PATRONES DE SEGURIDAD Y AUTENTICACIÓN · MÓDULO 2

Autenticación integrada de IIS y del navegador

Guía de la lección · Guía del laboratorio / examen

LearnWisej

Guía de la lección

Elegir el límite del sitio IIS, los proveedores de la autenticación de Windows y el orden de los desafíos, la negociación del navegador y la directiva de intranet, los SPN, la evidencia de Kerberos, la protección extendida y los proxies, y diagnosticar un fallo por capas. Qué significa esto para un desarrollador que protege los caminos de inicio de sesión, identidad y autorización de una aplicación Wisej.NET en producción — y cómo leer este módulo.

Enfoque de producción

Elegir el límite del sitio IIS, los proveedores de la autenticación de Windows y el orden de los desafíos, la negociación del navegador y la directiva de intranet, los SPN, la evidencia de Kerberos, la protección extendida y los proxies, y diagnosticar un fallo por capas.

1. El problema en producción

El personal abre la ruta de la intranet de AccessOps y espera iniciar sesión en silencio con su cuenta de Windows, mientras que los socios llegan a una página pública de inicio de sesión que nunca debe pedirles credenciales de Windows. Cuando el inicio de sesión silencioso falla, el síntoma es un aviso, un bucle de 401 o una página de error, y la causa está en IIS, el navegador, el directorio o un proxy antes de que se ejecute ningún código de Wisej.NET. Este módulo te enseña a configurar ese límite del host de forma deliberada y a distinguir un fallo del host de una denegación de la aplicación.

2. Conceptos clave

Concepto	Por qué importa
límite del sitio	Una aplicación IIS o un enlace separado por punto de entrada, para que la ruta de intranet solo Windows y la ruta pública Anonymous lleven cada una exactamente una directiva de autenticación visible.
desafío Negotiate	Un HTTP 401 que lleva `WWW-Authenticate: Negotiate` y/o `NTLM`; un navegador apto reintenta con un encabezado `Authorization`, y Negotiate selecciona Kerberos o recurre a NTLM.
evidencia de Kerberos	Un vale de servicio para el nombre de host canónico `HTTP/` en el cliente, correlacionado con el registro de inicio de sesión del servidor; el encabezado de respuesta por sí solo nunca demuestra qué proveedor actuó.
autenticación en modo kernel	Con `useKernelMode`, el controlador HTTP.sys realiza el protocolo de enlace de Windows, así que la cuenta que descifra los vales es normalmente la cuenta de equipo, salvo que `useAppPoolCredentials` indique otra cosa.
SPN	El nombre de entidad de servicio (`HTTP/accessops.contoso.test`) que indica al dominio para qué cuenta se cifra un vale; un SPN ausente o duplicado empuja en silencio a los clientes hacia NTLM o hacia un bucle.
protección extendida	Comprobaciones de enlace de canal y de enlace de servicio que atan el protocolo de enlace de Windows a la conexión TLS y al SPN esperado, algo que importa en cuanto TLS termina en un proxy.
principal del host en Wisej.NET	En ASP.NET Core, el usuario de Windows solo llega a la aplicación como `Application.User`, el `HttpContext.User` de la petición capturado por Wisej.NET; demuestra quién inició sesión, no qué puede leer.

3. Desarrollo de la lección

Una aplicación por punto de entrada

AccessOps tiene dos puertas de entrada. La ruta de la intranet es para el personal del dominio: en IIS instalas el servicio de rol de autenticación de Windows, lo habilitas en esa aplicación y deshabilitas allí Anonymous, de modo que cada petición recibe un desafío antes de que el ASP.NET Core Module la entregue a la aplicación. La ruta pública sirve la página de inicio de sesión de socios y, en el Módulo 5, el callback de OpenID Connect. El navegador del socio debe llegar a esas páginas antes de que la aplicación sepa quién es el socio, así que esa aplicación mantiene habilitado el transporte Anonymous y la aplicación Wisej.NET aplica el acceso por sí misma. Compartir una sola aplicación desafiaría el callback externo o abriría las pantallas de la intranet.

Mantén las rutas en aplicaciones IIS separadas o en enlaces separados con sus propios grupos de aplicaciones. En el laboratorio, la ruta de la intranet es una aplicación HTTPS aislada con un grupo dedicado, cuyo enlace, plataforma de destino y estado de autenticación anotas primero. Inventaría los demás modos de IIS en lugar de añadirlos: Basic envía una credencial fácil de descodificar y necesita

HTTPS en todas partes, Digest es un servicio de rol heredado, y la asignación de certificados de cliente sigue necesitando una directiva de confianza, revocación y asignación de cuentas.

Leer el desafío y demostrar el proveedor

La primera petición recibe un 401 con `WWW-Authenticate: Negotiate` y, si está configurado, `NTLM`. Un navegador que considera apto el host reintenta con un encabezado `Authorization`, IIS valida el intercambio y la petición siguiente devuelve 200. El fixture F01 del laboratorio registra exactamente esto: un desafío Negotiate seguido de 200 es un desafío del host seguido de una autenticación, y nada más. Negotiate es un envoltorio que puede llevar Kerberos o recurrir a NTLM según el cliente, el SPN y la configuración del proveedor, así que un encabezado Negotiate por sí solo no demuestra Kerberos.

Para afirmar Kerberos correlacionas dos evidencias: `klist` en el cliente desechable muestra un vale de servicio para `HTTP/accessops.contoso.test`, y el registro de inicio de sesión del servidor en ese mismo momento nombra Kerberos como paquete de autenticación. Sin ambas, anota el proveedor como indeterminado; un laboratorio en grupo de trabajo muestra desafíos pero nunca puede respaldar una afirmación de Kerberos. Registra los encabezados solo por esquema y estado, porque los valores de `Authorization` son credenciales y no deben acabar en una traza ni en una incidencia.

Proveedores, modo kernel, SPN y el navegador

La configuración acotada del laboratorio establece `<anonymousAuthentication enabled="false" />` y `<windowsAuthentication enabled="true" useKernelMode="true">` con la lista de proveedores vaciada y reconstruida como Negotiate y después NTLM. Mantén Negotiate en primer lugar cuando pruebes Kerberos, y prueba el recurso alternativo que pretendes en lugar de deducirlo del orden. Los atributos de persistencia de conexión `authPersistNonNTLM` y `authPersistSingleRequest` deciden durante cuánto tiempo se confía en una conexión autenticada. Según el paquete y la documentación de IIS de Microsoft, el modo kernel descifra normalmente los vales con la cuenta de equipo; cuando el SPN HTTP está registrado a nombre de una identidad de grupo personalizada, `useAppPoolCredentials` debe coincidir con esa topología. Consulta el SPN con `setspn -Q` y cambia los SPN solo junto con el equipo del directorio.

La protección extendida añade `tokenChecking`, `flags` y una lista de SPN bajo `extendedProtection`; decide primero si TLS termina en IIS o en un intermediario de confianza y prueba después a lo largo de ese camino exacto. El navegador tiene su propio voto: Edge envía credenciales en silencio solo a los hosts que trata como intranet o que los administradores incluyen en `AuthServerAllowlist`, así que un equipo unido al dominio no garantiza el inicio de sesión silencioso para cualquier FQDN, perfil o estado de la VPN. NTLM y algunas configuraciones de Negotiate necesitan además afinidad de conexión, y con el controlador Negotiate de Kestrel (el paquete `Microsoft.AspNetCore.Authentication.Negotiate`, que no forma parte del marco compartido) Microsoft exige afinidad de conexión persistente uno a uno detrás de un proxy. Una prueba directa contra el servidor es tu referencia; verifica el camino del proxy por separado.

Diagnosticar por capas

Trabaja de fuera hacia dentro. Un 401 antes de `Program.Main` pertenece al desafío del host: compara lo que vio el navegador con los campos del registro de IIS `sc-status`, `sc-substatus` y `sc-win32-status`, y comprueba después el SPN, la directiva del navegador y el proxy. Un 500.19 justo después de poner la configuración de autenticación en `web.config` es un error de configuración de IIS, normalmente una

sección bloqueada en un ámbito superior: lee el archivo y la sección indicados, aplica los mismos valores en la ubicación de nivel de servidor o mediante el Administrador de IIS, y deja el código en paz. Una página que carga con una identidad de Windows válida pero deniega un documento es una denegación de la aplicación, que es el resultado que quieres para una cuenta sin la concesión Reader. Una página que funciona mientras falla un recurso compartido de archivos o una llamada a SQL es el segundo salto, el tema del Módulo 3.

Una vez que IIS ha autenticado la petición, Wisej.NET captura `HttpContext.User`, y `Application.User` lo devuelve salvo que la sesión haya asignado su propio principal. `Application.UserIdentity` solo existe en la compilación para .NET Framework. Por eso el arranque de la intranet de AccessOps trata la falta de una identidad de Windows como un fallo del host y busca la concesión por separado:

```
static void Main()
{
    // IIS answered the challenge; Wisej captured HttpContext.User.
    if (!Application.IsAuthenticated ||
        Application.User.Identity is not WindowsIdentity windows)
    {
        new HostFaultPage().Show();   // host layer, not an app deny
        return;
    }

    // The Windows account is evidence; the grant is the permission.
    var grant = AccessGrants.FindForAccount(windows.User?.Value);
    new DocumentsPage(grant).Show(); // DocumentService denies a null grant
}
```

El laboratorio demuestra esta separación dos veces: en IIS dentro de un dominio Windows, una segunda cuenta sin Reader se deniega después de una autenticación del host correcta; en cualquier máquina de desarrollo, el PolicyHarness deniega una identidad autenticada cuya concesión no permite leer, con cero lecturas del repositorio. Guarda la configuración original de IIS para que la reversión sea un solo paso.

Regla de seguridad

Mantén separadas las identidades y decide en el servidor. El principal del host, el principal de la aplicación Wisej.NET y el token efectivo de Windows son tres hechos distintos, y ninguno de ellos es un permiso. Cada lectura protegida comprueba la concesión vigente, el tenant y el registro en el límite del servicio antes de que se ejecute el repositorio, y un botón oculto, un claim de rol o una pestaña con la sesión cerrada no demuestran nada hasta que esa comprobación deniega.

Objetivos de aprendizaje

Al terminar este módulo serás capaz de:

- ✓ Elegir el modo de autenticación de IIS para cada punto de entrada de AccessOps —intranet solo Windows, transporte Anonymous para el inicio de sesión público y el callback— y mantener ambos en aplicaciones o enlaces separados.

- ✓ Leer un desafío 401 Negotiate o NTLM y demostrar si se usó Kerberos a partir de la evidencia correlacionada del vale y del inicio de sesión en el servidor, en lugar del encabezado de respuesta.
- ✓ Configurar los proveedores de la autenticación de Windows, el modo kernel, el SPN HTTP y la protección extendida, y explicar cómo la directiva de intranet del navegador y la afinidad de conexión del proxy afectan al inicio de sesión silencioso.
- ✓ Diagnosticar un fallo por capas: desafío del host, bloqueo de configuración de IIS (500.19), denegación de la aplicación y acceso en el segundo salto.

Guía del laboratorio / examen

Lo que construirás en el laboratorio práctico, el enfoque sugerido y los entregables requeridos.

Laboratorio práctico

Publica la ruta de la intranet de AccessOps en una aplicación IIS HTTPS aislada con un grupo de aplicaciones dedicado, anota el enlace, la plataforma de destino y el estado de autenticación, y aplica después la configuración de ubicación acotada windows-auth para habilitar la autenticación de Windows y deshabilitar Anonymous. Desde un cliente del dominio, abre el FQDN canónico como CONTOSO\reader1, anota el esquema del desafío, el resultado de la petición siguiente y la identidad de la aplicación ocultada, consulta el SPN HTTP y compara el vale del cliente con la evidencia de inicio de sesión del servidor; inicia sesión después con una segunda cuenta sin Reader y captura una denegación de la aplicación tras una autenticación del host correcta antes de restaurar la configuración original. El desafío, el proveedor negociado y la evidencia del SPN solo pueden verificarse en el entorno de laboratorio con IIS y un dominio Windows (un grupo de trabajo muestra desafíos pero no puede afirmar Kerberos, así que allí anota un resultado indeterminado); en una máquina de desarrollo sencilla, el PolicyHarness demuestra en local que una identidad autenticada sin la concesión Reader se sigue denegando con cero lecturas del repositorio.

Punto de partida

Abre la solución AccessOps del Módulo 1, con su `DocumentService`, el repositorio que cuenta lecturas, los fixtures de los tenants A y B y el PolicyHarness autónomo. Necesitas una aplicación IIS HTTPS aislada, dos cuentas de prueba del dominio, Edge y permiso para leer los registros de IIS; sin dominio, ejecuta los pasos de IIS en un grupo de trabajo y los pasos de la política en el PolicyHarness.

Enfoque sugerido

- ✓ Publica la ruta de la intranet en su propia aplicación y grupo de IIS, y guarda la configuración de autenticación, el enlace y la plataforma de destino actuales como referencia para la reversión antes de cambiar nada.
- ✓ Aplica la configuración de ubicación acotada (Anonymous desactivado, Windows activado, modo kernel, proveedores vaciados y reconstruidos como Negotiate y después NTLM); si IIS responde 500.19, establece los mismos valores en el nivel de servidor o en el Administrador de IIS en lugar de desbloquear secciones.
- ✓ Abre `https://accessops.contoso.test` desde un cliente del dominio como `CONTOSO\reader1` y anota el esquema del 401, el estado de la petición siguiente y la identidad ocultada que muestra la vista de diagnóstico, nunca el valor de `Authorization`.
- ✓ Ejecuta `setspn -Q HTTP/accessops.contoso.test` y `klist`, correlaciona el vale del cliente con el registro de inicio de sesión del servidor y escribe Kerberos, NTLM o indeterminado solo a partir de esa evidencia.
- ✓ Inicia sesión con la segunda cuenta sin Reader, captura la denegación de `DocumentService` con cero lecturas del repositorio, añade el caso equivalente al PolicyHarness y restaura después la configuración guardada y confirma que el sitio funciona.

Entregables requeridos

- ✓ Configuración efectiva de autenticación de IIS para las rutas de intranet y pública
- ✓ Traza del desafío ocultada con esquema, estado y resultado de la petición siguiente
- ✓ Evidencia del SPN y del vale, o un resultado explícito de proveedor indeterminado
- ✓ Usuario autenticado por el host y denegado por la política de AccessOps, con un caso del PolicyHarness para la misma regla
- ✓ Nota de diagnóstico por capas que separa el fallo de IIS de la denegación de la aplicación, con la configuración de reversión

Preguntas de repaso

- ✓ El navegador muestra un desafío Negotiate seguido de 200 y la vista de diagnóstico muestra el nombre de cuenta correcto. ¿Qué puedes afirmar sobre Kerberos y qué evidencia falta todavía?
- ✓ Un socio informa de que la página pública de inicio de sesión le pide credenciales de Windows. ¿Qué configuración o límite de IIS inspeccionarías primero, y por qué la corrección no está en el código de Wisej.NET?
- ✓ El inicio de sesión silencioso funciona cuando navegas directamente al servidor pero entra en bucle a través del equilibrador de carga. ¿Qué dos propiedades del camino del proxy compararías y qué rompería cada una?

Regla de seguridad

Mantén separadas las identidades y decide en el servidor. El principal del host, el principal de la aplicación Wisej.NET y el token efectivo de Windows son tres hechos distintos, y ninguno de ellos es un permiso. Cada lectura protegida comprueba la concesión vigente, el tenant y el registro en el límite del servicio antes de que se ejecute el repositorio, y un botón oculto, un claim de rol o una pestaña con la sesión cerrada no demuestran nada hasta que esa comprobación deniega.