Fundamentos de Seguridad en Redes

Por: Yanior Guerrero Guzmán

Las tres principales metas de la seguridad en redes:

- Confidencialidad
- Integridad
- Disponibilidad

Confidencialidad
La confidencialidad se refiere a la protección de los datos frente a accesos no autorizados o de terceras partes.

Integridad
La integridad se refiriere a la seguridad de que los datos enviados no son alterados o destruidos de manera no autorizada. El mensaje enviado debe ser idéntico al recibido.

Disponibilidad
Disponibilidad se define como la continua operatividad de los sistemas de computadoras. Todos los componentes del sistema deben proveer de sus servicios continuamente. Aquí se incluyen los servidores de aplicaciones y de bases de datos, Dispositivos de almacenamiento y las redes punto a punto.

Equilibrio en política de seguridad
Las políticas de seguridad deben permitir acceso transparente y seguro manteniendo un rendimiento óptimo.

- **Acceso transparente:** conectividad, rendimiento, facilidad de uso y manejo, disponibilidad.
- **Seguridad**: Autentificación, autorización, registro de operaciones, seguridad en transacciones, confidencialidad e integridad de datos.

El primer nivel de seguridad
La seguridad de nivel inicial es proveer mecanismos físicos para la protección de los elementos sensibles de la red y de los datos, así como de las copias de seguridad. Las reglas de seguridad dentro de las políticas deben existir antes de que la red se conecte al backbone corporativo. A continuación se citan algunas de las más importantes:

- Proveer de una Buena documentación sobre la corporate security policy
- Controlar la descarga de software
- Asegurarse del buen adiestramiento de los usuarios
- Proveer de una buena documentación sobre el plan de recuperación ante desastres.

La formación de los usuarios es especialmente necesaria en cuanto al uso y control de passwords. La password no se debe compartir con nadie. La información de tu computadora y probablemente la de los demás depende de la fortaleza de tu clave y de lo secreta que esta sea. Por lo tanto para crear una clave de paso se deben tener en cuenta los siguientes criterios:

- La longitud en caracteres de la clave nunca debe ser menor de 8 caracteres
- Mezcle letras mayúsculas con minúsculas, números y símbolos.
- Puede usar las primeras letras de palabras de una canción o una frase, para recordarla sin recurrir a fechas, nombres o cualquier palabra de diccionario.
- Nunca comparta su password con nadie, ni siquiera un amigo, familiar o compañero de trabajo usted ya no tiene el control y ellos se pueden relajar al no ser su propia clave.

Un criterio de seguridad que no se tiene muy en cuenta es que los portátiles encabezan el ranquin del equipamiento informático que más robado y con ellos gran cantidad de información que suele incluir claves de pasos. Se puede prevenir con un cuidado especial a estas piezas e incluso asegurando con candados el portátil al espacio de trabajo. Estos consejos también son extensibles para cualquier hardware y en especial soportes de almacenamiento sobre todo por la información sensible que pueden contener.

Por extraño que parezca existen los llamados Dumpters drivers que son personas que hacen un uso muy particular de ingeniería social para buscar debilidades y posibles claves. Los husmeadores de basura buscan en papeleras de reciclaje, canastas de fax, papeleras normales y a veces en la basura documentos que revelen alguna clave de usuario o alguna información que le pueda ayudar a adivinarla. Cuando se quiera deshacer de información confidencial asegúrese primero de destruirla (incluyendo aquí también soportes como CD, Disquetes, etc.).

Vulnerabilidad, amenazas y ataques

Vulnerabilidad es una debilidad intrínseca en las redes y dispositivos. Esto incluye a los routers, switches, equipos de escritorio, servidores e incluso a los propios sistemas de seguridad. Los atacantes son personas con cierto nivel de cualificación que les permite tomar ventajas sobre las debilidades de un sistema. Finalmente usan una variedad de herramientas, scripts y programas que les permiten lanzar su ataque. El nivel de seguridad del sistema determinará el número y la envergadura de la amenaza posible.

Las tres vulnerabilidades primarias son:

- Debilidades tecnológicas
- Debilidades de configuración.
- Debilidades de la política de seguridad.
-

Debilidades tecnológicas

Las computadoras y las redes tienen flaquezas de seguridad intrínsecas incluyendo las del propio protocolo TCP/IP, sistemas operativos y equipos de networking.

Debilidades de configuración

Configuraciones operativas pero que no compensan con ellas las debilidades de los dispositivos de red. Ejemplo no configurar la clave de paso del usuario administrador de un dispositivo de red como por ejemplo un router, o hacerlo sin activar el cifrado de las claves.

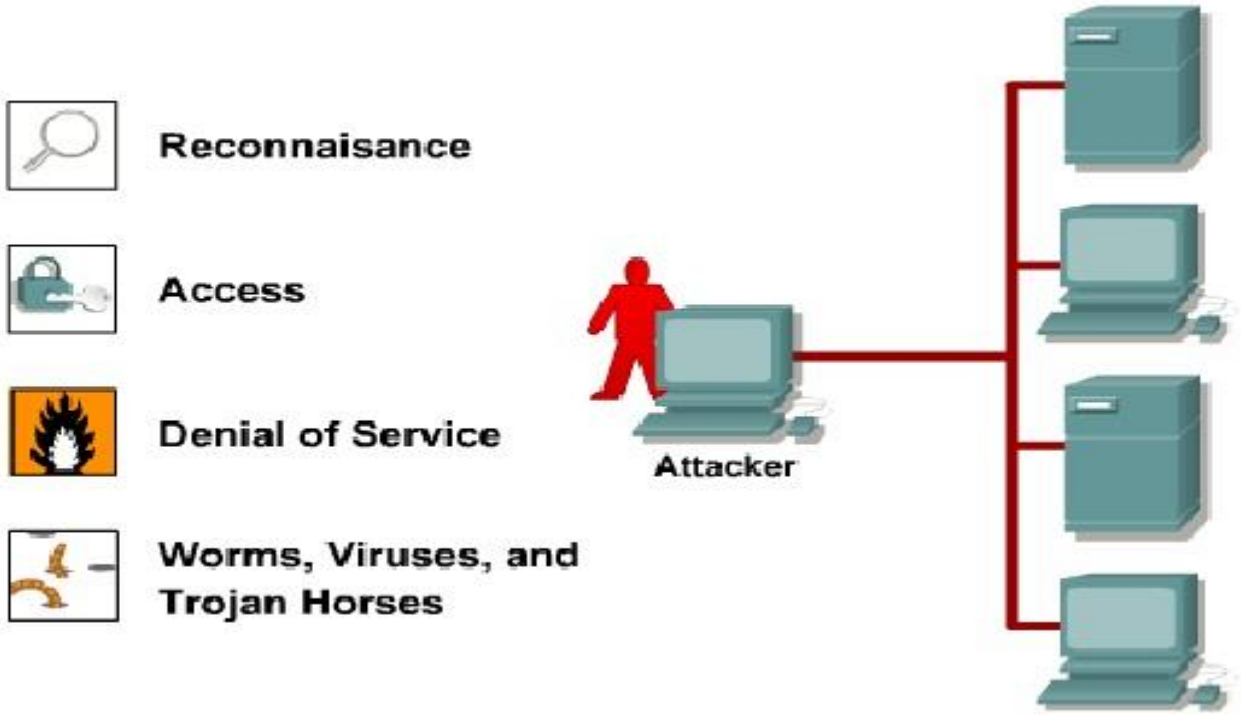
Debilidades de la política de seguridad

Provienen normalmente del incumplimiento de las reglas de seguridad por parte de los usuarios o por desconocimiento de posibles amenazas no contempladas en el diseño.

Hay 4 clases primarias de amenazas a la seguridad de la red.

1. **Unstructured threats (Amenazas no estructuradas) (Hakers):** principalmente son ataques de individuos inexpertos que utilizan herramientas sencillas de ataque disponibles en Internet así como algunos shell scripts y password crackers
2. **Structured threats (Crakers):** provienen de hackers que están mas motivados y tecnológicamente más competente. Este tipo de personas conoce las vulnerabilidades del sistemay pueden entenderlas y crear exploit-code y scripts para un ataque más refinado.
3. **External threats:** Los ataques externos provienen de individuos u organizaciones Externas a la compañía..
4. **Internal threats:** Los ataques internos provienen de alguien que tiene acceso autorizado a nuestro sistema ya sea con una cuenta en nuestro servidor de autentificación o bien acceso físico a nuestros equipos y nuestra red..

Hay cuatro clases de ataques primarios
Como se muestra en las figura siguiente



1. **Reconnaissance**: Reconocimiento es un descubrimiento y mapeo de nuestro sistema, servicios y posibles vulnerabilidades. Es conocido como recuento de información previa a un ataque. Y en la mayoría de los casos precede a un ataque Denialof Service (DoS). Reconocimiento es como el ladrón que estudia una residencia para ver el punto de entrada más débil para llegar a la casa objetivo.
2. **Access (Acceso)**: El acceso es la habilidad del intruso para ganar acceso no autorizado en un dispositivo en el que inicialmente no tiene cuenta ni clave de paso. Esto implica que el intruso previamente a conseguido una cuenta por descuido de un usuario y posiblemente la clave o bien ha ejecutado un script para

romperla o ha explotado una vulnerabilidad del sistema o de una aplicación que este atacando normalmente con el interés de ganar acceso como usuario root.

3. **Denial of service (DoS):** En un ataque Denial of service (DoS) el atacante consigue deshabilitar o corromper servicios de red con la intención de que los usuarios de la red no puedan hacer uso de ellos. Los ataques DoS implican el crashing del sistema o el relencitamiento hasta el punto de su casi inutilidad. Aunque algunos ataques DoS pueden ser tan simples como borrar o corromper información en la mayoría de ellos consisten en la ejecución no autorizada de un hackscript. El atacante no necesita privilegios especiales en el dispositivo o servicio destino si bien es el objetivo que desean finalmente conseguir. Porello suelen ser tan ferores.
4. **Worms, Viruses, and Trojan horses**: El software malicioso se inserta en un host con el único objetivo de dañar el sistema o la red , corromper ficheros, replicarse y en muchos casos finalizar denegando el acceso a la red y/o al sistema o a un servicio de este. Hoy en día las herramientas de ataque son poderosas y por desgracia cubren nuevos peligros más sofisticados como por ejemplo gusanos como Slamer y´Blaster y los nuevos ataques DoS.

Los ataques de reconocimiento pueden consistir en lo siguiente:

- Packet sniffers
- Port scans
- Ping sweeps
- Internet information queries

Ejemplos obtener ip posibles de atacar con nslookup, consultas whois enorganismos como ARIN organismo de registro de direcciones de Internet http://ws.arin.net/cgi-bin/whois.pl

Network snooping and packet sniffing son términos comunes para describir eleavesdropping (espionaje). Eavesdropping consiste en escuchar conversaciones(sesiones de red), espiando y en muchos casos capturando paquetes de datos la información obtenida puede ser usada como base para otros ataques más severoen la red. Un ejemplo de datos susceptibles de eavesdropping es el protocolo SNMP version1 community strings, -que se envía con texto plano (sin cifrar). Un intruso podríaespiar las peticiones SNMP y obtener información relevante de la red y de los equipos interconectados. Otro ejemplo consiste en la captura de cuentas de usuarios y claves de paso conforme cruzan la red.

Tipos de eavesdropping

Un método común de espionaje en comunicaciones es capturar paquetes TCP/IP ode otro tipo y decodificar el contenido usando un analizador de protocolo unautilidad similar. Los dos usos más frecuentes son:

- **Information gathering**: Identificación de usuarios y claves de paso o información que transporte números de tarjetas de credito o informaciónpersonal sensible.
- **Information theft**: Robo de información etwork, el espia puede capturar la información conforme circula en la intranet o en internet con el interés detener copia o incluso ocultarla a su destinatario. Su principales objetivos son instituciones financieras y números de tarjetas de crédito. Otro ejemplo es intentar capturar y crackear un fichero de claves

Herramientas usadas para realizar avesdropping

Las siguientes herramientas se usan para el espionaje en red:

- Analizadores de red o de protocolos
- Capturadores de paquetes en entornos de red local

Metodos para contrarestar estos ataques
Two of the most effective methods for counteracting eavesdropping are as follows:

1. Implementar y forzar el uso de directivas de seguridad que prohiban el empleo de protocolos con debilidades conocidas para sufrir eavesdropping
2. Usar sistemas de cifrado (Data encryption) que aseguren las necesidades mínimas de la organización sin imponer un excesivo uso de recursos delsistema o de los usuarios.
3. Implementar redes totalmente conmutadas (switched networks)

Cifrado de datos (Encrypted data)
El cifrado de asegura los datos susceptibles de ataques de espionaje, claves de paso o simplemente la manipulación indebida de la información. Algunos beneficios que aporta el cifrado son los siguientes:

- Almost every company has transactions, which, if viewed by aneavesdropper, could have negative consequences. El cifrado asegura queestos datos sensibles atraviesen la red sin poder ser observados e inclusocon ayuda de algunas técnicas de firma digital averiguar si han sido cambiados o alterados.
- El descifrado es necesario cuando los datos alcanzan el destinatario en lared donde resida es muy importante que el sistema de descifrado sólo pueda realizarlo el destinatario implicado.
- Si el cifrado se realiza después de las cabeceras de datagrama UDP o TCP deforma que solo este cifrado los datos transportados permite que todos los routers intermedios y switches encaminen o reenvíen el trafico como si se tratara de cualquier otro paquete preservando la calidad de servicio (QoS)en el tráfico de la red y trasladando el peso del proceso sólo a los equipos terminales de la comunicación..

Password Attacks
Los ataques a claves de paso pueden ser implementados usando varios métodos incluyendo el de fuerza bruta. , Caballos de troya, IP spoofing, y packet sniffers. Aunque el packet sniffers y el IP spoofing pueden capturar cuentas de usuarios y sus claves; Los ataques para obtener claves normalmente consisten en repetidos intentos para identificar el usuario posible y su contraseña posible usando varias combinaciones de caracteres. Estos intentos reciben el nombre de ataques por fuerza bruta.

Lo normal es que el ataque de fuerza bruta se realice con un programa que escudriña la red buscando recursos compartidos, servicios y servidores donde intentar pasar el nivel de seguridad de Login-in.

Si el atacante tiene éxito y gana acceso al recurso tendrá los mismos privilegios que el usuario cuya cuenta ha sido comprometida y si es una cuenta con privilegios suficientes el agujero de seguridad es proporcional a estos. Normalmente el atacante intentará crear una puerta trasera para futuros accesos sin cambiar el estado ni la clave de la cuenta capturada y no levantar sospechas.

Los métodos más comunes de los programas de fuerza bruta son:

- Dictionary cracking—Ataques de diccionario Los hashes de todas las claves se comparan con los hashes de todas las palabras de un diccionario para cada uno de los usuarios. Este método es extremadamente rápido y permite encontrar todas las claves simples.
- Brute-force computation—Computación de cracteres Este método utiliza un particular conjunto de caracteres como desde la A-Z or A-Z más 0-9 y computa el hash para cada posible combinación de N de esos caracteres conel de la posible password, su inconveniente es el tiempo requerido para completar el ataque.
- Este método usa un juego de caracteres en particular, como AZ o AZ plus 09, y calcula el hash para cada contraseña posible compuesta por esos caracteres. Siempre calculará la contraseña si esa contraseña se compone del conjunto de caracteres que ha seleccionado para probar. El inconveniente es que se necesita tiempo para completar este tipo de ataque.

Trust exploitation
Aunque es más una técnica que un ataque en si mismo, La explotación de confianzas se refiere a un ataque en el cual un individuo toma ventajas de una relación de confianza en una red. Un ejemplo clásico es una conexión perimetral a una red desde otra corporativa . Estas segmentos de red a menudo albergan dominios DNS, servidores SMTP y HTTP, Como estos servidores suelen estar en el mismo segmento el compromiso de uno suele implicar el posible compromiso de los otros porque los sistemas normalmente mantienen confianzas entre ellos.

Otro ejemplo es un sistema fuera del firewall que mantiene una confianza con otro dentro del cortafuego. Cuando el sistema externo está comprometido a través de él se puede obtener ventajas para atacar al interno. Otro forma de acceso involucra un escala en los privilegios, esto ocurre cuando un usuario obtiene privilegios o derechos especiales que no habían sido asignados directamente al usuario por el administrador sino que han sido heredados indebidamente en el acceso sobre objetos. Estos objetos pueden ser ficheros, comandos, programas o sobre componentes y dispositivos de red. Su intención es ganar privilegios administrativos que le permitan instalar sniffers, crear puertas traseras y poder borrar los ficheros de Log para eliminar huellas.

Los ataques de explotación de confianza se pueden mitigar a través de unas ajustadas restricciones en el nivel de seguridad sin sobrepasar las funciones que deben cubrir la confianza en una red. Para los sistemas externos al corta fuego nunca asignar privilegios absolutos para un sistema en el interior, tales confianzas deben limitarse a protocolos específicos y deben ser autentificados severamente por algo más que la IP siempre que sea posible

Port Redirection
El ataque de re-dirección de puertos es un tipo de ataque de explotación de confianza que utiliza un host con seguridad comprometida para pasar el trafico a través del cortafuego el cual de otro modo hubiese sido eliminado. Considere un firewall con tres interfaces y un host en cada interfaz El host externo puede alcanzar otro en el segmento donde están los servicios públicos (comúnmente conocido como zona desmilitarizada DMZ ; pero no un host interno. El host en lazona DMZ sin embargo si puede alcanzar el hos interno, si un hacker fuera capaz de comprometer el equipo de la zona DMZ podría intentar instalar software redirector de trafico desde el host externo al interno. De esta forma ninguna de las comunicaciones (host externo a intermedio, e intermedio a interno) incumplirían las reglas del cortafuego, ahora el host externo mediante el proceso de redirección de puerto en el servidor público tiene un tunel hacia el interno. Un programa ejemplo que puede realizar este tipo de tareas es NETCAT.Como se ha indicado anteriormente para minimizar este tipo de ataque es el uso de modelo de relación de confianza especifico en cada red, asumiendo un sistema bajo ataque un host basado en software detector IDS puede detectar un hacker y prevenir la instalación de este tipo de utilidades en el equipo intermedio.

Man-in-the-middle attack
El ataque denominado como hombre en el medio requiere que el hacker tenga acceso a los paquetes que cruzan a través de la red donde se encuentra.

Un ejemplo podría ser alguien que está trabajando en un ISP y tiene acceso a los paquetes que se transfieren entre las redes de los usuarios y la del propio PSI(Proveedor de Servicios de Internet).

Estos ataques se implementan normalmente utilizando Sniffers y protocolos de enrutamiento y transporte. El uso posible de este ataque es el robo de información,hijacking de una sesión para ganar acceso a una red privada, análisis del trafico para derivar información acerca de una red, de sus usuarios y sus preferencias,búsqueda de un posible DoS, corrupción de datos y suplantación de información y sesiones.

El ataque Man-in-the-middle se puede mitigar mediante el cifrado en un túnel IPSecque solo le permitiría ver datos cifrados.

Social engineering (Ingenieria social)
Es el sistema más simple y no necesita de un gran nivel de conocimientos informáticos, solo debe ser capaz de obtener información de cierto valor como localización de los servidores, de los ficheros importantes, usuarios existentes y posiblemente mediante engaños también claves. Luego el proceso de hacking es más simple.

DoS

Los siguientes son algunos de las amenazas (tretas) DoS más comunes:

- **Ping of death** – Ping de la muerte .Este ataque modifica la cabecera IP para indicar que hay más datos en el paquete de los que realmente se transportan causando que el sistema receptor se bloquee.
- **SYN flood attack** – Ataque por inundación SYN. Este ataque abrealeatoriamente muchos puertos y muchas conexiones TCP, intentandoestablecer el máximo de conexiones ficticias posibles para negar acceso posible a otros usuarios. Este ataque se suele ejecutar con analizadores de protocolos u tros específicos y más egfectivos.
- **Packet fragmentation and reassembly** – Este ataque explota el desbordamiento del buffer (buffer–overrun bug) en un PC o equipo de interconexión de red.
- **E-mail bombs** – Bomba E-Mail es un programa capaz de enviar E-Mailsinutiles a individuos, lista de correos o dominios monopolizando el servidor de correo.
- **CPU hogging** – Este ataque consiste en programas tales como troyanos ovirus que ahogan la CPU consumiendo el máximo posible de ciclos de reloj,memoria u otros recursos..
- **Malicious applets** – Este ataque proviene de códigos Java, JavaScript, oActiveX que actuan como troyanos o virus para conseguir destrucción dedatos o captura de recursos del sistema.
- **Misconfiguring routers** – Desconfiguración de routers para crear un bucle de enrutamiento deshabilitando el tráfico especialmente el Web.
- **The chargen attack** – Este ataque establece conexiones entre servicios UDP, produciendo un intenso intercambio de datos. El host de intercambio de datos es conectado al servicio Echo en el mismo o en un sistema diferente causando la congestión de la red con el trafico de eco.
- **Out-of-band attacks such as WinNuke** – Este ataque envía datos fuera de rango al Puerto 139 en un equipo con Widows 95 o NT 4. Se requiere la dirección IP de la víctima antes de lanzar el ataque.
- **Denial of Service** - DoS puede ocurrir accidentalmente causado por una mala configuración o mal uso proveniente de un usuario legitimado por elsistema o un administrador.
- **Land.c** – Programas que envían paquetes TCP SYN en los que tanto eldestinatario como el origen son la misma dirección IP. También suelen usarel mismo Puerto de

origen y destino (como el 113 o el 139) en el host destino causa el bloqueo del sistema.
- **Teardrop.c** – Ien este ataque se provoca un proceso de fragmentación depaquetes IP de tal modo que su reensamblado causa problemas en el destino y aborta la comunicación.
- **Targa.c** – Ataque DoS Multiplataforma que integra ataques llamados bonk, jolt, land, nestea, netear, syndrop, teardrop, y winnuke en un solo exploit.

Masquerade/IP spoofing (Enmascaramiento ilicito de IP)

Con este ataque, el intruso es capaz de manipular paquetes TCP/IP falsificando ladirección IP origen, aparentado ser otro usuario. El intruso asume pues la identidad de un usuario válido obteniendo sus privilegios en los sistemas que sólo validen suIP. Durante un ataque.

IP Spoofing el atacante externo a la red pretende parecer una computadora válida tomando una IP válida en el rango de la red o usando una IPexterna autorizada para acceder a ciertos recursos de red.

Normalmente el spoofing solo persigue insertar datos o comandos malintencionados en un stream de datos pasados entre un cliente y un servidor o una comunicación peer-to-peer. El atacante no espera respuesta de las aplicaciones atacadas no le importa. Es el ataque típico a debilidades conocidas de servidores DNS.

Si persiguiera obtener respuesta el atacante debería cambiar las tablas de enrutamiento para que apuntasen a una IP falsificada (spoofed IP).

Esto implicaría recibir todo el trafico destinado a esa red IP e intentar responder como lo haría otro usuario. Por desgracia esta técnica no solo la usan los atacantes externos siendo si cabe más común en atacantes internos.

Algunas de las herramientas que se suelen usar con esta técnica son las siguientes:
- Analizadores de protocolo y password sniffers
- Modificación de número de secuencia
- Herramientas de escaneo que prueban puertos TCP para servicios específicos, redes o arquitecturas de sistema o ciertos S.O.

Después de obtener información de las herramientas de escaneo el intruso buscalas vulnerabilidades asociadas a estos.

Distributed DoS (DDoS)

Este ataque intenta saturar la red con datos espureos.

DDoS usa un sistema de ataque similar al estándar DoS pero opera a una mayor escala. Típicamente cientos o miles de puntos de ataque para saturar o abatir al equipo destino.

Ejemplos de ataques DDoS :
- Smurf
- Tribe Flood Network (TFN)
- Stacheldraht

SMURF attack: El ataque Smurf se inicia perpetrando un envío masivo de paquetes ICMP echo request, es decir ping, con una spoofed IP hacia una dirección de broadcast con la esperanza de que se magnificara la respuesta hacia la IP falsificada, que es el objetivo del ataque. Si el dispositivo de enrutamiento además ejecuta Broadcast de capa 3 hacia broadcast de capa 2 se multiplicara el trafico por el numero de host con respuesta a los paquetes eco.

Ejemplo asumiendo una red de 100 hosts y que el atacante utiliza un enlace T1. El atacante envía stream de 768 kbps de ICMP echo o paquetes PING con la IP de la victima falsificada y con destino la IP de broadcast del sitio de rebote. El ping golpea el sitio de rebote con un broadcast que responden 100 ordenadores hacia el equipo falseado por la IP de origen un total de 76.8 Mbs de ancho de banda se usan en las respuestas a los ping desde el sitio de rebote una vez multiplicado el trafico.

Deshabilitando la capacidad de broadcast dirigidos en la infraestructura de la red se previene que sea usada como sitio de rebote.

Tribe flood network (TFN): La inundación de tribu en la red (TFN) y La inundación de tribu en la red 2000 (TFN2K) son herramientas distribuidas usadas para lanzar ataques DoS coordinados desde muchas Fuentes contra uno o más destinos. Un ataque TFN tiene la capacidad de generar paquetes con IP origen falsificada el intruso atacante envía instrucciones a un equipo con software master para que las reenvié a la lista de servidores TFN o demonio o programas residentes que generan el ataque específico sobre el destino la IP de origen y el puerto pueden ser aleatorios y el tamaño de los paquetes alterado. Por suerte el uso de un TFN Master dentro de la red origen del ataque magnificado implica obtener fácilmente la lista de los equipos infectados con el TFN Server

Stacheldraht attack: Stacheldraht, Germanismo de "barbed wire" “alambre deespinos”, combina características de varios ataques DoS , incluyendo Tribe FloodNetwork (TFN). También añade características especiales como el cifrado de la comunicación entre el atacante y el stacheldraht masters, y la actualización automática de los agentes. Hay una fase inicial de máxima intrución en la cual una herramienta automática se usa para comprometer un gran número de equipos controlados remotamente como root (RootKit) para luego ser usados en el ataque DoS hacia otros sistemas.

Malware (Software malicioso): Worm, virus, and Trojan horse, Spayware,SpanWorm, virus, and Trojan horse

Worms (Gusanos)
La anatomía de ataque de software gusano consiste en:El gusano se instala el mismo aprovechándose de una debilidad del sistema o de un exploit que la provoque.

- Mecanismo de propagación—Después de conseguir el acceso a un equipo el gusano se replica y selecciona nuevas victimas.
- Payload (carga útil)—Tras haber infectado un dispositivo con un gusano el atacante tiene acceso a él con privilegios de usuario y puede usar otros exploit locales para escalar en privilegios hasta el nivel de administrador.

Lo normal es que un gusano sea un programa que se auto contiene y se replica solo copiándose en el destino explotando vulnerabilidades de los sistemas volviendo a empezar el ciclo. Mientras que un virus requiere un vector para su transporte su código de un sistema a otro. Un vector puede ser un documento de procesador de texto, hoja de cálculo, etc con macros o script embebidos,, un E-mail o un ejecutable con el virus

incrustado, los más antiguos lo hacían en el sector de arranque de soportes removibles. La clave diferencial entre un virus y un gusano es que el primero require la interacción del ser humano para facilitar su expansión. Para mitigar los ataques de los gusanos se requiere una rápida intervención para aislar la parte del sistema infectado. Para ello es necesaria una correcta coordinación entre los administradores de sistemas, los ingenieros de redes y los operarios de seguridad para una rápida detección y respuesta ante un incidente de un gusano. A continuación están los pasos recomendados para mitigar un ataque de un gusano:

1. Contención
2. Vacunación
3. Cuarentena
4. Tratamiento

Viruses and Trojan Horses(Virus y caballos de Troya)

Los Virus son software malicioso que se adjuntan a otro programa y que ejecutan un función indeseada en la estación de trabajo del usuario. Un troyano se diferencia solo en que el programa entero esta hecho para parecer una utilidad cuando de hecho es una herramienta que un atacante tiene dentro de nuestro sistema y que normalmente se introduce vía E-Mail.

La seguridad de una red es un proceso constante construido en base a unas políticas de seguridad.

Para comenzar la la rueda de la seguridad primero se desarrolla la política de seguridad junto con los criterios de ponderación y cumpliendo las siguientes tareas:

- Identificar los objetivos para la seguridad en la organización.
- Documentar los recursos a proteger.
- Identificar la infraestructura de la red con mapas de red e inventarios actualizados
- Identificar los recursos críticos que necesitan ser protegidos, como los departamentos de finanzas, recursos humanos, desarrollo. A esto se le llama

Análisis de riesgos

Tras desarrollar la política de seguridad, realiza un recorrido de prueba a de seguridad con los 4 pasos de la rueda de seguridad. Estos pasos de la rueda de seguridad son 1º asegurar, 2º Monitorizar, 3º Testear y4º Mejorar y vuelta a empezar

Secure

Asegure su red aplicando políticas de seguridad que incluyan antivirus en todos los equipos y su constante actualización e implementando las siguientes soluciones de seguridad Threat Defense: Permita sólo el trafico y los servicios válidos y necesarios. IntrusionPrevention Systems (IPS), y también un sistema Inline intrusion detection systems(IDS), Controle las vulnerabilidades del sistema con los últimos parches-Vulnerability patchingUtilice conexiones seguras : VPNs, SSH, SSL Trust and Identity

- Authentication
- Policy enforcement

Monitor
Monitorear la seguridad implica dos métodos simultáneos activo y pasivo. El método activo más común es la auditoría de los ficheros de LOG.

Los métodos pasivos incluyen el uso de dispositivos intrusion detection system(IDS) para detectar automáticamente intrusiones. Este método require un pequeño grupo de administradores de red para mantener actualizada la monitorización. Estos sistemas pueden detectar violaciones de seguridad en tiempo real y pueden ser configurados para ofrecer una respuesta automática antes de que el intruso cause daños.

Test
En la fase de testeo de la rueda de la seguridad, La seguridad de la red es chequeada de forma proactiva.

Improve (mejoras)
La fase de mejoras de la rueda de la seguridad implica el análisis de los datos recabados durante la monitorización y el testeo y posteriormente implementar mecanismos de mejora que se documentaran en las políticas de seguridad y se implementarán en la fase de aseguramiento de la red. Para mantener una red loa más segura posible este ciclo se debe repetir permanentemente puesto que nuevos riesgos y vulnerabilidades aparecen cada día.