enero, 2024

Elementos esenciales de Metasp

todo lo que necesitas

grupo de visión

akash basfor

Explotación:

Comando: `use exploit/[nombre_exploit]`

Descripción: Selecciona un módulo de exploit para una vulnerabilidad específica.

Táctica: identificar las vulnerabilidades objetivo y elegir los exploits adecuados.

Generación de carga útil:

Comando: `generar -t [tipo_carga útil]` Descripción: Genera una carga útil para varias plataformas.

Táctica: cree cargas útiles personalizadas para evasión y objetivos específicos

Post-Explotación:

Comando: `post/multi/manage/shell_to_meterpreter` Descripción: Transforma una sesión de shell en una sesión de Meterpreter más potente.

Táctica: actualice a Meterpreter para obtener capacidades avanzadas posteriores a la explotación.

Movimiento lateral:

Comando: ` use post/windows/manage/psexec `

Descripción: Ejecuta comandos en sistemas Windows remotos usando PsExec.

Táctica: moverse lateralmente dentro de una red aprovechando las credenciales existentes.

Explotar la integración de la base de datos:

Comando: `db_import [path_to_nmap_results]` Descripción: Importa los resultados del escaneo de Nmap a la base de datos de Metasploit

Táctica: aprovechar la base de datos para una explotación específica y eficiente.

Secuencias de comandos de recursos:

Comando: `recurso [script_path]`

Descripción: Ejecuta una serie de comandos de Metasploit desde un script.

Táctica: Automatizar tareas repetitivas y escenarios de ataque complejos.

Evasión AV:

Comando: `generar -t [tipo_carga útil] -e [codificador]` Descripción: Codifica cargas útiles para evadir la detección antivirus.

Táctica: eludir las medidas de seguridad ofuscando las cargas útiles.

Fuerza bruta:

Comando: ` utilizar auxiliar/escáner/ssh/ssh_login `

Descripción: Credenciales SSH de fuerza bruta utilizando una lista de palabras específica

Táctica: obtener acceso no autorizado mediante la adivinación de credenciales

Explotación del lado del cliente:

Comando: ` use exploit/windows/browser/[exploit_name]`

Descripción: Apunta a vulnerabilidades del lado del cliente en navegadores web.

Táctica: explotar las interacciones del usuario para obtener acceso.

Pivotando:

Comando: `set route [subred] [session_id]`

Descripción: permite el enrutamiento a través de un host comprometido para llegar a otras subredes.

Táctica: Mantener el acceso y moverse lateralmente a través de redes segmentadas.

Recopilación de pruebas:

Comando: `post/multi/gather/arp_scanner`

Descripción: Recopila tablas ARP de hosts comprometidos.

Táctica: recopilar información de la red para su posterior análisis.

Informes:

Comando: `db_export -f [formato] -a [ruta]`

Descripción: Exporta resultados de escaneo y explota datos de la base de datos Metasploit.

Táctica: Preparar informes completos para las partes interesadas.

Suplantación de DNS:

Comando: ` use auxiliar/spoof/dns/nbns_response ` Descripción: Falsifica las respuestas del Servicio de nombres NetBIOS (NBNS).

Táctica: Redirigir el tráfico para robo de credenciales o ataques de intermediario.

Pruebas de aplicaciones web:

Descripción: use auxiliar/scanner/http/dir_scanner ` Comando: `
Busca directorios en un servidor web.

Táctica: Identificar rutas ocultas y posibles vulnerabilidades en aplicaciones web

Explotación de bases de datos:

Comando: `use auxiliar/escáner/mssql/mssql_login `

Descripción: Credenciales de MS SQL Server de fuerza bruta.

Táctica: explotar las debilidades en la seguridad de la base de datos.

Integración del kit de herramientas de ingeniería social:

Comando: ` use auxiliar/spoof/phishing_set`

Descripción: Se integra con el kit de herramientas de ingeniería social para campañas de phishing.

Táctica: simular ataques de ingeniería social del mundo real.

Explotación de redes inalámbricas:

Comando: ` use auxiliar/scanner/wifi/wifi_login ` Descripción: Intenta descifrar contraseñas de Wi-Fi.

Táctica: Obtener acceso no autorizado a redes inalámbricas.

Explotación de formatos de archivos:

Comando: `use exploit/windows/fileformat/[exploit_name]` Descripción: explota vulnerabilidades en formatos de archivo (por ejemplo, PDF, documentos de Office).

Táctica: Apuntar a los usuarios a través de archivos maliciosos.

Olfateo de credenciales

Comando: `use post/windows/gather/credentials/gpp` Descripción: Extrae contraseñas en texto plano de las Preferencias de directiva de grupo (GPP).

Táctica: recuperar las credenciales almacenadas para el lateral movimiento.

Secuencias de comandos de Meterpreter:

Comando: `meterpreter > run post/windows/manage/killav` Descripción: Ejecuta scripts de Meterpreter para tareas específicas (por ejemplo, deshabilitar antivirus).

Táctica: Automatizar acciones post-explotación.

Cargas útiles de PowerShell:

Comando: `use exploit/windows/local/payload` Descripción: Genera cargas útiles para la explotación de PowerShell.

Táctica: Explotar sistemas Windows usando PowerShell.

Explotación de dispositivos IoT:

Comando: `use exploit/linux/iot/[nombre_exploit]` Descripción: apunta a vulnerabilidades en dispositivos de Internet de las cosas (IoT).

Táctica: explotar la seguridad débil en los ecosistemas de IoT.

Reconocimiento de objetivos automatizado:

Comando: `use auxiliar/scanner/http/ssl_certificate` Descripción: Recopila información del certificado SSL de los servidores web.

Táctica: Automatizar el reconocimiento de vulnerabilidades SSL/TLS.

Antiforense:

Comando: ` use post/windows/manage/timestomp ` Descripción: Modifica las marcas de tiempo de los archivos para evadir el análisis forense.

Táctica: Cubrir huellas durante y después de la explotación.

Omitir UAC (Control de cuentas de usuario):

Comando: ` use exploit/windows/local/bypassuac ` Descripción:

Explota vulnerabilidades para evitar UAC en sistemas Windows.

Táctica: Eleve los privilegios y ejecute código con permisos más altos.

Suplantación de tokens:

Comando: `use incognito`

Descripción: Proporciona comandos para la manipulación de tokens y la escalada de privilegios.

Táctica: imitar a los usuarios con mayores privilegios para el movimiento lateral.

Explotando MS17-010 (EternalBlue):

Comando: ` use exploit/windows/smb/ms17_010_eternalblue `

Descripción: Explota la vulnerabilidad EternalBlue para la ejecución remota de código en sistemas Windows.

Táctica: Apunte a sistemas Windows sin parches para lograr un compromiso rápido.

Servicios de huellas dactilares:

Comando: ` usar auxiliar/escáner/huella digital/[servicio]`

Descripción: Servicios de toma de huellas dactilares para recopilar información sobre sus versiones y configuraciones.

Táctica: comprender los servicios de destino para una explotación precisa.

Recolección de credenciales automatizada:

Descripción: use post/windows/gather/credentials ` Comando: `

Recopila credenciales de sistemas Windows comprometidos.

Táctica: recopilar contraseñas para movimientos laterales y escalada de privilegios.

Desciframiento de contraseñas automatizado:

Comando: `use auxiliar/analyze/jtr_crack_fast` Descripción:

Analiza la salida de John the Ripper para descifrar hashes de contraseñas.

Táctica: descifrar hashes de contraseñas para acceder a credenciales.

Explotación de vulnerabilidades de aplicaciones web

Comando: `use exploit/multi/http/[exploit_name]` Descripción:

Apunta a vulnerabilidades en aplicaciones web.

Táctica: Explotar las debilidades de los servicios web para acceso no autorizado.

Evasión AV con Veil-Framework:

Comando: `use evasion/windows/` Descripción:

Genera cargas útiles con Veil-Framework para evadir la detección antivirus.

Táctica: mejorar la ofuscación de la carga útil para obtener mejores tasas de éxito.

Enumeración SNMP:

Comando: ` use auxiliar/scanner/snmp/snmp_enum `

Descripción: Enumera información de dispositivos habilitados para SNMP.

Táctica: recopilar detalles para el mapeo de la red y posibles vulnerabilidades.

Integración WiFi Piña:

Comando: ` use auxiliar/gather/wifi/pineapple `

Descripción: Se integra con WiFi Pineapple para reconocimiento de redes inalámbricas.

Táctica: recopilar información sobre redes WiFi y dispositivos conectados.

Explotación de VoIP

Comando: `use auxiliar/voip/`

Descripción: Explota las vulnerabilidades en los sistemas de voz sobre IP (VoIP).

Táctica: Apuntar a las debilidades en la infraestructura de comunicación.

Instrumental de administración de Windows (WMI) Explotación:

Comando: `use exploit/windows/wmi/`

Descripción: Explota las vulnerabilidades utilizando el Instrumental de administración de Windows.

Táctica: Aprovechar WMI para actividades posteriores a la explotación.