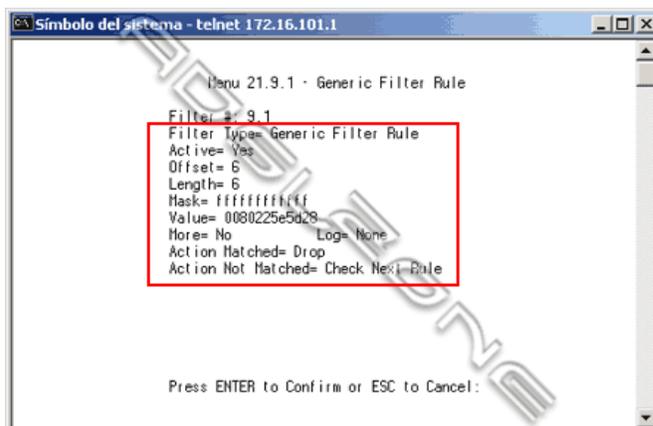
Creamos uno, en este caso el número 9 y le llamamos Bloqueando_MACs.



Y creamos la regla 1 del filtro 9, pero antes debemos de cambiar el tipo de filtro pulsando la barra espaciadora y cambiamos de TCP/IP Filter Rule a Generic Filter Rule.



Y cubrimos los siguientes campos:



Nos centramos en los campos siguientes:

Filter Type : Generic Filter Rule

Active: Yes

Offset: 6 (en el paquete que le llega al router, la dirección MAC comienza en el 7º byte, por lo que debemos de evitar los 6 primeros)

Length: 6 (número de bytes que tiene la MAC)

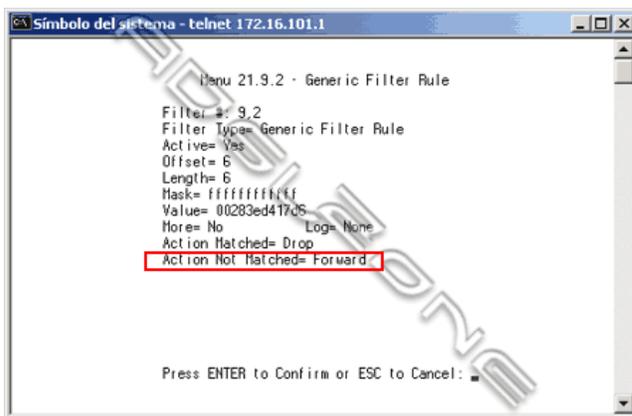
Mask: FFFFFFFF (con esta máscara bloqueamos solo esta MAC, es el "equivalente" a la conocida submask 255.255.255.255)

Value: 0080225e5d28 (dirección MAC del PC)

Action Matched: Drop (en caso de cumplirse la condición, se denegaría el acceso a los paquetes de este PC)

Action Not Matched: Check Next Rule (porque vamos a añadir otra regla a este filtro)

Añadimos la regla 2 del filtro 9 para otro PC.



y como no hay mas reglas, le indicamos que si no se cumplen las anteriores, que se permita el paquete de datos quedando el filtro como se indica a continuación:



Ahora debemos de indicarle al router que filtro debe de aplicar a todos los paquetes que le llegan, para eso en el menu **3.1 LAN Port Filter Setup**, ponemos el filtro **9** (el del ejemplo) en **device filters**, pero no en **protocol filters** que son usados para los filtros TCP/IP.



BIBLIOGRAFIAS:

<http://es.kioskea.net/contents/detection/ids.php3>

<http://auchwell.wordpress.com/2010/01/26/evitar-intruciones-en-nuestro-pc/>

<http://www.adslzone.net/tutorial-12.17.html>

<http://www.letheonline.net/conflicto.htm>

<http://msdn.microsoft.com/es-es/magazine/cc507635.aspx>

[http://msdn.microsoft.com/es-es/library/aa291347\(VS.71\).aspx](http://msdn.microsoft.com/es-es/library/aa291347(VS.71).aspx)

<http://es.wikipedia.org/wiki/Kerberos>

<http://observatorio.cnice.mec.es/modules.php?op=modload&name=News&file=article&sid=341>