Configuración de los sistemas informáticos (Bastionado de redes y sistemas)

Reducción del número de servicios, Telnet, RSSH, TFTP, entre otros

Los procesos en segundo plano que realizan distintas funciones, algunas relacionadas con el sistema operativo y otras no, se denominan servicios, y se están ejecutando permanentemente en el sistema.

Los servicios se pueden iniciar, detener, pausar, reanudar, etc. Estas acciones, normalmente, sólo las puede realizar el administrador de forma local o remota. Un ejemplo de servicio de sistema es el servicio de escritorio remoto, que permite conectarse remotamente al equipo.

Los servicios ejecutan procesos y los procesos tienen hilos, hay relación entre procesos e hilos y entre servicios e hilos.

Más información

- https://www.jesusninoc.com/07/07/7-gestion-de-procesos-en-powershell/#Servicios
- https://www.jesusninoc.com/11/10/analizar-servicios-con-powershell/

Hardening de procesos (eliminación de información de depuración en caso de errores, aleatorización de la memoria virtual para evitar exploits, etc.)

Ejercicios

- https://www.jesusninoc.com/06/25/utilizar-zonas-de-memoria-compartida-en-linux-mediante-wsl-desde-powershell/
- https://www.jesusninoc.com/03/20/analizar-con-cheat-engine-un-payload-de-ejecucion-de-comandos-arbitrarios-para-ejecutar-powershell/

Más información

- https://www.jesusninoc.com/01/12/tecnicas-de-inyeccion-de-procesos/
- https://www.jesusninoc.com/07/24/cheat-engine/
- https://www.jesusninoc.com/07/02/ver-el-mapa-de-memoria-ram-con-rammap/

Eliminación de protocolos de red innecesarios (ICMP, entre otros)

Más información

- https://www.jesusninoc.com/firewall/
- https://www.jesusninoc.com/02/09/mostrar-los-puertos-que-estan-abiertos-en-las-reglas-de-entrada-del-firewall-de-windows-desde-powershell-que-estan-habilitadas-y-permiten-conexion/

Securización de los sistemas de administración remota

Más información

- https://www.jesusninoc.com/01/03/instalacion-configuracion-y-uso-de-servicios-de-acceso-y-administracion-remota/

Sistemas de prevención y protección frente a virus e intrusiones (antivirus, HIDS, etc.)

Uno de los programas principales para evitar la propagación de aplicaciones no deseadas es el antivirus.

Ejercicios

Simulación de ransomware

- https://www.jesusninoc.com/03/26/leer-los-ficheros-que-h

ay-dentro-de-un-directorio-cifrarlos-con-un-algoritmo-sencillo-y-almacenarlos-en-un-nuevo-directorio/
- https://www.jesusninoc.com/03/27/leer-los-ficheros-que-hay-dentro-de-un-directorio-cifrarlos-almacenarlos-en-un-directorio-y-comprimir-el-directorio/

Simulación de keylogger

- https://www.jesusninoc.com/03/11/keylogger-sencillo-con-powershell/
- https://www.jesusninoc.com/07/16/transfer-keylogger-log-file-between-server-and-client-sockets-tcp/
- https://www.jesusninoc.com/01/22/capturar-las-teclas-que-se-pulsan-y-mostrarlas-en-powershell/
- https://www.jesusninoc.com/01/22/capturar-las-teclas-que-se-pulsan-desde-powershell-y-calcular-el-tiempo-que-se-tarda-en-pulsar-una-tecla-y-otra-despues/
- https://www.jesusninoc.com/01/22/capturar-las-teclas-que-se-pulsan-desde-powershell-y-calcular-el-tiempo-total-que-transcurre-desde-el-inicio-hasta-que-se-empezo-a-pulsar-la-primera-letra-y-se-siguen-pulsando-hasta-finalizar/

Simulación de keylogger con canal encubierto

- https://www.jesusninoc.com/03/11/keylogger-sencillo-con-powershell/
- https://www.jesusninoc.com/03/11/enviar-datos-a-un-formulario-de-google-docs-desde-powershell/

Más información

- https://www.jesusninoc.com/07/05/5-gestion-del-software-en-powershell/#Antivirus
- https://www.jesusninoc.com/01/10/ejercicios-de-seguridad-practica-sobre-virus-en-powershell/

Configuración de actualizaciones y parches automáticos

Cada día aparecen nuevas vulnerabilidades 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 necesarias para los sistemas operativos.

Los sistemas de gestión de actualizaciones permiten que éstas se descarguen y se instalen con orden, de no ser así podrían aparecer problemas si el sistema operativo comenzara a descargar todas las actualizaciones a la vez, 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.

Gracias a los sistemas de actualizaciones, el tiempo que va desde que se registra un fallo hasta que se corrige es muy pequeño.

Las actualizaciones pueden ser del sistema operativo, de programas, de controladores, etc.

Ejercicio

- https://www.jesusninoc.com/02/07/ejercicios-de-powershel

l-ejercicios-de-actualizaciones/

Más información

- https://www.jesusninoc.com/07/05/5-gestion-del-software-en-powershell/#Actualizaciones

---

Sistemas de copias de seguridad

En cualquier sistema operativo hay que asegurarse de que no se van a perder datos, y que si se produce la pérdida, por lo menos se podrán restaurar los datos perdidos. La duda no es saber si un disco duro fallará o no, sino cuándo lo hará, y para esto tenemos que estar preparados.

Una copia de seguridad consiste simplemente en tener duplicados los archivos en algún dispositivo o medio de almacenamiento, los archivos pueden ser de los usuarios o propios del sistema operativo.

Tipos de copias se seguridad:

- Copia completa. Se almacenan todos los archivos de los que se desea hacer copia y se marcan como copiados. Este tipo de copia requiere gran cantidad de tiempo y suficiente espacio de almacenamiento para guardar la copia.
- Copia incremental (progresiva). Se almacenan los archivos que se han modificado desde la última copia completa o incremental y se marcan como copiados.

Ejercicio

- https://www.jesusninoc.com/06/04/ejercicios-de-powershell-explica-un-procedimiento-de-copias-de-seguridad-que-te-parezca-lo-mas-optimo-posible/

Más información

- https://www.jesusninoc.com/02/28/seguridad-informatica-con-powershell/#Copias_de_seguridad

---

Shadow IT y políticas de seguridad en entornos SaaS

Shadow IT son todos aquellos conectados a la red que no están dentro de los esquemas de gestión de los departamentos de informática, ya sean dispositivos personales no corporativos como portátiles, teléfonos móviles, tabletas, rastreadores de actividad física o dispositivos inteligentes, se conocen como BYOD (Bring Your Own Device, en inglés) y su uso supone un riesgo potencial para las empresas.