

Prueba - Seguridad y administración remota en Windows Server

En esta prueba validaremos nuestros conocimientos de administración remota en Windows Server utilizando PowerShell Remoting, configuración y seguridad de servicios críticos en Server Core, gestión de zonas DNS y asignación de IPs, así como la implementación de medidas de seguridad en la red y firewall.

Para lograrlo, necesitarás aplicar comandos y configuraciones en PowerShell, asegurando el cumplimiento de buenas prácticas de seguridad.

Lee todo el documento antes de comenzar el desarrollo **grupal de máximo tres integrantes**, para asegurarte de tener el máximo de puntaje y enfocar bien los esfuerzos.

Descripción

La empresa GreenApple del comercio, ha contratado tus servicios junto con tu equipo como consultores de sistemas para fortalecer la seguridad de sus servidores Windows Server. Actualmente, cuentan con un entorno de servidores remotos que deben ser configurados y asegurados para permitir una administración eficiente sin comprometer la integridad de los datos.

Tu tarea es implementar un esquema seguro de administración remota, optimizar el uso de PowerShell Remoting y configurar políticas de firewall, gestión de certificados y seguridad en los servicios críticos. Además, deberás garantizar una correcta asignación de IPs y seguridad en la gestión de zonas DNS.

Aplicando los conceptos y herramientas aprendidas hasta ahora, junto a tu equipo deberás realizar las configuraciones necesarias en un entorno Windows Server para demostrar que puedes administrar de manera segura un servidor remoto.

Requerimientos

1. Configuración de PowerShell Remoting seguro

- Configurar PowerShell Remoting en un servidor Windows Server asegurando la autenticación mediante Kerberos o certificados.
- Restringir el acceso a usuarios específicos mediante políticas de seguridad.
- Generar un script en PowerShell (.ps1) con los comandos utilizados y capturas de pantalla del resultado

(3 Puntos)

2. Implementación de seguridad en Server Core y Firewall

- Configurar los servicios críticos (DHCP y DNS) en Server Core, asegurando su correcto funcionamiento y minimizando la superficie de ataque.
- Implementar reglas de firewall para restringir accesos no autorizados mediante Windows Defender Firewall con políticas avanzadas.

(3 Puntos)

3. Gestión segura de zonas DNS y asignación de IPs

- Configurar y asegurar una zona DNS en Windows Server, limitando el acceso a la administración mediante permisos adecuados.
- Implementar una política de asignación de IPs estáticas y dinámicas utilizando DHCP de manera segura.

(4 Puntos)



¡Mucho éxito!

Consideraciones y recomendaciones

Proporcionar un documento PDF con la configuración aplicada y evidencias de su correcta implementación, además de capturas con los comandos utilizados.