UNIVERSIDAD DE TARAPACÁ
FACULTAD DE INGENIERÍA
INGENIERÍA CIVIL EN COMPUTACIÓN E INFORMÁTICA
ARICA – CHILE

Documento de requisitos

"Sistema de administración de un laboratorio de ciberseguridad controlado"

Equipo de Desarrollo:
Scarlet Gavia Mondaca
Empresa o Unidad: DICI
Curso: Proyecto IV ICCI
Profesor: Diego Aracena Pizarro

Arica 10 de octubre, 2025

Resumen o introducción

La ciberseguridad es una rama muy importante en la actualidad, a través de ella se puede proteger los datos y la información importante, ya que garantiza la protección, respaldo y resguardo de los datos, por ello, es esencial que los estudiantes adquieran habilidades para defender sus dispositivos y detectar posibles ataques de agentes externos.

Este proyecto tiene como objetivo diseñar e implementar un sistema de administración para el ramo de “Gestion de seguridad informática ”, para llevar a cabo este sistema se comenzará por realizar las instalaciones de distintos sistemas operativos de distribución “Linux” en cada uno de los servidores, los cuales tendrán distintas herramientas para que los alumnos puedan aplicar ataques y defensas controladas, se liberaran los puertos señalados por el cliente, se llevará un catastro de ruta de cada proceso que se realiza semanalmente, esto se llevará a cabo con un dashboard para llevar un monitoreo de los 4 servidores en simultáneo, este dashboard permitirá reiniciar los servidores y ejecutar cualquier aplicación que el cliente quiera instalar.

Asimismo, luego de estas configuraciones, el sistema deberá ser capaz de monitorear, registrar y analizar cada una de las actividades realizadas, ya sea en el servidor físico como ataques externos, con estos datos registrados en el sistema, este debe ser capaz de realizar un análisis, identificando y registrando cada intento de intrusión, lo que permitirá al cliente ver los ataque y poder realizar un análisis de estas capturas.

I. Definición del proyecto

Contexto

La computación y la tecnología son parte de nuestras vidas, estudiar computación te permite formar parte del grupo de personas que desarrollan los sistemas que están dando forma a los estilos de vida del futuro, la práctica de la ciberseguridad es esencial para esta rama de estudios, ya que permite que los alumnos desarrollen habilidades en defensa de sistemas y detección de ataques, sin embargo, es necesario que estas prácticas se realicen en un entorno controlado, donde los riesgos sean mínimos y la actividad de los alumnos pueda ser supervisada adecuadamente.

Problema

Los estudiantes aplicaran ataques y defensas en sistemas reales para desarrollar habilidades efectivas, sin embargo, estas prácticas presentan riesgos si se realizan en entornos no controlados, ya que los servidores podrían dañarse o los datos podrían comprometerse, el cliente con rol de administrador de estos servidores carecen de herramientas que les permitan supervisar y registrar las actividades de estos, lo que dificulta evaluar el conocimiento y orientar adecuadamente el aprendizaje.

Solución

Para dar solución a esta problemática, se propone la implementación de un sistema de administración para un laboratorio de ciberseguridad controlado, donde se trabajara con 4 servidores, cada uno con un sistema operativo diferente, estos estarán protegidos y configurados específicamente para prácticas de ataque y defensa, este sistema permitirá al cliente monitorear, registrar y analizar las actividades realizadas en los servidores, identificando los ataques realizados y evaluar las estrategias de defensa.

II. Requisitos del sistema

Requisitos de Alto Nivel (opcional)

ID	*Definición del requisito*
RAN1	Facilitar la supervisión y el análisis de las actividades realizadas.
RAN2	Garantizar servidores protegidos.
RAN3	El sistema debe contar con la tríada de ciberseguridad, prueba de penetración (pentesting), peritaje informáticos y seguridad informática en criptografía.

Requisitos funcionales

ID	*Definición del requisito*	*Importancia*
RF1	El sistema debe tener 2 perfiles de acceso, uno para administrador y otro para usuario.	**muy alto**
RF2	El sistema debe permitir que el perfil de administrador modifique datos o acciones en los servidores.	**muy alto**
RF3	El sistema debe permitir que el perfil de usuario solo pueda acceder a los datos registrados, sin opción de modificar.	**muy alto**
RF4	El sistema debe registrar todas las acciones y ataques realizados.	**alto**
RF5	El sistema debe mostrar los ataques producidos y las vulnerabilidades detectadas.	**alto**
RF6	El sistema debe permitir la gestión de múltiples servidores.	**alto**
RF7	El sistema debe permitir un monitoreo y seguimiento de los ataques ejecutados.	**alto**
RF8	El sistema debe mostrar en pantalla el tiempo real de los eventos.	**medio**
RF9	El sistema debe mostrar los procesos de los servidores.	**medio**
RF10	El sistema debe registrar cualquier actividad realizada en los servidores (reinicio, apagado,etc).	**medio**

Requisitos no funcionales

ID	*Definición del requisito*
RNF1	El sistema debe asegurar que los ataques realizados no afecten a otros sistemas de la empresa.
RNF2	Los servidores y el sistema deben estar siempre disponibles.
RNF3	El sistema debe ser capaz de manejar múltiples conexiones y acciones simultáneas.
RNF4	El sistema debe tener una interfaz intuitiva y permitir acceder fácilmente a la información de cada servidor.
RNF5	El sistema debe permitir agregar más servidores sin necesidad de reestructuración mayor.
RNF6	El sistema debe ser compatible con dashboard para la captura de datos.

III. Acta de acuerdo formal

Ejemplo

Yo Miguel Trigo Zapata en representación de DICI -, en adelante cliente usuario del proyecto Sistema de administración de un laboratorio de ciberseguridad controlado. Estoy de acuerdo con los requisitos planteados en este documento y autorizo al equipo de software el desarrollo del sistema (subsistema o aplicación) sugerido.

Firma del Cliente