Herramientas de Seguridad

Transcribed on July 26, 2025 at 10:18 AM by Minutes AI

Speaker 1 (00:00)

En esta sesión vamos a ver una introducción a algunas de las herramientas más utilizadas para la securización de redes, como por ejemplo son las ACL o Access Control List, los sistemas de detección y también prevención de intrusos, los proxys SSH y también un poco sobre la seguridad centrada en las DNS.

Las listas de control de acceso nos permiten, utilizando una colección de diferentes reglas, filtrar el tráfico de red a nivel de paquetes utilizando como base un criter.

De esta forma podemos por ejemplo gestionar el flujo de tráfico de control, etc.

Para ello se basan en diferentes variables como el protocolo de red, las direcciones IP de origen y destino, el número de puerto, ya sea TCP o UDP, etc.

En general se dividen en dos las ACL standard que trabajan sobre la capa 3 OSI y las ACL extendidas que pueden trabajar en las capas 3 y 4 también del modelo OSI.

Así que bueno, podemos encontrar esta funcionalidad en gran variedad de dispositivos, pero sobre todo está siempre siempre esta herramienta de las ACL en routers y switches.

El ejemplo que podéis ver aquí en la diapositiva es una regla de ACL de Cisco que permite el tráfico de paquetes si detecta en la cabecera IP una red del tipo 192.

568.16 y que vaya a la red de destino 192.168.100 con la subnet 24.

El valor es el valor inverso de la máscara de red que es el 255255002550.

Bien, ahora vamos a hablar de los IDS y los ips, que son los sistemas de detección de intrusión y los sistemas de prevención de intrusiones, pero esto lo veremos más en profundidad más adelante con la herramienta Snort.

De todas formas aquí haremos una pequeña introducción a estos sistemas y para qué sirven.

Los IDS monitorizan las LED en busca de actividad sospechosa contenida dentro del tráfico de red, generando alertas en caso positivo de una detección.

Puede ser del tipo HIDS que es hostpace de tipo de software desplegada directamente sobre el equipo host que se está por ejemplo monitorizando, o también puede ser un NIDS que son los network base que utiliza el hardware de red para realizar una monitorización pasiva del tráfico de red.

Para poder hacer esta operación normalmente hay que activar un puerto que pueda funcionar en modo que se llama mirror, espejo o promiscuo.

Este modo promiscuo es una característica que permite capturar todo el tráfico que circula a través de ese puerto.

Esto es fundamental para los clásicos sniffers de red, por ejemplo.

En cambio En cambio, Por otro lado, los ips examinan el tráfico de ander para detectar y prevenir posibles ataques contra la infraestructura.

Suelen estar ubicados justo detrás del cortafuegos, apoyándole como una capa más de seguridad, realizando acciones como por ejemplo enviar alertas, bloquear tráfico, rechazar paquetes, etc.

De forma habitual utilizan dos tipos de detección, los basados en firmas, que examinan patrones o firmas de determinados tipos de exploit o malware, y los basados en detección de anomalías, donde comparan el tráfico actual con patrones predefinidos de funcionamiento.

Otro elemento clave dentro del hardening de una red de datos es el proxy server o servidor proxy.

Básicamente es un gateway o una pasarela, que incluso puede ser un software o un hardware, una electrónica, y este se encarga de hacer el intercambio o hacer de intermediario entre las peticiones de acceso a diferentes recursos de la red, como pueden ser por ejemplo páginas web.

El tipo de proxy más importante o más utilizado en la seguridad es el proxy inverso.

Este tipo de proxy hace de canalizador de todo tipo de peticiones en las cuales aparecerá el mismo como origen, es decir, nunca se va a exponer la dirección IP verdadera.

De esta forma los dispositivos clientes y su identidad aparecerán siempre seguras detrás del proxy impreso.

Por lo tanto, este tipo de soluciones permite no sólo el anonimato en las conexiones, sino que también mejoran el rendimiento, ya que pueden actuar como caché o un balanceador de carga.

De hecho, los servidores proxy también se pueden considerar como un tipo de firewall, y hoy día los dos proxy más conocidos son Nginx y Apache.

Acceder de forma remota tanto a los servidores como a los dispositivos de nuestra red es una tarea fundamental y muy cotidiana, la cual debe estar lo más securizada posible.

Y aquí es donde entra el Secure Shell o el SSH, que es un protocolo cliente servidor que permite diferentes métodos de autenticación.

También nos permite ejecutar comandos de forma remota, transferencia de ficheros con un protocolo que se llama SFTP, etc.

Pero su característica más importante es que ofrece un gran nivel de cifrado e integridad en la información.

Pues bien, ¿Cómo funciona?

Pues como antes he comentado, es un protocolo cliente servidor, lo que significa que el cliente conecta con un servidor SSH.

El cliente SSH comienza el proceso de comunicaciones realizando una petición de conexión con el servidor SSH.

Éste le envía su clave pública para confirmar la identidad y en este punto empieza a funcionar la máquina criptográfica SSH, donde se va a utilizar un cifrado de tipo simétrico, además de un hashing para conseguir la máxima seguridad en el tráfico de la información.

De esta forma, aunque algún posible atacante estuviera situado dentro de la misma red de comunicaciones, los datos que recibiría estarán totalmente cifrados.

Eso sí, aunque SSH es un protocolo quizás el más seguro para conectar nuestros dispositivos, también puede tener fallos de seguridad.

Por ejemplo hay un CVE que es el CVE-2000-19842, el cual muestra un fallo de seguridad de autenticación asociada al Cisco iOS.

Por este motivo hay que estar siempre al día sobre posibles fallos de seguridad asociados a a este servicio y a cualquiera en general.

En la arquitectura SSH podemos ver los siguientes El primero es un servidor que autentica y autoriza las posibles conexiones SSH.

Después tenemos el cliente, que es el que realiza la petición de conexión SSH.

Una vez establecido tenemos lo que se llama la sesión, que es justo la conexión entre el cliente y el servidor.

Después tenemos un key generator.

Este key generator lo que hace es crear las claves que se llaman keys, que se van a utilizar en la conexión.

Después tenemos un agent, que es un agente que básicamente es un programa para gestionar la caché y las claves.

Después tenemos el signer, que es el que se encarga de firmar la autenticación en vez de utilizar contraseñas.

También tenemos lo que se llama un random sheet, esto es una semilla aleatoria que se genera por SSH para conseguir un número pseudo aleatorio para conseguir un buen cifrado.

Y ya finalmente tenemos los diferentes ficheros de configuración, que es donde se ajustan los parámetros de ambas conexiones.

De esto haremos un ejercicio más adelante.

Una parte crítica de la configuración de cualquier dispositivo desde el punto de vista de la seguridad son los certificados en PFSEN.

Podemos encontrarnos aquí System Certificates y aquí vemos que aquí tengo yo uno creado que es para scuid, pero aquí podemos hacer todo tipo de operaciones con ellos.

Podemos crearlos, diferentes utilidades, generarlos, exportarlos, etc.

Pero ¿Por qué son importantes los certificados, tanto PFSense como en cualquier dispositivo?

Eso sí, a partir de ahora voy a ir hablando de PFSense, pero tenéis que imaginar que esto vale para cualquier aparato que tenga algún tipo de gestor, tanto web o desde la línea de comandos, porque todas estas configuraciones que vamos a ir viendo en PFSense son muy genéricas.

Casi todas las máquinas que están orientadas a la seguridad de red tienen algo parecido, muy similar, que solo cambiará un poco la forma de acceder a ellos, pero en general todos tendrán una configuración muy similar a esta.

Pues bien, los certificados son importantísimos tanto para PFSense como tal, como para cualquier máquina.

Lo primero por la seguridad de la comunicación, porque ya que estos se utilizan para cifrar la comunicación entre los dispositivos y el servidor, en este caso el pfsen.

Con esto garantizamos que la información que se transmite está protegida y además sobre todo no se puede interceptar o no se puede escuchar, eso es clave.

También es vital para, por ejemplo, la autenticación de servidores y clientes, porque estos certificados también se utilizan para autenticar tanto al servidor como a los clientes que intentan conectarse.

Esto nos ayuda también a garantizar que estos dispositivos que se conectan a PFSense o a lo que sea, son legítimos y son confiables También por otro lado, un poco más orientado a la interfaz web, los certificados SSL TLS se usan para proteger la interfaz web de la administración, en este caso en DPF Sense.

Esto también nos garantiza que la comunicación entre el navegador del usuario y el pfsense también esté cifrada, porque claro, ahí va a llevar todo el tráfico de configuración que si alguien lo intercepta con un ataque MAN indemnito, pues podría captar credenciales, configuraciones, etc.

También los certificados son clave en lo que es la VPN y la autenticación de los usuarios.

Por ejemplo, si usamos algún tipo de función de VPN en pfsen o donde sea, los certificados son cruciales en la autenticación de clientes VPN y también en el establecimiento de túneles seguros.

En PFSense podemos ver que tenemos tres opciones a la hora de hablar de certificados.

Tenemos la sección de autoridades.

En esta sección lo que hacemos es centrarnos en las autoridades de certificación, que son las famosas CA.

Una autoridad de certificación es una entidad confiable que emite y administra certificados digitales.

Entonces en pfsen lo podemos usar para crear nuestras propias autoridades de certificación, para emitir certificados SSL y TLS para los servicios de PFSEN como por ejemplo la interfaz de administración o incluso para autenticar clientes VPN.

Después tenemos la sección de certificados.

En esta sección lo que podemos es generar, ver, importar y administrar cualquier certificado digital en PFS.

También podemos generar certificados autofirmados que se llaman Self subnet para uso interno o importarlo como certificados emitidos por una autoridad de certificación externa.

También nos podemos conectar con alguien externo y estos certificados se pueden utilizar para autenticar la entidad de PFSEN en servicios como por ejemplo HTTPs, para la interfaz de administración como antes, autenticar clientes de VPN, etc.

Y por último tenemos la sección de revocación.

Aquí lo que hacemos es administrar la la revocación de los certificados que estamos emitiendo por las diferentes autoridades de certificación de PFSEN.

La revocación implica invalidar su uso antes de la fecha de vencimiento.

Ojo con esto, es importante tener un control muy drástico de los certificados, por ejemplo si sospechamos que la clave privada asociada a un certificado ha sido comprometida o si el certificado ya no es válido por lo que sea.

En esta sección podemos ver esas listas de revocación de certificaciones que se llama CRL, que además la generan las autoridades de certificación y de esa forma nos permitiría ver si un certificado ha sido o no revocado, ya sea de PFSEN o uno externo que tuviéramos asociado con nosotros.

Pues bien, esto es un punto de vista general de los certificados.

Después veremos que son críticos para configuraciones como por ejemplo interceptar tráfico SSL en caso de que queramos gestionar las conexiones hacia fuera de páginas web, etc.

El protocolo DNS, que significa Domain Name System, tiende a convertirse por su propia naturaleza en el principal objetivo de la mayoría de los hackers de red.

Por eso es importante conocer su funcionamiento.

Principales amenazas y posibles soluciones DNS está relacionado directamente con otros servicios y protocolos de red.

Por este motivo su protección es uno de los puntos clave dentro del hardening empresarial.

Algunas de las amenazas directamente relacionadas con el DNS son los famosos DDOS o Distributed Denial of Service o Denegación de servicio Distribuida Pero no son los únicos, también podemos encontrar los ataques llamados Caché Poisoning o envejecimiento de la caché o DNS Spoofing, los cuales atacan las respuestas enviadas por los servidores alterando las direcciones IP reales.

Este tipo de ataque permite desde el robo de credenciales hasta incluso montar sitios web falsos para engañar al usuario redireccionando el acceso original.

Algunas de las claves que podemos utilizar para implementar un correcto hardening de DNS pueden La primera, tener un backup local del DNS.

La segunda sería utilizar IPAM que significa IP Address Management para obtener una visión global de la infraestructura.

El tercer punto es obvio, son las actualizaciones de los servidores DNS.

El cuarto punto, el RRL o Response Rate Limiting se usa para limitar el número de respuestas y evitar una saturación del servicio.

Después tenemos lo que se llama el DNSSEC o DNS Security Extension, el cual nos permite añadir validación a las respuestas y también tenemos el Response Policy Zones o R que sirve para controlar directamente las peticiones.

Las ACL o Access Control List o Lista de control de acceso son esenciales para filtrar el tráfico y definir reglas de acceso, reforzando la seguridad perimetral.

Por otro lado, los sistemas IDS e ips son fundamentales para la detección y una prevención de amenazas, proporcionando una respuesta activa ante intrusos.

Después un proxy actúa como intermediario mejorando la seguridad mediante el control de tráfico de Internet y ocultando la información de la red interna.

Después tenemos herramientas como SSH que es crucial para la gestión segura de dispositivos a través de redes que no son confiables como Internet, ofreciendo una comunicación cifrada.

Finalmente, la seguridad de DNS es vital para proteger contra la manipulación de DNS, asegurando la resolución de nombres de dominio de forma fiable.

Y seguramente llegamos al final de la sesión.

Os esperamos en el siguiente vídeo.