MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Webinar Gratuito
Windows

Alonso Eduardo Caballero Quezada

Consultor e Instructor en Hacking Ético y Forense Digital
e-mail: ReYDeS@gmail.com

Sitio web: http://www.mile-sec.com
Correo: capacitacion@mile-sec.com

Febrero 2019

Sobre MILE-SEC

MILE-SEC
Capacitación y Consultoría en
Hacking Ético & Forense Digital

MILESEC E.I.R.L, es una empresa de capitales Peruanos fundada en el año 2017, netamente dedicada a brindar servicios de capacitación a empresas, instituciones, organizaciones y profesionales, en las áreas de seguridad de la información y tecnologías de la información (T.I.), tales como; Pruebas de Penetracion, Hacking Ético, Evaluación de Vulnerabilidades, Forense de Computadoras y Forense Digital. Así mismo brinda servicios de consultorías especializadas en todas las áreas antes mencionadas.

Durante estos años ha realizado capacitaciones presenciales y consultorías tanto públicas cuanto privadas para Ecuador y Perú, en las ciudades de Lima, Cusco y Trujillo. Así mismo ha realizado capacitaciones online o virtuales.


http://www.mile-sec.com/

informes@mile-sec.com / mileseceirl@gmail.com

https://www.facebook.com/mileseceirl/

https://twitter.com/mileseceirl

https://www.linkedin.com/in/milesec/

Temario

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

- Introducción a las vulnerabilidades en Windows
- Seleccionar las herramientas
- Herramientas libres de Microsoft
- Herramientas de evaluación
- Herramientas para tareas específicas
- Obtener información sobre las vulnerabilidades en Windows
- Escanear el sistema
- NetBIOS y Detectar sesiones Nulas
- Mapear
- Obtener información
- Medidas correctivas contra las sesión nula
- Verificar permisos de compartidos
- Defectos en Windows
- Pruebas
- Explotar parches ausentes
- Utilizar Metasploit Framework
- Medidas correctivas explotación de vulnerabilidades de parches ausentes
- Ejecutar escaneos autenticados

Introducción

Microsoft Windows es uno de lo sistemas operativos más ampliamente utilizados del mundo. Y también es el más abusado. ¿Esto es debido a Microsoft no tiene cuidado sobre la seguridad comparado con otros proveedores?. La respuesta es corta es “no”. De hecho, numerosas vulnerabilidades de seguridad fueron pasadas por alto, especialmente en los días de Windows NT. Pero los productos Microsoft están tan generalizados en las redes de la actualidad, y consecuentemente Microsoft es el proveedor más fácil para elegir; por lo tanto los productos Microsoft terminan en el punto de mira de los atacantes maliciosos. Lo positivo es esta acción impulsa los requerimientos de una mejor seguridad.

Muchas de las fallas en seguridad no son nuevas. Son variantes de vulnerabilidades ya existentes durante mucho tiempo. Recordar la frase; “Mientras más cambian las cosas, más permanecen igual”. Eso también aplica aquí. La mayoría de ataques en Windows se pueden prevenir si los parches se aplican correctamente. Por lo tanto, la mala gestión de seguridad es frecuentemente la razón real por la cual los ataques contra Windows, siguen siendo exitosos.

Introducción a las vulnerabilidades en Windows

Dada la facilidad del uso de Windows, su servicio de directorio activo listo para la empresa, y la plataforma de desarrollo .NET rica en características, muchas organizaciones utilizan la plataforma Microsoft para gran parte de sus necesidades de redes y cómputo.

Cuando Windows y otro software de Microsoft son atacados, especialmente por un gusano o virus basado en Internet ampliamente diseminado, cientos de miles de organizaciones y millones de computadoras son afectadas. Muchos de los bien conocidos ataques contra Windows conducen a los siguientes problemas.

- Fuga de información sensible, incluyendo archivos conteniendo información sobre salud, y números de tarjeta de crédito
- Contraseñas han sido rotas, y utilizadas para realizar otros ataques
- Los sistemas han sido puestos fuera de línea por ataques de negación de servicio (DoS)
- Se ha obtenido control remoto
- Las bases de datos completas han sido copiadas o borradas

Seleccionar las herramientas

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Literalmente cientos de herramientas de Hacking Windows y herramientas de pruebas están disponibles. La clave para encontrar un conjunto de herramientas la cual pueda hacer lo requerido, y sea confortable al ser utilizado.

Muchas herramientas de seguridad funcionan únicamente en ciertas versiones de Windows.

Existen muchas herramientas de seguridad, y otras herramientas las cuales se instalan en Windows, especialmente programas los cuales se enlazan dentro de los controladores de la red y pila TCP/IP, estas vuelven más inestables a Windows. Referido directamente a un desempeño lento, inconvenientes generales de estabilidad, y eventuales pantallas azules de la muerte. Desafortunadamente, es frecuente la única manera de arreglar esto es reinstalar Windows y todas sus aplicaciones.

Una de las maneras para evaluar herramientas de manera “segura” es utilizar software de virtualización.

Herramientas libres de Microsoft

Se puede utilizar las siguientes herramientas libres de Microsoft Windows para evaluar los sistemas de diversas debilidades.

Programas incorporados en Windows. Para enumeración NetBIOS y servicios TCP/UDP:

- Nbtstat
- Netstat
- Net

Sysinternals. Para estimular, producir y vigilar servicios, procesos, y recursos de Windows, tanto a nivel local y a través de la red.

- Sysmon
- Sigcheck
- Autoruns

* https://docs.microsoft.com/en-us/sysinternals/

Herramientas de evaluación

Las herramientas “todo en uno” realizan una diversidad de pruebas en seguridad, incluyendo lo siguiente:

- Escaneo de puertos
- Huella del sistema operativo
- Romper contraseñas básicas
- Mapeo detallado de vulnerabilidades de diversas debilidades de seguridad, factibles de ser encontradas en sistemas Windows

Algunas de las herramientas son:

- OpenVas
- Nessus
- GFI-LanGuard
- Nexpose

* http://www.openvas.org/
* http://www.openvas.org/
* https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard
* https://www.rapid7.com/products/nexpose/

Herramientas para tareas específicas

La siguientes herramientas realizan tareas más específicas para descubrir fallas de seguridad relacionadas a Windows. Estas herramientas proporcionan una visión detallada de los sistemas Windows, y proporciona información la cual de otra manera no podría ser obtenida de las herramientas “todo en uno” de evaluación.

- Metasploit Framework
- NetScanTools Pro
- SoftPerfect Network Security Scanner
- TCPView
- Winfo

* https://www.rapid7.com/products/metasploit/
* https://www.netscantools.com/nstpromain.html
* https://www.softperfect.com/products/networkscanner/
* https://docs.microsoft.com/en-us/sysinternals/downloads/tcpview
* http://www.ntsecurity.nu/toolbox/winfo/

Obtener información sobre las vulnerabilidades en Windows

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Cuando se evalúa por vulnerabilidades, se inicia escaneando las computadoras para ver aquello factible de ser visto por los atacantes maliciosos.

Las explotaciones clásicas se aprovechan de la carencia de un firewall. Así mismo muchas de las explotaciones podrían afectar todas las versiones del sistema operativo Windows. Aunque siempre se debe tener en consideración, todo depende del escenario de evaluación, versión específica de Windows, nivel de parche, y fortalecimientos hechas al sistema.

Escanear el sistema

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Un sencillo proceso el cual puede identificar debilidades en los sistemas Windows.

Se inicia capturando información sobre los sistemas Windows ejecutando un escaneo inicial.

1. Ejecutar escaneos básicos para encontrar cuales puertos están abiertos en cada sistema Windows

2. Realizar enumeración del sistema operativo (como escanear por compartidos y versión específica del sistema operativo), utilizando herramientas todo en uno.

3. Determinar potenciales vulnerabilidades de seguridad

NetBIOS

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Se puede obtener información de Windows estimulando con las funciones y programas NetBIOS (Network Basic Input/Output System). NetBIOS permite a las aplicaciones hacer llamadas de red y comunicarse con otros hosts dentro de la LAN.

- Puertos UDP para navegación de red: 137 y 138
- Puertos TCP para SMB (Server Message Block): 139 y 445

Los siguientes “Hacks” pueden ser realizados contra sistemas Windows no protegidos ejecutando NetBIOS.

- Enumeración sin autenticar
- Compartidos

Detectar sesiones Nulas

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Una bien conocida vulnerabilidad dentro de Windows puede mapear una conexión anónima (o sesión nula), hacia un compartido oculto llamado IPC$ (Comunicación Interproceso). Este método de ataque puede ser utilizado para:

- Obtener información sobre la configuración del host Windows, como IDs de usuarios y nombres de compartidos
- Editar partes del registro de la computadora remota

Aunque Windows Server 2008 en adelante, como también desde Windows 7, no se permiten conexiones nulas por defecto. Aunque se puede configurar esto, aunque también se deberá deshabilitar el firewall de Windows, para esta vulnerabilidad cause problemas en la red.

Las más recientes versiones de Windows son más seguras comparados con sus predecesores, pero no se debe asumir todo está bien en el mundo de Windows.

Mapear

Para mapear una sesión nula se puede puede utilizar el comando “net”.

- El comando “net” requiere algunos parámetros.
- “net” seguido de “use”
- La dirección IP o nombre del host del sistema a mapear una conexión nula
- Una contraseña y nombre de usuario en blanco

Luego para confirma la sesión ha sido mapeada utilizar el comando “net” seguido de “use”.

Obtener información

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Con una conexión nula, se puede utilizar otras utilidades para obtener remotamente información crítica de Windows. Docenas de herramientas pueden obtener este tipo de información.

Con esta información obtenida se puede intentar lo siguiente:

- Romper las contraseñas de los usuarios encontrados.
- Mapear unidades de compartidos de red de las computadoras

Se pueden utilizar las siguientes aplicaciones para enumerar el sistema contra versiones de Windows anteriores a Server 2003 y Windows XP.

- Net view
- Winfo
- Dumpsec

* http://www.ntsecurity.nu/toolbox/winfo/
* https://www.systemtools.com/somarsoft/

Medidas correctivas contra las sesión nula

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Es una buena decisión para la empresa, actualizar hacia sistemas operativos más seguros, como Windows Server 2012 en adelante, como también a versiones de Windows 8 en adelante, los cuales no tienen las vulnerabilidades mencionadas.

- Bloquear NetBIOS en el servidor Windows, previniendo estos puertos TCP pasen a través del firewall de la red o personal
- Deshabilitar compartidos de archivos e impresión de redes Microsoft, para aquellos sistema en los cuales no se necesite
- Restringir conexiones anónimas hacia el sistema

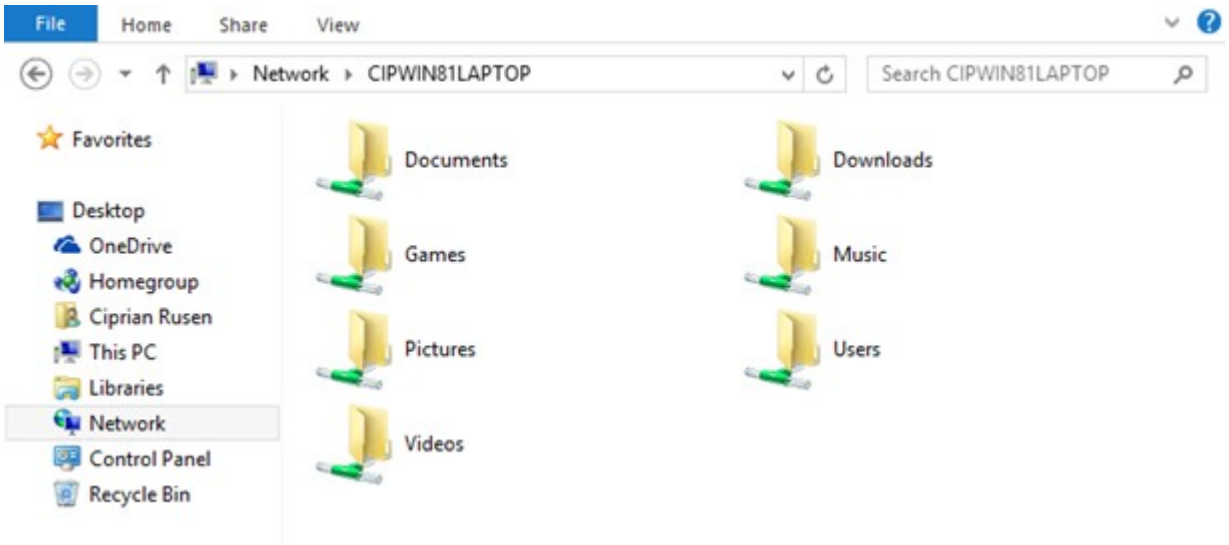
La alta seguridad puede crear problemas para la comunicación con el controlador de dominios y navegación en la red, razón por la cual se debe ser muy cuidadoso.

Verificar permisos de compartidos

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Los compartidos de Windows son las unidades de red disponibles cuando los usuarios navegan por la red Windows. Los compartidos de Windows están frecuentemente mal configurados, permitiendo a más personas tenga acceso del cual deberían.

Un navegador causal puede explotar esta vulnerabilidad de seguridad, pero un interno malicioso ganando acceso no autorizado hacia un sistema Windows, puede resultar en consecuencias serias de seguridad y cumplimiento, incluyendo fuga de información sensible, e incluso daño o borrado de archivos críticos.



Defectos en Windows

Los permisos compartidos por defecto dependen de la versión del sistema Windows.

Windows 2000/NT

Cuando se crean compartidos, el grupo “everyone” tiene completo acceso de control en el compartido por defecto para todos los archivos, como navegar, leer, y escribir.

Windows XP y posteriores

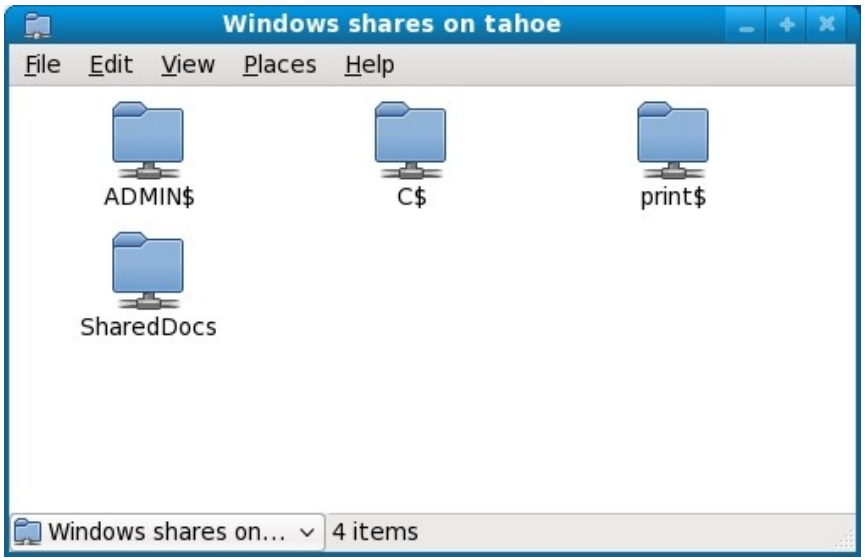
El grupo “everyone” tiene únicamente acceso de lectura a los compartidos.

Los permisos compartidos son diferentes de los permisos de los archivos. Cuando se crean compartidos se deben definir ambos.

Pruebas

Evaluar los permisos de los compartidos es una buena manera de obtener una vista global de quien accede hacia que. Esta prueba muestra cuan vulnerable pueden ser los compartidos de red e información sensible. Se puede encontrar compartidos con permisos por defecto, y accesos innecesarios habilitados.

La mejor manera de probar por debilidades en compartidos es autenticarse en el sistema Windows, mediante un usuario estándar local o del dominio, sin privilegios especiales, y ejecutar un programa para la enumeración, y así poder ver quien accede hacia que.



Explotar parches ausentes

Una cosa es estimular y presionar a Windows para encontrar vulnerabilidades, los cuales pueden conducir a algo de buena información, podría ser acceso hacia el sistema. Sin embargo, es otra cosa distinta encontrar una vulnerabilidad la cual proporcionará acceso completo al sistema, y todo en diez minutos. Esta no es una amenaza vacía para alguien ejecute “código arbitrario” en un sistema, el cual conduzca hacia la explotación de una vulnerabilidad. Con una herramienta como Metasploit, todo lo necesario es un parche ausente para ganar acceso, y demostrar como la red completa puede ser comprometida. Un parche ausente es una mina de oro para un atacante.

Incluso con todas las políticas escritas de seguridad, y las sofisticadas herramientas para la gestión de parches, en cada red se puede encontrar parches ausentes. Puede haber una razón para esto, como los falsos positivos de los escáneres de vulnerabilidades, o los parches ausentes se consideran de un riesgo aceptable. Incluso si se cree todos los sistemas tienen instalados los últimos parches, se debe estar seguro. “Confiar, pero verificar”.

Utilizar Metasploit Framework

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Después de encontrar vulnerabilidades, el siguiente paso es explotarlas. Para este propósito puede ser utilizado Metasploit Framework; el cual es una herramienta open source o de fuente abierta mantenida por Rapid7. Permite realizar diversas acciones aparte de explotar las vulnerabilidades encontradas.

Explotado el sistema, se pueden realizar diversas acciones denominadas como de “post-explotación”, como realizar capturas de pantalla, añadir usuarios con privilegios de administrador, activar servicios adicionales para realizar conexiones remotas visuales, también se tiene la capacidad de borrar o eliminar las huellas de muchas acciones realizadas.

Existen diversas versiones de Metasploit, las cuales se puede considerar usar libremente o comprar, en caso se requieran ciertas funcionalidades.

* https://www.rapid7.com/products/metasploit/

Medidas correctivas explotación de vulnerabilidades de parches

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Se debe parchar los sistemas, ya sea del sistema operativo Windows y cualquier aplicación Microsoft o de un tercero ejecutándose. Resulta más fácil decirlo a hacerlo. Esto debe ser combinado con otras recomendaciones para el fortalecimiento, y de esta manera asegurar mejor el sistema Windows.

Estos procesos de parchado pueden ser automatizados. Es factible utilizar WSUS (Windows Server Update Services) para parchar de manera centralizada.

Tener en consideración gestionar las actualizaciones de las aplicaciones de terceros, como Adobe, Java, etc. Para este propósito existen también herramientas comerciales.

* https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus
* https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard
* https://www.ivanti.com/products/endpoint-security

Ejecutar escaneos autenticados

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Otra prueba la cual se puede ejecutar contra los sistemas Windows es un escaneo “autenticado”, esencialmente buscando por vulnerabilidades como un usuario fiable. Este tipo de pruebas son muy beneficiosas, pues frecuentemente encuentran problemas en el sistema muy relevantes, e incluso debilidades de seguridad operacional (como un pobre cambio en los procesos de gestión, gestión débil de parches, y ausencia de clasificación de información), la cual no podría ser descubierta de otra manera.

Un interno confiable quien tiene acceso físico hacia la red y las herramientas correctas, puede incluso explotar vulnerabilidades más fácilmente. Esto es especialmente cierto si no existen listas de control de acceso interno, o IPSs implementados, ni tampoco mecanismos antimalware.

Una manera para buscar por debilidades en Windows mientras se está autenticado, es utilizado algún escáner de vulnerabilidades, definiendo credenciales de un usuario en el sistema.

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Webinar Gratuito
Windows

Alonso Eduardo Caballero Quezada

Consultor e Instructor en Hacking Ético y Forense Digital
e-mail: ReYDeS@gmail.com

Sitio web: http://www.mile-sec.com
Correo: capacitacion@mile-sec.com

Febrero 2019