1/3/2022

IO 6: TUTORIAL DE DISEÑO TÉCNICO E IMPLEMENTACIÓN DE UN WEBLAB – SEGURIDAD Y COMUNICACIONES

Co-funded by the European Union

1. INTRODUCCIÓN

Los equipos y recursos de laboratorio que se exponen al mundo a través de Internet como WebLabs, se vuelven automáticamente vulnerables y pueden ser atacados y / o accedidos por usuarios maliciosos. Por lo tanto, si bien este problema generalmente no es tomado demasiado en serio por aquellos grupos y universidades que desarrollan y usan WebLabs, en realidad es uno de los puntos más críticos que deben abordarse. En este sentido, los canales de comunicación, protocolos y arquitectura seleccionados para ofrecer los servicios de laboratorio en línea son de suma importancia, ya que afecta inmediatamente al nivel de seguridad.

Este documento revisa algunas de las amenazas de seguridad más típicas y las soluciones para las comunicaciones con el fin de hacer frente a tales riesgos.

2. AMENAZAS COMUNES DE SECURITTY EN WEBLABS

Las siguientes son las fuentes más comunes de amenazas relacionadas con WebLabs y los riesgos asociados a ellas:

- Los equipos (cámaras, ordenadores, interruptores, etc.) utilizan IPs. públicas. Cuando los dispositivos de laboratorio utilizan IP públicas, son visibles y accesibles para cualquier persona. Si bien esta es una solución muy pequeña para exponer los servicios de laboratorio y hacerlos accesibles, también conlleva un gran riesgo, ya que cualquier usuario o bot puede intentar acceder a dichos dispositivos.
- Los servicios WebLab no utilizan un sistema de autenticación. A veces, los WebLabs se dejan abiertos, por lo que cualquiera puede acceder a él. Esto se puede hacer ya sea por diseño o por error, pero en ambos casos, los usuarios maliciosos pueden tomar el control del laboratorio y hacer un mal uso de él, dañando potencialmente el equipo, monopolizándolo y evitando que otros lo usen o simplemente, el acceso a cámaras que no deberían estar disponibles para todos en cualquier momento.
- Los servicios no se ejecutan a través de HTTP. Incluso cuando existe un mecanismo de autenticación, si dicho mecanismo no depende de HTTP, la seguridad está en riesgo debido al uso del transporte no cifrado de las credenciales. Muchas páginas web y servicios de WebLab todavía se ejecutan en HTTP en lugar de HTTP, lo que está lejos de ser ideal.
- El acceso dado a los usuarios incluye el acceso completo al sistema operativo (SO). A veces, los WebLabs se basan en conexiones de tipo escritorio remoto. Cuando este es el caso, la persona que accede al WebLab tiene acceso a todo el sistema operativo. Incluso si el usuario en la computadora WebLab tiene privilegios limitados, lo que no siempre es el caso, esto también representa un gran peligro, ya que los usuarios pueden, por ejemplo, enviar correos electrónicos de phishing o spam desde direcciones remotas. No solo eso, los estudiantes que comparten el mismo usuario en la computadora del laboratorio también pueden encontrar archivos con datos de laboratorio y resultados obtenidos por otros estudiantes que ingresaron previamente a la computadora, ya sea que estos se dejaron allí a propósito o accidentalmente.

Las recomendaciones básicas para evitar los problemas anteriores son:

- Use IP privadas dentro de una VLAN/ VPN que esté protegida y le permita controlar quién puede acceder a qué recursos dentro de la red privada.
- Utilice siempre algún tipo de sistema de autenticación a nivel de protocolo de comunicaciones. El uso de la autenticación para acceder a una página web no es suficiente, ya que los usuarios pueden acceder a la página web en algún momento, cargar una aplicación web y mantenerla abierta y en funcionamiento si no se implementa la seguridad a nivel de protocolo de comunicaciones. Dichos usuarios pueden incluso descargar la aplicación y seguir usándola cuando lo deseen, sin tener que iniciar sesión y autenticarse en la página web nunca más.
- Instale siempre un certificado SSL para permitir el uso de HTTP y comunicaciones cifradas.

- Utilice una aplicación web que se comunique con los servicios de WebLab de forma limitada (como muestran los documentos 2a, 2b y 3) o, si se utiliza un tipo de acceso de escritorio remoto: 1) hágalo a través de un usuario en la máquina que se ha preparado para tener privilegios muy limitados y 2), limite el acceso visual al equipo remoto para que solo se muestre la aplicación de escritorio que controla el equipo de laboratorio y se puede acceder.