Meterpreter

23/11/2023

Guillermo Bellettini
Seguridad
Creado por: Nicolas Pavel Ballesteros Barrado

Contenido

¿Que es meterpreter?

Es un intérprete de comandos avanzado dentro del marco de Metasploit que se utiliza para realizar operaciones post-explotación en sistemas comprometidos.

¿Que es un Payload?

Es un fragmento de código malicioso que se entrega a la víctima durante un ataque. En Metasploit, el payload suele ser la carga útil de un exploit.

¿Que es un exploit?

Es un fragmento de código o técnica que aprovecha una vulnerabilidad en un sistema con el objetivo de ejecutar código malicioso o lograr un comportamiento no deseado.

Escriba las funciones que pueden realizar los llamados "modulos Auxiliares"

Realizan funciones diversas en Metasploit, como escaneo de puertos, recopilación de información o servicios básicos, sin aprovechar una vulnerabilidad específica.
Algunas de las funciones comunes incluyen:

Escaneo de Puertos: Identificar los puertos abiertos en un sistema o rango de direcciones IP.

Recopilación de Información: Obtener información sobre el sistema objetivo, como versiones de servicios, banners, y detalles de configuración.

Ataques de Fuerza Bruta: Realizar ataques de fuerza bruta para probar la fortaleza de contraseñas o credenciales débiles.

Ataques de Denegación de Servicio (DoS): Generar tráfico malicioso para evaluar la resistencia del sistema ante ataques DoS.

Explotación de Vulnerabilidades Comunes: Identificar y explotar vulnerabilidades conocidas en servicios y aplicaciones.

Manipulación de Archivos y Datos: Realizar operaciones como descarga, carga, y manipulación de archivos en el sistema objetivo.

Interacción con Servicios de Red: Interactuar con servicios de red, como SMTP, HTTP, FTP, para evaluar su seguridad.

Inyección de Paquetes: Enviar paquetes personalizados a través de la red para evaluar la seguridad de los protocolos.

Pruebas de Credenciales: Verificar la autenticación y autorización mediante pruebas de credenciales.

Ataques de Red: Realizar escaneo y descubrimiento de hosts en una red para evaluar su seguridad.

¿En que consiste un encoder?

Es una función en Metasploit que transforma el código de la carga útil (payload) de manera que mantenga su funcionalidad mientras evita detecciones de antivirus o intrusiones.