Ejercicios de seguridad: práctica sobre virus en PowerShell

Simular el funcionamiento de un antivirus mediante firmas

- https://www.jesusninoc.com/01/05/ejercicios-de-powershell-hacer-el-hash-de-cada-uno-de-los-modulos-que-ejecuta-el-proceso-notepad/
- https://www.jesusninoc.com/12/22/ejercicios-de-powershell-calcular-el-hash-sha256-de-todos-los-procesos-que-se-estan-ejecutando/
- https://www.jesusninoc.com/12/23/ejercicios-de-powershell-calcular-el-hash-sha256-de-todos-los-procesos-que-se-estan-ejecutando-crear-una-funcion-compleja/

Medios de transmisión de virus

- Software
    - Descargado
    - Vulnerabilidades
        - Navegadores
        - Cliente mail
    - Macros
    - Scripts
    - SSL
    - Recursos compartidos
- Hardware

        - USB
    - Radio
    - Personas
        - Compartir información

¿Qué podemos hacer utilizando PowerShell (comportamientos que tiene los virus)?

Software

– Enviar correo

https://www.jesusninoc.com/2015/06/05/enviar-correo-electronico-utilizando-outlook/

– Cifrar contenido

https://www.jesusninoc.com/2017/01/23/cifrar-con-un-algoritmo-sencillo-el-nombre-y-el-contenido-de-un-fichero-de-texto/

– Enviar posición del ratón

https://www.jesusninoc.com/2015/07/08/send-the-cursors-position-between-client-and-server-sockets-tcp/

– Enviar información de un keylogger

https://www.jesusninoc.com/2015/07/16/transfer-keylogger-log-file-between-server-and-client-sockets-tcp/

– Enviar capturas de la webcam

https://www.jesusninoc.com/2015/07/18/capture-a-single-image-from-a-webcam-and-transfer-image-between-server-and-client-

sockets-tcp/

– Enviar captura de pantalla

https://www.jesusninoc.com/2015/07/13/transfer-screenshot-between-server-and-client-sockets-tcp/

– Cambio de la directiva de ejecución para ejecutar scripts en los que no se confía

https://www.jesusninoc.com/2015/01/06/cambio-de-directiva-de-ejecucion-para-ejecutar-scripts-en-los-que-no-confia/

– Descargar y ejecutar un script cambiando la directiva de ejecución

https://www.jesusninoc.com/2015/01/08/descargar-y-ejecutar-un-script-cambiando-la-directiva-de-ejecucion/

– Descargar y ejecutar un script sin cambiar la directiva de ejecución

https://www.jesusninoc.com/2015/01/09/descargar-y-ejecutar-un-script-sin-cambiar-la-directiva-de-ejecucion/

– Download & Execute

https://www.jesusninoc.com/2016/11/15/formas-de-descargar-y-ejecutar-ficheros-desde-un-servidor-en-powershell/

– Payload Netcat download and reverse shell

https://www.jesusninoc.com/2015/02/19/payload-netcat-download-and-reverse-shell/

– Automatizar el inicio de sesión en Facebook

https://www.jesusninoc.com/2015/07/17/automatizar-el-inicio-de-sesion-en-facebook-de-forma-grafica-utilizando-powershell/

– Recoger información disponible en el sistema

https://www.jesusninoc.com/2016/10/09/windows-post-exploitation-cmdlets-execution-powershell/

– Desactivar la visualización de inmediato mediante PowerShell

https://www.jesusninoc.com/2018/07/17/desactivar-la-visualizacion-de-inmediato-mediante-powershell/

– Desactivar la visualización de inmediato desde PowerShell, abrir Notepad y escribir un texto

https://www.jesusninoc.com/2018/07/18/desactivar-la-visualizacion-de-inmediato-desde-powershell-abrir-notepad-y-escribir-un-texto/

– Modificación de programas para que dejen de funcionar

– Modificación de programas para que funcionen erróneamente

– Modificación sobre los datos

– Eliminación de programas y/o datos

– Acabar con el espacio libre en el disco rígido

– Hacer que el sistema funcione más lentamente

– Robo de información confidencial

– Seleccionar un archivo aleatorio del equipo y lo envía a la lista de direcciones de correo, el nombre es el mismo y tiene adjuntado el virus

– Responder mensajes de correo

– Activarse cuando el consumo de disco sea menor que x%

– Activarse cuando sea una hora en concreto

– Simular comportamiento de camaleón, hacer algo normal y por otro lado otra cosa (almacenar información sobre el sistema)

– Consumir recursos hasta agotarlos

– Dejar una puerta abierta para otro programa

– Mostrar las contraseñas de todas las conexiones inalámbricas

– Exportar cookie

– Importar cookie

– Instalar otros instaladores de cookies para sacar todas

– Abrir Firefox con el tamaño 1×1

https://www.jesusninoc.com/2016/06/06/abrir-firefox-con-el-tamano-1×1/

– Obtener información sobre los dispositivos USB conectados en un equipo del dominio con PowerShell

https://www.jesusninoc.com/2017/07/23/obtener-informacion-sobre-los-dispositivos-usb-conectados-en-un-equipo-del-dominio-con-powershell/

– Añadir virus a un BMP

– Descargar aplicaciones por ejemplo FTP

– Modificar proxy

https://www.jesusninoc.com/03/27/habilitar-o-deshabilitar-un-servidor-proxy-en-internet-explorer-utilizando-powershell/

– Bloquear el escritorio

– Permitir accesos remotos

http://www.jesusninoc.com/2016/05/08/permitir-conexiones-remotas/

– Eliminar un tipo de fichero por ejemplo MP3

– Modificar el contenido de ficheros

– Cifrar el contenido de ficheros

https://www.jesusninoc.com/2017/01/23/cifrar-con-un-algoritmo-sencillo-el-nombre-y-el-contenido-de-un-fichero-de-texto/

– Utilizar Outlook y cualquier otro programa que permita enviar información

– CAMBIAR LA PÁGINA DE INICIO EN INTERNET EXPLORER DESDE EL REGISTRO DE WINDOWS

https://www.jesusninoc.com/06/04/cambiar-la-pagina-de-inicio-en-internet-explorer-desde-el-registro-de-windows/

– Almacenar valores del Registro de Windows en una variable en PowerShell

https://www.jesusninoc.com/2017/07/29/almacenar-valores-del-registro-de-windows-en-una-variable-en-powershell/

– EJECUTAR LA INFORMACIÓN QUE SE ENCUENTRA EN UN VALOR DENTRO DE LA CLAVE

CLSID DEL REGISTRO DE WINDOWS

https://www.jesusninoc.com/06/04/ejecutar-la-informacion-que-se-encuentra-en-un-valor-dentro-de-la-clave-clsid-del-registro-de-windows/

– Abrir puertos y activar servicios

– Crear un usuario local con contraseña en Windows 10

https://www.jesusninoc.com/2017/02/05/crear-un-usuario-local-con-contrasena-en-windows-10/

– Crear ficheros y colocarlos de página principal

– Añadir líneas del registro para modificar el comportamiento de los navegadores

– Obtener información del sistema

– Añadirlo al arranque en el registro

– Crear un ejecutable para seguir con la infección

– Buscar unidades de disco duro y demás

– Cambiar un fichero JPG por un PS1

– Convertir PS2EXE

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