Herramientas preventivas y paliativas

Las principales serán las escuchas, accesos no autorizados y ataques de denegación de servicio. Se estudian las fases del ataque que son:

- Fase de investigación, penetración, persistencia, expansión y logro del objetivo.

Fase de investigación

Se estudia el objetivo del ataque. Se intentará recoger información sobre:

- Empresa / dispositivo objetivo.
- Dominio objetivo (whois)
- Servidores, plataforma y servicios

Contramedidas

Algunas medidas son:

- Restringir info. para que no se difunda por los servicios DNS y whois.
- Activar filtrado de paquetes para evitar la detección de la plataforma objetivo y sus servicios.
- Implementar un IDS para detectar posibles escaneos de puertos y alterar al admin.

Fase de penetración

El atacante intentará acceder al objetivo:

- Explotación de vulnerabilidades. Aplicaciones que permitan código arbitrario.
- Explorar una posible debilidad en las contraseñas.
- Identificar malas configuraciones en servicios.
- Buscar servicios abandonados o no actualizados.

Contramedidas

- Revisión de los ficheros log del filtrado de paquetes.
- Mantener equipos y servicios actualizados.
- Revisar configuraciones de servicios y usuarios.
- Deshabilitar servicios no utilizados o desinstalarlos.

Fase de persistencia

Atacante quiere no ser detectado:

- Puertas traseras en el sistema.
- Buscar y borrar archivos de auditoría o logs del sistema.

Contramedidas

- Guardar los logs en otra ubicación.
- Crear hash de los archivos del sistema para comprobar si se han modificado.

Fase de expansión

El objetivo final de un ataque no es el primer sistema atacado, sino que se utilizan saltos intermedios para intentar no ser rastreados. Un sistema puede ser víctima y atacante al mismo tiempo.

Contramedidas

- Filtrado de paquetes.
- Sistemas IDS.
- Control periódico de los archivos de log.

Escalado del ataque

Cuando el atacante compromete un equipo, intenta realizar el ataque desde ese punto y comprometer otros objetivos.

Reconocimiento

- Se deberá conocer la red y hacer una topología de la misma, sus servicios y vulnerabilidades.
- Se usan herramientas nslookup y whois.
- También se podrán conocer el rango de direcciones IP asignadas a la organización.

Contramedidas

Aplicar filtros para no permitir la transferencia de este tipo de paquetes ICMP.

Interceptación o eavesdropping

Proceso mediante el cual un agente capta información que no le iba dirigida. Se usa sniffing.

Contramedidas

- No permitir segmentos de red de fácil acceso.
- Utilizar cifrado en las comunicaciones y en el almacenamiento.
- No tener activadas tomas libres de red.
- Utilizar autenticación a nivel de capa de enlace.

Ataque por acceso

El atacante obtiene los privilegios para acceder a los dispositivos de forma ilegítima.
Principales técnicas:

- Explotación de contraseñas débiles.
- Explotar configuraciones como TFTP, FTP y acceso remoto de registro.
- Explotar fallas de aplicaciones. Desbordamiento de buffers.
- Ingeniería social.

EJ → MITM, manipulación de datos, etc

Ataque en routers o conmutadores

Ataques comunes:

- Sobrecarga en la tabla CAM de los switches.
- Acceso a diferentes VLANs.
- La utilización de STP para modificar el árbol de expansión.
- Falsificación de direcciones MAC.
- Inundación y saturación del servidor DHCP.