Technical Guide:
Hacking IIS

Advanced techniques for exploiting IIS servers

Iron CyberSec

Checklist IIS Audit

Checklist de Técnicas para explotación de Internet Information Services

1. IIS Shortname Enumeration

- **Descripción**: Permite enumerar nombres cortos de archivos y directorios en servidores IIS vulnerables, explotando una característica de compatibilidad con sistemas antiguos.
- **Uso**:
  - Usar herramientas como Shortscan para identificar nombres cortos.
  - Realizar fuzzing lógico con herramientas como FFUF, utilizando patrones como `LIDSFUZZ` para descubrir nombres completos.
  - Ejemplo práctico: Si se detectan nombres como `ASPNET~1`, se pueden probar variantes completas como `ASPNET_CLIENT`.

---

2. VIEWSTATE Deserialization RCE

- **Descripción**: Explotación de la deserialización insegura del VIEWSTATE en aplicaciones ASP.NET para lograr ejecución remota de código (RCE).
- **Uso**:
  - Extraer claves `machineKey` (validationKey y decryptionKey) del archivo `web.config`.
  - Generar VIEWSTATE maliciosos con herramientas como Viewgen o YSoSerial.Net.
  - Si se tiene acceso al archivo `web.config`, es posible manipular el VIEWSTATE para ejecutar código arbitrario en el servidor.

---

3. Web.config Upload Tricks

- **Descripción**: Subir un archivo `web.config` malicioso para alterar el comportamiento del servidor.
- **Uso**:
  - Identificar puntos de carga de archivos que no validen correctamente los tipos permitidos.
  - Crear un archivo `web.config` que habilite funcionalidades maliciosas, como ejecutar scripts o redirigir solicitudes.

---

4. Debug Mode con Stack Traces Detallados

- **Descripción**: Explotar el modo de depuración para extraer información sensible como rutas completas o detalles del sistema.
- **Uso**:
  - Analizar los mensajes de error generados por la aplicación cuando está en modo debug.

- Extraer información útil, como rutas de archivos, configuraciones del servidor o dependencias utilizadas.

---

5. ELMAH y Trace Debugging Scripts

- **Descripción**: Examinar registros detallados generados por herramientas como ELMAH o Trace.
- **Uso**:
  - Buscar endpoints como `/elmah.axd` o `/trace.axd` que puedan exponer registros detallados del sistema, incluyendo excepciones y configuraciones.

---

6. Telerik RCE

- **Descripción**: Explotar vulnerabilidades conocidas en componentes Telerik, como CVE-2019-18935, para lograr RCE.
- **Uso**:
  - Identificar versiones vulnerables del componente Telerik UI.
  - Utilizar exploits específicos disponibles públicamente para explotar la vulnerabilidad.

---

7. VHost Hopping

- **Descripción**: Descubrir aplicaciones internas en servidores IIS mediante enumeración de nombres virtuales (VHosts).
- **Uso**:
  - Realizar fuerza bruta sobre subdominios utilizando herramientas como Burp Suite Intruder.
  - Mapear subdominios descubiertos al IP correspondiente en el archivo `/etc/hosts`.
  - Ejemplo práctico: Descubrir un subdominio interno (`mssql.company.com`) que aloje un administrador de base de datos solo accesible internamente.

---

8. Local File Disclosure (LFD)

- **Descripción**: Acceder a archivos locales del servidor explotando rutas relativas.
- **Uso**:
  - Probar rutas como `../../web.config`, `../../global.asax` o `../../bin/Company.Web.Api.dll`.
  - Extraer información sensible o DLLs para análisis posterior.

---

9. Análisis de Código Fuente con DNSpy

- **Descripción**: Revertir ensamblados (.DLL) a código fuente utilizando DNSpy.
- **Uso**:
  - Descargar y usar DNSpy para cargar DLLs obtenidas desde servidores vulnerables y analizar su código fuente.

- Identificar vulnerabilidades específicas dentro del código revertido.

---

10. XXE (XML External Entity) con DTD Locales

- **Descripción**: Explotar vectores XXE usando entidades externas definidas localmente.
- **Uso**:
  - Crear un archivo XML malicioso que cargue DTDs locales, como `cim20.dtd`.
  - Leer archivos sensibles (como `web.config`) mediante fragmentos parciales filtrados a través de errores en identificadores.

---

11. Resolución del Error HTTPAPI 2.0 "404 Not Found"

- **Descripción**: Resolver errores HTTPAPI al interactuar con activos IIS que requieren un encabezado Host específico.
- **Uso**:
  - Configurar el archivo `/etc/hosts` para mapear el nombre correcto al IP correspondiente.
  - Realizar fuerza bruta sobre VHosts si no se conoce el subdominio exacto.
  - Ejemplo práctico: Ajustar el encabezado Host para acceder a aplicaciones internas que inicialmente devuelven un error "404 Not Found".

---

12. Local File Disclosure hacia RCE

- **Descripción**: Escalar desde la divulgación de archivos locales hasta la ejecución remota de código mediante deserialización insegura.
- **Uso**:
  - Leer el archivo `web.config` para obtener claves críticas (`machineKey`).
  - Generar VIEWSTATE maliciosos con herramientas como Viewgen o YSoSerial.Net.

---

13. Fuzzing Lógico con IIS Shortnames

- **Descripción**: Realizar fuzzing lógico sobre resultados obtenidos mediante enumeración de nombres cortos.
- **Uso**:
  - Usar patrones específicos con herramientas como FFUF para descubrir nombres completos basados en las salidas iniciales (`ASPNET~1` → `ASPNET_CLIENT`).

Este checklist detalla cada técnica mencionada en el documento, proporcionando explicaciones claras y ejemplos prácticos basados en los contextos descritos.