El servidor Citrix XML es un componente de Citrix XenApp y XenDesktop que se utiliza para enumerar y proporcionar entradas seguras para los usuarios que utilizan a la WebInterface o CloudGateway.

El Servicio XML Citrix es un servicio de Windows que forma parte del Citrix XenApp y XenDesktop.

Se utiliza para proporcionar datos enviados tras solicitudes a los componentes XML de Citrix. Esta tecnología se introduce con MetaFrame 1.8 SP2. Hasta XenApp 6.0 cada servidor XenApp puede ser un servidor XML. En XenApp 6.5 se introduce la arquitectura de controlador de trabajo y sólo un servidor con la función de controlador puede ser un server XML. Un servidor con la función de controlador es responsable de la gestión de las explotaciones.

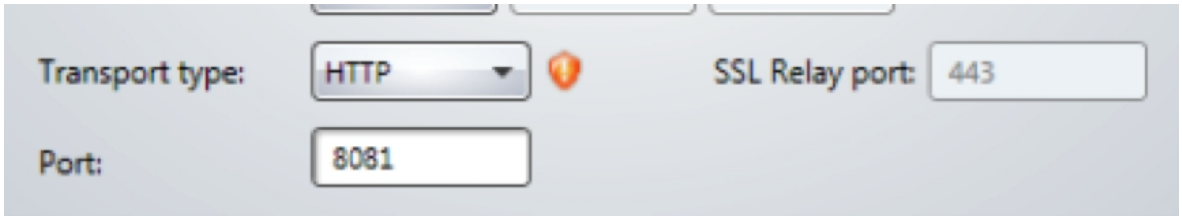
El servicio XML de Citrix es más comúnmente utilizado para proporcionar a los usuarios acceso a sus aplicaciones y escritorios a través de un portal web, aprovechando los servicios de WebInterface, CloudGateway (Storefront) o Access Gateway.

Se recomienda tener varios servidores Citrix XML, lo más cerca posible de los DataCollector (servidores de zona XenApp) y Desktop Delivery Controller (XenDesktop).

El protocolo XML de WebInterface y/o StoreFront utiliza texto plano en el envio de datos. Ello nos hace **potencialmente** posibles **victimas** para un ataque realizado internamente.

¿Seguridad?

Mi entorno de laboratorio será la mesa de pruebas para esta demostración. Mi actual granja utiliza el puerto 8081 para el transporte XML. No utilizamos ningún mecanismo de encriptación y securización del tráfico.

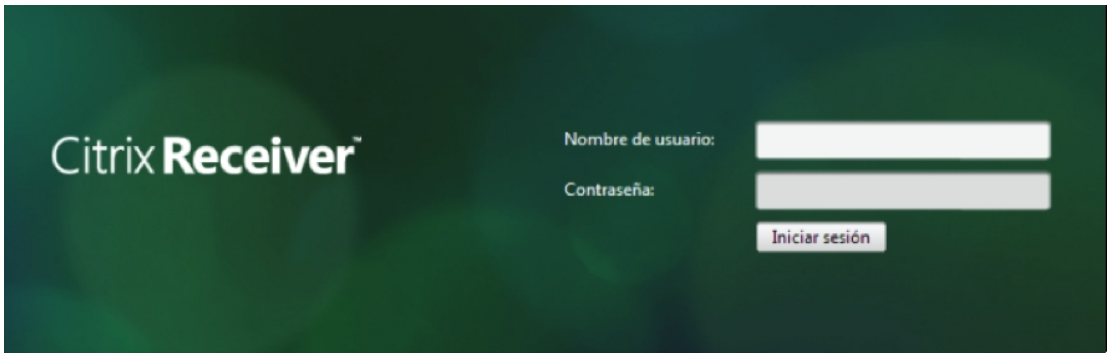


La prueba a realizar es sencilla. Vamos a realizar los siguientes pasos sobre un entorno de XenApp con CloudGateway.

1. Abrir URL CloudGateway
2. Validar-nos en StoreFront
3. Lanzar aplicación

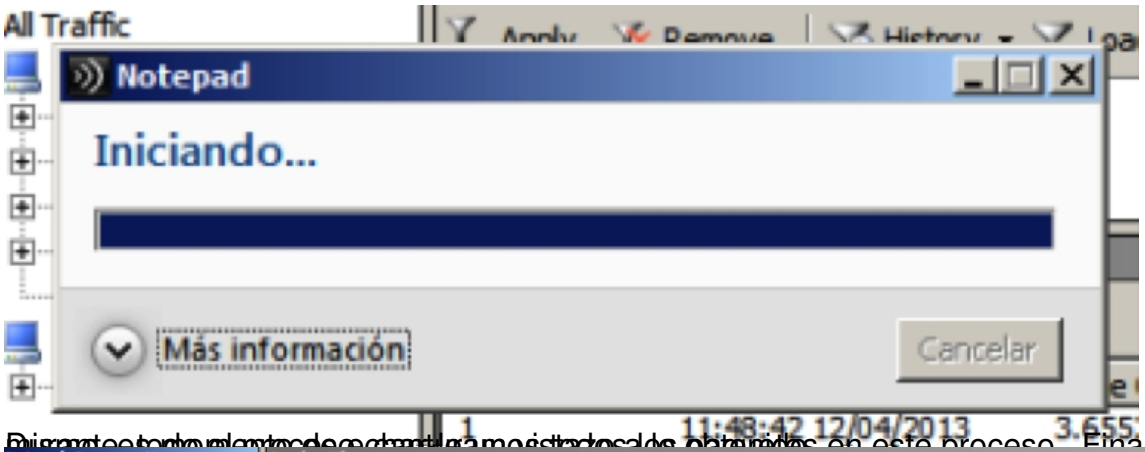
Durante este proceso vamos a lanzar un snifer de red, capturando todo el tráfico.

Conectamos en el entorno y nos validamos.

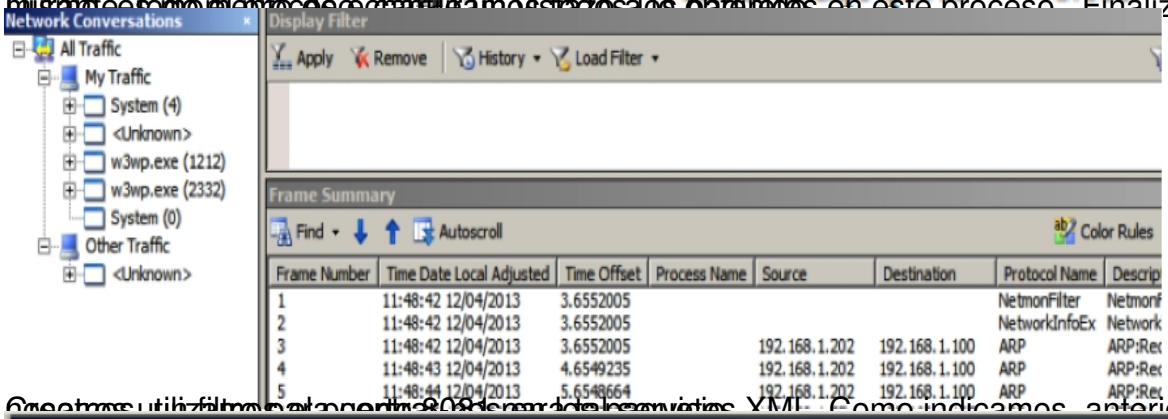


Se enumeran las aplicaciones disponibles.

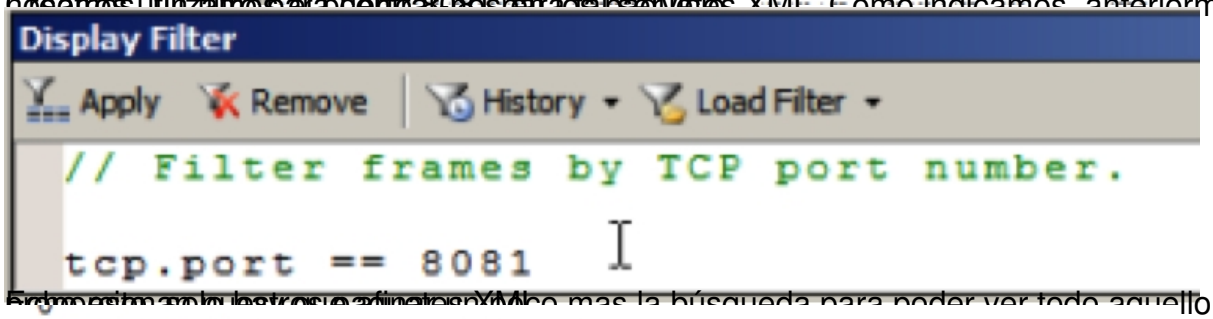
Lanzamos una aplicación.



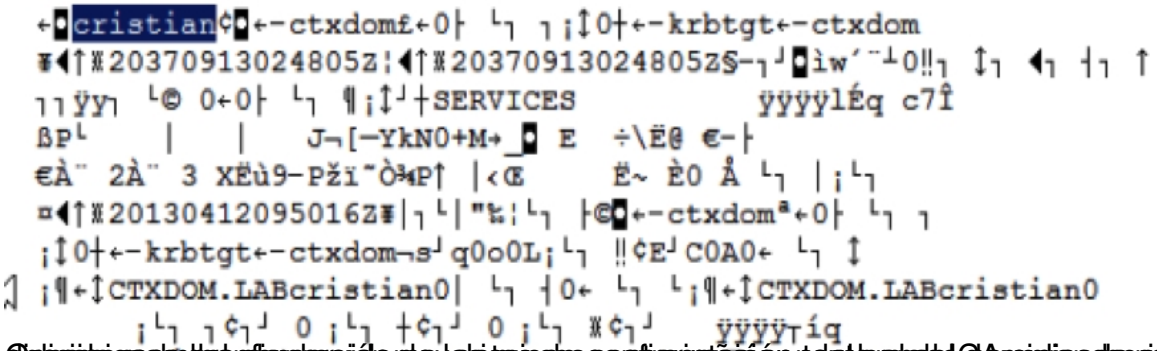
Pulsamos todos los botones de aceptar y comenzamos a obtener datos en este proceso. Finalizado el



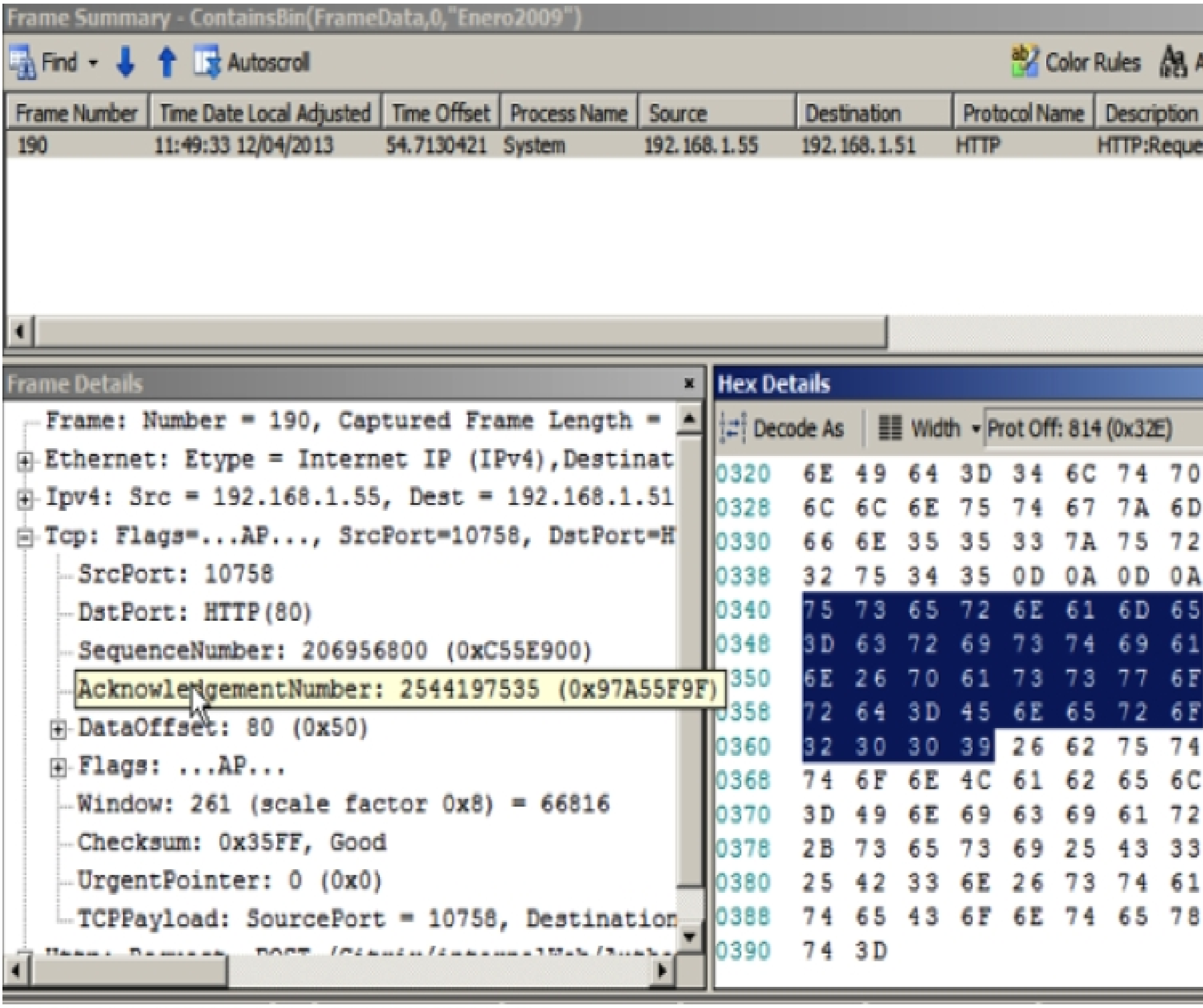
Creamos un filtro para el puerto 8081 que es donde escucha XML. Como indicamos anteriormente



Ordenamos todos los eventos XML mas la búsqueda para poder ver todo aquello que



Aplicamos un filtro de servicio, abrimos la configuración, nos vamos a la pestaña de Avanzado y pulsamos en la




```
Csrf-Token: B099922AA5FFCD2BBBA0176481CED7A2
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.17 (KHTML, like Gecko) Chrome/24.0.1312.57
Safari/537.17
Referer: http://192.168.1.51/Citrix/internalWeb/
Accept-Encoding: gzip,deflate,sdch
Accept-Language: es-ES,es;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
Cookie: CsrfToken=B099922AA5FFCD2BBBA0176481CED7A2;
CtxsPluginAssistantState=Done; ASP.NET_SessionId=
4ltpllnutgzmfn553zur2u45

username=cristian&password=[redacted]&buttonLabel=Iniciar+sesi%
C3%B3n&stateContext=
```