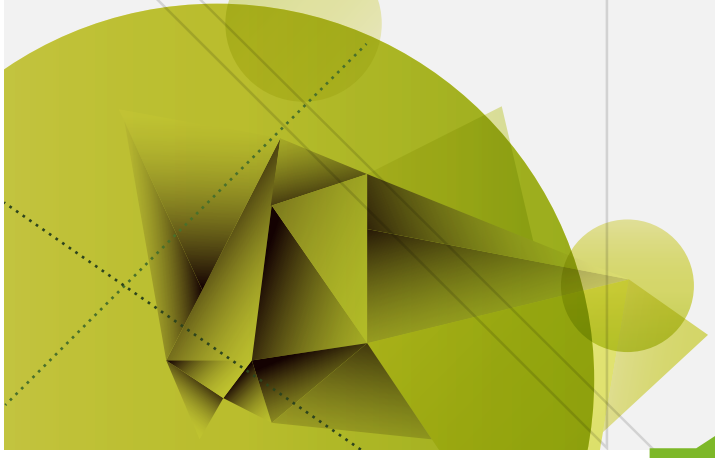
Seguridad en redes



Autor: Esteban Bejarano Forero

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Esteban Bejarano Forero / Carlos Andrés Díaz, / Bogotá D.C., Fundación Universitaria del Área Andina. 2017

978-958-5455-80-1

Catalogación en la fuente Fundación Universitaria del Área Andina (Bogotá).

Edición:
Fondo editorial Areandino
Fundación Universitaria del Área Andina
Calle 71 11-14, Bogotá D.C., Colombia
Tel.: (57-1) 7 42 19 64 ext. 1228
E-mail: publicaciones@areandina.edu.co
http://www.areandina.edu.co

Primera edición: noviembre de 2017

Corrección de estilo, diagramación y edición: Dirección Nacional de Operaciones virtuales
Diseño y compilación electrónica: Dirección Nacional de Investigación

Hecho en Colombia
Made in Colombia

Seguridad en redes

Autor: Esteban Bejarano Forero

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

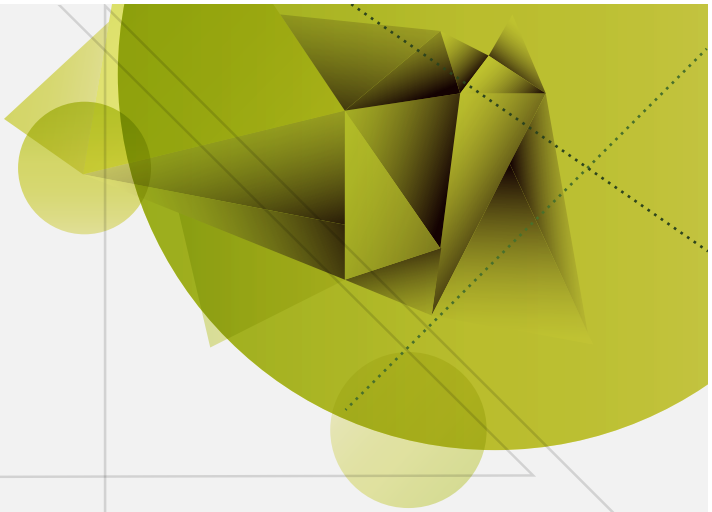
Índice

Índice

1

Unidad 1

Conceptos de seguridad



Seguridad en redes

Autor: Esteban Bejarano Forero

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

Por medio este módulo de Seguridad en redes, se buscará que el estudiante haga una preámbulo al amplio mundo de la seguridad, entendiendo la necesidad de proteger la información, ya que ese es el valor más preciado en toca empresa o entidad gubernamental.

Para lograr este objetivo, primeramente se verán los conceptos básicos de lo que se refiere a seguridad en la red, por qué se debe proteger la red contra quién o contra qué se debe proteger y el impacto que esto genera dentro de una organización, ya que en la actualidad es necesario que exista personal encargado de brindar soluciones de seguridad ya que constantemente hay amenazas de violación a la información. Como profesionales o como estudiantes, ustedes tienen la oportunidad de profundizar en toda esta gama amplia de la informática, ya que a nivel laboral es muy solicitado un profesional especializado en seguridad.

U1 Metodología

Como lectura de introducción, será de fácil entendimiento para el estudiante. Tómese el tiempo necesario para hacer la lectura concienzudamente. De desconocer algún concepto, se pueden apoyar en el Glosario general que aparece en el contenido del curso.

U1

Desarrollo temático

Conceptos de seguridad

Desde los inicios de los años 60, el concepto de redes se ha venido desarrollando de manera exponencial, pero desde sus inicios, el tema de seguridad en las redes no era un factor importante, no existía muchos conocimientos para atacar una red. Los primeros usuarios no buscaban afectar las actividades de las empresas o de otros usuarios. Internet no era un "lugar" seguro, ya que en ese momento no requería serlo.

No fue hasta finales del año 1988, cuando se comenzó a tomar muy en serio el tema de la seguridad en la red. El exponencial crecimiento del Internet, servicio que estaba dejando de ser exclusivo de las organizaciones Gubernamentales o de las grandes empresas; permitiendo así que otros sectores u personas pudieran acceder a este servicio. Por supuesto esto abrió las puertas para poder explorar más allá, generando nuevas amenazas contra las redes y la información que por ellas se mueve.

Un claro ejemplo de amenaza, el cual prendió las alarmas, fue protagonizado por Robert T. Morris en 1988. El cual fue el creador de un poderoso Worm (gusano) de internet y se encargó de transmitirlo en la red. Muchos ordenadores conectados a la red de internet quedaron infectados por este Gusano y quedaron inutilizables por varios días. Esto por supuesto generó un gran caos dentro de cada empresa afectada por esta infección en la red, sin mencionar las grandes pérdidas en millones de dólares que esto generó a nivel global.

Poco después de sucedido este incidente, se comenzaron a crear agencias para proteger la información y que este tipo de ataques no volvieran a suceder y si sucedían, encontrar una pronta solución a esto.

Con el paso de los años, se han hecho grandes esfuerzos, para proteger la información, pero paralelo a esto, los piratas informáticos o mejor conocidos como hackers han crecido en conocimiento ayudados por los rápidos y constantes cambios en la tecnología computacional y por la red de internet. Ahora la información es mucho más sencilla de compartir y poseer, esto permite que muchas más personas tengan a su alcance el conocimiento para poder ingresar a una red privada y atacarla o ver su contenido por sólo curiosidad.

Por estos motivos, en ese entonces y en la actualidad, es requerido crear mecanismos de protección de los datos y lo más importante, se requiere de gente preparada que pueda manejar estos sistemas de seguridad.

Definiciones

El concepto básico de la seguridad en redes se puede definir como:

Garantizar que se mantenga la información (de una empresa, entidad gubernamental, etc.) de manera íntegra, privada (confidencial), controlada, autentificada y disponible (solo para el personal autorizado), mediante políticas de seguridad informática (PSI). Más adelante se estudiará a profundidad este concepto.

Imagen 1. Red segura
Fuente: http://www.xpress.es/media/cache/size_6/uploads/webUsers/536/105/0fd/2b7/0a7/934/2d7/0b3/image/seguridad-de-la-informacion-536a010c9acd4.png

En todo caso, hay que reconocer que es 100% imposible tener una red segura, ya que siempre habrá algún lugar por dónde puede ser atacada la información, bien conocemos casos de entidades muy protegidas, o que se consideran muy seguras que a pesar de todo, sus páginas web o servidores fueron hackeadas o su seguridad fue vulnerada. Por eso es que en la seguridad de las redes, se debe buscar la fiabilidad (ver imagen 2), para que los datos transmitidos en una red actúen normalmente. Disminuyendo el riesgo de recibir ataques.

Como se puede ver en la imagen 2 la fiabilidad de la red encontramos tres conceptos ya mencionados anteriormente:

Confidencialidad, se busca que la información sea de uso o conocimiento exclusivo de un pequeño sector en la compañía, no es recomendable que todos los empleados tengan permisos de acceso y puedan afectar la **Integridad,** lo cual implicaría que los datos podrían ser manipulados, cambiados, borrados de su origen. Finalmente se encuentra la **Disponibilidad,** la cual le permite sólo al personal autorizado ingresar en cualquier momento y realizar actividades de Lectura y escritura sobre la información.

Fiabilidad de la red		
Confidencialidad	Integridad	Disponibilidad
Acceso a personal autorizado.	Los datos solo pueden ser modificados por los agentes o personal autorizado.	Pueden acceder en cualquier momento por los agentes autorizados.

Figura 1. Fiabilidad de la Red
Fuente: Propia.

Seguridad global

Para poder comprender el concepto de la seguridad global, primero debemos partir por los conceptos primarios de una red, los equipos que la componen:

Una red básica está compuesta por sistemas de comunicaciones: Routers, Switch, Firewalls, Access Point. Con ellos se pueden conectar equipos que requieren comunicarse entre sí: PC, Laptops, servidores, impresoras, teléfonos IP, etc. Toda la unión de esta red, se le conoce como red LAN (*Local Area Network o Red de Área Local*).

Un claro ejemplo de una red LAN, puede ser la imagen que se muestra a continuación:

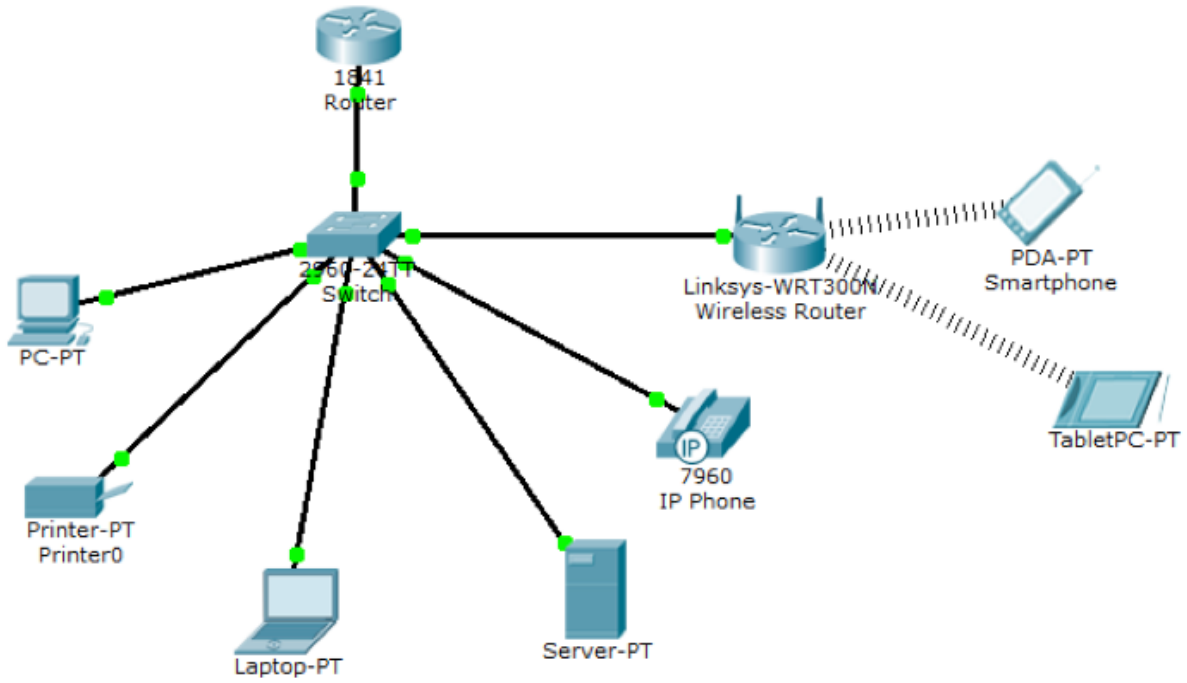


Imagen 2. LAN Oficina 1
Fuente: Propia.

En la imagen 2, se muestra un router, el cual no es necesario dentro de una sola red LAN, pero si se requiere conectar a otras redes LAN que no sean cercanas o si se requiere salida hacia internet, se necesita utilizar un router y la conectividad hacia el exterior que la puede ofrecer un proveedor de servicios de Telecomunicaciones, de tal manera que:

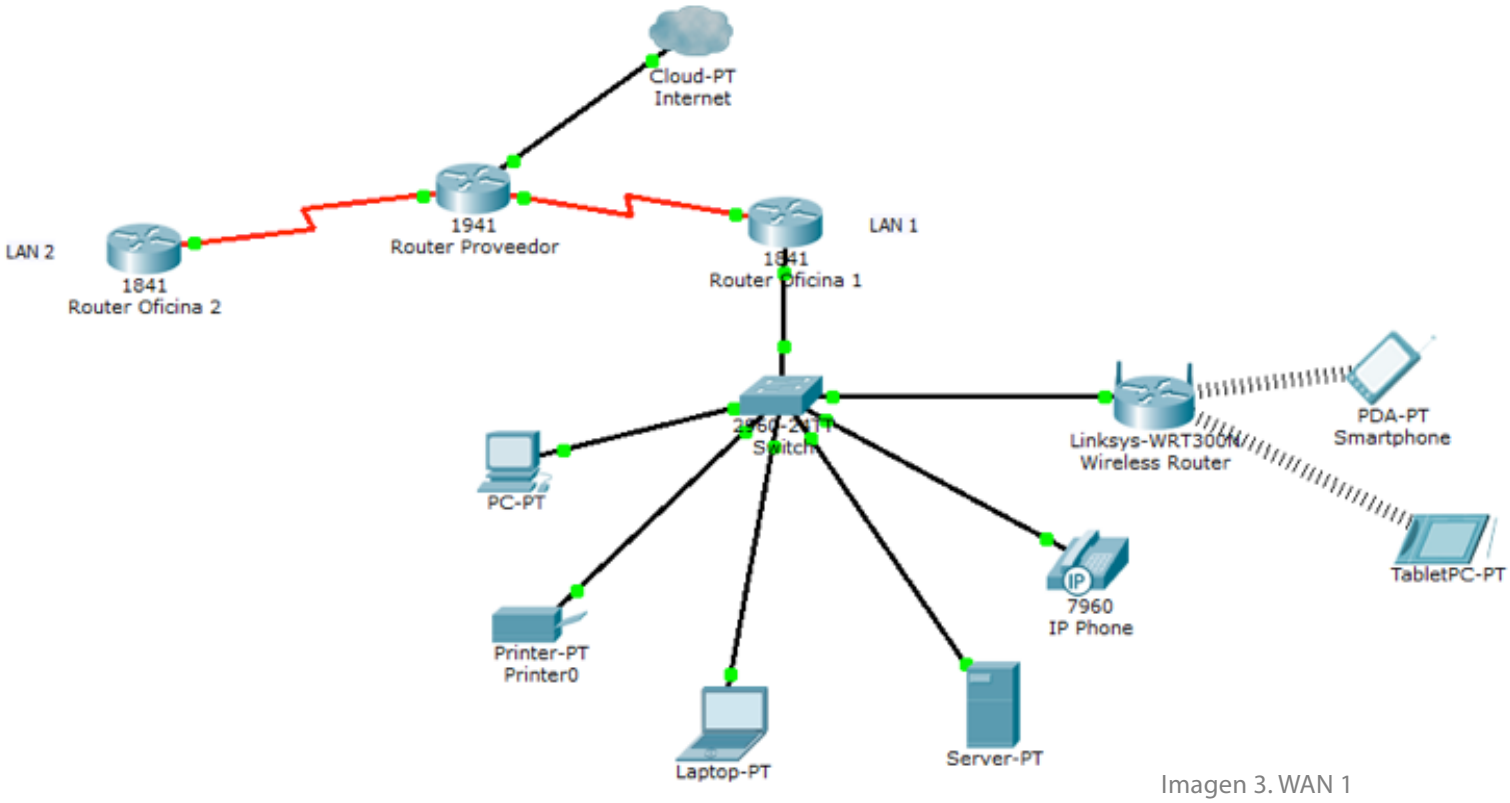


Imagen 3. WAN 1
Fuente: Propia.

Un proveedor tiene la necesidad de conectarse a otros proveedores y por medio de fibras submarinas que le permite conectarse a los grandes nodos de internet (Actualmente, los mayores nodos de interconexión del mundo se ubican en tan sólo cuatro países: Estados Unidos (Nueva York y Virginia), Alemania (Frankfurt), Holanda (Amsterdam) y Reino Unido (Londres). Este tipo de red se llama WAN (*Wide Area Network* – Red de Área Amplia) y se ejemplifica en la siguiente imagen:

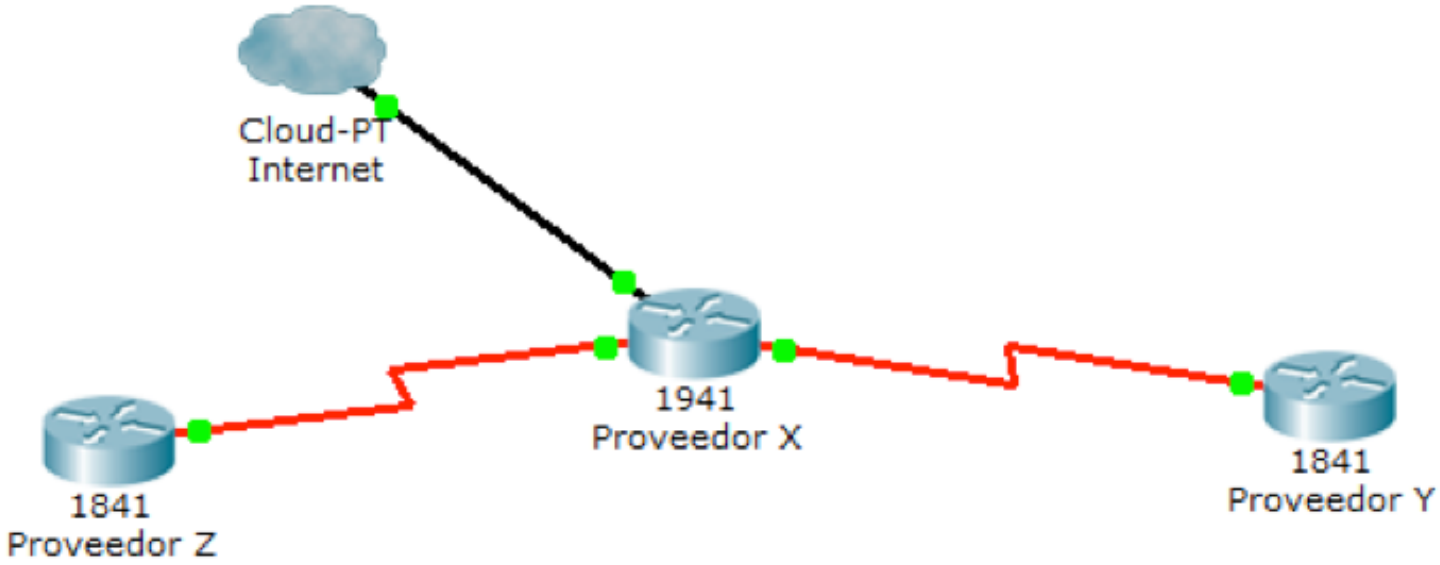


Imagen 4. WAN 2
Fuente: Propia.

Teniendo estos conceptos claros, si se quiere hablar de Seguridad Global, encontramos que es la necesidad de **proteger la red**, de manera que se pueda realizar una comunicación eficiente, rápida y segura (Confidencial, Integral, disponible). Para la transmisión y recepción de datos.

Pero para garantizar que esta comunicación sea eficiente tanto los clientes como los operadores de telecomunicaciones deben manejar políticas de seguridad y por supuesto estas políticas deben ser compatibles unas con otras para que la comunicación sea efectiva. De cumplirse todo esto, se puede decir que sí existe una Seguridad Global.

Impacto en la organización

La seguridad en redes está muy ligada a la continuidad del negocio, como se vio en la introducción de esta unidad, un ataque (ya sea virus, gusanos de internet, hackers, etc.) puede afectar enormemente el "core" del negocio, ya que perder datos o que se pierda la privacidad y la integridad de la información, pueda resultar en pérdidas económicas en una compañía, problemas legales y/o robo de propiedad intelectual.

Paralelamente a la implementación de políticas de seguridad, está un impacto negativo ya que para acceder a la información se requiere de cierto tipo de permisos o accesos, los cuales no todos los usuarios tienen permisos.

Por ejemplo, un empleado de la empresa XYZ, antes de aplicarse las PSI podía acceder sin problema al servidor de "matrices" y descargar un archivo en Access, copiándolo en su equipo personal e incluso lo podía guardar un una USB o algún dispositivo magnético y llevarlo a otro lugar. Suponiendo que es un empleado honesto, trabajaría desde otro lugar el archivo, sin alterarlo de manera que afecte negativamente a la Empresa XYZ. Pero ahora una vez aplicadas las PSI, este mismo usuario no tiene las credenciales o los permisos para ingresar a este servidor, así que debe hacer una solicitud oficial a su supervisor para que este a su vez solicite al área de seguridad y sistemas, permisos para ingresar a este servidor, justificando el motivo por el cual es requerido el ingreso. Sumado a esto, este usuario, ya no puede llevar con el esta información, ya que una de las políticas de seguridad es la creación de una regla que obliga desactivar todos los puertos USB y las unidades de DVD de los computadores.

Este tipo de cambios afectan negativamente la productividad de la empresa y a sus empleados, pero está garantizando que la información por ningún motivo corra riesgos y se pierda o sea leída por agentes externos que podrían utilizarla para su conveniencia.

Amenazas de seguridad moderna

Actualmente son muchos los factores que tienden ser una amenaza para nuestras redes, pero ¿qué es lo que se protege?

- Hardware: parte física, equipos de cómputo, servidores, equipos de red, Racks de comunicación, cableado.
- Software: la parte lógica, datos (información), códigos fuente, programas, sistemas operativos.

¿De quién o qué los debemos proteger?

A nivel físico, se deben proteger los equipos, de robos, de tenerlos en lugares adecuados para su correcto funcionamiento (los equipos de red deben estar en un cuarto de cableado dentro de un Rack de comunicaciones, con aire acondicionado. Este cuarto debe estar asegurado para que no sea de libre acceso). El hardware también debe tener mecanismos que los protejan o traten de protegerlos, frete a catástrofes naturales, como lo son terremotos, inundaciones, incendios, etc.

Pero también hay un factor importante y es el factor humano, nosotros somos los únicos capaces de programar, crear, destruir o violar la seguridad en una red. A continuación se muestra la forma como una red puede ser atacada por personas:

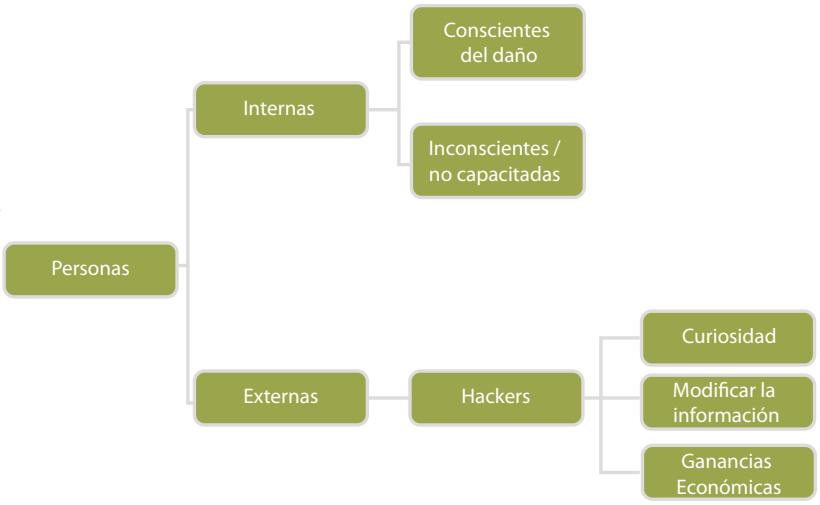


Imagen 5. Ataque físico
Fuente: Propia.

El anterior mapa conceptual, nos muestra que hay dos tipos de personas que pueden acceder a la red. Las primeras son personas que se pueden considerar como usuarios frecuentes o empleados de una empresa, de los cuales, algunos pueden ingresar a datos privados sin ser conscientes del riesgo que esto abarca pero también existe el personal interno que busca ingresar sin autorización a lugares restringidos, con el fin de obtener para su beneficio información, cambiar datos o incluso buscar la manera de obtener ganancias económicas.

Es por esto, que este tipo de posibilidades deben ser contempladas y deben ser auditadas cuando se está creando las normas de seguridad, con el fin de prevenir que este tipo de eventos sucedan dentro de la compañía. No se puede suponer un entorno de confianza donde no siempre existe. Los empleados internos son los que mejor pueden conocer los sistemas y sus debilidades.

El segundo tipo de personas que pueden intentar ingresar a la red, son de tipo externas, las cuales la gran mayoría no tienen otro fin que alterar o dañar la información. Están los curiosos, que a veces sólo por diversión buscan romper con la seguridad de una red y acceder a la información de una empresa.

Están las personas que buscan modificar la información simplemente para causar algún tipo de daño. Un ejemplo de este tipo de sucesos fue el ocurrido cuando la famosa página Megaupload fue cerrada por el FBI. En represalia el grupo conocido como Anonymous hackeó las páginas del departamento de Justicia de los Estados Unidos y la web de Universal Music, dejándolas sin funcionamiento por un breve periodo de tiempo.

Finalmente, el tercer grupo de intrusos, que buscan obtener beneficios económicos, esto se puede ver más frecuente en entidades bancarias, las cuales son muy atacadas con el fin de obtener números de cuentas bancarias o números de tarjetas de crédito.

A nivel lógico, podemos encontrar varios actores que pueden afectar nuestras redes:

- Virus: Ee un software malicioso que se inserta en un fichero ejecutable con el fin de generar una función indeseada en un equipo de la red o más específico en computadores o servidores.
- Gusanos (worm): es un programa capaz de ejecutar por sí mismo un código arbitrario y expandirse dentro de la red infectando los host que encuentre a su paso. En ocasiones incluso puede incluir virus que pueden dañar los equipos infectados.
- Troyano: es una aplicación que se esconde dentro de un programa, que al ser ejecutado realiza funciones ocultas que atacan a la computadora desde adentro, sin que el usuario de cuenta de lo que está sucediendo.
- Bugs de programación: son errores frecuentes que se presenta cuando los programadores de algún software de manera involuntaria, dejan algún error que el acceso a la memoria de un fichero.
- Canales abiertos: son puertos de comunicación lógicos, que al quedar habilitados o abiertos y al no ser custodiados o vigilados, permiten la transferencia de información violando la seguridad de la red.
- Negación de acceso: envían un número extremadamente grande de solicitudes en una red esto ocasiona que la calidad de funcionamiento del dispositivo que está siendo bombardeado con estas so-

licitudes sea inferior. Esto ocasiona que el dispositivo atacado no esté disponible para acceso colapsando aplicaciones y procesos.

Principios fundamentales de las redes seguras

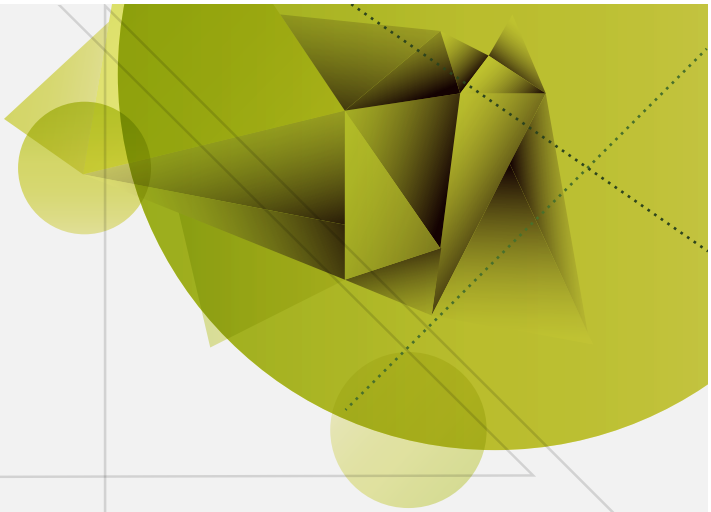
Para poder hablar de redes seguras hay aspectos básicos que se deben tener en cuenta:

- Manejo de password y usuarios de Red: por lo general el usuario de red es único y no se puede cambiar, pero el password sí se aconseja ser cambiado constantemente, hay empresas que suelen obligar a cambiarlo cada 45 días, por ejemplo. Estas claves de acceso son personales y no se deben estar publicando, tampoco se deben dejar anotadas en algún lugar donde cualquier persona las pueda ver y acceder.
- Se recomienda que en el momento de crear un password, no se utilicen fechas, nombres o datos que estén relacionadas con los usuarios. La clave debe contener mayúsculas y minúsculas, mezclando números y/o caracteres especiales (#$*+ @!;.,) y deben ser por lo menos de 8 caracteres de largo.
- Se debe restringir el acceso de red a servicios críticos, como se vio en el tema de "amenazas de seguridad moderna" hay canales abiertos, que no se conocen que están habilitados, por esa razón es importante realizar un estudio exhaustivo buscando estos puertos lógicos TCP/IP que están habilitados y que no se están utilizando y cerrarlos.
- Para los equipos de cómputo, se recomienda que se deshabilite las funciones de Telnet y Ping y deshabilitar también el panel de control, ya que desde ahí hay muchas funciones que se pueden habilitar y esto puede ser un riesgo informático.
- Se debe disminuir los privilegios de acceso a los usuarios a los servidores y por supuesto a toda la plataforma de red.
- Se debe realizar constante actualización de los antivirus y del software del sistema operativo, ya que por lo general estas actualizaciones tienen nueva protección contra recientes peligros como virus, troyanos, etc.
- Como administradores de infraestructura o de redes nuestra obligación es estar un paso delante de los hackers, debemos estar en una constante actualización de todos los temas relacionados con la seguridad, debemos realizar certificaciones de seguridad, seminarios, postgrados, buscar en la red sitios que den tips sobre seguridad, etc.

1

Unidad 1

Políticas de seguridad



Seguridad en redes

Autor: Esteban Bejarano Forero

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

En esta unidad, se conocerá qué es una política de seguridad, para qué sirven dentro de la seguridad en redes, los elementos que la componen, los aspectos más importantes a tener en cuenta a la hora de crear una PSI. Se analizarán los riesgos que hay que tener en cuenta al crear las PSI, dando algunas recomendaciones básicas que se deben siempre tener en cuenta como medidas preventivas para la seguridad de la información ante distintos ataques a los que se expone. Estos principios básicos que se expondrán, con el fin de preparar temáticamente al estudiante, frente a una posible necesidad de crear este tipo de políticas dentro del ambiente laboral donde se desenvuelva.

U1 Metodología

Es importante entender las diferencias que se presentan en cada temática que se desarrolla dentro del documento. Cree mapas conceptuales dividiendo cada tema dependiendo la organización y las prioridades que se presenten.

U1

Desarrollo temático

Políticas de seguridad

Las Políticas de Seguridad Informática (PSI), son documentos creados dentro de una organización, con el propósito de ser aplicado dentro de ella, difundiendo los principios de seguridad por los cuales la compañía se debe regir para que su información permanezca a salvo, explicando el por qué y el para qué de esta necesidad (estableciendo qué se entiende como bienes de la empresa y cómo serán protegidos).

Con las PSI se trazan las "normas" para el correcto manejo de contraseñas, permisos y(o formas correctas de navegación en la web y en la red corporativa, el manejo de envío y recibo de correos, entre otros. Determina la manera como se deben cumplir estas reglas con el fin de mantener a los datos de la empresa a salvo, ya sea de malos manejos internos, como también de posibles ataques externos. Se describe los deberes y derechos de cada usuario y se determina el nivel de jerarquía para el manejo de la información.

Está claro que al implementar una PSI se verán afectados los usuarios y algunos procedimientos que se manejaban en la empresa (de esto se habló en la unidad pasada), pero se debe buscar que a la hora de crearse e implementarse, la actividad de los usuarios no quede limitada a cero ya que esto por obvias razones no le conviene a la empresa. Es por ello que las PSI deben ser efectivas de tal manera que tanto los usuarios como los administradores de la red puedan aceptarlas y las puedan aplicar. Para esto es muy importante que estas políticas sean creadas con el personal indicado, como es el personal de seguridad física y lógica, los directivos de cada área organizacional de la empresa y un grupo de auditores con conocimiento en redes, los cuales puedan validar los controles que se están saltando y cuales se deben implementar.

Elementos de una Política de Seguridad Informática

Para lograr que se realice el proyecto de seguridad informática se deben tener en cuenta los siguientes elementos en las PSI:

a. Autorización: son permisos, los cuales determinan quién y cómo pueden utilizar los recursos de la empresa.

b. Mínimo privilegio: un elemento importante es la restricción de los accesos y autorizaciones del personal, con el fin de sólo poder acceder a los recursos que se requiere para hacer su trabajo y no tener autorización de ingreso a otras redes o recursos que no tienen que ver con su área de trabajo.

c. Responsabilidad individual: las políticas de seguridad, deben aclarar que todos los

usuarios de la empresa son responsables de sus actos y del manejo que le hagan a la información. Este elemento implica que todo el personal y sobre todo los que tienen autorización (de manipulación de la información) deben estar conscientes de sus actividades y deben conocer que cada movimiento que realicen dentro de la red será registrado, guardado y monitoreado.

d. Separación de obligaciones: las funciones deben estar divididas entre las diferentes personas relacionadas a la misma actividad o función, con el fin de que ninguna persona cometa un fraude o ataque sin ser detectado. La separación de obligaciones funciona mejor cuando cada una de las personas involucradas tiene diferentes actividades y puntos de vista.

e. Auditoría: se requiere realizar el monitoreo de cada actividad de los usuarios con privilegios durante su inicio y hasta después de ser terminadas sus actividades. Con este elemento se garantiza que al hacer una revisión de los registros, donde estarán guardadas todas las actividades las cuales ayudarán a realizar una reconstrucción de las acciones de cada usuario.

f. Redundancia: el elemento de redundancia afecta al trabajo y a la información. Se debe impedir que muchas copias de una misma información sean almacenadas en diferentes lugares.

Parámetros para establecer Políticas de Seguridad

Los parámetros más importantes a tener en cuenta a la hora de crear y poner en marcha las Políticas de Seguridad, son:

- Es importante documentarse con cada líder de las áreas de la compañía, la forma cómo funciona cada área en específico, ya que es necesario entender el procedimiento que se realiza, con el fin de detectar factores en los que las PSI harían la cobertura requerida, pero también donde la implementación de estas podrían afectar la productividad de una o varias áreas de la compañía.
- Este tipo de actividades es necesario también sea acompañado por Auditores especializados, los cuales brindarán asesoría y verificarán qué tipo de fallas se están presentando. De esta manera esta cooperación facilitará la implementación de las PSI.
- La comunicación interna es la base fundamental para un buen resultado en la implementación de las PSI, por esta razón es de carácter obligatorio que todo empleado y/o usuario sea informado de los cambios que se realizaran debido a la institución de estas nuevas "normas de juego". Es importante brindar capacitaciones donde se les enseñe a los usuarios los principios **básicos de seguridad.**
- Es un requisito indispensable identificar el personal que tendrá derecho a acceder a los datos y también delimitar hasta qué punto pueden manipular la información, ya que a pesar de tener "derechos de ingreso" no todos tendrán derecho de modificación o escritura. Es importante definir con cada responsable los alcances y los compromisos en cuanto al buen manejo de la información, ya que legalmente también sería posible tomar medidas para castigar a los responsables por perdida, daño o robo de la información.
- Se debe realizar procesos de monitoreo de movimientos y el comportamiento de los usuarios en cuanto a los nuevos

cambios realizados debido a la implementación de PSI, con el fin de identificar falencias y al mismo tiempo realizar las correcciones necesarias.

Riesgos

Un ambiente informático está conformado por recursos de infraestructura, recursos humanos y recursos adicionales:

Recursos de Infraestructura:

- Información: son los datos y uno de los valores más importantes de cualquier entidad.
- Software: son los programas, los sistemas operativos, códigos fuente, con los cuales se pueden acceder, modificar y/o borrar la información.
- Hardware, los equipos de cómputo, servidores, equipos de red, impresoras, los cuales son un puente entre la el personal y la interfaz virtual.

Recursos humanos:

- Personas: son los administradores de red, los usuarios, gerentes, etc.

Recursos adicionales:

- Accesorios: muebles, sillas, papelería en general, etc.

Ya identificados estos recursos, los cuales pueden estar expuestos a varios tipos de riesgos, no sólo los ataques a la información por parte de hackers informáticos ya que como se pudo ver, también hay posibilidades de riesgos físicos. En conclusión, se puede determinar que los riesgos más comunes son:

- Ataques informáticos: ya anteriormente se ha hablado de estos ataques, pero es importante resaltar que este tipo de ataque es por lo general de riesgo lógico, ya que es la forma como el atacante intenta ingresar mediante los "huecos de seguridad" en la red y atacar la información.
- Infección por virus, troyanos, gusanos, etc.: este tipo de ataques pueden poner en riesgo no solo la información de una compañía, también pueden dañar equipos de cómputo o partes de estos equipos.
- Error del software: no es un suceso muy común, pero puede presentarse errores en los aplicativos, los cuales pueden producir que se pierda la información guardada.
- Borrado accidental: la eliminación de una partición o unidad lógica, eliminación de datos almacenados en los servidores o en los propios equipos de cómputo de forma accidental.
- Error de hardware: los dispositivos de almacenamiento como lo son los discos duros, USB están formados por componentes electrónicos y mecánicos, los cuales no están exentos de fallar y al hacerlo, la información guardada allí se verá afectada de manera total o parcial.
- Desastre natural: no nos olvidemos de la posibilidad de pérdida física del medio de almacenamiento que contiene los datos, ya sea por un siniestro que ocasione daños materiales por una pérdida accidental.
- Robo de equipo: el acceso no controlado a los equipos puede ocasionar robo parcial o total del equipo, lo cual también significa pérdida total de la información.

Se han dejado estos últimos tres apartados (error en hardware, desastre natural y robo de equipo) con un propósito especial, ya que en un curso de seguridad de redes es claro que se tienen que abarcar los ataques lógicos y validar las vulnerabilidades en la red, pero casi nunca se le da importancia a los posibles riesgos físicos, de los cuales absolutamente nadie ni nada está a salvo de no sufrirlo.

Muchas empresas se dedican a mantener sus redes de datos seguras, frente ataques o intrusos en la red, pero todavía hay muchas falencias en la prevención de ataques físicos ya sea en los cuartos donde están los equipos de red y servidores o en las oficinas donde se encuentra la mayoría de los usuarios y por donde constantemente se está moviendo mucha información.

Esto es un riesgo alto que se debe tener en cuenta a la hora de implementar políticas de seguridad informática, ya que el o los atacantes pueden optar por desistir la búsqueda de vulnerabilidades lógicas y enfocarse en las físicas, debido a que le resulta más sencillo robar un dispositivo de almacenamiento, una laptop, o cualquier dispositivo que contenga información en lugar de hacer el intento por medio de software. Es por esta razón que la seguridad física es muy importante, un ladrón, un fenómeno natural, es igual o más peligroso que un hacker. Así que al no tener en cuenta los factores físicos, los otros esfuerzos para mantener una red segura no servirán de nada.

Está claro que la idea de este módulo no es enseñar cómo construir cuartos seguros para nuestros equipos de redes o cómo crear un sistema de alarma contra incendios, pero si es importante que se tengan presente todos estos aspectos a la hora de realizar PSI, como ya se dijo, el análisis de riesgos debe ser integral, de manera que la información se vea protegida por todos los medios posibles.

Riesgos físicos		
¿Qué está en riesgo?		
Hardware		
Acceso físico	Desastres naturales	Desastres del entorno
■ Robo de discos duros o dispositivos de almacenamiento. ■ Robo de laptops o equipos de red. ■ Copia no autorizada de datos entre equipos.	■ Terremotos ■ Inundaciones ■ Humedad ■ Tormentas eléctricas	■ Descargas eléctricas ■ Incendios ■ Altas temperaturas ■ Ruido eléctrico

Figura 1. Riesgos físicos
Fuente: Propia

Los riesgos físicos tienen que ver directamente con el hardware que utiliza una compañía. Este es el elemento más costoso de cualquier sistema informático, ya que abarca los equipos de cómputo (que por lo general hay un equipo por cada usuario, incluso, hay usuarios que se les asignan dos o más equipos). Los equipos de red, los cuales son costosos y requieren un cuidado especial debido a que deben estar encendidos todo el tiempo y esto generan temperaturas altas donde se encuentran.

Acceso físico

En primera instancia se encuentra el acceso físico al que se puede tener a estos equipos, cualquier persona con malas intenciones y que tenga la posibilidad de acceder a algún sector de una compañía, puede fácilmente robar información, robar dispositivos de almacenamiento o incluso robar equipos enteros o partes de estos.

Si no se tiene control y vigilancia, no servirá de nada tener una red robusta y protegida o que el equipo esté protegido con clave de acceso, el ladrón podrá adueñarse de esta información, extraer el disco duro del equipo, por ejemplo y no necesariamente necesita privilegios en el sistema para realizar este acto delictivo.

Si hay usuarios que no acostumbran dejar bloqueados sus equipos, el ladrón puede colocar un dispositivo de almacenamiento y comenzar a copiar la información que está en este equipo.

Desastres naturales

También se debe tener en cuenta el riesgo de los desastres naturales, obviamente entendiendo que en este factor como seres humanos estamos muy limitados, pero si se puede realizar cierto tipo de prevenciones cuando un evento como este ocurra.

Por ejemplo, para prevenir que los equipos sufran daños graves, lo más recomendable es:

Para los equipos de red, deben dejarse en un lugar apartado y en un rack de comunicaciones, el cual permite no solo protegerlos de caídas, sino también de acceso físico a ellos no autorizado. Para los equipos de cómputo, es aconsejable no dejarlos en el suelo, no tanto por prevención a terremotos, sino por prevención a inundaciones ya que con un simple contacto con el agua, los equipos electrónicos se pueden dañar e incluso ocasionar cortos circuitos.

Los equipos también deben ser protegidos contra tormentas eléctricas, es por ello que es muy importante que las locaciones cuenten con cableado estructurado y que haya polos a tierra, que garanticen que si hay riesgo de rayos, estos no dañen los equipos, ya que están protegidos por el polo a tierra. Otra forma de protección es sencillamente desconectar los equipos cuando se presenten tormentas eléctricas, ya que este fenómeno se podría decir que sí es predecible, de esta manera se estará salvando no solo la información de estos equipos, sino también todo el hardware.

Desastres de entorno

Finalmente están los desastres del entorno, las altas corrientes, los cortos circuitos, los cortes del flujo eléctrico muchas veces pueden ocasionar daños irreparables en el hardware, es por esto que como ya se mencionó, se debe contar con un sistema de toma regulada, las cuales protegen considerablemente los equipos.

Los incendios son casi siempre ligados a problemas eléctricos, ya que hay posibilidades de que después de un corto circuito, se produzca un incendio. Es por esto que se recomienda tener instalado en las oficinas extintores o sistemas de detección de humo, los cuales podrían ayudar a salvar los equipos del fuego y por supuesto al personal.

Aparte del fuego y el calor generado, en un incendio existe un tercer elemento perjudicial para los equipos: el humo, un potente abrasivo que ataca especialmente los discos magnéticos y ópticos.

Es importante tener en cuenta las temperaturas extremas, ya sea un calor excesivo o un frio intenso, perjudican gravemente a todos los equipos. Para controlar la temperatura ambiente en el entorno de operaciones es aconsejable la utilización de aire acondicionado, el cual influirá positivamente en el rendimiento de los usuarios y de las máquinas o equipos que allí se encuentren.

Una vez conocidos y evaluados de cualquier forma los riesgos a los que nos enfrentamos se podrán definir las políticas e implementar las soluciones prácticas para minimizar sus efectos.

Cuando ya se ha realizado este análisis (de una manera más profunda) no falta nada más sino presentar los posibles costos a los responsables de la organización. Nunca se debe olvidar que el gasto de proteger un recurso ante una amenaza debe ser inferior al gasto que se produciría si la amenaza se convirtiera en realidad. Los riesgos se pueden minimizar, pero nunca eliminarlos completamente (pasa a nivel físico y a nivel lógico), por lo que se recomienda que en las PSI no solo se planifique la prevención ante de un problema sino también la manera como se hará la recuperación de llegarse a presentar una amenaza.

Niveles de trabajo

1. **La confidencialidad:** indica que la información solo puede accedida por personal calificado o el personal que fue escogido para esta labor, no todos los usuarios pueden tener permisos para validar los datos de la empresa.
2. **Autorización:** la información es accedida sólo por los usuarios que tienen los privilegios para hacerlo.
3. **Disponibilidad:** toda la información debe estar disponible para los usuarios autorizados en cualquier momento que sea requerido.
4. **Integridad:** la información debe estar completa, son modificaciones de acuerdo a los últimos cambios realizados por agentes autorizados.
5. **Utilidad:** los datos manejados y los recursos utilizados para manipular estos datos cumplen la función por la cual fueron creados.
6. **Autenticidad:** el sistema está en la capacidad de reconocer la identidad de los usuarios que se loguean de manera correcta (con su correspondiente usuario y password).
7. **Posesión:** los administradores de un sistema deben estar en la capacidad de controlarlo siempre, ya que perder el control compromete la información para que sea vista por agentes externos y maliciosos.
8. **Observancia:** la información relacionada con las acciones y actividades de los usuarios se encuentra debidamente monitoreada y registrada.

Algoritmo

Para poder crear el algoritmo de las Políticas de seguridad, se debe tener bien claro ¿qué es lo que se quiere proteger?

Por lo que ya se ha visto, lo que se desea proteger es el hardware, el software y los datos. Cualquiera de estos tres puede estar gravemente amenazado y se pueden presentar muchos ataques sobre ellos (aunque principalmente frente a los datos, los cuales son los más complicados de recuperar).

Siempre se debe hablar de dos grandes entidades que estarán siendo realizando movimiento de la información: La primera es la transmisora (TX) de la recepción, ella produce la información, la otra el receptor (RX) de la información. Y se dice que hay una comunicación normal y segura cuando TX envía la información y RX la recibe sin ningún inconveniente o contratiempo (figura 2).

Figura 2. Comunicación Efectiva
Fuente: Propia.

El siguiente algoritmo, divide los tipos de ataques en 4 grupos:

Un ataque de interrupción se presenta si hace que los datos transmitidos se pierdan, queden inutilizables o no disponibles:

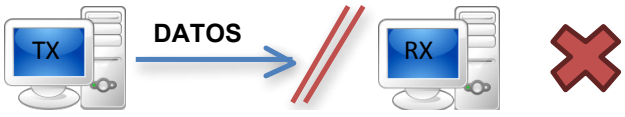


Figura 3. Interrupción
Fuente: Propia.

Un ataque de interceptación se presenta cuando los datos transmitidos son captados por un tercero no autorizado, colocando en riesgo la privacidad de la información:

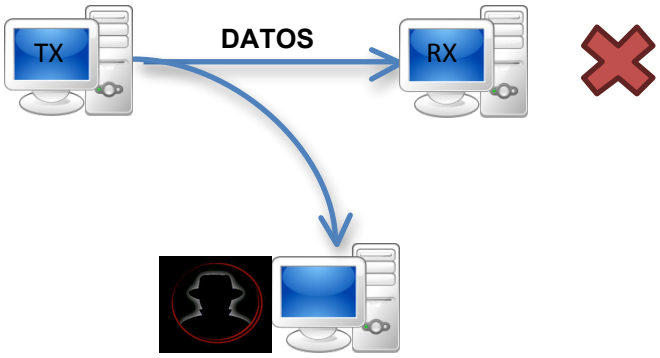


Figura 4. Interceptación
Fuente: Propia.

Un ataque de modificación, se presenta cuando los datos transmitidos además de ser interceptados, también son cambiados, modificados o incluso destruidos, por un tercero no autorizado:

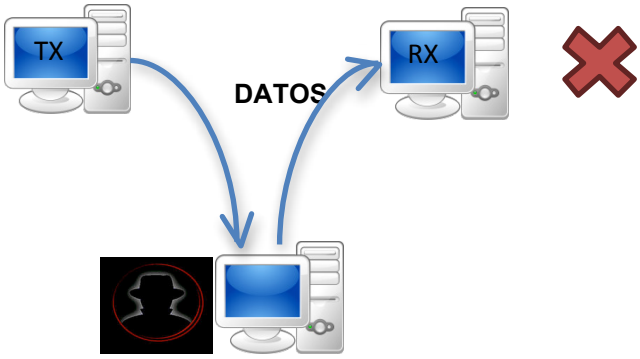


Figura 5. Modificación
Fuente: Propia.

Un ataque de modificación, se presenta cuando los datos transmitidos además de ser interceptados, también son cambiados, modificados o incluso destruidos, por un tercero no autorizado:

Finalmente se presenta el ataque de fabricación, de manera que sea difícil determinar que los datos generados son realmente de un tercero no autorizado o de una fuente confiable.

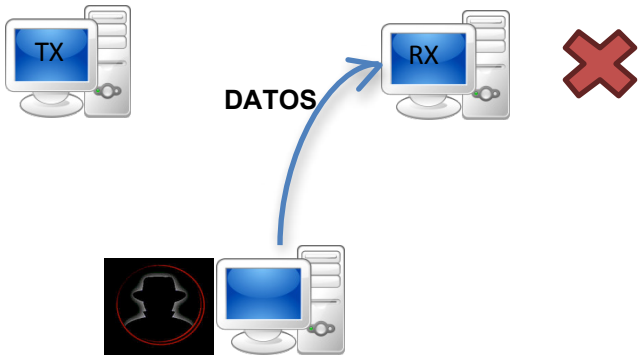
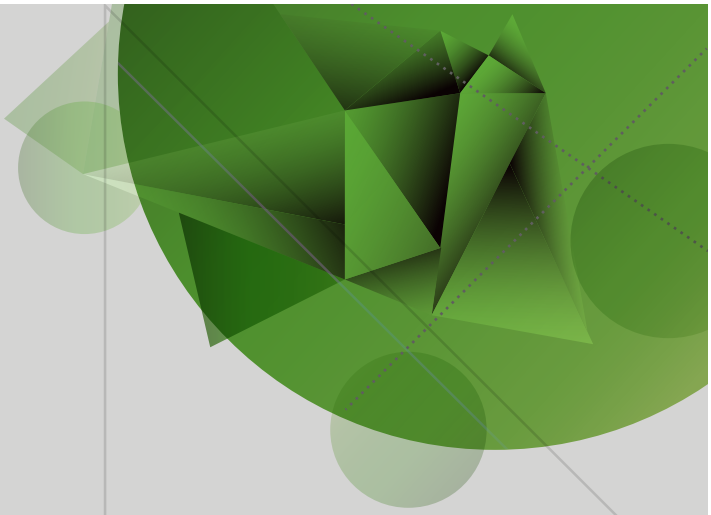


Figura 6. Fabricación
Fuente: Propia.

2

Unidad 2

Metodologías de ataque



Seguridad en redes

Autor: Esteban Bejarano Forero

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

En esta unidad se analizará diferentes formas como una red podría ser atacada, de esta manera se puede determinar los planes de acción para proteger una red, e incluso dejar de utilizar algunas de los protocolos que se expondrán en este capítulo.

U2 Metodología

Se recomienda realizar una lectura dedicada de cada uno de las metodologías que se presentarán en el capítulo. Adicional es importante que el estudiante investigue por su cuenta medios de defensa o la manera como se puede proteger la red, frente a la vulnerabilidad que existe en los protocolos que se expondrán.

Se recomienda seguir la actividad de repaso "usando WireShark" con el que se podrá identificar algunos de los riesgos que se presenta en la red.

U2

Desarrollo temático

Metodologías de ataque

En la actualidad hay muchas modalidades de ataque a nuestras redes, es por ello que es importante estar preparados y protegidos contra la mayor cantidad de estos. Es imposible decir que estaremos a "salvo" de ataques todo el tiempo, ya que siempre existirán vulnerabilidades en nuestras redes que permitirán a agentes externos atacar y como ya se vio en la unidad pasada el riesgo es que la información se vea afectada, siendo observada, modificada e incluso borrada.

Por esta razón es importante conocer algunas de las metodologías de ataque, con el fin de evaluar las posibles fallas de seguridad en la red.

Denial of Service (DoS) Negación de servicio

Este ataque consiste en que el atacante tiene la posibilidad de generar muchas solicitudes a un mismo recurso o servicio con el fin que los usuarios que pertenecen a la red y tienen los derechos a acceder a este recurso no lo puedan lograr. Esto es claro, si se entiende que por medio de otras políticas de seguridad y también por la capacidad que puedan tener los recursos, solo es posible aceptar un número limitado de solicitudes. El atacante al hacer tantas solicitudes, está saturando la capacidad del recurso y esto hace que cuando algún funcionario o persona autorizada quiera ingresar, no lo pueda hacer.

Existen distintas maneras de atacar una red con DoS, unas de ellas son:

- Consumo de los recursos de la red: Los equipos conectados a la red, requieren de la capacidad de la red para poderse comunicar con otros y con los recursos, pero si esta red se utiliza inapropiadamente y los recursos se ven afectados por la saturación en la red (hay que recordar que el ancho de banda es un recurso finito o limitado), esto deja sin poder operar a los equipos que necesitan legítimamente los recursos que hay en la red.

  Los hackers pueden recurrir a varias formas para causar esta negación, pueden generar saturación con pings extendidos de gran tamaño, o pueden generar reacciones de eco entre equipos, los cuales producen que rápidamente las redes se saturen y por ende colapse o incluso logran que la red se caiga de manera frecuente sin aparente explicación. De esta forma ninguno de los usuarios podrá acceder a los recursos.

  Un ejemplo más claro de esto, se puede ver con páginas de internet, que en ciertas ocasiones pueden llegar a ser visitadas por muchas personas, esto hace que la página se congestione y los que quieran intentar ingresar no puedan, o sea se les niega el acceso a la información o al servicio.
- Algunas veces los ataques de DoS pueden ocasionar que la capacidad de

almacenamiento de los equipos se llene, de manera que ya no se puede almacenar más información. Por supuesto siempre existirán usuarios que no son expertos en el tema informático, por tal motivo puede que ni se den cuenta que su disco está lleno y por ello no pueden trabajar bien. El hacker puede crear scrips o procesos repetitivos que no afectan realmente la capacidad de los discos duros de los equipos, pero si hacen que el las CPU generen una gran cantidad de proceso que no se requiere. O incluso por medio de FTP anónimo puede almacenar basura dentro de los equipos, llenando los discos duros.

Las graves consecuencias de estos ataques se centran en que no se puede acceder a la información, esto quiere decir que no sirve de nada tener un servicio al cual no se puede acceder de manera rápida o en el momento en el que se desea. Esto por supuesto genera malestar en los usuarios, pérdida de tiempo y por supuesto pérdida de dinero. Es por ello que se debe tener en cuenta algunas medidas de prevención frente a estas anomalías en la red:

- Deshabilitar la mayor cantidad posible de puertos que no se estén utilizando, ya que esta es una de las primeras ventanas que utilizan los hackers para ingresar a la red.
- Desde los router o incluso desde los switch se pueden crear acces list, en los cuales se almacenarán las MAC que tienen permisos de navegación en la red, los demás serán rechazados por ser desconocidos.
- Verifique de vez en cuando el comportamiento de la red, identifique si es normal que en horas del día se presenten grandes movimientos de datos. Es importante llevar una "bitácora" donde quede registrado el uso diario de BW y se compare con otros días. Existen software especializado que por medio de protocolos SNMP pueden monitorear el uso del ancho de banda de cada red y de cada equipo perteneciente a ella y pueden validad qué capacidad de ancho de banda se está utilizando.
- De ser posible se recomienda tener una contingencia con el fin de poder migrar lo servicios más críticos y de esa manera no se vea afectada la operación.

Craking de passwords

Esta modalidad de ataque busca tratar de comparar las contraseñas de los usuarios (los que están autorizados y los cuales están encriptadas) con passwords que puedan llegar a ser parecidos y a la vez se encriptan para tratar de hallar una similitud con el original. Este tipo de ataque se llama ataque de diccionario y su efectividad depende de factores como:

La cantidad de passwords almacenados en el diccionario.

El tipo de password que se quiera averiguar, ya que no es lo mismo intentar averiguar la clave de Outlook.com que la clave de ingreso a la base de datos de una entidad gubernamental.

Otra forma de atacar un password es por medio de los intentos por "suerte" el cual se basa en el intento de adivinar cuál es la clave, haciendo múltiples intentos.

Estos ataques son unos de los más comunes por complejos que suenen, ya que existen algoritmos muy potentes que pueden almacenar millones de contraseñas, las cuales tarde o temprano pueden llegar a coincidir con la real. Es por ello que se aconseja cambiar continuamente las claves de acceso y no manejar una clave genérica, ya que si averiguan una para un sistema, automáticamente tienen ingreso a las demás.

Como ya se ha mencionado en la unidad pasada, es importante manejar un esquema de creación de contraseñas, que obligue a tener contraseñas que no sean comunes, donde no estén relacionadas con datos personales o de fácil adquisición, que sean mínimo de 8 caracteres y preferiblemente sean cambiados cada cierto periodo de tiempo. Esto complica en gran manera el intento por el craking de passwords.

La siguiente tabla dejará mejor explicado la importancia de una contraseña más robusta: Se supone una velocidad de búsqueda entre 100.000 y 200.000 passwords por segundo.

number of Characters	Numbers only	Upper or lower case letters	upper or lower case letters mixed	numbers, upper and lower case letters	numbers, upper and lower case letters, symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 secs	10 secs
6	Instantly	Instantly	8 secs	3 mins	13 mins
7	Instantly	Instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1qt years

Key:

k – Thousand (1,000 or 10^{-3})
m – Million (1,000,000 or 10^{-6})
bn – Billion (1,000,000,000 or 10^{-9})
tn – Trillion (1,000,000,000,000 or 10^{-12})
qd – Quadrillion (1,000,000,000,000,000 or 10^{-15})
qt – Quintillion (1,000,000,000,000,000,000 or 10^{-18})

Figura 1. Complejidad de Passwords
Fuente: https://www.inetsolution.com/turnleft/post/Complex-Passwords-Harder-to-Crack-but-It-May-Not-Matter.aspx

Con esto se puede concluir que entre más caracteres y símbolos se utilicen, es menor la probabilidad de que sea violado un password.

Problemas de seguridad en el FTP

Para entender los problemas que este protocolo presenta, primero se debe validar qué se puede realizar con FTP. Básicamente FTP es un protocolo estándar en la red, el cual permite u ofrece servicios de transferencia de archivos de un host a otro sobre TCP. Con este protocolo, se puede obtener no solo archivos, sino también el nombre, el tamaño del archivo, por medio de cualquier red basada en TCP/IP. He ahí donde se comienzan a presentar las vulnerabilidades del FTP, porque este no presenta la posibilidad de encriptar los archivos que se pueden descargar entre host o entre servidores. Claros casos de ataques por medio de este protocolo, son los siguientes:

- **Ataque de fuerza bruta:** es uno de los medios más comunes, el cual se basa en que el atacante intenta adivinar el password y el usuario, realizando la implementación de algoritmos que generan miles de combinaciones por minuto. Esto implica que si un password es débil, corre el riesgo de ser descubierto fácilmente.
- **FTP Bounce Back:** cuando se utiliza transferencia de archivos por FTP, el host o servidor FTP de origen genera la petición al servidor FTP de destino, el hacker puede tomar ventaja de esta petición, con un comando llamado PORT, el cual solicita acceso a los puertos y finalmente hacerse parecer a un intermediario en la transferencia de la información. De esta manera tiene la posibilidad de realizar el escaneo de los puertos de cualquiera de los host y así tener acceso a la información transmitida.
- **Negación de servicio:** un hacker puede montar un ataque de negación de servicio, con el servidor FTP para inhabilitar perfiles de usuario en el sistema. Esto lo logra, realizando repetidos intentos de inicio de sesión con contraseñas incorrectas en un perfil de usuario y debido a que en muchas ocasiones hay restricciones de seguridad, después de determinados intentos se realiza la inhabilitación del usuario. De esta manera, cuando el usuario afectado quiera ingresar con la contraseña correcta, no lo podrá hacer, porque su cuenta se encontrará bloqueada.

Captura de paquetes: como ya se mencionó, la transferencia de archivos se realiza sin cifrado, la información más vulnerable o sensible (usuarios y passwords) pueden ser leídos fácilmente por medio de técnicas de captura de paquetes, uno de los más comunes es el conocido Wireshark[1], el cual permite capturar los paquetes transmitidos, decodificarlos y así poder tener acceso a ellos.

Figura 2. Logo de WireShark
Fuente: Propia.

[1] Para más información sobre| cómo utilizar wireshark, visitar su página oficial: https://www.wireshark.org/

TFTP

TFTP (Trivial File Transport Protocol o en español protocolo de transferencia de archivos trivial) Es un mecanismo sencillo de transferencia de archivos no orientado a conexión (UDP) semejante a FTP, este protocolo no admite ningún mecanismo de autenticación ni cifrado, por lo que su presencia puede suponer un riesgo de seguridad. No se recomienda instalar el cliente de TFTP en los sistemas con acceso a Internet, a no ser que sea estrictamente necesario, ya que un intruso puede correr un ataque de diccionario, con una gran posibilidad de averiguar claves y usuarios y de esa manera conocer los datos que se transmitieron.

Este protocolo se recomienda sólo utilizar en redes que no tengan salida a la red, esto garantiza completa integridad de la información.

Telnet

Es un protocolo (TCP, puerto 23), basado en texto que permite a una máquina comportarse como un terminal virtual y conectarse remotamente a otro equipo a través de Internet. Este tipo de conexión sólo se puede realizar si el administrador del equipo remoto da los permisos de conectividad, entregando claves y el /los usuario(s) con el que se puede realizar el acceso.

Claramente se puede ver que el hecho de poder ingresar a algún equipo a través de Internet ya implica un riesgo de ataque enorme, debido a las diversas formas como un atacante puede intentar ingresar. Por medio de Telnet también se puede ingresar a bases de datos, correos electrónicos, etc., esto aumenta el riesgo.

Adicional, como pasa con FTP o TFTP, Telnet no utiliza ningún tipo de cifrado, lo que indica que todo el tráfico que se mueve entre equipos, se realiza con texto claro. O sea que con un sniffer es muy fácil para el atacante averiguar el password y el usuario de sesión. Por esta razón no se recomienda utilizar una sesión de Telnet entre sedes remotas, se recomienda utilizar aplicaciones equivalentes, pero con posibilidad de cifrado para la transmisión de datos (SSH por ejemplo).

Adicional, otra forma como un hacker puede atacar una red o equipo por medio de Telnet, es por medio de ataques por fuerza bruta, los cuales como ya se mencionaron anteriormente, consta en que el atacante genera un algoritmo que permite crear combinaciones tanto de usuarios como de passwords, con el fin de hallar el correcto y así poder ingresar a la red o al equipo remoto.

Comandos "r"

Estos comandos se presentan exclusivamente dentro del sistema operativo de UNIX, donde la r, significa remote, por lo tanto con ellos se puede realizar el ingreso remoto entre máquinas, con el fin de hacer el ingreso a terminales remotos y transferencia de ficheros. Las herramientas cliente utilizadas en este lenguaje son rsh, rlogin y rcp y para los servidores remotos rexecd, rshd o rlogind.

Por ejemplo rlogin (TCP, puerto 513), quien es muy parecido al telnet, se utiliza como terminal virtual en un sistema Unix, rsh (TCP, puerto 514) es utilizado para ejecutar comandos en una máquina remota sin necesidad de ingresar a ella y rcp, permite copiar ficheros entre diferentes máquinas:

Estos servicios buscan quitar la molestia a los usuarios de tener que utilizar claves de ingreso, esto se logra aplicando un esquema de fiabilidad, ya sea por parte del usuario o el equipo o ambos. Esto significa que cualquier usuario puede hacer el uso o el ingreso a cualquier máquina remota sin necesidad de que se le exija una clave, si y sólo si, este intenta ingresar desde un equipo confiable y un usuario confiable (que sea conocido dentro de la base de datos).

Como se puede ver, las relaciones de confianza entre equipos Unix pueden ser muy útiles y cómodas para los usuarios, pero al mismo tiempo muy peligrosas: ya que se está confiando plenamente en sistemas remotos, por lo que si su seguridad se ve comprometida también se ve la de los usuarios y su información. Es por ello que se requiere que las máquinas fiables sean equipos de la misma organización únicamente, y administrados por la misma persona; además, es necesario tener siempre presente que si se tiene habilitados los servicios r-* cualquier usuario puede establecer relaciones de confianza, lo que puede suponer una gran amenaza a la información e integridad de la red.

Una vez adquirido el acceso no autorizado, muchas otras computadoras son accesibles. El hacker accede a los directorios de la máquina atacada, y de ahí puede continuar con su cadena de accesos, obteniendo más información.

Seguridad en NetBIOS

Los protocolos NetBIOS a través de TCP/IP (NBT) no requieren autenticación y como ya se ha visto en apartados anteriores, son vulnerables a la suplantación. Se trata de una característica del diseño. Un usuario malintencionado fácilmente puede utilizar indebidamente la naturaleza del protocolo, que no realiza ninguna autenticación, para enviar un datagrama con un conflicto de nombres a un host o servidor de destino y provocar que renuncie a su nombre y que deje de responder a las consultas, ya que por lo general estos equipos están configurados para responder a sólo un número limitado de peticiones para que su CPU no se vea afectada al atender tantas peticiones.

Al recibir un datagrama con un conflicto de nombres no solicitado, el servidor deja de responder al nombre NetBIOS que presenta el conflicto y puede mostrar un mensaje de error donde se indique que existe un nombre duplicado en la red o que no es posible el acceso a la base de datos en el momento. Esto significa que el hacker realiza un ataque de negación de servicio.

Asimismo, es posible que el equipo afectado experimente alguno de los siguientes síntomas:

Problemas de conectividad intermitente

Puede que el equipo presente problemas intermitentes al comunicarse con otro equipo. Esto se debe a la saturación que genera el datagrama, y como el recurso de red es limitado, al existir saturación se presentará intermitencias o caídas en la red.

Conflicto del servicio de nombres NetBIOS

- Algunas herramientas, como Entorno de red, no funcionan.
- Los equivalentes del comando **net send** no funcionan.
- El servidor afectado no autentica los inicios de sesión del dominio.
- Quizás no pueda obtener acceso a

los recursos compartidos y a los servicios básicos de NetBIOS, como la resolución de nombres NetBIOS.

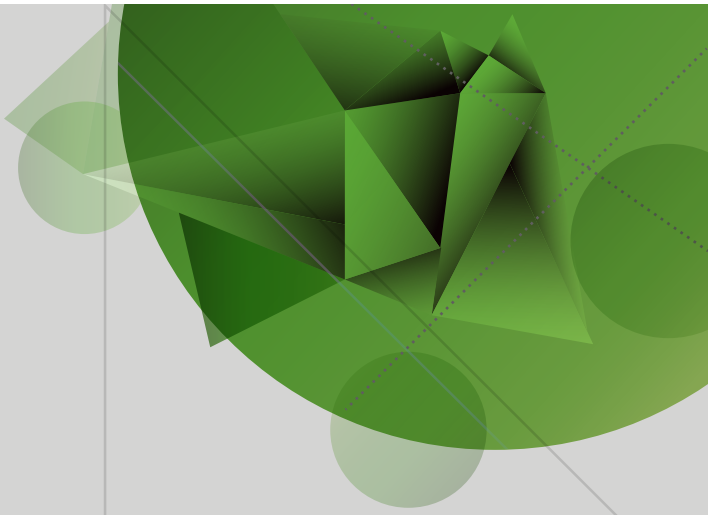
Asimismo, el comando **nbtstat-n** puede mostrar el estado "Conflicto" junto al servicio de nombres NetBIOS.

Esta revisión cambia el comportamiento de Windows para aceptar un datagrama con un conflicto de nombres solamente como respuesta directa al intento de registrar un nombre.

2

Unidad 2

Herramientas de control y seguimiento de accesos



Seguridad en redes

Autor: Esteban Bejarano Forero

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

A diferencia del tema de la semana pasada, en esta se verán algunas de las herramientas que permitirán tener mejor protegida nuestra red. Es válido recordar que estas soluciones, no garantizan una protección al 100% en nuestra red, pero sí permite tener una mejor seguridad en la red, todo esto combinado con una buena administración de un firewall y buenos sistemas antivirus, cierran grandes posibilidades de ser atacados.

U2 Metodología

Muchos de los temas que se verán en esta unidad, requieren no sólo ser leídos con detenimiento, también se recomienda que sean practicados en interfaces UNIX. En internet se puede encontrar muchos tutoriales con los que se puede aprender a manipular muchos de los programas o soluciones que se verán a continuación.

U2

Desarrollo temático

Herramientas de control y seguimiento de accesos

En esta unidad se estudiará herramientas que permiten tener un mayor control en la red, con esto se puede buscar alternativas que contribuyan a la seguridad de la información, y la prevención de ataques no deseados. Estas herramientas permiten analizar los datos transmitidos y recibidos de diversos protocolos, como lo son TCP. UDP, DNS, TELNET, FTP, etc.

Hay que tener mucho cuidado con algunas de las herramientas que se verán en esta unidad, ya que algunas pueden ser utilizadas para usos correctos, pero también pueden ser utilizadas para afectar la red de datos.

TCP – Wrappers

Es una librería que provee un sencillo control de acceso y un logueo para aplicaciones que sean soportadas y que requieran realizar conexiones por internet. Esta herramienta se utiliza en sistemas operativos de Unix, lo cual implica que es un software de dominio público.

TCP – Wrapper es un host basado en ACL (Access Control list, Lista de control de acceso), el cual trabaja conjunto con los sistemas de red, con el fin de filtrar el acceso a la red desde internet. A la vez permite ejecutar determinados comandos para poder realizar acciones específicas de forma automática. TCP Wrappers presenta una importante ventaja sobre un firewall (aunque no se puede pretender que remplace a uno, ya que lo recomendable es que trabaje en conjunto a un firewall o a un sistema avanzado de seguridad), ya que trabaja sobre la capa de aplicación (modelo OSI). Esto permite filtrar peticiones cuando es usada una encriptación. Servicios comunes como FTP, Telnet, POP3, RLOGIN, RSH, REXEC, TFTP, etc., son soportados por TCP Wrappers.

El principio básico de este software se basa en un programa que se instala en el "/etc/inetd.conf". Ya instalado, se puede proceder a realizar cierta configuración o combinación de comandos.

Los ficheros principales implicados en TCP Wrappers son "/etc/host.allow" (Este archivo describe los nombres de los equipos, IP's, redes o servidores que tienen permisos para utilizar los servicios locales) y "/etc/host.deny" (Este archivo describe los nombres de los equipos, IP's, redes o servidores que no tienen permisos para utilizar los servicios locales). Es en estos archivos donde se definirán las reglas que deben utilizarse para el filtrado de los paquetes.

Adicional, existen unos daemons o demonios, los cuales Son servicios que existen en sistemas operativos Unix como por ejemplo sshd (servicio SSH), slapd (servicio LDAP) o proftpd (servicio FTP). Existe también el comodín "ALL" que hace que dicha política afecte a todos los demonios del sistema.

La sintaxis básica de estos ficheros es la siguiente:

Demonio: dirección: acción.

O

Demonio: dirección.

Para entender un poco mejor la forma como estos comandos trabajan, se mostrará a continuación algunos ejemplos.

Permitir acceso ssh únicamente a unas IPs.

/etc/hosts.allow Permitir acceso a las IPs 10.201.100.1; 10.202.10.1; 192.168.10.1 y negar el resto:

Sshd : 10.201.100.1 10.202.10.1 192.168.10.1

Sshd: ALL.

Permitir también el uso de sendmail a una subred y unos hosts concretos.

/etc/hosts.allow Permitir acceso a las IPs 10.201.100.1; 10.202.10.1; 192.168.10.1, sendmail y negar el resto **/etc/hosts.deny**:

Sshd : 10.201.100.1 10.202.10.1 192.168.10.1

Sendmail : 192.168.110.0/24 ejemplo.com.

ALL : ALL

Permitir el acceso a varios servicios dentro de una red LAN vía /etc/hosts.allow y denegar el resto vía /etc/hosts.deny:

Popd : 192.168.10.1

Imapd : 192.168.11.1 255.255.255.0

Sendmail : 192.168.12.1 255.255.255.0

Sshd : 192.168.13.1 255.255.255.0

ALL : ALL.

Como Se puede observar hay muchas posibilidades para otorgar o denegar un servicio, se recomienda al estudiante que practique con otras configuraciones, ya que estos ejemplos son muy básicos y pueden ir aumentando su complejidad dependiendo la necesidad que exista o la lista de protocolos que se requiera aplicar.

Como ya se mencionó anteriormente, TCP-Wrappers es una herramienta muy útil que permite restringir, denegar permisos de acceso o también monitorear la actividad de la red, pero esto no implica que este pueda reemplazar la protección que brinda un Firewall, por tal motivo se recomienda utilizar ambos. El firewall siempre debe ir adelante del TCP-Wrappers y no al revés.

Netlog

Este software es de dominio público y trabaja con servicios basados en IP (TCP y UDP) e ICMP. Esta herramienta permite básicamente crear logs de las actividades o tráfico que se presentan en la red. Este produce archivos que se permiten leer, donde muestra detalladamente datos como fechas y horas, direcciones MAC, indica también si transmitirlo o si recibió. Este tipo de información es realmente importante, ya que como se ha estudiado, hay muchas posibilidades que se realicen ataques a una red que pueden

pasar desapercibidos si se llevan a cabo con extremada velocidad, con intervalos muy cortos de tiempo de conexión, y de manera repetida al mismo elemento de la red, esto como ya se ha visto tiene que ver con ataques de negación de servicio. Esto se logra generando un ataque que se repita 10 veces en un milisegundo, en el registro de conexiones solo aparecería un solo intento de ataque, mientras que en realidad se realizaron 10. Si la vulnerabilidad la hubiera alcanzado en la novena conexión, no habría aparecido en el registro, y aun así se habría violado la seguridad.

Estas vulnerabilidades pueden ser corregidas con Netlog, el cual, está conformado por un conjunto de programas que trabajan de manera conjunta para generar trazas de los paquetes movidos en la red, sobre todo aquellos que pueden ser sospechosos y que indican un posible ataque a una máquina. Los 5 subprogramas que componen este programa principal son los siguientes:

- **TCPLogger:** genera trazas sobre todos los paquetes que usan el protocolo TCP.
- **UDPLogger:** genera trazas sobre los paquetes que usan el protocol UDP.
- **ICMPLogger:** genera igualmente trazas, pero de las conexiones basadas en ICMP.

Estos 3 programas pueden guardar su información en formato ASCII o en formato binario. En el segundo caso, el programa contiene un extractor que permite consultar los archivos generados, e incluso contiene un buscador que permite acceder patrones de búsqueda, como por ejemplo el tráfico de una red en particular, el de una máquina o los intentos de conexión a un puerto definido por el usuario.

- **Etherscan:** esta herramienta monitorea el uso de otros protocolos con actividad inusual, y nos indica qué archivos se han modificado o llevado por el uso de dichos protocolos.
- **Nstat:** es usado principalmente para detectar cambios en los patrones del uso de la red. Este subprograma, a su vez, posee herramientas que nos dan información sobre ciertos periodos de tiempo, o nos dan la posibilidad de graficar determinados datos.

Argus

Es una herramienta que permite hacer análisis de incidentes con el tráfico IP que se pueda encontrar en la red analizada. Con esta herramienta se puede hacer monitoreo del flujo de red en tiempo real, recolectar datos del flujo de red, identificar el flujo de datos que procesan los programas de los equipos que están dentro de la red y ofrece herramientas para las auditorías de datos.

Con Argus se puede realizar una optimización dirigida a la red, basado en los siguientes parámetros:

- **Identificar:** descubre e identifica el comportamiento de la red.
- **Analiza: r**ecoger y transformar los datos en métricas de optimización, establecen probabilidades de ocurrencia y líneas de base priorizar eventos.
- **Planea:** establece criterios de aceptación, permite implementar acciones de ser necesario.
- **Traza:** monitorea indicadores de comportamiento de red para realizar cambios.
- **Controla:** corrige las desviaciones de criterios.

Imagen 1. Parámetros de ARGUS
Fuente: http://www.cert.org/flocon/2010/presentations/Bullard_IntroductionToArgus.pdf

Tcpdump

Este software es una buena herramienta que permite ser trabajada por de comandos en Linux y Unix. Con ella se puede **analizar e interceptar tráfico de datos entrante y saliente** dentro de una red a la que se encuentre conectado el equipo. En la mayoría de los casos, en Unix se requiere tener privilegios de súper usuario para poder ejecutar TCPDUMP, pero también es posible establecer la configuración de tal forma que pueda ser utilizado por usuarios sin privilegios.

Adicional, Tcpdump permite ver los paquetes de datos que viajan dentro de la red en el cual previamente se han volcado los paquetes de red.

Algunos ejemplos prácticos de este servicio, se describen a continuación:

- Capturar tráfico cuya dirección IP de origen sea 192.168.2.1 tcpdump src host 192.168.2.1
- Capturar tráfico cuya dirección origen o destino sea 192.168.1.1 tcpdump host 192.168.1.1
- Capturar tráfico con destino a la dirección MAC A0:4F:A5:2E:E9:51 tcpdump ether dst A0:4F:A5:2E:E9:51
- Capturar tráfico con destino el puerto 23 tcpdump dst port 23
- Capturar todo el tráfico excepto el https tcpdump tcp and not port 443
- Capturar el tráfico Web tcpdump tcp and port 80
- Capturar (TCP, UDP, ICMP, ARP)

  Tcpdump –i eth0[1] tcp

  Tcpdump –i eth1 udp

  Tcpdump –i eth0 acmp

  Tcpdump –i eth0 arp

Estos ejemplos sólo son una pequeña muestra de todas las posibilidades que se tienen para la captura de tráfico, esta herramienta es muy útil y sencilla de manejar. Por supuesto hay configuraciones más avanzadas que son más complejas, pero no es algo que se salga del alcance de la persona que quiera profundizar en el tema y emplearlo en su red.

SATAN (Security Administrator Tool for Analyzing Networks)

Este software trabaja con sistemas UNIX, es de libre distribución (dominio público) y es una efectiva herramienta de seguridad para ayudar a administradores de redes a controlarla de manera efectiva, ya que permite identificar las máquinas que están conectadas a la red, puede chequear los datos básicos, como IP, MAC address y los servicios que se están realizando en cada máquina. Puede generar una base de datos con todas las máquinas que identifica y las almacena para posteriores revisiones y comparaciones entre máquinas. Puede identificar máquinas sospechosas que no parezcan pertenecer originalmente a la red o que se ingresaron recientemente, lo que le permite identificarlas y si no cumplen con el perfil de seguridad son rechazadas y/o se bloquea los accesos que estas máquinas puedan tener a la red.

Este aplicativo funciona vía web, lo que permite su ingreso desde cualquier ordenador, tiene tres tipos de advertencias o alarmas dado el caso de encontrar falencias o equipos sospechosos. (Nivel bajo, nivel normal y nivel alto). Una vez realizado el escáner de los equipos conectados, directamente desde la web genera un reporte, con una resumida explicación de la falla.

SATAN tiene la posibilidad de verificar varios tipos de protocolos como lo son: NFS, NIS, FTP, DNS, REXD, puede determinar qué tipo de sistema operativo tienen las máquinas analizadas. Algunos de los problemas encontrados por SATAN, se muestran a continuación:

- NFS file systems exported to arbitrary hosts.
- NFS file systems exported to unprivileged programs.
- NFS file systems exported via the portmapper.

[1] Para capturar todo el tráfico de entrada y salida de una interfaz de red concreta (eth0, eth1…), se utiliza parámetro "-i" seguido del identificador de la interfaz donde se encuentra conectado:

- NIS password file access from arbitrary hosts.
- Old, sendmail versions.
- REXD access from arbitrary hosts.
- X server access control disabled.
- Arbitrary files accessible via TFTP.
- Remote shell access from arbitrary hosts.
- Writable anonymous FTP home directory (tomado de http://www.porcupine.org/satan/summary.html).

El inconveniente con SATAN es que también puede utilizarse como herramienta para acceder sin permisos a la información de redes ajenas, descubriendo su topología y consiguiendo información de los equipos.

ISS (Internet Security Scannner)

Hasta el 2006, era una herramienta de dominio público, hasta que fue adquirida ese año por IBM. Esta herramienta es un sistema de gestión centralizada que unifica la gestión y análisis de red, servidor y escritorio Endpoint Security agentes y redes pequeñas o electrodomésticos con acceso a la red. Proporciona comandos, control y capacidades de monitoreo para todos los productos de seguridad de IBM.

Muchas de las opciones que ofrece este aplicativo se describen a continuación:

- **Gestión de la sesión:** permite controlar los tiempos de espera de sesión para consolas locales y remotas y configurar el número máximo de sesiones simultáneas.
- **Sesiones activas consola:** las sesiones de consola activas pueden ver todas las sesiones de consola activas que están conectadas al servidor de aplicaciones. También se puede enviar un mensaje a uno o más usuarios activos.
- **Inicio de sesión personalizado:** permite personalizar un banner de inicio de sesión y controlar si un usuario debe reconocer el inicio de sesión en el sistema.
- **Gestión de usuarios:** realiza control de gestión de usuarios. Además de la gestión de los grupos y usuarios, adicional tiene la configuración de seguridad de los siguientes elementos:
  - Gestión de inactividad del usuario (que incluye incapacitantes usuarios con largos períodos de inactividad).
  - Monitoreo de intentos de conexión simultáneos.
  - Ajuste de la duración de la vigilancia de exitosos y fallidos intentos de conexión, nombres de usuarios concurrentes, cambios de permisos, y los cambios de pertenencia a grupos.
  - Configuración de notificaciones para las conexiones concurrentes, cambios de permisos, y los cambios de pertenencia a grupos.
- **Historial de cuenta:** muestra los detalles de los inicios de sesiones exitosas y fallidas, cambios de pertenencia a grupos, y los cambios de permisos para un usuario.
- **Reglas de cuarentena:** realiza las siguientes tareas:
  - Crear una regla de cuarentena que se basa en un evento de tráfico de la red.
  - Activar o desactivar las reglas de cuarentena activas.
  - Ver reglas de cuarentena activas y caducados.

- Promover una regla de cuarentena activa a un grupo o un sitio completo.

- **Autorización dual:** controla si ciertas acciones requieren la aprobación de un segundo personal autorizado. La autorización dual está disponible para las siguientes acciones:
  - Implementación de una política.
  - Extracción de un despliegue de políticas.
  - Añadir una actualización agente (XPU).
  - Quitar una actualización de agente (XPU).
  - Inicio de un agente.
  - Detener un agente.
  - Reinicio de un agente.
- **Entradas de auditoría:** las entradas de auditoría se crearon para sesiones máximas concurrentes, la configuración de inicio de sesión, gestión de usuarios, gestión de sesiones, y de gestión de reglas de cuarentena.

Como se puede apreciar en esta breve descripción de ISS, es una herramienta muy robusta desde que fue adquirida por IBM, pero ya no es un software libre y por lo tanto su utilización significa un costo elevado.

Courtney

Este software libre, permite hacer contra peso a la mala utilización de SATAN, ya que monitorea la red y detecta los posibles ataques que se puedan realizar con este Software. Courtney trabaja en conjunto con tcpdump, ya que permite realizar el control de peticiones tipo TCP/IP, ya que verifica si se está presentando continuas peticiones sobre los puertos TCP y UDP dentro de la red, si se detectan peticiones Courtney tiene la posibilidad de generar alarmas o avisos por medio de syslog. De esta manera se puede verificar en tiempo real lo que el atacante está tratando de chequear en los puertos que son vulnerables.

Por ejemplo, si una máquina se conecta a distintos servicios en una ventana de tiempo, Courtney está en la capacidad de identificarlo como un potencial host SATAN. Una vez identificado, genera una alarma.

NOCOL (Network Operations Center On-Line)

Es un sistema de monitoreo muy conocido y utilizado, el cual corre en sistemas UNIX, el cual permite monitorear redes y dispositivos conectados a estas redes. Este sistema es capaz de monitorear protocolos como DNS, NTP, TCP o puertos de internet, syslogs, servidores radius, etc.

La información que recibe NOCOL, es transformada al lenguaje que este software maneja y la escribe con el fin que pueda ser procesada y evaluada. De acuerdo al algoritmo interno, se puede determiner la gravedad del evento que se está evaluando, los cuales están divididos en cuatro niveles: crítico, error, peligro e información.

Algunos de los servicios de monitoreo que pueden ser controlados por NOCOL, son los que se muestran a continuación:

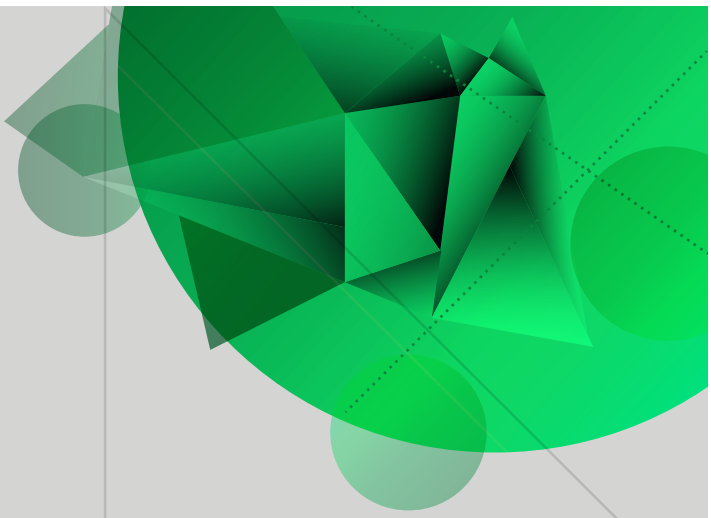
ICMP ping	RPC portmapper
OSI ping	Ethernet load
TCP ports	Nameserver
Radius server	Syslog messages
Mailq	NTP
UPS (APC) battery	Unix host performance
BGP peers	SNMP variables
Data throughput	

Actualmente, este poderoso software ha sido remplazado por SNIPS, el cual cumple con las mismas funciones y sigue siendo software libre.

3

Unidad 3

Securizando el acceso y los ficheros de los dispositivos



Seguridad en redes

Autor: Esteban Bejarano Forero

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

Si bien los temas ya evaluados en las unidades anteriores, han tenido mucho que ver con sistemas basados en UNIX, no se puede dejar de lado la parte de seguridad que brindan prestigiosas marcas como lo es Cisco.

Por tal motivo, en esta unidad se verá la forma como ellos explican el modelo de securización de la red, basados en políticas creadas por Cisco.

U3 Metodología

Para este capítulo, es muy importante tener en cuenta la forma como se configuran los equipos de Cisco, los cuales ya fueron explicados en otro módulo de la carrera. Sin embargo, en esta unidad se realizará una breve descripción de la forma como se pueden configurar estos equipos.

Para poder entender un poco más el funcionamiento de estos equipos, se aconseja al estudiante ver algunos tutoriales en internet. No se busca que se logre un nivel experto, pero sí que tengan un conocimiento básico.

Securizando el acceso y los ficheros de los dispositivos

Como ya se ha visto a lo largo de todo el módulo, la seguridad dentro de una infraestructura de red grande, es compleja y por ende comienza a ser más complicado protegerla de manera que se mantenga íntegra. Dentro de toda red, existen equipos que determinan una mayor importancia dentro de la misma, estos equipos, por lo general son los más apetecidos, ya que por lo general son los que dominan las principales funciones de toda una infraestructura de red.

Es importante analizar los diversos problemas que se podrían presentar si un atacante lograra hacerse al control de un equipo principal, este podría deshabilitar, eliminar, cambiar, afectar la funcionalidad de una red. Por tal motivo es indispensable que se creen acciones de seguridad basadas en las políticas de seguridad informática de la empresa, con el fin de tener métodos que permitan actuar frente a ese tipo de eventos.

Para poder trabajar la seguridad de accesos a nivel general, se deben tener los siguientes parámetros:

Seguridad en los equipos de borde

El primer equipo que se presenta en los límites de una red, es el router de borde, este es el último equipo que es encuentra entre la red privada y las redes públicas como el Internet. Estos equipos son unos de los más importantes, debido a que todo el tráfico de internet pasa por este medio. Esto significa que estos router cumplen la función de defensa de la red privada (LAN). También implica que se pueden crear políticas que restrinjan el tipo de datos que puede salir y entrar a la red.

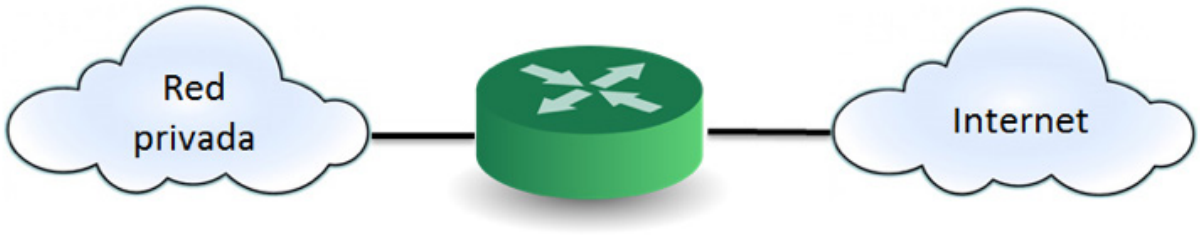


Imagen 1. Router de borde
Fuente: Propia.

Esta es una de las principales razones por la que los atacantes buscan ingresar a los router de Borde, ya que teniendo el control de estos, por supuesto podrán ingresar sin mayor problema al resto de la red. Por lo general estos equipos son administrados por los PSI (proveedores de servicios de Internet), así que ellos son los encargados de realizar las políticas de seguridad, en coordinación con los administradores de la red de la red privada.

El segundo equipo de borde es el Firewall (rompe muros), el cual se encarga de reforzar las políticas de seguridad que se implementan en los router de borde, controla de acceso adicional ya que monitorea el estado de las conexiones que se realizan dentro de la red.

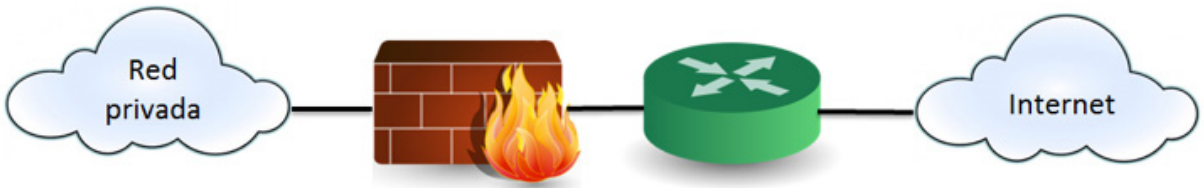


Imagen 2. Red con Implementación de Firewall
Fuente: Propia.

Existe una variante en la seguridad, el cual permite un acceso libre a ciertos servidores o equipos, los cuales necesariamente deben ser accedidos mediante Internet o redes externas a la empresa. Esta variante se conoce como DMZ (demilitarized zone). Para implementar un DMZ, se debe contar con el apoyo del Firewall, ya que en este se encuentran los permisos y se pueden habilitar o deshabilitar las conexiones requeridas. En la variante DMZ, el router de borde provee protección filtrando cierto tipo de tráfico, pero deja la mayoría de la protección a cargo del firewall.

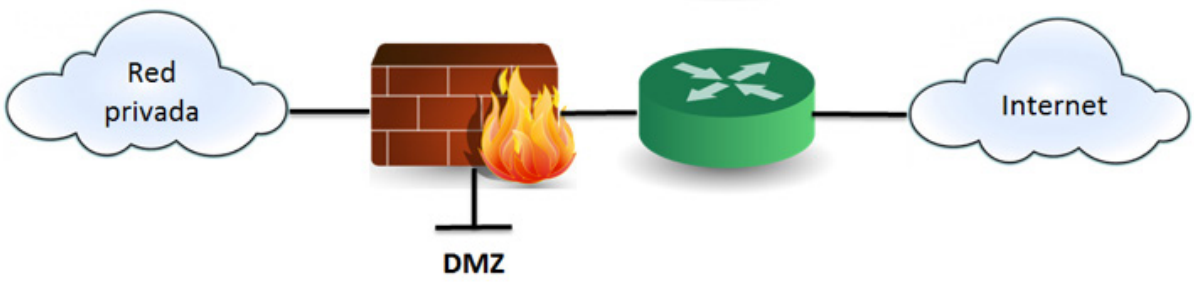


Imagen 3. Red con Implementación de Firewall y variante DMZ
Fuente: Propia.

Existen otros parámetros que se deben tener en cuenta en cuanto a la seguridad de los Router:

Seguridad física, la cual se habló un poco en la primera unidad, donde se ve la necesidad de cuidar físicamente los equipos, tenerlos en un lugar protegido, con acceso restringido (donde sólo el personal autorizado pueda ingresar).

Seguridad de los sistemas operativos: se debe procurar mantener actualizados los SO de los equipos, ya que muchas actualizaciones incluyen algunos parámetros que permiten que la red sea más estable. También es importante configurar la memoria de procesamiento de estos equipos, con el fin de agilizar la carga de transmisión y recepción de datos y evitar ataques de DoS.

Bloqueo de puertos: es importante hacer el bloqueo de los puertos y los servicios que no se utilizan dentro de la red, esto limita las posibilidades de ataques.

Restricciones de acceso: un router tiene la posibilidad de accederse por varios usuarios (si se tiene un usuario y password), pero es importante que estos usuarios sean limitados y se manejen esquemas de permisos, ya que no todos deberían estar en la capacidad de modificar la configuración de los equipos (escritura, lectura), algunos usuarios sólo requieren permisos de lectura, esto evita que se borren o se realicen malas configuraciones.

Se debe tener presente que se puede realizar restricciones para que sólo algunos usuarios puedan tener accesos locales y remotos. Recordemos que los accesos remotos son más complicados y vulnerables a los ataques, por esa razón deben existir restricciones para que no cualquiera pueda intentar ingresar a los router.

Configuración de un acceso administrativo seguro

El tema de contraseñas fuertes ya se ha venido tratando a lo largo del módulo. Pero Cisco hace un enfoque fuerte con respecto a este tema, ya que ofrece diversas formas de proteger los accesos por contraseñas de los equipos.

Se sugiere tener contraseñas mayores a 8 dígitos, donde se mezclen mayúsculas, minúsculas, números y caracteres especiales. No utilizar nombres o números familiarizados con cosas personales. Hacer el cambio periódico de estas contraseñas y por supuesto no publicar o dejar a simple vista las contraseñas. Un administrador de red está en la obligación de mantener la seguridad y por lo tanto debe tener contraseñas fuertes.

Para los equipos Cisco, poder ingresar a sus puertos de consola, terminales virtuales y puertos auxiliares, se requiere del uso de contraseñas, esto refuerza la seguridad. También se puede otorgar niveles de privilegios. Estas son maneras de mantener a salvo los accesos a los terminales de red.

Un ejemplo para cada tipo de acceso se muestra a continuación:

Modo privilegiado

Se quiere restringir el acceso al modo EXEC privilegiado del router con una contraseña, se ingresa la siguiente línea de comando:

```
ROUTER_BORDE(config)#enable secret $eguRid4d
ROUTER_BORDE(config)#
```

Imagen 4
Fuente: Propia.

Línea de consola

Por defecto el puerto de línea de consola no solicita contraseña, pero se le puede asignar una:

```
ROUTER_BORDE(config)#line console 0
ROUTER_BORDE(config-line)#password R3d$egur4
ROUTER_BORDE(config-line)#login
```

Imagen 5
Fuente: Propia.

Líneas de terminal virtual

Este terminal lo que permite es indicar cuántos usuarios a la vez (máximo 5) pueden iniciar sesión desde terminales virtuales (SSH o Telnet) en el Router, para crear un password, se ingresa el siguiente comando:

```
ROUTER_BORDE(config)#line vty 0 4
ROUTER_BORDE(config-line)#password m0duLo$eguRid4d
ROUTER_BORDE(config-line)#login
```

Imagen 6
Fuente: Propia.

Línea auxiliar

Algunas veces se usa el puerto auxiliar para configurar y monitorear remotamente el router usando una conexión de módem dialup, aunque esto ya no es tan común:

```
ROUTER_BORDE(config)#line aux 0
ROUTER_BORDE(config-line)#password $ecuR3mOd3
ROUTER_BORDE(config-line)#login
```

Imagen 7
Fuente: Propia.

Para todo este tipo de contraseñas, es importante que se realice la codificación de las contraseñas, ya que por defecto, si se realiza el comando show running-config, se podrá ver todas las contraseñas que se han creado:

```
ROUTER_BORDE#sho running-config
enable secret $eguRid4d
...
line con 0
 password R3d$egur4
 login
!
line aux 0
 password $ecuR3mOd3
 login
!
line vty 0 4
 password m0duLo$eguRid4d
 login
```

Para evitar lo anterior, se puede utilizar el comando

```
ROUTER_BORDE(config)# service password-encryption
```

De esta manera, al volver a correr el comando show running-config, lo que se vería es algo así:

```
ROUTER_BORDE#sho running-config
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
...

line con 0
 password 7 0822455D0A16
 login
!
line aux 0
 password 7 0865494D1C2B561A3D0F5F
 login
!
line vty 0 4
 password 7 082C1C4A1C350A53170C1936232F702C
 login
```

Otra configuración de seguridad, es la deshabilitación de conexiones no utilizadas. Por defecto, en los equipos Cisco, al tener una sesión activa, se puede mantener por 10 minutos sin caducar una vez se realiza una última actividad. Este tiempo se puede disminuir, con el fin de reducir el tiempo que podría tener un atacante para acceder al modo privilegiado.

Configuración de SSH

El ingreso remoto es un tema importante en la seguridad de una red. Como se vio en la unidad pasada, métodos de acceso remoto como lo es Telnet, no son muy confiables, es por ello que surge la necesidad de buscar nuevas alternativas de acceso remoto, ya que esto significa grandes beneficios. Es por esto que se crea el protocolo SSH (Secure Shell), ya que soporta la necesidad de confidencialidad e integridad de la sesión, ya que realiza el cifrado de la conexión.

Por supuesto Cisco, también permite su acceso mediante SSH. Para poderlo configurar en estos equipos, se debe:

1. Verificar que el router tenga un nombre de host único y se debe configurar el nombre de dominio IP de la red:

```
ROUTER_BORDE (config) #ip domain-name nombre-dominio
```

2. Es muy importante que cada Router de destino tenga un Nombre de host único.
3. Asegurar que cada router de destino esté utilizando el nombre de dominio que corresponde a la red.
4. Habilite sesiones SSH vty de entrada usando los comandos de línea vty login local y transport input ssh.

```
ROUTER_BORDE# config terminal
ROUTER_BORDE(config)#ip domain-name aandina.com
ROUTER_BORDE(config)#crypto key generate rsa general-keys
modulus 1024
```

El intervalo de tiempo por defecto que tienen los router para que responda el cliente SSH durante la fase de negociación SSH es de 120 segundos, por supuesto puede ser mo9dificado, con el uso del comando ip ssh time-out **segundos** en el modo de configuración global.

Adicional, por defecto, el usuario tiene tres intentos para ingresar por SSH. Para configurar un número diferente de intentos consecutivos SSH, se debe usar el comando ip ssh authentication-retries **entero** en el modo de configuración global.

```
ROUTER_BORDE# config terminal
ROUTER_BORDE(config)#ip ssh time out 80
ROUTER_BORDE(config)#ip ssh authentication-retries 2
```

CLI basada en roles

Cisco introdujo la función de CLI basado en roles en sus sistemas operativos, con el fin de permitir mayor flexibilidad en los niveles de privilegios, esto significa que un administrador de la red, puede crear diferentes perfiles para diferentes usuarios, con el fin que no todos tengan los mismos privilegios. Con esta función, la red presenta:

- Seguridad: el acceso a la CLI basado en roles mejora la seguridad del router, permitiendo que los usuarios puedan realizar determinados comandos dentro del equipo. No todos los usuarios tendrán las mismas posibilidades, por ejemplo, mientras que un usuario con altas posibilidades de vistas, o modificaciones, puede crear o borrar rutas, un usuario con bajos permisos sólo los podrá ver o incluso ni siquiera tendrá acceso a esta información.
- Disponibilidad: el acceso a la CLI basado en roles impide que se efectúe la utilización de comandos de modificación de la configuración por parte de usuarios no autorizados.
- Eficiencia operativa: el acceso a la CLI basado en roles sólo le permite ver a los usuarios los comandos a los que tienen permisos. Esto le permite al usuario identificar fácilmente los comandos a los que puede acceder, sin necesidad de tener que ver la gran cantidad de opciones que un router puede tener.

El acceso a la CLI basado en roles, permite crear tres tipos de vista:

- Vista de root: un administrador debe estar en esta vista, para poder realizar cualquier tipo de configuración, Sólo un usuario con la opción de vista de root puede configurar nuevas vistas, agregar o remover comandos de las vistas existentes. Es decir, tiene los privilegios más altos.
- Vista de CLI: no posee jerarquías de comandos y, por lo tanto, no hay posibilidad de tener vistas superiores o inferiores. A este tipo de usuarios se les asignan las vistas que tendrá disponibles y los comandos que podrá utilizar.
- Supervista: en este tipo de vista, el administrador decide qué comandos pueden ser utilizados y hasta qué punto pueden acceder a la información del router (como por ejemplo la configuración del Router, o el enrutamiento que está manejando). Con las supervistas el administrador de redes puede asignar a los usuarios y grupos de usuarios múltiples vistas CLI de una sola vez, en lugar de tener que asignar vistas CLI uno por uno.

La vista de root es la más importante de las tres y se necesita para poder crear vistas CLI y supervistas.

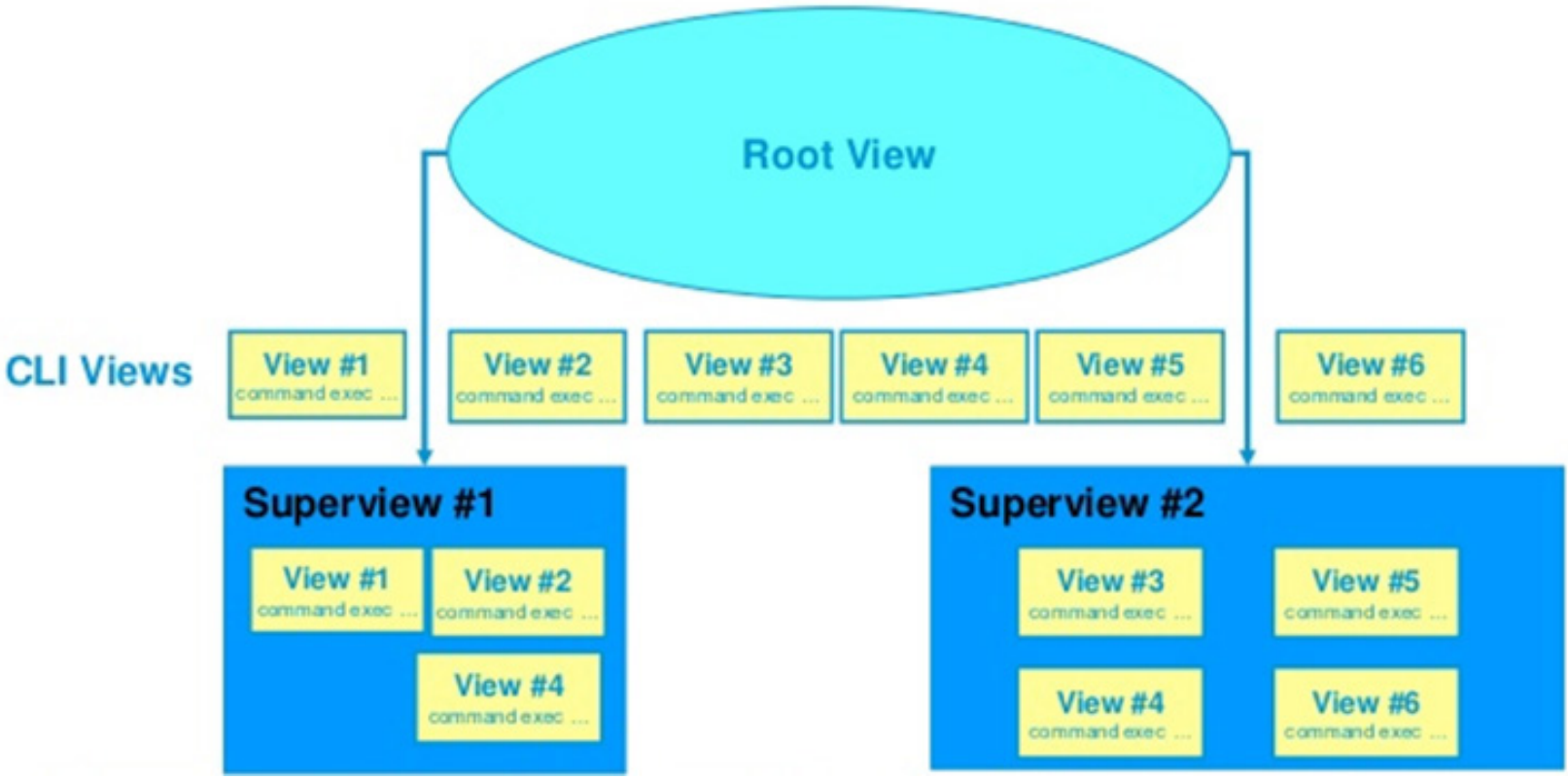


Imagen 8. Tipos de vista
Fuente: http://image.slidesharecdn.com/ccnasv11ch02eb-120920104518-phpapp01/95/ccnas-v11-ch02eb-56-728.jpg?cb=1348138169

Como se puede ver en el gráfico, las Supervistas contienen Vistas CLI, pero no pueden ejecutar comandos, pero en dos diferentes supervistas se pueden ver las vistas CLI.

Un administrador de la red, debe tener en cuenta lo siguiente para poder habilitar vistas CLI:

- Paso 1. Habilitar AAA (*Authentication, Authorization, and Accounting*) con el comando de configuración global `aaa new-model`. Salga e ingrese a la vista de root con el comando `enable view`.
- Paso 2. Crear una vista con el comando `parser view nombre-vista`. Esto habilita el modo de configuración de la vista.
- Paso 3. Asignar una contraseña secret a la vista usando el comando `secret contraseña-encriptada`.
- Paso 4. Asignar comandos a la vista seleccionada usando el comando `commands parser-mode {include | include-exclusive | exclude} [all] [interface nombre-interfaz | comando]` en el modo de configuración de vista.

```
ROUTER_BORDE (config)# parser view first
00:11:40:%PARSER-6-VIEW_CREATED:view 'first' successfully
created.
ROUTER_BORDE (config-view)# secret 5 firstpass
ROUTER_BORDE (config-view)# command exec include show
version
ROUTER_BORDE (config-view)# command exec include configure
terminal
ROUTER_BORDE (config-view)# command exec include all show ip
ROUTER_BORDE (config-view)# exit
ROUTER_BORDE (config)# parser view second
00:13:42:%PARSER-6-VIEW_CREATED:view 'second' successfully
created.
ROUTER_BORDE (config-view)# secret 5 secondpass
ROUTER_BORDE (config-view)# command exec include-exclusive
show ip interface
ROUTER_BORDE (config-view)# command exec include logout
ROUTER_BORDE (config-view)# exit
!
!
ROUTER_BORDE (config-view)# do show run | beg view
parser view first
 secret 5 $1$MCmh$QuZaU8PIMPlff9sFCZvgW/
 commands exec include configure terminal
 commands exec include configure
 commands exec include all show ip
 commands exec include show version
 commands exec include show
!
parser view second
 secret 5 $1$iP2M$R16BXKecMEiQesxLyqygW.
 commands exec include-exclusive show ip interface
 commands exec include show ip
 commands exec include show
 commands exec include logout
```

Los pasos para crear una supervista, son prácticamente los mismos, pero se debe tener en cuenta un cambio en el comando commands para asignar comandos, debe usarse el comando view nombre-vista para asignar vistas.

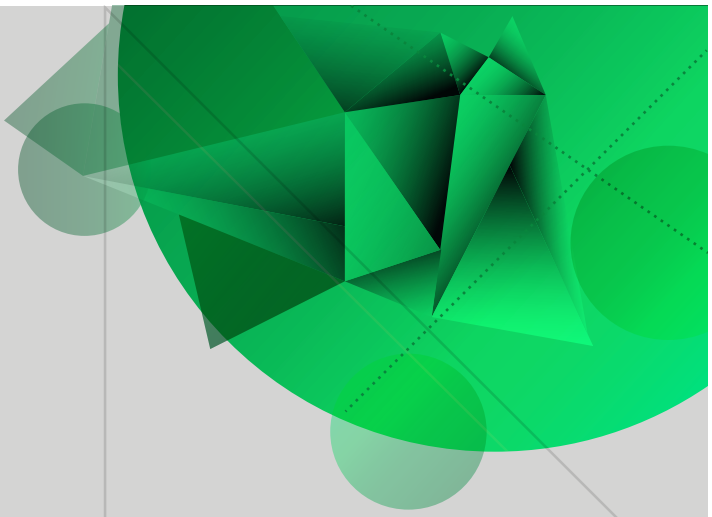
- Paso 1. Crear una vista usando el comando `parser view nombre-vista superview` e ingresar al modo de configuración de supervista.
- Paso 2. Asignar una contraseña secret a la vista usando el comando `secret contraseña-cifrada.`
- Paso 3. Asigne una vista existente usando el comando `view nombre-vista` en el modo de configuración de vista.

```
parser view su_view1 superview
 secret 5 <encoded password>
 view view_one
 view view_two
!
parser view su_view2 superview
 secret 5 <encoded password>
 view view_three
 view view_four
```

3

Unidad 3

Dispositivos de monitorización



Seguridad en redes

Autor: Esteban Bejarano Forero

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

En este capítulo, se continuará viendo parámetros importantes correspondientes a "securizando la red". Se mostrará su utilidad y algunas de las configuraciones que se pueden realizar para ser implementadas.

U3 Metodología

Es importante realizar las prácticas que se realizarán en las actividades complementarias, para probar las configuraciones que se presentarán en esta unidad.

Dispositivos de monitorización

Continuando con el amplio tema de la securización de la red, se deben tener en cuenta que existen varias formas de realizar el monitoreo de los dispositivos de red. A continuación se mostrarán cuatro de las más relevantes, las cuales todas son configurables en equipos Cisco.

Crear el backup de la configuración y guardar la imagen del IOS

Volvamos al tema que más nos preocupa en este módulo: la seguridad y los riesgos que se pueden correr si un atacante quiere acceder a nuestra red y peor aún si logra tener acceso al router de borde o algún otro. Este atacante, tendría el poder de modificar, crear, e incluso eliminar la configuración de un equipo. Si esto llega a ocurrir, no habría forma de recuperar la configuración. Es por este motivo que se hace indispensable realizar copias de seguridad de las configuraciones de los router y de las imágenes de IOS.

Algunos equipos Cisco, tienen la opción de recuperar las configuraciones e imágenes de presentarse un formateo de la memoria flash o un borrado del archivo de configuración de inicio en la NVRAM, este se conoce como *Resilient Configuration* (configuración resistente). Esta función sólo está disponible para sistemas que soporten una interfaz flash *Advanced Technology Attachment* (ATA) PCMCIA. Una vez asegurada la imagen, se negará todas las solicitudes para copiarla, modificarla o eliminarla. La copia segura de la configuración de inicio se almacena en flash junto con la imagen segura del IOS.

Los comandos que se utilizan para asegurar las funciones de configuración resistente, son los dos siguientes:

Comando secure boot-image

El comando **secure boot-image** habilita la resistencia de la imagen del IOS de Cisco, al mismo tiempo se crea una entrada en el registro. Esta función puede ser deshabilitada solo por medio de una sesión de consola usando la forma **no** del comando.

Es importante tener en cuenta que este comando sólo funciona adecuadamente cuando el sistema está configurado para ejecutar una imagen de un dispositivo de almacenamiento externo con una interfaz ATA (*Advanced Technology Attachment*). Adicionalmente, la imagen actual debe ser cargada desde un dispositivo de almacenamiento permanente para ser asegurada.

Comando secure boot-config

Permite tomar una instantánea de la

configuración actual del router y archivarla de manera segura en el dispositivo de almacenamiento permanente. El archivo de configuración está oculto y no puede ser visto o eliminado directamente desde el prompt de la vista CLI.

Si se llegara a presentar que se pierda la contraseña de acceso al router o no se tiene esta contraseña, existe un proceso que se puede realizar conectando un equipo por medio de cable de consola al router, pero este proceso debe verse con mayor atención en un nivel un poco más avanzado de configuración de equipos Cisco.

Sin embargo es importante aclarar que esta recuperación de contraseñas es por medio de acceso físico al router, por tal motivo nuevamente se insiste en que el tema de la seguridad Informática no sólo se puede tener en cuenta a nivel virtual, también se debe tener en cuenta la importancia de tener una buena seguridad a nivel físico.

Administración y reportes seguros

Todo administrador de una red, tiene la responsabilidad de manejar seguramente su red, conocer cada uno de los dispositivos principales que están dentro de su red y por supuesto, debe tener el control de todos ellos. Esto no es una tarea fácil y suele complicarse más cuando se habla de una empresa con proporciones enormes y que a la vez requiere muchos equipos de red conectados entre sí. Esto se debe tener presente y más si se llega a presentar un ataque en la red. El administrador debe tener presente los equipos que pueden estar en riesgo, el personal que tiene acceso a los equipos o a las configuraciones de estos. Crear un plan para la administración de cambios debe ser parte de una política de seguridad informática.

Es por esta razón, que es importante llevar el registro de la información de los dispositivos conocidos, con lo cual se logra tener un control de los movimientos, nuevas configuraciones, ingresos, etc. Toda la información que se quiera recolectar, debe estar completamente reflejada y explicada den las Políticas de seguridad Informática.

Estos syslogs, se pueden obtener de la mayoría o casi todos los equipos de red y en tiempo real, sólo se requiere habilitar algunas funciones dentro de cada equipo, como por ejemplo el protocolo SNMP *Simple Network Management Protocol* (Protocolo Simple de Administración de Red). El cual permite detectar el intercambio de información de administración entre dispositivos de red, con el propósito de monitorear y efectuar cambios en la configuración de los dispositivos.

Tener habilitadas estas funciones, permitirá que si se llega a presentar algún problema, se pueda consultar estos syslogs y se valide la forma de contrarestar problemas en la red o amenazas de seguridad.

Cuando se registra y se administra información, el flujo de información entre los hosts de administración y los dispositivos administrados puede tomar alguno de los siguientes caminos:

Fuera de banda (out of band - OOB) Flujos de información en una red de administración dedicada en los cuales no reside tráfico de internet.

En banda (in band) Flujos de información que atraviesan la red de Internet a través de canales de datos comunes.

Veamos el siguiente ejemplo, basados en la siguiente gráfica:

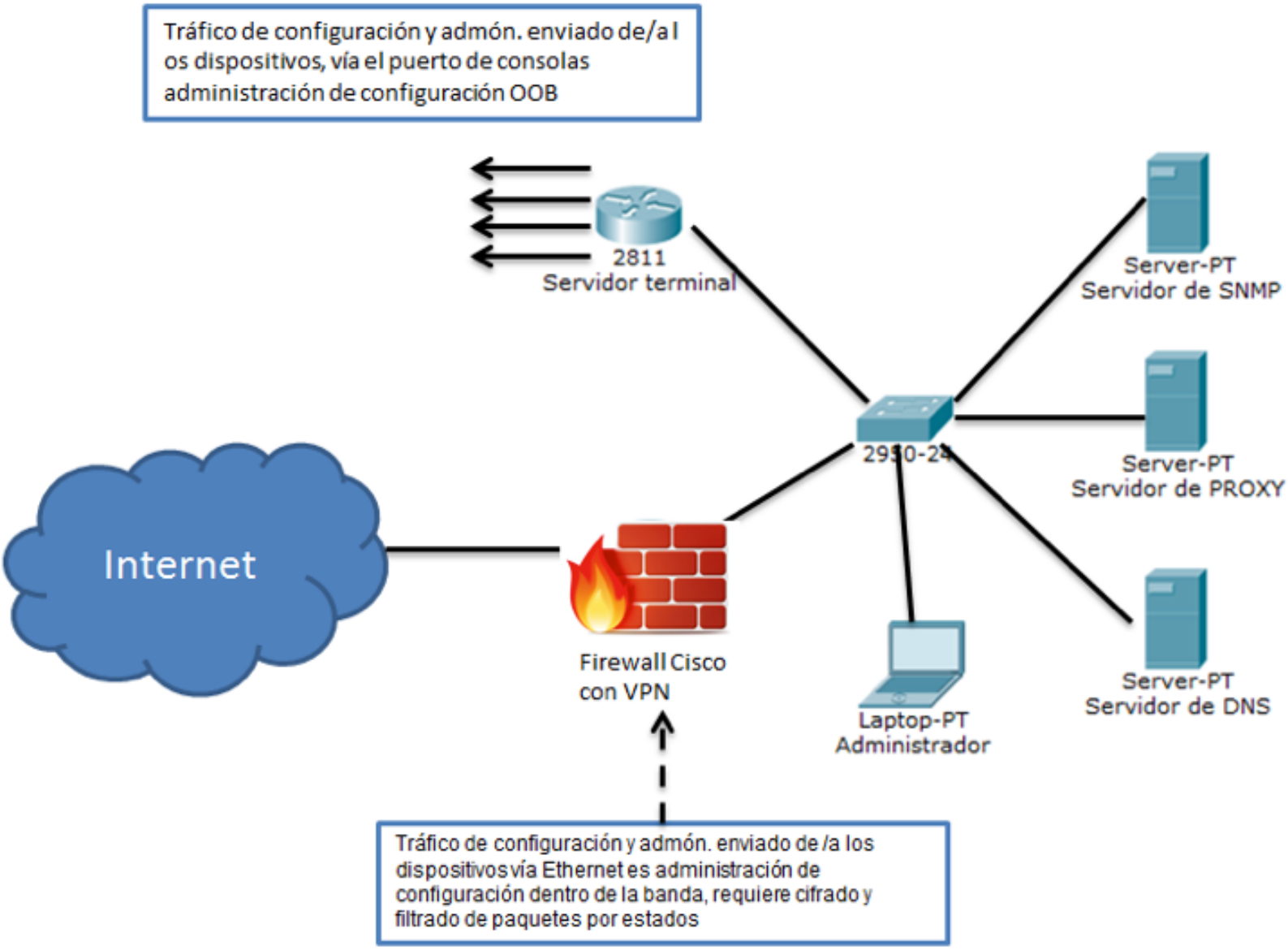


Imagen 1. Ejemplo de red empresarial
Fuente: Propia.

Esta red tiene dos segmentos de red separados por un router Cisco que tiene la función de firewall y un dispositivo VPN (*Virtual Private Network*). Al lado izquierdo del firewall están conectados servidores y dispositivos de administración y los servidores terminales que ofrecen conexiones directas OOB a cualquier dispositivo que solicite administración en la red de producción.

El otro lado del firewall se conecta con la red de Internet. La administración en banda ocurre sólo cuando una aplicación de administración no usa OOB. Si un dispositivo debe contactar a un host de administración por medio del envío de datos a través de la red de Internet, ese tráfico debería ser enviado de manera segura usando un túnel VPN. El túnel sólo debe permitir el tráfico requerido y limitado para administración y reportes de estos dispositivos. El firewall Cisco está configurado para permitir pasar información syslog al segmento de administración. Adicionalmente, se permite Telnet, SSH y SNMP.

Uso de Syslog para la Seguridad de Redes

Es importante realizar la implementación de sistemas de registro de actividades en los equipos Cisco, ya que con esta opción se pueden realizar validaciones como: registro de los cambios de configuración, estado en tiempo real de las interfaces e incluso posibles intentos de violación de la información o configuración del dispositivo.

Los router Cisco, pueden configurarse para que envíen mensajes, mediante:

- **SNMP traps:** los eventos de los routers, como la superación de un umbral, pueden ser procesados por el router y reenviados como traps SNMP a un servidor SNMP externo.
- **Syslogs:** es la herramienta de registro de mensajes más popular, ya que proporciona capacidades de almacenamiento de registro de largo plazo y una ubicación central para todos los mensajes del router.
- **Terminales:** las sesiones EXEC habilitadas pueden ser configuradas para recibir mensajes de registro en cualquiera de las líneas de terminal. Este tipo de registro no se almacena en el router y, por lo tanto, solo es útil para el usuario en esa línea.
- **Consola:** los mensajes se registran a la consola y pueden ser visualizados cuando se modifica o se prueba el router usando software de emulación de terminal mientras se está conectado al puerto de consola del router.

Los mensajes de registro de los routers Cisco contienen tres partes principales:

Fecha de evento

Nombre y nivel de severidad

Texto del mensaje

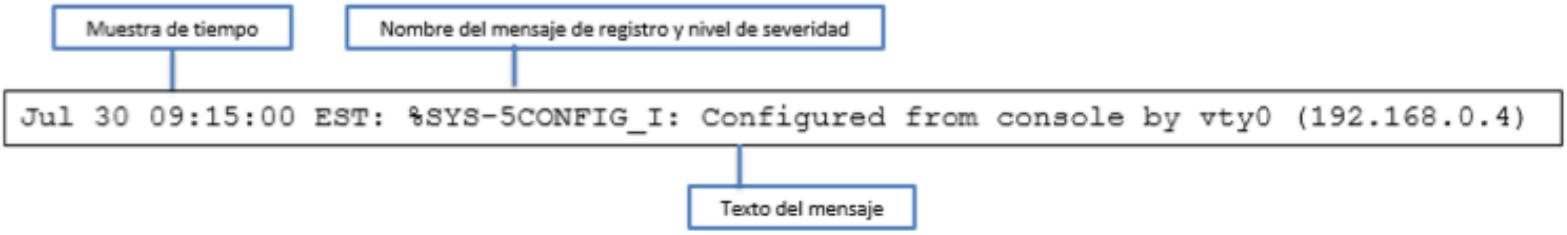


Imagen 2. Ejemplo de mensaje de Syslog
Fuente: Propia.

En el ejemplo se ve un mensaje con nivel 5, donde se indica que alguien configuró el router por medio del puerto vty0.

A continuación se realizará los siguientes pasos para configurar el registro del sistema:

1. Establecer el host de registro de destino usando el comando logging host.

2. (Opcional) Establezca el nivel de severidad del registro (trap) usando el comando logging trap nivel.
3. Establecer la interfaz de origen usando el comando logging source-interface. Esto especifica que los paquetes syslog contienen la dirección IPv4 o IPv6 de una interfaz particular, sin importar cuál interfaz usa el paquete para salir del router.
4. Habilite el registro usando el comando logging on.

Una configuración ejemplo sería así:

```
RouterA (config)#
RouterA (config)# logging host [hots name | ip addres]
RouterA (config)# logging trap level
RouterA (config)# logging source – interface interface – type interface
number
RouterA (config)# logging on
```

Se debe tener en cuenta que:

Host name es el nombre del dispositivo que se elegirá para que sea el servidor de Syslog.

IP addres, es la IP de este servidor.

Level, limita el número de mensajes del servidor de Syslog, se puede elegir entre 0 y 7.

Interface – type, es el típo de interface que se utilizará.

Interface number es el número de la interface que se utilizará.

```
RouterA (config)#
RouterA (config)# logging host syslog_ser 10.201.12.1
RouterA (config)# logging trap 5
RouterA (config)# logging source – interface gigaethernet 0/0
RouterA (config)# logging on
```

Uso de SNMP para la Seguridad de Redes

SNMP permite administrar nodos remotos, este protocolo permite realizar el intercambio de información entre un administrador y los dispositivos de red. Permite también administrar el rendimiento de la red, encontrar y solucionar problemas de la red.

Existen tres versiones de SNMP:

Versión SNMP 1: la versión más antigua y más básica de SNMP.

· Pros: con el apoyo de la mayoría de los dispositivos que son compatibles SNMP; fácil de configurar.

· Contras: la seguridad limitada, ya que sólo utiliza una contraseña simple ("cadena de comunidad") y los datos se envían en texto claro (sin cifrar); sólo debe utilizarse dentro de las LAN detrás de los firewall, y no en las WAN; sólo es compatible con contadores de 32 bits que no es suficiente para el monitoreo de ancho de banda con altas cargas de algunos gigabits / segundo.

· SNMP versión 2c: Añade 64 contadores bit.

· Pros: Soporta 64 contadores bit para controlar el uso del ancho de banda en las redes de gigabits / segundo cargas.

· Contras: la seguridad limitada (misma situación que con SNMP V1).

· Versión SNMP 3: añade autenticación y cifrado.

· Pros: ofertas cuentas de usuarios y autenticación para múltiples usuarios y cifrado opcional de los paquetes de datos, lo que hace que sea mucho más seguro; además de todas las ventajas de la versión 2c.

· Contras: ninguno.

Para tratar las vulnerabilidades de versiones anteriores de SNMP, SNMPv3 autentica y encripta paquetes a través de la red para proporcionar un acceso seguro a los dispositivos. SNMPv3 proporciona las siguientes funciones de seguridad:

Integridad del mensaje - Asegura que un paquete no haya sido manipulado durante el tránsito.

Autenticación - Determina que el mensaje proviene de una fuente válida.

Encriptación - Desordena el contenido de un paquete para evitar que sea visto por una fuente no autorizada.

Control de Acceso - Restringe ciertas acciones en porciones específicas de datos.

Utilización de características automatizadas

Inicialmente los routers de Cisco tienen muchos servicios habilitados por defecto. Esto se debe a que se procura que sea más fácil el proceso de configuración mínimo para tener el dispositivo plenamente operativo. Por esta razón, algunos de los servicios que se encuentran por defecto pueden hacer que el dispositivo se vuelva vulnerable a ataques si no se deshabilitan. Estos no son los únicos riesgos de seguridad ya que los mismos administradores de la red pueden habilitar otros servicios en los routers que llegar a crear riesgos significativos en la red. Ambas situaciones deben tomarse en cuenta al asegurar la red.

Un ejemplo más claro de esto, es el Protocolo de Descubrimiento de Cisco (Cisco *Discovery Protocol* - **CDP**) es un ejemplo de un servicio habilitado por defecto en los routers de Cisco. Se usa principalmente para obtener direcciones de protocolo de los dispositivos de Cisco que están al rededor y para descubrir las plataformas de esos dispositivos. Peligrosamente, un atacante puede usar este servicio para descubrir dispositivos en la red local. Adicionalmente, los atacantes no necesitan tener dispositivos habilitados para CDP.

El propósito de CDP es el de facilitar la tarea del administrador al descubrir y resolver problemas en otros dispositivos Cisco de la red. Sin embargo, por las implicancias de seguridad, el uso de CDP debe restringirse.

Se recomienda realizar algunas validaciones o bloqueos que permitirán cerciorarse que un dispositivo sea seguro:

- Deshabilitar las interfaces que no se estén utilizando.
- Deshabilitar los servicios que son innecesarios.
- Deshabilitar y restringir los servicios de administración, como SNMP.
- Deshabilitar servicios de escaneo, como ICMP.
- Asegurar la seguridad del acceso terminal.
- Deshabilitar ARP (Protocolo de Resolución de Direcciones (*Adress Resolution Protocol*).
- Deshabilitar broadcasts dirigidos por IP para evitar posibles ataques por DoS.

Cisco, tiene herramientas de auditoría de seguridad que permiten al administrador de la red determinar las vulnerabilidades existentes en la configuración actual. Esta permite efectuar validaciones en las configuraciones comparándolas con configuraciones recomendadas y recolectando discrepancias. Al identificarse las vulnerabilidades, los administradores de red deben modificar la configuración para reducirlas o eliminarlas:

Tres herramientas de auditoría de seguridad son:

- **El asistente de Auditoría de Seguridad:** proporciona una lista de vulnerabilidades y luego permite al administrador elegir cuáles cambios en la configuración potencialmente relacionados con la seguridad implementarán en el router.
- **AutoSecure de Cisco:** el comando autosecure inicia una auditoría de seguridad y luego permite cambios de configuración. Basándose en el modo seleccionado, los cambios de configuración pueden ser automáticos o requerir participación del administrador de la red.
- **One-Step Lockdown:** proporciona una lista de vulnerabilidades y luego efectúa los cambios de configuración recomendados para la seguridad automáticamente.

Autenticación, autorización y contabilidad (Authentication, Authorization, and Accounting - AAA)

Por políticas de seguridad informática, se debe restringir los accesos para el ingreso a una red privada. Sólo los usuarios autorizados deberían tener permisos para ingresar a ciertos servicios, dependiendo también su rango. También se debe implementar un sistema de registro de auditoría que monitoree quién inicia sesión, cuándo y qué hace mientras está conectado. Por esta razón, el protocolo AAA, permite trabajar una seguridad de acceso aceptable.

Los router Cisco tienen esta opción, con el fin de poder acceder a una base de datos local de usuario y contraseña.

Para ayudar a proporcionar registros de auditoría, puede implementarse la autenticación de base de datos local usando uno de los siguientes comandos:

```
username nombre-usuario password contraseña

username nombre-usuario secret contraseña
```

La seguridad AAA administrativa y de red tiene tres componentes funcionales en el ambiente Cisco:

Autenticación AAA

Permite autenticar usuarios para que puedan tener acceso administrativo o para que tengan acceso remoto a una red. Existen dos modos para solicitar los servicios de AAA:

- Modo carácter: el usuario realiza una solicitud que le permita establecer un proceso administrativo de modo EXEC con el router.
- Modo paquete: el usuario realiza una solicitud para establecer una conexión con un dispositivo que esté dentro de la red a través del router.

Para una red verdaderamente segura, también es importante configurar el router para acceso administrativo y acceso remoto a la red LAN seguros mediante el uso de los servicios AAA.

Autorización AAA

Ya identificado el usuario correctamente, contra la fuente de datos AAA seleccionada, se les permite el acceso a recursos específicos en la red. De esta manera el usuario es limitado a sólo lo que puede realizar en la red, luego de que es autenticado.

La autorización, que se implementa inmediatamente después de que el usuario se autentica, es automática: esto implica que no se necesita la participación por parte del usuario luego de haberse autentificado.

Registro de Auditoría AAA

Recolecta y reporta datos de uso para que puedan ser empleados para posibles auditorías que se requieran realizar en el futuro. Los datos recolectados pueden incluir el inicio y fin de conexiones, comandos ejecutados, números de paquetes y número de bytes.

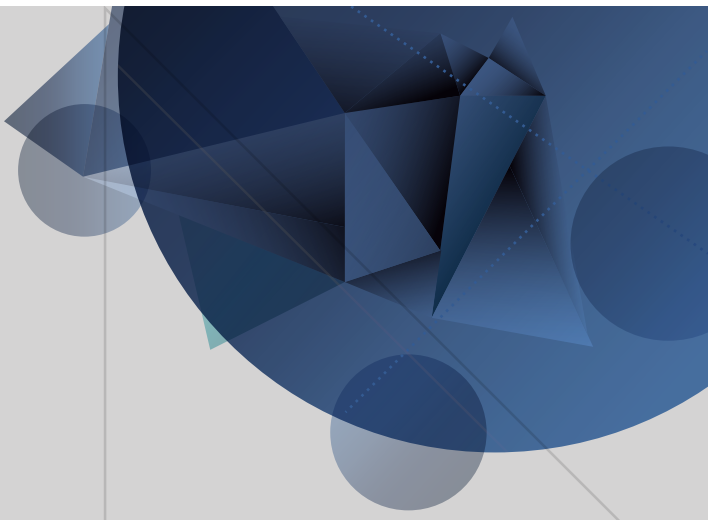
El registro de auditoría se implementa usando una solución AAA basada en servidor. Estas estadísticas pueden ser extraídas para crear reportes detallados sobre la configuración de la red.

El registro de auditoría proporciona una mejor rendición que la que ofrece la autenticación. Los servidores AAA mantienen un registro detallado de absolutamente todo lo que hace el usuario una vez autenticado en el dispositivo. Esto incluye todos los comandos de configuración realizados por el usuario. El registro contiene varios campos de datos, incluyendo el nombre de usuario, la fecha y hora y el comando ingresado por el usuario. Esta información es útil al solucionar problemas en los dispositivos. También proporciona protección contra individuos malintencionados.

4

Unidad 4

Corta fuegos (Firewall)



Seguridad en redes

Autor: Esteban Bejarano Forero

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

En esta unidad, se explicará con profundidad lo que es un Firewall, ya que en unidades pasadas se ha hablado mucho de él, pero no se le ha entregado la atención que se merece, ya que en la actualidad, tener implementados equipos como estos, son casi una obligación para poder mantener un poco más segura nuestras redes de datos.

U4 Metodología

La unidad que se verá a continuación es el complemento de la sección anterior "Securizando la red", por tal motivo se recomienda realizar una lectura cuidadosa con el fin de entender algunas funcionalidades extras de los equipos firewall, los cuales no se profundizaron de la unidad pasada.

Corta fuegos (Firewall)

Como ya se vio en pasadas unidades, desde la aparición de tecnologías que permitieron que las redes se intercomunicaran y el surgimiento de Internet, con ellos surgieron también los problemas de seguridad. Estas dificultades, pueden ser remediados o atenuados mediante el uso de tecnologías de firewall especializados, los cuales crean un nivel de seguridad apropiado permitiendo al mismo tiempo el acceso a los servicios de Internet.

Implementación de tecnologías de Firewalls

Los firewall son por lo general dispositivos físicos, aunque también existen software que simulan ser firewalls (sólo recomendable para pequeñas redes), los cuales pueden crear políticas de seguridad que limitan el tráfico entre la red privada e Internet, esto quiere decir, que tienen la capacidad de decidir quién puede entrar a la red y utilizar los recursos disponibles dentro de las redes que pertenecen a la organización. Esto obliga a que todo el tráfico pase por medio de los Firewall, con el fin que pueda ser analizado y se determine que puede transitar y qué será bloqueado.

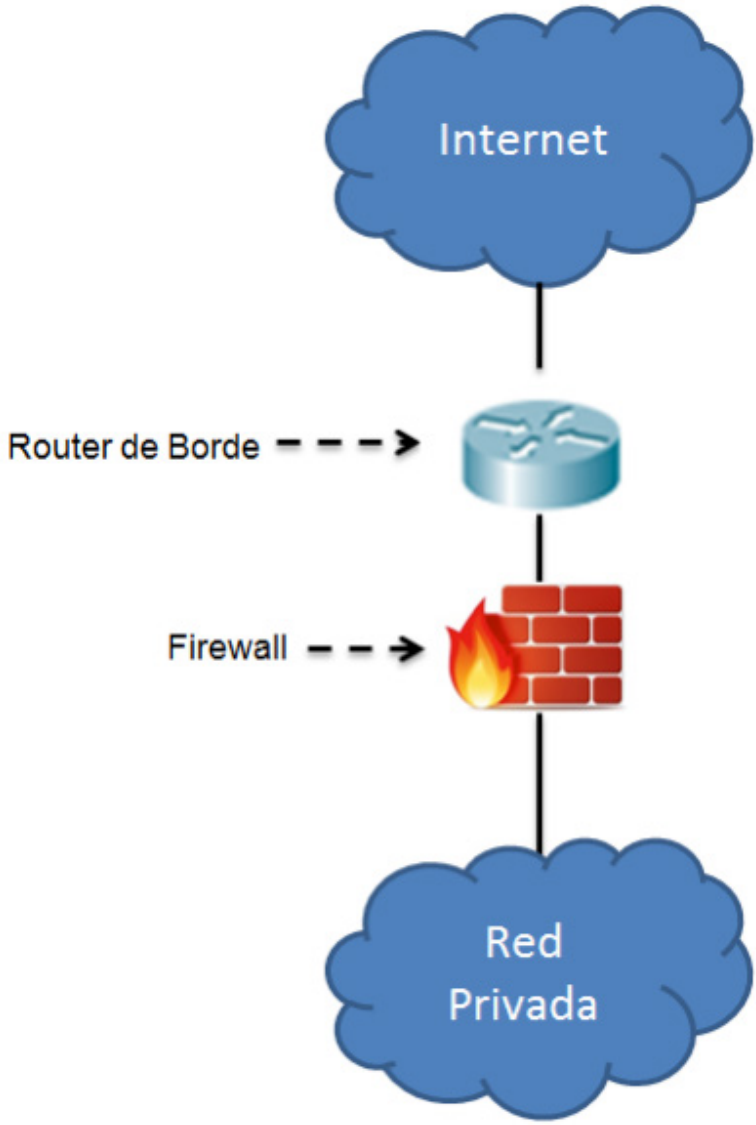


Imagen 1. Red con implementación de un firewall
Fuente: Propia.

Es importante tener claridad en lo que es y no es un Firewall, lo que permite y lo que no permite realizar:

Un firewall **no** es un ruteador, así como se muestra en la figura 1, la composición de una red necesita de un router de borde y de un firewall. El firewall tampoco es un servidor que funciona como defensa. Es parte del conjunto encargado de realizar perímetros de defensa que protegen la información dentro de una organización. Pero es importante que las Políticas de seguridad sean claras para que el Firewall pueda entrar a interactuar de manera correcta o si no, se estaría desperdiciando este recurso y finalmente no se estaría protegiendo correctamente la red privada.

Un Firewall tampoco es un Antivirus, a pesar que toda la información pasa por él, este no puede garantizar en un 100% que no existan virus, ya que debe tenerse en cuenta que todo el tráfico pasa por él y es imposible que pueda analizar todos los paquetes que pasan por él.

Por otro lado, por medio de los firewall, se puede realizar control de acceso, creando políticas que permitan el acceso de o negación a servidores. Adicional permite mejorar el control de la seguridad ya que se puede centralizar la información, esto debido a que toda la información está obligada a pasar por el firewall (como ya se había mencionado anteriormente).

Beneficios de un Firewall

Los firewall pueden administrar los accesos posibles de internet a la red privada, esto quiere decir que evita que cualquiera pueda acceder a los servidores u otros equipos de red detrás del firewall. Es decir que la red privada y su seguridad depende de lo exigente que pueda ser las restricciones que puedan existir por parte del Firewall.

El firewall puede realizar monitoreo en la red o en las mediaciones y si aparece alguna actividad sospechosa, este generara una alarma ante la posibilidad de que ocurra un ataque, o suceda algún problema en el tránsito de los datos.

- Concentra la seguridad Centraliza los accesos.
- Genera alarmas de seguridad.
- Traduce direcciones (NAT).
- Monitorea y registra el uso de Servicios de WWW y FTP.
- Internet.

Adicionalmente:

- Puede prevenir la exposición de hosts y aplicaciones sensibles a usuarios no confiables.
- Puede sanitizar el flujo de protocolos, previniendo la explotación de fallas en los protocolos.
- Puede bloquearse el acceso de datos maliciosos a servidores y clientes.
- Puede hacer que la aplicación de la política de seguridad se torne simple, escalable y robusta.
- Puede reducir la complejidad de la administración de la seguridad de la red al reducir la mayoría del control de acceso a la red a algunos puntos.

Firewall como traductor de NAT (*Network Address Translator*)

Actualmente existe un fuerte riesgo de disminución de asignamiento de direcciones

IP (en IPv4), lo que significa que ahora es más escaso la asignación de redes públicas, estas asignaciones son realizadas por las empresas de servicios de telecomunicaciones debido a esto hoy no es posible obtener suficientes registros de direcciones IP para responder a la población de usuarios en demanda de los servicios. Es en esta instancia, donde un es muy útil también ya que tiene la opción de utilizar un Traductor de Direcciones de Red (NAT – *Network Address Translator*) esto permite, hacer que los ordenadores /servidores/ otros equipos de red que utilizan un rango de direcciones privadas se conecten a Internet usando una **única dirección IP pública.** Gracias a esto sólo se utilizan una dirección IP y no tantas como máquinas existieran, esto garantiza un gran ahorro de direcciones IP.

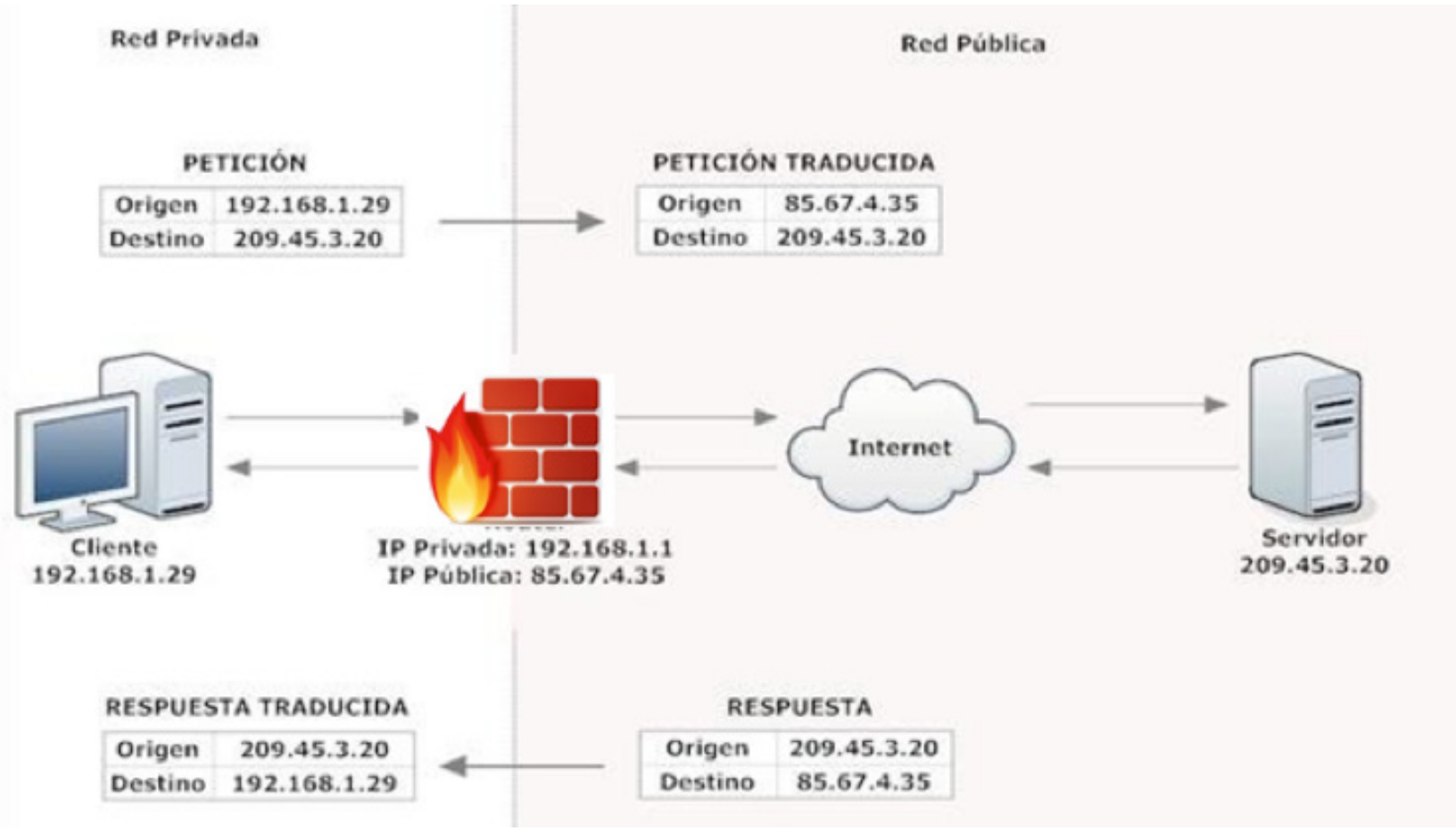


Imagen 2. Ejemplo de solución de NAT
Fuente: http://www.xatakaon.com/tecnologia-de-redes/nat-network-address-translation-que-es-y-como-funciona

Este es un problema que sólo se presenta con IPv4, pero con la implementación de IPv6, esta necesidad de NAT, ya no se vería como un tema de ahorro de direccionamiento, sino un tema de ahorro de recursos y dinero, ya que tener acceso a una red pública tiene un costo elevado y más si es a nivel corporativo. Pero la profundidad de este tema está fuera del alcance de este curso.

Limitaciones de un Firewall

Los Firewall no están en la capacidad de proteger la red, contra ataques que se encuentren fuera de su filtro. Por ejemplo, viendo la siguiente figura:

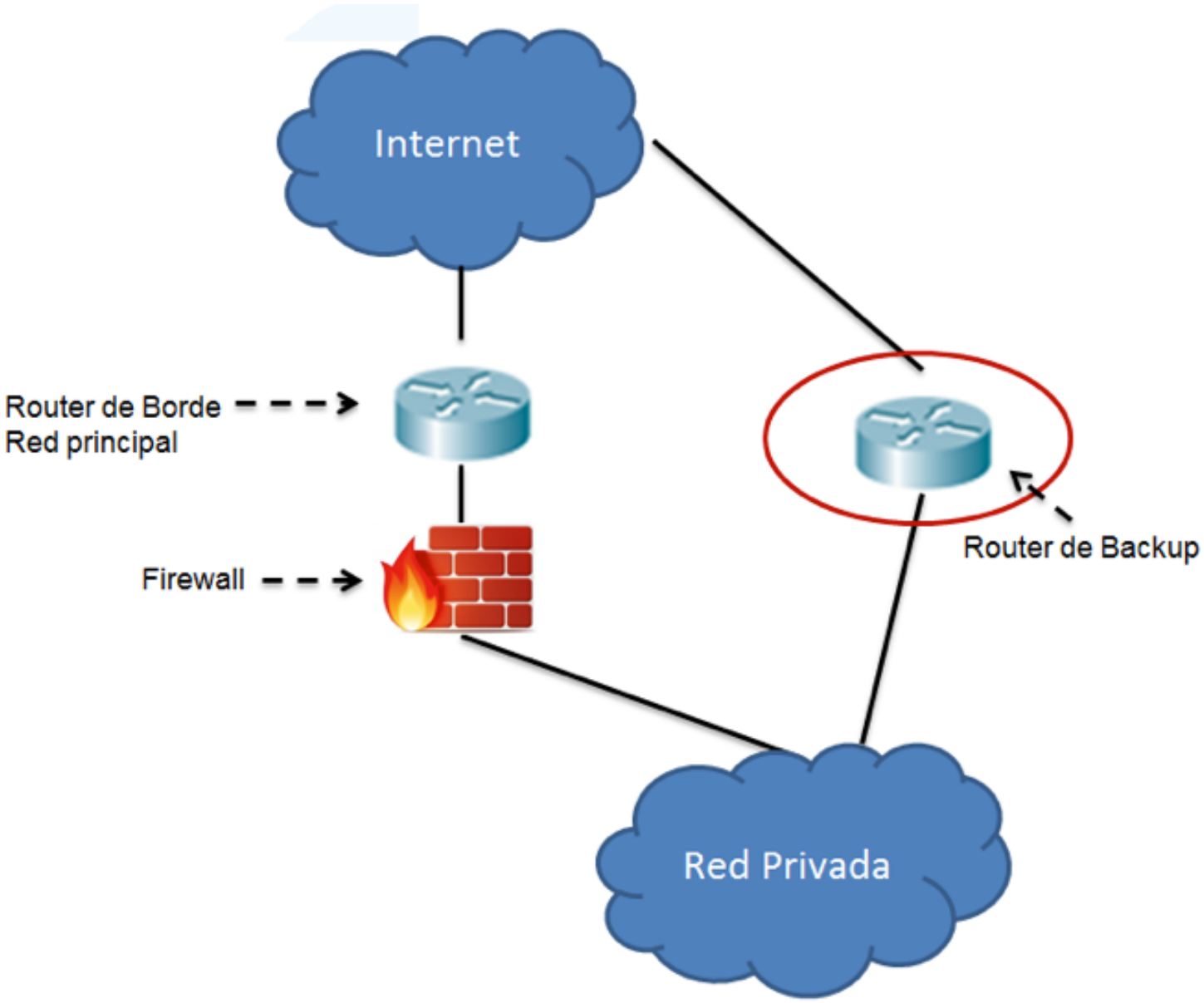


Imagen 3. Canal de Back up sin protección de Firewall
Fuente: Propia.

Parece increíble, pero hoy en día, muchos administradores de red siguen cometiendo errores como el mostrado en la figura 3. Donde se muestra que la red principal si tiene su firewall, pero por alguna razón el canal de backup no pasa por el firewall, esto es una gran brecha de seguridad que puede poner fácilmente en riesgo la seguridad de la red corporativa. Para este tipo de casos, el Firewall no puede hacer nada con los ataques que intenten realizarse por el canal de Backup.

- Si un firewall está mal configurado, se pueden presentar consecuencias serias (único punto de falla), donde muchos servicios no podrán ser habilitados, y donde el tráfico que debería permitirse entrar y/o salir no podrá circular. O en el peor de los casos, un firewall mal configurado será más bien una ventana abierta para que cualquier tráfico entre a la red privada.
- Muchas aplicaciones no pueden pasar a través del firewall en forma segura.
- Los usuarios con ciertos privilegios en la red, pueden intentar buscar maneras de sortear el firewall para recibir material bloqueado, exponiendo la red a potenciales ataques.
- El rendimiento de la red puede disminuir. Debido a que todo el tráfico pasa por un solo equipo, esto hace que la memoria o la CPU se sature y vuelva lenta la red, por esa razón, es necesario que a medida que crece una red, se realice la actualización o cambio de equipos de Firewall por equipos más robustos, que estén en la capacidad de soportar todo el tráfico que pasará por ellos. Estos cambios también implicarían costos altos, ya que no son equipos baratos y de fácil adquisición.
- Puede engañarse al firewall y hacerse tunneling de tráfico no autorizado o puede disfrazárselo como tráfico legítimo.

Tipos de Firewall

Para no extenderse entre la amplia gama de firewall existentes, estos se han clasificado en dos grupos:

- **Nivel de Red:** toman las decisiones de operación en función las direcciones de origen, destino y el port en cada paquete IP. Los firewall de este tipo son muy rápidos y no presentan problemas de "pico de botella" con el tráfico que circula por ellos.

  Estos equipos realizan una decisión de "pasa, no pasa" para cada paquete que recibe. El router examina cada datagrama para determinar si se aplican sus reglas de filtrado. Las reglas de filtrado se basan en la información contenida en el header del paquete. Esta información consiste en la dirección IP de origen, la IP de destino, el protocolo encapsulado (TCP, UDP, ICMP), el port TCP/UDP de origen y de destino, etc. Toda esta información es controlada contra las reglas de filtrado definidas, pudiendo ser enrutada si existe una regla que lo permite, descartada si una regla así lo indica y si no existe regla comparable un parámetro previamente configurado determinará si el paquete pasa o no.
- **Nivel de aplicación:** corren proxy servers, los cuales evitan el tráfico directo entre redes, realizando una exhausta auditoría del tráfico que pasa a través de él. Estos tipos de Firewall tienen la capacidad de trabajar tareas de creación de NAT, ya que pueden enmascarar la ubicación original (la de la red privada).

En estos firewalls se instala un software específico para cada aplicación a controlar (un proxy server); de hecho si no se instala los servicios relativos a la aplicación, las comunicaciones no podrán ser enrutadas.

Otra ventaja que trae el uso de este tipo de firewall es que permite el filtrado de protocolos, por ejemplo se podría configurar el proxy server que atiende el FTP para que pueda aceptar conexiones pero denegar el uso del comando put asegurando de esta forma que no nos puedan escribir ningún archivo.

Firewalls como parte fundamental del diseño de redes

En muchas ocasiones se requiere crear una zona delimitada o conocida como DMZ, la cual es parte de la red que se conecta directamente al firewall pero que tiene un acceso menos restringido desde Internet.

Con una DMZ, es común permitir tipos específicos de tráfico desde fuera, siempre que sea el tipo de tráfico correcto y que su destino sea la DMZ. Este tipo de tráfico generalmente es correo electrónico, DNS, HTTP o HTTPS.

Veamos un ejemplo gráfico de una correcta configuración de una red, con un DMZ configurado:

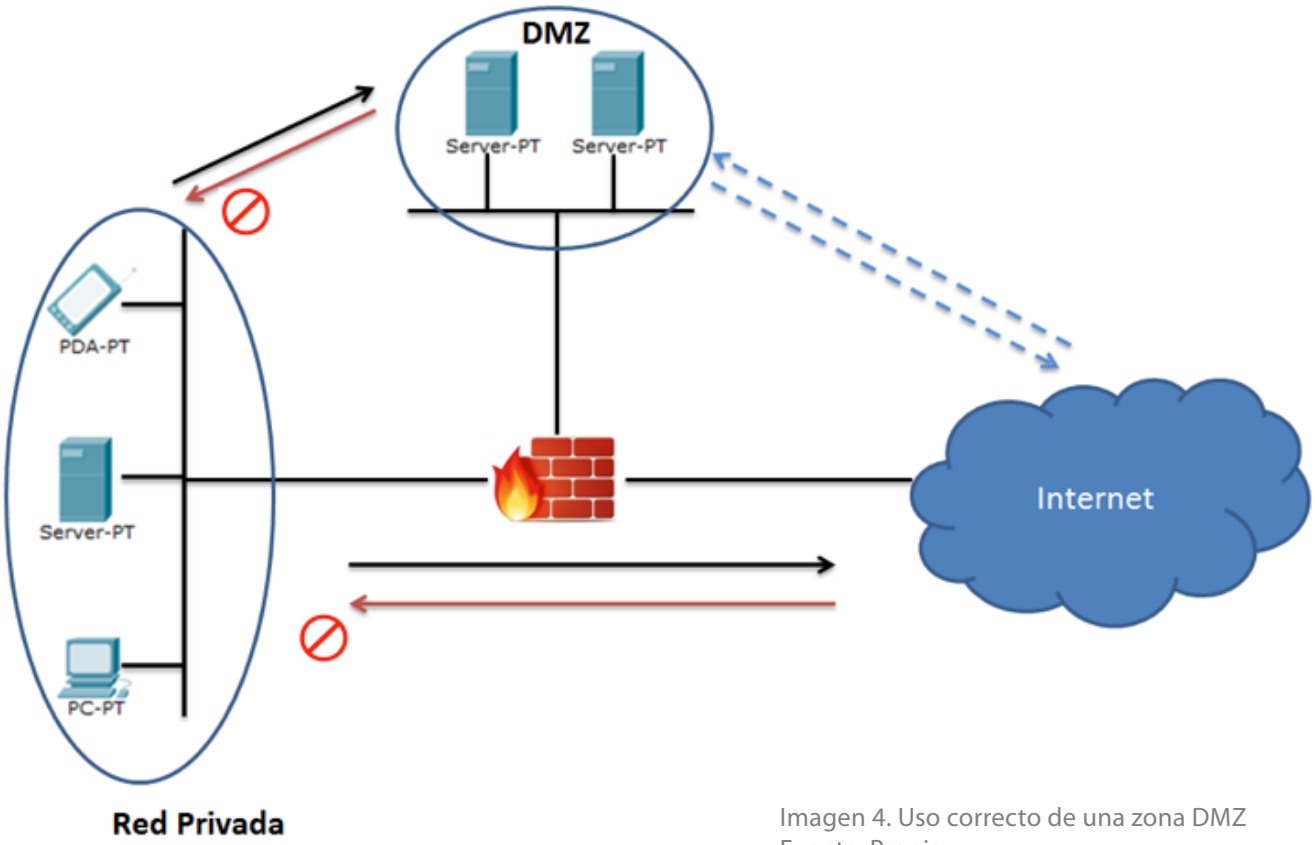


Imagen 4. Uso correcto de una zona DMZ
Fuente: Propia.

La configuración que se ve en la imagen 4, es la ideal si se quiere implementar una DMZ, el ideal es que todo el tráfico que sale de la Red Privada, pueda llegar sin ningún problema a Internet, pero, el tráfico que llega desde internet hacia la red privada tiene algunas restricciones, donde sólo puede acceder a la DMZ, pero no puede pasar de ahí a la red privada.

Implementación de la prevención de la intrusión

Los retos existentes a nivel de seguridad, son actualmente muy trabajados por las tecnologías de Firewall y por los controles de acceso estilo AAA. Pero estos sistemas dejas de ser útiles un ataque logra ingresar a la red o un virus comienza a atacar internamente la red. Por lo tanto se requiere de otras implementaciones que sean eficientes y prevengan y detengan intrusiones, como lo son IDS (Sistema de Detección de Intrusiones) e IPS (sistema de Prevención de Intrusiones).

Características de IDS

IDS (*Intrusion Detection System*), fue implementado con el fin de monitorear el tráfico de red de manera pasiva. IDS en lugar de reenviar los paquetes originales, los copia y los analiza. Realiza comparaciones entre las firmas maliciosas y el tráfico capturado, todo esto en modo offline.

Este modo de trabajo, tiene la ventaja de no afectar el flujo real de los paquetes que se mueven en la red, pero sí tiene la desventaja que no puede evitar que el tráfico malicioso realice ataques de un solo paquete, logrando afectar su objetivo antes que IDS pueda realizar una respuesta para detener el ataque, además siempre necesitará de otros elementos de red como firewalls o routers para responder el ataque.

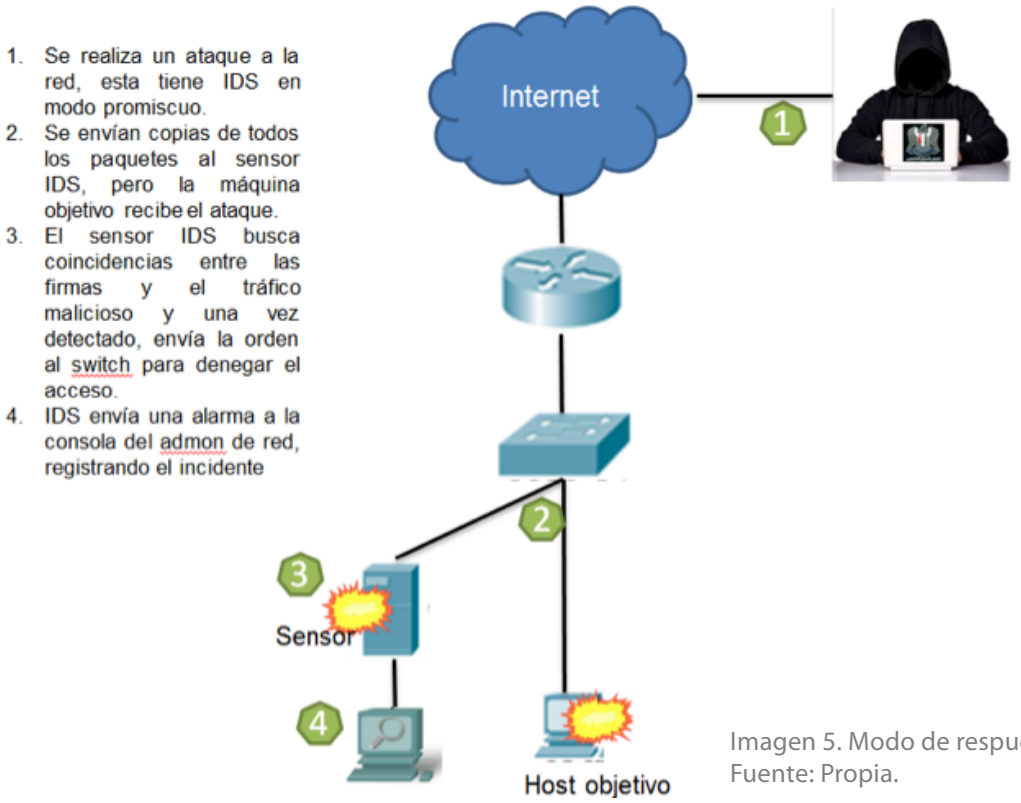


Imagen 5. Modo de respuesta IDS
Fuente: Propia.

Ventajas y desventajas de IDS

Algunas de las ventajas son:

- Se despliega en modo promiscuo.
- Como el sensor IDS no está en línea, no tiene impacto en el desempeño de la red.
- No introduce latencia o problemas de flujo de tráfico.
- Si un sensor falla, no afecta el desempeño de la red: solo afecta la capacidad del IDS de analizar los datos.

Las desventajas de:

- Al desplegar una plataforma IDS en modo promiscuo Las acciones de respuesta del sensor IDS no pueden detener el paquete atacante y no garantizan la detención de una conexión.
- Son menos útiles en la detención de virus de correo electrónico y ataques automatizados como gusanos, debido a la rapidez con la que estos ataques pueden viajar y dividirse en la red.
- Los usuarios administradores deben dedicar tiempo al ajuste de los sensores IDS para lograr los niveles esperados de detección de intrusiones.
- Finalmente, como los sensores IDS no operan en línea, la implementación IDS es más vulnerable a las técnicas de evasión usadas por varias amenazas.

Características de IPS

IPS (*Intrusion Prevention* System – Sistema de prevención de intrusión) realiza un apoyo a la tecnología IDS. IPS trabaja online, lo que implica que todo el tráfico de entrada y salida debe pasar a través de el para ser procesado, esto es realmente importante, ya que para que el tráfico pueda continuar su rumbo, deben ser analizados primero. Esto implica que puede detectar inmediatamente intentos de ataques o problemas que se presenten en la red.

La ventaja de operar en modo en línea es que el IPS puede evitar que los ataques de un solo paquete alcancen su objetivo. La desventaja es que un IPS mal configurado o una solución IPS inapropiada pueden tener efectos negativos en el flujo de paquetes del tráfico reenviado, ya que se pueden perder datos o puede ocasionar lentitud en la red.

Las tecnologías IDS e IPS usan firmas[1] para detectar patrones de mal uso en el tráfico de la red. Las firmas son usadas para detectar brechas de seguridad severas, ataques de red comunes y recolección de información.

[1] Una firma es un grupo de reglas que usa el IDS o IPS para detectar actividad típica de intrusiones

1. Se realiza un ataque a la red, esta tiene IPS y trabaja en línea
2. El sensor IPS analiza los paquetes que llegan a él y realiza el análisis del tráfico malicioso y las firmas, de esta manera detecta el ataque y lo detiene.
3. El sensor IPS envía una alarma a la consola de administración para tener un registro del evento
4. El sensor IPS descarta el tráfico malicioso

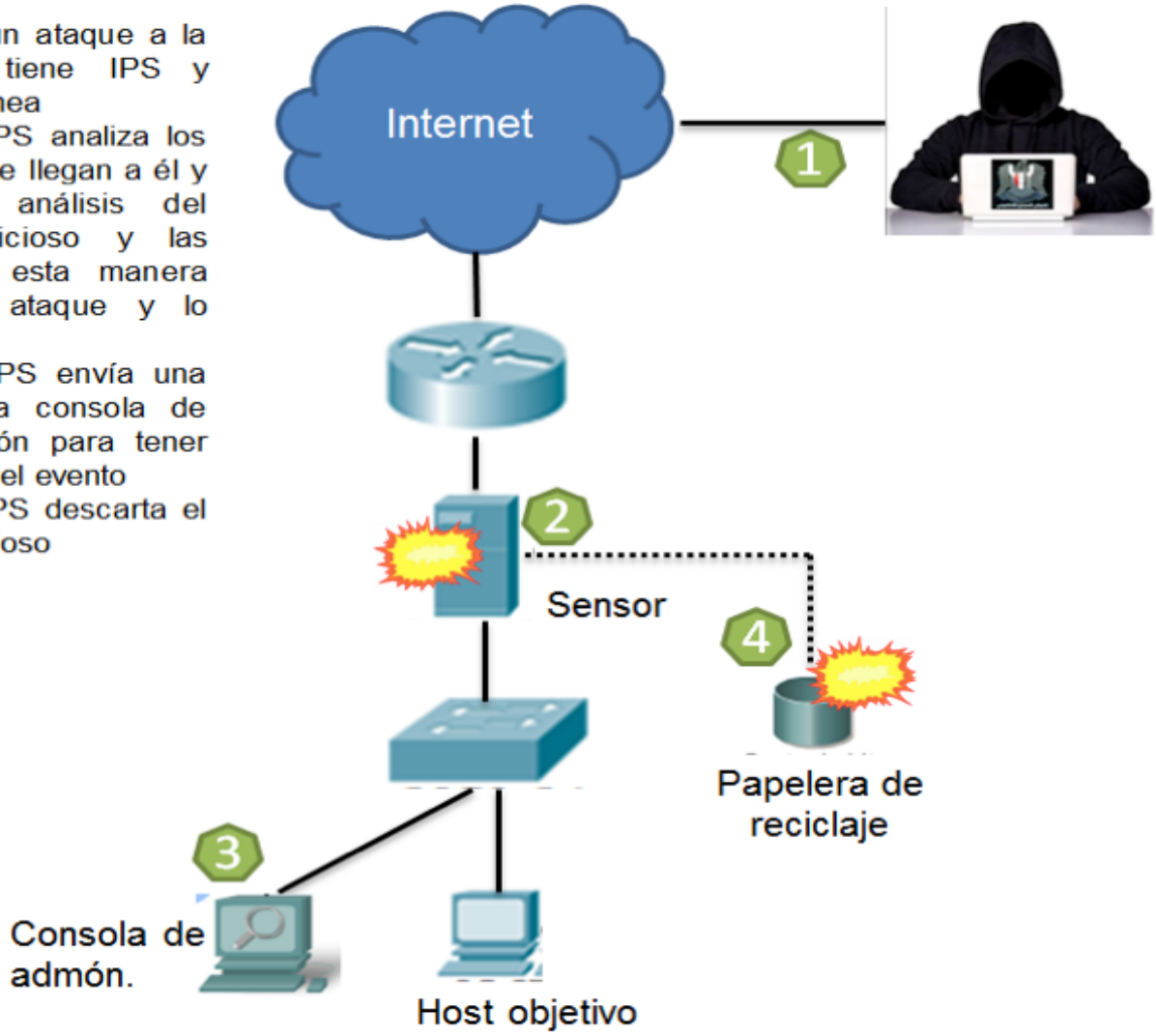


Imagen 6. Modo de respuesta IPS
Fuente: Propia

Ventajas y desventajas de IPS

Las ventajas de IPS son:

- Se puede configurar un sensor IPS para realizar un descarte de paquetes que puede detener el paquete disparador, los paquetes de una conexión o los paquetes originados en una dirección IP determinada.
- Al estar en línea, el sensor IPS puede usar técnicas de normalización del flujo para reducir o eliminar muchas de las capacidades de evasión existentes.

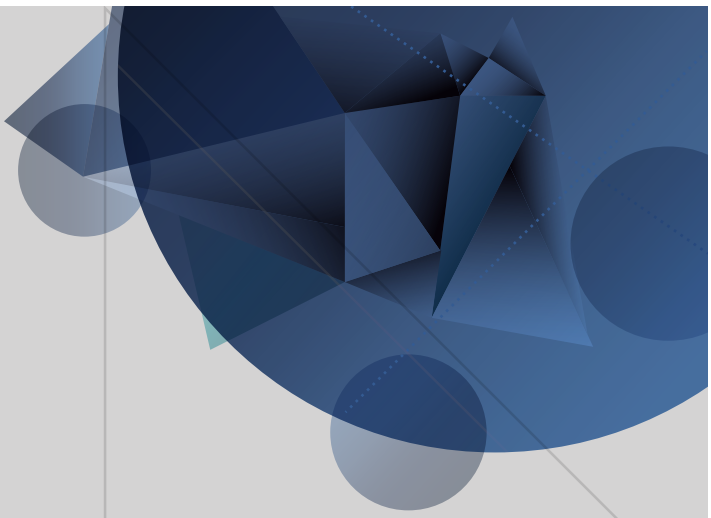
Las desventajas de IPS son:

- Los errores, la falla y la sobrecarga del IPS con demasiado tráfico pueden tener efectos negativos en el desempeño de la red. Esto ocurre porque el IPS debe ser desplegado en línea y el tráfico debe poder pasar a través de él.
- Un sensor IPS puede afectar el rendimiento de la red introduciendo latencia y jitter. Por lo tanto, el sensor IPS debe ser de tamaño e implementación apropiados para que las aplicaciones sensibles al tiempo, no sufran efectos negativos.

4

Unidad 4

Gestionar una red segura



Seguridad en redes

Autor: Esteban Bejarano Forero

AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO

Introducción

Para finalizar este módulo de seguridad en la red, se retomará un poco el tema de políticas de seguridad informática, pero esta vez enfocada en soluciones que se encuentran en el mercado actualmente. Se revisará los procesos por los que debe pasar una política de seguridad para poder tener una continuidad a pesar del paso del tiempo, claro está, modificando parámetros, lineamientos, ajustándose a las variantes, etc.

U4 Metodología

Esta última unidad vuelve un poco al tema de políticas de seguridad, así que es recomendable que se haga un pequeño repaso a esa unidad.

Gestionar una red segura

Un sistema de seguridad en la red nunca podrá evitaren su totalidad que los activos sean vulnerables a amenazas, esto debido a que a medida que crecen los sistemas de seguridad o protección de la red, también se desarrollan nuevos ataques y se identifican vulnerabilidades que pueden ser usadas para violar soluciones de seguridad. Además, los sistemas de seguridad pueden ser vencidos si la comunidad de usuarios finales no sigue las prácticas y procedimientos de seguridad.

Debe mantenerse una política de seguridad redundante que identifique los activos de la empresa, especifique los requisitos de hardware y software para la protección de esos activos, clarifique los roles y responsabilidades del personal y establezca el procedimiento hierático apropiado para responder a brechas de seguridad. Al instituir y seguir políticas de seguridad, las empresas pueden disminuir las pérdidas y daños que resultan de ataques a su red.

Ciclo de vida de una red segura

El ciclo de vida de red segura es un proceso de revisión y reevaluación de las necesidades de seguridad y de equipamiento a medida que la red cambia. Uno de los aspectos importantes de esta evaluación constante es entender cuáles activos de la organización deben ser protegidos, incluso mientras que los activos cambian.

Un ciclo de vida de una red segura se basa en el estándar SDLC (*System Development Life Circle*), está constituido por 5 fases:

Inicio

Requiere definir tres niveles de impacto (bajo, medio, alto) debido a brechas de seguridad, estos niveles ayudan a realizar la correcta elección de controles de seguridad que correspondan a los sistemas de información.

Adicional describe inicialmente las necesidades de seguridad básicas del sistema que define el ambiente de amenazas en el que éste se desenvuelve.

Adquisición y desarrollo

Tiene a su cargo varias tareas de seguridad:

- **Evaluación de riesgos:** identificar los requisitos de protección del sistema a través de un proceso formal de evaluación de riesgos. Basado en la evaluación de riesgos que se realiza en la primera etapa (inicio).
- **Requisitos funcionales de seguridad:** realizar el análisis de las principales necesidades operativas al relacionarse la política de seguridad de la información de

la empresa, el ambiente de seguridad del sistema y la arquitectura de seguridad de la empresa.

- **Requisitos de garantía de seguridad:** tratar las actividades de desarrollo requeridas y la evidencia de garantía necesaria para producir el nivel deseado de confianza en que la seguridad de la información.
- **Consideración y reporte de costos de seguridad:** establecer qué parte del costo de desarrollo debe reservar a la seguridad de la información en el ciclo de vida del sistema. Estos costos incluyen hardware, software, personal y capacitación.
- **Planeamiento de seguridad:** describe con detalle los sistemas de información e incluye adjuntos o referencias a documentos claves que soportan el programa de seguridad de la información de la organización. Los documentos que soportan el programa de seguridad de la información incluyen plan de contingencias, un plan de administración de configuración, evaluación de riesgos, plan de respuesta a incidentes, plan de capacitación en seguridad, pruebas de seguridad y resultados de evaluaciones, reglas de comportamiento, acuerdos de interconexión de sistemas, autorizaciones y acreditaciones de seguridad y un plan de acción e hitos.
- **Desarrollo de un control de seguridad:** busca asegurar que los controles de seguridad descriptos en los planes de seguridad sean diseñados, desarrollados e implementados.
- **Prueba y evaluación de seguridad del desarrollo:** aseguramiento de los controles de seguridad desarrollados para un nuevo sistema de información con el fin de detectar que estén trabajando correcta y efectivamente.

Implementación

Las tareas de seguridad en esta fase son:

- **Inspección y aceptación:** aprobar y confirmar que la funcionalidad definida por la especificación esté contenida en las prestaciones.
- **Integración del sistema:** certificar de que el sistema esté compuesto en el sitio operativo donde se despliega el sistema de información.
- **Certificación de seguridad:** usar técnicas e instrucciones de revisión establecidos. Este paso otorga familiaridad a los empleados de la organización de que se están tomando las moderaciones y contramedidas adecuadas. La certificación de seguridad también revela y detalla las debilidades conocidas del sistema de información.
- **Acreditación de seguridad:** suministrar la credencial de seguridad necesaria para resolver, recopilar y transmitir la información solicitada. Esta credencial es otorgada por un empleado superior de la organización y está establecida en la confianza confirmada de los controles de seguridad a un nivel establecido de garantía.

Operaciones y mantenimiento

Las tareas de seguridad en la fase de operaciones y mantenimiento son:

- **Administración y control de la configuración:** considerar los potenciales impactos de seguridad que pueden ser causados por cambios definidos a un sistema de información o su contexto. Las instrucciones de gestión y control de la

configuración son críticos para implantar un punto de partida de mecanismos de hardware, software y firmware y luego controlar y mantener una descripción precisa de los cambios al sistema.

- **Monitoreo continuo:** certificar de que los controles continúen siendo seguros por medio de pruebas periódicas. Informar el estado de seguridad del sistema de información a los empleados correspondientes es una actividad fundamental en un programa de seguridad de la información.

Descarte

Las tareas de seguridad en la fase de descarte son:

- **Preservación de la información:** detener la información según sea requerido para cumplir con las obligaciones legales y hacer lugar a futuros cambios tecnológicos que pueden volver obsoleto al método de desempeño.
- **Saneamiento de los medios:** certificar de que los datos sean eliminados y sobreescritos según sea necesario.
- **Descarte de hardware y software:** retirar el hardware y el software según las órdenes del empleado de seguridad del sistema de información.

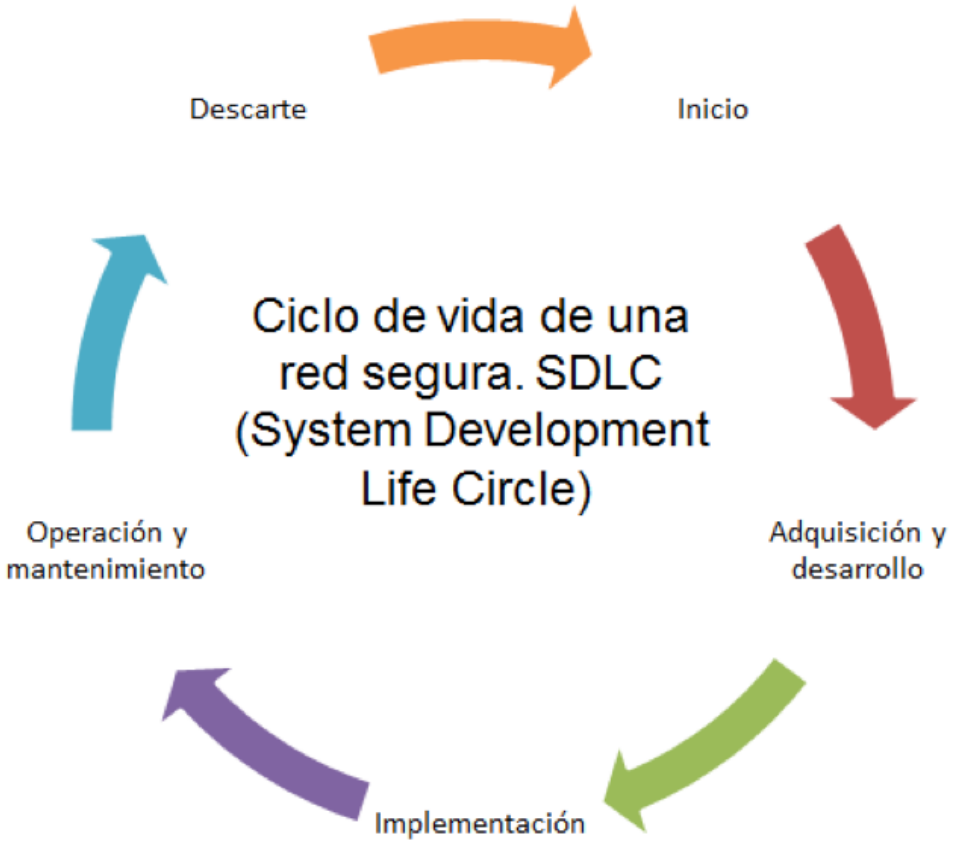


Imagen 1. SDLC, ciclo de vida de una red segura
Fuente: Propia.

Red de Autodefensa

Cisco, ofrece esta solución para prevenir, identificar y adaptarse a las amenazas, donde su enfoque en la red está bajo los lineamientos y exigencias actuales, permitiendo que el acoplamiento a nuevas amenazas sea más sencillo.

Para lograr esto, la red de Autodefensa sigue tres principios:

- **Integración:** toda la infraestructura de red, debe estar asegurada en su totalidad.
- **Colaboración:** los servicios de red, deben obligatoriamente trabajar en conjunto con los esquemas de seguridad y así fortalecer cada área.
- **Adaptación:** la red debe cambiar (para mejorar) a medida que crecen las necesidades de la red y las amenazas posibles.

Adicional, esta plataforma ofrece algunos servicios que permiten que la plataforma se mantenga Fuerte, segura y flexible:

- **Control de amenazas:** unifica a los servicios y dispositivos que hagan limitar la posibilidad de amenazas y que estas se expandan a toda la red.
- **Comunicaciones seguras:** unifica a los servicios y dispositivos que aseguren la privacidad de toda clase de comunicaciones que puedan ser vulnerables a ataques.
- **Control operativo y administración de políticas:** conjunto de herramientas que componen un framework para una gestión y aplicación de las políticas escalables que amplíe la seguridad de extremo a extremo.

Imagen 2. Definición de red
Fuente: https://www.cisco.com/web/ES/publicaciones/07-08-cisco-red-autodefensa-elementos-estrategicos.pdf

El enfoque de la Red Autodefensiva incluye las siguientes herramientas para proporcionar servicios de seguridad:

- El Administrador de Seguridad de Cisco proporciona gestión de políticas.
- El Sistema de Respuesta, Análisis y Monitoreo de Seguridad de Cisco (MARS) proporciona gestión de amenazas.
- El software IOS de Cisco, las Cisco Adaptive Security Appliances y el Software Cisco para Sensores de Sistemas de Prevención de Intrusiones proporcionan seguridad a las redes.
- Los dispositivos NAC de Cisco y el Agente de Seguridad de Cisco proporcionan seguridad de punto final.

Existen varios beneficios adicionales que resultan de este enfoque englobador y exhaustivo:

Visibilidad y protección de 360 grados: defensa comprensiva y proactiva de la red. Los datos de amenazas de toda la infraestructura se transmiten eficientemente en una amplia variedad de sistemas y dispositivos. La identificación de amenazas multivector captura violaciones a las políticas, explotaciones de vulnerabilidades y comportamientos extraños.

Control simplificado: activa la gestión de políticas en toda la red y la ejecución de las políticas en toda la infraestructura en una extensa variedad de sistemas y dispositivos.

Resistencia de los negocios: asegura los procedimientos de la empresa. La asistencia y similitud en varios sistemas, estaciones de trabajo y administración permite respuestas adaptadas a las amenazas en tiempo real.

Construcción de una política integral de seguridad

Como base principal para construir una política de seguridad, se debe entender que lo que más se quiere proteger, son los activos de la empresa, ya partiendo de este punto, se debe evaluar qué se puede considerar como ese activo tan valioso que se quiere proteger.

Es claro que toda la normatividad debe quedar plasmada en un documento, y este documento debe contener toda la información clara, organizada y específica, donde se les informe a los usuarios, personal y/o administradores los requisitos que se están exigiendo con respecto al uso adecuado que deben tener con los recursos tecnológicos y los activos de información.

Ya teniendo claro lo anterior, veamos rápidamente la forma como se podría construir una política integral de seguridad:

Manejo de la jerarquía de las políticas

Se debe tener presente que no toda la política de seguridad es la misma para todos los usuarios o áreas de trabajo, es por ello que se requiere realizar distinción dependiendo el área donde se encuentre el usuario, por tal motivo se presentan tres grupos que a grandes rasgos pueden representar una estructura jerárquica:

Política gobernante: describe los objetivos de seguridad para los administradores y personal técnico, abarca los temas de seguridad entre las unidades de negocios y los diferentes departamentos de la compañía.

Las políticas gobernantes incluyen varios componentes:

- Declaración del tema que la política trata.

- Cómo se aplica la política al ambiente.
- Roles y responsabilidades de los afectados por la política.
- Acciones, actividades y procesos permitidos y prohibidos.
- Consecuencias del incumplimiento.

Política técnica: indica las responsabilidades por parte del personal técnico con el fin que ellos también cumplan sus responsabilidades con respecto a la seguridad. En esencia, son manuales de seguridad que describen lo que el personal técnico debe hacer, pero no cómo los individuos realizan sus funciones.

Política de usuario final: esta política trabaja con toda la normatividad que debe conocer y obedecer los usuarios finales. Muchos grupos destino diferentes requieren políticas de usuario final, y cada grupo puede tener que aceptar una política de usuario diferente. Por ejemplo, la política de usuario final de los empleados puede ser diferente de la de los clientes.

Estándares, guías y procedimientos

Las políticas se deben manifestar en documentos. Los documentos estándares, guías y procedimientos son los que contienen los detalles de lo definido en las políticas.

Documentos estándar: permiten al personal informático a mantener estabilidad en las operaciones de la red. Incluyen las tecnologías necesarias para usos específicos, las exigencias de versión de hardware y software, exigencias de programas y cualquier otro criterio que debe seguirse en la organización. Esto ayuda al personal informático a mejorar la validez y la claridad en el diseño, el mantenimiento y la resolución de problemas.

Documentos guía: facilitan listas de propuestas sobre cómo mejorar las cosas. Son parecidas a los estándares pero más flexibles y no tan obligatorias. Las guías pueden ser usadas para definir cómo se desarrollan los estándares y para garantizar adherencia a las políticas de seguridad en general.

Algunas de las guías más útiles, que pueden ser halladas en los repositorios de las organizaciones, son denominadas buenas prácticas.

Documentos de procedimientos: estos documentos tienden a ser más largos y detallados que los estándares y las guías. Los documentos de procedimientos incluyen detalles de ejecución, generalmente instrucciones y gráficos paso a paso. Los documentos de procedimientos son extremadamente importantes en organizaciones grandes para proporcionar la estabilidad de despliegue necesaria en un ambiente seguro.

Roles y responsabilidades

Todas las personas que forman parte de una organización, desde el CEO (*Chief Executive Officer*) hasta los empleados más recientes, son consideradas usuarios finales de la red y deben estar reflejados en la política de seguridad de la organización. El desarrollo y mantenimiento de la política de seguridad se delega a roles específicos dentro del departamento de IT.

Es de gran relevancia indagar con los administradores de altos cargos los conceptos que se estén desarrollando en la política de

seguridad, con el fin que ellos evalúen si están siendo integra y legalmente vinculante.

Concientización y capacitación en seguridad

No es suficiente con crear un documento donde se divulgue todos los estándares de seguridad dentro de una organización, se requiere tener presente que todo el personal requiere ser capacitado y educado para los cambios que llegarán con la implementación de las nuevas políticas de seguridad. Esto es realmente importante hacerlo, ya que es muy probable que los usuarios no puedan volver a realizar ciertas actividades a las que ya estaban acostumbrados, o de lo contrario, que tengan que realizar actividades a las cuales nunca se imaginaron tendrían que cumplir.

Los programas de concientización en seguridad generalmente tienen dos componentes principales:

Campañas de concientización

Estos eventos por lo general están creados para todas las áreas de la organización, ya que buscan cambiar la forma como los usuarios solían comportarse y adicional se buscaría reforzar las buenas prácticas de seguridad.

Existen muchos métodos que pueden ayudar a realizar estas actividades, como por ejemplo Charlas, videos, envíos masivos de correos electrónicos con la información, creación de concursos donde se premie a los usuarios que mejor se desenvuelvan con la nueva normatividad, carteles, etc.

Capacitación y educación

La capacitación busca enseñar habilidades que le permitan al usuario realizar las tareas específicas. Las habilidades que adquieren los usuarios durante la capacitación, respaldan las campañas de concientización que se realicen dentro de la organización.

La educación integra todas las habilidades y competencias de seguridad de las especialidades funcionales a un "cuerpo" común de conocimientos, agrega un estudio multidisciplinario de conceptos, problemas y principios (tecnológicos y sociales) y busca producir especialistas y profesionales de la seguridad informática capaces de visión y respuesta proactiva.

Leyes y ética

En muchas de las empresas en la actualidad, una de las consideraciones más importantes en el establecimiento de políticas de seguridad y la implementación de programas de concientización es el cumplimiento de la ley. Los profesionales de la seguridad en redes deben estar familiarizados con las leyes y los códigos de ética que son vinculantes para los profesionales de la seguridad de los sistemas de información. La mayoría de los países tienen tres tipos de leyes: criminales, civiles y administrativas.

Leyes

Las leyes criminales están relacionadas con los crímenes y sus penas generalmente involucran multas o prisión, o ambas.

No todos los gobiernos aceptan o clasifican sus leyes de la misma manera. Esto puede impedir llevar a juicio a los criminales de computadoras o redes que crucen fronteras internacionales.

Ética

La ética es un estándar que rige por sobre la ley. Es un grupo de principios morales

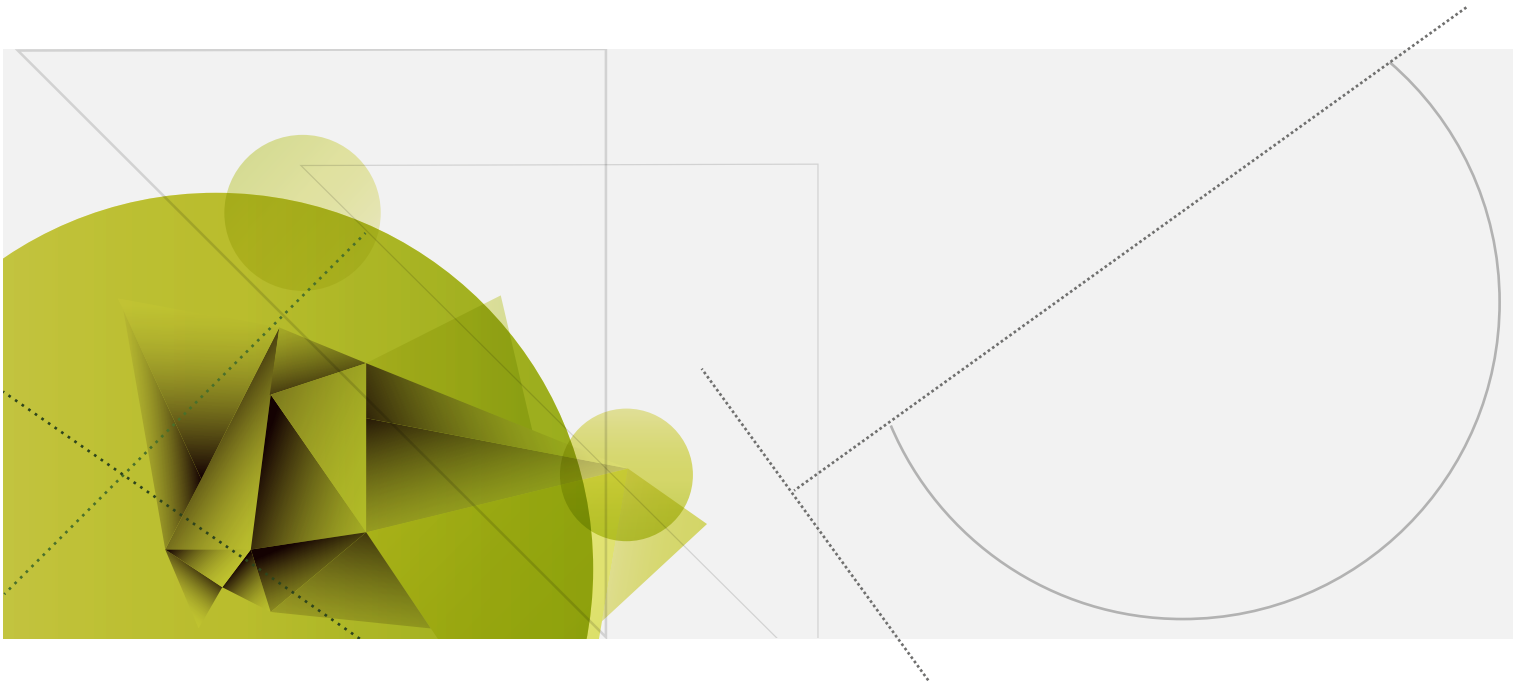
que gobiernan el comportamiento civil. Los principios éticos generalmente son la base de muchas de las leyes que están actualmente vigentes. Estos principios generalmente se formalizan en códigos de ética. Los individuos que violen los códigos de ética pueden enfrentar consecuencias como pérdidas de certificaciones, pérdida de su empleo o incluso juicios en cortes criminales o civiles.

A medida que las normas sociales para el uso de sistemas informáticos evolucionen, el Código de Conducta Ética cambiará y los profesionales de seguridad de la información esparcirán los nuevos conceptos en sus organizaciones y productos. Las precauciones pueden requerir un juicio ético para el uso o la determinación de los límites o controles.

Bibliografia

- Carling, M. & Degler, S. (2000). Administración de Sistemas Linux. Guía Avanzada.
- Guttman, B. & Bagwill, R. (1997). Internet Security Policy: A Technical Guide.
- Harrington, J. (2006). Manual práctico de seguridad de redes. Madrid, España: Anaya Interactiva.
- Katz, M. (2013). Redes y seguridad. Buenos Aires, Argentina: Alfaomega.
- McClure, S. & Scambray, J. (2002). Hacking Expose, Network Security Secres & Solutions. Tercera Edición. Osborne/McGraw-Hill.
- Stallings, W. (2004). Fundamentos de seguridad en redes: aplicaciones y estándares. Madrid, España: Pearson Educación S.A.
- Siyan, K. & Hare, C. (1997). Firewalls y la seguridad en Internet. Segunda Edición, Prentice-Hall Hiberoamericana, S.A.
- Vladimirov, A., Gavrilenko, K. & Mikhailovsky, A. (2010). Hacking wireless: seguridad de redes inalámbricas. Madrid, España: Anaya.

Esta obra se terminó de editar en el mes de noviembre
Tipografá Myriad Pro 12 puntos
Bogotá D.C,-Colombia.



AREANDINA
Fundación Universitaria del Área Andina

MIEMBRO DE LA RED
ILUMNO