Realiza un laboratorio teniendo en cuenta el siguiente entorno.

* Una máquina virtual ejecutara Windows server 2012R2. Esta máquina deberá tener el protocolo SMB habilitado además de tener habilitado la detección de redes y recursos compartidos, de manera que un cliente Windows 7 tenga acceso a estos recursos, asi mismo deberá tener habilitado el escritorio remoto de manera que desde Windows 7 sea posible el acceso remoto al servidor, finalmente deberá tener instalado el rol IIS para dar servicio de servidor web.
* Otra máquina virtual ejecutara Windows 7 profesional o Ultimate. Es importante que esta maquina este en el mismo segmento de red que el servidor. Y también deberá tener habilitado la detección de redes y recursos compartidos de manera que puedan compartir carpetas entre cliente y servidor.
* Una tercera maquina ejecutará kali Linux, la cual será maquina atacante, se emplearán herramientas como NMAP y Metasploit. Con el objetivo de aprovechar la vulnerabilidad eternalblue para realizar un ataque.

**Requisitos de entrega.**

Realizar un documento, donde mostrara, los pasos necesarios con capturas de pantalla que muestre el uso de NMAP y metasploit. El documento debe contener.

* Portada.
* Tabla de contenido.
* Introducción.
* Marco teórico (NMAP, Metasploit, Kali Linux, Windows 7 y server 2012, EternalBlue, vulnerabilidades en Windows).
* Desarrollo del laboratorio. Mostrar evidencias de la implementación del entorno con las tres máquinas. **“IMPORTANTE LAS TRES MAQUINAS DEBEN ESTAR ALOJADAS EN UNA RED INTERNA DE NINGUNA MANERA DEBEN INTERACTUAR CON LA RED LOCAL”.** Mostrar que hay carpetas compartidas y hacen ping entre ellas.
* Mostrar el uso de la herramienta NMAP mínimo 10 ejemplos, mostrar pantalla del resultado y explicar los resultados obtenidos, y como podrían aprovecharse esos resultados para lograr una explotación.
* Mostrar el uso de metasploit para explotar la vulnerabilidad eternalblue en Windows 7.
* Una vez dentro de la sesión investigar, aplicar y mostrar que hace cada uno de los comandos disponibles al ejecutar help en el meterpreter.
* Muestra como explotar alguna de las vulnerabilidades identificadas en el server 2012. Y utiliza keyscan, screenshot y migra el proceso.
* Redacta un párrafo indicando como proteger los sistemas para prevenir este tipo de ataques, asi mismo sugerencias para administradores de sistemas para su prevención.
* Conclusiones.
* Bibliografía.

**Luego de la entrega, cada grupo mostrara en tiempo real el proceso de explotación y uso de meterpreter.**

Actividad de Laboratorio: Explotación de Vulnerabilidades en un Entorno Controlado

# Portada

Incluya:  
- Nombre del cadi  
- Nombre de los integrantes del grupo  
- Fecha de entrega

# Tabla de contenido

Incluya una tabla de contenido automática en Word (Referencias > Tabla de contenido).

# Introducción

Breve descripción del propósito del laboratorio y la importancia de comprender las vulnerabilidades en sistemas operativos.

# Marco teórico

Defina y explique los siguientes conceptos:

- Nmap  
- Metasploit  
- Kali Linux  
- Windows 7 y Windows Server 2012  
- EternalBlue  
- Vulnerabilidades comunes en sistemas Windows

# Desarrollo del laboratorio

Incluya evidencias de la implementación del entorno con las tres máquinas virtuales:  
- Windows Server 2012 R2 (Servidor)  
- Windows 7 Profesional/Ultimate (Cliente)  
- Kali Linux (Atacante)  
  
Debe mostrar que existen carpetas compartidas y que las máquinas se comunican entre sí mediante ping.  
IMPORTANTE: Todas las máquinas deben estar en una RED INTERNA, sin conexión a la red local o internet.

# Uso de Nmap

Presente mínimo 10 ejemplos de comandos de Nmap. Para cada comando incluya:  
- El comando utilizado.  
- Captura de pantalla del resultado.  
- Explicación de los resultados obtenidos.  
- Cómo podrían aprovecharse esos resultados para planificar una explotación.

# Uso de Metasploit

Documente paso a paso el proceso de explotación de la vulnerabilidad EternalBlue en Windows 7.  
  
Una vez obtenida la sesión de Meterpreter:  
- Investigue y explique el funcionamiento de los comandos disponibles al ejecutar 'help'.

# Explotación en Windows Server 2012 R2

Identifique una vulnerabilidad en el servidor Windows Server 2012 R2.  
Muestre paso a paso el proceso de explotación, incluyendo capturas y evidencia.

- Demuestre el uso de los comandos keyscan, screenshot y migrates.

# Recomendaciones de seguridad

Redacte un párrafo con estrategias para proteger los sistemas y prevenir este tipo de ataques. Incluya sugerencias para administradores de sistemas sobre buenas prácticas de seguridad.

# Conclusiones

Redacte las conclusiones sobre el aprendizaje y experiencias obtenidas durante el laboratorio.

# Bibliografía

Incluya las fuentes consultadas, siguiendo el formato APA.