Implantación de mecanismos de seguridad activa (Seguridad y alta disponibilidad)

Ataques y contramedidas en sistemas personales

Clasificación de los ataques

Los tipos de ataques informáticos son muy variados, una posible clasificación debido a su sencillez para comprender cómo funcionan los ataques es la siguiente (es un ejemplo de clasificación, muchas posibles clasificaciones):

Phishing: se dirige a una persona concreta para robar sus datos, ya se trate de credenciales de acceso a sistemas o de números de tarjetas de crédito. Por lo general, el ciberdelincuente se hace pasar por una persona o empresa de confianza.

Más información

- https://www.jesusninoc.com/phishing/
- https://www.jesusninoc.com/fraude/
- https://www.jesusninoc.com/spam/

Malware: consiste, en esencia, en un programa o código que se instala en el sistema informático y asume el control, muchas veces sin que la empresa sea consciente.

Más información

- https://www.jesusninoc.com/01/10/ejercicios-de-seguridad-practica-sobre-virus/#Medios_de_transmision
- https://www.jesusninoc.com/01/10/ejercicios-de-seguridad-practica-sobre-virus/#%C2%BFQue_podemos_hacer_utilizando_PowerShell

---

Ejercicios

- https://www.jesusninoc.com/01/10/ejercicios-de-seguridad-practica-sobre-virus/#Simular_el_funcionamiento_de_un_antivirus_mediante_firmas

---

Ataques web: los ataques web son códigos que se infiltran en páginas web o navegadores para dañarlos.

Más información

- https://www.jesusninoc.com/web/

Ejercicios

- **Subir y ejecutar un fichero .exe a un servidor web**
  - https://www.jesusninoc.com/02/01/convertir-un-script-de-powershell-en-un-ejecutable-de-windows-convertir-un-formulario-en-powershell/#Descargar_e_instalar_PS2EXE_aplicacion

_que_convierte_de_PS1_a_EXE_siendo_administrador_de_PowerShell

---

Anatomía de ataques y análisis de software malicioso

El objetivo de los ataques es buscar alguna vulnerabilidad hasta encontrarla e intentar explotarla, algunos tipos de vulnerabilidades son:

- Vulnerabilidades de desbordamiento de buffer.
- Vulnerabilidades de condición de carrera (race condition).
- Vulnerabilidades de error de formato de cadena (format string bugs).
- Vulnerabilidades de Cross Site Scripting (XSS).
- Vulnerabilidades de Inyección SQL.
- Vulnerabilidades de denegación del servicio.
- Vulnerabilidades de ventanas engañosas (Window Spoofing).
- Etc.

Herramientas preventivas. Instalación y configuración

Lo primero que hemos de hacer es un análisis de las posibles amenazas que puede sufrir el sistema informático, una estimación de las pérdidas que esas amenazas podrían suponer y un estudio de las probabilidades de que ocurran.

A partir de este análisis habrá que diseñar una política de seguridad en la que se establezcan las responsabilidades y reglas a seguir para evitar esas amenazas o minimizar los efectos si se llegan a producir.

La prevención sirve para evitar desviaciones respecto a la política de seguridad.

Ejemplo: utilizar el cifrado en la transmisión de la información evita que un posible atacante capture (y entienda) información en un sistema de red.

Algunos mecanismos de prevención:

- Mecanismos de identificación y autenticación
- Mecanismos de control de acceso
- Mecanismos de separación
- Mecanismos de seguridad en las comunicaciones

Herramientas paliativas. Instalación y configuración

Las herramientas paliativas se aplican cuando se ha detectado una violación de la seguridad del sistema para recuperar su normal funcionamiento.

Ejemplo: las copias de seguridad.

Dentro de este grupo de mecanismos hay un subgrupo llamado mecanismos de análisis forense cuyo objetivo es, no solo devolver el sistema a su situación normal, sino averiguar también el alcance de la violación, lo que ha hecho el intruso en el sistema y qué puerta ha utilizado para entrar en el sistema. De esta forma se previenen posibles ataques posteriores.

Actualización de sistemas y aplicaciones

Cada día aparecen nuevas vulnerabilidad en los sistemas operativos y en los programas, es importante mantener el sistema operativo actualizado con los últimos parches de seguridad.

Las actualizaciones sirven para evitar problemas o

corregirlos, de esta forma el sistema operativo se mantiene seguro, las actualizaciones son importantes y necesarias para los sistemas operativos.

Los sistemas de gestión de actualizaciones permiten que las actualizaciones se descarguen y se instalen con orden, de no ser así puede suponer un problema si el sistema operativo comienza a descargar todas las actualizaciones a la vez y en algunos casos pueden llegar a saturar ciertos recursos como por ejemplo la conexión de red, para resolver este problema algunos sistemas operativos tienen programas que descargan las actualizaciones y las envían a otros ordenadores a la red de una manera ordenada.

Seguridad en la conexión con redes públicas

Para concretar la explicación hablamos sobre las redes inalámbricas.

Estos son algunos puntos que estarían bien considerar:

- Estar atento, la señal Wi-Fi pública es inherentemente insegura, de manera que tenga cuidado.
- Recordar que cualquier dispositivo podría estar en riesgo.
- Tratar todos los enlaces Wi-Fi con desconfianza.
- Tratar de verificar que es una conexión inalámbrica legítima y no se trata de un enlace falso.
- Usar una red privada virtual (VPN).
- Considerar otras opciones más seguras como usar el teléfono móvil.
- Proteger el dispositivo contra ciberataques.

Pautas y prácticas seguras

- Tener cuidado con los adjuntos en el correo electrónico.
- Actualizar el software del sistema operativo

periódicamente.
- Utilizar mejores contraseñas y cambiarlas cada cierto tiempo.
- Usar antivirus y aplicaciones anti-malware.
- Cerrar las sesiones al terminar cualquier operación en una web.
- Evitar realizar operaciones privadas en redes abiertas y públicas.
- Activar el Firewall del sistema.
- Evitar software poco conocido.
- Realizar copias de seguridad.

Seguridad en la red corporativa

Monitorización del tráfico en redes

Una herramienta básica para observar los mensajes intercambiados entre aplicaciones es un analizador de protocolos (packet sniffer). Un analizador de protocolos es un elemento pasivo, únicamente observa mensajes que son transmitidos y recibidos desde y hacia un elemento de la red, pero nunca envía él mismo mensajes. En su lugar, un analizador de protocolos recibe una copia de los mensajes que están siendo recibidos o enviados en el terminal donde está ejecutándose.

Está compuesto principalmente de dos elementos: una librería de captura de paquetes, que recibe una copia de cada trama de enlace de datos que se envía o recibe, y un analizador de paquetes, que muestra los campos correspondientes a cada uno de los paquetes capturados. Para realizar esto, el analizador de paquetes ha de conocer los protocolos que está analizando de manera que la información mostrada sea coherente. Es decir, si capturamos un mensaje HTTP, el analizador de paquetes ha de saber que este mensaje se encuentra encapsulado en un segmento TCP, que a su vez se encuentra encapsulado en un paquete IP y éste a su vez en una trama de Ethernet.

Más información

- https://www.jesusninoc.com/05/29/introduccion-wireshark/
- https://www.jesusninoc.com/02/06/rawcap-analizador-de-red/
- https://www.jesusninoc.com/02/06/enviar-un-mensaje-udp-a-un-ordenador-desde-powershell-y-analizar-con-rawcap-analizador-de-red-que-utiliza-sockets-sin-formato/
- https://www.jesusninoc.com/07/20/softperfect-network-protocol-analyzer/
- https://www.jesusninoc.com/softperfect-network-protocol-analyzer/
- https://www.jesusninoc.com/08/09/colasoft-packet-player/
- https://www.jesusninoc.com/01/24/ejercicios-de-routerboard-de-mikrotik-conectarse-a-un-routerboard-de-mikrotik-establecer-una-direccion-ip-en-el-dispositivo-y-capturar-trafico-con-la-herramienta-packet-sniffer/

Seguridad en los protocolos para comunicaciones inalámbricas

El problema de las redes WiFi es la seguridad. Existen varias alternativas para garantizar la seguridad de las redes que usan estos estándares.

Consejos que fortalecen la seguridad de las redes inalámbricas:

- Evitar conexiones abiertas.
- Cambiar las contraseñas de acceso.
- Evitar que se pueda tener acceso a través de Internet al router.
- Filtrado de direcciones MAC y direcciones IP.

- Revisar los logs.

Riesgos potenciales de los servicios de red

Algunos riesgos:

- Ser víctima de un ataque «Man in the Middle».
- Robo de datos personales, información confidencial y/o credenciales.
- Interceptar una transacción online.
- Falsos puntos de acceso.
- Router vulnerado.

Más información

- https://www.jesusninoc.com/02/17/riesgos-en-la-empresa/

Intentos de penetración

Las pruebas de penetración (también llamadas «pen testing») son una práctica para poner a prueba un sistema informático, red o aplicación web para encontrar vulnerabilidades que un atacante podría explotar.