

UNIVERSIDAD DEL BÍO-BÍO

FACULTAD DE INGENIERÍA

DEPARTAMENTO DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA



Nombre alumnos:

Nicolás Ignacio Loyola Rivas

Alexis Alejandro Villa Vera

Informe de Proyecto de Título para optar al título de:

Ingeniero Civil en Automatización

Plataforma remota de conexión y manipulación al brazo robótico Scorbot-ER Vplus del laboratorio de Sistemas Automatizados de Producción CIMUBB

Profesor Guía: **D.SC. Ángel Ernesto Rubio Rodríguez.**

Profesor Co-Guía: **Luis Humberto Vera Quiroga.**

Concepción, abril de 2023

Nicolás I. Loyola R. - Alexis A. Villa V.

Plataforma remota de conexión y manipulación al brazo robótico Scorbot-ER Vplus del laboratorio de Sistemas Automatizados de Producción CIMUBB

Nicolás Loyola Rivas
Alexis Villa Vera

Informe de Proyecto de
Título para optar al
Título de

Ingeniero Civil en Automatización
Abril 2023

Resumen

El presente trabajo de título tiene como objetivo principal diseñar y desarrollar una aplicación web que permita el monitoreo y la manipulación remota del robot Scorbot ER Vplus instalado en el laboratorio CIM de la Universidad del Bío-Bío, considerando el desarrollo web correspondiente de la plataforma de control, el acceso remoto al servidor del laboratorio, monitoreo mediante webcams locales instaladas en cada estación del laboratorio y aspectos de ciberseguridad pertinentes para una plataforma segura, proyecto presentado para dar conformidad a los requisitos de titulación de la carrera Ingeniería Civil en Automatización.

Debido a la contingencia mundial en cuanto a conectividad e industria 4.0, se propone el desarrollo de una aplicación web para el monitoreo y manipulación remota del brazo robótico Scorbot-ER Vplus, tomando en cuenta sus funcionalidades y posibles aplicaciones a nivel académico, con el fin de simular una experiencia de laboratorio presencial lo más completa posible. Actualmente, el laboratorio CIM de la UBB no cuenta con un sistema web de laboratorios en el cual los estudiantes y académicos puedan realizar experimentos y ensayos de manera práctica para las asignaturas que requieran la utilización de estos recursos. Por esta razón, se propone el desarrollo de una plataforma web que permita el monitoreo mediante cámaras instaladas en el laboratorio y la manipulación del brazo robótico mediante web para aplicaciones académicas. Además del diseño y desarrollo de la aplicación web, se consideran aspectos de seguridad de la información con énfasis dedicado a la protección y cifrado de los datos implicados en esta plataforma.

La ventaja de disponer de este tipo de sistemas de laboratorios remotos en las distintas instalaciones de la universidad, tanto para profesores como para estudiantes, cobra suma importancia a niveles académicos, debido a que permitirá desarrollar e implementar programas necesarios para la integración de procesos industriales en las carreras afines que requieran de este tipo de actividades prácticas y de la utilización de este brazo robótico para aplicaciones futuras, integrando distintos niveles de programación y comunicación entre dispositivos para el desarrollo tecnológico y la integración de técnicas y estrategias de I+D, ya que se trata de un proyecto de gran envergadura en cuanto a investigación y desarrollo de comunicación entre dispositivos y desarrollo web.

Los beneficios que trae este trabajo de título consisten en otorgar herramientas prácticas para la utilización del laboratorio tanto en la universidad como de forma remota, además de lograr un control seguro de este sistema a partir de una plataforma web desarrollada a lo largo de este trabajo, en conjunto a la instalación de una red física de computadoras, dentro de la cual se podrá intercambiar información entre servidores y estaciones mediante la tecnología sockets para poder realizar distintas experiencias de laboratorio. Además, se integran y complementan múltiples lenguajes de programación y herramientas tecnológicas para el desarrollo del estudiante. Los lenguajes de programación de este proyecto quedan establecidos y definidos en este informe, pero no deberían existir complicaciones al querer extrapolarlo a distintos lenguajes de programación y marcos de trabajo si es que el estudiante se siente más fuerte en alguna tecnología en particular y se quisiera seguir complementando con funcionalidades a este proyecto de título.

Índice

| | | |
|-------|---|-----|
| 1. | INTRODUCCIÓN..... | 8 |
| 1.1 | INTRODUCCIÓN GENERAL..... | 8 |
| 1.2 | PLANTEAMIENTO DEL PROBLEMA..... | 11 |
| 1.3 | OBJETIVOS | 17 |
| 1.3.1 | OBJETIVOS GENERALES..... | 17 |
| 1.3.2 | OBJETIVOS ESPECÍFICOS | 17 |
| 2. | ALCANCE DEL PROYECTO..... | 18 |
| 3. | ESTADO DEL ARTE | 22 |
| 4. | SCORBOT-ER VPLUS..... | 28 |
| 4.1 | COMPONENTES MECÁNICOS DEL ROBOT | 29 |
| 4.2 | TECNOLOGÍAS | 32 |
| 4.4 | COMUNICACIÓN SERIAL CON EL ROBOT | 35 |
| 5 | DISEÑO DE SOFTWARE..... | 36 |
| 5.1 | REQUERIMIENTOS FUNCIONALES | 38 |
| 5.2 | CASOS DE USO E HISTORIAS DE USUARIO | 39 |
| 5.3 | DIAGRAMA DE CASOS DE USO | 44 |
| 5.4 | MOCKUP..... | 48 |
| 6 | DESARROLLO DE LA APLICACIÓN WEB PARA MONITOREO Y CONTROL REMOTO 54 | |
| 6.1 | Interfaz de control y creación de rutinas | 56 |
| 6.2 | Manipulación y movimiento de Scorbob-ER Vplus | 62 |
| 6.3 | Métodos de operación del Scorbob..... | 62 |
| 6.4 | Modo Manual | 62 |
| 6.5 | Coordenadas Cartesianas (XYZ) | 63 |
| 6.6 | Coordenadas de Ejes..... | 63 |
| 6.7 | Comandos utilizados en modo directo. | 64 |
| 6.8 | Definición y grabado de posiciones | 64 |
| 6.9 | Movimiento a posiciones grabadas..... | 64 |
| 6.10 | Comandos de control de ejes | 64 |
| 7 | RED LOCAL LABORATORIO CIM | 66 |
| 8 | CIBERSEGURIDAD | 69 |
| 8.1 | Vectores de ataque..... | 70 |
| 8.2 | Pruebas de penetración y Hacking ético | 89 |
| 8.3 | Seguridad PHP | 103 |

| | | |
|----|-------------------|-----|
| 9 | CONCLUSIONES..... | 110 |
| 10 | REFERENCIAS | 112 |

Índice de Figuras

| | |
|--|----|
| Figura 1.1 – Laboratorio de Sistemas Automatizados de Manufactura. | 11 |
| Figura 1.2 – Arquitectura de la aplicación web basada en cliente/servidor. | 13 |
| Figura 3.1 – Logo LabsLand..... | 23 |
| Figura 3.2 – Logo eLab/TeleLab. | 23 |
| Figura 3.3 – Logo Splashtop..... | 24 |
| Figura 3.4 – Universidad Susquehanna..... | 25 |
| Figura 3.5 – Robot Swivl..... | 26 |
| Figura 4.1 – Brazo Robótico Scorbot-ER Vplus..... | 28 |
| Figura 4.2 – Encoder o codificador..... | 29 |
| Tabla 4.3 – Tecnologías implementadas para el desarrollo de la aplicación web y control del robot..... | 34 |
| Figura 5.1 – Login de usuario..... | 36 |
| Figura 5.2 – Rol de administrador..... | 40 |
| Figura 5.3 – Rol de profesor..... | 41 |
| Figura 5.4 – Rol de estudiante..... | 41 |
| Figura 5.5 – Flujo de usuario con rol de administrador..... | 42 |
| Figura 5.6 – Flujo de usuario con rol de profesor..... | 42 |
| Figura 5.7 – Flujo de usuario con rol de estudiante..... | 43 |
| Figura 5.8 – Casos de uso para rol de administrador..... | 45 |
| Figura 5.9 – Casos de uso para rol de profesor..... | 46 |
| Figura 5.10 – Casos de uso para rol de estudiante..... | 47 |
| Figura 5.11 – Login | 49 |
| Figura 5.12 – Home | 49 |
| Figura 5.13 – Interfaz de control y monitoreo..... | 50 |
| Figura 5.14 – Historial de usuario..... | 51 |
| Figura 5.15 – Solicitud de horarios | 51 |
| Figura 5.16 – Configuración de cuenta | 52 |
| Figura 5.17 – Registro de usuarios..... | 52 |
| Figura 5.18 – Control de usuarios | 53 |
| Figura 6.1 – Distribución óptima de los dispositivos en el laboratorio..... | 55 |

| | |
|---|-----|
| Figura 6.2 – Vista principal de la interfaz. | 57 |
| Figura 6.3 – Réplica de interfaz teach pendant. | 58 |
| Figura 7.1 – Configuración para fijar direcciones IP en estaciones y servidor. | 67 |
| Figura 8.1 – Herramienta nmap para encontrar escanear dispositivos o redes. | 81 |
| Figura 8.2 – Herramienta Wireshark para interceptar tráfico de red. | 82 |
| Figura 8.3 – Análisis de puertos con nmap. | 91 |
| Figura 8.4 – Comunicación establecida entre las dos máquinas. | 93 |
| Figura 8.5 – netdiscover en Kali Linux. | 93 |
| Figura 8.6 – Procedimiento para IP Spoofing. | 94 |
| Figura 8.7 – Análisis de tráfico mediante Wireshark. | 95 |
| Figura 8.8 – Análisis de tráfico mediante Wireshark. | 97 |
| Figura 8.9 – Ataque de fuerza bruta a un servidor mediante SSH. | 99 |
| Figura 8.10 – Herramienta para la explotación de inyección SQLMap. | 100 |
| Figura 8.11 – Herramienta Metasploit. | 101 |
| Figura 8.12 – Burp Suite. | 102 |
| Figura 8.13 – Herramienta de estadísticas de las actividades de red netstat. | 103 |
| Figura 8.14 – Encriptación de contraseñas mediante PHP. | 104 |
| Figura 8.16 – Tokenización de información sensible del usuario. | 106 |
| Figura 8.17 – Relación de parámetros. | 107 |
| Figura 8.18 – Columna intentos_fallidos. | 108 |

1. INTRODUCCIÓN

1.1 INTRODUCCIÓN GENERAL

Considerando el pleno auge de la cuarta revolución industrial, que ha logrado complementar técnicas avanzadas de producción con tecnologías inteligentes integradas, y que la automatización es un proceso que se lleva a cabo desde hace un par de años con el fin de mejorar la eficiencia de ciertos sistemas en concreto, se propone un laboratorio remoto para aplicaciones académicas tanto para estudiantes como para profesores que permita monitorear el laboratorio CIM de la Universidad del Bío-Bío de manera remota, además de que se podrá controlar la estación de trabajo en la que está el Scorbot-ER Vplus, pudiendo programar distintas aplicaciones o rutinas independientes con cada brazo robótico o estación. Se plantea utilizar herramientas tecnológicas correspondientes al desarrollo web e implementar mejoras y optimizaciones en sistemas ya existentes, con gran énfasis en agregar funcionalidades a procesos que sirven para el desarrollo profesional y académico de la comunidad universitaria. Todo esto dentro de una misma red local instalada y configurada para lograr una correcta comunicación entre servidor y estaciones mediante la tecnología sockets, integrada como complemento al desarrollo de la aplicación web.

Como se trata de una aplicación de monitoreo, control y manipulación del robot de forma remota, se deberá generar un acceso remoto al servidor del laboratorio CIM, que será el encargado de administrar las prácticas y además enviará información y comandos de control y movimiento a las estaciones de trabajo, para lograr la interacción entre el usuario y el brazo robótico. Para lograr esto, se propone establecer y configurar un acceso remoto mediante VPN (en primera instancia) hacia el servidor, para poder acceder a la red local del laboratorio desde cualquier otro punto, integrando de esta forma una capa de seguridad valiosa a la hora de conectarse y realizar alguna práctica, ya que mediante esta forma de acceder, se filtra el punto de acceso del usuario, por lo que un ciberdelincuente nunca podrá saber desde donde se conecta hacia el laboratorio, ya que se establece un túnel entre el usuario y el servidor de la red de laboratorio. Para el comportamiento ideal de esta aplicación, se debería contar con un acceso remoto desde internet, siempre y cuando sea desplegada de una manera segura y robusta. Esto implicaría contratar algún servicio de hosting y dominio en la nube como los servicios de AWS, Azure o Google.

Ahora, se deben definir claramente los conceptos de servidor y estaciones, ya que no se deben confundir estos componentes en la arquitectura de red establecida y propuesta para este trabajo de título.

Una estación consta de un PC con sus correspondientes periféricos (mouse, teclado, monitor), tres webcams conectadas de manera serial a la estación y un robot Scrobot-ER Vplus, que será el personaje principal de este trabajo de título, ya que se desarrollará una interfaz de control que permitirá moverlo manualmente, ejecutar comandos establecidos y generar rutinas de movimiento.

El servidor es una computadora dedicada que permitirá administrar las prácticas realizadas y solicitadas por el usuario, conectándose y enviando información a las distintas estaciones de trabajo, mediante las funcionalidades de la plataforma, que corresponde a una aplicación web desarrollada y montada en este servidor. Además, se debe configurar esta máquina para que se pueda acceder de forma remota y así estar dentro de la red de forma virtual. Se propone realizar esta conexión mediante la configuración de una VPN en el servidor y luego configurada en el equipo del usuario que desea interactuar con esta plataforma, permitiendo acceder desde cualquier punto a la red local del laboratorio, considerando que se trataría de una conexión segura, ya que se asume que la persona que desea conectarse es un usuario o estudiante validado y confiable. Además, este servidor tendrá instalada una base de datos que será desarrollada en este proyecto para satisfacer todas las funcionalidades que tendrá la aplicación, logrando que cada usuario quede registrado, además de sus horarios de ingreso, salida, errores, puntos almacenados, rutinas, entre otras funcionalidades.

Una vez que la aplicación esté completamente desarrollada y validada, mediante pruebas de desempeño y experiencias prácticas, se propone contratar un servicio externo de hosting y dominio para alojar la plataforma en un servidor remoto de Amazon, Azure o Google, con el objetivo de tener un servicio en línea, con la aplicación siempre disponible, base de datos y seguridad integrada en el servicio de infraestructura en la nube. Esto mejoraría notablemente el desempeño de la aplicación, además que se podría lograr generar el acceso remoto de forma ideal y profesional, considerando que estos servicios son claves y fundamentales en cada compañía

dedicada al desarrollo o fabricación de software.

Para lograr todo esto, es que se plantea el desarrollo desde cero de una aplicación web que permita una mejora continua y una optimización con respecto a funcionalidades y desempeño de los brazos robóticos instalados y disponibles en el laboratorio CIM de la Universidad del Bío-Bío como estaciones de trabajo, con el objetivo de poder realizar prácticas de laboratorio en un entorno real de forma remota, pudiendo conectarse desde prácticamente cualquier lugar que tenga un acceso a internet estable mediante VPN, o idealmente desde internet al contar con alguno de los servicios cloud que existen en el mercado de infraestructura como servicio. Esta plataforma permite monitorear y también controlar en tiempo real todas las estaciones que estén conectadas a la misma red, siempre y cuando se tenga conectado alguno de los modelos de los brazos robóticos Scrobot a dicha estación, de otra forma, este proyecto no tiene sentido. Considerar también que las estaciones deben estar encendidas y disponibles para poder establecer conexión con esta aplicación.

En el laboratorio CIM existen recursos tecnológicos y de integración que permiten simular y automatizar procesos productivos a escala, sirviendo como maquetas o modelos de sistemas industriales reales. Una aplicación típica en la industria es la manipulación y clasificación de objetos utilizando un brazo robótico para moverlos en conjunto con una aplicación de software de control o interfaz gráfica, monitoreo y algoritmos que permitan clasificar estos objetos a partir de su color o de su peso, por ejemplo.

El laboratorio CIM de la UBB permite integrar este tipo de procesos industriales en una asignatura que logra enseñar y capacitar a los alumnos sobre las posibles alternativas que se tienen a nivel académico para poder establecer estrategias de producción relacionadas directamente con la robótica y la automatización de procesos productivos simulando un entorno industrial.

1.2 PLANTEAMIENTO DEL PROBLEMA

El Laboratorio de Sistemas Automatizados de Producción CIM de la UBB siempre innova con respecto a sistemas de manufactura, robótica, gestión de producción, control numérico, automatización y visión por computador. La disponibilidad de estos recursos pedagógicos en la universidad es de alta importancia y de carácter muy valioso para carreras afines a la ingeniería relacionadas a la automatización, electrónica y programación. Su utilización permite generar experiencias prácticas necesarias para la integración de procesos, pero debido a la gran cantidad de estudiantes que se interesan cada día más por la robótica, se genera un colapso en la utilización de sus recursos, ya que es necesario coordinar su disponibilidad y posterior reserva con el personal autorizado en los horarios correspondientes, considerando exclusivamente los bloques de clases de la UBB. Este proyecto permitirá generar y disponer de un recurso valioso para la implementación de experiencias de laboratorio a cualquier hora, previa coordinación con el personal académico y mientras el servidor y las estaciones se mantengan encendidos.



Figura 1.1 – Laboratorio de Sistemas Automatizados de Manufactura.

Es por esto que se propone el diseño y el desarrollo de un sistema remoto del laboratorio CIM, para ser utilizado a través de una conexión remota al escritorio del computador del laboratorio mediante la web, protegido y resguardado por tecnologías y estrategias de seguridad informática implementadas por el grupo de trabajo, con la finalidad de tener un sistema seguro.

Este sistema, entonces, tendrá la capacidad de proveer la conexión remota al servidor del laboratorio, con el objetivo de utilizar una aplicación web desarrollada y desplegada en ese servidor para enviar mensajes mediante la tecnología sockets hacia las estaciones que estén conectadas para establecer la comunicación serial con el brazo robótico a partir de los mensajes que se enviarán desde la plataforma hacia la estación conectada. Se propone una interfaz gráfica del lado cliente lo más amigable e intuitiva posible, además del monitoreo por cámaras que están instaladas en cada estación.

Este sistema deberá actualizarse regularmente respecto a todas sus versiones de software, firmware y hardware, para así mantener una correcta seguridad informática, ya que una de las principales causas de vulnerabilidades informáticas se debe a la desactualización de softwares o de sistemas operativos en los equipos de las víctimas. Se propone actualizar las versiones de software y sistemas operativos como mínimo una vez por semana, automatizando estas tareas para mejorar el desempeño de la aplicación, considerando que se recibirán reportes una vez finalizadas las actualizaciones. Además, continuando con ciber seguridad, se debe garantizar una correcta asignación y encriptación de contraseñas para los usuarios (sean estudiantes o docentes), entre otras estrategias de seguridad de la información que agregarán más capas de seguridad a la aplicación web [1], como autenticación y validación de credenciales, por ejemplo.

Entonces, para poder lograr el correcto funcionamiento de este sistema, se desarrolla una aplicación web basada en la arquitectura cliente/servidor para las solicitudes e interacciones entre los clientes (usuarios) y el servidor, que se definirá a lo largo de este trabajo. En primera instancia, se trabaja de manera local, es decir, se implementa esta arquitectura solamente con los equipos que están disponibles en el laboratorio, dentro de la red local. Para la correcta implementación de este proyecto, el usuario o cliente debe interactuar con la aplicación mediante el servicio de internet, accediendo, enviando y recibiendo solicitudes y respuestas a través de la web mediante el protocolo HTTPS independiente de la geolocalización del estudiante o docente.

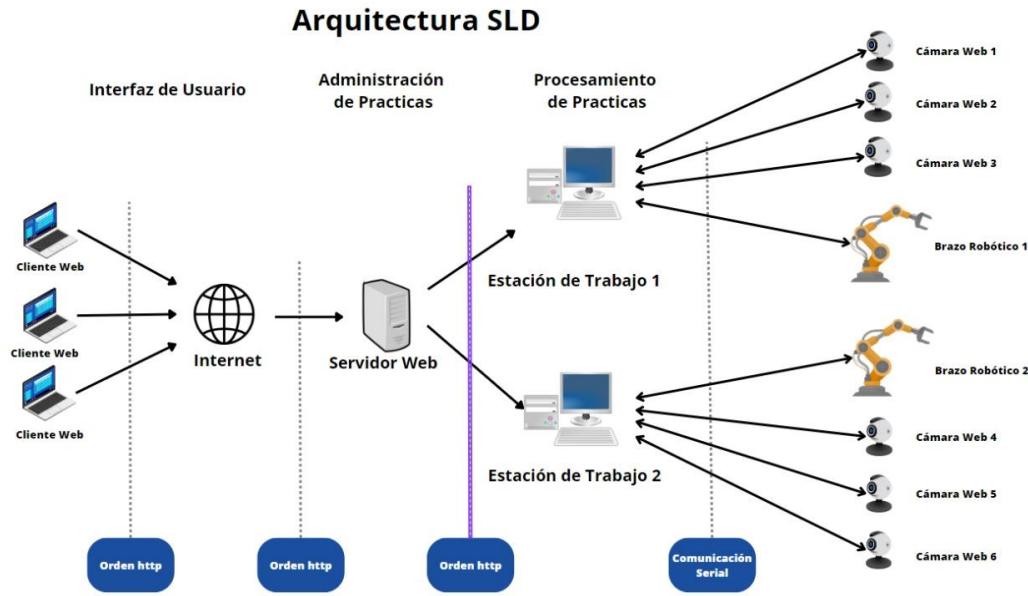


Figura 1.2 – Arquitectura de la aplicación web basada en cliente/servidor.

Una vez dentro de la aplicación, se despliega una ventana principal de acceso, donde el usuario deberá ingresar su correo institucional y su contraseña correctamente. Para esto, se debe haber creado una base de datos que registre a todos los usuarios que tendrán acceso a la plataforma y que valide la información correctamente. En primera instancia, se creará una cuenta de administrador para poder aplicar, integrar y validar todas las funcionalidades de la plataforma, así como también la navegación. Con la cuenta de administrador, se pueden registrar nuevas cuentas de estudiante, profesor y administrador, que corresponden a cuentas que tienen distintas funcionalidades a partir de los distintos roles a definir en este informe.

Estos datos serán recibidos y validados por la base de datos instalada y configurada en el servidor que está en el laboratorio, disponiendo de los recursos del brazo robótico y de esta aplicación web. La plataforma de la aplicación tendrá una función integrada para poder solicitar horarios, previa coordinación con los docentes o el personal a cargo, entre otras funcionalidades que permitirán llevar a cabo una experiencia virtual de laboratorio lo más fiel a una experiencia real. Las solicitudes para utilizar la estación de trabajo del Scorbot se realizan mediante la plataforma, que establece una comunicación entre servidor y estación mediante sockets y el lenguaje de programación Python. Una vez dentro, se podrá escoger la estación a la que se quiera acceder y la rutina que se quiera realizar, o comenzar a registrar puntos para crear nuevas rutinas

y mover el brazo mediante los comandos de la botonera, por ejemplo.

Como se menciona previamente, los datos son administrados por el servidor, que será el ente encargado de permitir acceder e interactuar con cada una de las estaciones disponibles y configuradas para recibir y transmitir información en la red mediante sockets previamente configurados y programados para transmitir datos desde la aplicación hacia los brazos robóticos, independiente de cuantos estén conectados en red. Todo esto está implementado mediante servicios web y programación en Python del lado del servidor, lo que hace que el sistema pueda ser portable a varios dispositivos y sistemas operativos, como Linux, por ejemplo. Además, la interacción permitirá integrar distintas funcionalidades, definidas en el apartado de casos de uso y requerimientos funcionales.

Los datos son enviados desde el servidor, quien será el administrador de las funcionalidades de la plataforma hacia una estación, la cual podrá ejecutar las solicitudes mientras se encuentre disponible y encendida. En caso de que estén ocupadas las estaciones, se deberá escoger la que tenga menos cola por atender. Esta comunicación se realiza mediante sockets entre cada una de las máquinas de la arquitectura cliente/servidor, considerando la red local establecida y preconfigurada en el laboratorio CIM.

La información es ejecutada mediante comandos por consola, que establecen la comunicación serial con el brazo robótico y ejecutan las instrucciones enviadas por la plataforma. Una vez procesados los datos (recibidos e interpretados desde el servidor a la estación), se interpretan en el lenguaje de programación C# en la estación de trabajo, que logra establecer la comunicación entre dicha estación y el brazo robótico, realizando la acción solicitada. Además, siempre se podrá monitorear el comportamiento del robot mediante webcams conectadas de forma serial a cada una de las estaciones de trabajo, pudiendo verificar que las acciones y rutinas se están ejecutando correctamente, o si es que existe algún error en la ejecución, podrá ser alertado siendo visto en tiempo real o con cierta mensajería a desarrollar en algún trabajo posterior a este proyecto de título. La respuesta a este sistema será la ejecución y el control del movimiento del brazo robótico para distintas aplicaciones o actividades académicas.

Ahora, con respecto a la base de datos, contendrá todas las cuentas de usuario creadas, además de las relaciones que se requieren para desarrollar completamente las funcionalidades de este proyecto, ya que se va a requerir de cierta autenticación y validación en base a este registro para poder ingresar a la plataforma y desarrollar las distintas interacciones entre las variables definidas en el proceso para poder ejecutar correctamente cada funcionalidad de esta aplicación. Un usuario que no esté registrado en la base de datos del sistema simplemente no podrá acceder a la aplicación. Por esta razón se propone utilizar el correo institucional de la universidad para crear las cuentas ya que facilita el filtro de las personas que van a ingresar al laboratorio remoto. Estos datos serán recibidos por el lado del servidor, que administrará y permitirá el acceso exclusivamente a las cuentas que estén registradas.

Luego, la aplicación de monitoreo será una vista de la aplicación que se podrá ejecutar desde el mismo sitio web (siempre que el horario solicitado haya sido confirmado por el rol de administrador y que se pueda acceder a una de las practicas o experiencias) y se abrirá en un segmento adicional a la interfaz de control, permitiendo la visualización en tiempo real de la experiencia de forma remota por medio de webcams distribuidas estratégicamente en la estación, con el fin de poder observar el brazo robótico mientras ejecuta la programación y el control definidos por el usuario o estudiante.

Además, se podrá tener un registro de las experiencias de laboratorio correspondientes a cada usuario, almacenadas en un anexo denominado ‘Historial’, que desplegará información histórica de las prácticas que se han llevado a cabo por estudiante, a fin de verificar si el sistema funciona correctamente y si tiene buen desempeño a partir de los registros de cada usuario, que tendrá considerado un historial de errores y los momentos en los que se produce el error en la ejecución y movimiento del Scorbot, con fecha y hora de notificación.

De la misma forma en la que se inicia sesión con alguna de las cuentas de usuario validadas en la base de datos se podrá salir de la plataforma destruyendo la sesión activa actual.

Por último, para concretar una plataforma segura y confiable, se debe contar con la ciberseguridad necesaria para evitar en lo posible ataques de ciberdelincuentes o, en su defecto,

estar preparado para lo peor. Para esto, se debe considerar un correcto manejo y distribución de contraseñas, autenticación de la información, cifrado de datos, actualización de versiones, configuraciones pertinentes en el servidor tanto a nivel de hardware como de software, etc. Es decir, se deben generar patrones y capas de seguridad informática para eliminar en su mayoría las vulnerabilidades que puedan existir o directamente disminuir las brechas de seguridad de la aplicación.

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

- Desarrollar aplicación web para monitoreo y control remoto del robot Scorbob ER Vplus mediante el framework Django programado en Python.

1.3.2 OBJETIVOS ESPECÍFICOS

- Investigar las metodologías, lenguajes y protocolos para la conectividad remota.
- Desarrollar aplicación de escritorio para control y visualización mediante webcams.
- Implementar aplicación web para el ingreso y coordinación del proceso compartido, incluyendo aspectos de ciberseguridad, cifrado y autenticación de información.
- Desarrollar documentación oficial del funcionamiento del programa.

2. ALCANCE DEL PROYECTO

El alcance de este proyecto considera el desarrollo de una completa aplicación web orientada a la utilización, incorporación e implementación de distintas herramientas tecnológicas que permiten la integración de varios sistemas y lenguajes para llevar a cabo los objetivos planteados en primera instancia.

Este capítulo está considerado también para establecer los límites de este trabajo de título, ya que tiene un potencial tremendo para la innovación y el desarrollo tecnológico e integración de herramientas más sofisticadas orientadas al aprendizaje en un entorno universitario. Se pretende detallar las consideraciones y funcionalidades de la aplicación como mínimo proyecto viable, con el fin de orientar el desarrollo hacia un objetivo concreto y evitar desvíos en la planificación del proyecto.

Ahora bien, este trabajo de título comprende el complejo desarrollo de una plataforma orientada al control y monitoreo remoto de las distintas estaciones de trabajo instaladas en el laboratorio CIM de la UBB, que lo diferenciarán de otros proyectos similares y que marcarán una gran diferencia a nivel de desarrollo ya que integra muchas tecnologías en una sola aplicación.

Este sistema, entre otras características, permitirá utilizar de manera remota las funcionalidades de algún brazo robot Scorbob disponible en el laboratorio CIM, comunicándose de manera serial con estos dispositivos. Además, el sistema registrará datos e información que permitirá tener una vista general del historial de las ejecuciones, puntos almacenados y rutinas almacenadas y relacionadas con cada usuario o estudiante. Solamente se considerarán ejecuciones de manera real con el brazo robótico. Se plantea un gemelo virtual para posteriores proyectos relacionados a este trabajo, o relacionados con él.

Además, considerará tres distintos niveles o roles de usuario, cada uno con distintas funcionalidades y módulos relacionados al nivel de usuario correspondiente. Los usuarios solamente podrán ser registrados en la base de datos por el administrador del sistema.

Este sistema, además, permitirá registrar datos que permitirán desplegar información estadística de las prácticas y experiencias realizadas, tanto por estudiantes como por profesores. Por otro lado, los estudiantes sólo podrán acceder a las prácticas de la asignatura en la que estén inscritos, previamente validados por la base de datos y las políticas de seguridad y autenticación integradas en el desarrollo del software. El rol de estudiante podrá solicitar al rol de profesor la reserva de horas para las asignaturas, que podrá, a su vez, confirmar el horario solicitado por el estudiante en caso de que esté disponible la estación.

Previo a listar las características y funcionalidades de esta aplicación, se deben detallar claramente los roles de cada usuario, considerando sus características, funcionalidades, accesos, permisos, entre otras cualidades:

Estudiante: este usuario tiene como funcionalidad principal el control y el monitoreo en tiempo real de una de las estaciones disponibles para esta aplicación. Puede acceder a la vista principal, a la vista de interfaz de control con vista limitada de sus rutinas solamente, a la solicitud de horarios, al historial con vista limitada a sus actividades y a la configuración de cuenta.

Profesor: este rol de usuario tiene como funcionalidad principal la confirmación de horarios y el monitoreo y supervisión de las actividades de cada experiencia de laboratorio. Puede acceder a la vista principal, a la vista de interfaz de control con vista privilegiada de las rutinas, a la confirmación de horarios, vista de solo lectura de las asignaturas, al historial con vista privilegiada de todos los estudiantes y a la configuración de cuenta.

Administrador: este rol de usuario tiene como funcionalidad principal la de administrar todas las características, funcionalidades, vistas, usuarios, asignaturas, rutinas, mantención, estaciones, cámaras. Tiene acceso a todas las vistas de la aplicación y tiene permisos privilegiados dentro de la plataforma. Puede crear, editar y eliminar usuarios, asignaturas, rutinas, puntos.

Ahora se listan las distintas características y funcionalidades a grandes rasgos de este software:

- Selección de estación: La aplicación incluirá una selección de una de las tres estaciones, considerando la disponibilidad y el estado del brazo robótico.
- Interfaz de control y monitoreo: El sitio web incluirá una interfaz con las funcionalidades de monitoreo en tiempo real de la estación seleccionada, control del brazo robótico mediante la botonera, almacenamiento de puntos en la memoria del Scorbot y creación de rutinas para el brazo robótico.
- Almacenamiento de puntos: Los usuarios validados de la universidad y que puedan acceder a una estación disponible podrán almacenar puntos en la interfaz de control, logrando el movimiento del brazo robótico a una posición deseada mediante una réplica funcional de la botonera física.
- Historial: Los usuarios podrán revisar el historial de sus experiencias de laboratorio, con detalles valiosos para el monitoreo y la mejora continua del desempeño de esta aplicación.
- Solicitud de horarios: Los usuarios con el rol de estudiantes podrán solicitar horarios para uso del brazo robótico, siendo confirmados por el rol de profesor, quién será el encargado de administrar la disponibilidad de las estaciones de trabajo.
- Registro de usuarios: Esta funcionalidad es exclusiva para el rol de administrador, quien tendrá la capacidad de crear nuevas cuentas de usuario, editar, eliminar, definir roles y otras características.
- Configuración de cuenta: Cada usuario tendrá un panel en el que podrá modificar y actualizar su información.

Con respecto a la tecnología, en el capítulo 4 se detalla más a fondo cada software, lenguaje de programación y herramienta utilizada e implementada para el desarrollo de esta aplicación. Principalmente, el entorno de programación utilizado es Django, del lenguaje de programación de alto nivel Python. Se escoge este framework ya que es bastante sólido en cuanto a navegación, ruteo y mapeo de vistas, tiene buenas capas de seguridad integradas en su sistema, cuenta con un propio servidor para aplicaciones, permite la incrustación de código HTML, CSS,

JavaScript y PHP de manera sencilla y amigable, además de que se puede ejecutar código Python nativo en la misma aplicación. Cuenta con una fácil sincronización con bases de datos, panel de administración, entre otras múltiples funcionalidades que lo posicionan dentro de las mejores tecnologías para desarrollo web.

Las limitaciones de este proyecto se relacionan directamente a problemas de alimentación eléctrica o disponibilidad de las estaciones de trabajo.

3. ESTADO DEL ARTE

En esta etapa del proyecto se investiga sobre las tecnologías más recientes con respecto al área que engloba este tipo de proyectos y aplicaciones.

Si bien se vienen implementando estas nuevas herramientas desde hace un par de años, no fue sino con la pandemia mundial que se les tomó real importancia a estas plataformas digitales, ya que tanto alumnos como docentes se vieron en la necesidad de extrapolar ciertas experiencias prácticas de clases y de laboratorio a las nuevas condiciones de trabajo y aprendizaje.

Esta nueva metodología para asistir a clases, mejor conocida como e-learning, es la responsable de preparar y certificar a los nuevos profesionales, por lo que se deben aprovechar al máximo los recursos tecnológicos con el fin de optimizar las condiciones de aprendizaje y que, en vez de ser un problema, se generen nuevas instancias y un acercamiento a la tecnología por parte de alumnos y profesores.

Una de las estrategias utilizadas para facilitar el aprendizaje es la conocida como laboratorio remoto, que cuenta con sistemas informáticos con herramientas y funcionalidades suficientes para recrear un laboratorio de manera virtual. Además, cuentan con todos los dispositivos, plataformas, instrumentos, controles y acceso a equipos reales, lo que permite utilizar el laboratorio convencional existente, pero de forma virtual.

La demanda de este tipo de experiencias ha llevado a que incluso se ofrezcan servicios de laboratorios remotos. Uno de sus grandes exponentes en español es LabsLand, una plataforma en la que se puede acceder mediante internet a laboratorios reales que se pueden controlar a través de un ordenador sin necesidad de preinstalar nada. Se trata de laboratorios de alta calidad para diversos niveles educativos y distintas asignaturas, implementados en colegios y universidades [2]. Además, permite gestionar un espacio propio personalizado, gestionar estudiantes, horarios, entre otras funcionalidades.



Figura 3.1 – Logo LabsLand.

El servicio de LabsLand cuenta con laboratorios remotos de química, robótica, flotabilidad, entre otros, que permiten la experiencia práctica y didáctica con elementos que corresponden a las asignaturas antes mencionadas.

Así mismo, existen otras plataformas como eLAB/TeleLab que están diseñadas para interactuar de forma online con laboratorios de instrumentación industrial. Los estudiantes pueden cargar y descargar programas en un PLC directamente a través de internet. Este controlador está físicamente cableado a un proceso real a escala, con sensores y actuadores reales. Un sistema de audio y video le permite al estudiante monitorear y escuchar en tiempo real, mientras realiza la experiencia.



Figura 3.2 – Logo eLab/TeleLab.

De la misma forma, existen otras plataformas que permiten el acceso remoto a laboratorios de informática para estudiantes y para profesores, como la plataforma virtual Splashtop, que proporciona acceso remoto a su laboratorio físico en franjas de horarios

programadas. Esta plataforma permite acceso a ordenadores Windows o Mac, que suelen utilizar una combinación de herramientas de hardware y de software específicas que no se pueden transferir a la nube. Splashtop tiene su propio software de escritorio remoto y ofrece a los usuarios una forma sencilla y segura de controlar remotamente los ordenadores y las máquinas virtuales de la escuela, universidad o distrito en tiempo real desde cualquier otro dispositivo.



Figura 3.3 – Logo Splashtop.

Gracias al software de escritorio de Splashtop, el usuario puede acceder y tomar control de los computadores desde sus propios dispositivos, ya sea Windows, Mac, Chromebook, iPads, Android, etc. Una vez conectados, podrán visualizar la pantalla de la computadora remota en su propio dispositivo y podrán utilizar cualquier aplicación o archivo como si estuvieran sentados frente a él.

Este tipo de laboratorios y experiencias remotas son elementos esenciales de los programas que verdaderamente son eficaces dentro del aprendizaje híbrido, ya que, al ser capaces de acceder de forma remota a los distintos laboratorios, aseguran que los estudiantes y profesores tengan los mismos recursos informáticos disponibles como si estuvieran de forma presencial y además con acceso desde cualquier dispositivo, en cualquier lugar y en cualquier momento.

La Universidad de Susquehanna, por ejemplo, también cuenta con un sistema de conexión remota a sus laboratorios y computadores de la institución, llamado Remote Labs. Esta interfaz permite conectarse a los distintos ordenadores instalados en el campus de la universidad, y se puede tratar de un equipo con sistema operativo Windows o Mac.



Figura 3.4 – Universidad Susquehanna.

Al igual que Susquehanna, la Universidad de Edinburgh y la Universidad de Londres también implementan este tipo de sistemas virtuales llamado Remote Labs, con el enfoque claro en mantener la calidad de aprendizaje y la conectividad en el acceso a experiencias prácticas a pesar de la distancia.

A su vez, con respecto al área de la electrónica embebida y a la programación de microcontroladores, existen distintas implementaciones como trabajos académicos de nivel superior que se han encargado de realizar plataformas en línea o valerse de distintas tecnologías para integrar sistemas de laboratorios remotos con dispositivos embebidos, como el proyecto de “Implementación de un Laboratorio Remoto de Arduino con Raspberry Pi” [3], “Mejora de un laboratorio remoto de electrónica digital mediante el uso de una Raspberry Pi 4” [4] y “Laboratorio remoto para experimentación sobre Internet de las Cosas” [5].

Este tipo de experiencias prácticas y experimentos con procesos reales, pero a distancia, permiten consolidar los conceptos y la información adquirida en las aulas teóricas y en la investigación personal de cada estudiante. A pesar incluso de la modalidad remota, las experiencias de laboratorio se mantienen activas en la malla del estudiante gracias a las nuevas tecnologías basadas en comunicación web y en el internet de las cosas, que pueden ser utilizadas e integradas para mejorar la accesibilidad a los experimentos de laboratorio [6].

En Chile igual se han implementado sistemas robotizados para la facilitación de instancias académicas, como, por ejemplo, la implementación del robot Swivl, que es un sistema robótico de movimiento y tracking, es decir, sigue al usuario en forma automática, pudiendo operar en un rango de hasta 9 metros. Cuenta con una visión panorámica de 360°, inclinación de 25°, tiene aplicaciones compatibles con sistemas iOS y Android, almacenamiento en la nube, audio inalámbrico y puertos de comunicación.



Figura 3.5 – Robot Swivl.

Este tipo de equipos robotizados se han integrado a las distintas metodologías para impartir clases en pandemia. De hecho, el año 2021 se implementaron estas tecnologías en clases remotas en las escuelas de Chillán [7], con el objetivo de mejorar la calidad de la interacción entre profesores y alumnos y apoyar a los establecimientos educacionales en la realización de clases remotas o híbridas. Estos robots realizan seguimiento automático del profesor por todo el salón de clases, controlados por Tablet y asentados por trípodes, garantizando la estabilidad del robot a pesar del movimiento. Además, estos dispositivos facilitan que los directivos y los docentes de los establecimientos concreten el desafío de mantener la continuidad de las clases y asegurar una educación a distancia de calidad.

Ahora, el monitoreo remoto se ha transformado en una herramienta valiosísima a nivel tecnológico, independiente de la aplicación que se desee desarrollar. Gracias a estas tecnologías y herramientas, es posible tener un control y una visualización en tiempo real de variables, datos, marcos de trabajo, frames, dashboards, procesos, robots, industria, entre miles de aplicaciones variadas en cuanto a tecnología. La integración de un sistema de visión en tiempo real en el laboratorio, o en la estación de trabajo que se desea experimentar y trabajar permite llevar un monitoreo del espacio físico del laboratorio independiente del lugar donde se esté ubicado. Por ejemplo, al lograr que la interfaz de monitoreo permita tener en tiempo real cámaras mostrando las instalaciones del establecimiento, es posible llevar un correcto procedimiento al mover el robot independiente de su aplicación.

Esto limita los comportamientos no deseados del brazo antropomórfico ya que se pueden observar mediante video los puntos críticos del lugar físico, con el fin de no estropear o golpear el robot a medida que se va moviendo mediante la interfaz de control.

Gracias al desarrollo mediante lenguajes de programación orientados a las acciones del servidor, es posible acceder a los dispositivos multimedia de la estación, como cámaras y micrófonos, por ejemplo, para lograr una completa integración de dispositivos y un completo aprendizaje durante la experiencia práctica del laboratorio.

Los lenguajes implementados para lograr la interfaz de monitoreo son JavaScript y PHP, que, mediante sus funciones integradas y una correcta lógica de programación del lado del servidor, es posible integrar los dispositivos que permiten la transmisión de vídeo en tiempo real.

Por otro lado, la plataforma de control, que claramente mueve al robot y permite ejecutar distintas rutinas, además de guardar puntos para poder establecer movimientos programados por el usuario, está también desarrollado con lenguaje PHP del lado del servidor, integrando, además, lenguajes de programación que permiten la comunicación serial como C# o Python para enviar datos seriales por el puerto de comunicación hacia el robot Scrobot. Independiente del lenguaje, es posible comunicarse con el brazo robótico fácilmente mediante pequeños scripts programados, cada uno integrado en cada botón.

Luego de establecer los distintos programas que se comunican con el robot mediante la interacción con el usuario, se programan varios archivos por lotes que serán ejecutados a nivel de consola en el servidor que está conectado al brazo robótico, con el fin de poder ejecutar varias acciones en segundo plano mientras el Scrobot está en línea con el usuario, el cual puede monitorear cada movimiento a través de la interfaz o plataforma de monitoreo que contiene la transmisión mediante cámaras de la estación de trabajo.

Una vez integradas todas estas tecnologías y ficheros, es posible dar rienda suelta al usuario o cliente para que pueda interactuar con la plataforma y que logre así replicar una experiencia de laboratorio lo más cercana a la realidad.

4. SCORBOT-ER VPLUS

Previo al desarrollo y arquitectura del software como tal, se debe esclarecer e identificar el dispositivo que tendrá el papel principal en esta aplicación. Fuera del desarrollo web, el brazo robótico Scorbob-ER Vplus debe ser detallado y analizado mecánicamente y a nivel de comunicación y transmisión de datos. Se trata de un robot vertical articulado de tipo antropomórfico, diseñado para formación, investigación y aplicaciones en laboratorio de tipo académicas. Cuenta con cinco articulaciones (base, hombro, codo, inclinación de la pinza y giro de pinza). Su controlador autónomo trabaja en tiempo real, permitiendo ejecutar simultánea e independientemente hasta un total de 20 programas en memoria. El entorno interno del controlador incluye el lenguaje ACL, que se compone de listas de reglas que detallan puertos de servicio disponibles en las terminales del robot con capacidades de programación avanzada multitarea en tiempo real. Se trata de un robot rápido, seguro, flexible y fiable para aplicaciones académicas. El laboratorio CIM de la UBB tiene uno de estos dispositivos robóticos totalmente funcional y programable por los mismos estudiantes, que cumple el rol protagonista a nivel de ejecución en este trabajo de título.



Figura 4.1 – Brazo Robótico Scorbob-ER Vplus.

Para una documentación mucho más detallada con respecto a este equipo, existe un manual de usuario bastante completo donde se puede obtener información importante con respecto al Scorbot-ER Vplus, como, por ejemplo, las conexiones del robot, la instalación, los drivers, armado, programación, etc. [8].

4.1 COMPONENTES MECÁNICOS DEL ROBOT

Este robot está diseñado para replicar un brazo antropomórfico, por lo que se recurre a la integración de distintos elementos mecánicos, componentes y dispositivos electrónicos para lograr un buen desempeño en el movimiento de cada uno de los ejes y servomotores del Scorbot.

La localización y el movimiento de cada eje de este robot son medidos por un codificador óptico integrado al eje de cada uno de los motores que lo componen, con orificios alrededor de este. Entonces, cuando el eje del robot se mueve, el codificador transmuta la señal analógica medida por un sensor fotosensible a una serie de pulsos eléctricos. La cantidad de pulsos medidos es proporcional a la cantidad de movimiento rotacional de cada eje. Es decir, el controlador toma los pulsos obtenidos de esta manera y dependiendo de cuantos sean, determina la nueva posición angular de cada motor que compone al brazo robótico.



Figura 4.2 – Encoder o codificador.

Además, incorpora micro interruptores en cada articulación que establecen los límites físicos para el movimiento de los ejes. Estos dispositivos sirven para que no existan choques entre las articulaciones del robot. Cuando todos los interruptores están activados, significa que el brazo está ubicado en la posición de referencia o “Home”. Al encender el sistema, el robot debería ser enviado a dicha posición mediante una instrucción que se realiza inmediatamente al ingresar a la plataforma de control remoto.

El Scorbob está provisto de una pinza mecánica con cojines de agarre de goma, que pueden ser removidos para acoplar otro tipo de componentes, como herramientas de succión, cámaras, etc. De esta forma, se extienden las posibilidades de control y de programación de este brazo robótico, ya que se pueden implementar distintos dispositivos que pueden servir de herramienta al robot y así se pueden desarrollar distintos programas para distintas aplicaciones de la estación de trabajo.

Las articulaciones del brazo robótico y la pinza son operadas por servomotores de corriente continua. El sentido del giro y la posición angular de cada servomotor definen la posición de un eje o bien el estado de la pinza. Dependiendo de la polaridad del voltaje de operación aplicado a los servomotores, se tiene un sentido en el giro de cada servomotor, que tiene integrado un codificador para lograr el control refinado de cada movimiento. De esta forma se logra el movimiento controlado de cada articulación, siendo parametrizada desde la interfaz de control desarrollada en el trabajo de título previo.

La interfaz de control permitirá abrir y cerrar la pinza, mover cada eje por separado, cambiar el modo de operación de manual a automático, ejes a XYZ, encender o apagar motores, cambiar velocidad, entre otras funcionalidades. Además, se tiene integrada una réplica semi completa del teach pendant que está en el laboratorio y que sirve de interfaz de control y movimiento del robot, que se comunica y da instrucciones al brazo robótico de forma serial, replicando la botonera de operación del robot.

En este proyecto no se considera el modelamiento matemático del Scorbob ya que eso fue correspondiente al trabajo de título previo, por lo que se establece el enfoque de este proyecto de título netamente a la programación y logros de los objetivos con respecto a generar un sistema de

laboratorio remoto mediante programación web e instrucciones para comunicación serial con el servidor instalado en el laboratorio que da vida a la estación o estaciones de trabajo en la que están instalados los Scrobot-ER Vplus. De cualquier manera, es posible encontrar el procedimiento teórico y las demostraciones de los movimientos cartesianos, angulares y de la cinética del brazo robótico en la documentación de “Fundamentos de la Robótica” [9] y en el libro de Peter Corke “Robotics, Vision and Control” [10], además de los apuntes y video clases del docente de la Universidad del Bío-Bío, Ángel Ernesto Rubio.

Todo esto es considerado como la interfaz de hardware de este proyecto, que integra un servidor como cerebro de las demás ramas de la red, que corresponden a las estaciones de trabajo conectadas en serie con un brazo robótico. El estudiante debe contar estrictamente con los periféricos comunes y básicos para la navegación en un computador portátil, como lo son un mouse, un monitor y un teclado, por lo menos. Para el monitoreo de la ejecución de esta aplicación, se consideran tres webcams por estación, que permitirán mostrar en tiempo real el video de la estación y la rutina o puntos de movimiento que se están ejecutando en el laboratorio.

El desarrollo de software y su correcta arquitectura, interfaz y definiciones se detallarán a continuación.

4.2 TECNOLOGÍAS

En este capítulo se detallan y especifican las distintas tecnologías que servirán de soporte para lograr el desarrollo de este proyecto. Considerando que casi la totalidad de este trabajo es desarrollado mediante software y lenguajes de programación, este desglose se enfoca en dichas herramientas.

| | |
|---|---|
|  | HTML es un lenguaje de marcado para la elaboración de páginas web. Se trata de una estandarización que define una estructura básica y código especializado para definir el contenido de una página web. |
|  | CSS es un lenguaje de diseño gráfico para definir y crear la presentación de un archivo estructurado HTML. |
|  | PHP es un lenguaje de programación que se adapta especialmente al desarrollo web. Permite interactuar fácilmente con una base de datos. |
|  | XAMPP es un entorno para trabajar con PHP. Es una distribución de Apache gratuita y fácil de instalar. |
|  | MySQL es un sistema de administración de bases de datos relacionales. Utiliza múltiples tablas para almacenar y organizar la información de la aplicación web. |

| | |
|---|--|
|  | <p>Bootstrap es un conjunto de herramientas para diseño de aplicaciones web. Contiene plantillas con distintos elementos basados en HTML y CSS.</p> |
|  | <p>Visual Studio Community es un entorno de desarrollo bastante completo, extensible y gratuito para crear aplicaciones modernas para distintos sistemas operativos.</p> |
|  | <p>Python es uno de los lenguajes de programación más utilizados en la actualidad. Permite trabajar de forma rápida e integra sistemas efectivamente.</p> |
|  | <p>Fing es un escáner de red, permite descubrir todos los dispositivos conectados a la misma red, identificándolos para trabajar con ellos.</p> |
|  | <p>JavaScript es un robusto lenguaje de programación que se puede aplicar a un documento HTML y usarse para crear interactividad dinámica en los sitios web.</p> |
|  | <p>Git es un sistema de control de versiones distribuido para realizar un seguimiento de los cambios en el código de software durante el desarrollo del mismo. Permite que varios desarrolladores colaboren en la misma base de código</p> |
|  | <p>Miro es una herramienta de colaboración en línea que permite a los equipos trabajar juntos en proyectos, diagramas, diseños, notas y mucho más. Es una aplicación web que permite a los usuarios crear, compartir y colaborar en tableros visuales.</p> |

| | |
|---|--|
|  | <p>Django es un framework de desarrollo web de alto nivel y de código abierto, escrito en Python. Se enfoca en la eficiencia, reutilización y eliminación de trabajo repetitivo.</p> |
|  | <p>GitHub es una plataforma de alojamiento y colaboración de código fuente para proyectos de software. Permite a los desarrolladores alojar su código fuente en línea y colaborar con otros desarrolladores para trabajar juntos en proyectos de software.</p> |

Tabla 4.3 – Tecnologías implementadas para el desarrollo de la aplicación web y control del robot.

4.4 COMUNICACIÓN SERIAL CON EL SCORBOT

A continuación, se documenta el procedimiento para establecer correctamente la conexión serial y comunicación con el brazo robótico.

En primer lugar, el Scorbob debe estar conectado a un puerto COM del equipo o estación de trabajo, representado físicamente por un computador de torre instalado en la red local del laboratorio CIM. Se debe verificar que el Scorbob pueda ejecutar movimientos o rutinas directamente desde la estación de trabajo, de esta forma, se puede asegurar que el servidor envíe las peticiones para que el brazo logre moverse a partir de esta conexión en red.

Para cada estación de trabajo se establece una comunicación serial con 9600 baudios de velocidad, 8 bits de datos, sin paridad y con 1 bit de parada. Estos parámetros de comunicación quedarán establecidos en el programa y no serán modificables desde la interfaz de usuario del lado cliente. El puerto quedará establecido mediante la programación y pre configuración que será definida a nivel de hardware, es decir, por equipo. Esto quiere decir que las estaciones de trabajo deben tener una dirección IP fija para que puedan establecer la conexión segura y estable con las peticiones que el servidor les envía.

Ahora, la interfaz de control instalada y montada en el servidor remoto dispuesto en el laboratorio permite enviar mensajes por protocolo HTTPS a las estaciones, que se reciben y ejecutan mediante la definición y configuración de sockets en cada dispositivo, además de ciertas funciones del lenguaje de programación Python que permitirán establecer correctamente el envío y recepción de mensajes, datos y archivos entre computadores conectados en la misma red. Es por esto que el proceso de configuración previa en la red local es fundamental para el desarrollo de esta aplicación.

En cada estación existirá un archivo Python que estará escuchando permanentemente los mensajes que se le envían mediante plataforma, para así ejecutar movimientos y comandos a partir del mensaje enviado desde el servidor hacia la estación.

5 DISEÑO DE SOFTWARE

Este capítulo pretende explicar y detallar el procedimiento paso a paso para lograr el desarrollo de la aplicación web que permitirá controlar el brazo robótico y monitorear en tiempo real el movimiento del Scorbot, comenzando principalmente por la etapa de diseño de software. Para lograr abarcar correctamente todo el diseño y desarrollo de esta aplicación, se adjuntarán a este documento ciertos entregables que intentarán cubrir la mayor parte del diseño y desarrollo del software, desde el diseño preliminar de la aplicación hasta el manual del usuario final.

Para la primera etapa del desarrollo de software web como tal, se propone una planificación y diseño de la plataforma o interfaz de control y monitoreo, que servirá para identificar la navegación del sitio web y las distintas vistas que se podrán desplegar tanto para los usuarios con rol de administrador como para los de profesor y estudiante. Adjunto a este informe se entregará un documento con todas las vistas de la aplicación y los accesos que tendrá cada rol de usuario. Este entregable es conocido dentro del mundo del desarrollo como Mockup.



Figura 5.1 – Login de usuario.

Una vez definido el diseño preliminar o mockup de la aplicación web, se utiliza el software de control de versiones Git que es esencial para administrar los cambios que se realizan al código a través del tiempo, sobre todo considerando que se trata de un desarrollo tanto del lado del cliente, como del lado del servidor. Este control de versiones permite fácilmente seguir los

cambios realizados al proyecto, desarrollar la aplicación en modo colaborativo e incluso poder volver a versiones anteriores del proyecto si es necesario. Tener un proyecto en un repositorio en la nube es bastante beneficioso ya que prioriza la disponibilidad e integración del código y de los ficheros al momento de necesitarlos.

Luego del diseño de la interfaz de usuario, corresponde la entrega y documentación de los requerimientos funcionales de esta aplicación o software. Esta documentación considera las características específicas y las funciones que la aplicación debería proveer para satisfacer las necesidades del usuario final.

Principalmente se debe considerar la autenticación de los usuarios. Esta aplicación le permite exclusivamente al rol de administrador crear distintas cuentas de usuario, permitir iniciar sesión con dichas cuentas y también poder cerrar la sesión. La aplicación también debería tener integrado un sistema de recuperación de contraseñas y una vista con funcionalidades para administrar la cuenta de usuario.

También se debe tener en consideración la definición formal de los distintos roles de usuario y los permisos y accesos que tiene dentro del sitio web. Esta aplicación les permite a los administradores poder gestionar los distintos roles de usuario y sus permisos dentro de la plataforma, tanto como para permitir el acceso a ciertas vistas, como también para restringir ciertos accesos a otras vistas dentro de la aplicación. A pesar de que se definieron los roles al principio de este documento, se ahondará con mayor profundidad en este capítulo, donde se declararán y especificarán todas las funcionalidades y los distintos permisos que tendrá cada rol de usuario para este software.

Considerar que el administrador, así como puede crear cuentas de usuario, también tendrá los permisos para poder leer, actualizar y eliminar cuentas de usuario y asignaturas, dependiendo de lo que se requiera. El alcance de este proyecto de título solo considera una asignatura por defecto, pero para futuros proyectos se podrían integrar distintas asignaturas, experiencias, capacitaciones, etc.

La navegación fue diseñada y desarrollada de forma tal que sea lo más amigable con el usuario, considerando también que se podrá utilizar por cualquier usuario validado de la Universidad del Bío - Bío. Además, se incluye un módulo de reportes, mensajería y análisis dentro de la aplicación que provee información valiosa respecto a la actividad del usuario, estación utilizada, errores de movimiento, mal desempeño del control y del monitoreo, etc. Se adjunta, además, un documento adicional que tiene considerado todos los posibles errores y escenarios con el fin de lograr solucionarlos una vez la aplicación sea desplegada, conocido como Troubleshooting dentro del mundo del desarrollo.

Luego de desplegar la aplicación, se debería pasar a la etapa de mantenimiento y de mejora continua, lo que debería considerar la integración de servicios externos, el futuro crecimiento y la incorporación de nuevas herramientas, estaciones, brazos robóticos, etc.

A continuación, se detalla minuciosamente la etapa de requerimientos funcionales, que permitirá representar lo que la aplicación finalmente realizará mediante la definición de características y funcionalidades.

5.1 REQUERIMIENTOS FUNCIONALES

El primer paso para la documentación de los requerimientos funcionales de este software es declarar el alcance, que fue definido preliminarmente en el capítulo 2, dedicado a la declaración formalizada del alcance de este proyecto.

Luego, se deben detallar los requerimientos funcionales del sitio web, considerando el rol de usuario estudiante como el consumidor final de las funcionalidades de la plataforma:

- El usuario será capaz de seleccionar una de las estaciones del laboratorio CIM, siempre y cuando esté encendida y disponible, previa confirmación con el profesor.
- El usuario será capaz de visualizar en tiempo real el monitoreo mediante video del estado actual del brazo robótico. Dentro de esa misma vista, el usuario será capaz de seleccionar entre la función de control directo por la botonera o el control mediante

rutinas con puntos almacenados y comandos generales.

- Para la funcionalidad de botonera, el usuario será capaz de utilizar todas las funciones que tiene incorporada el teach pendant, tanto como mover cada eje por separado, como también ejecutar comandos generales como home, open, close, etc.
- Para la funcionalidad de rutinas, el usuario será capaz de seleccionar puntos almacenados en memoria, comandos, delay y velocidad. Además, podrá agregar más puntos a medida que los necesite. También será capaz de almacenar las rutinas en memoria y listar las que ya estén almacenadas con su cuenta de usuario.
- El usuario será capaz de visualizar el historial de experiencias y accesos vinculado a su cuenta de usuario.
- El usuario será capaz de solicitar un horario para acceder a una estación deseada y así no perjudicar el desempeño de la aplicación en caso de no tener acceso a una estación de trabajo. El usuario con rol de profesor tendrá la funcionalidad de confirmar dichos horarios solicitados por algún estudiante.
- El usuario será capaz de modificar ciertas características y parámetros personales de su cuenta de usuario.
- El usuario con rol de administrador podrá crear, ver, actualizar y eliminar usuarios, asignaturas, puntos, rutinas.

A continuación de la etapa de requerimientos funcionales, y como complemento a esta documentación, se deben detallar los casos de uso y las historias de usuario para la aplicación web RemoteCIM, que serán entregadas en un archivo adjuntado a este informe.

5.2 CASOS DE USO E HISTORIAS DE USUARIO

Los casos de uso son la mejor forma de capturar los requerimientos funcionales de la aplicación al describir cómo los usuarios van a interactuar finalmente con el sistema para lograr sus objetivos. Para este trabajo de título, los casos de uso van a consistir en un objetivo principal, actores que interactuarán con el sistema y una serie de pasos o mejor conocidos como escenarios, que describen detalladamente cómo el usuario final logra el objetivo.

Con respecto a las historias de usuario, serán adjuntadas como complemento a este informe, ya que, si se detallan en este mismo documento, se extendería demasiado y no se lograría el orden y el formato con el que fueron diseñadas.

Estrictamente, todos los usuarios que vayan a interactuar con esta plataforma deben ser de la Universidad del Bío-Bío, ya sea como alumno regular o como académico validado. Para esto se deben realizar filtros y cuentas de usuario con el correo institucional, con el objetivo de evitar brechas de seguridad y posibles ataques al sitio web.

Además de la aplicación como tal, se debe considerar una base de datos que almacene la información de todos los usuarios, puntos almacenados, rutinas, historial, etc. Considerar también el uso de servidores, tanto para la aplicación, como para la base de datos. Una vez desplegada, una buena mejora para este desarrollo sería poder incorporar un servicio externo de hosting y dominio para este sitio web, como, por ejemplo, servicios de infraestructura en la nube.

Los actores de este sistema serán los mismos usuarios, ya que no se cuenta con la interacción de otros sistemas o servicios externos. Para este proyecto de título, los actores serán los usuarios con rol de estudiantes, rol de profesores y rol de administradores, cada uno con objetivos concretos y flujos de usuario definidos a continuación.

| | |
|--------------------------|--|
| ID | Actor 1 |
| Rol | Administrador |
| Descripción | El administrador del sistema, definido como un académico responsable o un miembro de confianza de la universidad, con perfil deseado de administrador de sistemas informáticos. |
| Responsabilidades | Administrar la plataforma considerando todas sus funcionalidades, vistas, características, usuarios, rutinas, asignaturas, puntos almacenados. Además, debe prestar soporte y mantención una vez desplegada la aplicación. |

Figura 5.2 – Rol de administrador.

| | |
|--------------------------|---|
| ID | Actor 2 |
| Rol | Profesor |
| Descripción | Docente perteneciente al Departamento de Ingeniería Eléctrica y Electrónica de la Universidad del Bío - Bío. |
| Responsabilidades | Encargado de la gestión de asignaturas y la asignación de experiencias prácticas mediante la vista de confirmación de horarios. Puede monitorear y analizar el historial de todos los usuarios con rol de estudiante. |

Figura 5.3 – Rol de profesor.

| | |
|--------------------------|--|
| ID | Actor 3 |
| Rol | Estudiante |
| Descripción | Estudiante perteneciente a la Universidad del Bío - Bío. Debe estar validado como alumno regular y debe permanecer al menos a una asignatura donde se implemente esa plataforma. |
| Responsabilidades | Encargado de realizar las experiencias prácticas de ejecución de control y monitoreo del brazo robótico. Puede almacenar puntos y rutinas. |

Figura 5.4 – Rol de estudiante.

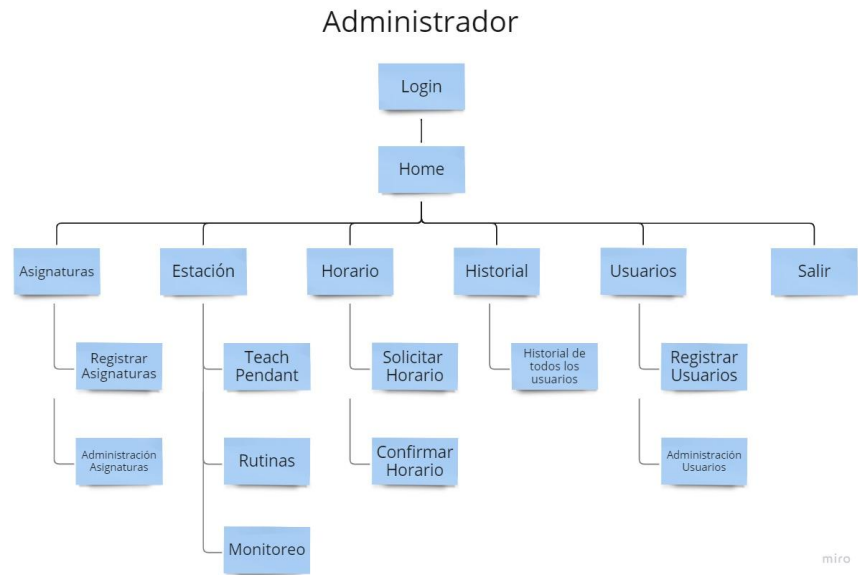


Figura 5.5 – Flujo de usuario con rol de administrador.

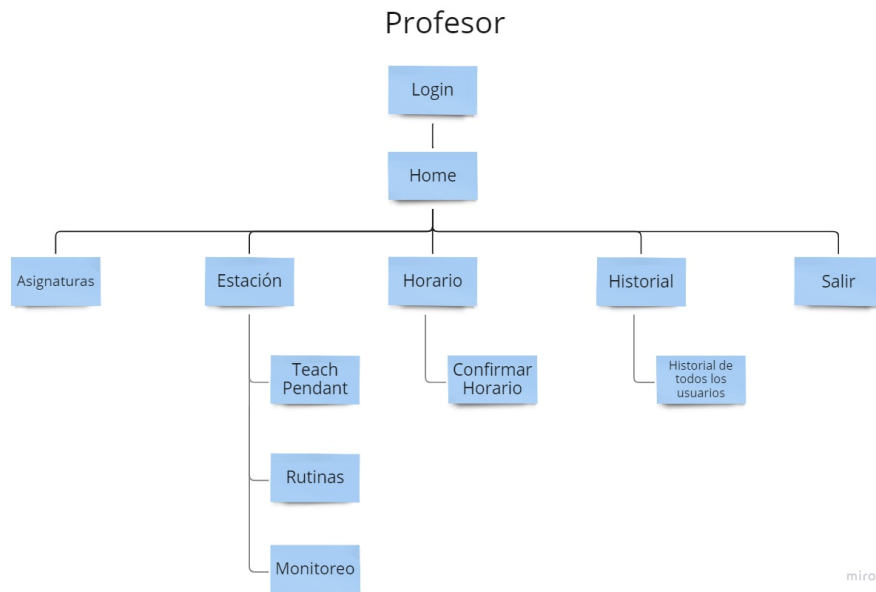


Figura 5.6 – Flujo de usuario con rol de profesor.

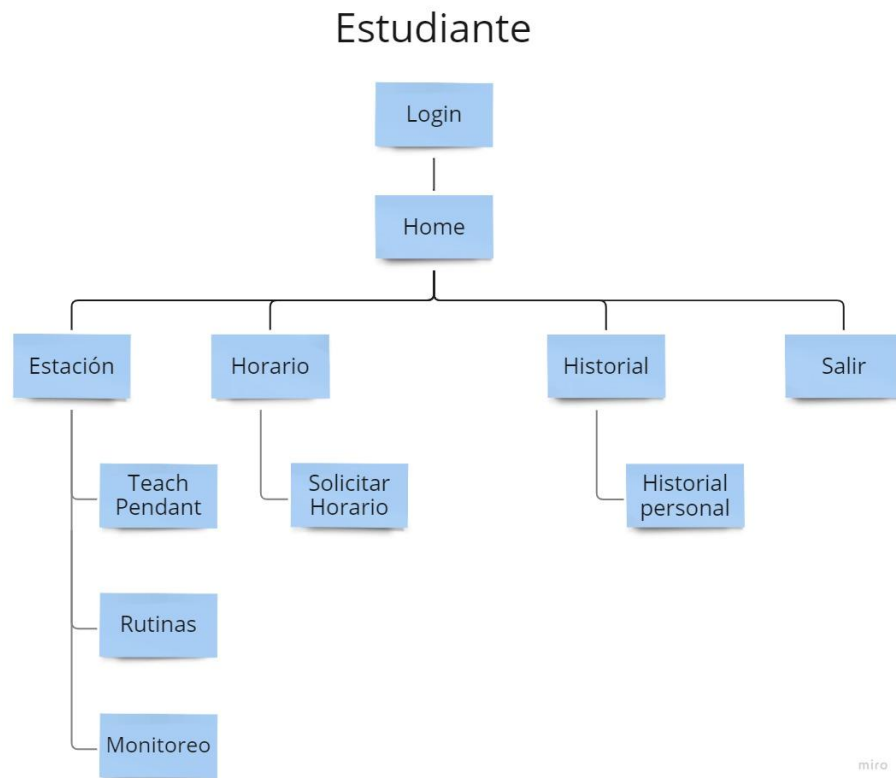


Figura 5.7 – Flujo de usuario con rol de estudiante.

5.3 DIAGRAMA DE CASOS DE USO

A continuación, se presentan los diagramas que representan los casos de uso, llamados diagramas de casos de uso. Este es una representación gráfica de las interacciones entre los actores (usuarios) y el sistema en términos de los casos de uso, que se definen como los objetivos o tareas que los actores quieren lograr con cierta funcionalidad o con el sistema.

Los actores se representan por figuras stick y los casos de uso son representados por óvalos. Las flechas indican la comunicación entre los actores y el sistema, y puede ser etiquetado para mostrar la naturaleza de la interacción.

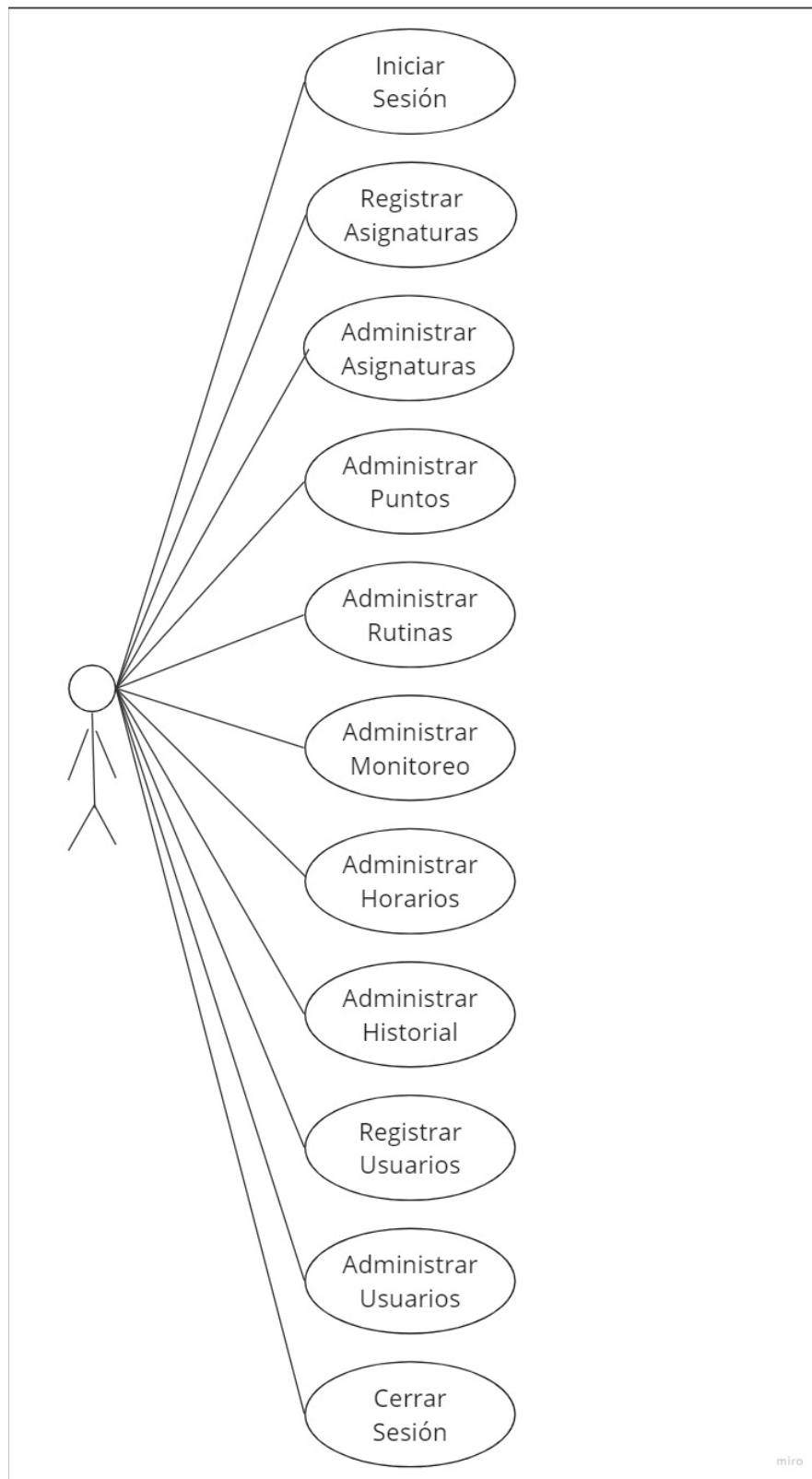


Figura 5.8 – Casos de uso para rol de administrador.

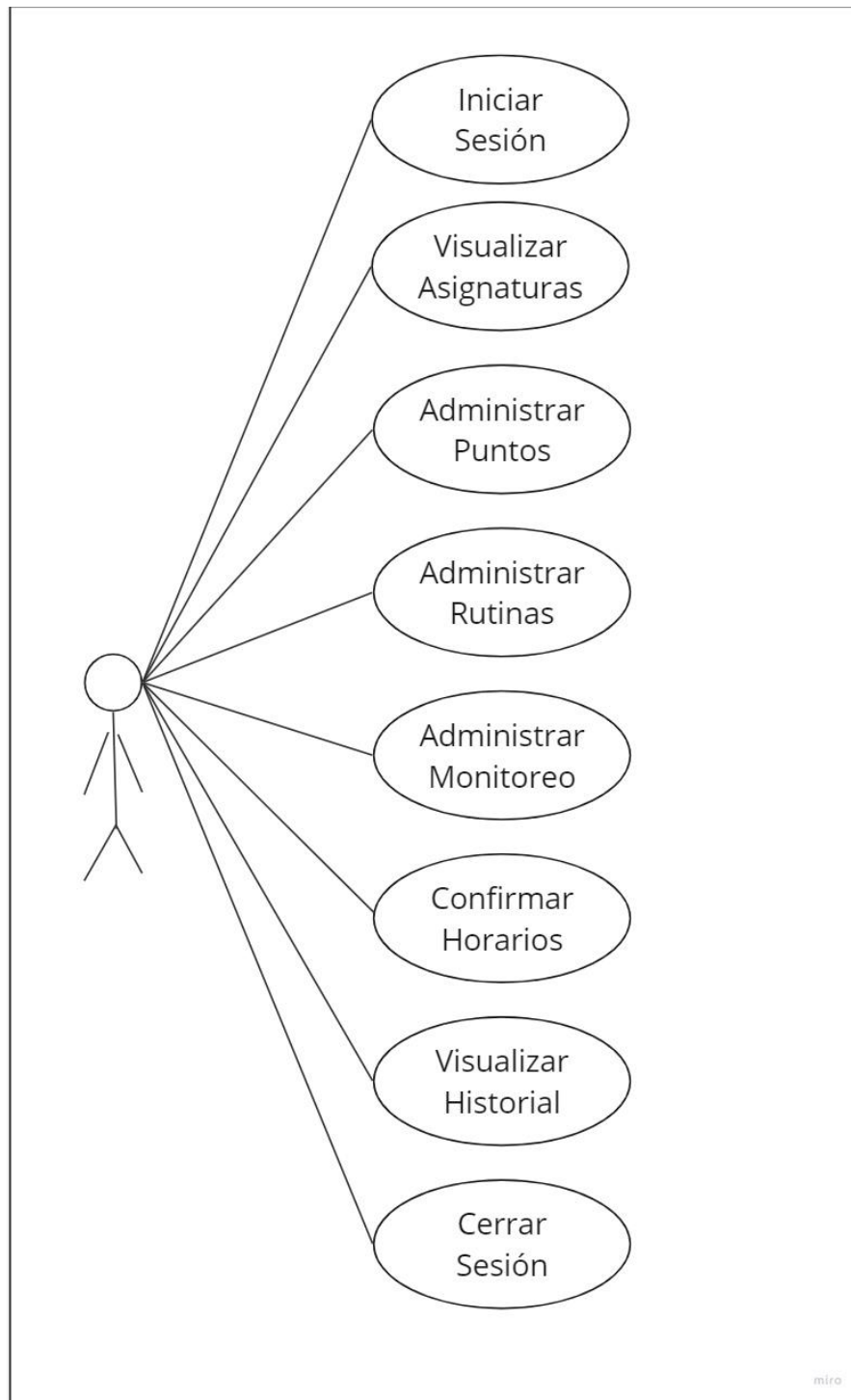


Figura 5.9 – Casos de uso para rol de profesor.



miro

Figura 5.10 – Casos de uso para rol de estudiante.

5.4 MOCKUP

Esta etapa considera el diseño preliminar y la representación visual o prototipado de la interfaz final para el usuario, considerando los objetivos de la aplicación. Para el diseño y desarrollo de este entregable, se recurre a la herramienta web de Miro, que permite trabajar de manera ágil distintos esquemas, plantillas, diagramas, entre otros diagramas.

El objetivo principal de este entregable es poder recibir retroalimentación en cuanto al diseño, navegación y estética de la aplicación a desarrollar. Esto permite identificar tempranamente ciertos errores en la navegación, acceso a vistas, funcionalidades, etc.

A continuación, se detallarán las distintas vistas, los objetivos principales de cada una y los distintos accesos a partir de la definición de los roles de usuario previamente establecidos. Las vistas se listan a continuación:

- Login
- Home
- Interfaz
- Historial
- Solicitud de horarios
- Configuración de cuenta
- Registro de usuarios



Figura 5.11 – Login

Esta vista permite validar y autenticar el acceso a los distintos usuarios, siempre y cuando dicho usuario esté registrado en la base de datos. No existen diferencias de ingreso entre los distintos roles de usuario. Es la pantalla por defecto al ingresar a la plataforma.



Figura 5.12 – Home

Esta vista permite escoger una de las estaciones para poder realizar las experiencias de control y movimiento del brazo robótico, así como también el monitoreo de video en tiempo real de la estación. Al seleccionar una estación, se verifica si está disponible y se establece una comunicación mediante sockets. Para lograr esto, en cada estación debe estar ejecutándose un

programa que escuche permanentemente los mensajes entrantes a la estación desde el servidor.

Considerar que, al momento de ingresar a cualquiera de las estaciones, se debe ejecutar el comando 'Home' en el brazo robótico. De esta forma, es posible comenzar la manipulación del robot en base a su origen, lo que permite un mayor control de sus ejes y acelera la comprensión de todo el espectro de movimientos que puede lograr.



Figura 5.13 – Interfaz de control y monitoreo

Esta es la vista principal de la plataforma, que tiene las funcionalidades integradas de control de movimiento, monitoreo, botonera en tiempo real y creación de rutinas. El usuario será capaz de poder mover el brazo robótico, ejecutar comando preparados en la memoria, almacenar puntos y vectores, además de poder visualizar en tiempo real el monitoreo del brazo mediante cámaras web. Por último, el usuario tendrá una funcionalidad para crear, almacenar y ejecutar rutinas con el Scorbob, que se define como una secuencia de movimientos y comandos para ciertas aplicaciones de manufactura y almacenamiento.



Figura 5.14 – Historial de usuario

El usuario con rol de estudiante tendrá acceso a esta vista para visualizar información valiosa de sus accesos a plataforma, experiencias realizadas, puntos almacenados, rutinas almacenadas, entre otros datos. El usuario con rol de profesor tendrá acceso a esta vista, pero con privilegios para ver todas las cuentas de usuario y sus correspondientes datos. De esta forma, se puede tener un control de acceso y un monitoreo de los datos y de la actividad de los usuarios, para toma de decisiones o administración de las experiencias.

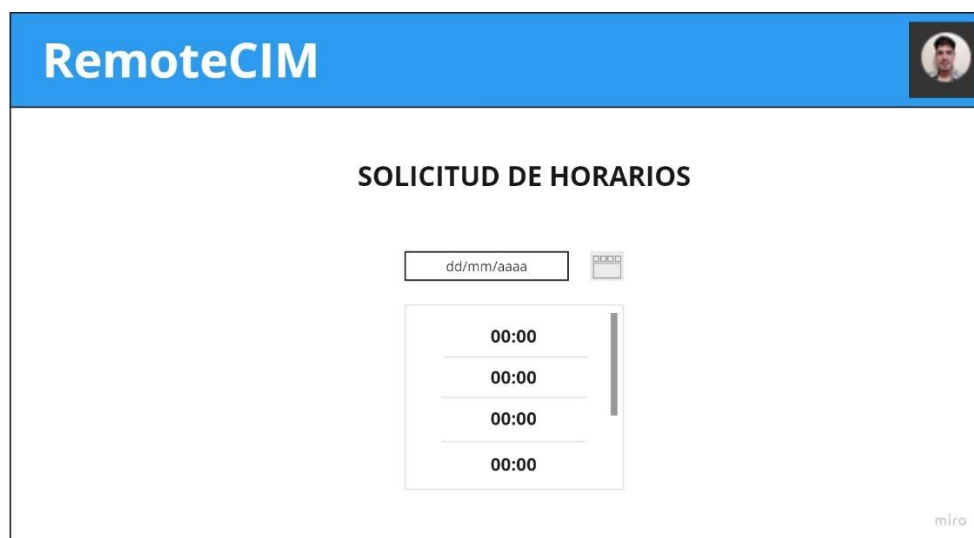


Figura 5.15 – Solicitud de horarios

En esta vista, el usuario con rol de estudiante podrá solicitar horarios para utilizar cierta estación. Una vez solicitado, se notificará al usuario con rol de profesor asignado a la experiencia de laboratorio. Luego, el usuario con rol de profesor deberá ser capaz de confirmar la solicitud del usuario estudiante y asignarle un bloque de tiempo para que interactúe con la plataforma y el brazo robótico.

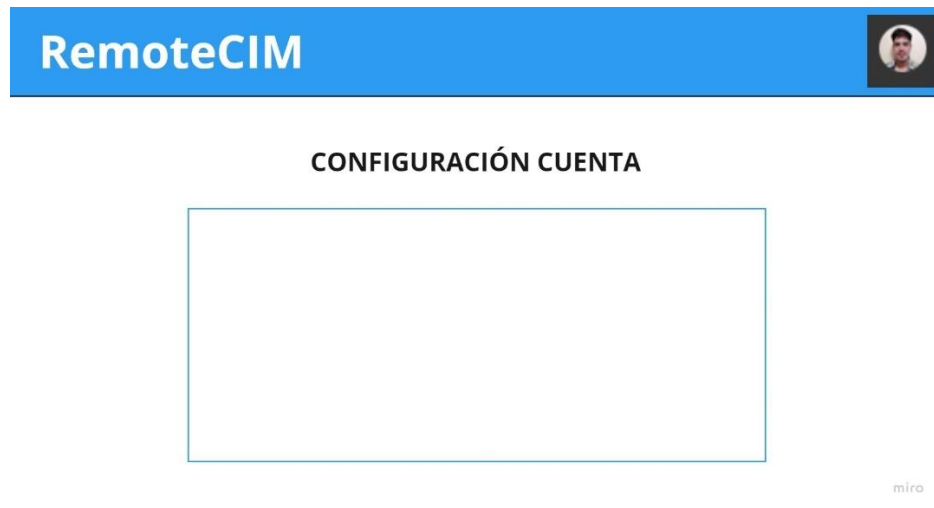


Figura 5.16 – Configuración de cuenta

En esa vista, cada usuario tendrá un panel con ciertos privilegios y posibles configuraciones que le permitirá ajustar información relevante para su cuenta de usuario.

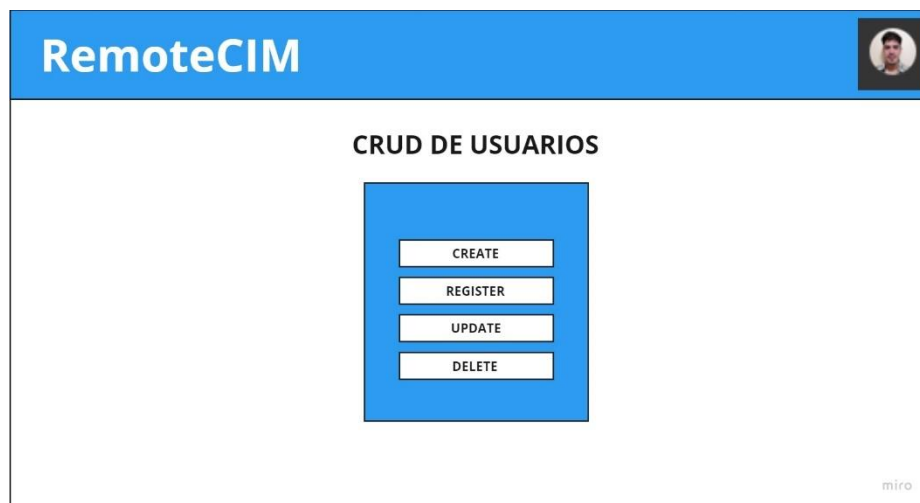


Figura 5.17 – Registro de usuarios

Esta vista es exclusiva para el rol de administrador, ya que podrá crear y registrar usuarios en la base de datos, ingresando información de identificación como nombre de usuario, correo institucional y contraseña. El usuario creado podrá cambiar su contraseña siempre que quiera. Se deben establecer expresiones regulares para la creación de contraseñas.



Figura 5.18 – Control de usuarios

Esta vista es exclusiva para el rol de administrador, ya que permite administrar y gestionar la información de todos los usuarios registrados en la plataforma. En esta vista se integran funcionalidades de edición, actualización y eliminación de cuentas de usuario.

6 DESARROLLO DE LA APLICACIÓN WEB PARA MONITOREO Y CONTROL REMOTO

En este capítulo se abarca principalmente el desarrollo de la aplicación mediante el framework Django, escrito en el lenguaje de alto nivel Python. Se especifican los módulos a implementar, basados en la etapa de diseño en el capítulo anterior.

Para desarrollar correctamente esta aplicación web, se utiliza un entorno de desarrollo de alto nivel llamado Django, escrito y establecido en el lenguaje de programación Python. Tiene muchas ventajas por sobre otros entornos y lenguajes. Por ejemplo, está basado en el patrón de diseño Modelo – Vista – Controlador, que permite separar los datos, la lógica de programación y la presentación de diferentes componentes.

Además, cuenta con un mapa relacional de objetos que permite a los desarrolladores interactuar con la base de datos utilizando código nativo de Python en vez de SQL, por ejemplo. Por otro lado, tiene una interfaz de administración integrada que permite a los desarrolladores gestionar fácilmente el contenido del sitio web. Otra de las características y ventajas bastante importante de este entorno es que tiene una serie de características de seguridad integradas, como protección contra ataques CSRF, XSS y SQL Injection.

Django prioriza la escalabilidad de las aplicaciones, es decir, permite crear aplicaciones web de cualquier tamaño, siempre y cuando se tenga la infraestructura necesaria. La comunidad de desarrolladores que tiene Django brinda soporte y recursos valiosos, por lo que es bastante versátil para construir una amplia variedad de aplicaciones web, desde simples blogs hasta complejas aplicaciones empresariales.

Por último, Django cuenta con una documentación muy completa y detallada que facilita su aprendizaje y utilización. Además, se puede extender fácilmente con bibliotecas y paquetes de terceros para agregar nuevas funcionalidades.

Entonces, como se puede incrustar código HTML, CSS y JavaScript en el framework de Django, se logran realizar sitios web de manera rápida y dinámica. El desarrollo de esta aplicación considera desarrollo del lado del cliente y del lado del servidor, por lo que se deben mapear las vistas para lograr una correcta navegación y que cumpla con todos los requisitos planteados en el capítulo anterior.

La sección de transmisión por video se desarrolla mediante JavaScript. Se crean los cuadros para poder representar la transmisión mediante HTML y CSS y se activan los medios de navegación para poder visualizar el video en un sitio web o navegador web. La disposición óptima del sistema de monitoreo debería ser la siguiente:

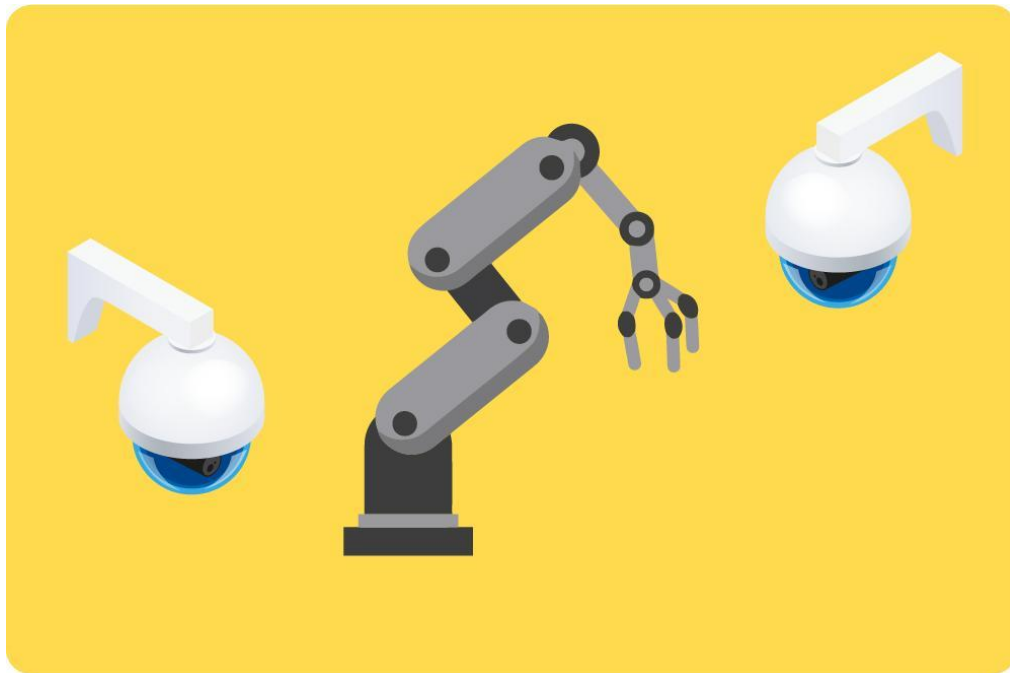


Figura 6.1 – Distribución óptima de los dispositivos en el laboratorio.

Luego de haber desarrollado la interfaz de control y monitoreo en Django, se desarrollan programas ejecutables en el lenguaje C#, dentro del entorno Visual Studio Community, que serán los ficheros que finalmente permitirán el movimiento y control del brazo robótico. Para esto se deben enviar mensajes desde el servidor hacia la estación mediante sockets y dependiendo del mensaje enviado, el sistema informático ejecutará cierto programa o comando en el brazo robot.

La interfaz de monitoreo y de control estará disponible para el usuario con rol de estudiante, profesor y administrador y será posible acceder a ella desde la aplicación web luego de validar correctamente los datos de usuario. El cliente o usuario tendrá visión del laboratorio en todo momento.

Las cámaras serán localizadas como objetos gracias al lenguaje dinámico JavaScript. Esto permitirá posicionarlas y ubicarlas dentro de un contenedor en el sitio web, para así poder desplegar la transmisión de video en tiempo real, complementando a la interfaz de control.

Una vez lograda la transmisión en directo del brazo robótico, se puede tener un control mucho más seguro de los movimientos de este dispositivo, ya que se puede ver lo que hace en tiempo real. Esto permite, además de complementar el aprendizaje para los estudiantes, asegurarse de que el robot no realice movimientos peligrosos para su integridad.

6.1 Interfaz de control y creación de rutinas

A continuación, se presenta la interfaz gráfica desarrollada en Django y que será desplegada para el usuario estudiante, profesor o administrador al momento de realizar una experiencia de laboratorio remota, que permitirá mover el brazo robótico en los distintos ejes, realizar movimientos circulares o lineales, abrir la pinza, entre otras funciones.

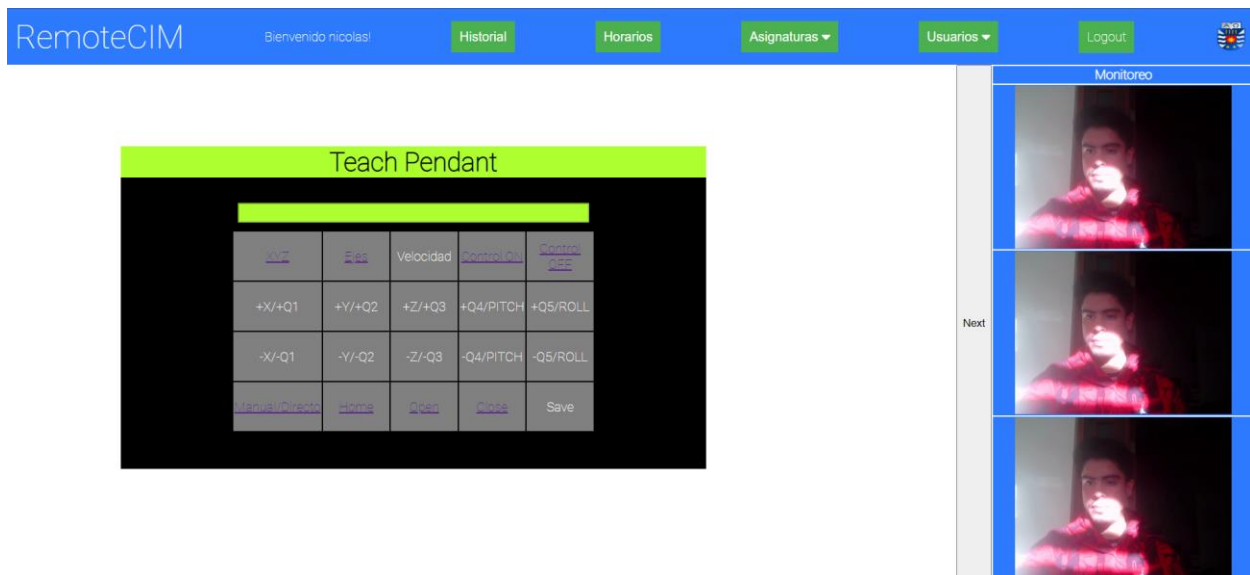


Figura 6.2 – Vista principal de la interfaz.

Se toma como referencia el control que se hace de forma serial mediante el teach pendant en el laboratorio CIM. El objetivo principal es replicar prácticamente casi todas las funcionalidades del actuador, que permite interactuar con el robot en tiempo real. Entonces, al tener el monitoreo del robot en tiempo real y, además, poder mover el robot a disposición del alumno, considerando las limitaciones físicas de la estación, es posible complementar un aprendizaje sólido para el alumno al interactuar con plataformas de desarrollo universitario que permitan integrar sistemas más inteligentes y de forma remota o digitalizada, priorizando la comodidad y la disponibilidad de ciertos recursos universitarios que podrían ser a futuro un recurso oficial para la universidad, siempre y cuando se cuente con la infraestructura y el personal capacitado para esto.

Gracias a esta interfaz, es posible darle instrucciones de movimiento al robot para que se mueva en distintos ejes considerando el respectivo sentido de giro de cada motor. Además, se puede abrir la pinza, cerrarla, apagar o encender los motores para movimientos manuales, llevarlo a la posición de referencia, mover los ejes, mover en XYZ, cambiar la velocidad, entre otras funcionalidades.

Además, se tiene una entrada de texto que simula ser la pantalla LCD que tiene el actuador del Scorbot en el laboratorio, ya que al darle una instrucción al brazo robot, este desplegará un mensaje para conocer el estado de la ejecución de aquella instrucción, por lo que se podrá tener un

monitoreo incluso del dispositivo embebido que está en el laboratorio, a pesar de que sea una simple simulación.

Dentro de esta misma interfaz, se tiene un botón llamado ‘Save’ que permite registrar un punto en la base de datos del usuario y en la memoria del robot. Para esto, el robot se debe mover, posicionar en un punto específico que se quiera almacenar y luego pulsar el botón para almacenar esa posición y registrarla en la base de datos en la tabla del usuario.

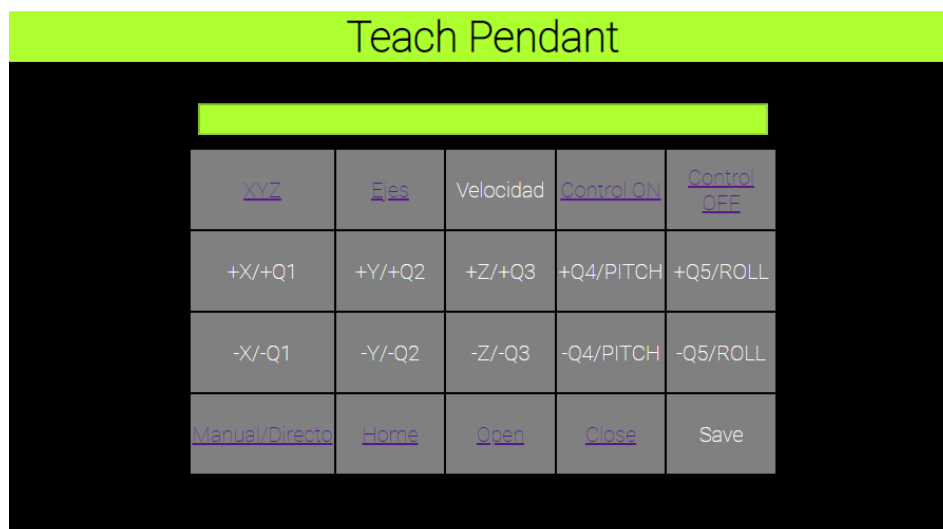


Figura 6.3 – Réplica de interfaz teach pendant.

Al registrar un punto, se le puede asignar un nombre representativo a dicho registro limitado o condicionado a normas establecidas mediante código, conocidas como expresiones regulares. Por último, se tiene la funcionalidad de eliminar uno de los puntos almacenados, a disposición de lo que decida el rol de profesor y administrador, dependiendo del uso que se le dé a la plataforma y del desempeño del brazo robótico al realizar dicho movimiento.

Finalmente, se tiene un último contenedor que permite interactuar con el usuario para crear rutinas a partir de los puntos que se vayan almacenando y acciones predeterminadas del robot como abrir la pinza, cerrar, cambiar velocidad, volver a puntos de referencia, etc.

Además, como se puede apreciar, tiene botones con funcionalidades como cargar una rutina, que está asociada a la cuenta de usuario y sólo a esa cuenta, además de que se puede guardar una nueva rutina y crear una nueva, que solicitará un nombre para luego almacenarse. Esto implica que se debe contar con una base de datos dedicada exclusivamente a almacenar los puntos que se vayan guardando para luego solicitarlos a esta misma base de datos en la etapa de creación de rutinas.

También se pueden agregar comandos a las filas que ya existen, con un límite establecido mediante código de 30 comandos posibles. También se pueden sacar comandos de la rutina si se desea modificar la ejecución o probar con nuevos ensayos. El botón de Ejecutar envía esta rutina como datos que se puedan interpretar por un algoritmo y una lógica desarrollados que permitan escribir en C# todas las instrucciones que se declararon y se asignaron a dicha rutina. Entonces, envía una solicitud al servidor para que cree un archivo de texto, lo almacene y lo extrapole al lenguaje de comunicación que logra la comunicación serial (en este caso C#, pero podría ser cualquier otro). De esta forma, se puede controlar el brazo robótico mediante rutinas de programación, acercando la aplicación del robot a una simulación de un entorno industrial si el alumno quiere programarlo de esa manera.

Todo el desarrollo de esta plataforma fue realizado en el entorno Django, teniendo a Python como lenguaje base para la estructura del sitio web, complementado estructuras y elementos en HTML y con funciones y estilos de CSS para mejorar la experiencia del usuario del lado del cliente y hacerlo lo más amigable posible, sin que deje de ser una plataforma de carácter universitario.

La comunicación con la base de datos se realiza también mediante las funciones y herramientas que Django posee, por lo que es bastante sencillo vincular los datos, crear tablas y actualizar variables.

La comunicación entre servidor y estaciones se realiza mediante la tecnología de sockets. Se crea un socket en el servidor y un socket en cada una de las estaciones. Luego, se establece la comunicación mediante estos puertos y se envían y reciben mensajes. El servidor es quien envía

mensajes desde la plataforma e interfaz de control y la estación recibe. Dependiendo del mensaje que reciba la estación, ejecutará ciertos comandos por consola en su sistema operativo, pudiendo ejecutar distintas acciones en base a lo que el servidor requiera. Considerar que se deben integrar capas de seguridad sólidas, ya que lo que logra realizar el servidor sobre la estación podría ser perjudicial si es que es vulnerado.

Para el desarrollo a nivel de codificación de este proyecto, se priorizó la escritura de código limpio y mantenible, bien organizado con el objetivo principal de comprender de manera sencilla la estructura y las relaciones entre clases y funcionalidades de la aplicación. Además, se consideraron nombres de las vistas, variables y de funciones representativos a cada etapa del proyecto, para evitar confusiones o mal entendimiento del código. Otra de las buenas prácticas al momento de codificar son los comentarios explicativos de cada funcionalidad o navegación y la integración de estándares de código establecidos. Bajo la misma premisa, se consideró el desarrollo del código de forma modular, para optimizar el desempeño y las relaciones y funcionalidades de cada vista, lo que lo hace sencillamente mantenible, fácil de leer y modificar.

Dentro del proceso de desarrollo de la aplicación web, se consideraron etapas de pruebas de software, principalmente enfocado a pruebas de optimización de código, herramientas que se pueden automatizar sencillamente en Python. Además, se realizaron pruebas exhaustivas para esta aplicación, consistentes en pruebas de carga, de velocidad de respuesta y de ciber resiliencia. Se considera que está desarrollado de manera robusta para al menos desplegarla en una asignatura, además de que está creado en un entorno de Python bastante sólido.

Las pruebas del software aseguran que la aplicación es estable y funcional, libre de bugs y errores, lo que optimiza el funcionamiento y desempeño del sitio web, priorizando la experiencia del usuario, un concepto bastante importante y considerable en el mundo del desarrollo de software y de aplicaciones web. Cabe destacar que esta aplicación pudo haber sido desarrollada como aplicación de escritorio, pero considerando la funcionalidad remota de este software se realizó como aplicación web.

Además, dentro de la etapa de desarrollo del software, se consideraron capas de seguridad

adicionales a las que cuenta Django. Esto se traduce a un sistema web mucho más robusto y seguro con respecto a la información sensible de cada uno de los usuarios. Se implementaron técnicas sólidas de encriptación, autenticación, autorización y validación para proteger los datos de los usuarios y prevenir accesos no autorizados.

Adjunto en el repositorio del proyecto, se tiene un manual de usuario documentado específicamente para lograr que la aplicación pueda ser comprendida y utilizada por cualquier miembro perteneciente a la universidad. Dentro del proyecto también se establece una correcta y valiosa documentación del código y de los procesos necesarios para montar la aplicación y comprender su funcionalidad, configurar la red y establecer la comunicación.

Por último, considerar la mejora continua típica de este tipo de aplicaciones, incorporando retroalimentación de los usuarios e indicadores claves de desempeño. Se pueden implementar herramientas de análisis para monitorear el uso e identificar áreas en las que se puedan incorporar mejoras de software.

6.2 Manipulación y movimiento de Scrobot-ER Vplus

Como se especifica anteriormente, cada botón tendrá asignado un comando que entenderá el Scrobot y lo ejecutará. Cada botón tiene asignada una función que envía un comando mediante sockets hacia la estación, que está conectada al robot. Este mensaje, permite ejecutar comandos por consola, lo que logra ejecutar acciones en el brazo robótico. Considerar que un mensaje ejecuta una sola acción, pero con mayor desarrollo, un solo comando podría ejecutar distintos comandos uno tras otro en la estación de trabajo. Es por esto que se hace tanto énfasis en la ciber seguridad de esta aplicación, ya que un mensaje podría destruir o encriptar archivos fácilmente o ejecutar software malicioso o acciones peligrosas en la estación de trabajo.

Se debe considerar que en este punto las cámaras deberían estar activadas, es decir, debe ser posible visualizar las funcionalidades y el movimiento del robot en tiempo real. La recomendación es que las transmisiones deberían comenzar al inicio de experiencia de control, aunque se podría seleccionar manualmente si se quisiese.

6.3 Métodos de operación del Scrobot

A continuación, se mencionan las órdenes básicas utilizadas en el desarrollo de la interfaz web para operar el robot SCORBOT-ER Vplus. La operación del sistema robótico tiene 2 formas de funcionar:

- **DIRECT**: Modo directo. El usuario tiene control explícito de los ejes, y el controlador ejecuta inmediatamente las órdenes que el usuario envía.
- **EDIT**: las órdenes son insertadas en un programa de usuario, que puede después ser guardado y ejecutado.

6.4 Modo Manual

El modo Manual está disponible exclusivamente cuando el sistema funciona en modo directo. Este modo permite el control directo de los ejes del robot cuando la botonera de enseñanza no está conectada.

Para activar el modo manual se envía el comando “M”, que también será utilizado para salir de este modo.

6.5 Coordenadas Cartesianas (XYZ)

El sistema de las coordenadas cartesianas, o XYZ, es un sistema geométrico utilizado para especificar la posición del PCH o punto central de la herramienta (generalmente es una pinza) del robot por medio de la definición de la distancia, en unidades lineales, de su punto de origen (el centro de la base) a lo largo de los tres ejes lineales. Para completar la definición de la posición, se especifica la inclinación y el giro en unidades de ángulos.

Cuando se ejecuta un movimiento del robot en modo XYZ, unos o todos los ejes se mueven para mover el PCH a lo largo de uno de los ejes X, Y o Z. Para activar el sistema XYZ se debe enviar el comando “X” por el puerto serial al que está conectado el robot.

Los comandos a continuación realizan los siguientes movimientos en el modo XYZ:

- Q PCH se mueve en el eje +X y -X
- W PCH se mueve en el eje +Y y -Y
- E PCH se mueve en el eje +Z y -Z
- R Cambia la inclinación; el PCH es estable

6.6 Coordenadas de Ejes

Las coordenadas de ejes o Joints, especifican la locación de cada eje según la cuenta de su codificador. Cuando el eje se mueve, el codificador óptico genera una serie de señales eléctricas altas y bajas alternadas. El número de señales es proporcional a la cantidad de movimiento del eje; el controlador las cuenta y determina qué distancia recorrió dicho eje. Similarmente, un movimiento o una posición del robot pueden ser definidos como un específico número de cuentas del codificador para cada eje, con relación a la posición de Inicio, o a otra coordenada.

Para activar el sistema de coordenadas de ejes se debe enviar el comando “J” por el puerto serie asociado al brazo robótico.

Los comandos a continuación producen los siguientes movimientos en el modo ejes:

- Q Mueve el eje 1 (base)
- W Mueve el eje 2 (hombro)
- E Mueve el eje 3 (codo)
- R Mueve el eje 4 (inclinación)
- T Mueve el eje 5 (giro)
- Y Abre/cierra la pinza (eje 6)

6.7 Comandos utilizados en modo directo.

A continuación, se mencionan ciertos comandos que podrían servir para poder desarrollar una rutina de operación desde la interfaz web.

6.8 Definición y grabado de posiciones

- **defp pos:** Define una posición llamada pos en el grupo A. Este comando sirve para definir una posición, reservando un espacio en la memoria del controlador. El nombre puede ser numérico o alfanumérico de hasta 5 caracteres.
- **delp pos:** Borra la posición existente llamada pos. Sirve para borrar una posición ya definida. Libera ese espacio reservado en memoria.
- **undef pos:** Borra el contenido de la posición existente llamada pos. Elimina los valores de las coordenadas grabadas pero la posición sigue definida.
- **here pos:** Almacena en la posición pos definida anteriormente las coordenadas joint.

6.9 Movimiento a posiciones grabadas

- **move pos:** El robot se mueve a la posición grabada en pos.
- **movel pos:** La pinza se mueve desde la posición actual hasta la posición pos en línea recta, siempre y cuando este movimiento sea posible.

6.10 Comandos de control de ejes

- **open:** Abre la pinza.
- **close:** Cierra la pinza.
- **con:** Habilita el servo control de todos los ejes, o de algún grupo en particular.
- **coff:** Deshabilita el servo control de todos los ejes, o de algún grupo en particular.
- **speed var:** Establece la velocidad de los ejes del grupo A para las instrucciones MOVE y MOVES. La variable var será un porcentaje del valor de velocidad máxima.
- **A:** Aborta la ejecución de programas.

7 RED LOCAL LABORATORIO CIM

En este capítulo se detalla el procedimiento práctico para configurar la red local del laboratorio CIM paso a paso. Esta sección se encarga de establecer las conexiones y las medidas consideradas para lograr una red local segura y con mínimas brechas de seguridad, ya que se trata de una plataforma utilizada por académicos y alumnos de la universidad, que podría comprometer información sensible de los usuarios si es que llega a ser vulnerada.

Este procedimiento debe ser riguroso y confiable, ya que, si no se configura de la forma adecuada, podría traducirse a fallos en la seguridad de la red, comprometiendo todos los dispositivos que estén conectados a ella, o que registren información del uso de la aplicación. Favorablemente, es posible crear una red robusta con seguir unos simples pasos. Esta sección pretende documentar el procedimiento para crear la red local y luego configurarla considerando los aspectos de ciber seguridad que deberían ser implementados. Realizar una configuración manual desde cero se traduce a un beneficio en cuanto a seguridad, conociendo las principales vulnerabilidades y las principales amenazas y métodos de defensa informática.

Se debe implementar el direccionamiento y el enrutamiento IP adecuado, debido a las complejidades que se pueden presentar por algunas de las problemáticas que se explicitarán en el capítulo de Ciberseguridad. Además, se debe tener un control óptimo de la red con respecto a intrusos, generación y creación de cuentas para los usuarios que tengan acceso, además de poder configurar el uso compartido de archivos, carpetas, ficheros, etc. Todo esto engloba un sistema completo para el control y el manejo de la red, controlando eficientemente tanto el acceso externo de dispositivos, como la exposición de los datos sensibles que viajan por la red local.

Se implementan distintas técnicas de ciber seguridad para robustecer la red local que se crea en el laboratorio, con respecto al servidor de la estación y a la configuración del switch en la red. En primera instancia, se define una lista blanca exclusivamente para esa red que limita los dispositivos que se quieren conectar a la red. De esta forma, se pueden amortiguar algunas amenazas de carácter cibernético. Además, se realiza un filtrado de MAC que complementa la técnica antes desarrollada.

Principalmente, se deben fijar las direcciones IP de cada estación y del servidor. Esto implica que siempre se podrá acceder a la estación desde la plataforma, ya que se establecen los sockets con direcciones IP fijas. En caso de que las direcciones IP se obtengan dinámicamente el protocolo DHCP, se debería integrar una nueva funcionalidad a la aplicación para poder obtener dicha dirección de manera automática.

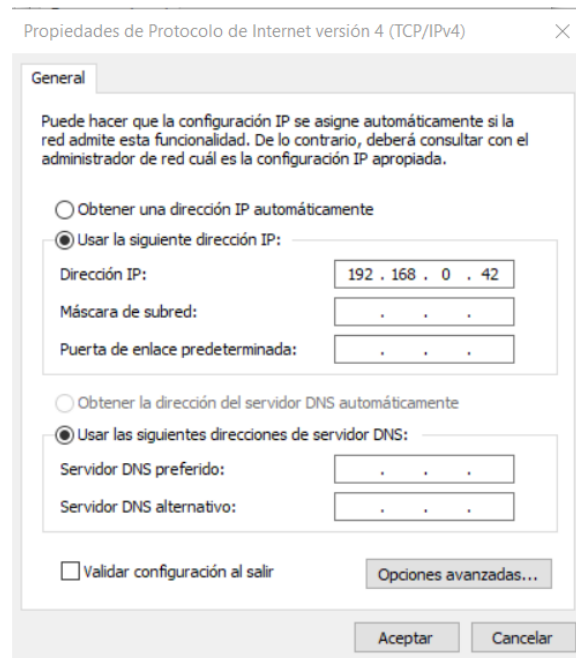


Figura 7.1 – Configuración para fijar direcciones IP en estaciones y servidor.

La Figura 7.1 muestra la ventana para fijar las direcciones IP en una máquina. Esto permite que siempre se tenga la misma identificación para dicha estación, lo que acelera el proceso de comunicación y conexión de esta aplicación. Se establecen IP fijas para servidor y estaciones, ya que son parte importante del desarrollo óptimo de la plataforma. Esta configuración de red permite interactuar entre máquinas de forma sencilla.

Finalmente, una vez instalada la red y los equipos configurados, se pueden establecer estrategias de seguridad mediante un host local que permita analizar el tráfico, crear filtros para usuarios conectados, filtrar por IP o por MAC a distintos dispositivos, crear un Honeypot para evitar o prevenir ataques, abrir o cerrar puertos dependiendo de la aplicación, entre otras varias técnicas y estrategias de hacking ético para resguardar la red local a nivel físico.

Se propone una mantención semanal del sistema, para verificar el comportamiento, analizar si existen intrusos, o si se tiene una vulneración en la plataforma. Además, se deben realizar periódicamente actualizaciones al sistema operativo y a la plataforma web.

8 CIBERSEGURIDAD

En este capítulo se detalla el procedimiento teórico y práctico para poder implementar distintos aspectos de ciberseguridad a la plataforma, agregando múltiples capas de seguridad informática que serán parte de la aplicación web, para consolidar la integridad de los datos. El objetivo de este capítulo se basa en concientizar sobre las distintas vulnerabilidades a las que podría estar expuesta esta aplicación y, de esta forma, poder prevenirlas tomando las medidas a nivel de programación en el código de la aplicación web, como también explicitando estrategias de defensa para que no se vea vulnerada la plataforma por errores humanos. De esta forma se integran múltiples capas de defensa, para que la información de este sitio web este resguardada y segura dado que tendrá información sensible de los estudiantes y profesores.

Entonces, para este capítulo se especifican distintos vectores de ataque (métodos y técnicas de vulneración, principales amenazas, procedimientos, herramientas, etc.) que podrían perjudicar la seguridad del sitio web con el fin de tener en consideración causas importantes de vulneraciones y así poder especificar la forma de llevar a cabo múltiples estrategias defensivas para poder amortiguar las amenazas, una vez conociendo las metodologías de ataque.

El procedimiento defensivo corresponde a configuraciones del servidor, actualizaciones de sistema operativo, restricciones a ciertos ficheros, encriptación de información sensible, etc. Además, se implementan técnicas defensivas integradas en el framework Django, a nivel de código en Python y a nivel físico dentro de la red de laboratorio. Considerar el término de ciber resiliencia, es decir, prepararse para lo peor y esperar lo mejor, en caso de ser atacados o vulnerados [11].

Considerando lo sensible que es la información que pudiese ser expuesta o vulnerada en esta aplicación, se requiere extremo cuidado al momento de trabajar con una plataforma de carácter universitario, ya que se debe velar por la autenticación, validación y seguridad de los datos de los usuarios registrados, ya que no se desea para nada la vulneración de información tan sensible, menos si se trata de contenido académico y valioso para la universidad. Lamentablemente, los métodos defensivos no acreditan una seguridad al 100%, pero si limitan y acotan los vectores de ataque en el campo de la informática y de la seguridad de la información.

Con el concepto de ciber seguridad se hace mención incluso a aspectos físicos de la red local del laboratorio y a dispositivos que son parte del sistema informático en cuestión, como computadores, celulares, circuitos embebidos, cámaras, incluso el brazo robótico. Considerando esto, se plantean varias estrategias para la defensa del sistema informático de laboratorio, con el fin de amortiguar cualquier tipo de amenaza que pueda existir en el sitio web y red local.

Cabe destacar que las brechas de seguridad se deben a errores netamente humanos, es por esto, que se debe siempre concientizar y preparar al personal operador de los sistemas informáticos o aplicaciones web para que no sean víctima de algún tipo de amenaza o directamente de ciber delincuentes. Para hacer incluso más énfasis en este tópico, es posible afirmar que hay registro de muchos ataques que han sido realizado básicamente mediante dispositivos USB o similares, que, al ser utilizado por la víctima, comparte información privada sin notarlo o se instalan y descargan archivos maliciosos en su equipo sin notarlo, corrompiendo la seguridad y privacidad de su información. Los ciber delincuentes son conscientes de que la principal vulnerabilidad son los usuarios, por lo que siempre están desarrollando nuevas estrategias para poder obtener información importante y delicada de cada persona conectada a la web, sobre todo dentro una red local.

8.1 Vectores de ataque

Para esta sección, se consideran ciertos tipos de ataques que podrían amenazar la seguridad y la confidencialidad de la información disponible en la plataforma web de monitoreo y de control, con la finalidad de establecer técnicas defensivas que aseguren la calidad y la integridad de los datos compartidos por los usuarios. Por ejemplo, si se vulnera la sección de monitoreo, será posible tener acceso al laboratorio en tiempo real, ya que se implementa un sistema de visión por cámaras, lo que se considera bastante peligroso si esto lo domina una persona con fines maliciosos o si algún ciber delincuente logra tener el control de la plataforma, ya que podrá ver lo que ocurre en tiempo real en el laboratorio físico de la universidad.

Este tipo de ataques y vulneraciones son posibles de efectuar con conocimientos básicos y también avanzados de informática, así como también existen personas dedicadas a encontrar vulnerabilidades en algunos sistemas informáticos y explotarlos, o directamente secuestrar

información para exigir un monto de dinero a cambio de los datos vulnerados.

Entonces, en este capítulo se plantean estrategias ofensivas y defensivas de ciber seguridad y hacking ético, con ejemplos prácticos y teóricos para complementar la información representada, con el objetivo de lograr una seguridad sólida en el código de la aplicación y en la red local del laboratorio, además de concientizar y en cierta forma capacitar a los usuarios de la interfaz, sean estos estudiantes o profesores.

Los ataques más comunes y conocidos, pero no por eso menos efectivos, son los ataques de ingeniería social. Este tipo de amenazas se enfocan en lograr manipular a las víctimas para obtener información valiosa como cuentas, contraseñas, direcciones, números de teléfono, familiares asociados, etc. Los ciber delincuentes engañan a sus víctimas haciéndose pasar por otra persona u organización, como, por ejemplo, algún ejecutivo de un banco o similares que entreguen confianza al usuario y así poder sacarle información sensible de manera más rápida. La Universidad del Bío Bío es víctima de este tipo de ataques recurrentemente, en los cuales un usuario con malas intenciones automatiza correos electrónicos hacia el personal universitario con el fin de hacerlos caer en algún enlace malicioso o infectar los sistemas con algún tipo de malware. Este tipo de ataques por correo electrónico es conocido como Phishing.

Existen miles de vectores de ataque relacionados a ingeniería social, como llamadas telefónicas, correos, visitas personales, redes sociales, entre otros. Los atacantes se han vuelto tan fuertes en este campo que logran entrar de lleno en la vida de la víctima al obtener toda su confianza. Entonces, para implementar un sistema seguro a nivel informático, se deben tener nociones de ciertos ataques como estos para así poder establecer distintas capas de seguridad, no necesariamente a nivel de codificación, sino que también a nivel personal y operativo.

Desde correos electrónicos hasta llamadas telefónicas con técnicas avanzadas como DeepFake Voice, que permite a los atacantes camuflar su voz con una que sea mucho más familiar a la de la víctima, por ejemplo. Los ciber delincuentes han perfeccionado miles de técnicas de ingeniería social para vulnerar de la manera más sencilla a sus víctimas y explotar sus equipos, servicios, cuentas o directamente robarles información valiosa para un fin mayor, que dependerá

directamente de las intenciones del ciber atacante. Algunas técnicas llegan a ser tan básicas y sencillas que cualquier persona podría implementarlas, sin necesariamente tener conocimientos de redes.

Para este tipo de situaciones, no se pueden integrar capas tan seguras ni métodos infalibles con respecto a la seguridad ya que depende netamente del personal humano que esté a cargo u operando la aplicación web. Si se trata de una persona que no está preparada o no tiene consciencia sobre este tipo de amenazas podría ser fácilmente vulnerada y perder datos valiosos o perjudicar a otras personas que estén dentro de su misma red.

De esta forma, se hace hincapié en ser lo más desconfiado posible al recibir llamadas, responder correos, visitar enlaces de dudosa proveniencia, etc. Considerar que acceder a un enlace malicioso podría descargar malware automáticamente en la computadora o dispositivo desde el que se intenta acceder, u ofrecer información valiosa para el atacante solamente con ejecutar una descarga o abrir un archivo de este tipo, lo que justamente se desea evitar en este tipo de aplicaciones, ya que son de carácter universitario y académico, entonces una sola vulneración podría afectar a miles de usuarios a la vez.

Cabe destacar que este tipo de ataques son muy difíciles de identificar, por lo que se vuelve a hacer hincapié en tratar de siempre estar alerta ante distintos tipos de señales que podrían demostrar un engaño, como, por ejemplo, la ortografía de los correos o mensajes, la proveniencia de los enlaces, el dominio del sitio al que se está accediendo, etc. Tal vez una de las estrategias defensivas o, en estricto rigor, de prevención de amenazas podría ser establecer cuentas de usuario o servidores o incluso computadores con cuentas exclusivas para este servicio web, con el fin de poder amortiguar ciertas amenazas, ya que se pueden evitar correos de terceros maliciosos o llamados telefónicos con actividades delictuales.

Dentro de este tipo de ataques está el Phishing, que consiste en vulneraciones por correo electrónico, el Vishing, que corresponde a ataques mediante llamadas telefónicas, el Spoofing, que también consiste en usurpar una identidad electrónica para ocultar la identidad del atacante, entre muchos otros variados ataques y formas de vulneración que, incluso se consideran técnicas tan

sencillas como mirar por encima del hombro de la víctima pueden resultar en un poderoso ataque de ingeniería social.

Entonces, como se puede apreciar en los párrafos previos, no basta con proteger 100% la plataforma, ya que siempre existen brechas en cuanto a la seguridad que son explotadas por ciber delincuentes al saber que existen canales de ingreso que tienen que ver netamente con el personal humano que interactúa con el servicio de control del brazo robótico, algo que es bastante delicado por lo demás. En base a esto se desarrolla este capítulo, con el fin de amortiguar amenazas y establecer capas defensivas para el sistema de laboratorio virtual o remoto.

Ahora, con respecto a los ataques basado en redes y como punto de partida para comprender la información que se detalla a continuación, se debe esclarecer que las tablas de enrutamiento son uno de los componentes esenciales para que un router pueda cumplir su función, la que consiste en dirigir a los paquetes de datos al destino a través de la ruta más adecuada, ya que se detallarán ataques que involucran las tablas de enrutamiento como principal vulnerabilidad y que pueden perjudicar ampliamente la aplicación a nivel de red.

Las tablas de enrutamiento son un conjunto de reglas que sirven para determinar qué camino deben seguir los paquetes de datos que se van intercambiando regularmente dentro de la red local. Todo esto ocurre a través de una red que trabaje con el protocolo IP generalmente, ya que es un estándar de facto de casi todos los dispositivos más modernos.

Ahora, el peligro está en manipular estas tablas de enrutamiento con fines maliciosos, ya que es posible realizar ataques o enviar paquetes de información con cabeceras personalizadas y preconfiguradas para enviar solicitudes maliciosas a una víctima en particular.

Los paquetes de datos IP están compuestos por una cabecera o header que contiene la información necesaria para trasladar el paquete desde el emisor hasta el receptor, considerando los campos que pueda necesitar el protocolo de red. Además, los paquetes de datos tienen una carga útil o payload, que corresponde a los datos que se desean trasladar y un trailer o cola, que contiene código de detección de errores.

Hay ataques, como el IP Spoofing, que vulneran las tablas de enrutamiento del router local, permitiendo controlar el tráfico de datos dentro de la red a disposición de cualquier persona que vulnere dichas tablas, por lo que se debe tener especial cuidado con el control de esta información a nivel de red. Entonces, para este tipo de ataques, se propone una segura instalación y configuración de los componentes y equipos de red dispuestos en el laboratorio, para no ser vulnerado tan fácil de esta manera. Esto quiere decir que se deben configurar sólidamente parámetros del punto de acceso como nombre de usuario y contraseña lo más personalizada posible para evitar estas vulneraciones, además de integrar distintas estrategias de defensa como filtrado de MAC, listas blancas para ciertos dispositivos, encriptación en la información valiosa del router, etc.

El MAC Spoofing, por ejemplo, es una técnica para enmascarar la dirección física o dirección MAC de un dispositivo dentro del laboratorio, por ejemplo, que está codificada en la tarjeta de red de cualquier dispositivo con conexión a internet dentro del establecimiento físico del laboratorio.

Cabe destacar que esta dirección física o MAC, se caracteriza por ser inequívoca o estar grabada en el dispositivo y ser una combinación de números hexadecimales única en el mundo, es decir, no existen dos dispositivos con la misma dirección MAC en el mundo.

Sin embargo, existen variadas herramientas que pueden hacer al sistema operativo creer que un controlador de interfaces de red tiene la dirección MAC del dispositivo de otro usuario. Este proceso se conoce como suplantación de dirección MAC. En estricto rigor, esta técnica implica el cambio de identidad de una computadora o dispositivo dentro de la misma red, para camuflar a un dispositivo dentro de la red con la dirección de cualquier otro de los dispositivos que estén en la misma red.

Estas técnicas, en particular, se llevan a cabo con fines legítimos e ilegales por igual. Ahora, se propone realizar una correcta configuración en el switch y router de la red local con el fin de que no se pueda acceder tan fácilmente a esta información tan delicada.

Para solucionar esto, o por lo menos hacer que este proceso sea más complejo, es posible realizar un filtrado de MAC, que permite restringir el acceso a la red a un dispositivo en concreto o a un grupo de equipos, así como también se puede crear una lista blanca que sí permita el acceso a la red, pero solo a ciertos dispositivos determinados y especificados con la dirección MAC. Los routers tienen integrada esta función, siendo posible crear tanto listas blancas como negras, lo que determina cuales dispositivos pueden conectarse a la red y cuáles no. Se propone realizar un correcto proceso de filtro y de restricción de dispositivos.

Para este proyecto se propone realizar un filtrado de MAC y una lista blanca, para así poder regular quienes se pueden conectar a la red local del laboratorio y quienes no, para poder tener un control mucho más sólido con respecto a quien ingresa a la red. En el caso que exista un comportamiento extraño o sospechoso con respecto a esta medida, se deberá tomar acción inmediatamente considerando que las direcciones físicas o MAC son exclusivas de cada dispositivo.

Se propone esta solución a realizar en la red local del laboratorio con el fin de evitar que algún ciber delincuente pueda ingresar y robar o interceptar los paquetes de datos que se transmiten en la red local, ya que sería bastante peligroso que cualquier persona tenga acceso a modificar las tablas de enrutamiento y direccionamiento del router, por lo explicado previamente. Si una persona intercambia las direcciones MAC o de identificación de los dispositivos, podría obtener información en su computador o celular que corresponde a paquetes de datos que corresponden a otro dispositivo dentro de la misma red, como, por ejemplo, mensajería, correos electrónicos, imágenes, vídeos, etc.

A partir de esto pueden nacer otros tipos de vulneraciones, como el famoso ataque Man in the Middle, o, en español, Hombre en el Medio. Este es un ataque destinado a interceptar, sin autorización, la comunicación entre dos dispositivos conectados a una red. Este ataque le permite a un agente malintencionado manipular el tráfico interceptado de diferentes formas, generalmente para escuchar la comunicación y obtener información sensible, como credenciales de acceso, información financiera, cuentas de usuario, etc.

Si se vulnera con algún ataque similar a estos, estaríamos en presencia de una vulneración bastante peligrosa para cualquier usuario, ya que se tendría información valiosa, sensible o delicada a disposición del atacante. De ahí en adelante, la integridad de estos datos queda en las manos del ciber delincuente, por lo que podría realizar cualquier tipo de acción maliciosa con estos datos, como, por ejemplo, revelar fotografías íntimas, explotar cuentas de usuario, robar dinero, realizar transferencias electrónicas, usurpar información valiosa para cobrar por la liberación de los datos, entre muchas otras cosas peligrosas que podría llevar a cabo un delincuente.

Además, los atacantes siempre priorizan y se preparan teórica y prácticamente para realizar amenazas avanzadas y continuas. Esto quiere decir, que un ciber ataque sólido considera distintos vectores de ataque en conjunto para una sola víctima, como también la perduración de este tipo de vulneraciones y los ataques continuos para seguir teniendo el control del usuario.

Si se logra un ataque Man in the Middle, por ejemplo, se puede sobre cargar el canal de comunicación al enviar o inyectar miles de solicitudes al otro dispositivo, lo que finalmente provocará una caída del servicio, considerándose un ataque de explotación de denegación de servicios.

Para prevenir este tipo de ataques se dispone una herramienta integrada en algunos sistemas operativos dedicados al Hacking Ético como Sniffer, el cual es un programa de captura de las tramas de una red de computadoras.

Para esto, el hacker configura su tarjeta de red en modo promiscuo, permitiendo que en la capa de enlace de datos no sean descartadas las tramas que no son destinadas a esa dirección MAC o dirección física de la tarjeta, de esta forma se puede olfatear (“sniff”) todo el tráfico que viaja por la red.

Se usa con fines tanto éticos como malicioso, ya que se puede utilizar para robar contraseñas, interceptar correos electrónicos, espiar conversaciones de chat, etc. Para proteger la información de esta aplicación web, se vuelve a citar el cifrado de información, como método de

protección en caso de ser víctimas de un ataque.

Si la información no está cifrada, viaja como texto plano mediante el protocolo IP, lo que podría revelar fácilmente el par nombre de usuario y contraseña. Otra buena opción es integrar una sólida autenticación del emisor del datagrama y el receptor de los paquetes de información y el integrar firmas digitales para el acceso de los usuarios.

Para este tipo de ataques de red, existen sistemas de protección de las comunicaciones que actúan monitorizando el tráfico que entra o sale de la red, con distintas características y ventajas para la ciberseguridad de una empresa o institución.

Uno de estos sistemas es el conocido como IDS o sistema de detección de intrusiones, que es un sistema o una aplicación usada para detectar accesos no autorizados a un ordenador o a una red, es decir, monitorizan el tráfico entrante y lo cotejan con una base de datos actualizada. Ante cualquier actividad sospechosa, emiten una alerta a los administradores del sistema que deberían tomar las medidas oportunas.

Se propone un IDS programado para el laboratorio, incluido el filtrado de MAC, es decir, generar una lista blanca para la red del CIMUBB, filtrando a los usuarios que deberían tener acceso o no a la red.

Otro de estos sistemas a favor de la seguridad es el conocido como IPS o sistema de prevención de intrusiones, definido como un software que se utiliza para proteger a los sistemas de ataques e intrusiones.

Llevan a cabo un análisis en tiempo real de las conexiones y los protocolos para determinar si se está produciendo o se va a producir un incidente, identificando ataques según patrones, anomalías o comportamientos sospechosos, permitiendo el acceso a la red, implementando políticas que se basan en el contenido del tráfico monitorizado. Es decir, el IPS además de lanzar alarmas al personal, puede descartar paquetes y desconectar conexiones.

Otras recomendaciones para tener una experiencia de trabajo más seguro a nivel

informático es utilizar una VPN. Esta es una conexión a una red privada virtual, es decir, permite crear una red local sin necesidad de que sus dispositivos o integrantes estén conectados entre sí, sino a través de internet.

La VPN genera un túnel de datos, lo que quiere decir que el tráfico de un dispositivo va hacia el dispositivo del proveedor de internet, pero desde ahí se dirige directo al servidor VPN, donde la conexión está cifrada, de modo que el proveedor de internet no es consciente de a donde se está accediendo.

Se utilizan ampliamente para los sistemas de teletrabajo, para trabajadores que no están físicamente en la oficina o empresas con varias sucursales en distintas ciudades, por ejemplo. Esto produce una disminución considerable en el riesgo a ser vulnerada la información de un usuario o trabajador, ya que el acceso está protegido, la conexión está previsiblemente cifrada y el usuario tiene el mismo acceso que si estuviera presencialmente en la oficina. Una buena recomendación es utilizar este servicio para cuando se necesite registrar información sensible en cierta plataforma, como iniciar sesión en cuentas bancarias o realizar transacciones, por ejemplo.

Otra buena técnica de seguridad informática es el sandboxing. Consiste en la ejecución de programas o aplicaciones en un espacio virtual limitado, en el cual se pueden controlar todos los procesos sin que afecten al resto del equipo. Es una caja de arena, haciendo referencia a los espacios de juegos donde los niños pueden jugar sin correr peligro mientras son supervisados por sus padres.

Al emplear esta técnica, los programas se ejecutan en un entorno virtual controlado. Es decir, solo funcionan dentro de ese espacio virtual de prueba y no tienen acceso al resto de recursos o procesos del equipo. Si ejecutamos un programa infectado en un sandbox, el malware como virus o ransomware quedará encerrado en ese entorno de pruebas y no podrá dañar el resto del equipo. De esta forma, si se descubre alguna amenaza en un programa ejecutado en un entorno sandbox, se bloquearía su ejecución en el entorno real y el sistema no se vería afectado. Consiste en una medida de seguridad preventiva que ejecuta los programas en un espacio virtual cerrado capaz de detectar si se trata de una aplicación confiable o no.

Para este trabajo, se propone realizar pruebas de análisis de redes constantemente, una vez por semana al menos, con el fin de un sistema virtual para realizar experiencias de penetración, o instalar directamente un servidor con herramientas de ciber seguridad como Kali Linux. De esta forma, se podrán realizar pruebas de vulnerabilidades en una máquina virtual con la aplicación en tiempo real de ejecución para validar las capas de seguridad a nivel de código y poder reaccionar en contra de ellos de distintas maneras, sin comprometer los equipos personales.

También existen ataques que están enfocados en técnicas de Hacking Ético y pruebas de penetración. El más básico de ellos es el ataque de Fuerza Bruta, que consiste netamente en utilizar una base de datos de más de 2 billones de contraseñas utilizadas por la mayoría de los usuarios como ensayo y error para ingresar a las cuentas de usuario, obtener llaves de encriptación o incluso encontrar páginas web ocultas.

El atacante intenta todas las combinaciones posibles de usuario-contraseña esperando que coincidan en alguna de estas combinaciones. Es decir, estos ataques se logran mediante fuerza bruta, considerando que se fuerza excesivamente con millones de intentos para ingresar a las cuentas privadas de la víctima. Es uno de los ataques más antiguos, pero siguen siendo efectivos y populares entre hackers. Para este trabajo, se propone un nivel fuerte en seguridad de contraseñas, además de un correcto cifrado y encriptación de la información sensible.

Similarmente, existe un ataque llamado Ataque de Diccionario, definido como un método para romper la seguridad de un inicio de sesión de un computador, una aplicación web u otro recurso de tecnología de la información al entrar sistemáticamente cada palabra en un diccionario como si fuera una contraseña.

Puede ser utilizado para encontrar la llave de encriptación de un mensaje o documento previamente encriptado. Estos ataques siguen funcionando debido a que muchos usuarios de computadores o negocios insisten en utilizar palabras ordinarias como contraseñas, por lo que se insiste en utilizar y crear contraseñas fuertes en ese sentido, con letras tanto mayúsculas como minúsculas, números, caracteres, símbolos, etc.

Con respecto a esto, una buena práctica de seguridad es nunca reutilizar las contraseñas, ya que, si consiguen vulnerar una sola cuenta, es probable que sean todas igual de vulnerables. Además, siempre se recomienda utilizar el doble factor de autenticación 2FA, considerado como un nivel extra en la seguridad de dispositivos, utilizado para asegurar el acceso a ciertas cuentas online.

Para este trabajo se propone un sistema fuerte de contraseñas, con el fin de que no se puedan vulnerar de manera sencilla, o que no se encuentren fácilmente en estas bases de datos y así no comprometer esta información a este tipo de ataques, como el de fuerza bruta o el de diccionario.

Otra herramienta bastante utilizada y recurrente en los ataques a nivel de red es nmap. Es una función open source o de código abierto utilizada para el diagnóstico de redes e implementaciones de seguridad informática.

Se trata de una herramienta de escaneo de puertos y descubrimiento de hosts, permitiendo obtener una gran cantidad de información sobre equipos de la red, escanear hosts levantados y si tienen puertos abiertos. Otras ventajas que tiene es que puede ser utilizado para tareas como inventariar la red al conocer todos los dispositivos conectados a ella, manipular servicios, monitorear, etc. Con nmap es muy fácil conocer el estado de la red, los dispositivos conectados a ella y sus puertos abiertos, que está considerado como una información extremadamente sensible, ya que se puede rastrear la información, interceptarla o enviar y subir malware o archivos maliciosos por los puertos abiertos, al saber la dirección, el protocolo, etc.

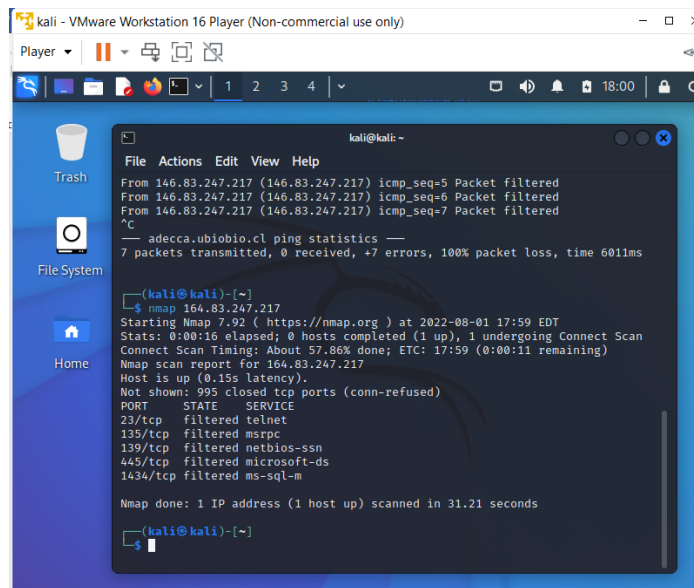


Figura 8.1 – Herramienta nmap para encontrar escanear dispositivos o redes.

Se debe considerar lo útil de esta herramienta, ya que los ataques basados en Hacking tradicional primero buscan una dirección IP de la víctima, luego algún puerto que esté abierto, obtener información importante de ese puerto (como recursos, protocolos, conexiones, etc.), para de esta forma obtener vulnerabilidades con respecto a la información importante de cada puerto del dispositivo.

Similarmente existe una herramienta bastante utilizada y reconocida dentro del mundo hacker llamada Wireshark. Este es un analizador de protocolos ampliamente utilizado dentro del hacking ético, ya que permite visualizar que sucede dentro de la red a un nivel microscópico y es el estándar de facto en empresas comerciales, agencias de gobierno e instituciones educativas. Con esta herramienta es posible realizar un análisis de la red y encontrar soluciones a problemas de redes de comunicaciones, para el análisis de datos y protocolos. Ofrece una interfaz gráfica y muchas opciones de organización y filtrado de información.

De esta forma, permite ver todo el tráfico que pasa a través de una red (usualmente Ethernet, aunque es compatible con algunas otras) estableciendo la configuración en modo promiscuo. Gracias a Wireshark, es posible examinar o capturar información y analizarla a través de sus detalles y sumarios por cada paquete transferido. No tiene problemas de ejecución ya que

es ejecutado con permisos de super usuario.

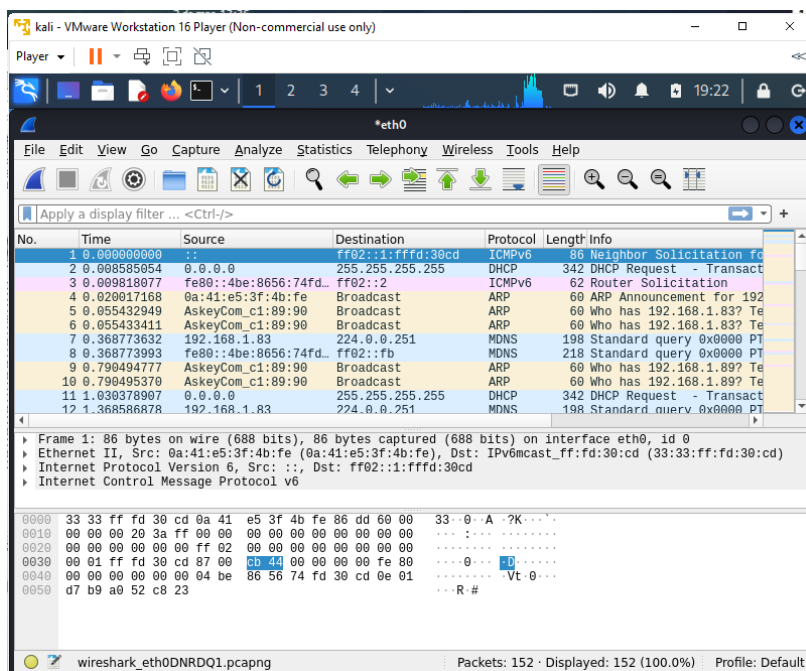


Figura 8.2 – Herramienta Wireshark para interceptar tráfico de red.

Para lograr un buen mecanismo de defensa con respecto a seguridad informática, se pueden utilizar muchas estrategias distintas, incluso complementarlas para lograr una red segura y fuerte digitalmente y tener también una plataforma igual de segura y confiable.

Una definición importante hasta este punto es el concepto de malware. Este es un término genérico utilizado para describir una gran variedad de software hostil o intrusivo, como virus informáticos, gusanos, caballos de troya, softwares de rescate, spyware, adwares, softwares de miedo, etc. Este puede tomar la forma de código ejecutable, scripts, contenido activo u otro tipo de software. Además, puede encriptar o eliminar datos confidenciales, modificar o desviar las funciones básicas de un ordenador o simplemente espiar la actividad informática de los usuarios. El malware es utilizado por los ciberdelincuentes para ganar dinero, con fines de sabotaje, por razones políticas, para hacer daño, etc.

Un rootkit es un paquete de software malicioso (o malware) que está diseñado para permanecer oculto en un ordenador mientras proporciona acceso y control remoto a algún

delincuente. Los ciber atacantes los utilizan para manipular el equipo sin el conocimiento o el consentimiento del usuario.

Puede contener una secuencia de herramientas que permiten robar contraseñas, información de tarjetas de crédito o banca online e información personal, dependiendo de la programación o la intención del ataque. Es posible que este tipo de malware pueda estar en el ordenador durante mucho tiempo, ocasionando daños importantes, ya que son difíciles de detectar y de eliminar.

Lo más común es infectarse mediante una vulnerabilidad en el sistema operativo o en alguna aplicación que se ejecuta en el ordenador, por lo que los ciber delincuentes se aprovechan y ejecutan código de explotación para obtener una posición privilegiada. Además, se puede infectar a través de dispositivos USB, correos electrónicos, archivos de descarga y aplicaciones móviles infectadas. Se debe mantener actualizados los programas de protección como antivirus y firewall, así como mantener el sistema actualizado para evitar vulnerabilidades. También es recomendable evitar la descarga de archivos de enlaces maliciosos y se promueve la utilización de contraseñas robustas, cambiándolas de manera frecuente para disminuir las brechas en cuanto a seguridad informática.

Por otro lado, el ransomware es una forma de malware que está en auge, bloquea los archivos o dispositivos del usuario y luego reclama un pago online anónimo para restaurar el acceso. Se trata de un malware de rescate, el cual impide a los usuarios acceder a su propio sistema o a sus archivos personales, exigiendo el pago de un rescate para poder acceder nuevamente a estos recursos. Es posible contraer este malware de muchas maneras, siendo el método más habitual mediante spam malicioso, correspondiente a mensajes no solicitados que se utilizan para enviar malware por correo electrónico, por ejemplo. Dicho correo, además, puede contener o incluir archivos adjuntos trampa, como PDF o documentos de Word, o incluso enlaces a sitios web maliciosos. Este tipo de ataque se vale de técnicas de ingeniería social para engañar a la gente con el fin de que abra estos archivos adjuntos o haga clic en vínculos que parecen legítimos, aparentando que proceden de una institución de confianza o de un amigo, profesor, colega, etc.

Las buenas prácticas defensivas anti ransomware incluyen la inversión en programas de seguridad informática como antivirus y similares, además de crear copias de seguridad de los datos regularmente, ya sea en la nube o en dispositivos externos USB o discos duros.

Con esto se vuelve a hacer énfasis en el concepto de ciber resiliencia, enfocado en esperar lo peor y prepararse para lo mejor. De esta forma, a pesar de ser atacados o vulnerados, será posible levantarse a pesar de los contratiempos y daños que pudieran comprometer la información de los distintos usuarios. Se debe estar siempre informado para evitar este tipo de ataques, ya que una de las formas más habituales en la que se infectan los ordenadores o equipos con ransomware es a través de la ingeniería social previamente detallada.

Es una muy buena práctica y recomendación formarse y además proporcionar información importante al grupo de trabajo con respecto a la detección de esta amenaza. El aprendizaje continuo es la mejor carta a favor para poder contrarrestar estos ataques y también para poder evitarlos.

Cuando se es vulnerado por ataques de este tipo, es posible además caer en un ataque del tipo backdoor, que consiste en una herramienta para ganar acceso remoto a otros equipos, complementando el modus operandi del ransomware, por ejemplo. Este es un tipo de virus diseñado para dar acceso a los usuarios maliciosos o atacantes, otorgando el control de cierto equipo o dispositivo infectado de manera remota. Se conocen también como puertas traseras, permitiendo al usuario malicioso controlar al equipo infectado, pudiendo enviar y recibir archivos, ejecutarlos o eliminarlos, mostrar mensajes, borrar o robar datos, reiniciar el equipo, conceder permisos o acceso a otras cuentas, etc. Es decir, es posible controlar el equipo como si estuviese sentado en un escritorio delante de él.

Algunos backdoors pueden venir previamente instalados en el sistema o aplicaciones utilizadas por el usuario, explotando una vulnerabilidad para entrar al equipo de manera inadvertida y hacerse con el control de este para realizar todo tipo de actividades a través del equipo infectado o robar información directamente sin que el usuario sea advertido. Ahora, siempre que estén bien configurados y solo permitan el acceso a usuarios legítimos, no deberían suponer un

problema, ya que ciertos desarrolladores los dejan a propósito para tener acceso a los equipos o aplicaciones y así poder actualizarlas o solucionar problemas de forma remota, es por esto que se propone el uso de este tipo de entrada secreta en la plataforma SLD, en caso de necesitar mantención una vez terminada, como actualizaciones, limpieza, mantención, agregar capas de seguridad, corregir errores, etc. El backdoor se puede implementar sencillamente al crear archivos con la extensión bat, que permiten acceder al símbolo del sistema y darle instrucciones al sistema operativo. Cabe destacar que se utilizan este tipo de archivos para lograr la comunicación serial hacia el brazo robótico mediante lenguaje web desde un punto remoto que tiene acceso al laboratorio virtual.

Ahora, con respecto a ataques en plataformas web, se tiene uno bastante conocido llamado DDoS, o mejor conocido como un ataque de denegación distribuida de servicios. Este tipo de ataque aprovecha los límites de capacidad específicos que se aplica a cualquier recurso de una aplicación web, así como a la infraestructura que habilita el sitio web de la empresa, institución, establecimiento, etc. Este ataque envía muchas solicitudes al recurso web atacado, con la intención de desbordar la capacidad de respuesta a solicitudes del sitio web para administrar varias peticiones y así evitar que este sitio o aplicación deje de funcionar correctamente.

Los objetivos más comunes de este tipo de ataques son los sitios de compra por internet, casinos en línea o cualquier tipo de empresa u organización que dependa de la prestación de servicios en línea. Se debe considerar que los recursos de red (como servidores web) tienen un límite finito de solicitudes que pueden atender al mismo tiempo. Además de este límite de capacidad, el canal que conecta el servidor a internet tiene un ancho de banda o capacidad limitados. Entonces, cuando la cantidad de solicitudes sobrepasa estos límites de capacidad de cualquier componente de la infraestructura, el nivel del servicio se verá afectado de forma que las respuestas a las solicitudes serán mucho más lentas de lo normal o que se ignoren algunas o todas las solicitudes de los usuarios.

Por regla general, la intención primordial del atacante es evitar por completo el funcionamiento normal del recurso web, es decir, busca una denegación total del servicio. El atacante también podría solicitar un pago para detener el ataque, lo que no es recomendable ya que

se trata de confiar en un ciber delincuente. Para prevenir de cierta forma este tipo de amenaza, se limita a nivel de código PHP la cantidad de solicitudes para el acceso a la plataforma, evitando de cierta manera la inundación de solicitudes en cortos períodos de tiempo, lo que se detallará a continuación.

Existe un ataque DDoS que consiste en una inundación de ping, sobrecargando un objetivo con solicitudes ICMP. Una inundación de ping es un ataque de denegación de servicio en el que el atacante intenta sobrecargar un dispositivo objetivo con paquetes de solicitud de eco ICMP, lo que provoca que el objetivo se vuelva inaccesible al tráfico normal. Cuando el ataque de tráfico proviene de múltiples dispositivos, el ataque se convierte en un ataque DDoS o de denegación de servicio distribuido. ICMP es un protocolo de la capa de internet que utilizan los dispositivos de red para comunicarse, intercambiando datos de estado o mensajes de error entre dispositivos. Una solicitud ICMP requiere algunos recursos del servidor para procesar cada solicitud y para enviar una respuesta. También requiere ancho de banda tanto en el mensaje entrante como en la respuesta saliente. Este ataque pretende sobrecargar la capacidad del dispositivo objetivo para responder al elevado número de solicitudes y sobrecargar la conexión de red con tráfico falso. Para esto se propone desactivar la funcionalidad ICMP del enrutador, ordenador u otro dispositivo instalado en el laboratorio.

Ahora, continuando con los ataques relacionados con redes, se tiene uno llamado RAP. Un Rogue Access Point Interno es un punto de acceso conectado a la red de alguna empresa o institución manejado por alguien que no ha sido aprobado. Permite el robo de información como contraseñas y datos confidenciales, así como acceso a la red por usuarios no autorizados, abriendo muchas vulnerabilidades para la red de computadores o dispositivos.

Un Rogue Access Point Externo no está conectado a la red de la organización, sino que se hace pasar por un Access Point auténtico, es decir, se hace pasar por una red inalámbrica abierta de algún aeropuerto, por ejemplo, para que los usuarios se conecten y ofrezcan sus datos a la aplicación del atacante. Por esta razón, los usuarios nunca deberían escribir información delicada en redes inalámbricas abiertas que no parezcan seguras.

Se debe evitar también el ataque Evil Twin o gemelo malvado, que consiste en que un ciber delincuente pone en funcionamiento una red Wifi que parece ser legítima pero que en realidad tiene el objetivo de robar datos de las víctimas, realizar ataques Man in the Middle, etc., ya que todo nuestro tráfico pasa a través del equipo del atacante y especialmente, si este no está cifrado (HTTP) puede ser fácilmente utilizado y robado. Se puede llevar a cabo muy fácilmente creando una red Wifi con el mismo SSID que el punto de acceso legítimo, incluso utilizando la misma dirección MAC para que sea más complicada su identificación e incluso evitar la conexión al punto de acceso legítimo para conectarse al falso, al combinarse con un ataque DDoS (denegando los servicios de la red legítima) para dar de baja el punto de acceso original y así dar prioridad a la conexión del punto de acceso malicioso.

Se debe evitar el conectarse a un punto de acceso público sobre los cuales no se tenga control alguno, utilizar 2FA para todas las cuentas mientras sea posible, desconfiar siempre y aprender a identificar intentos de Phishing, URL falsas, etc., utilizar solo sitios HTTPS y tratar de utilizar VPN dentro de lo posible, para encriptar el tráfico antes de abandonar el dispositivo.

Además, se debe tener conocimiento de los portales cautivos, que son programas o máquinas de una red informática que vigilan el tráfico HTTP y fuerza a los usuarios a pasar por una página especial si quieren navegar por internet de forma normal. El portal cautivo también es una página web, conocida como una página de login o acceso, que se presenta al usuario antes de acceder a la red wifi pública donde los usuarios pueden autenticarse utilizando sus propias credenciales. El programa intercepta todo el tráfico HTTP hasta que el usuario se autentifica. El portal se encargará de hacer que esta sesión caduque al cabo de un tiempo. También puede empezar a controlar el ancho de banda usado por cada cliente. Este ataque se utiliza en redes inalámbricas abiertas, con un mensaje de bienvenida a los usuarios, informando las condiciones de acceso como puertos permitidos, responsabilidad legal, etc. Se debe tener especial cuidado en confiar en cualquier página o portal web, ya que muchas veces existen imitaciones o páginas que se camuflan con otras para fines maliciosos.

Por otro lado, el forced browsing es un ataque donde el objetivo consiste en enumerar y acceder a recursos que no son referenciados por la aplicación, pero siguen siendo accesibles. Un

atacante puede utilizar técnicas de fuerza bruta para buscar contenidos desvinculados en el directorio del dominio, como archivos temporales, respaldos antiguos y archivos de configuración. Estos archivos pueden almacenar información sensible acerca de las aplicaciones de la web y sistemas operativos, como código fuente, credenciales, direcciones internas de la red, etc., que son considerados como recursos valiosos para los intrusos. Este concepto se debe considerar y mejorar a nivel de programación de la plataforma web, es decir, se debe lograr compensar esta vulnerabilidad a nivel de código.

A nivel empresarial o corporativo, uno de los ataques más efectivos es el conocido como Watering Hole Attack. Este ataque consiste en observar cuales son los sitios web que la organización más frecuente y utiliza para así infectarla con malware o utilizar un archivo como sustituto para robar información confidencial. Eventualmente, ciertos miembros de la empresa estarán infectados dentro de poco. Por esta razón, siempre se debe actualizar los softwares y sistemas operativos para remover las vulnerabilidades que permitan infectar a la plataforma de monitoreo del Scrobot, además de siempre monitorizar las redes de internet y los sitios web que se utilizan dentro del laboratorio CIM.

Una vez ingresando a ciertas plataformas o sitios web, es posible observar que la gran mayoría de ellas tienen un sistema de cookies. Este es un pequeño archivo que se almacena en el equipo local, con el fin de reducir las etapas de inicio de sesión en algunas plataformas de compra y venta, redes sociales, plataformas universitarias, etc. Almacena las preferencias de algunos usuarios y complementa sus servicios al ofrecer ciertas funciones o productos recomendados para el usuario en cuestión. Estos pequeños archivos no son dañinos, es decir, no infectan al equipo, pero pueden comprometer la privacidad de los usuarios, por lo que se debe tener especial cuidado en cederles permisos, ya que pueden ser vulnerados o robados. Una buena recomendación es tener una buena higiene digital con respecto a este tema, lo que quiere decir que se recomienda borrar o eliminar las cookies periódicamente. En particular para este proyecto, se descarta el sistema de cookies por seguridad, no son archivos dañinos para el sistema, pero si llegan a ser vulnerados podría ser perjudicial. Además, se integra un sistema de cierre de sesión sólido, que no almacene registros de los usuarios que están ingresando recurrentemente a la plataforma.

Similar a las cookies, existe un tipo de ataque que recopila información de los sitios online llamado Browser Fingerprinting. Este ataque es un poderoso método que utilizan los sitios web para recolectar información acerca del tipo de buscador que usa el usuario, la versión, así como el sistema operativo, plugin activo, zona horaria, lenguaje, resolución de pantalla y otras configuraciones activas del equipo personal del usuario. La gran mayoría de los sitios utilizan estos datos para personalizar anuncios o información que podría servirle al usuario. Para evitar este tipo de amenazas, se pueden utilizar complementos del buscador que sirvan para bloquear los anuncios, como también utilizar métodos de búsqueda privados, o el modo incógnito es una buena estrategia de defensa ante este ataque.

Otra forma de protegerse es desactivar JavaScript y Flash, ya que al estar desactivados los sitios web no podrán detectar la lista de plugins activos o fuentes que utiliza el usuario, por lo que tampoco serán capaces de instalar ciertas cookies en el buscador. Existe un buscador bastante famoso por la seguridad y privacidad que ofrece llamado Tor. Utilizar este buscador y un servicio de VPN es una de las mejores formas de navegar seguro en la web.

El ataque OS Fingerprint es el proceso de aprender que sistema operativo está corriendo en un dispositivo. Puede ser utilizado para analizar como administrador cuando se conecta un nuevo dispositivo a la red. Además, puede ser utilizado como parte de un scanner de reconocimiento en una red. Se plantea un script con distintas funciones de ciber seguridad integradas, incluyendo este método, con el fin de tener un registro de la actividad del sistema informático regularmente, programado para que una vez al día ejecute una acción de monitoreo del sistema de red del laboratorio, a fin de evitar vulnerabilidades o de actuar en caso de comportamientos sospechosos.

8.2 Pruebas de penetración y Hacking ético

Como se especifica previamente, para realizar las pruebas de penetración a la red local de laboratorio y a la plataforma web, que permitirán un escaneo preventivo o correctivo, se utiliza el sistema operativo Kali Linux, que se instala en uno de los equipos del laboratorio, ya que tiene integrado múltiples funciones dedicadas a encontrar vulnerabilidades en la red y es una suite

bastante potente para implementar estrategias y técnicas de hacking ético. Se utiliza bastante en laboratorios virtuales dentro de un mismo equipo, es decir, utilizar máquinas virtuales para realizar estos procedimientos de ataque y de análisis, ya que de esta forma no comprometemos la integridad de ningún dispositivo.

Dentro de las aplicaciones importantes de este sistema operativo están las conocidas investigaciones de seguridad informática, informática forense, ingeniería inversa, pruebas de penetración, etc. Para este trabajo se utilizan herramientas integradas en el sistema operativo Kali Linux, para luego crear distintos escenarios de protección y análisis que establecerán el proceso de ataque y de defensa para integrar nuevas capas de seguridad informática en la red de laboratorio, con el fin de buscar vulnerabilidades en la aplicación y resolverlas mediante estrategias de cuidado y seguridad informática y mediante código PHP y SQL, privando algunos recursos o agregando capas de seguridad tanto a la plataforma web como a la red de laboratorio.

La mayoría de los ataques, sino todos, comienzan con una etapa de Reconocimiento, es decir, se comienza siempre por estudiar a la víctima con respecto a las páginas web que frecuenta, lugares físicos o virtuales donde se instala, tipo de equipo que usa para conectarse a la web, sistema operativo, puertos abiertos, etc., es decir, se analiza a la víctima para encontrar posibles vulnerabilidades o brechas de seguridad. Esta información es realmente valiosa para un ciber delincuente, ya que intenta buscar vulnerabilidades a partir del movimiento de la víctima en la red.

Para esta etapa se utiliza una herramienta bastante poderosa con respecto al escaneo de vulnerabilidades y reconocimiento virtual llamada nmap. Esta herramienta de penetración viene integrada en el sistema operativo Kali Linux, por lo que no requiere previa instalación ni nada similar, de hecho, es posible utilizar sus recursos y funcionalidades de manera muy sencilla y rápida.

Por ejemplo, para efectos prácticos, se realiza un escaneo a la máquina local desde la máquina instalada con el sistema operativo de hacking ético, es decir, desde el sistema operativo Kali Linux es posible escanear el equipo local donde está la máquina virtual e incluso podría escanear cualquier dispositivo que esté conectado a la misma red local LAN. Se ha de considerar

que nmap podría ser un complemento de otras herramientas de hacking para establecer un ataque y defensa mucho más sólido y dedicado a una víctima en específico.

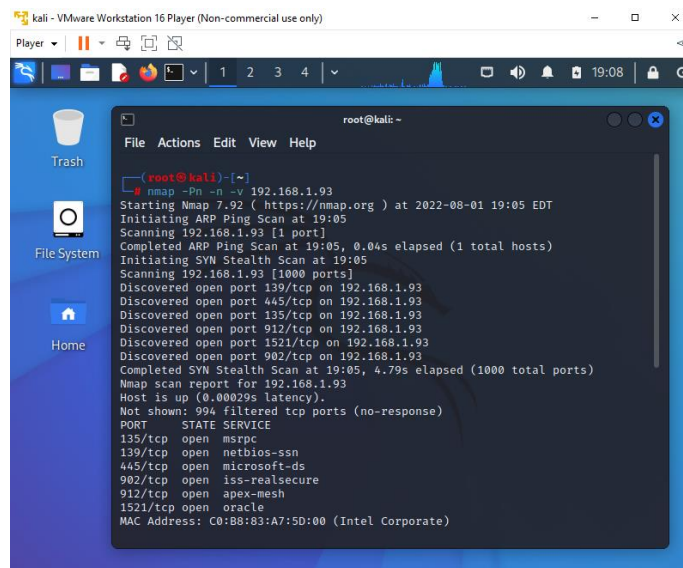


Figura 8.3 – Análisis de puertos con nmap.

Como se aprecia en la figura, es posible escanear un dispositivo y conocer todos sus puertos abiertos al conocer su dirección IP. Como se trata de un escaneo al equipo local (desde la máquina virtual Kali Linux a un notebook personal dentro de la misma red), es verdaderamente sencillo encontrar su dirección IP, por lo que sólo basta con tener leves conocimientos en redes y de las funcionalidades de nmap para poder encontrar información valiosa a partir de direcciones IP.

Con esta información, es posible determinar los puertos abiertos del equipo donde se está estableciendo comunicación, incluso se puede obtener la dirección MAC, como también se puede observar claramente qué tipo de servicio y protocolo de comunicación está utilizando cada puerto. Ahora, si se logra complementar la información detallada en la etapa teórica de este capítulo, se podrían integrar y definir ataques de penetración avanzados considerando toda esta información. Considerar nuevamente que los ciber delincuentes utilizan esta información para complementarla con más información relacionada a métodos de ataque o de amenazas digitales, utilizando distintas herramientas del sistema operativo Kali o herramientas disponibles en la web para analizar a una víctima.

Por ejemplo, si un ente externo malicioso logra tener acceso a la red local de alguna manera, podría fácilmente realizar un ataque de MAC Spoofing o IP Spoofing (o ambos), es decir, reemplazar la MAC o la dirección IP de un equipo atacante (dependiendo del caso) por la de otro dispositivo conectado a la red, para que los datos que en un principio le correspondían, ahora se transmitan hacia el equipo atacante.

Además, como se tienen los puertos que están abiertos en el equipo, con su protocolo de comunicación y el propio servicio para ese puerto es posible enviar información o datos de manera maliciosa al considerar esta vulnerabilidad y descuido, si es que no se tiene un control en el flujo de la comunicación de ese puerto. Un ataque que puede ser sencillamente realizado bajo estas circunstancias es el de Man in the Middle o el de fuerza bruta o diccionario, por ejemplo.

Se propone realizar un escaneo de puertos regularmente, con el rol de administrador de sistemas para no ser vulnerado por alguno de los ataques relacionados a esta área, supervisar el tráfico de datos en la red y para cerrar las brechas de seguridad. Esta supervisión verifica si los paquetes de datos se envían a través de los puertos previstos, si los firewalls bloquean involuntariamente puertos importantes y si los puertos abiertos no utilizados deben cerrarse. Además, se debe considerar que nmap se utiliza exclusivamente en entornos controlados, de otra forma, si se utiliza en otro equipo sin consentimiento, puede ser considerado un intento de ataque al sistema, por lo que es una herramienta ilegal en ese sentido. Las herramientas de análisis de puertos son útiles tanto para un atacante que intente vulnerar la red como para un administrador de TI que intente protegerla.

De esta forma, se plantea una estrategia de ataque leve con el fin de adquirir conclusiones clave con respecto a la seguridad a nivel de red y luego de programación. Esta prueba consiste en utilizar herramientas de hacking ético, realizando una pequeña prueba de Spoofing y así analizar lo crítico que puede ser si se implementa en un sistema que se quiera vulnerar. En primera instancia, se debe verificar que ambos equipos estén en la misma red. Para este caso, se tiene una máquina Kali Linux, tratando de atacar al equipo real que tiene instalada la plataforma de control. Para verificar la comunicación se establece una serie de mensajes con el protocolo ICMP, más conocido como ping de red.

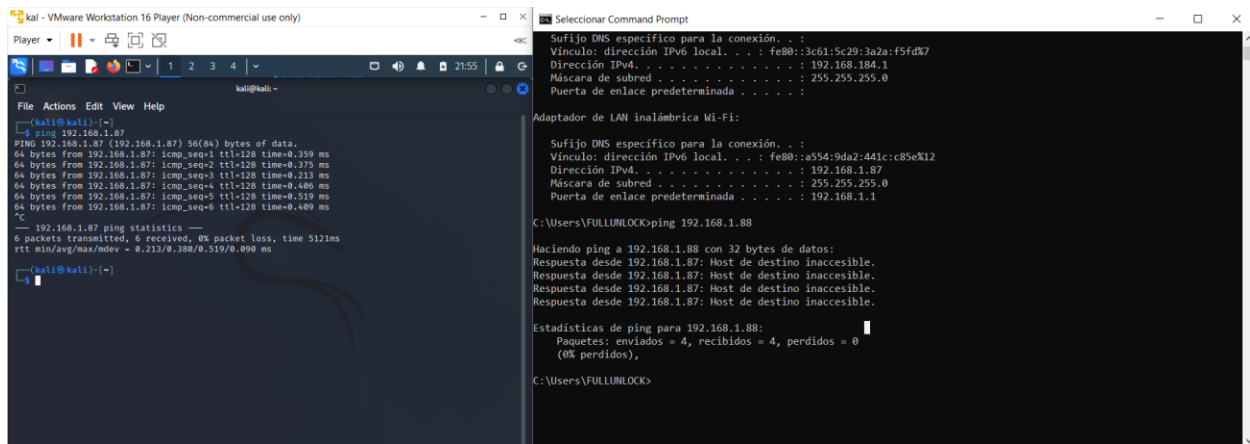


Figura 8.4 – Comunicación establecida entre las dos máquinas.

Esta figura muestra que existe comunicación entre las dos máquinas, ya que se envían mensajes ICMP para verificar que tienen conexión entre ellas. Como complemento a estas vulneraciones, existe también un comando super efectivo y verdaderamente útil para monitorear la red local y de cierta forma poder encontrar intrusos llamado netdiscover. Solo basta con ejecutarlo desde la consola de comandos de Kali para rastrear información valiosa de la red. Cabe destacar que este tipo de procedimientos son exclusivamente para encontrar vulnerabilidades en la red y compensarlas con algún procedimiento o estrategia.

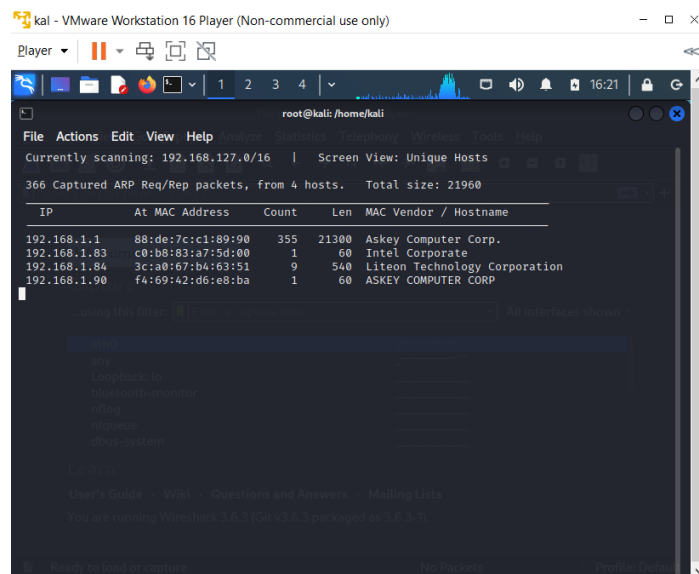
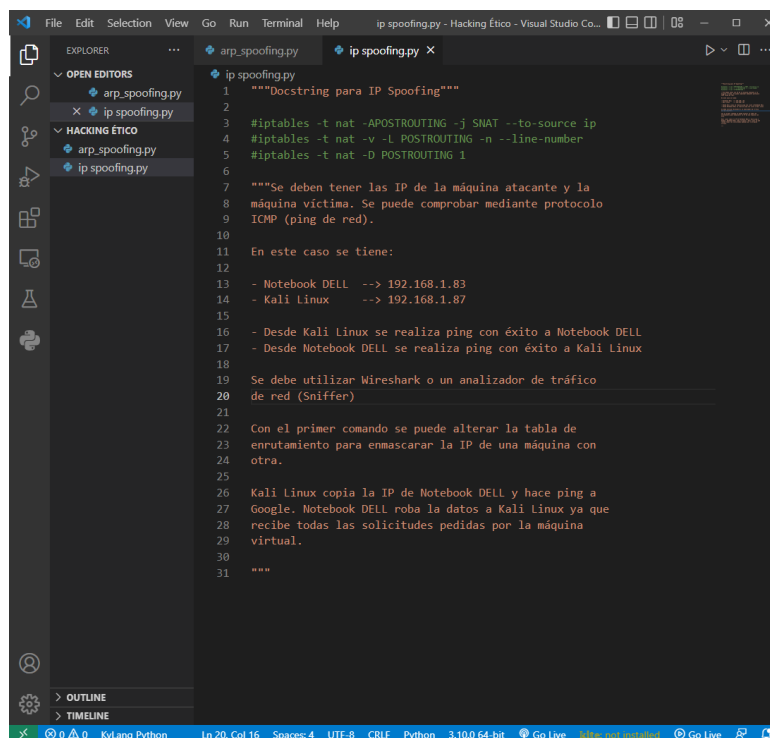


Figura 8.5 – netdiscover en Kali Linux.

Una vez que se conocen los usuarios conectados a la red, es posible monitorear su tráfico, como también alterar el direccionamiento y el enrutamiento de los paquetes de datos. Luego, se debe utilizar un comando en Kali Linux llamado iptables, que permite acceder a las tablas de enrutamiento del router y así poder modificar las direcciones IP y MAC de cualquier dispositivo, pudiendo interceptar las comunicaciones, monitorearlas y directamente robar información desde un equipo o desde algún servidor web, como Google, Facebook, Instagram, etc. Con este comando y algunas extensiones, es posible alterar la dirección IP o MAC de un dispositivo, cambiándola con otra para recibir el tráfico de datos que le pertenece a la máquina vulnerada. Dicho de mejor forma, la máquina Kali Linux cambia su dirección IP por la del equipo local (notebook personal) en la que está montado el laboratorio. De esta forma, todo el tráfico en la red que se dirigía al equipo local ahora estará dirigido hacia Kali Linux, lo que se traduce directamente a un robo de información por parte de la máquina. Este procedimiento es solo como demostración, y se utiliza en entornos controlados, ya que no se quiere llegar a caer en algún ataque de este tipo.



```
1  """Docstring para IP Spoofing"""
2
3  #iptables -t nat -A POSTROUTING -j SNAT --to-source ip
4  #iptables -t nat -v -L POSTROUTING -n --line-number
5  #iptables -t nat -D POSTROUTING 1
6
7  """Se deben tener las IP de la máquina atacante y la
8  máquina víctima. Se puede comprobar mediante protocolo
9  ICMP (ping de red).
10
11  En este caso se tiene:
12
13  - Notebook DELL --> 192.168.1.83
14  - Kali Linux --> 192.168.1.87
15
16  - Desde Kali Linux se realiza ping con éxito a Notebook DELL
17  - Desde Notebook DELL se realiza ping con éxito a Kali Linux
18
19  Se debe utilizar Wireshark o un analizador de tráfico
20  de red (Sniffer)
21
22  Con el primer comando se puede alterar la tabla de
23  enrutamiento para enmascarar la IP de una máquina con
24  otra.
25
26  Kali Linux copia la IP de Notebook DELL y hace ping a
27  Google. Notebook DELL roba la datos a Kali Linux ya que
28  recibe todas las solicitudes pedidas por la máquina
29  virtual.
30
31  """
```

Figura 8.6 – Procedimiento para IP Spoofing.

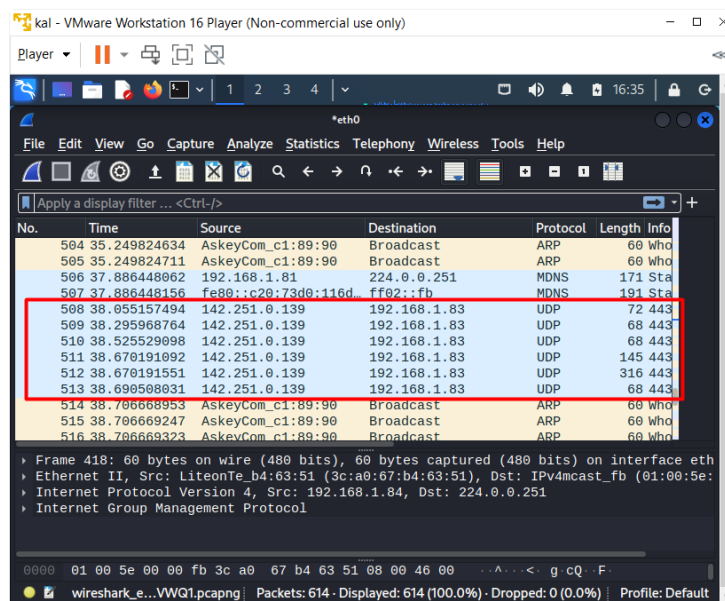


Figura 8.7 – Análisis de tráfico mediante Wireshark.

En la Figura 8.7 se puede apreciar el procedimiento a seguir para realizar un sencillo pero certero ataque de IP Spoofing dentro de una misma red local. Como se puede observar, con este simple procedimiento es posible que una máquina o dispositivo le robe información fácilmente a otra mediante simples comandos que modifican la tabla de enrutamiento del router. Como se puede observar en la Figura 8.8, se tiene el análisis del tráfico de la red mediante Wireshark, un analizador de red o Sniffer.

En esta captura de pantalla se puede observar que la IP 192.168.1.83, que corresponde al equipo local, está recibiendo datos desde un servidor de Google, que representa a la solicitud hecha por la máquina virtual Kali Linux una vez que se auto asignó la IP del equipo Dell. Esto quiere decir, que el equipo local Dell está recibiendo la información que debería llegarle a Kali Linux, lo que implica una modificación en el enrutamiento de los paquetes IP. Esto quiere decir que cualquier individuo que ingrese de manera ilícita podrá modificar las direcciones IP o las MAC para cambiar el enrutamiento de una manera sencilla, con leves conocimientos sobre redes y protocolos de comunicación. Este ataque se traduce directamente a robar información.

Ahora, este modo de actuar podría ser utilizado de otra manera. Si consideramos que sólo utilizamos un solo servidor de Google para este actuar, y que se tiene respuesta instantánea desde

ese servidor hacia el equipo local, es decir, Google está enviando solicitudes de vuelta a la dirección IP del notebook Dell sin supervisión ni conocimiento del usuario, se podría decir que si se tienen múltiples servidores y se automatizan para enviar constante miles de solicitudes a una sola dirección o dominio, colapsará el servicio en algún momento ya que no será capaz de soportar ni de interpretar o responder a tantas solicitudes a la vez, lo que se traduce directamente a un ataque de denegación de servicios o DDoS. Complementando métodos de vulneración se alcanza una amplia superficie de ataque para el atacante y la víctima, dándole dominio al ciber delincuente para que haga prácticamente lo que quiera dentro de una sola red local.

Nota: Se realizan algunos scripts de hacking ético en Python, además de documentación para guiar a los futuros usuarios de la plataforma y del laboratorio para que puedan realizar una mantención constante, así como un monitoreo general de la red cada cierto tiempo para no caer en ataques de ciber delincuentes. Estos archivos se adjuntarán con este informe en su versión final. Considerar que la mayoría de los scripts programados se realizaron en el sistema operativo Kali Linux, por lo que están desarrollados enfocados en sistemas operativos Linux.

Wireshark es un Sniffer de redes, es decir, permite olfatear e interpretar e interceptar los mensajes y solicitudes dentro de la red para poder tener un detalle completo del direccionamiento, el enrutamiento de mensajes, protocolos, información, etc. Se aprecia que la información viaja cifrada dependiendo del protocolo. Considerar que, si se tiene un ciber delincuente dentro de la red, o un malware instalado a la fuerza por un ciber ataque, este podría monitorear la información y las transacciones de datos entre dispositivos o servidores web, por ejemplo.

A pesar de esto, no tiene mucha relevancia ni es una verdadera amenaza mientras la información viaje cifrada por la red, ya que el ciber delincuente o el malware de espionaje no podrá comprender ni saber descifrar los datos. Sin embargo, si el atacante tiene las capacidades, conocimientos y herramientas, podría montar un punto de acceso falso, que imite al punto de acceso local, botarlo mediante un ataque de denegación de servicios como se explicó previamente y lograr que los distintos dispositivos de la red se conecten a él, por lo que podrá tener control total de la comunicación dentro de la red. Otra forma de proceder sería lograr que los distintos usuarios ingresen a un Evil Twin o un gemelo malvado de una página web que todos dentro de la red

utilicen, o que un usuario en específico use (en caso de un ataque dedicado, recordar la etapa de reconocimiento previa a un ataque), que no tenga un sistema de encriptación y que, al disponer del nombre de usuario y contraseña en un sistema de ingreso, la información viaje en texto plano, siendo fácilmente descifrada.

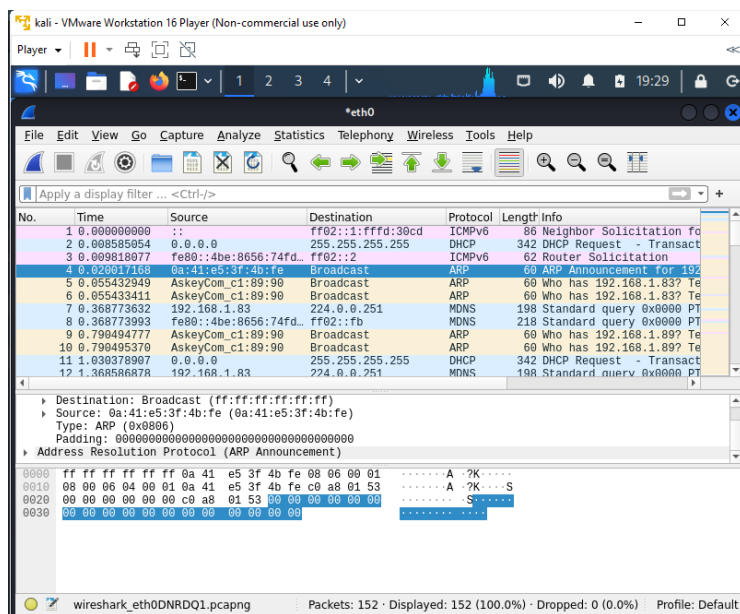


Figura 8.8 – Análisis de tráfico mediante Wireshark.

Gracias a Wireshark, se puede obtener información bastante importante con respecto a los mensajes dentro de una red. Por ejemplo, si se tiene un monitoreo extensivo mediante Wireshark, será posible determinar prácticamente todo el tráfico dentro de la red local, independiente de si está encriptado o no, los protocolos de comunicación, direccionamiento de la red, enrutamiento, entre muchas otras cosas.

Ahora, si se tiene mensajes del protocolo HTTP será posible obtener prácticamente toda la información de ese mensaje, ya que no viaja encriptado (como su forma segura HTTPS), entonces, será bastante peligroso si enviamos datos sensibles como contraseñas o claves de acceso mediante este protocolo, ya que cualquier persona que esté estudiando esta interceptación de mensajes, tendrá acceso a las contraseñas o claves como texto plano y no encriptados. Wireshark es una herramienta clave para los ataques Man in the Middle, puesto que forma parte de un sistema de interceptación de mensajes, independiente de su protocolo, lo que involucra una amenaza para

los usuarios que no tienen consentimiento de este tipo de ataques. Además, complementado con otro tipo de ataques como el filtrado de MAC o el envenenamiento ARP, será posible obtener información mucho más sencilla y valiosa para cualquier ciber delincuente.

De forma similar, existe el DNS Spoofing, el MAC Spoofing y el ARP Spoofing basados en el mismo procedimiento de ataque y de reconocimiento. Gracias a los comandos integrados en Kali Linux y ciertas funciones integradas en Python, es posible utilizar herramientas y funciones dedicadas para el reemplazo o para directamente camuflar las direcciones de cada uno de los dispositivos dentro de la red, ya que el procedimiento es bastante similar al detallado previamente. Además, es la base para un ataque Man in the Middle y para el uso de técnicas como el packet injection, ya que, al poder redireccionar la ruta de datos, es posible realizar muchas tareas con fines maliciosos o éticos, como en este proyecto.

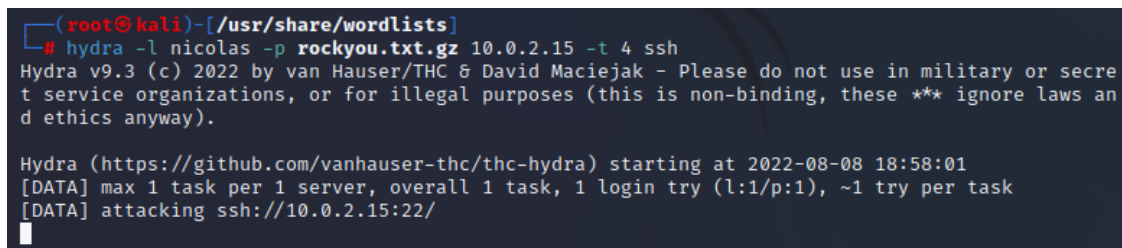
Así como el procedimiento para IP Spoofing, también se realiza un envenenamiento de ARP, para luego lograr un ataque Man in the Middle. Este script se realiza en Python, en el sistema operativo Kali Linux. Estos ataques traen consigo conocimientos prácticos que complementan la investigación teórica, lo que logra un conocimiento más sólido con respecto a seguridad web y seguridad local aplicado a este trabajo de título.

Se debe considerar y recalcar nuevamente, de que este tipo de estrategias que se realizan en este trabajo son exclusivamente de forma ética, es decir, se utilizan estrategias de defensa y de penetración y de hacking ético para fortalecer los conocimientos en redes y seguridad informática, con el fin de considerar la mayoría de amenazas más comunes para luego defender de la mejor manera la plataforma web, desde el nivel de red o del laboratorio físico hasta el nivel de intercambio de información y de mensajes dentro de la misma red del laboratorio.

Con el desarrollo de estas herramientas de forma práctica, es posible obtener conocimiento sólido sobre distintos vectores de ataque y estrategias de ataque, para así poder defender la aplicación web de la mejor manera. La experiencia práctica permite identificar las principales vulnerabilidades a nivel de laboratorio físico y de plataforma virtual, incluyendo aspectos de seguridad que deben fortalecerse a nivel de usuario como a nivel de programación.

Esto con el objetivo de crear una aplicación robusta tanto a nivel de código como a nivel de seguridad, creando un entorno seguro para todos los usuarios que requieren de la utilización de estos recursos de laboratorio.

Por ejemplo, para realizar ataques de fuerza bruta se utiliza una herramienta de auditoría de inicio de sesión que viene integrada en Kali Linux llamada Hydra. Esta herramienta permite a los investigadores y consultores de seguridad revelar lo sencillo que es obtener acceso no autorizado a un sistema de forma remota, al implementar de manera sencilla ataques de este tipo. Se utiliza la herramienta Hydra para realizar el ataque al formulario de la plataforma web, considerando que el método de consulta a la base de datos es POST. De esta forma, es posible encontrar ciertas vulnerabilidades a nivel de código o permisos en la aplicación, con el objetivo de corregirlos inmediatamente.



```
(root@kali)-[/usr/share/wordlists]
# hydra -l nicolas -p rockyou.txt.gz 10.0.2.15 -t 4 ssh
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-08 18:58:01
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://10.0.2.15:22/
```

Figura 8.9 – Ataque de fuerza bruta a un servidor mediante SSH.

Se propone una herramienta bastante útil basada en Python para encontrar vulnerabilidades con respecto a la inyección de código SQL malicioso en un sitio web. SQLMap tiene funciones para detectar y aprovechar las vulnerabilidades del código SQL de una aplicación para aprovechar estas brechas y explotarlas.

procedimiento implementado en este trabajo, ya que se utilizan funciones de Kali Linux orientadas a la ciber seguridad. Para escoger un exploit y el payload, se requiere de información previa sobre el sistema objetivo, como la versión del sistema operativo, servicios de red instalados, puertos abiertos, etc. Esta información puede ser obtenida mediante el escaneo de puertos con nmap y OS Fingerprint, por dar un ejemplo.

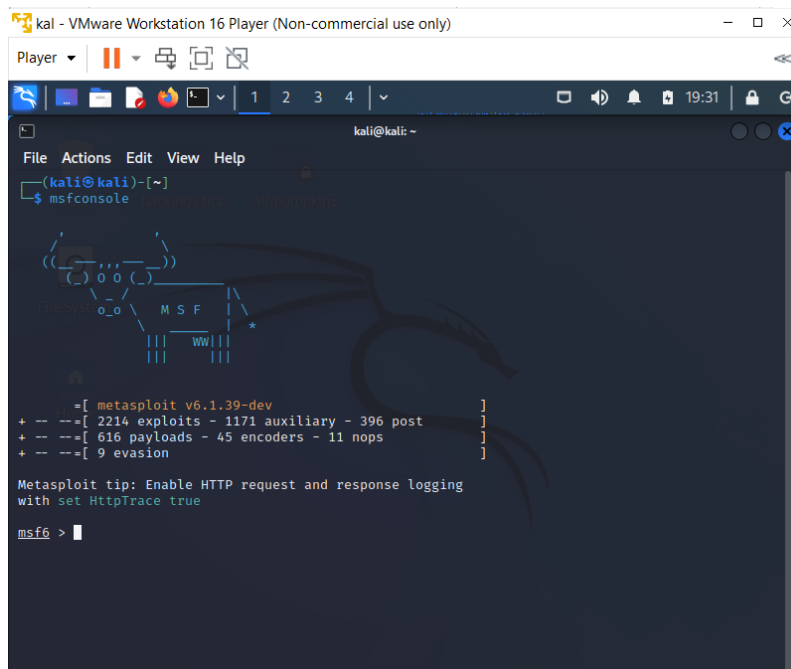


Figura 8.11 – Herramienta Metasploit.

Uno de los payload más potentes de Metasploit Framework es Meterpreter. Este payload permite obtener una gran cantidad de información sobre un objetivo comprometido en la vulneración, así como también permite manipular ciertas características del sistema objetivo. Cuenta con un intérprete que permite interactuar con el objetivo por medio de una serie de instrucciones directas fáciles de dominar y recordar, que sirven para llevar a cabo procesos post-explotación. La comunicación entre Meterpreter y la máquina remota es vía SSL, lo que quiere decir que la información intercambiada entre ambas máquinas viaja cifrada. Tiene muchas funcionalidades dedicado a la amenaza, como saber lo que ha digitado el usuario en su equipo, obteniendo fácilmente claves, usuarios, direcciones, mensajes, etc., es posible además consultar la cuenta de usuario, elevar privilegios, volver a la cuenta de usuario no privilegiada, migrar el proceso a otro proceso activo, gestionar tablas de enrutamiento del sistema vulnerado, comandos

básicos de consulta de sistemas basados en UNIX, abrir micrófono del equipo, capturar la pantalla, abrir la cámara, etc. Es por esto que este payload es de los más utilizados en ciber ataques, considerando todas las funcionalidades que tiene para el control y acceso a distintos recursos del equipo vulnerado.

Ahora, para implementar pruebas de penetración sólidas y así encontrar las distintas vulnerabilidades, se utiliza una herramienta fundamental dentro de la seguridad informática llamada Burp Suite, que permite realizar pruebas de seguridad de aplicaciones web. Entre sus principales funciones se encuentra el servidor proxy que permite inspeccionar y modificar el tráfico siendo un intermediario entre el navegador y la aplicación destino, que se definió previamente como ataque Man in the Middle, además tiene un escáner de vulnerabilidades que automatiza la detección de varios tipos de vulnerabilidades de aplicaciones web, un repetidor que se usa para modificar y reenviar solicitudes individuales al servidor, entre otras muchas funcionalidades.

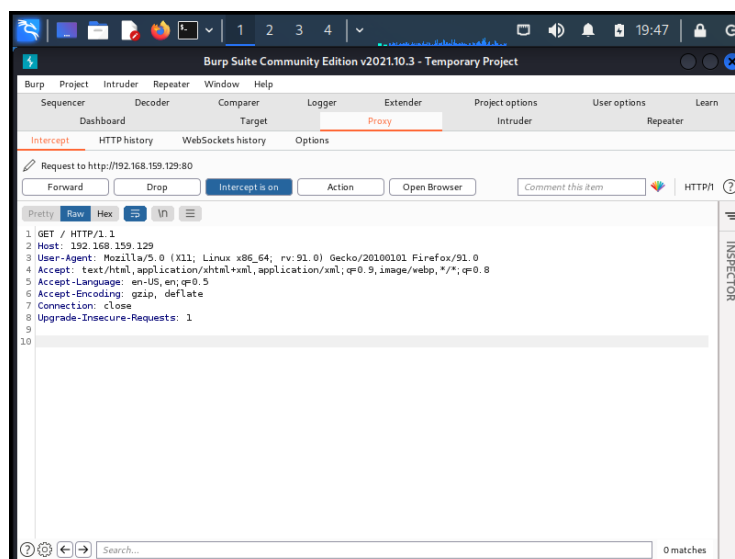


Figura 8.12 – Burp Suite.

Dentro de Kali Linux, se tiene integrado BeEF, que es una poderosa herramienta con capacidades para realizar captura de información, Ingeniería Social, descubrimiento de Red, inclusión de payloads de metasploit framework, tunneling, scanner XSS, persistencia, entre otras opciones más.

Además de estas herramientas ya mencionadas, existen varias más como whoami, hostname, ipconfig, netstat, etc., que entregan información importante del nombre de usuario del equipo, el huésped local, la configuración de los distintos dispositivos conectados a la red y las redes u ordenadores asociados, así como estadísticas básicas de las actividades de la red a dicho equipo, respectivamente. Estas herramientas se utilizan a nivel de comandos por consola para así poder obtener esta información, que es considerablemente valiosa para un usuario con conocimientos avanzados en redes y pruebas de penetración. Con el nombre de usuario de un ordenador, es posible ejecutar un ataque de fuerza bruta o de diccionario fácilmente, por ejemplo.

```

Microsoft Windows [Versión 10.0.19044.1826]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\FULLUNLOCK>netstat

Conexiones activas

Proto Dirección local Dirección remota Estado
TCP 127.0.0.1:27060 www:60931 ESTABLISHED
TCP 127.0.0.1:48080 www:49770 ESTABLISHED
TCP 127.0.0.1:48080 www:62142 ESTABLISHED
TCP 127.0.0.1:49669 www:49678 ESTABLISHED
TCP 127.0.0.1:49678 www:49669 ESTABLISHED
TCP 127.0.0.1:49770 www:48080 ESTABLISHED
TCP 127.0.0.1:50080 www:48080 TIME_WAIT
TCP 127.0.0.1:50082 www:48080 TIME_WAIT
TCP 127.0.0.1:50083 www:48080 TIME_WAIT
TCP 127.0.0.1:50084 www:48080 TIME_WAIT
TCP 127.0.0.1:50085 www:48080 TIME_WAIT
TCP 127.0.0.1:50087 www:48080 TIME_WAIT
TCP 127.0.0.1:50088 www:48080 TIME_WAIT
TCP 127.0.0.1:50089 www:48080 TIME_WAIT
TCP 127.0.0.1:50090 www:48080 TIME_WAIT
TCP 127.0.0.1:50091 www:48080 TIME_WAIT
TCP 127.0.0.1:50092 www:48080 TIME_WAIT
TCP 127.0.0.1:50094 www:48080 TIME_WAIT
TCP 127.0.0.1:50098 www:48080 TIME_WAIT
TCP 127.0.0.1:50100 www:48080 TIME_WAIT
TCP 127.0.0.1:50101 www:48080 TIME_WAIT
TCP 127.0.0.1:50103 www:48080 TIME_WAIT

```

Figura 8.13 – Herramienta de estadísticas de las actividades de red netstat.

8.3 Seguridad PHP

Para esta etapa se tiene la aplicación web SLD desarrollada y programada, pero sin ninguna capa de defensa más que las capas de seguridad definidas e implementadas a nivel de laboratorio como red local. Entonces, se deben plantear e integrar distintas estrategias a nivel de código para evitar ataques y amenazas de ciber delincuentes, o al menos, prevenirlos y amortiguarlos de la mejor forma. Como primera medida de seguridad a nivel de código, se debe considerar la integridad de la información, así como la protección de datos importantes como la contraseña, por ejemplo. Para esto se tiene una encriptación a nivel de código que logra una sencilla pero efectiva encriptación de contraseñas.

```

1  <?php
2
3  require 'database.php';
4
5  $message = '';
6
7  if (!empty($_POST['email']) && !empty($_POST['password'])) {
8      $sql = "INSERT INTO users (email, password) VALUES (:email, :password)";
9      $stmt = $conn->prepare($sql);
10     $stmt->bindParam(':email', $_POST['email']);
11     $password = password_hash($_POST['password'], PASSWORD_BCRYPT);
12     $stmt->bindParam(':password', $password);
13
14     if ($stmt->execute()) {
15         $message = 'Se ha creado un usuario correctamente';
16     } else {
17         $message = 'Ha habido un error al crear al usuario';
18     }
19 }
20 ?>




```





✓ Mostrando filas 0 - 0 (total de 1, La consulta tardó 0,0000 segundos.)

SELECT * FROM `users`

☐ Mostrar todo | Número de filas: 25 | Filtrar filas:






+ Opciones


| | id | email | password |
|---|----|--------------------|--|
| <input type="checkbox"/>  Editar  Copiar  Borrar | 7 | aerubio@ubiobio.cl | \$2y\$10\$IPrAhHFSzcAlctjrPnmfeu4jrnTsK6FgyIWW1aG132D... |

☐ Seleccionar todo | Para los elementos que están marcados:  Editar  Copiar  Borrar  Exportar

☐ Mostrar todo | Número de filas: 25 | Filtrar filas:

Operaciones sobre los resultados de la consulta

 Imprimir  Copiar al portapapeles  Exportar  Mostrar gráfico  Crear vista

 Guardar esta consulta en favoritos

Etiqueta: ☐ Permitir que todo usuario pueda acceder a este favorito

Figura 8.14 – Encriptación de contraseñas mediante PHP.

Como se observa en la Figura 8.14, en la línea 11 del código del script de Registro de usuarios, se utiliza la función `password_hash()`, que crea un hash de contraseña fuerte, a partir de una función matemática. Además, se observa que en la base de datos de la aplicación se tiene la contraseña encriptada y no almacenada como texto plano.

Ahora, como el ingreso a la plataforma SLD es mediante la autenticación y validación a partir de los registros y consultas hacia la base de datos, se debe considerar la defensa para uno de

los ataques más básicos contra plataformas web similares a la SLD, el Cross-Site Scripting o XSS. Este ataque ocurre cuando un ciber delincuente logra inyectar un script de JavaScript en la salida de la aplicación web vulnerada, de tal manera que ese script se ejecuta en el navegador del cliente (estudiante o administrador, en este caso). Esta amenaza se produce principalmente por validar incorrectamente los datos del usuario, ingresando información maliciosa en los campos de validación y autenticación de la persona y se suele inyectar mediante un formulario web o mediante un enlace alterado.

Para evitar este tipo de ataque tan básico, se debe hacer uso de `preg_match()`, una función que realiza una comparación con una expresión regular, de esta forma es posible filtrar los ingresos por teclado del formulario, como por ejemplo los caracteres especiales, que, si se utilizan con fines maliciosos, pueden de cierta forma vulnerar la base de datos y la plataforma, ya que a partir de estos caracteres es posible inyectar scripts maliciosos en un formulario, por ejemplo. Otra forma de evitar este tipo de ataque es quitando la etiqueta de cierre en los archivos PHP, de esta forma, no se podrá seguir ejecutando código externo de otros lenguajes en ese archivo, como scripts de JavaScript o de Python, por ejemplo.

```
12  
13     if(preg_match('/^[0-9a-zA-ZñÑ]+$/ ', $_POST['password'])){  
14
```

Figura 8.15 – Integración función `preg_match()`.

Otra posible amenaza, similar a la anterior, es el Cross-Site Request Forgeries o CSRF, que se produce cuando el atacante provoca que el usuario ejecute una acción de forma no intencionada en una aplicación en la que ha iniciado sesión. Cualquier tipo de acción que pueda realizar un usuario logeado en un sitio web, lo podrá realizar también el atacante, ya sea actualizar el perfil, añadir objetos a la cesta de compra, postear mensajes en un foro, etc. Este ataque se puede llevar a cabo con muy pocos conocimientos de hacking o de informática, ya que, un buen ciber delincuente, que busca vulnerabilidades en sitios web, podrá recurrir a las herramientas de desarrollador integradas en todos los navegadores, por lo que se deberá asegurar la información sensible de la aplicación para que no sea modificada externamente.

Para prevenir este ataque, se utilizan tokens, que son elementos encriptados. Es decir, es posible sustituir los datos sensibles de un usuario por un equivalente no sensible, creando un contenido encriptado que no pueda ser leído a simple vista como texto plano. Luego, al momento de desencriptarlo, es posible volver a tener esa información de forma clara y legible. Entonces, para integrar una nueva capa de seguridad y prevenir o amortiguar el ataque CSRF, se utiliza una función de PHP llamada md5(), que permite tomar ciertas variables en el campo del usuario (por ejemplo, nombre del usuario y password) y crear un token encriptado para la base de datos.

```

7  if (!empty($_POST['email']) && !empty($_POST['password'])) {
8      $token = md5($_POST['email'] + $_POST['password']);
9      $sql = "INSERT INTO users (email, password, token) VALUES (:email, :password, :token)";
10     $stmt = $conn->prepare($sql);
11     $stmt->bindParam(':email', $_POST['email']);
12     $password = password_hash($_POST['password'], PASSWORD_BCRYPT);
13     $stmt->bindParam(':password', $password);
14     $stmt->bindParam(':token', $token);

```

| id | email | password | token |
|----|--------------------|---|--------------------------------|
| 7 | aerubio@ubiobio.cl | \$2y\$10\$IPrAhHFSzcAlctjrPnmfeu4jrnTsK6FgyiWW1aG132D... | |
| 10 | alumno@ubiobio.cl | \$2y\$10\$m93qjPjKc5baKeOA9gpoYONOAAbWv3VCZ9DcNsyQUHK6... | cfd208495d565ef6e7dff9f98764da |

Figura 8.16 – Tokenización de información sensible del usuario.

En la Figura 8.16 se puede observar que en la línea 8 del script de Registro se integra un token gracias a la función md5() de PHP. En este caso, se toma el campo de email y el campo de password del formulario de registro de un nuevo usuario para poder crear esta nueva variable. Luego, se debe crear una nueva columna en la tabla de la base de datos, como se observa en la Figura 7.16, además de que en esa nueva columna se almacena el token encriptado.

Otro de los ataques muy comunes es el de SQL Injection, que se produce cuando el atacante intenta inyectar código SQL malicioso en la base de datos de la víctima, y fuerza a la base de datos a ejecutar esa sentencia. Este ataque puede realizar tareas como destruir las tablas de la base de datos o extraer información delicada como correos electrónicos o contraseñas con simplemente ingresar una sentencia SQL en los campos del formulario de ingreso o de registro.

Si no se protegen las urls de la aplicación, los formularios o el proceso de subir

información a la base de datos, es posible ser vulnerados por este tipo de ataques. Para esto, es fundamental filtrar ciertos caracteres o funcionalidades con los métodos y estrategias detalladas previamente, como `preg_match()`. De esta forma, es posible mitigar de sobre manera este tipo de vulnerabilidad.

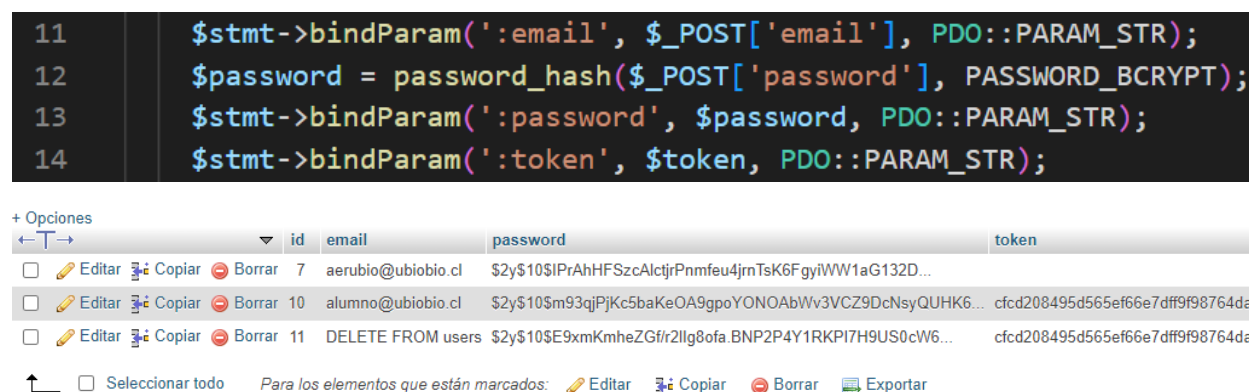


Figura 8.17 – Relación de parámetros.

En la Figura se observa la integración de la función `PDO::PARAM_STR`, que permite identificar que lo que se esté guardando en la base de datos sea una cadena de texto (o parámetros de tipo string) y que no sea un código de sentencia SQL o de cualquier otro lenguaje que tenga fines maliciosos. De esta forma, si se trata de inyectar código de cualquier lenguaje (en este caso SQL), el programa lo almacenará en la base de datos como texto o como un string.

Un ataque similar es el Code Injection, que permite al atacante inyectar código fuente en la aplicación de forma que pueda ser interpretado y ejecutado. Este código fuente se puede insertar directamente desde un elemento HTML de entrada, o la aplicación web puede ser manipulada para que sea cargado desde el sistema de archivos local o desde una fuente externa como una URL. Cuando la inyección de código se produce por la inclusión de un archivo externo se le denomina Remote File Inclusion o RFI, con el objetivo exclusivo de inyectar código malicioso en el sistema web.

Para esto, se debe realizar una lista blanca que compruebe los sitios o vistas exclusivas de la aplicación web, de manera que no se pueda acceder a otro enlace que no sea los que están programados y considerados dentro de la plataforma. Otra opción es eliminar la etiqueta de cerrado

en los archivos PHP, para que no se pueda inyectar código fuente malicioso.

El ataque de fuerza bruta también es uno de los ataques más conocidos en el mundo del hacking y pentesting y que se aplica a sistemas web. Consiste en probar todas las combinaciones de los datos de usuario o la mayoría de ellas gracias a una base de datos de más de 2 billones de contraseñas, comparando todas las posibilidades posibles e intentando ingresar por fuerza bruta a la aplicación. Este ataque es conocido también como búsqueda exhaustiva, utilizado netamente cuando no se tiene conocimientos de otros algoritmos de ataque disponibles. Esta técnica maliciosa es utilizada por hackers para descifrar contraseñas y así tener acceso a datos sensibles del usuario vulnerado. Para llevarlo a cabo, se utiliza un software con un algoritmo simple que realiza la sucesión de varias combinaciones de caracteres compuestos por dígitos, espacios y letras hasta una longitud máxima definida, con el fin de hacer coincidir un nombre de usuario con una contraseña y así desbloquear la llave para el ingreso a la plataforma.

Una de las posibles soluciones, es limitar el sistema de ingreso al SLD con ciertos intentos fallidos (tres intentos posibles, por ejemplo) y, cuando se supere ese límite de intentos, implementar un captcha, que corresponde a un test controlado por una máquina, en lugar de ser controlado por un humano. Mientras no se tenga un dominio para esta aplicación, no es posible integrar el captcha de Google, por lo que por el momento solamente es posible limitar el número de intentos disponibles para el ingreso.

Una posible solución es crear una nueva columna en la base de datos que considere los intentos que un usuario ha tratado de realizar para poder ingresar a la plataforma mediante fuerza bruta. La actualización de los intentos fallidos de ingreso se desarrolla a nivel de código.

+ Opciones

| | | | id | email | password | intentos_fallidos | token |
|--------------------------|--------|--------|--------|-------|--------------------|--|-------|
| <input type="checkbox"/> | Editar | Copiar | Borrar | 7 | aerubio@ubiobio.cl | \$2y\$10\$IPrAhHFSzcAlctjrPnmfeu4jrnTsK6FgyiWW1aG132D... | NULL |
| <input type="checkbox"/> | Editar | Copiar | Borrar | 10 | alumno@ubiobio.cl | \$2y\$10\$m93qjPjKc5baKeOA9gpoYONOA9Wv3VCZ9DcNsyQUHK6... | NULL |

↑

☐ Seleccionar todo

Para los elementos que están marcados:

Editar

Copiar

Borrar

Exportar

Figura 8.18 – Columna intentos_fallidos.

Otra forma de evitar estos ataques robotizados es encriptar la contraseña en PHP. Para esto se puede utilizar el método `crypt()` y `salt()`, que generarán un hash, además del método `password_hash()` que fue implementado en primera instancia en la aplicación del SLD. De esta forma, las contraseñas ya no se tratarán como texto plano en la base de datos, sino que se considerarán como una cadena de datos encriptados, dificultando la vulneración de la información sensible del usuario.

Gracias a todo este procedimiento a nivel de código, integración de funciones y herramientas de PHP para agregar capas de seguridad, se tiene una plataforma mucho más segura y amigable con la información y los datos de los usuarios. El objetivo siempre es cuidar la integridad y la disponibilidad de la información sensible de cada persona que vaya a interactuar con SLD. Se pretende desarrollar nuevas estrategias de ciber seguridad e integrar nuevas técnicas, herramientas y funciones de PHP o de otros lenguajes que permitan cuidar la integridad de los datos sensibles de los usuarios que están almacenados en la base de datos. Se propone una mejora continua en los aspectos de seguridad y una investigación constante sobre este tema para futuros proyectos o continuaciones de este trabajo.

9 CONCLUSIONES

Finalmente, concluida la etapa de diseño de este sistema de laboratorios a distancia o RemoteCIM, se obtiene una interfaz funcional para utilizar con propósitos educativos, donde, desde el punto de vista de programación e integración de los distintos sistemas y lenguajes de programación, proporciona un gran potencial de desarrollo para la realización de actividades prácticas en el laboratorio.

Hasta este punto, la plataforma desarrollada contempla comunicación y monitoreo remoto para la interacción y visualización de comportamiento y funcionamiento del brazo robótico de la manera más segura posible. La mejora continua y el constante aprendizaje y concientización con respecto a las vulnerabilidades digitales y de la información sensible son los mejores aliados a la hora de utilizar una plataforma de este tipo, ya que involucra tener que manipular datos comprometedores de los usuarios, tanto alumnos como docentes.

El presente proyecto trae consigo múltiples conocimientos con respecto a nuevas tecnologías que corresponden a la nueva revolución industrial a la que nos enfrentamos como estudiantes y futuros profesionales, además de la integración de múltiples herramientas tecnológicas, lenguajes de programación y tecnologías novedosas con respecto a la seguridad de la información.

A modo de experiencia, las metodologías que se implementan en cuanto a programación y ciber seguridad son aspectos muy relevantes para el desarrollo y la compilación de este tipo de sistemas y aplicaciones web. Se requiere un sistema con múltiples capas de seguridad para que sea confiable y genere un entorno respetable y seguro para con el usuario tanto como con la universidad. La investigación y comprensión de los distintos tipos de amenazas cibernéticas nos brinda nociones de las vulnerabilidades que pueden existir en nuestra interfaz, y así implementar posibles soluciones o estrategias existentes hasta la fecha para poder combatirlas.

La información debe ser correctamente cifrada y oculta mediante distintas técnicas de ciberseguridad y así no comprometer la integridad de nuestra información confidencial o sensible

de las personas que accedan a la interfaz o de algún cercano (familiar, pareja, amigos). Es por esta razón, que es indispensable la explicación y concientización sobre esta área, que no deja de ser fundamental al momento de navegar en la web, ya que siempre se está vulnerable dentro de la navegación, pero con ciertos conocimientos o técnicas adquiridas con el aprendizaje constante de nuevas tecnologías se van implementando y desarrollando mejoras en aspectos de seguridad.

10 REFERENCIAS

- [1] Á. Chirou, Seguridad Informática, Buenos Aires, 2021.
- [2] C. Cano, «LabsLand,» 16 Agosto 2022. [En línea]. Available: <https://labsland.com/es>.
- [3] S. M. Atilano Fernández-Pacheco, «Implementation of an Arduino Remote Laboratory with Raspberry Pi,» Madrid, 2019.
- [4] O. Oballe-Peinados, J. Castellanos Ramos, J. A. Sánchez Durán, R. Navas González y J. A. Hidalgo López, «Mejora de un laboratorio remoto de Electrónica Digital mediante el uso de una Raspberry Pi 4,» Málaga, 2022.
- [5] S. Martin, «Laboratorio remoto para experimentación sobre Internet de las Cosas,» de *Herramientas y recursos distribuidos en educación para la experimentación remota*, Madrid, 2022.
- [6] I. Calvo , E. Zulueta, U. Gangoiti y J. M. López, «Laboratorio remotos y virtuales en enseñanzas técnicas y científicas,» ResearchGate, Bilbao, 2009.
- [7] E. Brizuela, «daemchillan,» Dirección Educación, 1 Septiembre 2021. [En línea]. Available: <https://daemchillan.cl/2021/09/01/tecnologia-de-punta-para-clases-hibridas-en-chillan/>.
- [8] E. ROBOTEC, SCORBOT-ER Vplus User's Manual, 1996.
- [9] A. Barrientos, L. F. Peñin, C. Balaguer y R. Aracil, Fundamentos de Robótica, Madrid: Concepción Fernández Madrid, 1997.
- [10] P. Corke, Robotics, Vision and Control, Springer, 2017.
- [11] Á. Chirou, Seguridad Informática, Buenos Aires, 2021.