Herramientas / Técnicas básicas de Hardening para redes

Redes internas: Intranet y redes de área local

Segmentación de la red local

- Proporciona aislamiento de los servicios en las diferentes redes
- Permite mitigar los efectos de una intrusión
- Segmentación física y lógica

Acceso remoto a la red

Importante mantener los dispositivos que se conecten a la red actualizados. Desde el Firewall, Antivirus y que cumplan las políticas de seguridad corporativas.

El NAC (Network Access Control) permite la segmentación a nivel de Software y es una protección frente a los dispositivos que quieren conectarse a la red sin identificación.

VPN (Virtual Private Network)

Proporciona un canal seguro de comunicación entre un dispositivo externo a la red corporativa y la misma red.

Virtual Network segmentation

Creación de una red virtual desde dispositivos virtuales. La ventaja es que podemos garantizar un aislamiento del trafico entre redes de la virtual network, ademas de generar la red de forma mucho mas rápida y dinámicamente. Al ser virtual, no existen dispositivos físicos a los que conectar cables, sino se gestiona todo a través de software de visualización, como Hyper-V o VmWare.

Ademas, se pueden aplicar extensiones antes del enrutamiento como:

- Inspección de paquetes de red
- IDS / Firewall
- Filtrado de paquetes de red

A si mismo, se pueden habilitar servicios como:

- MAC Address spoofing
- DHCP Guard
- Router Guard
- Port ACL, basado en IP & MAC

Red perimetral

Sensorizacion

Uno de los mecanismos de protección frente a amenazas a nuestra red.

Para llevar a cabo esta técnica, debemos:

- Monitorizar activamente la red
  - Sesiones que puedan existir
  - Comportamientos sospechosos de los usuarios
- Para monitorizar la red, debemos distribuir los sensores de forma correcta en la misma red.

Los sensores deben ser capaces de analizar outliers en el uso de protocolos, encontrar firmas de malware dentro de los paquetes que envía el malware a su sistema de C&C. Estos sensores generan alertas que se deben analizar para determinar si efectivamente, existe una amenaza en nuestra red, o es un falso positivo.

Mecanismos de protección:

- IDS
- IPS

Intrusion Detection System Detecta posibles intrusiones y alerta a los administradores del sistema de las amenazas detectadas.

Política asociada al IDS:

- Quien monitoriza?
- Derechos administrativos de acceso al IDS?
- Como se gestionan los incidentes en caso de alerta?
- Políticas de actualización del IDS?
- Donde se ubica el IDS?

Tipos de IDS:

- NIDS (Network-based IDS): Monitoriza el trafico entre los dispositivos de red
- HIDS (Host-based IDS): Detecta trafico desde dentro del computador.
  - Especialmente útil en protección contra Malware.
- Basado en firmas (Signature-based IDS): Basa su análisis en firmas catalogadas de malware.
- Basado en anomalías (Anomaly-based IDS): A partir de una linea base, podemos ser capaces de detectar nuevas amenazas no catalogadas. (Suele producir bastantes falsos positivos)

Intrusion Prevention System Se consideran IDS + la capacidad de actuar frente a la amenaza detectada. Tiene las mismas estructuras como las definidas en IDS.

Snort

Es una herramienta de IDS o IPS. Mas adelante, se analizara mas.

Cuando SNORT esta monitorizando muchas interfaces y redes simultáneamente, se requiere el uso de herramientas de visualización de datos, para que se pueda seguir el análisis en tiempo real y de forma comprensible. Asisten dos interfaces traficas para Snort:

- SGUIL
  - Información mas detallada, a nivel de sesiones http
- sorba
  - Información muy categorizada sobre las alertas recibidas

Protección de dispositivos de red

Procedimientos generales:

- Realizar copias de seguridad (Fuera de la red), tanto de firmware, como de archivos de configuración.
- Deshabilitar los protocolos no usados
- **Encriptacion de ficheros de configuracion:** (Transmisión y actualización)
- **Acceso seguro:** Política de contraseñas seguras para los servicios activos

Buenas practicas

- Siempre usar AH, con claves SSH, no con contraseñas
- Si es posible, restringir configuración de red en remoto
- Deshabilitar los puertos no usados
- Usar capacidades de seguridades de puerto (MAC flooding)
- Usar la seguridad a nivel de puerto para evitar ataques, como el falseado de DHCP (DHCP snooping)
- Política de actualización del firmware y los sistemas operativos de los conmutadores/enrutadores