Microsoft Security
Workshop Implementing PowerShell
Security Best Practices

Introducido en 2006, Windows PowerShell es un lenguaje de secuencias de comandos, un shell de línea de comandos y una plataforma de secuencias de comandos basada en Microsoft .NET Framework. A pesar de la designación de secuencias de comandos, Windows PowerShell presenta una variedad de características comunes para los lenguajes de programación, incluida su naturaleza orientada a objetos, extensibilidad, sintaxis similar a C # y la capacidad de interactuar directamente con clases .NET, sus propiedades y métodos.

El objetivo principal de Windows PowerShell era ayudar a los profesionales de TI y usuarios avanzados a controlar y automatizar la administración del sistema operativo Windows y las aplicaciones que se ejecutan en Windows.

Para aprovechar los beneficios que ofrece Windows PowerShell y, al mismo tiempo, minimizar los riesgos relacionados con la seguridad, es fundamental comprender los aspectos principales de la seguridad operativa de Windows PowerShell. Otro aspecto que es fundamental considerar en el contexto de este curso es el papel de Windows PowerShell en las vulnerabilidades de seguridad.

Este taller ofrece debates y formación práctica para PowerShell. aprenderá sobre los fundamentos de PowerShell, incluido su diseño arquitectónico, sus ediciones y versiones, y los conceptos básicos de la interacción con PowerShell.

Luego, explorará las técnicas basadas en Windows PowerShell más comunes empleadas por los piratas informáticos para aprovechar el acceso existente a un sistema operativo Windows para facilitar la instalación de software malicioso, realizar tareas de reconocimiento, establecer su persistencia en la computadora de destino y promover el movimiento lateral. . También revisará algunas de las herramientas de seguridad basadas en Windows PowerShell que facilitan las pruebas de penetración, el análisis forense y la ingeniería inversa de las vulnerabilidades de Windows PowerShell. Para concluir el curso, proporcionará un resumen de las tecnologías recomendadas por Blue Team que están orientadas a implementar una seguridad integral y de defensa en profundidad contra los ataques basados en Windows PowerShell.

Este taller es parte de una serie más amplia de talleres ofrecidos por Microsoft sobre la práctica de la seguridad. Si bien no es necesario que haya completado ninguno de los otros cursos de la serie Security Workshop antes de realizar este taller, se recomienda encarecidamente que comience con el primer curso de la serie, Microsoft Security Workshop: Enterprise Security Fundamentals.

• 40551: Taller de seguridad de Microsoft: Fundamentos de seguridad empresarial.
• 40552: Taller de seguridad de Microsoft: Gestión de identidad.

• 40553: Taller de seguridad de Microsoft: Planificación de una empresa segura: mejora de la detección.
• 40554: Taller de seguridad de Microsoft: Implementación de características de seguridad de Windows 10.
• 40555: Taller de seguridad de Microsoft: Implementación de las mejores prácticas de seguridad de PowerShell.

Perfil de audiencia

Este curso está dirigido a profesionales de TI que requieren una comprensión más profunda de las características y vulnerabilidades de seguridad de Windows PowerShell y para aumentar su nivel de conocimiento a través de una experiencia predominantemente práctica en la implementación de características de seguridad de Windows PowerShell.

Prerrequisitos

Además de su experiencia profesional, los estudiantes que realicen esta formación ya deben tener los siguientes conocimientos técnicos:

• Una buena base para acceder y utilizar comandos sencillos de Windows PowerShell.
• El ecosistema de ciberseguridad actual.
• Experiencia en administración, mantenimiento y resolución de problemas de clientes y servidores de Windows.
• Experiencia básica y comprensión de las tecnologías de red de Windows, para incluir la configuración de red del Firewall de Windows, DNS, DHCP, WiFi y conceptos de servicios en la nube.
• Experiencia básica y comprensión de Active Directory, incluidas las funciones de un controlador de dominio, servicios de inicio de sesión y comprensión de la política de grupo.
• Conocimiento y experiencia relevante en administración de sistemas, utilizando Windows 10.

Los estudiantes que toman esta capacitación pueden cumplir con los requisitos previos al obtener conocimientos y habilidades equivalentes a través de la experiencia práctica como administrador de seguridad, administrador del sistema o administrador de red. Los alumnos deben tener una buena base para acceder y utilizar comandos sencillos de Windows PowerShell. Este conocimiento se puede obtener en INF210x, Conceptos básicos de Windows PowerShell.
Al finalizar el curso.
Después de completar este curso, los estudiantes podrán:

• Proporcionar una descripción general de Windows PowerShell.
• Describir las ediciones y versiones de PowerShell.
• Instale y use Windows PowerShell y PowerShell Core.
• Gestionar la ejecución de scripts de PowerShell locales.
• Administrar la ejecución remota de Windows PowerShell.
• Gestionar la ejecución remota de PowerShell Core.
• Describir las implicaciones de seguridad del uso del modo de lenguaje restringido.
• Describir la arquitectura y los componentes de Windows PowerShell DSC.

• Recomendar la configuración de registro y auditoría de Windows PowerShell.
• Proporcione ejemplos de ataques basados en Windows PowerShell.
• Utilice herramientas de seguridad basadas en Windows PowerShell.
• Proporcionar una descripción general de las tecnologías relacionadas con la seguridad basadas en Windows PowerShell.
• Implementar el registro de Windows PowerShell mediante la configuración de estado deseado (DSC).
• Identificar y mitigar las vulnerabilidades basadas en Windows PowerShell.
• Implementar una administración suficiente (JEA).

Temario

Módulo 1: Fundamentos de PowerShell

Introducido en 2006, Windows PowerShell es un lenguaje de secuencias de comandos, un shell de línea de comandos y una plataforma de secuencias de comandos basada en Microsoft .NET Framework. A pesar de la designación de secuencias de comandos, Windows PowerShell presenta una variedad de características comunes para los lenguajes de programación, incluida su naturaleza orientada a objetos, extensibilidad, sintaxis similar a C # y la capacidad de interactuar directamente con clases .NET, sus propiedades y métodos. El objetivo principal de Windows PowerShell era ayudar a los profesionales de TI y usuarios avanzados a controlar y automatizar la administración del sistema operativo Windows y las aplicaciones que se ejecutan en Windows. Con la introducción de .NET Core en 2016, Microsoft extendió el alcance de PowerShell a otras plataformas de sistemas operativos, lo que llevó a un proyecto de código abierto alojado en GitHub, llamado PowerShell Core. Puede usar PowerShell Core en macOS 10.12, una variedad de distribuciones de Linux de 64 bits, además del sistema operativo Windows de 32 y 64 bits, incluido Windows 10 que se ejecuta en dispositivos de Máquina de Computación con Conjunto de Instrucciones Reducido Avanzado (ARM). En este módulo, aprenderá sobre los fundamentos de PowerShell, incluido su diseño arquitectónico, sus ediciones y versiones, y los conceptos básicos de la interacción con PowerShell.

• Descripción general de Windows PowerShell.
• Ediciones y versiones de PowerShell.
• Ejecución de PowerShell.

Módulo 2: Seguridad operativa de PowerShel

Para aprovechar los beneficios que ofrece Windows PowerShell y, al mismo tiempo, minimizar los riesgos relacionados con la seguridad, es fundamental comprender los aspectos principales de la seguridad operativa de Windows PowerShell. En este módulo, aprenderá a mejorar la seguridad del sistema operativo aprovechando las características y tecnologías integradas de Windows PowerShell que forman parte del entorno operativo de Windows PowerShell. Otro aspecto que es fundamental considerar en el contexto de este módulo es el papel de Windows PowerShell en las vulnerabilidades de seguridad. Según datos empíricos, en la mayoría de los casos, Windows PowerShell se utiliza como herramienta de posexplotación. Esto implica que,

en el punto en el que se inicia una sesión de Windows PowerShell, un atacante ya obtuvo acceso al contexto de seguridad en el que opera el sistema de destino o el usuario de destino. Este es el tipo de escenario en el que se enfocará este módulo. En este caso, Windows PowerShell sirve como motor potente y extremadamente flexible para ejecutar tareas arbitrarias en las computadoras locales y remotas, lo que, dicho sea de paso, es la misma razón que hizo que Windows PowerShell fuera extremadamente popular entre los administradores de sistemas. Obviamente, existen otros tipos de ataques que dependen de Windows PowerShell para obtener acceso no autorizado a un sistema de destino. En este tipo de escenario, Windows PowerShell sirve como herramienta de explotación. Exploraremos este tipo de ataques en el último módulo de este curso.

- Gestión de la ejecución de scripts locales.
- Administrar las capacidades de ejecución remota de Windows PowerShell.
- Administrar las capacidades de ejecución remota de PowerShell Core.
- Modo de idioma.

Módulo 3: Implementación de seguridad basada en PowerShell

En el módulo anterior, aprendió acerca de una serie de características relacionadas con la seguridad integradas en Windows PowerShell y tecnologías que forman parte del entorno operativo de Windows PowerShell que lo ayudan con su aplicación. El propósito de este módulo es presentar los métodos más comunes y efectivos de aprovechar Windows PowerShell para mejorar la seguridad del sistema operativo. Estos métodos incluyen:> Protección contra cambios de configuración no deseados confiando en la Configuración de estado deseado (DSC) de PowerShell> Implementación del principio de privilegio mínimo en escenarios de administración remota mediante Just Enough Administration (JEA)> Seguimiento y auditoría de eventos que podrían indicar intentos de explotación por mediante el registro de Windows PowerShell.

- Windows PowerShell DSC.
- Administración suficiente (JEA).
- Auditoría y registro de Windows PowerShell.

Módulo 4: Exploits basados en Windows PowerShell y su mitigación

Las organizaciones no pueden identificar de manera integral las brechas en la detección y respuesta de seguridad centrándose únicamente en las estrategias de prevención de violaciones. Comprender cómo no solo proteger sino también detectar y responder a las infracciones es tan importante, si no más, que tomar medidas para evitar que ocurra una infracción en primer lugar. Al planificar los peores escenarios a través de Red Teaming (ataque y penetración en el mundo real), las organizaciones pueden desarrollar las capacidades necesarias para detectar intentos de explotación y mejorar significativamente las respuestas asociadas con violaciones de seguridad. Red Teaming se ha convertido en una de las partes más esenciales del desarrollo y la seguridad de las plataformas y los servicios de Microsoft. El Equipo Rojo asume el papel de adversarios sofisticados y permite a Microsoft validar y mejorar la seguridad, fortalecer las defensas e impulsar una mayor efectividad de todo el programa de seguridad. Red Teams permite a Microsoft probar la detección y respuesta de infracciones, así

como medir con precisión la preparación y los impactos de los ataques del mundo real. El propósito del Equipo Azul es buscar defensas creativas y confiables para detectar y frustrar los ataques orquestados por el Equipo Rojo. El Equipo Azul está compuesto por un conjunto dedicado de personal de seguridad o miembros de todas las organizaciones de respuesta a incidentes de seguridad, ingeniería y operaciones. Independientemente de su composición, son independientes y operan por separado del Equipo Rojo. El Blue Team sigue los procesos de seguridad establecidos y utiliza las últimas herramientas y tecnologías para detectar y responder a los ataques y la penetración. En este módulo, primero abordaremos la seguridad basada en Windows PowerShell desde la perspectiva del Red Team. Exploraremos las técnicas basadas en Windows PowerShell más comunes empleadas por los piratas informáticos para aprovechar el acceso existente a un sistema operativo Windows para facilitar la instalación de software malicioso, realizar tareas de reconocimiento, establecer su persistencia en la computadora de destino y promover el movimiento lateral. También revisaremos algunas de las herramientas de seguridad basadas en Windows PowerShell que facilitan las pruebas de penetración, el análisis forense y la ingeniería inversa de las vulnerabilidades de Windows PowerShell. Para concluir el módulo y el curso, proporcionaremos un resumen de las tecnologías recomendadas por el Equipo Azul que están orientadas a implementar una seguridad integral y de defensa en profundidad contra los ataques basados en Windows PowerShell. Hay muchas vulnerabilidades documentadas que utilizan las capacidades de Windows PowerShell para llevar a cabo ataques que apuntan a fallas de seguridad presentes en sistemas sin parchear o desactualizados o para expandir lateralmente el alcance de tales ataques una vez que un solo sistema se ve comprometido. Tenga en cuenta que la descripción general de estos exploits presentada en este módulo no pretende ser exhaustiva. Nuestra intención es ilustrar los patrones comunes que siguen tales exploits y resaltar la importancia de una estrategia de defensa integral en profundidad.

- Ataques basados en Windows PowerShell.
- Herramientas de seguridad basadas en Windows PowerShell.
- Resumen de tecnologías relacionadas con la seguridad de Windows PowerShell.
- Labs: implementación de la seguridad de Windows PowerShell.
  - Implementar el registro de Windows PowerShell mediante DSC.
  - Realizar un exploit basado en Windows PowerShell.
  - Implementar la administración suficiente.