Desarrollo de un entorno de simulación como laboratorio de prácticas especializado en ciberseguridad

Jose García Mena

Grado de Ingeniería Informática

TFG del área Seguridad informática

Nombre Tutor/a de TFG

Jorge Miguel Moneo

Profesor/a responsable de la asignatura

Pau Perea Paños

Fecha Entrega

11/06/2024

Dedico este trabajo a todos los que han estado a mi lado durante estos últimos y duros años de mi vida por el apoyo que me han dado. En especial, a mi familia, que ha estado a mi lado en todo momento.

Por último, se lo dedico a quien se hubiera sentido más orgulloso en este momento si siguiera con nosotros...

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Desarrollo de un entorno de simulación como laboratorio de prácticas especializado en ciberseguridad*
Nombre del autor:	*Jose García Mena*
Nombre del director/a:	*Jorge Miguel Moneo*
Nombre del PRA:	*Pau Perea Paños*
Fecha de entrega (06/2024):	*06/2024*
Titulación o programa:	*Grado de Ingeniería Informática*
Área del Trabajo Final:	*Seguridad informática*
Idioma del trabajo:	*Castellano*
Palabras clave	*Ciberseguridad, Cloud, Docencia*

Resumen del Trabajo

La evolución tecnológica desde la aparición de la informática, que se ha acelerado en los últimos años, ha impulsado el desarrollo de soluciones cada vez más avanzadas. Actualmente, cualquier proyecto debe considerar el uso de nuevas tecnologías como un elemento estratégico y diferenciador. Por ello, en el ámbito de la educación, definir y aprovechar adecuadamente la tecnología permite desarrollar entornos de aprendizaje innovadores que fomentan la motivación y favorecen la adquisición de competencias del alumnado.

Por otro lado, esta misma evolución tecnológica ha acelerado el desarrollo del software, haciendo que la ciberseguridad se haya convertido en un elemento clave del panorama tecnológico actual. El creciente auge de esta área técnica ha propiciado un incremento en la demanda de especialistas en el sector y, con ello, de la oferta de formaciones especializadas.

El presente trabajo aborda todos estos conceptos mediante la creación de una simulación de red empresarial en un entorno de cloud privado, enfocada a la formación en ciberseguridad. El entorno creado ofrece al alumnado la visión global de un sistema productivo empresarial, donde poder desarrollar contenidos educativos especializados en ciberseguridad. El desarrollo realizado abarca desde la creación de la arquitectura del sistema hasta la propuesta de recursos didácticos que pueden ser desarrollados en él. Además, se ha implementado un procedimiento de automatización del despliegue del entorno que permite su replicación y la coexistencia de múltiples instancias del sistema de forma simultánea. Adicionalmente, se ha definido un proceso de gamificación basado en una competición de CTF, con el objetivo de aumentar la motivación del alumnado.

Abstract

Technological evolution since the advent of information technology, which has accelerated in recent years, has driven the development of increasingly advanced solutions. Currently, any project must consider the use of new technologies as a strategic and differentiating element. Therefore, in the field of education, defining and making the best use of technology makes it possible to develop innovative learning environments that foster motivation and promote the acquisition of student competencies.

On the other hand, this same technological evolution has accelerated software development, making cybersecurity a key element in today's technological landscape. The growing boom in this technical area has led to an increase in the demand for specialists in the sector and, with it, the offer of specialized training.

This paper addresses all these concepts through the creation of an enterprise network simulation in a private cloud environment, focused on cybersecurity training. The created environment offers students the global vision of a productive business system, where they can develop specialized educational content in cybersecurity. The development carried out ranges from the creation of the system architecture to the proposal of didactic resources that can be developed in it. In addition, an environment deployment automation procedure has been implemented that allows its replication and the coexistence of multiple instances of the system simultaneously. Additionally, a gamification process based on a CTF competition has been defined, with the aim of increasing student motivation.

Índice

Lista de figuras

Lista de tablas

1. Introducción

1.1. Contexto y justificación del trabajo

En la actualidad, el aumento del uso de nuevas tecnologías por parte de las empresas y la aparición de tendencias tecnológicas como la digitalización, el *big data* o la expansión de los servicios en la nube han generado una creciente demanda de profesionales especializados en tecnologías de la información, como señala el Informe sobre el futuro del empleo de 2023 (World Economic Forum, 2023). Este incremento en la demanda de técnicos especialistas ha creado un déficit de puestos de trabajo que ha propiciado un auge en el ámbito de la enseñanza en titulaciones para la especialización de puestos técnicos en todos los ámbitos de las TIC.

Una de las áreas que más expansión ha tenido en los últimos años ha sido la ciberseguridad, debido a la importancia que ha adquirido lo que podríamos considerar el activo más importante en las empresas actualmente, la información, y con ello la necesidad de protegerse frente a robos u otro tipo de amenazas. Los riesgos derivados de la expansión de las nuevas tecnologías mencionada, hace que la necesidad de profesionales altamente cualificados en esta área crezca de forma exponencial, tal y como señala la Asociación Española de Empresas de Consultoría en su artículo, la demanda de talento en ciberseguridad superará en un 50% a la oferta en 2024 (AEC - Asociación Española de Empresas de Consultoría, 2024).

La alta especialización que requieren las titulaciones en nuevas tecnologías y concretamente la formación en ciberseguridad hace necesario, o al menos altamente recomendable, permitir que los alumnos tengan una visión lo más realista posible de un sistema productivo. El éxito de la formación de estos titulados depende en gran medida de que sean capaces de poner en contexto los distintos componentes y tecnologías que forman parte de los sistemas productivos de las empresas.

Si bien es cierto que los currículos de las titulaciones oficiales establecen los requisitos formativos necesarios para cubrir en gran medida los conocimientos básicos que requiere los técnicos especialistas en nuevas tecnologías, el enfoque clásico de la docencia en la formación profesional encapsula o segmenta estos conocimientos de forma que no permite al alumnado tener una visión global de los sistemas y las relaciones que se establecen entre ellos en los entornos empresariales reales que se encontrarán al acceder al mercado laboral. Además, nos encontramos con una creciente demanda de formaciones específicas no regladas que capaciten a los técnicos en nuevas áreas tecnológicas derivadas de las tendencias actuales del mercado, como puede ser las tecnologías en la nube o la ciberseguridad.

La presente memoria pretende describir un enfoque docente innovador que permita la adaptación de la tecnología a los planes de estudio de las titulaciones, en particular, dentro del área de enseñanzas especializadas en ciberseguridad. Su desarrollo e implementación en un entorno educativo permitirá ofrecer una visión realista de los entornos empresariales por medio de la creación de una simulación de infraestructura de red corporativa orientada a la docencia en ciberseguridad. Este enfoque proporcionará una visión global de una arquitectura compleja basada en el diseño de una infraestructura empresarial y las

interrelaciones entre sus componentes, mejorando con ello de forma significativa la formación de los alumnos que cursen estas titulaciones.

Debido a que el entorno será un sistema compartido por numerosos alumnos con distintas capacidades, y dados los conocimientos y capacidades que adquiere el alumnado que se especializa en ciberseguridad, es esencial enfocar el desarrollo de la infraestructura y el diseño de los laboratorios teniendo en cuenta la aplicación de todas las medidas de seguridad necesarias para garantizar la integridad y la estabilidad del sistema en todo momento.

1.2. Objetivos del trabajo

El objetivo del presente trabajo es diseñar e implantar un laboratorio que simule la infraestructura de una empresa desde la perspectiva de la seguridad informática. Este laboratorio incluirá todos los componentes necesarios para la realización de una formación específica en ciberseguridad por medio del desarrollo de una simulación de infraestructura empresarial sobre un sistema de nube privada destinado a la realización de prácticas de un centro formativo. De esta manera, se ofrecerá al alumnado un enfoque con una visión global de un sistema de seguridad completo de una red empresarial.

El presente trabajo busca la realización de los siguientes objetivos:

- Desarrollar una arquitectura de sistema que cumpla con las especificaciones necesarias para crear un entorno simulado que ofrezca los recursos necesarios para abordar los contenidos didácticos establecidos en una formación orientada hacia la ciberseguridad.
- Preparar el software y los elementos necesarios para la automatización del despliegue de la simulación.
- Desarrollar la documentación necesaria para la utilización del sistema por parte de los usuarios.
- Desarrollar un proceso de gamificación de la infraestructura como elemento motivacional sobre el proceso de aprendizaje.
- Elaborar una memoria que documente el trabajo realizado para poder adaptarla posteriormente a otras titulaciones o especializaciones.

1.3. Impacto en sostenibilidad, ético-social y de diversidad

A continuación, se detallan los puntos relevantes que ofrece el desarrollo del presente trabajo con respecto al compromiso ético y global definido como competencia transversal en los másteres y grados de la UOC (*Doñate*, 2020). Esta competencia queda definida de la siguiente forma:

> «Actuar de manera honesta, ética, sostenible, socialmente responsable y respetuosa con los derechos humanos y la diversidad, tanto en la práctica académica como en la profesional»

Con respecto a la sostenibilidad, el desarrollo de un entorno de nube privada como laboratorio de prácticas en un centro docente como el propuesto en este documento, contribuirá a la sostenibilidad ambiental y con ello tiene una relación directa con los ODS7

y ODS13, debido a la eficiencia que aporta este tipo de infraestructuras si se establece una correcta planificación de la adquisición y uso de los recursos informáticos, y energéticos.

La centralización de los recursos proporcionados a los estudiantes en una infraestructura compartida reduce la necesidad de inversión en la actualización del hardware de equipos físicos de trabajo de los alumnos. Esto es debido a que no será necesario el cumplimiento de las características requeridas para desplegar toda la infraestructura en un entorno local. Aunque no es objeto de estudio en este trabajo, cabe destacar que la reducción de requisitos de los equipos de trabajo de los estudiantes podría incluso llevar a la sustitución completa de sus puntos de conexión al sistema por terminales ligeros con un bajo consumo de energía y una vida útil mucho mayor. Todo el procesamiento necesario para el desarrollo de los contenidos se centralizaría en el sistema de nube.

Otra característica de los sistemas de *cloud* privado, que tampoco es objeto de estudio en este trabajo, pero cabe destacar, es que, debido a la naturaleza del sistema, su gestión se realiza siempre por mecanismos de acceso remoto. Esto posibilita, mediante el desarrollo de los servicios adecuados que garanticen en todo momento el acceso de forma segura al sistema, que se pueda impulsar la formación online, evitando desplazamientos de los usuarios y con ello reduciendo las emisiones derivadas de estos.

Por otro lado, con respecto al compromiso ético-social, el enfoque didáctico de la ciberseguridad que se abordará en este trabajo busca, además de desarrollar un entorno didáctico innovador y adecuado para la realización de las actividades propuestas, fomentar el conocimiento de los estudiantes en el área y con ello ofrecerles una visión responsable alineada con el ODS16, que promueve las sociedades justas, pacíficas e inclusivas. De forma transversal, es necesario que la formación incluya un punto de vista ético y responsable del uso de los recursos y la información. El alumnado que haga uso de la infraestructura debe ser consciente de las capacidades que va a adquirir y los riesgos que conlleva el mal uso de ellas. Esto propiciará que los profesionales que finalicen la docencia adquieran una visión crítica y asimilen los conocimientos necesarios para afrontar los retos globales actuales en materia de ciberseguridad y tratamiento de la información.

Finalmente, cabe subrayar que el trabajo propuesto se desarrolla para un entorno educativo, lo que favorece los aspectos referentes a la diversidad y la tolerancia, que son abordados en el ODS10, y, que son intrínsecos en la educación actual, concienciada significativamente con los valores que representa.

1.4. Enfoque y método seguido

El enfoque que se establecerá para el desarrollo del laboratorio se basará en la adaptación de un sistema de nube privada disponible como laboratorio de prácticas de un centro educativo. Utilizando los recursos que proporciona este sistema, se pretende integrar en una simulación de una red todos los elementos necesarios para abordar adecuadamente contenidos didácticos sobre seguridad, cubriendo así los requisitos tecnológicos para el desarrollo práctico de una titulación especializada en ciberseguridad.

Como se ha comentado al inicio, el punto de partida es un centro docente el cual ya ofrece un entorno de *cloud* consolidado de forma adecuada para la realización de prácticas del alumnado. Además, este centro también ofrece una formación específica en

ciberseguridad que dispone de una serie de módulos didácticos que servirán como referente de los contenidos específico en ciberseguridad que serán incluidos en el sistema.

La experiencia previa adquirida en los ámbitos mencionados, la madurez del sistema y la consolidación de los contenidos didácticos respalda la estrategia de adaptación de recursos y contenidos para realizar el desarrollo y la evolución del sistema que se propone en este proyecto. La experiencia previa en todos los ámbitos ayudará de forma significativa al desarrollo de las mejoras que se propongan ahora y a la creación de un sistema adaptable a futuras implantaciones, cambios o revisiones del contenido.

Con respecto a la metodología que se adoptará para el desarrollo del entorno de simulación como laboratorio de prácticas especializado en ciberseguridad, objeto de este trabajo, se basará en un enfoque en cascada o *waterfall*. Se selecciona esta metodología debido a que inicialmente disponemos de los requisitos y el alcance del sistema a implementar.

A continuación, se detallan las distintas fases adoptadas para el desarrollo del trabajo:

0. Definición de la propuesta y plan de trabajo.
1. Análisis y toma de requisitos. En esta fase se hará una definición del sistema actual y los requisitos, tanto didácticos como tecnológicos para el desarrollo de los contenidos.
2. Diseño de la arquitectura de la simulación.
3. Implementación del sistema y desarrollo de los contenidos didácticos.
4. Resultados, documentación del sistema y del proceso de automatización.
5. Conclusiones. Revisión del trabajo realizado, desarrollo de conclusiones y propuestas de mejora o cambios a futuro.

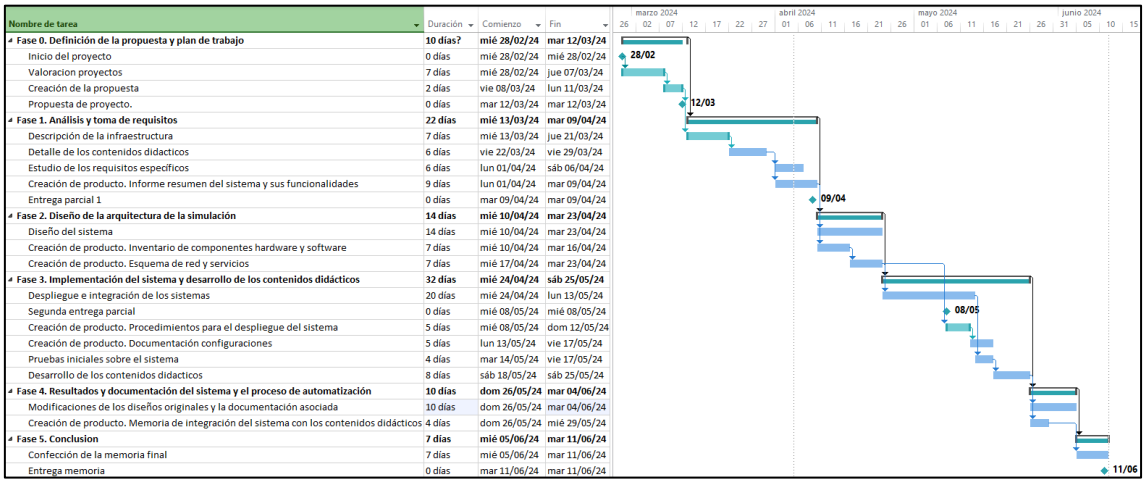
1.5. Planificación del Trabajo

A nivel general los recursos necesarios para la realización del proyecto se obtendrán directamente del entorno de nube privada para el cual se va a desarrollar el proyecto. Por otro lado, los contenidos didácticos en ciberseguridad que se utilizarán durante el desarrollo se basarán en una adaptación de una serie de contenidos protegidos por derechos de autor por medio de una generalización de los mismos para que puedan ser utilizados en el presente trabajo. Esta adaptación permitirá reutilizar los contenidos de forma general adaptando la estructura del sistema a los contenidos específicos de cualquier formación en ciberseguridad que disponga de los recursos necesarios para desplegar el sistema.

Con respecto a la automatización planificada del proceso de despliegue de la nueva infraestructura, se valora la posibilidad de utilizar software libre que permita la implementación de infraestructura como código. Este recurso es de libre acceso, aunque de momento no se ha implantado en el sistema actual debido a la simplicidad de las tareas que se realizan actualmente en él.

A continuación, se aborda la planificación del trabajo definida, adaptán. Para su desarrollo se han adaptado como fases del proyecto las fases estándar de la metodología de gestión de proyectos definida anteriormente. Por lo tanto, como se puede observar en la figura 1, el diagrama de Gantt del proyecto se desarrolla en base a la adaptación de las fases definidas

en las metodologías de gestión de proyectos en cascada. A continuación, se puede observar la planificación del trabajo definida.



Nombre de tarea	Duración	Comienzo	Fin
Fase 0. Definición de la propuesta y plan de trabajo	**10 días?**	**mié 28/02/24**	**mar 12/03/24**
Inicio del proyecto	0 días	mié 28/02/24	mié 28/02/24
Valoracion proyectos	7 días	mié 28/02/24	jue 07/03/24
Creación de la propuesta	2 días	vie 08/03/24	lun 11/03/24
Propuesta de proyecto.	0 días	mar 12/03/24	mar 12/03/24
Fase 1. Análisis y toma de requisitos	**22 días**	**mié 13/03/24**	**mar 09/04/24**
Descripción de la infraestructura	7 días	mié 13/03/24	jue 21/03/24
Detalle de los contenidos didacticos	6 días	vie 22/03/24	vie 29/03/24
Estudio de los requisitos específicos	6 días	lun 01/04/24	sáb 06/04/24
Creación de producto. Informe resumen del sistema y sus funcionalidades	9 días	lun 01/04/24	mar 09/04/24
Entrega parcial 1	0 días	mar 09/04/24	mar 09/04/24
Fase 2. Diseño de la arquitectura de la simulación	**14 días**	**mié 10/04/24**	**mar 23/04/24**
Diseño del sistema	14 días	mié 10/04/24	mar 23/04/24
Creación de producto. Inventario de componentes hardware y software	7 días	mié 10/04/24	mar 16/04/24
Creación de producto. Esquema de red y servicios	7 días	mié 17/04/24	mar 23/04/24
Fase 3. Implementación del sistema y desarrollo de los contenidos didácticos	**32 días**	**mié 24/04/24**	**sáb 25/05/24**
Despliegue e integración de los sistemas	20 días	mié 24/04/24	lun 13/05/24
Segunda entrega parcial	0 días	mié 08/05/24	mié 08/05/24
Creación de producto. Procedimientos para el despliegue del sistema	5 días	mié 08/05/24	dom 12/05/24
Creación de producto. Documentación configuraciones	5 días	lun 13/05/24	vie 17/05/24
Pruebas iniciales sobre el sistema	4 días	mar 14/05/24	vie 17/05/24
Desarrollo de los contenidos didacticos	8 días	sáb 18/05/24	sáb 25/05/24
Fase 4. Resultados y documentación del sistema y el proceso de automatización	**10 días**	**dom 26/05/24**	**mar 04/06/24**
Modificaciones de los diseños originales y la documentación asociada	10 días	dom 26/05/24	mar 04/06/24
Creación de producto. Memoria de integración del sistema con los contenidos didácticos	4 días	dom 26/05/24	mié 29/05/24
Fase 5. Conclusion	**7 días**	**mié 05/06/24**	**mar 11/06/24**
Confección de la memoria final	7 días	mié 05/06/24	mar 11/06/24
Entrega memoria	0 días	mar 11/06/24	mar 11/06/24

Figura 1. Diagrama de Gantt con la planificación de las tareas de proyecto

Según se observa en el diagrama, cada fase del proyecto contempla una serie de actividades y un conjunto de entregables que se deben llevar a cabo para completarlas. Por su otro lado, el desarrollo de los capítulos de la memoria es acorde a la planificación definida, por lo que, la evolución del proyecto servirá como base para desarrollar la memoria.

Por otro lado, se han establecido como hitos del proyecto las entregas de las pruebas de evaluación continua (PEC) de la asignatura. Estas entregas llevarán asociada una evolución correspondiente del proyecto y un conjunto de entregables que servirán como documentación asociada al sistema y la arquitectura resultante. A continuación, se puede ver el detalle de las entregas propuestas:

- Propuesta de proyecto. 12/03/2024
  - Desarrollo de la propuesta de proyecto.
  - Desarrollo del capítulo 1 Introducción de la memoria.
  - Desarrollo del capítulo 2 Estado del arte de la memoria.
- Primera entrega parcial. 09/04/2024
  - Desarrollo del capítulo 3 Análisis del sistema actual y los contenidos.
  - Desarrollo del capítulo 4 Descripción de los contenidos didácticos.
  - Desarrollo del capítulo 5 Definición de requisitos del nuevo sistema.
  - Entrega “Informe resumen de requisitos y funcionalidades del sistema”
- Segunda entrega parcial. 08/05/2024
  - Desarrollo del capítulo 6 Diseño del sistema.
  - Entrega “Informe resumen del diseño de la arquitectura de la solución”
  - Entrega “Esquemas de red y de la arquitectura de servicios.”
- Entrega de la memoria. 11/06/2024
  - Desarrollo del capítulo 7 “Implementación del sistema”
  - Desarrollo del capítulo 8 “Resultados”
  - Desarrollo del capítulo 9 “Conclusiones”
  - Entrega “Procedimiento para el despliegue del sistema”

- Entrega "Documentación de las configuraciones de los distintos elementos que componen la simulación"
- Entrega "Descripción de los contenidos didácticos y propuesta de prácticas"
- Entrega "Documento con la definición del proceso de gamificación"

Con respecto a las particularidades de la planificación, es importante destacar que se da por iniciado el proyecto el pasado día 28 de febrero con el inicio de las tareas referentes a la valoración de opciones y el desarrollo inicial de esta documentación. Por otro lado, la planificación finaliza el 11 de junio con la entrega de la última PEC asociada a la asignatura.

La mayoría de las actividades detalladas se realizarán de forma secuencial, a excepción del desarrollo de los entregables que se harán en paralelo a otras actividades. Esto es debido a dos motivos, en primer lugar, los entregables o productos finales del proyecto, documentarán o se basarán en el trabajo realizado en otras tareas y por lo tanto son susceptibles de ser llevados en paralelo a las tareas para mantener la información actualizada. En segundo lugar, este proyecto será realizado exclusivamente por mí, por lo que los recursos humanos asociados a su desarrollo establecen el carácter secuencial de su planificación.

1.6. Breve sumario de productos obtenidos

Al concluir el proyecto se dispondrá del diseño de un laboratorio global especializado que simulará una red empresarial destinada a la formación en ciberseguridad. Este diseño estará formado por un conjunto de documentos que describirán la arquitectura del sistema simulado y permitirán su implantación en un entorno de *cloud* privado.

A continuación, se detallan de forma general los documentos que se obtendrán al finalizar el trabajo:

- Informe resumen de requisitos y funcionalidades del sistema.
- Informe resumen del diseño de la arquitectura de la solución.
- Esquemas de red y de la arquitectura de servicios.
- Procedimientos para la automatización del despliegue del sistema.
- Documentación de las configuraciones de los distintos elementos que componen la simulación.
- Descripción de los contenidos didácticos y las prácticas asociadas.
- Documento con la definición del proceso de gamificación.

Al finalizar el desarrollo del sistema se desplegará la simulación de la infraestructura basándose en la documentación generada. El objetivo de este despliegue será la realización de un conjunto de pruebas que permitan determinar si los resultados obtenidos cumplen con los requisitos establecidos para el desarrollo de las actividades propuestas. Esta última fase del proyecto permitirá ofrecer un informe con los resultados y las conclusiones sobre el desarrollo propuesto en este trabajo.

1.7. Breve descripción de los otros capítulos de la memoria

A continuación, se ofrece una breve descripción de los capítulos que componen esta memoria y serán desarrollados en profundidad para documentar el trabajo realizado en este trabajo.

- Capítulo 2. Estado del arte: Se abordan como referencia sistemas o proyectos que muestran similitudes y que ayudan a enfocar los objetivos de este trabajo, además de servir como base de conocimiento para el desarrollo que se propone.
- Capítulo 3. Análisis del sistema actual y los contenidos: Se estudia y analiza el sistema y las capacidades que ofrece, así como los contenidos didácticos sobre ciberseguridad que se abordarán durante el desarrollo de este trabajo.
- Capítulo 4. Definición de requisitos del nuevo sistema: Se realizará un análisis de los requisitos necesarios para la implementación de la simulación que permita desarrollar los contenidos.
- Capítulo 5. Descripción de los contenidos didácticos: Se realizará la descripción de los contenidos didácticos que serán abordados en el curso de ciberseguridad.
- Capítulo 6. Diseño del sistema. Se desarrollan los esquemas de red y servicios, así como el detalle de los elementos que los componen.
- Capítulo 7. Implementación del sistema: Se detallan los pasos necesarios para la implementación, el proceso de automatización y la gamificación del sistema.
- Capítulo 8. Resultados. Se analizarán y evaluarán el sistema obtenido y su capacidad para ofrecer un entorno adecuado para el desarrollo del aprendizaje en ciberseguridad.
- Capítulo 9. Conclusiones. Reflexión sobre el trabajo realizado y la consecución de los objetivos planteados, así como de posibles problemas encontrados o vías de mejora a futuro que pueden desarrollarse.
- Capítulo 10. Glosario. Definición de acrónimos y términos que se utilizan en el presente documento.
- Capítulo 11. Bibliografía. Listado de referencias utilizadas durante el desarrollo de la memoria y la documentación asociada al sistema.

2. Estado del arte

La evolución tecnológica vivida desde la aparición de la informática, que se ha acelerado en los últimos años, se ha convertido en un elemento estratégico de cualquier proyecto relacionado con las tecnologías de la información y la comunicación (TIC). Los continuos avances en hardware, software y metodologías de implementación tienen una importancia clave en el diseño y desarrollo de nuevas soluciones tecnológicas. Por otro lado, este desarrollo tecnológico enfocado en los procesos de aprendizaje favorece la aparición de nuevas tendencias educativas, que abren la posibilidad al desarrollo de elementos novedosos e innovadores para hacer más atractivos los procesos de formación y con ello el proceso de adquisición de nuevas competencias.

En el contexto de este trabajo, que aborda la implementación de un entorno de *cloud* privado como plataforma de prácticas para el desarrollo de formación en ciberseguridad, es necesario entender la influencia de la evolución tecnológica de los últimos años en las áreas que servirán de base para este sistema.

Como punto de partida, es necesario mencionar la evolución del hardware, que ha seguido estrictamente la ley formulada por Gordon Moore en 1965 (Moore, 1965), que anticipaba que la capacidad de integración de los chips se duplicaría cada 18 meses y que hoy en día sigue vigente. Este aumento de la capacidad de integración de los circuitos, gracias a las mejoras en los procesos de litografía, que en la actualidad se encuentran en 4nm, permite el aumento continuado de la capacidad de procesamiento y almacenamiento. Este aumento de la capacidad de proceso ha impulsado el desarrollo de tecnologías que permitan compartir los recursos y con ello aprovechar al máximo la creciente capacidad de cómputo.

Una de estas tecnologías es la virtualización, que surgió en la década de 1960 como resultado de los esfuerzos de IBM para mejorar la segmentación de los *mainframes* y optimizar la utilización de la CPU (Creasy, 1981), pero que fue popularizada a principios de este siglo, con la irrupción en el panorama tecnológico de Vmware (Bugnion et al., 2012). Esta empresa, fundada en 1998 y que a día de hoy sigue siendo una de las empresas de referencia en el sector, revolucionó la virtualización y la popularizó en los centros de datos y como software de consumo. La clave de esta evolución fue el cambio de paradigma que supuso esta tecnología, permitiendo abstraer a los sistemas operativos del hardware físico donde se ejecutaban mediante una capa de hardware virtual que facilita la compartición de recursos y mejora la tolerancia a fallos (Rosenblum y Garfinkel, 2005).

Esta capacidad de abstracción sobre el hardware, aportada por la virtualización, permitió que los sistemas productivos de las empresas funcionaran sobre una capa de recursos (pool) compuesta por agrupaciones de servidores (clústeres) que ofrecían la capacidad de procesamiento y memoria. Por otro lado, el almacenamiento de los archivos de las máquinas virtuales correspondientes a estos sistemas productivos, entre ellos los sistemas de ficheros, quedaron reducidos a simples archivos que se guardaban en dispositivos especializados con alta tolerancia a fallos. Este nivel de abstracción se convirtió en un elemento clave en el panorama tecnológico del momento, ya que permitía compartir de forma eficiente y segura los recursos del hardware físico entre distintos sistemas virtuales.

Con la virtualización como nuevo paradigma, la industria pudo centrar su atención en el desarrollo de nuevas tecnologías basadas totalmente en el software. Estas tecnologías se enfocaron en la automatización de los procesos de despliegue y administración de los entornos virtualizados. Entre las muchas tecnologías surgidas a raíz de este momento, la nube fue sin duda el siguiente gran avance tecnológico. El nacimiento de la nube aportó un nuevo nivel de abstracción sobre las plataformas de virtualización, en este caso, sobre las tareas de gestión de los recursos virtuales (Armbrust et al., 2010). Una de las grandes ventajas que aporta la nube es su capacidad de gestión de recursos, la cual permite mejorar considerablemente la eficiencia de las tareas de gestión de infraestructuras. Asimismo, la nube facilita el desarrollo continuo de herramientas para la automatización de procesos de implantación y despliegue.

Todas estas tecnologías hacen de los sistemas de *cloud* un elemento clave en el panorama tecnológico actual y que, como no puede ser de otra manera, enfocadas en los procesos de enseñanza-aprendizaje, ofrecen unas posibilidades innegables a la hora de crear entornos adecuados para el aprendizaje en cualquier ámbito relacionado con las TIC. Revisando la literatura encontramos innumerables trabajos de final de grado y tesis que presentan diferentes enfoques sobre la implementación de un *cloud* privado como laboratorio de prácticas para realizar procesos de formación. Un buen ejemplo de las posibilidades que ofrecen estos entornos en los procesos de aprendizaje lo encontramos en el trabajo de fin de grado titulado "Explotación de OpenNebula como plataforma *cloud* IaaS para la docencia" (Sola Caraballo, 2015), que analiza las posibilidades de Opennebula (OpenNebula Systems, 2008), un proyecto de *cloud* privado basado en código abierto como plataforma para el desarrollo y despliegue de recursos informáticos orientados a la docencia.

Buscando un enfoque más específico y con mayor similitud a las características del presente trabajo, encontramos la tesis "Reingeniería del Laboratorio de Seguridad Informática: análisis, diseño e implementación de un Cyber Range" (Gallardo y Guerrero, 2021). Esta tesis analiza las posibilidades de un entorno como el planteado en esta memoria, en concreto desarrolla la idea de utilizar tecnologías de *cloud* y herramientas de infraestructura como código (*IaC*) para el desarrollo de entornos y tecnologías de *Cyber range*. Esta tesis ofrece una visión más próxima a la ciberseguridad y por lo tanto más cercana a los objetivos que se buscan en este TFG.

Como vemos, el momento tecnológico actual ofrece innumerables posibilidades en el ámbito de la educación, favoreciendo el desarrollo de nuevas e innovadoras metodologías que promuevan una experiencia de aprendizaje más atractiva y efectiva. Entre estas tendencias podemos destacar la gamificación como una de las que ha ganado relevancia en los últimos años. Esta metodología que consiste en la integración de mecánicas y elementos de juegos en contextos educativos (Deterding et al., 2011) permite aumentar la motivación y participación de los estudiantes en los procesos de aprendizaje, y con ello mejorar la adquisición de competencias.

Basándonos en el conocimiento y las conclusiones de los documentos y estudios vistos hasta ahora, las posibilidades que ofrece el desarrollo de una simulación de infraestructura empresarial completa como laboratorio de prácticas enfocado en la ciberseguridad, son innegables. Además, según hemos visto, si se añaden las características adecuadas que permitan que el sistema sea replicable, lo cual es necesario para su reutilización en un

curso de formación, ofrece una gran versatilidad y mejora su aplicabilidad en un entorno real. Finalmente, según se ha comentado, la inclusión de un proceso de gamificación en un entorno como el propuesto, permitirá aumentar la motivación y el compromiso de los estudiantes, haciendo que el aprendizaje sea más interactivo y efectivo.

3. Análisis del sistema actual y los contenidos

3.1 Descripción de la infraestructura corporativa

La siguiente descripción detalla la infraestructura de una red corporativa que incluye el diseño adecuado para permitir el desarrollo de un servicio de *cloud* privado como laboratorio de prácticas en un entorno educativo como el tratado en el presente trabajo. Este diseño debe ofrecer las máximas garantías de seguridad para proteger los recursos garantizando el acceso y la seguridad de la información para todos los usuarios independientemente del rol o la actividad que realicen en la organización. La arquitectura de la red y del sistema se ha diseñado aplicando la seguridad en todos los niveles con el objetivo de proteger y aislar los distintos ámbitos o áreas empresariales de la organización.

En la figura 2, vemos el esquema lógico de la arquitectura de la red de la organización. Su diseño estructura el sistema creando una división en distintas zonas a partir de un firewall empresarial que es el núcleo central de la red. Este dispositivo es un firewall de capa 7 (*NGFW*) que aporta todas las capacidades y funcionalidades de seguridad que ofrecen este tipo de dispositivos en la actualidad.

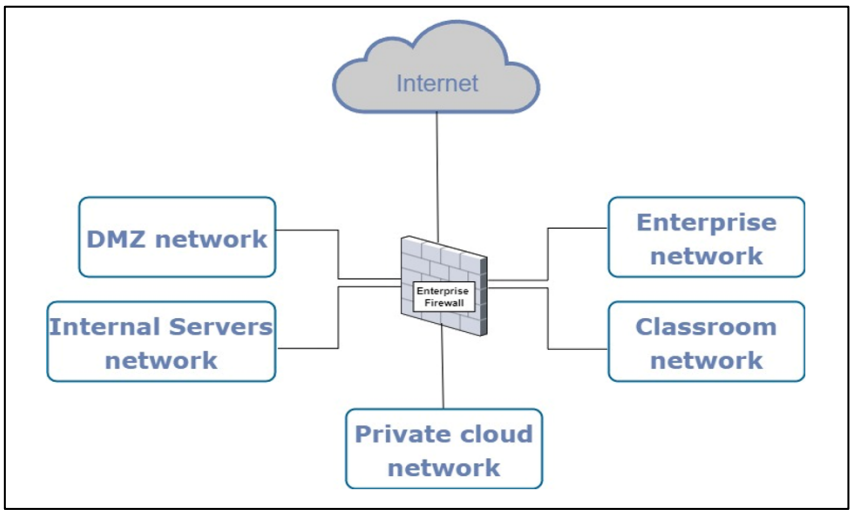


Figura 2. Esquema lógico de la arquitectura de la red de la empresa

Este diseño debe ser complementado con una segmentación física acorde en las capas inferiores de la arquitectura vista en la figura 2. Esta segmentación se realiza mediante switches y routers independientes en las distintas zonas que se establecen a partir del firewall. Esta configuración consigue que cada una de las zonas sea totalmente independiente y que el tráfico entre ellas quede siempre filtrado por el firewall.

Para garantizar la seguridad en toda la red corporativa, se deben implementar medidas de seguridad adicionales. El sistema debe estar diseñado bajo la premisa de que la seguridad no se basa en un único elemento dentro de una red o sistema, sino que es un concepto transversal que debe estar presente en todos los elementos que formen parte del diseño de un sistema. Por lo tanto, la arquitectura debe complementar todo un conjunto de medidas de seguridad en todas las capas que la componen para garantizar en todo momento el acceso seguro a todos los servicios ofrecidos por la red. Esto permite que los usuarios desarrollen sus actividades con garantías y de forma independiente a las actividades realizadas en otras zonas o áreas de la organización.

3.2 Arquitectura de la zona del *cloud* privado

La arquitectura de red del *cloud* privado de la organización, representada en la figura 3, refleja la misma filosofía de seguridad y segmentación observada en la red corporativa. Todo el tráfico generado en esta zona es filtrado por un firewall interno.

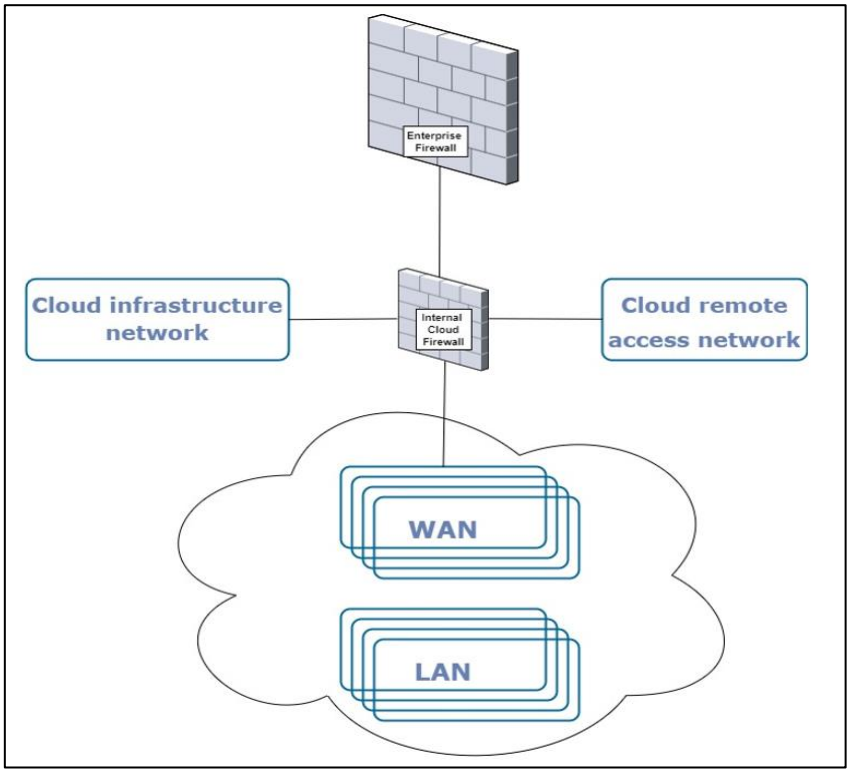


Figura 3. Esquema lógico de la arquitectura del *cloud* privado

Siguiendo los principios de diseño establecido para la red corporativa, la zona del *cloud* privado, queda segmentada del resto de servicios y componentes de la arquitectura de la organización tanto a nivel de red, como a nivel de infraestructura utilizando para su implementación dispositivos hardware totalmente independientes. Todos los dispositivos que integran el sistema están aislados de forma que la única comunicación con la red corporativa es a través de la conexión con el firewall central de la red.

Por su parte, la zona del *cloud* también queda segmentada en múltiples zonas de seguridad con niveles de criticidad diferenciados. Es importante destacar que en este caso la segmentación se realiza a nivel lógico ya que físicamente todos los dispositivos que componen esta zona son compartidos entre los distintos sistemas virtuales que implementan la arquitectura del sistema, la red del *cloud* y los sistemas que ofrece.

- **Zona navegación**. Para la navegación y el acceso a los servicios corporativos se utiliza una de las zonas del firewall interno que conecta el servicio de *cloud* privado con el firewall central de la red.
- **Zona infraestructura**. La zona de la infraestructura del *cloud* alberga los distintos hosts que ofrecen el pool de recursos que utiliza la infraestructura. Esta zona es la única con dispositivos físicos (hosts). El acceso a esta zona queda reservado únicamente a los servicios que implementan el sistema de nube privada.

- **Zona acceso remoto**. La zona de la red para el acceso remoto al *cloud*, ofrece varios servicios de conexión remota (VPN, Microsoft RDWeb) para que los alumnos puedan acceder a los recursos ofrecidos por el sistema. Esta zona tiene limitado restringido el acceso solo a los recursos ofrecidos por el entorno de *cloud*, sin permitir el acceso a Internet o a cualquier otro servicio corporativo.
- **Zonas *cloud***. Las zonas desplegadas en el servicio de *cloud* privado quedan implementadas por medio de un conjunto de VLANs preconfiguradas y asociadas a usuarios o grupo de usuarios dentro del sistema de nube. Como se puede observar en la figura 3, se establece una división entre redes WAN y redes LAN. Este esquema permite desarrollar distintas prácticas y contenidos de bajo nivel simulando un entorno real.

  En primer lugar, lo que se denomina red WAN en el *cloud* es una red que tiene acceso a Internet a través de la red corporativa, por lo que es direccionable, es decir, puede ser alcanzada tanto desde la red de acceso remoto como desde las aulas docentes.

  Por otro lado, encontramos las denominadas redes LAN. Estas redes son VLANS aisladas sin capacidad de direccionamiento hacia la organización. Están diseñadas con el objeto de que sea el propio alumno el que implemente los mecanismos de interconexión entre ellas y las redes WAN (routers, firewall) en el desarrollo de los contenidos prácticos de las distintas especialidades.

  En la figura 4 podemos observar un diseño básico de red que se puede realizar con el sistema descrito y que será el utilizado como base del sistema de esta propuesta.

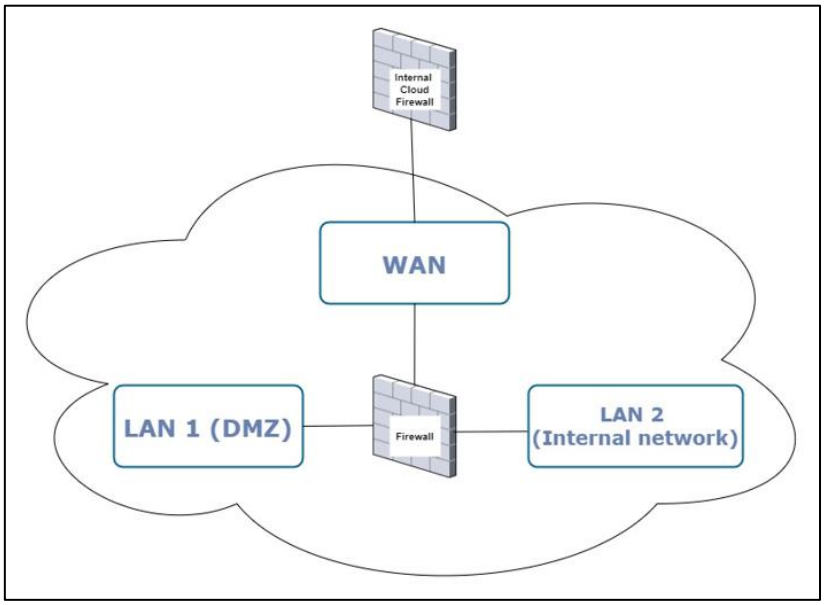


Figura 4. Simulación de una red básica en el sistema de *cloud* privado

3.3 Implementación del entorno de *cloud* privado

La implementación del servicio de *cloud* se realiza utilizando la plataforma de software OpenNebula sobre una infraestructura de virtualización clásica que sirve como base del sistema. La elección de OpenNebula para este proyecto responde a las ventajas que ofrece esta aplicación de código abierto frente a otras plataformas de características similares que pueden ser resumidas en los siguientes 3 puntos:

- Flexibilidad, escalabilidad y simplicidad: OpenNebula proporciona un entorno altamente flexible y escalable. Esto permite adaptarse a cambios en las necesidades de la infraestructura de forma rápida y adecuar los recursos según las necesidades del servicio. Por otro lado, esta plataforma de *cloud*, presenta un diseño simple y centralizado, que facilita una implementación y despliegue rápidos del sistema, reduciendo el tiempo de puesta en marcha necesario para su implementación o para su adaptación a cambios en el entorno.
- Software de código abierto: Al ser una plataforma de código libre, la aplicación puede ser utilizada sin incrementar los costos debido al licenciamiento. Esto permite ofrecer una solución profesional con un presupuesto limitado, como es el caso de estudio que aborda este trabajo, una formación con un alto grado de especialización, pero con un coste asequible, que la haga atractiva para un público amplio.
- Comunidad y Soporte: En la actualidad OpenNebula es una de las grandes alternativas en el mercado de los sistemas de *cloud* privado. Esto hace que cuente con una gran comunidad de usuarios, lo que facilita el acceso a recursos de aprendizaje y conocimiento en general sobre el sistema. Por otra parte, en la actualidad, la titularidad del proyecto está en manos de la empresa OpenNebula Systems que ofrece una modalidad de soporte comercial garantizando el acceso a asistencia técnica especializada y profesional, lo que ofrece mayores garantías sobre la continuidad de un despliegue basado en este sistema.

La infraestructura física que soporta la implementación del sistema de nube tiene un esquema típico de un entorno virtualizado, se basa en un *cluster* de servidores físicos que proporciona el procesamiento y la memoria que necesita el sistema, y un dispositivo de almacenamiento especializado que se ofrece al clúster por medio de una SAN (*Storage Area Network*) basada en *Fibre Channel*. Por otro lado, todo el entorno de red se realiza sobre un único switch que interconecta los hosts físicos.

Este diseño proporciona una serie de medidas de seguridad adicionales e intrínsecas a este tipo de tecnologías, gracias a la capacidad de abstracción sobre el hardware que ofrecen. Entre otras mejoras, vemos que dicha abstracción permite que los recursos computacionales se ofrezcan como pools que son utilizados por las instancias virtuales que finalmente ofrecen los servicios virtuales a los usuarios del sistema. Sobre esta infraestructura física se establece la configuración lógica por medio de VLANs y dispositivos virtuales (consolas de gestión y firewall) que permiten la implementación del esquema visto en la figura 3.

Finalmente, la capa de *cloud* implementada con OpenNebula añade un nuevo nivel de abstracción de cara al usuario automatizando las tareas de despliegue de instancias que se realizan sobre la infraestructura y que sirve como base del sistema. Es importante mencionar que las instancias virtuales no se contextualizan durante el despliegue. Esta decisión de diseño, que difiere de una implementación de nube estándar, se toma para permitir un control total de las instancias por parte de los usuarios y simular un entorno no administrado por un servicio de *cloud*. La falta de contexto de las imágenes implica que los usuarios deben realizar las tareas de personalización del sistema operativo tras el despliegue de un nuevo sistema para ajustar la configuración a las necesidades de su implementación.

La no contextualización de las instancias de sistemas virtuales hace necesario establecer una serie de mecanismos que faciliten el trabajo sobre el entorno y además ofrecen características adicionales a la simulación.

- La configuración de las redes que ofrece el sistema es fija, es decir, cada una de las VLANS correspondientes a redes WAN tiene un direccionamiento único y determinado en el diseño. La asignación de configuraciones dinámicas en estas redes se realiza por medio de un servicio DHCP específico de la infraestructura, simulando así un entorno WAN real donde el proveedor de servicios determina las características del direccionamiento.
- Las instancias virtuales deben ser configuradas al inicio por los usuarios del sistema. En el caso de los sistemas Windows, las plantillas base se generalizan utilizando la aplicación Sysprep lo que permite ofrecer la configuración básica inicial del sistema en el primer arranque de cada instancia. Este mismo procedimiento se realiza con algunas distribuciones Linux que lo permiten, como Ubuntu, que ofrece un modo OEM para la generalización de la imagen del sistema similar a Sysprep para Windows.

4. Descripción de los recursos de aprendizaje

El planteamiento del curso en ciberseguridad que se aborda en este trabajo se basa en la combinación de clases teóricas, estudio de casos reales y prácticas. Por otro lado, el enfoque que adopta el curso se fundamenta en investigaciones y prácticas educativas reconocidas en el campo de la ciberseguridad, así como en la integración de metodologías reconocidas e innovadoras dentro del campo de la docencia.

Para la estructuración de los contenidos curso, se han seguido los modelos y estándares ofrecidos por entidades y organizaciones de reconocimiento en el ámbito de la ciberseguridad, como es el National Institute of Standards and Technology (NIST) y el Center for Internet Security (CIS). Los estándares proporcionados por estas entidades permiten definir el conjunto de contenidos que serán abordados y que aseguran una correcta especialización en el campo de la ciberseguridad. Además, se han tomado como referencia modelos educativos que destacan la importancia de un enfoque integral que combina la teoría, práctica y evaluación continua de la formación en ciberseguridad, lo cual mejora significativamente las habilidades y competencias de los estudiantes (Workman, 2021).

Como se ha comentado anteriormente, el objetivo final del presente trabajo es la evolución de los contenidos prácticos hacia laboratorios que simulen entornos reales, proporcionando un enfoque contextualizado que ayude a los estudiantes a adquirir las competencias relevantes dentro de las materias que se estudian. Estos objetivos se basan en distintos estudios que ponen de manifiesto la importancia de ofrecer una formación que equilibre correctamente los contenidos teóricos y prácticos para facilitar y mejorar la su asimilación por parte de los estudiantes (Prince y Felder, 2006).

Además, el desarrollo de una infraestructura empresarial simulada se alinea adecuadamente con las recomendaciones realizadas por Kolb en su teoría del aprendizaje experiencial (Kold, 2014), que pone de relieve la mejora del aprendizaje basada en la experiencia directa. En nuestro caso, la creación de un entorno completo permite simular un entorno real que ofrece al alumnado una experiencia simulada similar a lo que encontrará en un entorno empresarial. En este sentido también es interesante destacar la importancia de metodologías de aprendizaje basadas en problemas (Hmelo-Silver, 2004). Según la tesis de Hmlelo y Silver, el Problem-Based Learning mejora significativamente las habilidades en resolución de problemas y el aprendizaje profundo de los contenidos por parte del alumnado.

A continuación, se presenta una descripción de los contenidos didácticos del curso en seguridad informática organizados en 5 módulos, cada uno de los cuales aborda un área específica dentro de la ciberseguridad. No todos los contenidos serán incluidos en la propuesta del sistema desarrollada en este trabajo. Junto a la descripción se comentarán si los contenidos serán abordados desde un punto de vista teórico, los que son susceptibles de integrarse en el nuevo sistema y aquellos que no serán integrados debido a problemas de licenciamiento o derechos de propiedad sobre ellos.

A continuación, se detallan cada uno de los módulos que componen el curso:

- **Módulo 1: Introducción al curso.** Este primer módulo del curso realiza una introducción al curso y al entorno en el que se desarrollan los contenidos. Este módulo se divide en los siguientes capítulos:
    1. Descripción del curso y sus contenidos.
    2. Introducción al laboratorio de seguridad.
    3. Implementación de una arquitectura básica de seguridad.

  A partir del segundo capítulo de este módulo se inician los contenidos prácticos que requieren el uso de infraestructura. En esta primera toma de contacto, la infraestructura es muy básica y se utiliza como introducción al sistema a través de un conjunto de prácticas elementales. Estas prácticas incluyen el despliegue de un firewall como bastión de una infraestructura y la publicación de servicios a través de este.

- **Módulo 2: Espacio de ejecución seguro.** Este segundo módulo constituye una introducción al área técnica de la ciberseguridad desarrollando una serie de conceptos y recursos básicos desde la perspectiva de la seguridad informática para la implantación de sistemas informáticos con el objetivo de garantizar su protección. El segundo módulo se compone de los siguientes capítulos:
    1. Estándares sobre sistemas de ejecución segura.
    2. Bastionado de sistemas.
    3. Sistemas de detección de vulnerabilidades.
    4. Sistemas de gestión de eventos e información de seguridad.

  El primer capítulo del módulo introduce una serie de contenidos teóricos que definen varios estándares de ejecución segura. El módulo aborda conceptos y estándares básicos en ciberseguridad como el ENS, NIST y fuentes de recursos de gran valor dentro del mundo de la ciberseguridad como son el CIS, el Incibe o el CCN entre otros.

  El resto de los capítulos de este módulo se centran en el desarrollo e implementación de un conjunto de técnicas necesarias para asegurar el entorno de ejecución de un sistema informático.

- **Módulo 3: Hacking ético.** Este módulo se centra en el desarrollo de los contenidos relacionados con las auditorías de seguridad, así como el conjunto de técnicas y herramientas utilizadas en el proceso de pentesting. Su desarrollo queda dividido en los siguientes capítulos:
    1. Introducción al hacking ético: Fases, alcance, tipos de auditoría.
    2. Recopilación de información.
    3. Análisis de vulnerabilidades.
    4. Herramientas y técnicas de ataque.
    5. Documentación de la auditoría.

  El primer capítulo del módulo hace una introducción a la filosofía del hacking ético desde el punto de vista de la auditoría de seguridad. En él se abordan los principios éticos de esta especialidad enfatizando la importancia del cumplimiento legal y ético necesario en el desarrollo de esta actividad profesional.

  A partir del segundo capítulo se inician los contenidos prácticos por medio del estudio de las técnicas y herramientas utilizadas en el proceso de pentesting. El contenido

práctico del módulo aborda desde las fases iniciales de un ataque, comenzando con la recopilación de información y llegando finalmente a las técnicas empleadas post-explotación.

Finalmente, el último capítulo de este módulo vuelve a introducir un conjunto de conceptos teóricos necesarios para la realización de la documentación asociada a una auditoría de seguridad.

- **Módulo 4: Gestión y respuesta ante incidentes.** El cuarto módulo del curso ofrece los conocimientos y habilidades relacionadas con la gestión y respuesta ante incidentes de seguridad.
    1. Fuentes de información de amenazas.
    2. Fases del ciclo de vida de un incidente.
        2.1. Preparación ante incidentes.
        2.2. Detección y análisis de incidentes.
        2.3. Contención, mitigación y recuperación.
        2.4. Tratamiento post-incidente: Informe y notificación.

  El primer capítulo ofrece de nuevo los contenidos teóricos que introduce conceptos básicos dentro de esta disciplina como son indicadores de amenaza o alertas tempranas sobre incidentes de seguridad.

  El segundo capítulo del módulo se enfoca nuevamente en los aspectos prácticos fundamentales de la gestión de incidentes, proporcionando los recursos necesarios para desarrollar las técnicas de preparación y detección de amenazas, junto con el desarrollo del conjunto de acciones necesarias para el tratamiento del incidente y las acciones necesarias durante la fase post-incidente.

- **Módulo 5: Seguridad con new generation firewall.** Este último módulo aborda las capacidades y mejoras que aportan los firewalls de nueva generación. Debido a que su realización se lleva a cabo con software propietario queda fuera de la propuesta actual y no será tratado en adelante.

5. Definición de requisitos del nuevo sistema

5.1 Análisis de requisitos

En esta sección se detallan los requisitos necesarios para cumplir con el propósito de diseño del sistema. Estos requerimientos están compuestos por un conjunto de requisitos funcionales específicos para el desarrollo propuesto y otro conjunto de requisitos no funcionales pero que están directamente relacionados con la creación de un entorno compartido y que permiten garantizar el funcionamiento adecuado del sistema para todos los usuarios del *cloud*.

En primer lugar, se detalla el conjunto de requisitos específicos para el desarrollo didáctico propuesto. Inicialmente el alumno únicamente necesita un terminal de usuario físico que le de acceso a los recursos del laboratorio. Este terminal no requiere de grandes prestaciones ya que todo el procesamiento necesario se realizará en el entorno de *cloud*. El terminal deberá contar únicamente con un conjunto de aplicaciones que le permitirán conectarse remotamente a los distintos servicios ofrecidos por el sistema.

- Cliente de conexión RDP.
- Cliente de conexión SSH.
- Navegador Web.
- Cliente VPN.

En este punto es importante destacar que, a excepción de los sistemas utilizados durante el primer módulo de la titulación, el resto de los elementos que componen la infraestructura de la simulación y que serán presentados conforme se desarrollen los contenidos, deberán ser reutilizados con el avance del curso, permitiendo que el alumno vea las interrelaciones que se producen entre ellos, y proporcionándole la visibilidad de un entorno real.

A continuación, se detallan los requisitos específicos que deben ser contemplados para abordar los contenidos didácticos propuestos:

- Módulo 1. Introducción al curso.
  - Credenciales de acceso al *cloud*.
  - Instancia de un firewall.
  - Instancia de un servidor para su publicación.
- Módulo 2. Espacio de ejecución seguro.
  - Instancia de un sistema que permita realizar el bastionado.
  - Instancia de sistema de detección de vulnerabilidades.
  - Instancia de un SIEM.
- Módulo 3. Hacking ético.
  - Instancia de sistema con las herramientas adecuadas para realizar una auditoría.
  - Sistemas vulnerables.
- Módulo 4. Gestión y respuesta ante incidentes.
  - Acceso a un conjunto de logs para su evaluación.

Por último, como el objetivo final del desarrollo es la integración de todos los sistemas que componen la simulación en una única infraestructura, será imprescindible dotar al sistema de los servicios de red básicos que se pueden encontrar en una red corporativa como puede ser un servicio de directorio, DHCP u otro servicio que favorezca la realización de la simulación de un entorno empresarial real.

Además de los requisitos específicos mencionados, el sistema debe cubrir otra serie de requisitos no funcionales pero que deben ser tenidos en cuenta de cara a la implantación del sistema:

- El sistema debe ser diseñado de manera que sea replicable y permita el funcionamiento simultáneo de múltiples instancias.
- El despliegue debe automatizarse para facilitar su implantación.
- Los accesos al sistema de *cloud* tienen que estar centralizados y auditados.
- El acceso a los servicios ofrecidos por el sistema debe ser seguro y con garantías de trazabilidad.
- El desarrollo de las actividades docentes no debe impactar en el funcionamiento de las actividades de usuarios de otras especialidades.

Finalmente, es necesario tener en cuenta una serie de reglas y principios de obligatorio cumplimiento sobre un entorno de *cloud* compartido con el propósito mencionado hasta ahora, que permitan asegurar el desarrollo de las actividades con garantías de funcionamiento adecuadas para todos los usuarios del sistema y que deben tenerse en cuenta durante el desarrollo del diseño del sistema:

- Los docentes definirán los contenidos didácticos y su adaptación al sistema. También podrán proponer las modificaciones o mejoras que crean necesarias para el desarrollo adecuado de los contenidos educativos.
- Los administradores del sistema serán los responsables de la asignación, creación y modificación de los recursos informáticos que se provean en el desarrollo de la simulación, así como de la asignación de roles de usuario en el ámbito del sistema de *cloud*.
- Todos los accesos al sistema de *cloud* deberán ser autenticados por mecanismos seguros de forma que se pueda realizar la trazabilidad de la actividad de los usuarios del sistema.
- Los sistemas virtuales que no se integren con los mecanismos de validación centralizados de la organización, en concreto los sistemas virtuales que forman parte de la simulación, serán monitorizados en todo momento y deberán disponer de mecanismos de acceso con máximo privilegio para los administradores y docentes. En caso de que este mecanismo de acceso quede bloqueado durante el desarrollo de las actividades prácticas, el usuario del alumno será bloqueado y el sistema se desvinculará del entorno mientras se realiza una investigación sobre el sistema y las actividades realizadas por el alumno.
- Independientemente de las actividades que se realicen en el sistema, el desarrollo de los contenidos debe cumplir con las normativas y regulaciones locales e internacionales al respecto de la seguridad de los sistemas de información. Se establecerán los mecanismos necesarios para asegurar que la actividad

desarrollada en el sistema esté siempre dentro de los límites legales y éticos en materia de protección de datos y privacidad.

- El diseño del sistema se realizará de forma que sea escalable y replicable para permitir su adaptación a futuras modificaciones de los contenidos o los elementos que lo componen, de forma que permita el escalado o la ampliación en el número de alumnos que lo utilizan.

6. Diseño del sistema

6.1 Descripción del Sistema

El diseño de la simulación propone la arquitectura de una empresa que basa su actividad en una tienda virtual donde vende diferentes productos a través de una tienda Online. Todos los servicios son publicados por la empresa, tanto a nivel interno como hacía Internet, bajo el dominio SimHackCorp.lab. La elección de este caso de estudio como nuestro entorno de simulación se basa en la relevancia de este tipo de negocios en el momento actual. Muchas empresas basan su actividad en la venta de productos online, ya sea directamente o mediante un intermediario, siendo incluso en el segundo caso habitual que la empresa mantenga un catálogo público de productos basado en un entorno web. Como es lógico, este modelo de negocio ofrece un contexto interesante en el campo de la ciberseguridad, ya que las tiendas virtuales son objetivos frecuentes de ciberataques debido a su exposición a la red y el manejo de información sensible, como datos de clientes y transacciones financieras.

En este sentido, es importante destacar que la actividad empresarial no tiene una relevancia significativa, ya que hoy en día la mayoría de las empresas ofrecen en internet un conjunto de servicios similar. Estos servicios pueden no estar directamente enfocados en la venta de productos, pero suelen basarse en servicios web que les proporcionan visibilidad a través de Internet. Sin embargo, establecer una actividad para la empresa tiene una gran importancia a la hora de crear una narrativa y contextualizar la simulación. Estos conceptos, que se relacionan de forma muy directa con la creación de una simulación y el desarrollo de la gamificación del entorno.

Por otro lado, una arquitectura típica de un entorno que ofrece servicios a Internet deberá estar respaldada siempre por un conjunto de servicios internos necesarios para su correcto funcionamiento, como pueden ser servicios de bases de datos. En definitiva, este modelo ofrecerá una arquitectura de *frontend-backend* adecuada para el desarrollo de la simulación. Esta estructura definida para la red interna también permite contemplar los servicios habituales de las redes LAN de las empresas de tamaño medio o grande, como, por ejemplo, un servicio de directorio que centralice las validaciones de los usuarios, y todos los servicios asociados a este.

Por lo tanto, según lo visto podemos definir que los servicios públicos que ofrece la empresa a Internet a través de la red WAN será un servicio web con su tienda virtual donde presenta un catálogo de productos y una serie de funcionalidades para los usuarios como son la compra o evaluación de los productos mediante *ratings* y comentarios. Por otro lado, la organización tiene un segundo servicio web público, en este caso es la intranet corporativa que se encuentra en construcción. Este servidor tiene abierto un servicio FTP por motivos administrativos que es utilizado por la empresa que está desarrollando el sitio.

Por último, con respecto a los servicios públicos ofrecidos a Internet por la corporación, se pública un tercer sitio web con la interfaz de gestión de su solución de seguridad Wazuh, el SIEM corporativo encargado de recopilar los registros de seguridad de los distintos elementos de la red para realizar una supervisión de eventos de seguridad de forma efectiva.

Con respecto a los servicios internos, la empresa dispone de un servicio de bases de datos que se utiliza para gestionar el almacén, los productos y los pedidos. Este servicio tiene vinculadas algunas tablas con las aplicaciones públicas a Internet. Por otro lado, los trabajadores de la empresa utilizan determinadas aplicaciones de escritorio que acceden a los datos almacenados en dicho servidor.

La red basa su sistema de validación y administración de equipos en el Directorio Activo de Microsoft. Este servidor se encuentra ubicado en una red interna y es accesible por los terminales de usuario y las aplicaciones que requieran utilizar sus servicios de validación. Por otro lado, la empresa tiene una serie de equipos cliente que pertenecen a los trabajadores de los distintos departamentos.

Toda la arquitectura de la red presentada queda definida por medio de un firewall bastión encargado de segmentar las redes y que ofrece las características de seguridad definidas para este tipo de dispositivos. Entre las principales funcionalidades que aporta se encuentran la publicación de servicio y la implementación de un servicio VPN para el acceso remoto de los trabajadores.

6.2 Definición de la arquitectura de red y servicios

Según lo visto en el diseño propuesto, el sistema debe proveer al alumno de un entorno de red adecuado compuesto por un conjunto de elementos de red básicos que permitan simular de forma correcta un sistema empresarial.

A continuación, en la Figura 5 se propone un diseño de red apropiado que cumple con las especificaciones básicas de la red corporativa desarrollada en el apartado anterior y que permite cubrir las necesidades definidas en los módulos didácticos del curso vistos en el capítulo 5 y detallados en el punto anterior.

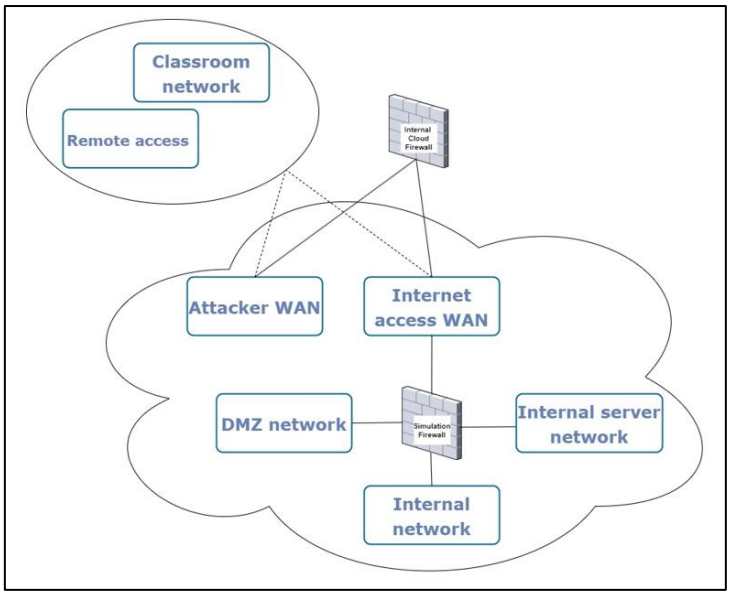


Figura 5. Esquema de red de la simulación

Como se puede observar en la figura 5, se deben definir un total de 5 VLANs, dos de ellas de tipo WAN, accesibles desde las redes remotas, y 3 LANs, enrutables solo a través del firewall del entorno de simulación. A continuación, se detalla el propósito de cada red:

- WAN1. Internet Access WAN. Esta red simula la conexión de la organización con un proveedor de servicios que le aprovisiona del acceso a Internet.
- WAN2. Attacker WAN. Esta red será utilizada durante el módulo 3 como red remota desde la que se producirá el ataque a la organización.
- LAN1. Internal network. Esta red simulará una red LAN corporativa. En ella solo se encontrarán los equipos de usuario.
- LAN2. DMZ network. Esta red simulará la zona desmilitarizada del firewall. Será la red desde donde se publiquen servicios hacia la WAN.
- LAN3. Internal Servers network. Esta red se corresponde con una zona donde encontraremos servidores que publicarán servicios de las redes corporativas. Estos servicios no serán accesibles desde la WAN.

Por otro lado, el sistema deberá contar con un conjunto de servicios básicos en una red corporativa y que ofrezcan un entorno de simulación adecuado para el desarrollo de las prácticas. Será necesario que el sistema proporcione los siguientes servicios:

- Servicio DNS.
- Servicio DHCP.
- Servicio de directorio.
- Servicio VPN de acceso.

Además de estos, los distintos servidores de la simulación contarán con los servicios básicos de conexión de una red empresarial real:

- Servicio SSH.
- Servicio RDP.
- Servicio Samba.

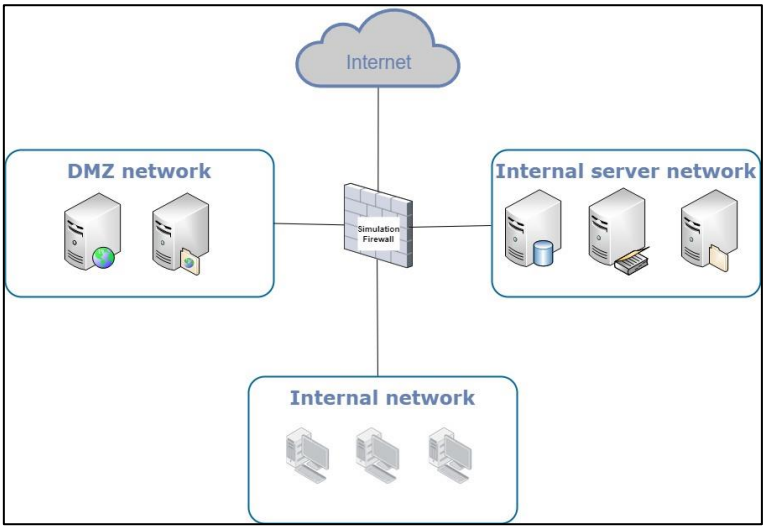


Figura 6. Esquema de red y servicios propuesto

6.3 Inventario de sistemas operativos y software empleado en el diseño

A continuación, se detallan los sistemas operativos seleccionados como base para las instancias que se utilizarán en la implementación:

- pfSense CE (Buechler y Scott, 2004). Se ha optado por esta distribución de software libre basada en FreeBSD para implementar el firewall bastión de la arquitectura. Su elección para nuestro diseño viene dada por su versatilidad y capacidad para ser instalado en la mayoría de las arquitecturas de hardware comunes, incluidas las instancias virtuales como la requerida en nuestro diseño. Además, ofrece un entorno de administración web bastante amigable que integra los entornos de gestión de los paquetes adicionales dentro de la consola de administración del dispositivo.
- Kali Linux (Aharoni y Kearns, 2013). Para la máquina que simula al atacante se ha seleccionado la distribución Kali Linux, uno de los sistemas operativos de referencia en su ámbito. Esta distribución Linux de código abierto basada en sus últimas versiones en Ubuntu (anteriormente en Debian), se caracteriza por ofrecer un conjunto de herramientas orientadas a la realización de auditorías de seguridad y pruebas de penetración en sistemas operativos.
- Debian (Debian Project, 1993). Los servidores que exponen sus servicios a Internet se implementarán con Debian, una distribución Linux de código abierto desarrollada por el proyecto Debian y mantenida por la comunidad. Esta distribución destaca dentro del segmento de sistemas operativos de servidor debido a su estabilidad y su diseño que tiene como uno de sus principios básicos la seguridad, fomentando la rápida distribución de parches para remediar problemas de seguridad.
- Ubuntu Desktop (Canonical, 2004). El equipo de usuario se implementará por medio de la distribución Ubuntu en su edición Desktop. Esta distribución Linux de código abierto derivada de Debian ofrece un entorno de trabajo adecuado para el usuario final gracias a su amigable interfaz y a una amplia selección utilidades de usuario que trae instaladas por defecto.
- Windows Server (Microsoft, 1993). Para la implementación del servicio de directorio, se opta por la implementación del sistema propietario de Microsoft. El directorio activo basado en Windows Server ofrece un conjunto de herramientas y servicios que facilitan la integración de todos los equipos cliente y dispositivos que forman parte de las redes LAN de los ecosistemas empresariales.

Por otro parte, a continuación, se detalla el software que se utilizará durante la implementación:

- Wazuh. Para la implementación de la plataforma de seguridad del sistema se utilizará este software de código abierto que integra las funcionalidades de un SIEM (Sistema de Información y Eventos de Seguridad) y un XDR (Detección y Respuesta Extendida). Su elección se debe a su gran funcionalidad, versatilidad y al hecho de que es uno de los estándares actuales del mercado en su ámbito.
- Nessus. Como herramienta para la auditoría de vulnerabilidades en los sistemas operativos, se utilizará la aplicación Tenable Nessus. Esta herramienta se destaca por ser una de las más potentes en su ámbito ofrece y, además, ofrece una versión

de su licenciamiento, Nessus Essentials que permite su utilización de forma gratuita para realizar auditorías de hasta 16 dispositivos.

- juice-shop. Este proyecto de software, mantenido por la organización OWASP Fundation (Curphey, 2001), proporciona un entorno adecuado para el aprendizaje sobre seguridad en las aplicaciones web. Se basa en un entorno web con ejemplos de las vulnerabilidades incluidas en el OWASP Top Ten[1], otro proyecto de la fundación que realiza un *ranking* sobre las vulnerabilidades con mayor impacto durante el periodo al que hace referencia.

6.4 Propuesta servicios

La implementación de esta propuesta se realizará por medio de los siguientes elementos.

6.4.1. Firewall perimetral

El firewall es el elemento central de cualquier red, no solo desde el punto de vista de la seguridad, sino también a su capacidad para enrutar redes internas. Esta capacidad es la que permitirá la coexistencia de varias instancias de nuestro entorno de forma simultánea. Para conseguir esta coexistencia, solo se tendrán que asignar distintas VLANs a las zonas WAN de los firewalls de los distintos entornos. Como veremos más adelante, esta interfaz del firewall recibirá la configuración IP del DHCP, al realizar un nuevo despliegue tendremos toda una red con direccionamiento privado tras él.

En nuestra propuesta, el firewall se implementará utilizando una instancia del sistema operativo pfSense con 4 zonas que diferenciarán todas las redes mencionadas anteriormente:

- Zona WAN: Esta zona se corresponde con la Internet Access WAN, vista en la figura 5, y representa la conexión de la red con Internet. Es la red que da acceso a la navegación de todos los sistemas y además la zona del firewall donde se publicarán los servicios ofrecidos por la organización. Por otro lado, será el punto de entrada a la red corporativa y por lo tanto la red que quedará expuesta a ataques desde Internet.
- Zona LAN: Esta zona será la Internal network y albergará los equipos cliente de la organización. Es la zona donde se encuentran los equipos que se utilizan como terminales cliente de la red.
- Zona DMZ: La zona desmilitarizada de red, denominada DMZ network, es la zona que se utiliza habitualmente para publicar servicios en Internet. Nuestra organización ofrecerá un conjunto de servicios a Internet que estarán desplegados en la DMZ, que serán detallados a continuación.
- Zona SERVERS: La zona Internal Servers network, proveerá de los servicios característicos de las redes internas de los entornos empresariales. En esta zona se ubicarán los servicios necesarios para el correcto funcionamiento de la red corporativa pero que no deben exponerse a Internet.

[1] Para mas información visitar la web del proyecto: https://owasp.org/www-project-top-ten/

Además de las funciones básicas de enrutamiento y publicación de servicios características de un firewall, este dispositivo realizará las siguientes funciones adicionales:

- Servidor VPN. Se implementará el acceso remoto a la infraestructura por medio del servicio OpenVPN integrado en pfSense.
- Servidor DHCP. Se utilizará el servicio integrado en pfSense para la configuración de red automática de los sistemas que lo requiera en las zonas internas de la red de la simulación.

6.4.2. Servidor Web de la aplicación Wazuh

Este servidor estará situado en la red DMZ de la organización y permitirá publicar la consola de administración del servicio de monitorización proporcionado por la aplicación Wazuh. Por otra parte, centralizar los logs del firewall y del directorio activo de la organización.

- Servidor basado en Debian y actualizado a las últimas versiones tanto de sistema operativo como de software.
- El servidor tendrá varios servicios abiertos:
  - Servicio HTTPS que proporciona acceso a la aplicación.
  - Servicio SSH para la conexión remota al sistema.

6.4.3. Servidor para auditorías basado en Nessus

Este servidor no estará integrado en la arquitectura de la red ya que será utilizado como un elemento adicional externo al entorno. Esto es debido a que su principal uso planificado será durante el desarrollo del módulo 2, como recurso para el aprendizaje de herramientas de auditoría de seguridad. Adicionalmente podrá ser utilizado por el atacante durante el desarrollo del módulo 3 pero su alcance quedará limitado a la parte externa de la red, por lo que solo permitirá realizar los escaneos iniciales sobre el entorno. Cuando avance el desarrollo del módulo 3, el alumno deberá utilizar otros sistemas para realizar la detección de vulnerabilidades como por ejemplo los scripts de Nmap o los módulos auxiliares de Metasploit. Debido a esto, este sistema se desplegará en la red WAN y quedará excluido del diseño que defina la arquitectura final del sistema.

Este servidor tendrá las siguientes características y servicios:

- Servidor basado en Debian y actualizado a las últimas versiones tanto de sistema operativo como de software.
- El servidor tendrá varios servicios abiertos:
  - Servicio HTTPS que proporciona acceso a la aplicación.
  - Servicio SSH para la conexión remota al sistema.

6.4.4. Servidor Web de tienda virtual Web

Basada en la aplicación juice-shop[2] de OWASP Fundation. Este servidor basado en Debian estará situado en la red DMZ de la organización y permitirá publicar la aplicación web juice-shop, desarrollada en JavaScript y basada en Node.js, Express y Angular, que ofrece un entorno CTF para la formación en ciberseguridad en las aplicaciones web. La herramienta

[2] Para mas información consultar la web del proyecto: https://owasp.org/www-project-juice-shop/

está diseñada como un conjunto retos o desafíos que incluyen de forma intencionada las vulnerabilidades de aplicaciones web incluidas en el TOP Ten de OWASP de 2017. Las características de este servidor son:

- Servidor basado en Debian y actualizado a las últimas versiones tanto de sistema operativo como de del software requerido para publicar la aplicación. El servidor no será vulnerable, pero la aplicación está diseñada de forma que ofrece un conjunto de vulnerabilidades clásicas en aplicaciones web.
- El servidor tendrá varios servicios abiertos:
  - Servicio HTTP que proporciona acceso a la aplicación.
  - Servicio SSH para la conexión remota al sistema.
- La aplicación web contiene vulnerabilidades de las siguientes categorías (consultar información detallada en el anexo correspondiente a la descripción de las vulnerabilidades en los sistemas):
  - Inyección SQL y NoSQL.
  - Cross-Site Scripting.
  - Broken Authentication.
  - Security Misconfigurations.

6.4.5. Servidor Web de la Intranet

Servidor web en construcción de la Intranet corporativa. Este servicio se implementa por medio de una instancia del sistema vulnerable "BASIC PENTESTING: 1"[3] proporcionada por el repositorio de retos de seguridad Vulnhub (referencia). Este servidor situado en la DMZ ofrece un conjunto de servicios que de forma habitual son publicados Internet, a continuación, podemos ver los detalles del sistema:

- Esta máquina basada en Debian es un entorno de servidor que ofrece un conjunto de retos de tipo boot2root.
- El servidor incluye los siguientes servicios:
  - Servicio HTTP.
  - Servicio FTP.
- El informe generado por Nessus incluye la siguiente vulnerabilidad de nivel crítico:
  - 50989 - ProFTPD Compromised Source Packages Trojaned Distribution.
- Por otro lado, la máquina incluye una serie de vulnerabilidades y errores de configuración que permiten acceder al sistema de forma ilícita por medio del servicio web.

6.4.6. Servicio de directorio

Servidor de Directorio Activo de Microsoft. Este servidor situado en la red SERVERS ofrecerá los servicios clásicos de las redes Microsoft.

- Servidor basado en Windows 2012 R2. El servidor tiene deshabilitadas las actualizaciones de sistema y no se ha parcheado desde la versión del reléase inicial.
- El servidor ofrece los siguientes servicios a la red interna:

[3] Puede consultarse información adicional sobre esta imagen prediseñada "BASIC PENTESTING: 1" del repositorio Vulnhub en https://www.vulnhub.com/entry/basic-pentesting-1,216/

  - Servicio de Directorio Activo.
  - Servicio LDAP.
  - Servicio DNS. Servicio básico para una red basada en el directorio de Microsoft.
  - Servicio SAMBA necesarios para el correcto funcionamiento de las directivas del Directorio Activo.
  - Servicio RDP para la conexión al sistema.
- La versión de Windows 2012 R2 utilizada tiene múltiples vulnerabilidades (consultar información detallada en el anexo correspondiente a la descripción de las vulnerabilidades en los sistemas). A continuación, se muestra un resumen incluyendo las vulnerabilidades de nivel alto y crítico mostradas por Nessus:

Tabla 1. Vulnerabilidades críticas y altas del servicio de directorio

Vulnerabilidad	CVE	Severidad
MS14-066 - Vulnerability in Schannel Could Allow Remote Code Execution	CVE-2014-6321	Critica
MS17-010 – High: Security Update for Microsoft Windows SMB Server (ETERNALBLUE)	CVE-2017-0144	Alta

  - 79638 - MS14-066 – Critica: Vulnerability in Schannel Could Allow Remote Code Execution (2992611).
  - 97833 - MS17-010 – High: Security Update for Microsoft Windows SMB Server (4013389).
- El servidor tiene errores de configuración que permiten realizar ataques adicionales:
  - El servidor DNS tiene activa la transferencia de zona lo que permite a un atacante realizar un ataque axfr y descargar todos los registros de la zona.
  - El servicio LDAP no está autenticado por lo que un usuario sin credenciales puede lanzar consultas al servicio de directorio.
  - Contraseña de administrador débil que facilita la realización de ataques de fuerza bruta al hash o a los servicios ofrecidos.

6.4.7. Servicio de bases de datos

Servidor de bases de datos. Este servicio se implementa por medio de una instancia virtual del sistema vulnerable de tipo CTF/boot2root denominada “PYEXP: 1”[4] del repositorio Vulnhub. Este servidor situado en la red SERVERS, simula el servicio MySQL corporativo.

- El sistema basa los retos que propone en una serie de servicios caracterizados por ser accesibles únicamente desde las redes internas de las organizaciones:
  - Servidor MySQL.
  - Servidor SSH.

6.4.8. Equipo del atacante

Este equipo situado en la red WAN remota se basa en la distribución de seguridad Kali Linux. Este equipo simulará el entorno de trabajo de un atacante externo a la organización.

[4] Puede consultarse información adicional sobre esta imagen prediseñada “PYEXP: 1 “ del repositorio Vulnhub en https://www.vulnhub.com/entry/pyexp-1,534/

6.4.9. Equipo cliente de la organización

Equipo cliente de la organización. Este equipo situado en la red LAN de la empresa se basará en un sistema Ubuntu Desktop. Este equipo simulará el entorno de trabajo de un empleado de la organización. Cabe destacar que este sistema, en este momento, es un elemento opcional que en esta versión de la arquitectura no será incluido. Queda en manos de los docentes que impartan el curso la decisión de incluirlo como elemento adicional.

6.5 Esquema final y resumen del diseño propuesto

A continuación, en la figura 7, vemos el esquema final del diseño propuesto de la arquitectura del sistema para la simulación de la red empresarial.

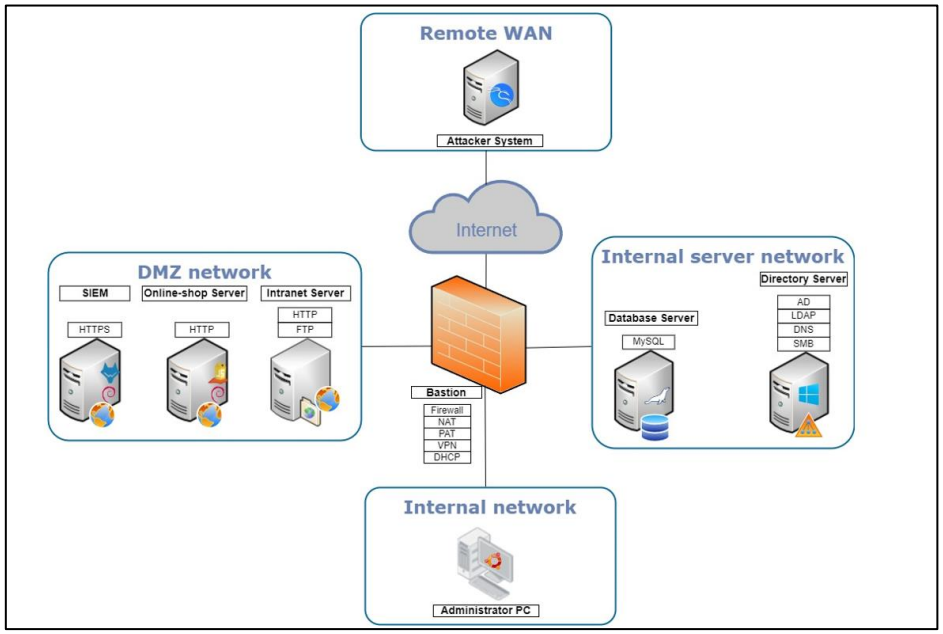


Figura 7. Esquema detallado de servidores y servicios

Como vemos en el esquema, la arquitectura se compone de los siguientes elementos:

- Firewall bastión:
  - Implementado sobre pfSense CE.
  - Realizará las siguientes funciones:
    - Segmentación de la red en 4 zonas: WAN, LAN, DMZ, SERVERS.
    - Publicación de servicios a Internet.
    - Servidor VPN de acceso.
    - Servidor DHCP para autoconfiguración de red.
- SIEM Wazuh:
  - Implementado sobre Debian.
  - Ubicado en la red DMZ.
  - Realizará las funciones de centralización y correlación de logs de los dispositivos de la red.
- Servidor web tienda virtual simulada:
  - Implementado sobre Debian.
  - Ubicado en la red DMZ.
  - Implementado con la plataforma juice-shop de OWASP Fundation.
  - Ofrece un entorno CTF para formación en ciberseguridad especializada en vulnerabilidades en aplicaciones web.
- Servidor web intranet corporativa simulada:
  - Implementado con una instancia del sistema Basic_Pentesting1 de VulnHub.
  - Ubicado en la red DMZ.
  - Ofrece un reto de boot2root enfocado en los servicios HTTP y FTP.

- Servidor de Directorio Activo corporativo:
  - Implementado sobre Windows Server 2012 R2.
  - Ubicado en la red SERVERS.
  - Ofrece los siguientes servicios a la red corporativa:
    - Servicio de directorio activo.
    - Servicio LDAP.
    - Servicio DNS.
    - Servicio SAMBA.
- Servidor de base de datos corporativo simulado:
  - Implementado con una instancia del sistema PYEXP1 de VulnHub.
  - Ubicado en la red SERVERS.
  - Ofrece un conjunto de retos boot2root enfocados en el servicio MySQL.
- Sistema atacante:
  - Implementado sobre Kali Linux.
  - Ubicado en la red remoteWAN.
  - Ofrece los recursos necesarios para realizar un ataque a un sistema informático.
- Equipo cliente del administrador (Opcional):
  - Implementado sobre Ubuntu Desktop.
  - Ubicado en la red LAN.
  - Ofrece el acceso a las herramientas básicas de un administrador encargado de la seguridad de la organización.

7. Implementación del sistema

7.1 Desarrollo del entorno de simulación

El desarrollo del entorno de simulación consiste en el despliegue en el *cloud* definido anteriormente de un conjunto de instancias virtuales personalizadas de los diferentes sistemas que componen la arquitectura de la red simulada. Cada una de estas instancias se configurará de forma adecuada para que cumpla con las especificaciones definidas en el diseño de la arquitectura realizado.

Las instancias de los distintos elementos que componen la red, según lo visto en el diseño propuesto, se basarán en los sistemas operativos característicos según los roles o funciones que realicen de forma particular. A continuación, se detalla el conjunto de sistemas operativos que se utilizarán en las distintas instancias:

- pfSense OS 2.7.2. El firewall de la red se implementará por medio de esta distribución en su última *release* y totalmente actualizada ya que no debe presentar vulnerabilidades que puedan poner en riesgo el funcionamiento de la arquitectura.
- Debian 11. Los sistemas Wazuh, Nessus y juice-shop, que no deben presentar vulnerabilidades a nivel de sistema operativo se instalarán sobre la versión 11 de Debian y serán actualizadas tras cada despliegue del entorno.
- Windows Server 2012. El servicio de directorio se desplegará con esta versión de Windows que actualmente se encuentra fuera de su ciclo de vida, por lo que proporciona un sistema adecuado para nuestro propósito debido a las vulnerabilidades conocidas que presenta esta antigua versión del sistema operativo de Microsoft.
- Kali Linux. Este sistema será desplegado basándose en la última distribución disponible desde la página oficial del proyecto. Además, como recomendación general debe estar actualizada para que contenga las últimas versiones de las herramientas que se utilizarán durante el proceso de ataque.
- Ubuntu desktop. Inicialmente este sistema se plantea como opcional por lo que se desplegará, cuando sea necesario, utilizando la última reléase disponible del sistema operativo. En esta primera versión de la arquitectura queda fuera del alcance de los contenidos que serán abordados.

Excepcionalmente, hay dos sistemas que se basan en imágenes preconfiguradas como entornos de aprendizaje enfocado en la ciberseguridad. Estas instancias vienen con el OS preinstalado por lo que no requieren una selección del mismo.

Como recursos adicionales para el desarrollo de la arquitectura, serán necesarias un conjunto de VLANs que se corresponderán con las distintas redes propuestas en el diseño. La asignación de las VLANs es la siguiente:

- WAN03 -> RemoteWAN
- WAN94 -> WAN
- LAN146 -> LAN
- LAN147 -> DMZ
- LAN150 -> SERVERS

7.2 Descripción de las instancias propuestas

A continuación, se ofrece una descripción detallada de las instancias que serán utilizadas en el desarrollo de la arquitectura de la red propuesta:

Tabla 2. Tabla resumen de las características de las instancias propuestas

Code name	DNS name	OS	Network	IP	Procesadores	Memoria (MB)
PfSenseBastion	pfsense.simhackcorp.lab	pfSense OS 2.7.2	WAN LAN DMZ SERVERS	DHCP 192.168.1.1 192.168.10.1 192.168.20.1	1	512
DebianWazuh	wazuhserver.simhackcorp.lab	Debian11	DMZ	192.168.10.50	2	8192
DebianNessus	nessusserver.simhackcorp.lab	Debian11	SERVERS	192.168.20.61	4	4096
juice-shop	online-shop.simhackcorp.lab	Debian11	DMZ	192.168.10.60	1	2048
Basic_Pentesting	intranet.simhackcorp.lab	-	DMZ	192.168.10.61	2	4096
Adserver	adserver.simhackcorp.lab	Windows Server 2012 R2	SERVERS	192.168.20.50	1	4096
Pyexp	ddbbserver.simhackcorp.lab	-	SERVERS	192.168.20.62	2	2048
UbuntuDesktop	systemadmin.SimHackCorp.lab	Ubuntu Desktop 2204	LAN	192.168.1.23	2	4096
Kali	-	Kali OS	RemoteWAN	DHCP	2	4096

7.3 Configuración

Basándonos en la descripción del punto anterior, la configuración final realizada sobre la plataforma de *cloud* de los distintos elementos que componen la arquitectura es la siguiente.

7.3.1. Firewall bastión

Este sistema se implementará por medio del despliegue de una instancia de pfSense con cuatro interfaces conectadas a las siguientes redes del sistema de *cloud* en el orden siguiente: WAN94, LAN146, LAN147 y LAN150.

Figura 8. Asignación de redes del firewall bastión

Tras el despliegue inicial del sistema se le aplicarán las siguientes configuraciones:

- Configuración de la red:

Tabla 3. Direccionamiento IP del firewall

Zona	IP	Tipo de direccionamiento
WAN	10.3.194.XX/24	Dinámico (DHCP del cloud)
LAN	192.168.1.1/24	Estático
DMZ	192.168.10.1/24	Estático
SERVERS	192.168.20.1/24	Estático

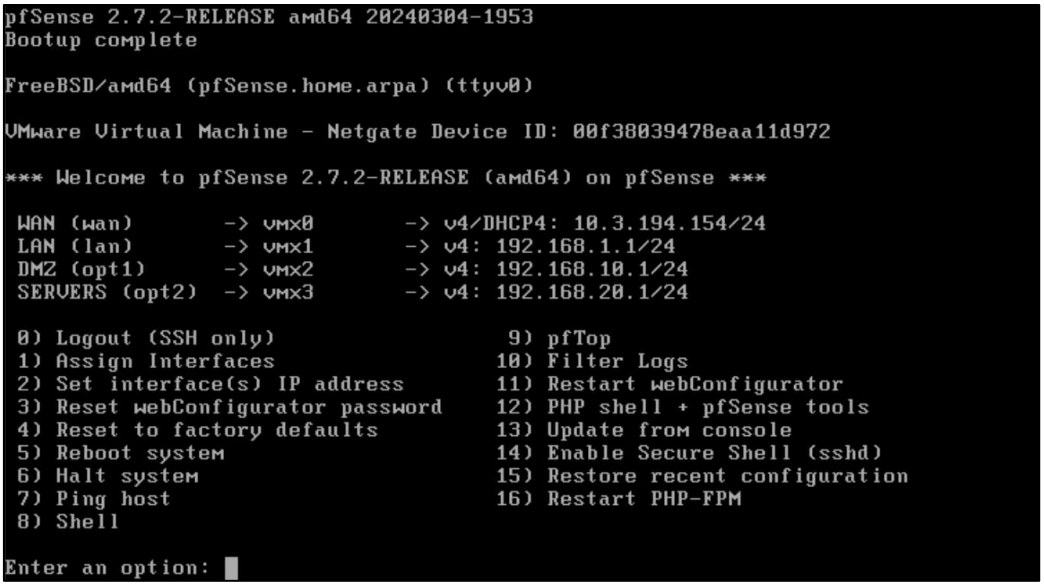


Figura 9. Configuración IP del firewall

- Instalación del paquete de pfSense OpenVPN Agent configuration

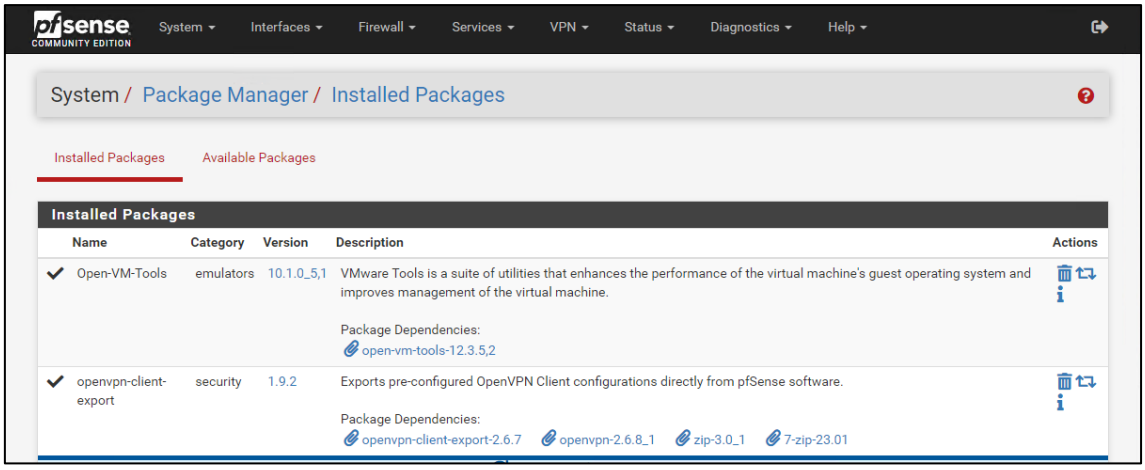


Figura 10. Instalación del paquete *openvpn-client-export*

- Creación del usuario sysadmin para la VPN

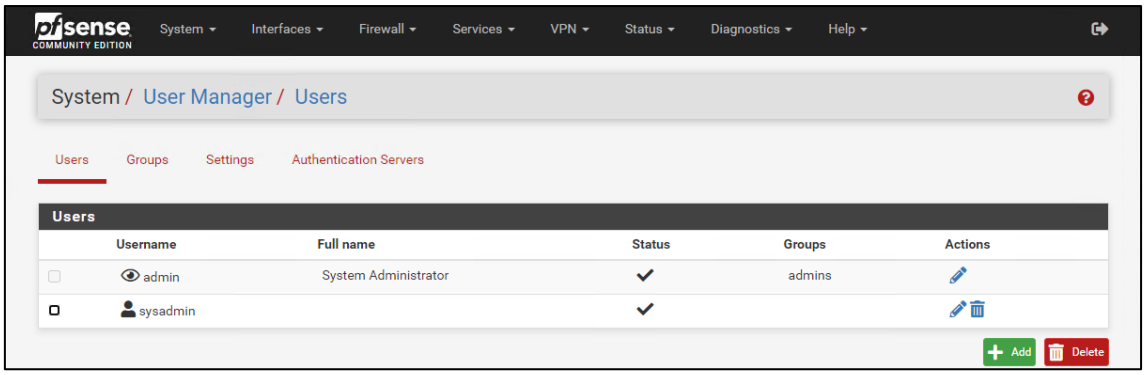


Figura 11. Usuario creado en el firewall para el acceso VPN

- Configuración del servicio de VPN con OpenVPN.

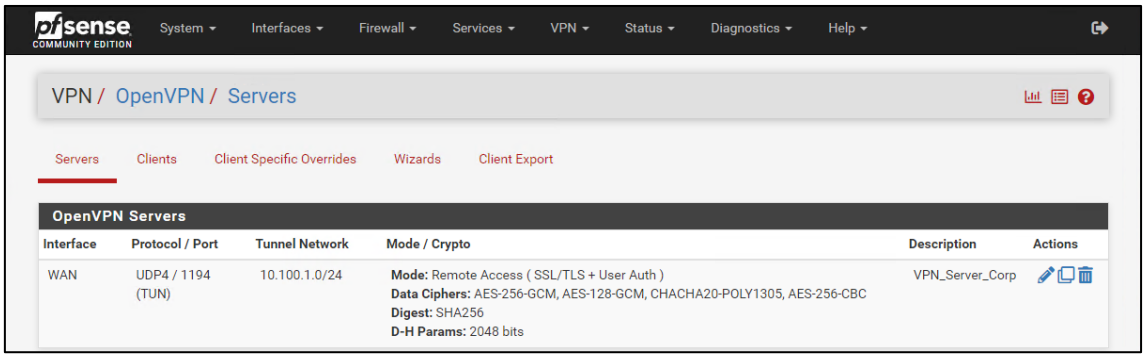


Figura 12. Parámetros de configuración del servidor VPN

- Configuración del paquete de generación de configuración del cliente.
- Configuración de direcciones IP virtuales para la publicación de servicios:
  - 10.3.194.60
  - 10.3.194.61
  - 10.3.194.62

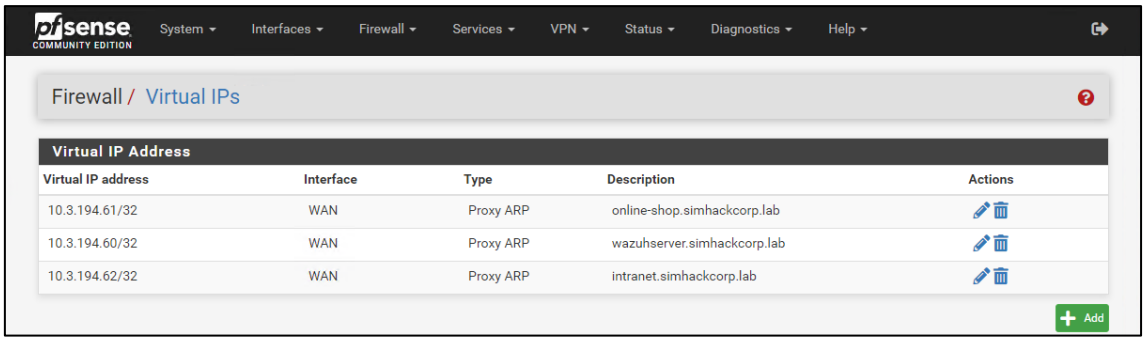


Figura 13. Direcciones IP virtuales asignadas al firewall

- Configuración de NAT 1:1 de los servicios publicados por el firewall

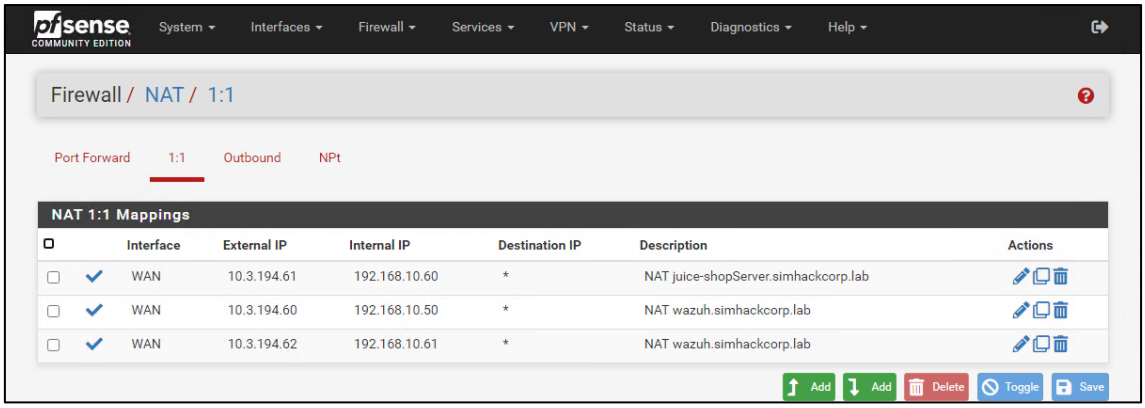


Figura 14. Configuración de NAT 1:1 para la publicación de servicios

- Creación de reglas de acceso para todas las zonas del firewall

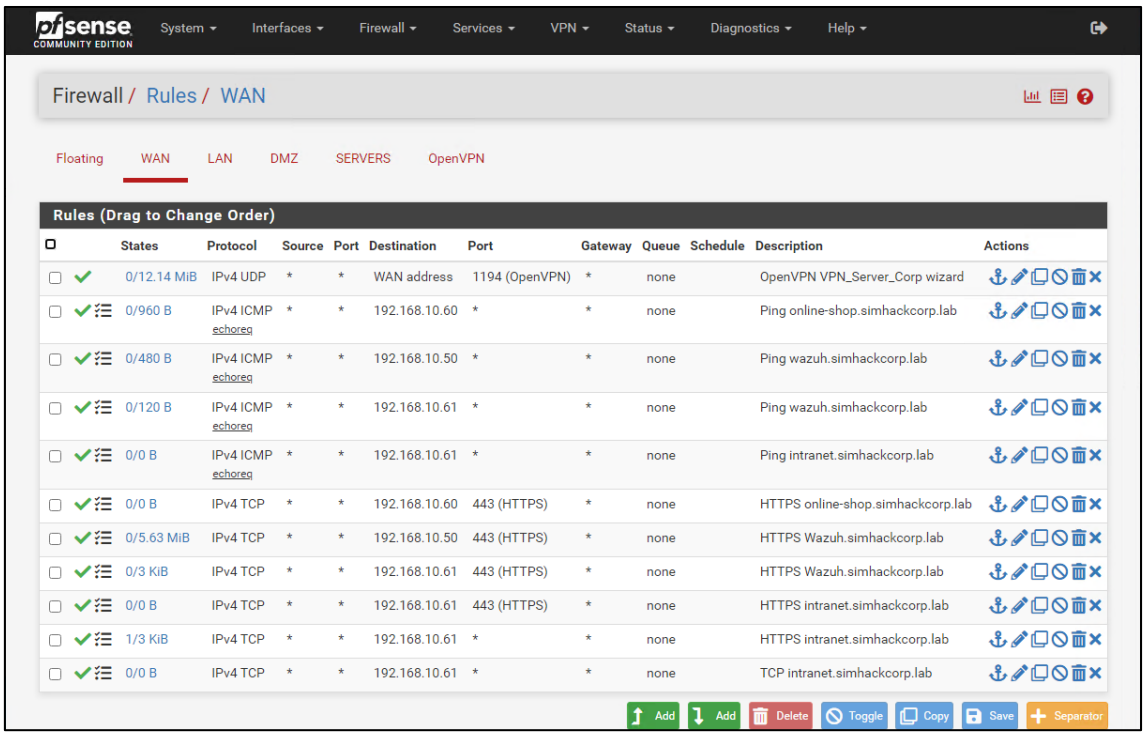


Figura 15. Conjunto de reglas definido en la zona WAN del firewall

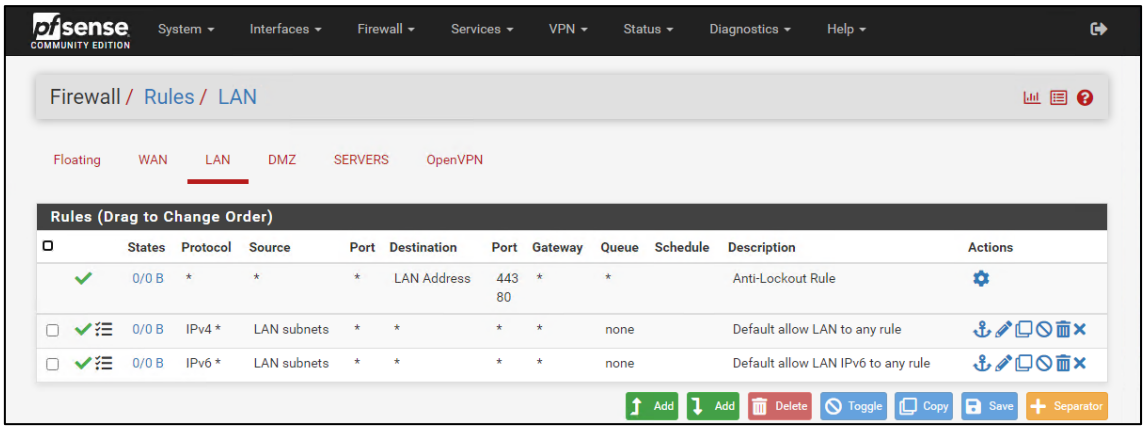


Figura 16. Conjunto de reglas definido en la zona LAN del firewall

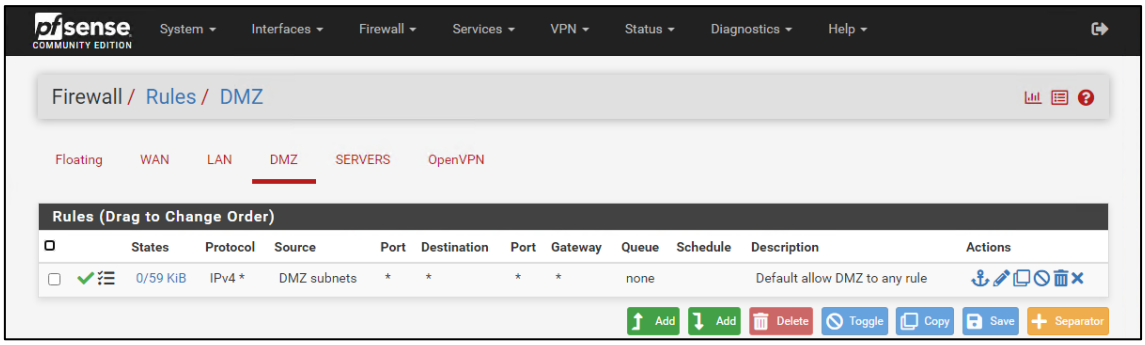


Figura 17. Conjunto de reglas definido en la zona DMZ del firewall

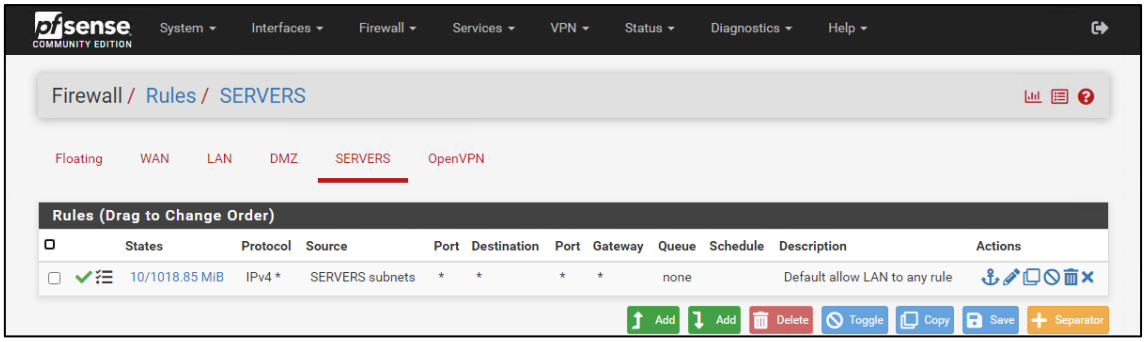


Figura 18. Conjunto de reglas definido en la zona SERVERS del firewall

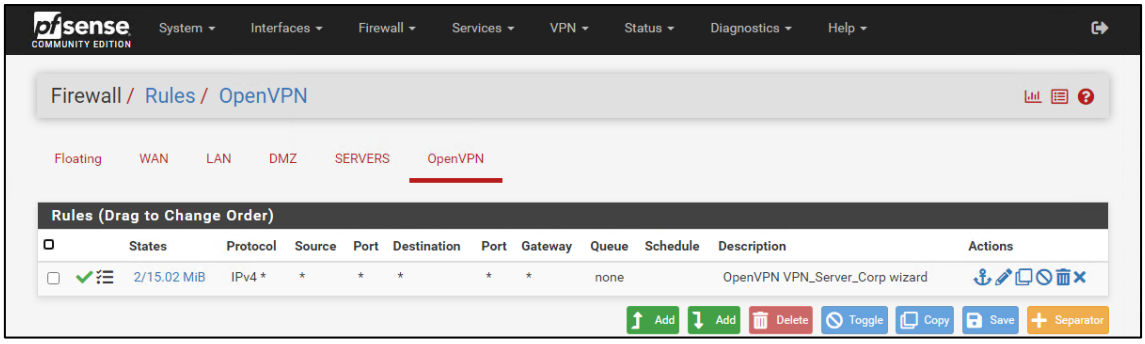


Figura 19. Conjunto de reglas definido en el firewall para el túnel VPN

7.3.2. Servicio de directorio

El servicio de directorio se implementará mediante el despliegue de una instancia básica de Windows Server 2012 con una interfaz conectada a la LAN150 del entorno de cloud. Tras su despliegue se completa el proceso de sysprep y se le configura una contraseña al usuario administrador del sistema. El resto de la configuración de este sistema se basa en la ejecución de un script de PowerShell que realiza la siguiente configuración de forma automática del sistema:

- Configuración de la red asignando la dirección IP 192.168.20.50 adecuada para la red SERVERS, establece el firewall como puerta de enlace y como DNS el 8.8.8.8 administrado por Google.
- Instalación y configuración de los servicios de DNS y Active Directory
- Se crean las entradas en el servicio DNS de todos los sistemas que forman parte del entorno.
- Se habilita la transferencia de zona para simhackcorp.lab en el servicio DNS.
- Se incluyen las flags que permitirán la implementación del proceso de gamificación que será tratado en detalle en el apartado 7.6.
- Instalación del agente de Wazuh.

7.3.3. Servidor de seguridad

La implementación del servidor de seguridad consiste en el despliegue de una instancia básica de Debian 11 con una interfaz de red conectada a la LAN147:

- Configuración de la red de forma adecuada para ajustarse al direccionamiento utilizado en la red DMZ. Para ello se configura la IP 192.168.10.50 de forma estática y la puerta de enlace será la 192.168.10.1 correspondiente al firewall de la red. El servicio DNS que utilice este sistema para la resolución será el que proporciona el servidor del Directorio Activo a la red interna de la organización.
- Instalación del servicio Wazuh mediante el proceso all-in-one según las especificaciones realizadas por el desarrollador.

7.3.4. Servidor de auditorías

Por su parte, el servidor de auditorías se basa en el despliegue de una instancia básica de Debian 11 con una interfaz de red conectada a la WAN94:

- La configuración de red se realizará automáticamente por el DHCP del entorno de *cloud*.
- Instalación del software Nessus Essential según la documentación oficial del desarrollador. Queda en manos del alumno la realización del registro de la licencia y la inicialización del software.

7.3.5. Servidor de bases de datos interno

Este servicio se realizará mediante el despliegue de una instancia de máquina virtual del sistema “PYEXP: 1” del repositorio de retos de ciberseguridad vulnhub, con una interfaz de red conectada a la LAN150:

- Configuración de la red de forma adecuada para ajustarse al direccionamiento utilizado en la red SERVERS. Para ello se configura la IP 192.168.20.62 de forma

estática y la puerta de enlace será la 192.168.20.1 correspondiente al firewall de la red. El servicio DNS que utilice este sistema para la resolución será el que proporciona el servidor del Directorio Activo a la red interna de la organización.
- Se incluyen las flags que permitirán la implementación del proceso de gamificación posteriormente.

7.3.6. Servidor Web tienda virtual

Para la implementación de la tienda virtual se realizará el despliegue de una instancia básica de Debian 11 con una interfaz de red conectada a la LAN147:

- Configuración de la red de forma adecuada para ajustarse al direccionamiento utilizado en la red DMZ. Para ello, se configura la IP 192.168.10.60 de forma estática y la puerta de enlace será la 192.168.10.1, correspondiente al firewall de la red. El servicio DNS que utilice este sistema para la resolución será el que proporciona el servidor del Directorio Activo a la red interna de la organización.
- Cambio del nombre de host a juice-shop.
- Ejecución del script de Bash InstallJuiceShop.sh que realiza el proceso de instalación de la aplicación juice-Shop.

7.3.7. Servidor Web de la intranet

El servidor web que simule la intranet corporativa se realizará desplegando una instancia de máquina virtual del sistema "BASIC PENTESTING: 1" del repositorio de retos de ciberseguridad Vulnhub, con una interfaz de red conectada a la LAN147:

- Configuración de la red de forma adecuada para ajustarse al direccionamiento utilizado en la red DMZ. Para ello se configura la IP 192.168.10.61 de forma estática y la puerta de enlace será la 192.168.10.1 correspondiente al firewall de la red El servicio DNS que utilice este sistema para la resolución será el que proporciona el servidor del Directorio Activo a la red interna de la organización.
- Se generan de forma manual, las flags que permitirán la implementación del proceso de gamificación posteriormente.

7.3.8. Equipo atacante

El despliegue del equipo atacante consiste en una instancia del sistema Kali en la WAN03:

- La configuración de red se realizará automáticamente por el DHCP del entorno de *cloud*. Queda en manos del alumno, durante el proceso de aprendizaje, su actualización y personalización.

7.3.9. Situación final del entorno y creación de plantillas

Tras realizar la configuración de todas las instancias según las especificaciones, como vemos en la figura 10, la arquitectura del sistema se compone de 8 instancias correspondientes a cada uno de los elementos definidos en el esquema de la arquitectura final de la arquitectura definido en el apartado 6.5.

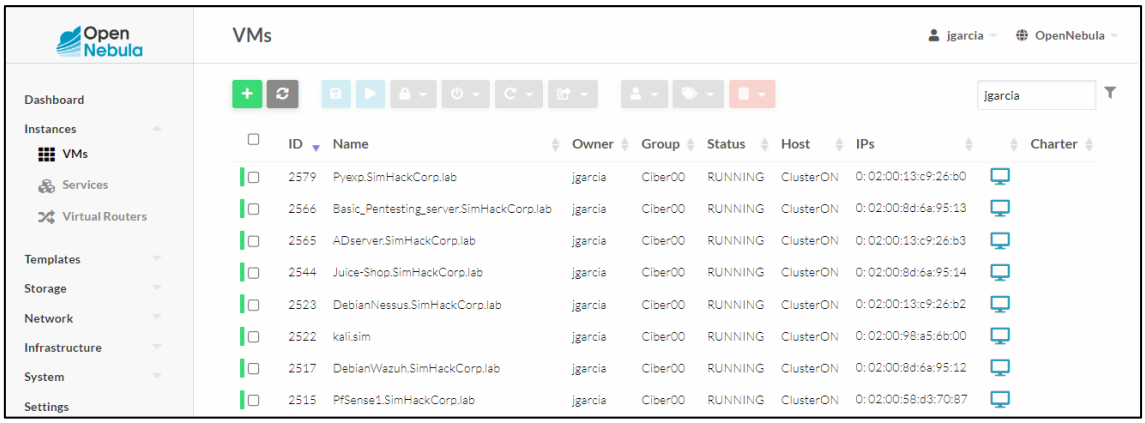


Figura 20. Visualización de las instancias generadas en la interfaz del sistema de cloud

Como se ha comentado anteriormente, uno de los objetivos es poder replicar el entorno sucesivas veces de cara a su reutilización como laboratorio de pruebas en formaciones orientadas a la ciberseguridad. Para poder desplegar distintas versiones del entorno, es necesario disponer de las distintas plantillas preconfiguradas de forma que se facilite el proceso de automatización del despliegue en numerosas ocasiones. Por ello, una vez finalizada la configuración de los distintos sistemas según las especificaciones anteriores se procede a la creación de las plantillas. En la figura 11 se puede observar el resultado de la generación de las plantillas.

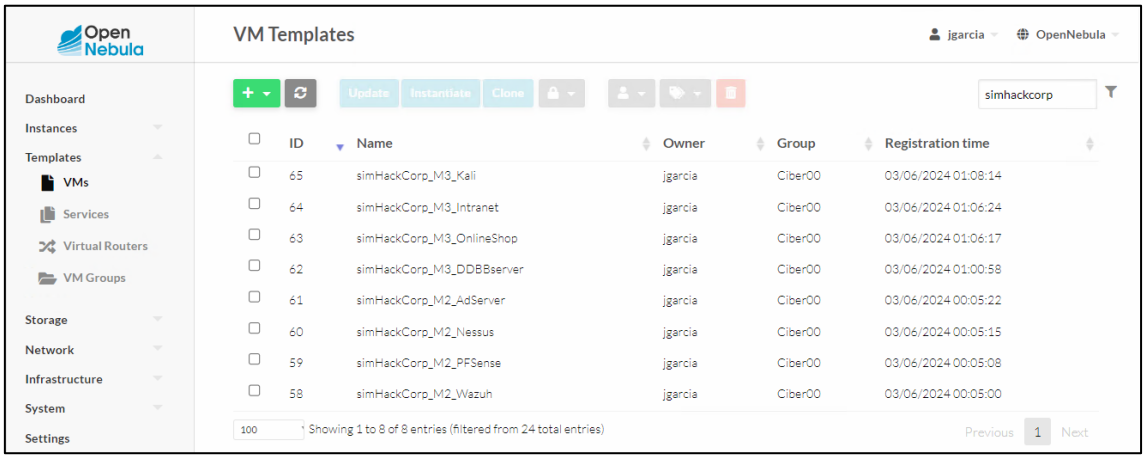


Figura 21. Conjunto de plantillas que componen la arquitectura de la red

7.4 Definición de las prácticas que abordan los contenidos didácticos

Como hemos visto hasta ahora, la infraestructura propuesta proveerá al alumnado de un conjunto de recursos especializados que pueden integrarse como base para el desarrollo de los contenidos didácticos del curso de ciberseguridad. A continuación, se aborda el contenido de cada uno de los módulos y se ofrece una propuesta de un conjunto de prácticas relacionadas con el módulo que pueden ser implementadas a partir de los recursos propuestos. Es importante mencionar que las propuestas realizadas son un simple ejemplo del potencial que ofrece la arquitectura desarrollada y por lo tanto no excluye el diseño de otras prácticas o actividades que aprovechen los recursos desplegados. En este sentido, cabe destacar que el desarrollo completo de los contenidos queda fuera del alcance de este trabajo y por lo tanto deberá ser desarrollado por el docente responsable del curso.

Con respecto a las prácticas propuestas, cada una de ellas viene acompañada de una breve descripción, que servirá como punto de partida para el desarrollo completo de los recursos de aprendizaje asociados al curso de seguridad. A continuación, se detalla la propuesta de prácticas para cada módulo.

7.4.1. Módulo 1. Introducción al curso

Introducción al curso. Como se ha comentado anteriormente, el primer módulo es una introducción al mundo de la ciberseguridad y al entorno de aprendizaje propuesto, por lo que los distintos sistemas que se utilizan no serán los de la simulación creada. Para la realización de las prácticas de este módulo, será el propio alumno el que despliegue las instancias los distintos sistemas mediante las plantillas adecuadas. Para su desarrollo, se proporcionará al alumno los recursos necesarios para el despliegue, las credenciales de acceso al sistema, las plantillas de sistema operativo necesarias y el conjunto de redes requerido.

Tras el despliegue, cada una de las prácticas asociadas permitirán al alumno adquirir los conocimientos básicos del entorno de *cloud* mientras se trabajan contenidos muy básicos de seguridad informática pero que servirán de base para el desarrollo de los siguientes módulos.

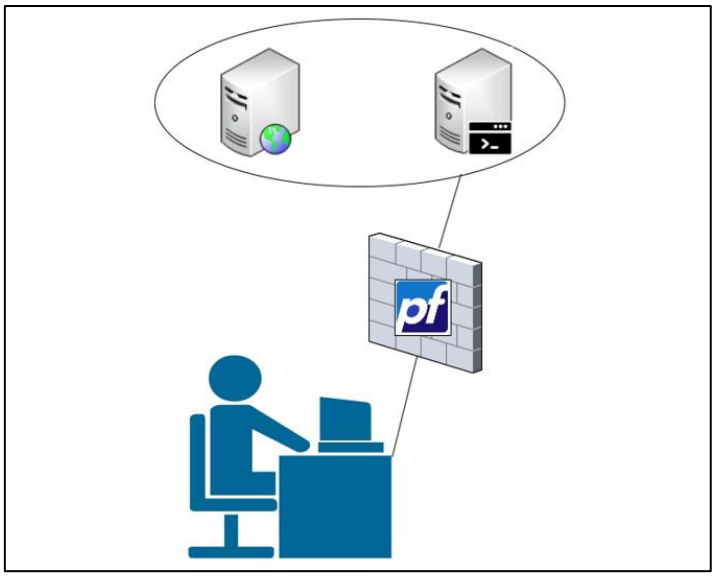


Figura 22. Situación inicial de la simulación del módulo 1

Como vemos en la figura 8, la arquitectura propuesta ofrece un entorno con un firewall perimetral básico de tres zonas, aunque durante el desarrollo de este módulo solo serán necesarias dos de ellas. Este módulo abordará la configuración básica de este tipo de arquitectura, reforzando los conceptos de zona de seguridad en un firewall bastión, y la caracterización que tiene cada tipo de zona, como por ejemplo el propósito de cada una o el nivel de seguridad que la caracteriza.

Finalmente, el módulo abordará el concepto de publicación de servicios en sus dos variantes, mediante la traducción de IP y la redirección de puertos. A continuación, se describe la propuesta de las prácticas que podrán ser realizadas durante el módulo 1.

Tabla 4. Práctica 1 del módulo 1

Práctica 1. Despliegue de un firewall perimetral.	
Descripción:	Despliegue de una instancia de pfSense con tres interfaces que corresponden a zonas básicas de la configuración de un firewall perimetral, WAN, LAN y DMZ.
Objetivos:	• Conocer el entorno de *cloud*. • Introducir conceptos básicos de seguridad como un firewall o sus zonas de seguridad.
Resultados de aprendizaje:	• Adquirir las habilidades adecuadas para trabajar con el entorno de *cloud*. • Adecuar la estructura general de un firewall que realiza la función de bastión en una organización. • Habrán adquirido los conocimientos básicos para diferenciar las características de una red WAN, LAN y DMZ.

Tabla 5. Práctica 2 del módulo 1

Práctica 2. Publicación de servicios: Port address translation (PAT).	
Descripción:	Despliegue de un sistema Debian en el cual se deberá instalar el servidor web Nginx y publicar el servicio SSH y HTTP a través de la ip del propio firewall utilizando la redirección de puertos (PAT).
Objetivos:	• Instalación de un servidor web. • Configuración de PAT sobre un firewall.
Resultados de aprendizaje:	• Instalación de un servicio web. • Configuración de reglas para la redirección de puertos. • Configuración de reglas de control de acceso en el firewall.

Tabla 6. Práctica 3 del módulo 1

Práctica 3. Publicación de servicios: Network address translation (NAT).	
Descripción:	Despliegue de un sistema Debian en el cual se deberá instalar el servidor web Nginx y se publicarán los servicios SSH y HTTP a través del firewall por medio de una IP virtual de forma que todas las peticiones que reciba el firewall sean reenviadas al sistema Linux.
Objetivos:	• Configuración de IP virtuales en el firewall. • Configuración de NAT sobre el firewall.
Resultados de aprendizaje:	• Configuración de IP virtuales en el firewall. • Configuración de la traducción de direcciones de red (NAT). • Configuración de reglas de control de acceso en el firewall.

7.4.2. Módulo 2. Espacio de ejecución seguro

Este segundo módulo, como se ha tratado anteriormente, aborda los conceptos relacionados con el bastionado de sistemas y la securización de entornos de red mediante aplicaciones especializadas en la detección de vulnerabilidades y el desarrollo de plataformas de unificación de logs.

Para el desarrollo de este módulo, se desplegará la arquitectura de la simulación completa, descartando los sistemas creados durante el primer módulo del curso y ofreciendo una primera visión básica del entorno desde el exterior de la red empresarial.

El desarrollo de las prácticas asociados a los contenidos didácticos de este segundo módulo se realizará sobre una infraestructura mixta. Por un lado, el alumno tendrá disponibles las plantillas básicas de sistema operativo necesarias para abordar los contenidos relacionados con el bastionado, junto con una instancia de un sistema Debian con la aplicación Nessus preinstalada que le permitirá realizar el análisis y evaluación de los equipos bastionados.

Por otro lado, se proveerá al alumnado de las credenciales de acceso al sistema Wazuh de la arquitectura final de la simulación. Este acceso se realizará por medio de la interfaz web del servidor Wazuh, publicada a través del firewall perimetral de la simulación.

Es importante mencionar que tanto el firewall de la simulación como el directorio activo están preconfigurados para integrarse con el sistema Wazuh. Por un lado, el firewall está reenviando los logs que genera al servicio de syslog remoto de Wazuh. Por su parte, el directorio activo de la simulación ya lleva el agente de Wazuh preinstalado y configurado para conectarse al servicio. Esta configuración básica de los servidores de la red, permitirán que el alumno conozca el entorno de la aplicación Wazuh y haga la configuración básica del servicio.

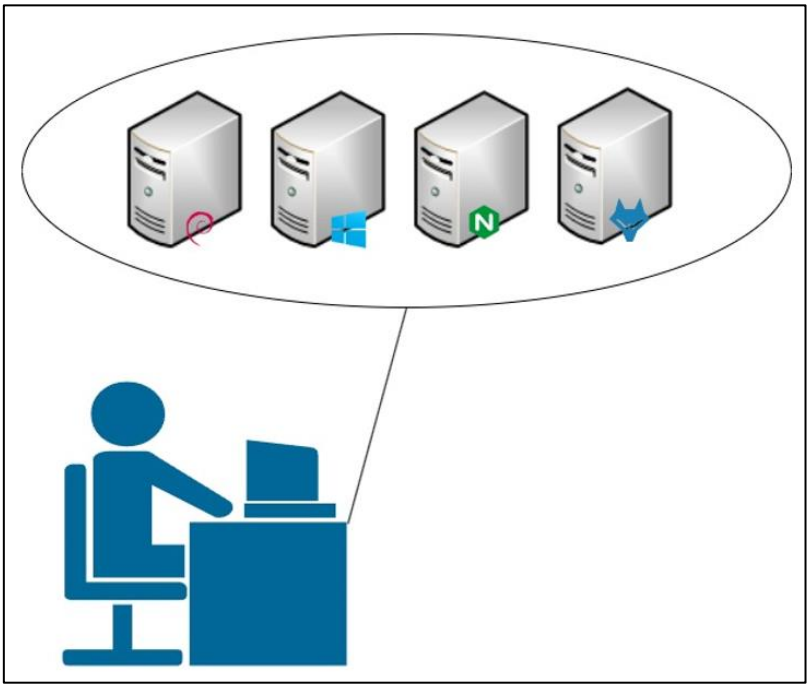


Figura 23. Situación inicial de la simulación del módulo 2

Tabla 7. Práctica 1 del módulo 2

Práctica 1. Bastionado de un OS	
Descripción:	Realizar el bastionado de un sistema operativo en base a la documentación obtenida de fuentes confiables en este ámbito como por ejemplo las guías proporcionadas por el Centro Criptográfico Nacional (CCN-CERT).
Objetivos:	• Realizar el bastionado de un sistema operativo.
Resultados de aprendizaje:	• Conocer el concepto de bastionado o fortificación de un sistema operativo. • Conocer fuentes de documentación adecuadas en el ámbito de la ciberseguridad.

Tabla 8. Práctica 2 del módulo 2

Práctica 2. Bastionado de un servicio	
Descripción:	Ampliación del trabajo realizado en la práctica 1 incluyendo el bastionado de un servicio sobre un sistema operativo ya fortificado.
Objetivos:	• Definir el concepto de servicio frente al de sistema operativo • Implementar las medidas adecuadas para realizar el bastionado del servicio basado en la documentación aportada por una fuente de información confiable.
Resultados de aprendizaje:	• Distinguir el concepto de servicio y sistema operativo. • Conocer los mecanismos de fortificación de un servicio

Tabla 9. Práctica 3 del módulo 2

Práctica 3. Uso de herramientas de detección de vulnerabilidades: NESSUS	
Descripción:	Introducción al uso de herramientas de detección de vulnerabilidades y la generación automática de informes de seguridad.
Objetivos:	• Configurar una herramienta de detección de vulnerabilidades. • Definir un proceso de escaneo utilizando la herramienta Nessus. • Generar un informe de vulnerabilidades.
Resultados de aprendizaje:	• Aprender a configurar una aplicación de escaneo de vulnerabilidades. • Conocer el proceso para realizar un escaneo de vulnerabilidades automatizado. • Generación de un informe de resultados automatizado.

Tabla 10. Práctica 4 del módulo 2

Práctica 4. Configuración básica SIEM: Wazuh	
Descripción:	Configuración básica de un SIEM que permita centralizar y analizar los logs de seguridad de una red.
Objetivos:	• Introducir conceptos básicos como SIEM o logs. • Conocer la herramienta Wazuh. • Realizar la configuración básica de agentes en el sistema. • Realizar la configuración básica para permitir la recepción de logs a través de la red.
Resultados de aprendizaje:	• Conocer el concepto de SIEM y XDR. • Aprender a realizar la configuración básica de un sistema de centralización de logs.

7.4.3. Módulo 3. Hacking ético

Este tercer módulo del curso ofrece contenidos específicos que capacitan al alumnado en el desarrollo de auditorías de seguridad y técnicas de pentesting. El objetivo es que los alumnos adquieran las habilidades necesarias para la ejecución de técnicas que les permitan identificar y explotar vulnerabilidades en sistemas bajo condiciones controladas y respetando un código ético, emulando las actividades que realizan los especialistas que forman parte de los equipos de Red Team.

Tabla 11. Práctica 1 del módulo 3

Práctica 1. OSINT	
Descripción:	Aprender los conceptos necesarios y técnicas básicas en la recolección de información de fuentes públicas (OSINT).
Objetivos:	• Conocer el concepto de OSINT. • Conocer el concepto de fuentes públicas de información. • Aprender técnicas y herramientas de recolección de información de fuentes públicas.
Resultados de aprendizaje:	• Aprender el concepto de OSINT y sus implicaciones. • Identificar y utilizar información extraída de fuentes públicas. • Aplicar técnicas y herramientas para la recolección automatizada de información.

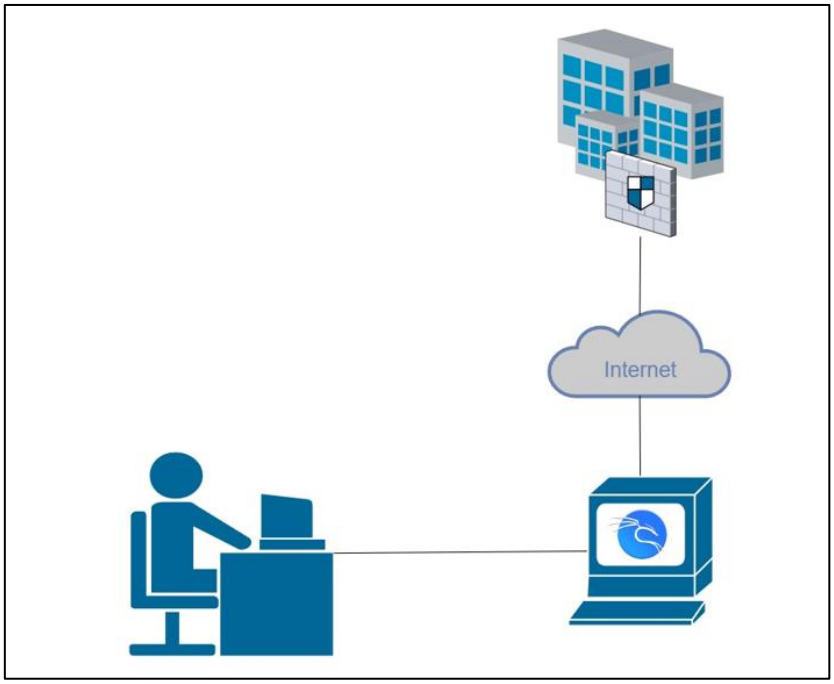


Figura 24. Situación inicial de la simulación de ataque en el módulo 3

Tabla 12. Práctica 2 del módulo 3

Práctica 2. Vulnerabilidades web	
Descripción:	Utilizar técnicas de ataque especializadas para extraer información y atacar sistemas informáticos basados en entorno web.
Objetivos:	• Conocer las principales vulnerabilidades de entorno web • Extraer información de las técnicas de recolección de información focalizando el objetivo en la tienda virtual de la simulación.
Resultados de aprendizaje:	• Aprender a identificar y explotar las principales vulnerabilidades web. • Aplicar técnicas de extracción de información en entornos web.

Tabla 13. Práctica 2 del módulo 3

Práctica 3. Análisis de vulnerabilidades. Nmap, NESSUS	
Descripción:	Aprender a utilizar herramientas de análisis de vulnerabilidades como Nmap y Nessus.
Objetivos:	• Conocer el funcionamiento de las herramientas Nmap y Nessus • Realizar escaneos de red y vulnerabilidades personalizados sobre sistemas operativos.
Resultados de aprendizaje:	• Aprender a identificar vulnerabilidades utilizando las herramientas y técnicas adecuadas según el entorno • Interpretar los resultados de los escaneos extrayendo la información adecuada. • Aprender a generar informes automatizados de los resultados obtenidos tras un escaneo de vulnerabilidades

Tabla 14. Práctica 4 del módulo 3

Práctica 4. Explotación inicial. Metasploit	
Descripción:	Utilizar el framework Metasploit como herramienta para la explotación de vulnerabilidades en sistemas operativos.
Objetivos:	• Conocer el entorno de Metasploit y sus componentes principales. • Conocer y poner en práctica las técnicas de ataque que permitan explotar vulnerabilidades y tomar el control o acceder a áreas del sistema operativo no autorizadas.
Resultados de aprendizaje:	• Identificar entre un conjunto de vulnerabilidades aquellas que permitan definir una estrategia de ataque adecuada. • Configurar adecuadamente los distintos elementos que requiere la ejecución de un *exploit* sobre Metasploit, como por ejemplo la selección de script adecuado para una vulnerabilidad, parámetros asociados y *payload* adecuado según la necesidad del ataque.

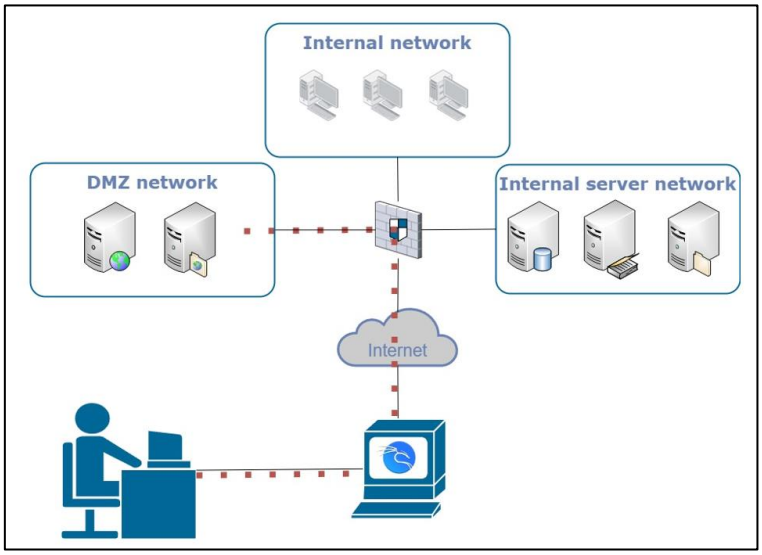


Figura 25. Situación de la simulación del módulo 3 tras la fase de explotación

Tabla 15. Práctica 5 del módulo 3

Práctica 5. Post-explotación 1. Movimiento lateral	
Descripción:	Realizar actividades de post-explotación enfocadas al reconocimiento de la red interna y el movimiento lateral dentro de la red objetivo.
Objetivos:	• Conocer las distintas técnicas que permiten realizar el reconocimiento de la red interna del objetivo (axfr). • Aplicar técnicas para encadenar ataques para alcanzar zonas internas de la red (Proxychains)
Resultados de aprendizaje:	• Utilizar el DNS interno como fuente de información de la estructura interna de la red. • Configurar correctamente el encadenamiento de ataques por medio de la herramienta Metasploit.

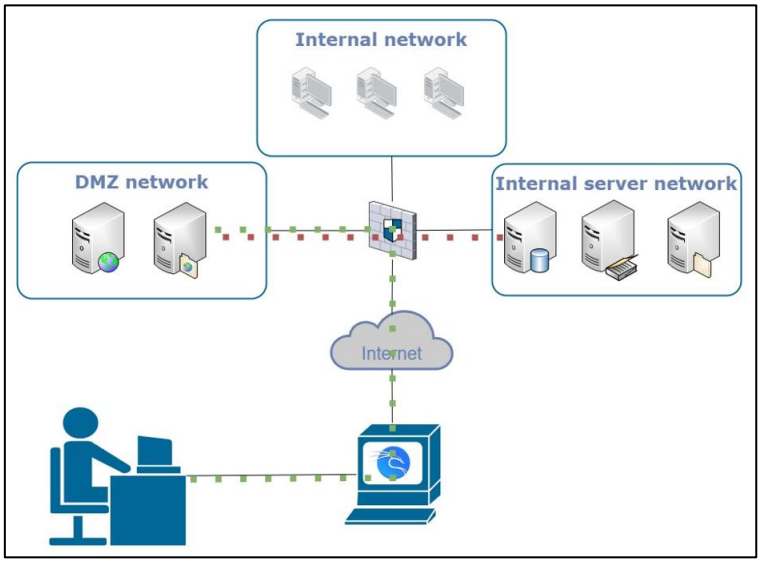


Figura 26. Situación de la simulación del módulo 3 durante la fase de *pivoting*

Tabla 16. Práctica 6 del módulo 3

Práctica 6. Post-explotación 2. Servicios internos	
Descripción:	Ampliar el conjunto de técnicas de ataque visto en la fase de explotación mediante la integración de técnicas de ataque sobre servicios internos como bases de datos bases de datos o el servicio de directorio.
Objetivos:	• Conocer las vulnerabilidades y técnicas de explotación de servicios internos. • Realizar ataques dirigidos a bases de datos o servicios vinculados al directorio activo, como SMB o LDAP.
Resultados de aprendizaje:	• Identificar servicios internos de una red • Realizar técnicas de ataque específicas para explotar vulnerabilidades en servicios internos.

7.4.4. Módulo 4. Gestión y respuesta ante incidentes

Este cuarto módulo del curso se enfoca en las herramientas y actividades relacionadas con la identificación y gestión de incidentes de seguridad. El objetivo de este módulo es que los

alumnos adquieran los conocimientos y habilidades necesarios para detectar, responder, documentar y delimitar el alcance de amenaza de seguridad que puedan surgir en un sistema informático.

Para llevar a cabo todas estas actividades, en este módulo se proporcionará a los alumnos un usuario que les permitirá acceder al entorno completo de la red. Además del acceso, se le proporcionarán las credenciales de todos los sistemas para que pueda realizar el análisis de todos ellos durante el desarrollo de las prácticas.

Uno de los recursos básicos de los que dispondrá el alumno es el SIEM implantado con Wazuh. Este sistema, configurado durante el desarrollo del módulo 2 para centralizar los logs del firewall y el directorio activo, permitirán trazar las actividades maliciosas realizadas durante el módulo 3. Toda la información recopilada servirá para finalizar el módulo realizando un informe sobre el incidente y planteando las propuestas de solución que sean necesarias.

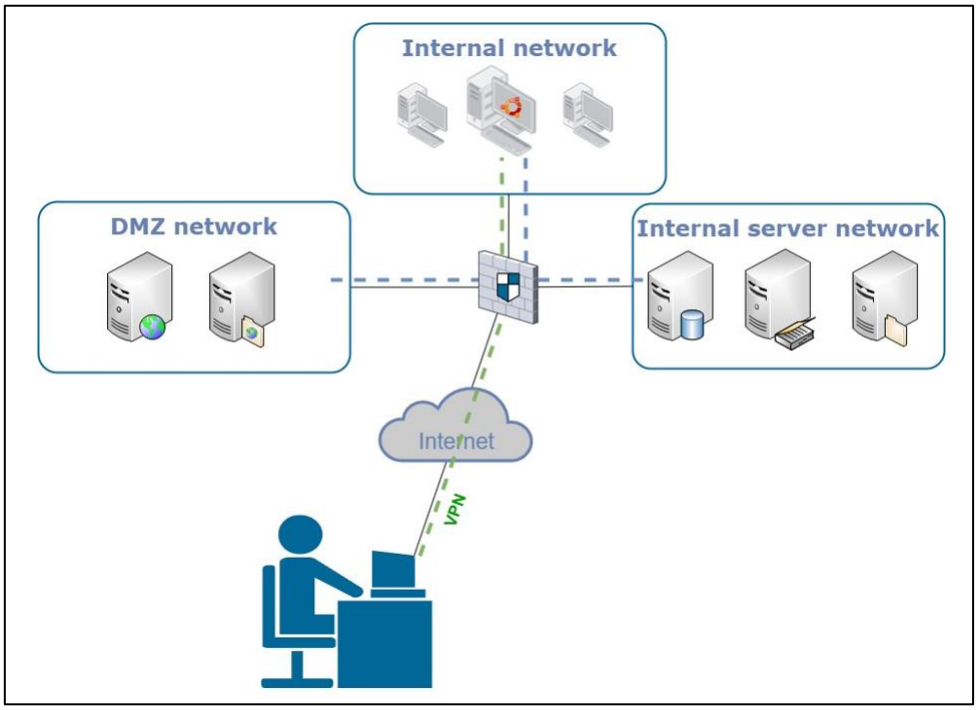


Figura 27. Situación inicial de la simulación en el módulo 4

Tabla 17. Práctica 1 del módulo 4

Práctica 1. Detección de Incidentes	
Descripción:	Acceder a los logs centralizados en el SIEM para identificar patrones de comportamiento sospechoso o anómalo que sirvan para identificar incidentes de seguridad.
Objetivos:	• Aprender a identificar amenazas y clasificar incidentes de seguridad.
Resultados de aprendizaje:	• Conocer el entorno y las características de un SIEM • Aprender a crear filtros y reglas de búsqueda de eventos • Aprender a identificar y clasificar incidentes de seguridad

Tabla 18. Práctica 2 del módulo 4

Práctica 2. Análisis Forense	
Descripción:	Realizar el análisis forense de los sistemas vulnerados en el desarrollo del módulo 3 para aprender a rastrear el origen y la cadena de eventos que llevaron al compromiso del sistema.
Objetivos:	• Aprender técnicas de análisis forense básicas.
Resultados de aprendizaje:	• Aprender los conceptos básicos del análisis forense de un sistema informático. • Adquirir las capacidades necesarias para rastrear y reconstruir la cadena de eventos de seguridad que conlleva un incidente de seguridad. • Aprender y aplicar el concepto de correlación de eventos para obtener una visión completa de la sucesión de eventos que se producen en un incidente de seguridad.

Tabla 19. Práctica 3 del módulo 4

Práctica 3. Contención, mitigación y recuperación	
Descripción:	Simulación de un ataque sobre uno de los sistemas vulnerables de forma que los estudiantes puedan aprender los procedimientos que se deben seguir para contener este tipo de amenazas.
Objetivos:	• Aprender a definir y aplicar un plan de respuesta ante incidentes. • Conocer medidas para contener o mitigar ataques.
Resultados de aprendizaje:	• Adquirir la capacidad para evaluar el impacto de ataque. • Conocer las acciones que se pueden ejecutar en el proceso de contención o mitigación de un incidente de seguridad.

Tabla 20. Práctica 4 del módulo 4

Práctica 4. Creación de Reglas de Detección Personalizadas	
Descripción:	Los estudiantes aprenderán a crear reglas personalizadas en el servidor Wazuh para detectar tipos de ataques específicos y comportamientos anómalos concretos en el entorno de red de la simulación.
Objetivos:	• Aprender el proceso de creación personalizada de reglas sobre el SIEM.
Resultados de aprendizaje:	• Conocer el formato de reglas que permite personalizar el sistema. • Aprender a crear, implantar y probar reglas en el entorno de Wazuh.

7.5 Proceso de automatización del despliegue del sistema

Como se ha comentado en los puntos anteriores, el desarrollo de la configuración del sistema se ha basado en la creación de todas las plantillas preconfiguradas de los distintos servicios que componen el sistema sobre la plataforma de *cloud*. Por otro lado, para automatizar los procesos de despliegue en entornos de *cloud* podemos encontrar varias soluciones que permiten la ejecución de infraestructura como código (IaC). Una de estas soluciones es Terraform, que además tiene soporte para OpenNebula, nuestro sistema de *cloud*.

Terraform es una herramienta de software que tiene como principal característica la creación de infraestructura en sistemas de *cloud* de forma declarativa, es decir, definiendo una serie de objetos y recursos en una estructura de archivos que permiten definir las

características y configuración de los despliegues. Por lo tanto, de forma general, el proceso de automatización del despliegue de un entorno basado en Terraform consiste en la creación de una estructura de directorios adecuada junto con un conjunto de archivos estructurados según el lenguaje HCL, lenguaje creado específicamente por HashiCorp (los desarrolladores del software), de forma que la aplicación los interpreta y aplica las configuraciones adecuadas sobre un entorno de *cloud*, ya sea público o como es nuestro caso un *cloud* privado.

El uso de Terraform como herramienta para la automatización de despliegues en sistemas de cloud es bastante sencillo, aunque requiere conocer el funcionamiento de la herramienta y estructurar correctamente el sistema de archivos que soportará la solución. El primer paso para poner en funcionamiento la aplicación es realizar la instalación. Este proceso para un sistema Debian, que es nuestro caso, se realiza con el procedimiento estándar de instalación mediante la inclusión de las fuentes adecuadas en el archivo sources.list y el comando apt. A continuación, se puede observar la secuencia de comandos realizada extraída desde la web de los desarrolladores:

```
wget -O- https://apt.releases.hashicorp.com/gpg | sudo gpg --dearmor -o
/usr/share/keyrings/hashicorp-archive-keyring.gpg

echo "deb [signed-by=/usr/share/keyrings/hashicorp-archive-keyring.gpg]
https://apt.releases.hashicorp.com $(lsb_release -cs) main" | sudo tee
/etc/apt/sources.list.d/hashicorp.list

sudo apt update && sudo apt install terraform
```

Una vez instalada la herramienta es necesario estructurar los directorios de la aplicación en función de los procesos de despliegue que se realizarán. En nuestro caso se ha creado una estructura de directorios de tres niveles. El último nivel que se corresponde con los procesos de despliegue que se realizarán, en nuestro caso se desplegará infraestructura al inicio del módulo 2 y del módulo 3. Este tercer nivel, contiene los ficheros que permiten definir la configuración del entorno que se quiere realizar. A continuación, se muestra la estructura completa realizada:

```
/terraform
      /sinhackcorp
            /module2
                  /main.tf
                  /provider.tf
                  /tf.tfvars
                  /variables.tf
            /module3
                  /main.tf
                  /provider.tf
                  /tf.tfvars
                  /variables.tf
```

Los archivos que se han definido y que permiten automatizar el despliegue para varias infraestructuras son los siguientes:

- `provider.tf`: Este primer archivo proporciona a la aplicación la información referente al proveedor de *cloud* que se utilizará y los parámetros de conexión con el entorno.

```
terraform {
  required_providers {
    opennebula = {
      source = "OpenNebula/opennebula"
      version = "~> 1.4"
    }
  }
}
provider "opennebula" {
  endpoint  = "http://localhost:2633/RPC2"
  username  = "username"
  password  = "Your_Secure.Password"
}
```

- `main.tf`: Este archivo es el que contiene la definición de los recursos que se desplegarán durante la ejecución. Para poder realizar el despliegue de varias arquitecturas hay que generalizar por medio de variables los distintos parámetros que no serán comunes para cada arquitectura. A continuación, se incluye como ejemplo una versión reducida de ejemplo del main.tf del módulo 2 (puede consultarse la versión completa del archivo en el Anexo correspondiente). Esta versión solo incluye un recurso a modo de ejemplo, pero generaliza el proceso de despliegue para varios sistemas utilizando la estructura de variables y la asignación de valores creada en los archivos `varibales.tf` y `tf.tfvar` respectivamente, que serán comentados posteriormente.

```
resource "opennebula_virtual_machine" "pfSense_SimHackCorp" {
  count       = length(lab_sets)
  name        = "Pfsense.SimHackCorp.lab_${count.index}"
  template_id = 59
  group       = var.lab_sets[count.index].group_name
  permissions = "600"

  context = {
    USER_NAME  = var.lab_sets[count.index].user_name
    GROUP_NAME = var.lab_sets[count.index].group_name
  }
  nic {
    network_id = var.lab_sets[count.index].network_id_wan
  }
  nic {
    network_id = var.lab_sets[count.index].network_id_lan
  }
  nic {
    network_id = var.lab_sets[count.index].network_id_dmz
  }
  nic {
    network_id = var.lab_sets[count.index].network_id_servers
  }}
```

- `varibales.tf`: Este tercer archivo declara las variables que serán utilizadas en el archivo main para generalizar su ejecución para varias arquitecturas.

```
variable "lab_sets" {
  description = "List of sets"
  type = list(object({
    user_name         = string
    group_name        = string
    network_id_wan    = string
    network_id_lan    = string
    network_id_dmz    = string
    network_id_servers = string
  }))
}
```

- `tf.tfvar`: Finalmente el último archivo que utilizaremos durante el despliegue, permite definir los valores para las distintas variables de cada uno de los sets de recursos que se corresponderán con las distintas arquitecturas que coexistirán de forma simultánea en el entorno.

```
lab_sets = [
  {
    user_name         = "username"
    group_name        = "groupname"
    network_id_wan    = "93"
    network_id_lan    = "244"
    network_id_dmz    = "245"
    network_id_servers = "248"
  },
  {
    user_name         = "other_username"
    group_name        = "other_ groupname"
    network_id_wan    = "92"
    network_id_lan    = "234"
    network_id_dmz    = "235"
    network_id_servers = "238"
  }
]
```

Una vez se han estructurado los directorios y se ha definido adecuadamente su contenido, la ejecución del despliegue se realiza por medio de 3 comandos:

- `terraform init`: este comando se ejecuta desde el directorio donde se encuentra el proyecto, en nuestro se ha ejecutado dos veces una por cada uno de los módulos donde se desplegará la infraestructura.

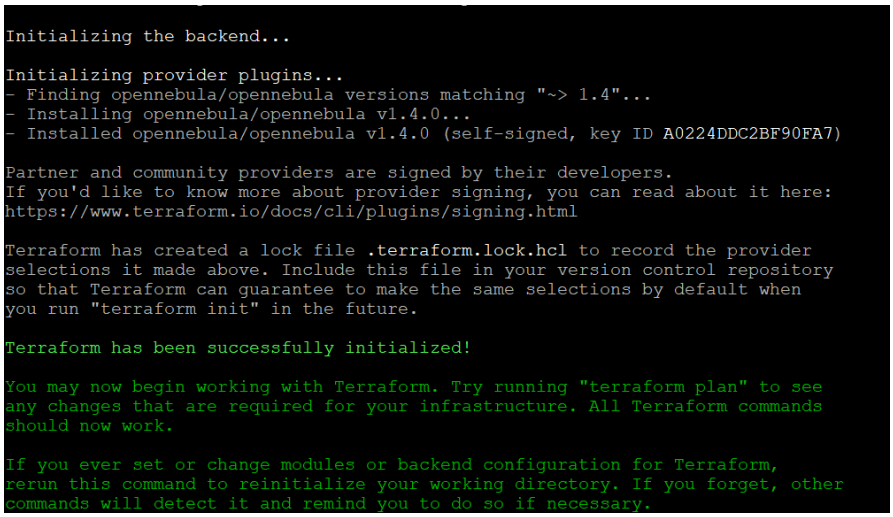


Figura 28. Resultado de la ejecución del comando de inicialización del despliegue

- `terraform plan:` Este segundo comando planifica el despliegue de la infraestructura. El parámetro -out permite generar la planificación de la infraestructura que se va a generar y se almacena en un archivo que servirá posteriormente para realizar el despliegue según las especificaciones indicadas por plan. En concreto el comando utilizado en nuestro caso será el siguiente:

```
terraform plan -var-file="tf.tfvars" -parallelism=2 -out module2.out
```

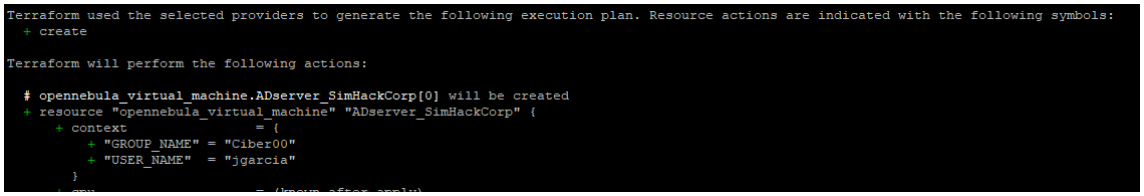


Figura 29. Inicio de la ejecución de la planificación del despliegue

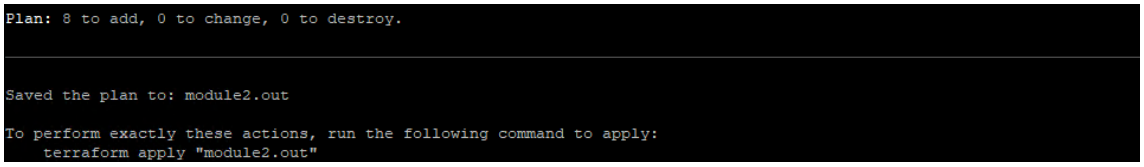


Figura 30. Finalización de la ejecución del comando de planificación

- `terraform apply:` El tercer comando, es el que finalmente lanza la infraestructura definida en el fichero module2.out, generado con el comando de planificación. Este último comando, inicia el proceso de creación de las instancias definidas y muestra como salida, un mensaje por cada instancia que se está desplegando y el tiempo que ha pasado desde la ejecución del comando. En concreto el comando utilizado en nuestro caso será el siguiente:

```
terraform apply -parallelism=2 “module2.out”
```

```
opennebula_virtual_machine.pfSense_SimHackCorp[0]: Creating...
opennebula_virtual_machine.pfSense_SimHackCorp[1]: Creating...
opennebula_virtual_machine.pfSense_SimHackCorp[0]: Still creating... [10s elapsed]
opennebula_virtual_machine.pfSense_SimHackCorp[1]: Still creating... [10s elapsed]
opennebula_virtual_machine.pfSense_SimHackCorp[0]: Still creating... [20s elapsed]
opennebula_virtual_machine.pfSense_SimHackCorp[1]: Still creating... [20s elapsed]
```

Figura 31. Inicio de la salida por pantalla tras la inicialización del despliegue

```
opennebula_virtual_machine.Wazuh_SimHackCorp[1]: Still creating... [3m20s elapsed]
opennebula_virtual_machine.Wazuh_SimHackCorp[1]: Still creating... [3m30s elapsed]
opennebula_virtual_machine.Wazuh_SimHackCorp[1]: Still creating... [3m40s elapsed]
opennebula_virtual_machine.Wazuh_SimHackCorp[1]: Creation complete after 3m49s [id=2884]

Apply complete! Resources: 8 added, 0 changed, 0 destroyed.
```

Figura 32. Salida por pantalla tras la finalización del despliegue

Finalmente, al acabar el proceso de despliegue, vemos en la infraestructura que se han generado las instancias correspondientes al módulo 2 del curso.

ID	Name	Owner	Group	Status	Host	IPs	Charter
2884	Wazuh.SimHackCorp.lab_1	[redacted]	Ciber01	RUNNING	ClusterON	0:02:00:17:fd:f8:c2	
2883	ADserver.SimHackCorp.lab_0	jgarcia	Ciber00	RUNNING	ClusterON	0:02:00:13:c9:26:b5	
2882	Wazuh.SimHackCorp.lab_0	jgarcia	Ciber00	RUNNING	ClusterON	0:02:00:8d:6a:95:16	
2881	ADserver.SimHackCorp.lab_1	[redacted]	Ciber01	RUNNING	ClusterON	0:02:00:86:40:b6:67	
2880	Nessus.SimHackCorp.lab_1	[redacted]	Ciber01	RUNNING	ClusterON	0:02:00:86:40:b6:66	
2879	Nessus.SimHackCorp.lab_0	jgarcia	Ciber00	RUNNING	ClusterON	0:02:00:13:c9:26:b4	
2878	Pfsense.SimHackCorp.lab_1	[redacted]	Ciber01	RUNNING	ClusterON	0:02:00:7c:51:95:2a	
2877	Pfsense.SimHackCorp.lab_0	jgarcia	Ciber00	RUNNING	ClusterON	0:02:00:58:d3:70:88	

Figura 33. Sistemas desplegados automáticamente correspondientes al módulo 2

Al realizar el mismo proceso para los recursos del módulo 3, se generan las 4 instancias que complementarán a las anteriores según la definición de la arquitectura realizada.

ID	Name	Owner	Group	Status	Host	IPs
2892	DDBBserver.SimHackCorp.lab_1	[redacted]	Ciber01	RUNNING	ClusterON	0:02:00:86:40:b6:68
2891	DDBBserver.SimHackCorp.lab_0	jgarcia	Ciber00	RUNNING	ClusterON	0:02:00:13:c9:26:b6
2890	OnlineShop.SimHackCorp.lab_0	jgarcia	Ciber00	RUNNING	ClusterON	0:02:00:8d:6a:95:18
2889	OnlineShop.SimHackCorp.lab_1	[redacted]	Ciber01	RUNNING	ClusterON	0:02:00:17:fd:f8:c4
2888	Intranet.SimHackCorp.lab_0	jgarcia	Ciber00	RUNNING	ClusterON	0:02:00:8d:6a:95:17
2887	Kali.SimHackCorp.lab_0	jgarcia	Ciber00	RUNNING	ClusterON	0:02:00:98:a5:6b:05
2886	Intranet.SimHackCorp.lab_1	[redacted]	Ciber01	RUNNING	ClusterON	0:02:00:17:fd:f8:c3
2885	Kali.SimHackCorp.lab_1	[redacted]	Ciber01	RUNNING	ClusterON	0:02:00:98:a5:6a:fe

Figura 34. Sistemas desplegados automáticamente correspondientes al módulo 3

Una vez la arquitectura finaliza su ciclo de vida, Terraform permite eliminar los conjuntos creados por medio de la parametrización adecuada del comando utilizando la acción *destroy*. A continuación, tenemos un ejemplo de uso del comando:

```
terraform destroy -var-file="tf.tfvars" -parallelism=4
```

```
Terraform used the selected providers to generate the following execution plan. Resource actions are indicated with the following symbols:
  - destroy

Terraform will perform the following actions:

  # opennebula_virtual_machine.ADserver_SimHackCorp[0] will be destroyed
  - resource "opennebula_virtual_machine" "ADserver_SimHackCorp" {
      - context                 = {
          - "GROUP_NAME" = "Ciber00"
          - "USER_NAME"  = "jgarcia"
        } -> null
```

Figura 35. Información mostrada por Terraform al planificar un proceso de eliminación

```
Plan: 0 to add, 0 to change, 8 to destroy.

Do you really want to destroy all resources?
  Terraform will destroy all your managed infrastructure, as shown above.
  There is no undo. Only 'yes' will be accepted to confirm.

  Enter a value: yes

opennebula_virtual_machine.Wazuh_SimHackCorp[1]: Destroying... [id=2884]
opennebula_virtual_machine.Wazuh_SimHackCorp[0]: Destroying... [id=2882]
opennebula_virtual_machine.Nessus_SimHackCorp[0]: Destroying... [id=2879]
opennebula_virtual_machine.pfSense_SimHackCorp[1]: Destroying... [id=2878]
opennebula_virtual_machine.Wazuh_SimHackCorp[1]: Still destroying... [id=2884, 10s elapsed]
opennebula_virtual_machine.Wazuh_SimHackCorp[0]: Still destroying... [id=2882, 10s elapsed]
```

Figura 36. Inicio del proceso de eliminación del entorno

```
opennebula_virtual_machine.pfSense_SimHackCorp[0]: Still destroying... [id=2877, 50s elapsed]
opennebula_virtual_machine.pfSense_SimHackCorp[0]: Destruction complete after 54s

Destroy complete! Resources: 8 destroyed.
```

Figura 37. Mensaje final tras la eliminación del entorno

Finalmente, cabe mencionar que, al realizar las pruebas del despliegue mediante el proceso de automatización mencionado, se han detectado varias situaciones que deberán ser abordadas antes de utilizar el sistema en un entorno de aprendizaje real. En primer lugar, las instancias genéricas utilizadas pierden la configuración de red lo que obliga a reconfigurarlas tras la finalización del proceso de despliegue.

Por otro lado, al desplegar varias instancias de la simulación, el direccionamiento que se asigna dinámicamente al firewall de la simulación en su red WAN, que depende del direccionamiento asignado dinámicamente por la red del entorno de cloud, y que es el punto de entrada al entorno creado, cambia de rango IP en función de la red WAN que se le asigna. Este cambio implica que la publicación de los servicios realizada por medio de la configuración NAT no sea correcta.

Para abordar ambos inconvenientes se puede reconfigurar de forma manual los direccionamientos y la configuración de la publicación de los servicios tras el despliegue inicial para adecuarlos al nuevo direccionamiento. Dado que el objetivo es la automatización completa del sistema, la solución adecuada que deberá ser abordada en un proceso de revisión del sistema previo a su implantación en un entorno formativo real, es el uso de las capacidades de contextualización que proporciona el entorno de *cloud*.

Como se ha comentado inicialmente, en la descripción del entorno de *cloud*, se ha tomado una decisión de diseño que es la no contextualización de la red de las instancias desplegadas. Esta configuración favorece el control de los alumnos sobre el direccionamiento de los sistemas. Debido a esto debemos definir otra estrategia para abordar la reconfiguración mencionada. Para ello, OpenNebula ofrece otra característica que consiste en la ejecución de scripts tras el despliegue de las instancias. Por lo tanto, en nuestro caso, el proceso de contextualización adecuado para nuestro entorno sería la ejecución de una serie de *scripts* que configuren las instancias tras el despliegue inicial de las para adecuar sus configuraciones de red según las necesidades específicas.

7.6 Gamificación del entorno

El proceso de gamificación del entorno propuesto se basa en una práctica habitual de los retos sobre ciberseguridad, el CTF (capture de flag). Este tipo de retos muy característico de los sistemas vulnerables que se suelen utilizar como entorno de aprendizaje orientados al pentesting, consiste en buscar determinadas "banderas" que se encuentran ocultas en los sistemas que se están vulnerando. Estas flags son secuencias de caracteres que deben ser encontradas por medio de la aplicación de distintas técnicas de ataque que permiten acceder a zonas del sistema o la aplicación que deberían estar protegidas. Este tipo de retos fomentan el interés ya que proporcionan un desafío adicional sobre el entorno y ayuda a que los estudiantes practiquen y refuercen sus habilidades en un contexto práctico y competitivo, incrementando así su motivación y compromiso con el aprendizaje.

En nuestra arquitectura, se ha implementado la gamificación como un reto de CTF a lo largo de toda la red, que se realizará en paralelo al desarrollo del contenido del módulo 3, Hacking ético. Al inicio de este tercer módulo del curso, se presentará el reto que consiste en encontrar un conjunto de banderas que se encuentran escondidas en distintos elementos de la red. Cada una de estas banderas tendrá asociada una puntuación que variará en función de la complejidad de su captura. El alumno podrá acceder a estas banderas atacando los distintos elementos que componen el sistema y con ello accediendo a la secuencia de caracteres que componen cada una de las *flags*. Concretamente se han escondido banderas en los siguientes servicios y servicios:

- intranet.simhackcorp.lab
    - Se ha incluido una *flag* en la raíz del servidor web.
    - Se ha incluido una *flag* en el archivo robots.txt del servicio web.
    - Se ha incluido una *flag* en la raíz del servidor ftp.
    - Se ha incluido una *flag* en la carpeta del usuario root.
- ddbbserver.simhackcorp.lab
    - Se ha incluido una *flag* en la carpeta del usuario root del servidor.
    - El timestamp asociado a la decodificación del registro que se encuentra en la base de datos será considerada una *flag*.
- ADserver.SimHackCorp.lab
    - Servidor DNS. Se ha creado un registro DNS de tipo txt que devuelve una cadena de caracteres. La flag podrá ser alcanzada utilizando el ataque axfr que devolverá la copia completa de la zona DNS del servidor.
    - En la carpeta de documentos del administrador del sistema se ha añadido un archivo denominado "flag.txt".
    - Se ha compartido una unidad de red oculta que tiene otro archivo "flag.txt".

Figura 38. Vista previa de la tabla de clasificación del reto CTF

Como elemento adicional, el sistema proveerá un entorno web que ofrecerá un *ranking* basado en la puntuación obtenida por cada jugador. Este elemento se basará en un diseño que utilizará la criptografía asimétrica y generación de resúmenes de archivos (hash). Utilizando estos dos mecanismos criptográficos de forma adecuada, se consigue que la aplicación lleve el control de las puntuaciones, evitando el uso de contraseñas y asegurando el proceso de gestión de las banderas y asignación de las puntuaciones.

Para implementar estos mecanismos de autenticación y validación, inicialmente el servidor deberá almacenar un archivo con los hashes de las distintas flags así como la puntuación de cada una de ellas. Además, el servidor también generará una pareja de claves que serán utilizadas posteriormente durante el registro y el proceso de validación de las banderas. La clave pública correspondiente al servidor deberá quedar accesible en la web para que los jugadores puedan descargarla en el momento que vayan a utilizarla.

Por su parte, previo al inicio del registro, el jugador deberá generar un par de claves propias. Posteriormente, al acceder al entorno web el jugador accederá al formulario de registro que le permitirá elegir su nombre de usuario y subir el archivo con su clave pública. El registro quedará completo una vez la aplicación vincule el nombre de usuario con la clave pública del jugador.

Figura 39. Vista previa del diseño de la interfaz del reto CTF

Este tipo de registro permite que el proceso de autenticación del jugador que quiera validar una bandera y adquirir la puntuación asociada se realice utilizando su clave privada como mecanismo de autenticación, añadiendo valor al sistema como prueba práctica de las posibilidades que ofrece la criptografía asimétrica. Basándonos en el funcionamiento de la criptografía de clave asimétrica, el diseño de la página de validación de bandera contendrá dos campos, el primero de ellos, un campo de texto donde el jugador deberá introducir su nombre de usuario. El segundo campo de texto se corresponderá con el espacio definido para que el jugador incluya la secuencia de caracteres correspondiente al cifrado y firma de la bandera. Para obtenerlo, el jugador tendrá que realizar un paso previo que consistirá en cifrar la bandera con la clave pública del servidor, que habrá descargado previamente, y firmarla utilizando su clave privada.

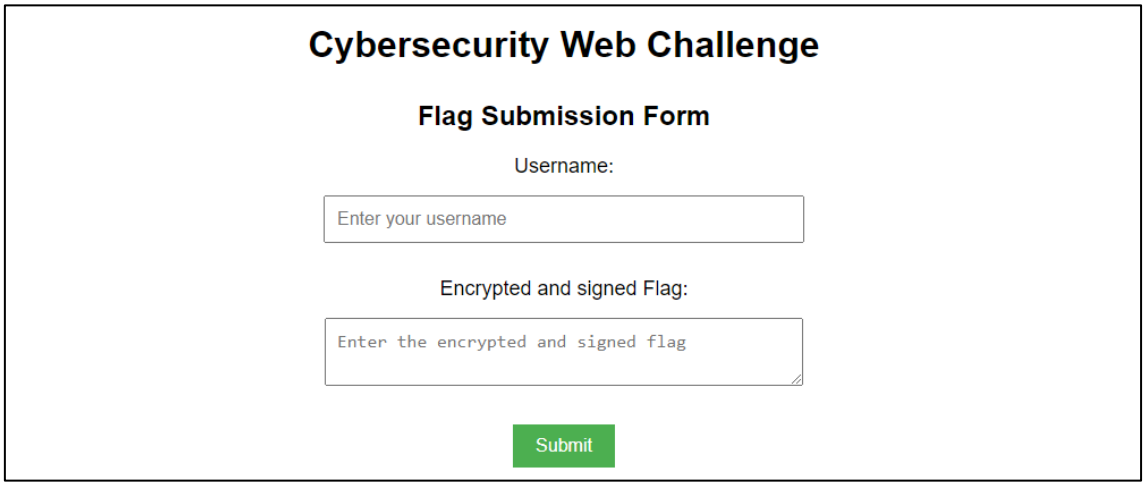


Figura 40. Vista previa del formulario de *submit* del reto de CTF

Según la mecánica definida, el jugador podrá ir acumulando puntos en su casillero del *ranking* adquiriendo las distintas banderas escondidas por la red. Una vez se capture una bandera, según lo comentado sobre el proceso de validación de bandera, el jugador deberá acceder a la página del entorno web de validación y rellenar los campos solicitados: la cadena de caracteres correspondiente a su nombre y el bloque de texto que contendrá el cifrado y firma de la bandera. Tras realizar el envío, el sistema de puntuación validará mediante la clave pública del usuario que la firma se corresponde con la del jugador, realizando el proceso de autenticación. Posteriormente, se descifrará el contenido del mensaje mediante la clave privada del servidor. Por último, el servidor calculará el hash de la bandera proporcionada por el jugador y lo comparará con el listado de hashes que tiene almacenados correspondiente a las banderas registradas inicialmente en la aplicación. De esta forma el servidor comprobará que efectivamente el jugador ha enviado una de las *flags* y se acumulará la puntuación establecida para esa bandera a la puntuación total del jugador. Tras la asignación de la puntuación al usuario, se actualizará el *ranking* y el resto de los participantes podrán consultar el nuevo estado de la competición.

Cabe destacar que en el momento actual el desarrollo del *ranking* está en una fase preliminar y solo se dispone de una vista previa del diseño de la interfaz. La implementación final de la aplicación requerirá incluir toda la mecánica mencionada anteriormente para la gestión de las claves de los jugadores, la generación de hashes en el servidor y los mencionados procesos de comprobación de firma y descifrado de la *flag*.

8. Resultados

Como hemos visto durante el desarrollo, el presente trabajo ha abordado la creación de una simulación de red empresarial orientada a ser utilizada como laboratorio de prácticas de formaciones especializadas en ciberseguridad. De forma general, podemos determinar que los resultados obtenidos cumplen adecuadamente con los objetivos planteados al inicio de este trabajo, ofreciendo una versión inicial del entorno apropiada para el propósito planteado.

A continuación, se propone un análisis de los objetivos y los distintos recursos proporcionados en el desarrollo del trabajo, destacando cómo estos elementos permiten cubrir y validar la consecución de los mismos:

- **Desarrollar una arquitectura de sistema que cumpla con las especificaciones necesarias para crear un entorno simulado que ofrezca los recursos necesarios para abordar los contenidos didácticos establecidos en una formación orientada hacia la ciberseguridad**.
  El resultado de la consecución de este primer objetivo queda constatado a través del diseño de la arquitectura proporcionado en el apartado 5 del capítulo 6, el cual queda plasmado en la figura 7. Adicionalmente, en el apartado 5 del capítulo 7, se realiza una propuesta de prácticas adaptadas a los contenidos didácticos definidos en el capítulo 4 y que pueden ser realizadas sobre los recursos proporcionados por la simulación de red implementada.
- **Preparar el software y los elementos necesarios para la automatización del despliegue de la simulación**.
  La consecución de este objetivo queda constatada mediante el proceso de automatización del despliegue visto en el apartado 4 del capítulo 7. Este capítulo define el proceso de despliegue de la simulación utilizando Terraform como software de automatización de las operaciones sobre el cloud. En este sentido, es importante mencionar que se ha detectado un problema durante las pruebas del proceso de despliegue. Como se comenta al final del apartado 4 del capítulo 7, el problema puede ser solventado de forma manual tras el despliegue, pero dado que el objetivo principal del proceso es la facilidad de uso y reutilización del entorno, será necesario realizar un proceso de revisión de la arquitectura previo a su puesta en práctica en una edición real de la formación, para solventar el problema según la solución propuesta en el citado apartado.
- **Desarrollar la documentación necesaria para la utilización del sistema por parte de los usuarios**.
  Este objetivo ha sido abordado y realizado mediante la generación de un conjunto de entregables que permiten documentar la arquitectura y todos los requisitos para su implantación, despliegue y utilización posterior. Estos entregables pueden ser consultados en el anexo III de esta memoria.
- **Desarrollar un proceso de gamificación de la infraestructura como elemento motivacional sobre el proceso de aprendizaje**.
  Este objetivo ha sido desarrollado en el apartado 6 del capítulo 7, que ha dado como resultado un proceso de gamificación que consiste en la creación de una competición enfocada en ciberseguridad basada en retos de CTF.

- **Elaborar una memoria que documente el trabajo realizado para poder adaptarla posteriormente a otras titulaciones o especializaciones**. Finalmente, la presente memoria cumple con el requisito establecido en el último objetivo del trabajo.

Como conclusión sobre los resultados obtenidos, el trabajo ha abordado cada uno de los objetivos planteados y, salvo un mínimo error detectado en el proceso de despliegue automatizado, se ha obtenido un sistema que cumple a la perfección con los requisitos planteados.

9. Conclusiones

A lo largo del presente trabajo se ha desarrollado la arquitectura de una red empresarial que sirve como entorno de simulación orientado a la formación especializada en ciberseguridad. La arquitectura desarrollada incluye todos los elementos y servicios básicos que encontramos habitualmente en una organización que basa su modelo de negocio en la venta de productos por internet.

Como se ha visto durante el desarrollo del trabajo y se ha detallado en el capítulo de resultados, el sistema implantado cumple con los requisitos establecidos para el desarrollo de formaciones especializadas en ciberseguridad en un entorno empresarial simulado. Este entorno permitirá que el alumnado que curse la formación obtenga una visión global de un sistema completo, proporcionándoles una experiencia de aprendizaje innovadora que les ofrezca una visión realista sobre las estructuras e interacciones que se producen entre los distintos elementos que componen las arquitecturas de las redes empresariales reales.

Por otro lado, la propuesta de prácticas definida establece un buen punto de partida para que los docentes que impartan la formación desarrollen contenidos específicos sobre ciberseguridad. Cabe mencionar que la arquitectura definida también abre la puerta a la creación de otros recursos didácticos no contemplados en esta primera versión de la propuesta de prácticas, los cuales podrán ser propuestos y definidos por los docentes que impartan la formación. Además, es importante destacar que, tal y como está definida la arquitectura del sistema, basada en un conjunto de instancias independientes, el entorno es totalmente modular, lo que facilita su adaptación a nuevos requisitos que puedan surgir en futuras revisiones, como por ejemplo, la sustitución de algunos servicios o la inclusión de nuevos elementos en el diseño.

También es importante mencionar el proceso de automatización del despliegue del entorno desarrollado. Aunque se requerirá un proceso de depuración previo a la implantación, el proceso de automatización definido, junto con las características del diseño de la arquitectura, permiten el despliegue de varias instancias del entorno que pueden coexistir simultáneamente. Este punto es de vital importancia debido a que una formación en ciberseguridad como la definida en este documento está pensada para ser impartida a un grupo de alumnos que utilizan los recursos compartidos que les proporciona el mismo entorno de *cloud*. Por último, cabe señalar que el proceso de automatización definido también favorece realizar el despliegue en sucesivas ediciones de la formación en ciberseguridad.

Finalmente, se ha incluido un elemento adicional que permitirá motivar al alumnado sobre la formación que está realizando y con ello mejorar la asimilación de contenidos. Este elemento es un proceso de gamificación basado en una competición de CTF, desarrollado a través de toda la arquitectura de la simulación. La implementación del reto, además de los beneficios evidentes vinculados a la gamificación, cuenta con una ingeniosa propuesta para la interfaz web de gestión de la tabla de clasificación, basada en el uso de criptografía asimétrica, lo que permite evitar el uso de credenciales y bases de datos. Este diseño de la interfaz permitirá reforzar y consolidar entre el alumnado que la utilice los conceptos y beneficios que aporta este tipo de criptografía.

10. Futuras líneas de trabajo

El trabajo realizado ofrece una gran cantidad de opciones de desarrollo y líneas de trabajo adicionales que permitan su evolución o incluso su adaptación hacia otras especialidades de formación en el ámbito de las TIC. A continuación, se presentan algunas de estas líneas que podrán ser seguidas a futuro con el objetivo de mejorar y ampliar el desarrollo realizado en este trabajo:

1. **Realización de un desarrollo específico de los sistemas genéricos vulnerables empleados durante este trabajo.** Esta línea de trabajo permitía personalizar el contenido y las vulnerabilidades de los sistemas para adecuarlos a necesidades futuras específicas de los docentes. Además, este desarrollo también permitiría modificar el contenido que ofrecen los servicios para adecuar o mejorar la contextualización del entorno con la narrativa definida, lo que favorece el realismo de la simulación.
2. **Creación de niveles de dificultad del proceso de auditoría del entorno.** Otra línea de trabajo interesante consistiría en la creación de niveles de dificultad en el proceso de auditoría. Esta línea de trabajo permitiría evolucionar el proceso de gamificación añadiendo retos de mayor dificultad con el objetivo de motivar al alumnado.
   Esta línea de trabajo podría enfocarse por medio de la integración de distintos sistemas operativos y versiones que cumplan con las especificaciones definidas para los elementos de la simulación, pero que deban ser vulnerados utilizando distintas técnicas, con niveles de dificultad más o menos avanzados.
3. **Adaptación de la arquitectura a otras especialidades de formación.** El diseño de la arquitectura y el proceso de despliegue es susceptible de ser reutilizado para simulaciones especializadas en otros ámbitos de las TIC. Por ejemplo, para adaptar el entorno hacia la formación en administración de sistemas se podría realizar un proceso de adaptación eliminando los sistemas vulnerables. Los distintos sistemas deberán ser sustituidos por versiones de los mismos servicios basados en sistemas operativos y aplicaciones en sus últimas *releases*, pero manteniendo los roles e interrelaciones de los distintos elementos del diseño.

11. Glosario

802.1X. Estándar IEEE para el control de acceso en redes LAN y WLAN. Su funcionamiento consiste en proporcionar mecanismos de autenticación para los dispositivos que acceden a una red informática.

ACL o lista de control de acceso. Elemento de filtrado de red que permite añadir un conjunto de reglas básicas de control del tráfico en dispositivos de red.

Boot to Root (BTR). Tipo de desafío de competiciones especializadas en ciberseguridad que plantean el reto de conseguir privilegios de superusuario en un sistema informático.

Capture The Flag (CTF). Tipo de desafío de competiciones especializadas en ciberseguridad que consiste en la inclusión de un conjunto de banderas (flags) ocultas en un sistema informático que deberá ser vulnerado para acceder a ellas.

Clúster. Conjunto de servidores o nodos de un sistema informático encargados de realizar la misma función con el objetivo de ofrecer capacidades de escalado, alta disponibilidad o tolerancia a fallos.

Core de red. Dispositivo central de una red informática con un diseño en estrella. A partir de este dispositivo central se interconectan los dispositivos que componen la capa de acceso de la red.

Cyber-range. Entorno de simulación diseñado para la realización de formación especializada en ciberseguridad basada en la emulación de escenario de ataque y defensa.

DHCP Snooping. Mecanismo de seguridad de los dispositivos de red que previene de los ataques de DHCP Spoofing filtrando los mensajes de servidores DHCP no confiables.

DHCP spoofing. Técnica de ataque informático que consiste en el envío de falsos mensajes DHCP con el objetivo de modificar la configuración IP de los clientes conectados a la red.

DMZ (Demilitarized Zone). Una zona desmilitarizada es una red local interna de una organización donde se ubican exclusivamente los recursos y servicios empresariales publicados a Internet, como pueden ser los servicios web o de correo. Esta red habitualmente recibirá las conexiones desde Internet y la LAN empresarial pero su nivel de seguridad debe ser mucho más restrictivo que el de la red local, no permitiendo realizar conexiones desde esta hacia los equipos internos de la organización. Las restricciones impuestas en esta red impedirán que, si un sistema ubicado en esta red queda comprometido, el acceso al resto de la red no sea posible.

EDR. Solución de ciberseguridad de respuesta y detección de amenazas enfocada en la monitorización continuada de la seguridad de los dispositivos clientes de los usuarios de una red informática.

Ethernet. Tecnología de interconexión de redes utilizada ampliamente en la implementación de redes de área local (LAN).

Fibre Channel. Tecnología de interconexión de redes de alta velocidad enfocada en el acceso a sistemas de almacenamiento centralizado. Habitualmente suelen emplearse en la implementación de SAN.

Firewall. Dispositivo de seguridad que permite controlar el tráfico en una red informática basando su funcionamiento en reglas que son aplicadas sobre el tráfico que circula por sus distintas zonas de seguridad.

IaC. La Infraestructure as code (infraestructura como código) es una tecnología que permite desplegar y gestionar infraestructuras y servicios utilizando scripts y ficheros estructurados que facilitan los procesos de despliegue y gestión de los recursos informáticos de un sistema de *cloud*.

LAN (Local Area Network). Las redes de área local son redes de pequeño ámbito como puede ser una empresa o un domicilio. Sus especificaciones y tecnologías de implementación suelen ofrecer limitaciones con respecto a la distancia o al tamaño de la infraestructura.

Modelo OSI. Modelo de 7 capas de referencia teórico que define los distintos niveles que intervienen en la comunicación de las redes de telecomunicaciones.

NGFW. Los firewalls de nueva generación o firewalls de capa 7 son la evolución del concepto clásico de cortafuegos que ofrece características o capacidades de filtrado avanzadas llegando incluso a permitir crear reglas e inspeccionar el tráfico en la capa de aplicación.

Pool de recursos. Término que se suele definir al elemento que resulta tras realizar la abstracción mediante software de un conjunto de elementos de hardware, como pueden ser servidores físicos, para convertirlos en un conjunto de recursos que pueden ser asignados dinámicamente según las necesidades de un sistema o servicio virtualizado que haga uso de ellos para su funcionamiento.

RAID. Agrupación de conjunto de discos que se define para otorgar al volumen resultante capacidades de tolerancia a fallos o incrementos en la velocidad de acceso.

Router. Los enrutadores son dispositivos de red que permiten la interconexión de distintas redes basando su funcionamiento en la capa 3 del modelo OSI. Estos dispositivos permiten encaminar el tráfico entre redes basadas en TCP/IP. Su funcionamiento se basa principalmente en la creación y mantenimiento de las tablas de enrutamiento. Esta tabla permite al router tomar decisiones sobre el camino que deben seguir los paquetes para alcanzar una red remota.

SAI. Un sistema de alimentación ininterrumpida es un dispositivo de suministro eléctrico de respaldo. Su principal función es ofrecer a un sistema informático autonomía eléctrica durante un breve periodo de tiempo en caso de una caída del suministro eléctrico general. Adicionalmente, también ofrece protección ante sobretensiones que se puedan producir en la red eléctrica que alimenta el sistema.

Sistema de Detección de Intrusiones (IDS). Sistema de seguridad informática encargado de la monitorización de las conexiones y el tráfico de una red informática en busca de actividades maliciosas para su registro y notificación.

Spanning Tree. Protocolo de red que opera en la capa 2 del modelo TCP/IP y asegura que solo exista un camino sin bucles entre todos los dispositivos de una red conmutada. Su principal función consiste en garantizar que los bucles en el cableado puedan derivar en caídas de la red debidas a tormentas de broadcast.

Storage Area Network (SAN). Red de alta velocidad que proporciona acceso de alta velocidad a sistemas de almacenamiento centralizado.

Switch. También llamado conmutador de red, su principal función es interconectar equipos y dispositivos en una red local (LAN). Este dispositivo de interconexión de red opera en las capas más bajas del modelo OSI, en concreto en la capa 2. Debido a esto, la comunicación entre dispositivos se basa en la capacidad del switch para almacenar las direcciones MAC y reenviar las tramas de datos hacia el puerto específico de destino. Al no disponer de funciones en las capas superiores de dicho modelo, los conmutadores requieren de otro tipo de dispositivos que ofrezcan capacidades de capa 3 y superiores en la red, como pueden ser routers o firewalls, para permitir el acceso a otras redes e Internet.

Throughput. Es el término empleado para definir la cantidad de información por unidad de tiempo que es capaz de procesar un dispositivo o una red informática. Su significado es similar al concepto del ancho de banda, que podríamos definir como la tasa de transferencia teórica que ofrece un dispositivo o una red, mientras que el throughput sería la tasa de transferencia real.

VLAN (Virtual local área network). Esta tecnología permite segmentar de forma lógica un dispositivo físico (switch) para crear varios conjuntos de puertos y que no puedan comunicarse entre ellos a través de la capa MAC de Ethernet. Esta división permite que la comunicación entre los distintos grupos de puertos deba ser gestionada en las capas superiores de la arquitectura de red.

VLAN hopping. Técnica de ataque a un sistema informático que consiste en la inyección de etiquetado de VLANs con el objetivo de acceder a redes virtuales a las que no pertenece el dispositivo.

WAN. (Wide Area Network). Las redes de área extensa son redes de gran ámbito y que permite la interconexión de redes de menor tamaño. Este tipo de redes suelen estar implementadas con tecnología especifica de interconexión para largas distancias y ofrecidas por proveedores de servicios como mecanismo de acceso a Internet.

12. Bibliografía

The Future of Jobs Report 2023 | World Economic Forum. (n.d.). Retrieved March 22, 2024, from https://www.weforum.org/publications/the-future-of-jobs-report-2023/

La demanda de talento en ciberseguridad superará en un 50% a la oferta en 2024. - AEC - Asociación española de empresas de consultoría. (n.d.). Retrieved March 21, 2024, from https://aecconsultoras.com/talento-noticia/la-demanda-de-talento-en-ciberseguridad-superara-en-un-50-a-la-oferta-en-2024/

La UOC incorpora el compromiso ético y global en sus grados y másteres. (s. f.). *Retrieved April 4 de abril de 2024, from https://www.uoc.edu/es/news/2020/135-competencia-etica-global*

Moore, G. E. (n.d.). Cramming more components onto integrated circuits, Reprinted from Electronics, volume 38, number 8, April 19, 1965, pp.114 ff. *IEEE Solid-State Circuits Society Newsletter*, *11*(3), 33–35. *https://doi.org/10.1109/N-SSC.2006.4785860*

Creasy, R. J. (n.d.). The Origin of the VM/370 Time-Sharing System. *IBM Journal of Research and Development*, *25*(5), 483–490. https://doi.org/10.1147/rd.255.0483

Bugnion, E., Devine, S., Rosenblum, M., Sugerman, J., & Wang, E. Y. (2012). Bringing Virtualization to the x86 Architecture with the Original VMware Workstation. *ACM Transactions on Computer Systems*, *30*(4), 1–51. https://doi.org/10.1145/2382553.2382554

Rosenblum, M., & Garfinkel, T. (2005). Virtual machine monitors: current technology and future trends. *Computer*, *38*(5), 39–47. https://doi.org/10.1109/MC.2005.176

Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. In *Communications of the ACM* (Vol. 53, Issue 4, pp. 50–58). ACM. https://doi.org/10.1145/1721654.1721672

Sola Caraballo, C. de. (2015). *Explotación de OpenNebula como plataforma cloud IaaS para la docencia*. https://idus.us.es/handle/11441/33874

Gallardo, R., & Guerrero, G. (2021). *Reingeniería del Laboratorio de Seguridad Informática: Análisis, diseño e implementación de un Cyber Range*. https://www.colibri.udelar.edu.uy/jspui/handle/20.500.12008/30925

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011). From game design elements to gamefulness: defining "gamification." *Proceedings of the 15th International Academic MindTrek Conference*, 9–15. https://doi.org/10.1145/2181037.2181040

Workman, M. D. (2021). An Exploratory Study of Mode Efficacy in Cybersecurity Training. *Journal of Cybersecurity Education, Research & Practice*, *2021*(1).

Prince, M. J., & Felder, R. M. (2006). Inductive Teaching and Learning Methods: Definitions, Comparisons, and Research Bases. *Journal of Engineering Education (Washington, D.C.)*, *95*(2), 123–138. https://doi.org/10.1002/j.2168-9830.2006.tb00884.x

Kolb, D. (2014). *Experiential Learning: Experience as the Source of Learning and Development Kolb, David.* (2nd edition). PH Professional Business.

Hmelo-Silver, C. E. (2004). Problem-Based Learning: What and How Do Students Learn? *Educational Psychology Review*, *16*(3), 235–266. https://doi.org/10.1023/B:EDPR.0000034022.16470.f3

Curphey, M. (2001). OWASP Foundation. Retrieved April 6, 2024, from https://owasp.org

Aharoni, M., & Kearns, D. (2013). Kali Linux. Retrieved April 6, 2024, from https://www.kali.org

Buechler, C., & Scott, D. (2004). pfSense CE. Retrieved April 6, 2024, from https://www.pfsense.org

Canonical. (2004). Ubuntu Desktop. Retrieved April 6, 2024, from https://ubuntu.com/desktop

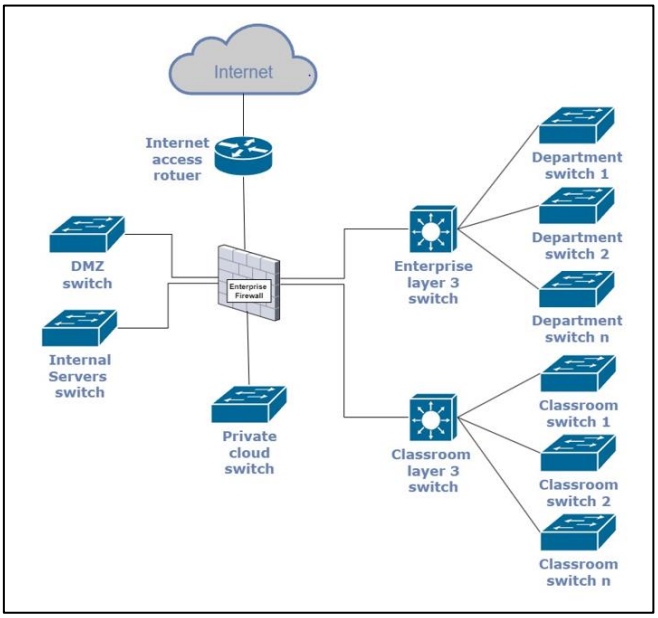
Debian Project. (1993). Debian. Retrieved April 6, 2024, from https://www.debian.org

Microsoft. (1993). Windows Server. Retrieved April 6, 2024, from https://www.microsoft.com/windows-server

Anexo I. Descripción de seguridad de la red corporativa

En el siguiente documento se describe el diseño de una red empresarial que garantice la seguridad en un entorno educativo con un sistema de cloud como el que se detalla en este trabajo. Como se ha comentado anteriormente, el centro educativo donde se implanta el sistema objeto de estudio ofrece enseñanza en distintos ámbitos TIC y por ello tiene usuarios con alto conocimiento en nuevas tecnologías, entre otras, sistemas, redes y seguridad. Aunque la seguridad en los sistemas de información debe ser una prioridad a todos los niveles, debido a la alta especialización de los usuarios de esta organización, se hace necesario diseñar los sistemas focalizando la atención en la seguridad de los sistemas de información desde todos los ámbitos de su desarrollo.

En primer lugar, el diseño físico de la red corporativa está basado en una arquitectura clásica de estrella extendida que permite una segmentación física entre las distintas zonas de la organización para favorecer la seguridad de la red. La implementación de esta arquitectura se basa en un firewall como nodo central de la red (*core*) que interconecta cada una de las zonas físicamente. La implementación de estas zonas se realiza por medio de distintos dispositivos según las necesidades de velocidad, *throughput* de los dispositivos, o complejidad interzonal. En la siguiente imagen se puede observar el esquema del diseño físico de la red empresarial del centro académico donde está implantado el sistema.



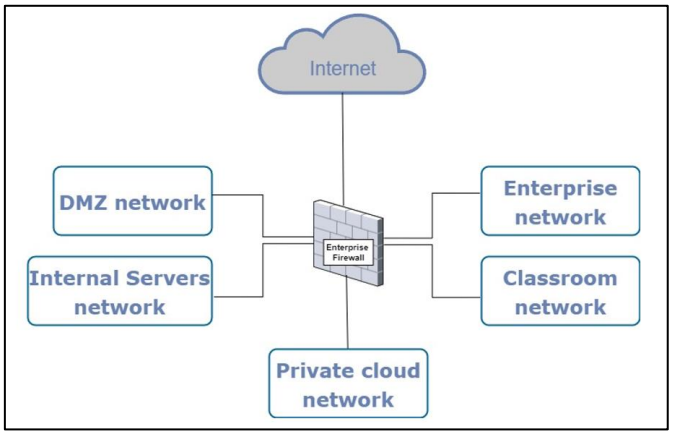
Como se ha comentado cada zona tiene una serie de dispositivos que implementan la arquitectura de las capas inferiores según las necesidades:

- El acceso a internet se implementa por medio de la conexión de una interfaz física del firewall con un router que da acceso a la red WAN del proveedor de servicios.
- Las zonas destinadas a ofrecer servicios a internet (DMZ) y a la red corporativa (Internal servers), se implementan con switches de tipo *Data Center* sin segmentación por VLANs. Estas dos zonas también disponen de interfaces físicas independientes para la conexión con el firewall empresarial.

- Las redes departamentales y de aulas docentes, se implementan con dos switches de capa 3 con capacidades de enrutamiento y filtrado básico. Estos switches extienden la red a otros dispositivos de nivel inferior, switches administrados, que también segmentan físicamente el tráfico entre los distintos departamentos o aulas. Es importante destacar que, a este nivel tan bajo, en ocasiones se hace necesaria una segmentación lógica. Esta segmentación se realiza mediante VLANs que permiten extender una red entre varios dispositivos físicos. Esta configuración se hace necesaria ya que nos encontramos con departamentos repartidos en varios espacios físicos y que por lo tanto se hace necesario que el tráfico de estos se extienda a través de la red de *switching*. Esta segmentación por medio de VLANs permite adaptar y segmentar de forma efectiva los departamentos a la estructura empresarial de la organización. Como se ha comentado, esta división lógica nunca mezcla las zonas de departamentos y aulas, que tiene una separación física a nivel de dispositivo.
- La red destinada al cloud privado se implementa con la misma filosofía de las redes de servicios, un switch de tipo *Data Center*. En este caso la implementación de las distintas redes de esta zona se realiza por medio de VLANs. Como se puede observar en el Anexo II, Diseño del sistema de cloud privado, esta segmentación lógica de la zona se complementa a nivel del diseño del sistema de cloud separando el tráfico de administración/acceso remoto del tráfico de los laboratorios, ofreciendo de esta forma interfaces a nivel de host independientes para las VLANS con distintos propósitos.

Como se ha visto hasta ahora, la arquitectura del sistema está diseñada para ofrecer segmentación a nivel físico. Esta segmentación evita que el tráfico de las distintas zonas pase a través de los mismos dispositivos, lo que reduce la posibilidad de ataques a la electrónica de red que podrían permitir a un usuario malintencionado saltar entre zonas para obtener acceso no autorizado o capturar tráfico sensible.

La segmentación física mencionada, se complementa en las capas superiores de la arquitectura con una segmentación lógica, implementada con distintas redes y zonas como se observa en la siguiente imagen.



Como vemos en la imagen, todo el tráfico de red pasa a través del firewall central de la organización. El direccionamiento de todas las redes es independiente para cada zona, lo

que proporciona la capacidad de sumarizar rutas para minimizar los costes de enrutamiento entre ellas.

Además de lo mencionado hasta ahora, el sistema está diseñado bajo la premisa de que la seguridad no se basa en un único elemento dentro de una red o sistema, sino que es un concepto transversal que debe estar presente en todos los elementos que formen parte del diseño de un sistema. Por lo tanto, la arquitectura mencionada se complementa con un conjunto de medidas de seguridad en todas las capas que garantizan en todo momento el acceso seguro a todos los servicios ofrecidos por la red. Esto permite que los usuarios desarrollen sus actividades con garantías y de forma independiente a las actividades realizadas en otras zonas o áreas de la organización.

Con respecto a la seguridad física, la organización cuenta con un centro de datos (CPD) con control de acceso y medidas de acondicionamiento del espacio para asegurar el funcionamiento continuo del sistema. A continuación, se detallan algunas de estas medidas de seguridad:

- Para garantizar el suministro eléctrico de los distintos sistemas que alberga el centro de datos, cada dispositivo que forma parte de esta infraestructura cuenta con fuentes de alimentación redundantes, que se abastecen por líneas de tensión diferenciadas. Cada una de estas líneas está protegida por sistemas de alimentación ininterrumpida (SAI) independientes que garantizan el suministro eléctrico de forma continua.
- El centro de datos cuenta con elementos que garantizan en todo momento la seguridad del espacio físico. Estos elementos de seguridad perimetral son, desde sistemas de videovigilancia, control de acceso físico y alarma, hasta incluso sistemas de emergencia como sistemas de extinción de incendios.
- Por otro lado, es imprescindible el acondicionamiento del centro de datos para garantizar que las condiciones de temperatura y humedad sean adecuadas y estables. Es por ello que el centro de datos cuenta con los sistemas de acondicionamiento climático necesarios para mantener en todo momento las condiciones adecuadas para el funcionamiento de los dispositivos ubicados en dicho espacio. Estos sistemas se complementan con sondas y sensores que ofrecen lecturas y capacidad de control remoto de las condiciones y los parámetros del sistema, permitiendo de esta forma establecer alertas y umbrales que generan alertas o incluso automatizan acciones para mitigar situaciones ambientales no deseadas que puedan impactar en el funcionamiento o rendimiento del sistema.

Por otro lado, la arquitectura de red se complementa con una serie de sistemas y medidas de seguridad para garantizar el correcto funcionamiento de las comunicaciones que se establecen sobre ellas:

- Los dispositivos de red y los servidores físicos que ofrecen los servicios de la red cuentan con enlaces redundantes para garantizar la disponibilidad y tolerancia a fallos. Esta redundancia garantiza la continuidad del servicio en caso de fallos en el cableado o en las interfaces de conexión.
- Los dispositivos de interconexión de las capas más bajas (switches) implementan medidas de seguridad de red a bajo nivel que evitan la creación de bucles en la interconexión de dispositivos por medio de la implementación del protocolo

Spanning Tree. Este protocolo es esencial para evitar la creación de tormentas de broadcast ya sea de forma intencionada o por error.

- En las zonas destinadas a la conexión de los clientes, se valida el acceso a los puertos de red por medio del protocolo 802.1X, tanto en la red cableada como en el acceso WIFI. Este protocolo permite una validación previa de los sistemas que intentan conectarse a la red, garantizando que solo los dispositivos autorizados puedan acceder a los recursos de la red.
- La electrónica de red implementa otra serie de medidas de seguridad a bajo nivel, como DHCP Snooping para evitar ataques de DHCP spoofing y VLAN hopping, que podría permitir a un atacante escuchar el tráfico de red de una VLAN distinta a la que tiene asignada.
- Todos los dispositivos de red que lo permiten (dispositivos que operan en las capas 3 y 4 del modelo OSI y firewalls) implementan Listas de Control de Acceso (ACLs) y reglas de filtrado para controlar el tráfico y las conexiones. Esta medida permite filtrar las comunicaciones entre dispositivos, autorizando únicamente los accesos requeridos en base al direccionamiento IP y los puertos o servicios específicos necesarios para el desarrollo de la actividad del origen de la comunicación.
- Se implementan sistemas de Detección de Intrusos (IDS) por medio de la redirección del tráfico de red a dispositivos específicos, encargados de la monitorización de las comunicaciones en busca de tráfico anómalo o actividades sospechosas. Estos sistemas no solo se establecen en las zonas que ofrecen servicios si no que están integrados en las zonas destinadas al desarrollo de la actividad de los usuarios de la red.

Por su parte, los sistemas que ofrecen los servicios de la organización, tanto para la parte corporativa como para el laboratorio, se implementan mediante infraestructuras de virtualización. Estas infraestructuras proporcionan una serie de medidas de seguridad implícitas en su diseño, gracias a la capacidad de abstracción sobre el hardware que ofrecen. Entre otras mejoras, vemos que dicha abstracción permite que los recursos computacionales se ofrezcan como pools que son utilizados por los sistemas virtuales que finalmente ofrecen los servicios. Para llevar a cabo esta abstracción, el sistema de virtualización se basa en un clúster de servidores físicos que proporciona el procesamiento y la memoria que necesita el sistema, y un sistema de almacenamiento especializado que se ofrece al clúster por medio de una SAN (Storage Area Network) basada en Fibre Channel.

Por ello, estos sistemas cuentan con un conjunto de medidas de seguridad para garantizar la continuidad del servicio. Estos sistemas se basan, en primer lugar, en dispositivos y configuraciones específicas que se establecen sobre el hardware de servidor, y en mecanismos de seguridad específicos para los sistemas de seguridad y aplicaciones que se ofrecen sobre ellos.

Con respecto al hardware de servidor y la infraestructura física que se implementa sobre este, podemos destacar algunas de las principales medidas de seguridad del sistema:

- En la medida de lo posible, todos los componentes internos de hardware de los servidores que implementan la estructura del sistema se redundan o se establecen configuraciones que permitan tolerar fallos en ellos. Entre otros, estos dispositivos deben contar con doble fuente de alimentación, como se ha mencionado

anteriormente, para garantizar el funcionamiento del sistema en caso de caída eléctrica o mal funcionamiento del propio dispositivo. Además, cuentan con interfaces de red Ethernet y Fibre Channel redundantes, y dispositivos internos que permitan establecer niveles de RAID a nivel del almacenamiento interno para garantizar la pérdida de un disco sin parada de servicio.

- Sistema de backup integrado con el sistema de virtualización. Este sistema de copias de seguridad ofrece la capacidad de recuperación de sistemas virtuales completos o incluso la granularidad necesaria para extraer o recuperar ficheros concretos dentro del sistema de ficheros de las máquinas virtuales.
- Sistemas de monitorización y chequeo de salud por medio del entorno virtual.

Por último, otro gran bloque de medidas de seguridad implementadas en el sistema serían medidas de alto nivel, definidas la mayoría de ellas en capa de aplicación.

- Centralización y control de acceso de usuarios por medio de la implantación de un servicio de directorio. De esta forma es más sencillo auditar la..., además se establecen políticas centralizadas en la complejidad de las contraseñas y la gestión de cuentas.
- Contraseñas de acceso a servicios cifradas (por ejemplo, protocolo SSL)
  Es imprescindible que las aplicaciones se comuniquen por medio de protocolos seguros (https para evitar la captura o modificación de las conexiones) y que se respeten buenas prácticas en el desarrollo de software para evitar vulnerabilidades típicas de aplicaciones web (XSS, SQLi, etc.) Estas vulnerabilidades siempre se basan en el no filtrado de los parámetros de entrada de las aplicaciones.
- Otra regla importante en el desarrollo de software es limitar los permisos que tiene el usuario que utiliza la aplicación para conectar con la base de datos. Un atacante podría utilizar una vulnerabilidad en la web para acceder a la base de datos. Si el usuario utilizado para realizar la conexión de la aplicación es el root o admin de la base de datos le estaremos dando al atacante acceso completo al sistema de base de datos.

Además de las medidas de seguridad definidas anteriormente, la organización cuenta con un servicio externo que realiza auditorías de seguridad. Esta empresa tiene un contrato para realizar auditorías de vulnerabilidades en los sistemas de forma periódica. Comentar, que además de las auditorías externas, se cuenta internamente con un servidor de auditorías que tiene instalada la aplicación Nessus y realiza auditorías automatizadas del sistema, así como una auditoría personalizada cuando se va a realizar el despliegue de un nuevo servicio o aplicación.

Por otro lado, para permitir la trazabilidad, correlación y en su caso poder trazar el alcance de un incidente, la organización cuenta con un sistema que centraliza los logs de todos los sistemas en un SIEM.

Finalmente, una de las últimas incorporaciones al sistema de seguridad y que se encuentra integrada con el SIEM de la organización es la implantación de un EDR para la auditoría y control de la seguridad en los equipos cliente.

Anexo II. Configuración del cliente para integración del Directorio Activo en el SIEM

Modificaciones hechas en el archivo ossec.conf para realizar la integración del Directorio Activo con Wazuh por medio del agente.

```
nano /var/ossec/etc/ossec.conf
<logall>yes</logall>

<remote>
  <connection>syslog</connection>
  <port>514</port>
  <protocol>udp</protocol>
  <allowed-ips>192.168.10.0/24</allowed-ips>
  <local_ip>192.168.10.50</local_ip>
</remote>
```

Anexo III. Entregables.

1. Informe resumen de requisitos y funcionalidades del sistema

Proyecto: Desarrollo de un entorno de simulación como laboratorio de prácticas especializado en ciberseguridad

Informe resumen de requisitos y funcionalidades del sistema

Contenido

Historial de Versiones

Fecha	Versión	Autor	Organización	Descripción
06/04/2024	1.0	Jose García		

Información del Proyecto

Empresa / Organización	
Proyecto	*Desarrollo de un entorno de simulación como laboratorio de prácticas especializado en ciberseguridad*

Aprobaciones

Nombre y Apellido	Cargo	Departamento u Organización	Fecha	Firma

1. Propósito

El propósito del siguiente informe es definir los requisitos necesarios para el desarrollo de un entorno empresarial simulado sobre un sistema de *cloud* privado que permita el desarrollo de contenidos didácticos enfocados en el aprendizaje especializado en ciberseguridad. El enfoque principal de este proyecto es la creación de un entorno educativo integral e innovador que permita desarrollar una experiencia práctica avanzada para fomentar el desarrollo de las competencias fundamentales requeridas por los técnicos especialistas en el mundo de la ciberseguridad.

Este entorno simulado permitirá a los estudiantes interactuar con escenarios de seguridad informática en un entorno controlado y realista, mediante la creación de prácticas en situaciones similares a las que deberán enfrentarse en su futuro profesional. La contextualización de los contenidos didácticos que se realizará fomentará el desarrollo y la comprensión de estos por parte de los alumnos.

El objetivo del presente informe no solo es establecer los requisitos técnicos fundamentales para el desarrollo del entorno, sino también definir los objetivos pedagógicos y su integración con el sistema que se desarrollará posteriormente. Se espera que el producto desarrollado por este proyecto contribuya significativamente a mejorar y evolucionar una titulación en ciberseguridad ofrecida en un centro educativo y con ello mejore la capacitación y preparación del alumnado para afrontar los retos y desafíos en el desempeño de su carrera profesional en el campo de la ciberseguridad.

2. Alcance del producto

El producto resultante de este desarrollo será la creación de una arquitectura de un sistema informático empresarial simulado. Esta simulación permitirá la realización de un proceso de enseñanza técnica sobre seguridad informática. Esta arquitectura se utilizará como base para el desarrollo de los contenidos didácticos sobre ciberseguridad que forman parte del plan de estudios de la titulación objetivo de este proyecto.

La creación de este entorno de laboratorio proporcionará una plataforma completa e innovadora que favorecerá el proceso de aprendizaje del alumnado. Permitirá desarrollar la formación de manera práctica y realista, ofreciendo un escenario simulado que refleje los desafíos y situaciones de un entorno empresarial real en el campo de la seguridad informática.

El sistema desarrollado proporcionará a los estudiantes un entorno empresarial real simulado mediante el cual podrán desarrollar las actividades prácticas en un sistema completo. Este sistema, les permitirá desarrollar y contextualizar las actividades de protección y detección ante amenazas, así como adquirir los conocimientos esenciales para la realización de auditorías de seguridad en un entorno que les proporcionará una visión completa de un sistema informático real. El entorno ofrecerá al alumnado la posibilidad de interactuar con todos los elementos que componen el sistema ofreciéndoles una visión integral de una red empresarial, lo que fomentara la adquisición de las habilidades esenciales para el desarrollo de su actividad laboral futura en el mundo de la ciberseguridad.

3. Descripción del uso previsto del sistema

El objetivo de uso principal del sistema es el desarrollo de la arquitectura de una red empresarial simulada como base para el desarrollo de talleres prácticos sobre contenidos didácticos sobre ciberseguridad. El sistema desarrollado debe contemplar un conjunto de sistemas y dispositivos para dar cobertura a los contenidos incluidos en el siguiente índice, que son desarrollados de forma general en una titulación técnica especializada en ciberseguridad y que se utilizará como base para la toma de requisitos del sistema:

- Módulo 1: Introducción al curso.
    4. Descripción del curso y sus contenidos.
    5. Introducción al laboratorio de seguridad.
    6. Implementación de una arquitectura básica de seguridad.
- Módulo 2: Espacio de ejecución seguro.
    6. Estándares sobre sistemas de ejecución segura.
    7. Bastionado de sistemas.
    8. Sistemas de detección de vulnerabilidades.
    9. Sistemas de gestión de eventos e información de seguridad.
- Módulo 3: Hacking ético.
    6. Introducción al hacking ético: Fases, alcance, tipos de auditoría.
    7. Recopilación de información
    8. Análisis de vulnerabilidades
    9. Herramientas y técnicas de ataque
    10. Documentación de la auditoría
- Módulo 4: Gestión y respuesta ante incidentes
    3. Fuentes de información de amenazas
    4. Fases del ciclo de vida de un incidente
        4.1. Preparación ante incidentes
        4.2. Detección y análisis de incidentes
        4.3. Contención, mitigación y recuperación.
        4.4. Tratamiento post-incidente: Informe y notificación.
- Módulo 5: Seguridad con new generation firewall
    13. Introducción a los firewalls de nueva generación (NGFWs).
    14. Funcionamiento y arquitectura de los NGFWs
    15. Políticas de seguridad y reglas de filtrado
    16. Integración con otras soluciones de seguridad
    17. Gestión y monitoreo de NGFW

4. Funcionalidades del producto

A continuación, se presenta una lista numerada de las principales funcionalidades del sistema propuesto.

1. El sistema proporcionará los recursos y las herramientas especializadas necesarias para la realización de actividades relacionadas con la seguridad.
2. El sistema proporcionará los elementos necesarios para desarrollar simulaciones de ataque y defensa informática.
3. El sistema establecerá los mecanismos de seguridad necesarios para proteger la integridad de los elementos utilizados por el resto de las titulaciones.

4. El desarrollo realizado ofrece las características necesarias para su automatización y replicación de forma sencilla.
5. El sistema permitirá monitorizar y analizar las actividades de los estudiantes dentro del entorno simulado.

5. Clases y características de los roles de usuarios

A continuación, se presenta una clasificación de los usuarios tipo que utilizarán el sistema en base a los principales roles de uso, así como una descripción de las principales funciones que desempeñan en el proceso de enseñanza/aprendizaje.

- Docente. Es el usuario responsable del proceso docente. Estará encargado de desarrollar los contenidos, así como de orientar y guiar al alumnado en el proceso de enseñanza.
  Sus características principales son:
  - Debe tener conocimiento de la materia que se imparte, del sistema de *cloud* y de la arquitectura de la simulación.
  - Es el responsable de preparar las actividades didácticas que permiten desarrollar los contenidos educativos.
  - Coordina la secuenciación de actividades didácticas que se realizarán por medio del sistema.
  - Tiene capacidad de acceso y gestión del entorno de *cloud* únicamente en el ámbito de la simulación.
  - Dispone de máximos privilegios en los sistemas que componen la simulación, pero no tiene rol de administración en el sistema de *cloud*.
- Alumnado. Es el conjunto de usuario destinatario del proceso de aprendizaje.
  Sus características principales son:
  - Debe tener los conocimientos básicos en redes y sistemas informáticos que le permitan acceder al sistema.
  - Tiene el nivel de acceso al sistema mínimo requerido para el desarrollo de los contenidos didácticos.
- Administrador del sistema. Es el usuario responsable del sistema informático.
  Sus características principales son:
  - Debe conocer el entorno de *cloud* y la arquitectura de la simulación.
  - Tiene la capacidad de desplegar los recursos requeridos para el desarrollo de la actividad docente.
  - Puede administrar el sistema de *cloud* y acceder con máximos privilegios a todos los sistemas desplegados.
  - Es el encargado de velar por el uso adecuado de los recursos informáticos.

6. Entorno operativo

La arquitectura resultante de la implantación debe ofrecer la integración con el entorno de la organización asegurando en todo momento la provisión de recursos y estableciendo los mecanismos necesarios para garantizar la seguridad del sistema de forma integral.

El sistema se implantará y desarrollará sobre un entorno de *cloud* privado basado en la plataforma OpenNebula. Este sistema proporcionará los recursos necesarios para la implantación de una simulación de un entorno informático real. El uso de esta plataforma de nube privada permite la gestión de recursos informáticos y ofrece un entorno flexible y escalable para el desarrollo de prácticas y contenidos didácticos para especialidades educativas orientadas a las TIC.

Tras la implantación del sistema, la arquitectura resultante proporcionará a los estudiantes todos los elementos de hardware virtual y software especializado necesarios para desarrollar las actividades didácticas propuestas en el plan de estudios. El entorno simulado que se proveerá incluirá las instancias, redes y otros elementos virtuales requeridos durante el desarrollo de los contenidos de las prácticas de seguridad.

El sistema de *cloud* privado es utilizado por otras titulaciones de forma habitual por lo que se hace esencial la implantación de las medidas necesarias que garanticen la coexistencia de los distintos grupos de usuarios en el mismo entorno. Debido a esto, es imprescindible el desarrollo de los mecanismos de acceso y protección necesarios para garantizar el correcto uso de los recursos informáticos del sistema.

7. Reglas y normas de uso del sistema

A continuación, se ofrece un listado de reglas y principios de obligatorio cumplimiento sobre el entorno de *cloud* docente para asegurar el desarrollo de las actividades con garantías de funcionamiento adecuadas para todos los usuarios del sistema y que aplican al sistema en desarrollo y deben tomarse en cuenta durante la toma de requerimientos contenidos en este documento y abordados en la fase de diseño del sistema.

- Los usuarios docentes definirán los contenidos didácticos y su adaptación al sistema. También podrán proponer las modificaciones o mejoras que crean necesarias para el desarrollo adecuado de los contenidos educativos.
- Los administradores del sistema serán los responsables de la asignación, creación y modificación de los recursos informáticos que se provean en el desarrollo de la simulación, así como de la asignación de roles de usuario en el ámbito del sistema de *cloud*.
- Todos los accesos al sistema de *cloud* deberán ser autenticados por mecanismos seguros de forma que se pueda realizar la trazabilidad de la actividad de los usuarios del sistema.
- Los sistemas virtuales que no se integren con los mecanismos de validación centralizados de la organización, en concreto los sistemas virtuales que forman parte de la simulación, serán monitorizados en todo momento y deberán disponer de mecanismos de acceso con máximo privilegio para los administradores y docentes. En caso de que este mecanismo de acceso quede bloqueado durante el desarrollo de las actividades prácticas, el usuario del alumno se bloqueará y el sistema será desvinculado del entorno mientras se realiza una investigación sobre el sistema y las actividades realizadas por el alumno.
- Independientemente de las actividades que se realicen en el sistema, el desarrollo de los contenidos debe cumplir con las normativas y regulaciones locales e internacionales al respecto de la seguridad de los sistemas de información. Se establecerán los mecanismos necesarios para asegurar que la actividad desarrollada en el sistema esté siempre dentro de los límites legales y éticos en materia de protección de datos y privacidad.
- El diseño del sistema se realizará de forma que sea escalable y replicable para permitir su adaptación a futuras modificaciones de los contenidos o los elementos que lo componen, de forma que permita el escalado o la ampliación en el número de alumnos que lo utilizan.

8. Requerimientos funcionales

A nivel general se pueden establecer una serie de requisitos básicos que deben ser complementados con los requisitos específicos que permitan desarrollar los contenidos. Este primer conjunto de requisitos básicos se corresponde con las necesidades de conexión de los terminales cliente utilizados por los usuarios del sistema. Estos terminales deben disponer de los siguientes elementos de software para acceder a todos los servicios ofrecidos por el entorno:

- Cliente de conexión RDP.
- Cliente de conexión SSH.
- Navegador Web.

Tras la evaluación de los contenidos didácticos se han definido una serie de requisitos específicos necesarios para el desarrollo de la actividad lectiva, a continuación, se muestra el detalle de dichos requisitos:

- Módulo 1
    - Credenciales de acceso al sistema de *cloud*.
    - Instancia de un firewall.
    - Una o más instancias de sistemas para su publicación en el firewall.
- Módulo 2
    - Una o más instancias de sistemas para realizar procedimientos de bastionado.
    - Una o más instancias de sistemas que provean software de detección de vulnerabilidades.
    - Instancia de un SIEM.
- Módulo 3
    - Instancia de sistema con las herramientas adecuadas para realizar una auditoría.
    - Una o más instancias de sistemas vulnerables.
- Módulo 4
    - Una o más instancias de sistemas que proporcionen los logs necesarios para evaluar un incidente.
- Módulo 5
    - Firewall de nueva generación con capacidades de filtrado avanzadas.

Por último, como el objetivo final del desarrollo es la integración de todos los sistemas que componen la simulación en una única infraestructura, será imprescindible dotar al sistema de los servicios de red básicos que se pueden encontrar en una red corporativa como puede ser un servicio de directorio, DHCP u otro servicio que favorezca el correcto funcionamiento del sistema.

9. Requerimientos no funcionales

- El sistema debe ser diseñado de manera que sea replicable y permita el funcionamiento simultáneo de múltiples instancias.
- El despliegue debe automatizarse para facilitar su implantación.
- Los accesos al sistema de cloud tienen que estar centralizados y auditados.
- El acceso a los servicios ofrecidos por el sistema debe ser seguro y con garantías de trazabilidad.
- El desarrollo de las actividades docentes no debe impactar en el funcionamiento de las actividades de usuarios de otras especialidades.

Proyecto: Desarrollo de un entorno de simulación como laboratorio de prácticas especializado en ciberseguridad

Informe resumen del diseño de la arquitectura de la solución

Contenido

Historial de Versiones

Fecha	Versión	Autor	Organización	Descripción
07/05/2024	1.0	Jose García		

Información del Proyecto

Empresa / Organización	
Proyecto	*Desarrollo de un entorno de simulación como laboratorio de prácticas especializado en ciberseguridad*

Aprobaciones

Nombre y Apellido	Cargo	Departamento u Organización	Fecha	Firma

1. Propósito

El propósito del presente informe sobre el diseño de la arquitectura de la solución es presentar una descripción de los distintos elementos que componen el sistema propuesto para la simulación del entorno empresarial utilizado como laboratorio de prácticas de una formación especializada en ciberseguridad. A continuación, se presentará un resumen que incluye los elementos necesarios para comprender el diseño realizado y los elementos que componen el sistema propuesto.

Por medio de los siguientes apartados se presenta una guía que debe servir como referencia sobre los componentes clave que conforman el sistema, así como los servicios que se ofrecen y sus interrelaciones de forma que sirva de ayuda para la comprensión del sistema y su futura replicación o revisión.

El presente informe puede servir de guía para algunos de los tipos de usuarios que harán uso del sistema, principalmente los administradores del sistema y los docentes. A partir de la información proporcionada en este informe se podrá generar documentación adicional destinada al desarrollo de los contenidos por parte de los docentes enfocado al alumnado que realice la formación.

2. Descripción del sistema

El diseño de la simulación propone la arquitectura de una empresa que basa su actividad en una tienda virtual donde vende diferentes productos a través de una tienda Online. Todos los servicios son publicados por la empresa, tanto a nivel interno como hacía Internet, bajo el dominio SimHackCorp.lab.

La red WAN de la empresa ofrece a internet un servicio web con su tienda virtual donde ofrece un catálogo de productos y una serie de funcionalidades para los usuarios como son la compra o evaluación de los productos mediante *ratings* y comentarios. Por otro lado, la organización tiene un segundo servicio web público, en este caso es la intranet corporativa que se encuentra en construcción. Este servidor tiene abierto un servicio FTP por motivos administrativos que es utilizado por la empresa que está desarrollando el sitio.

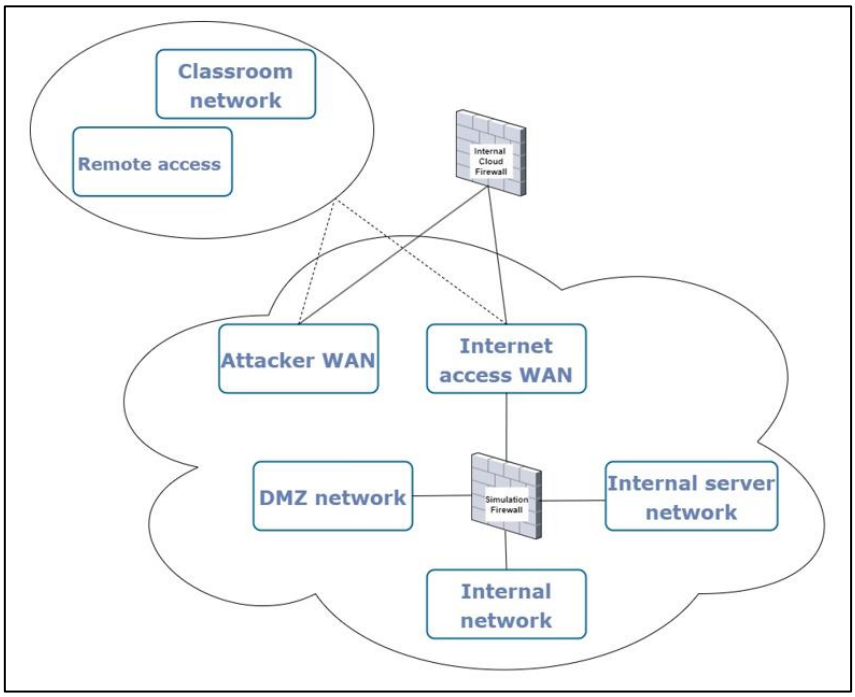
Por último, con respecto a los servicios públicos ofrecidos a Internet por la corporación, se pública un tercer sitio web con la interfaz de gestión de su solución de seguridad Wazuh, el SIEM corporativo encargado de recopilar los registros de seguridad de los distintos elementos de la red para realizar una supervisión de eventos de seguridad de forma efectiva.

Además, la empresa dispone de un servicio de bases de datos que se utiliza para gestionar el almacén, los productos y los pedidos. Este servicio tiene vinculadas algunas tablas con las aplicaciones públicas a Internet. Por otro lado, los trabajadores de la empresa utilizan determinadas aplicaciones de escritorio que acceden a los datos almacenados en dicho servidor.

La red basa su sistema de validación y administración de equipos en el Directorio Activo de Microsoft. Este servidor se encuentra ubicado en una red interna y es accesible por los terminales de usuario y las aplicaciones que requieran utilizar sus servicios de validación. Por otro lado, la empresa tiene una serie de equipos cliente que pertenecen a los trabajadores de los distintos departamentos.

Toda la arquitectura de la red presentada queda definida por medio de un firewall bastión encargado de segmentar las redes y que ofrece las características de seguridad definidas para este tipo de dispositivos. Entre las principales funcionalidades que aporta se encuentran la publicación de servicio y la implementación de un servicio VPN para el acceso remoto de los trabajadores.

3. Topología de red

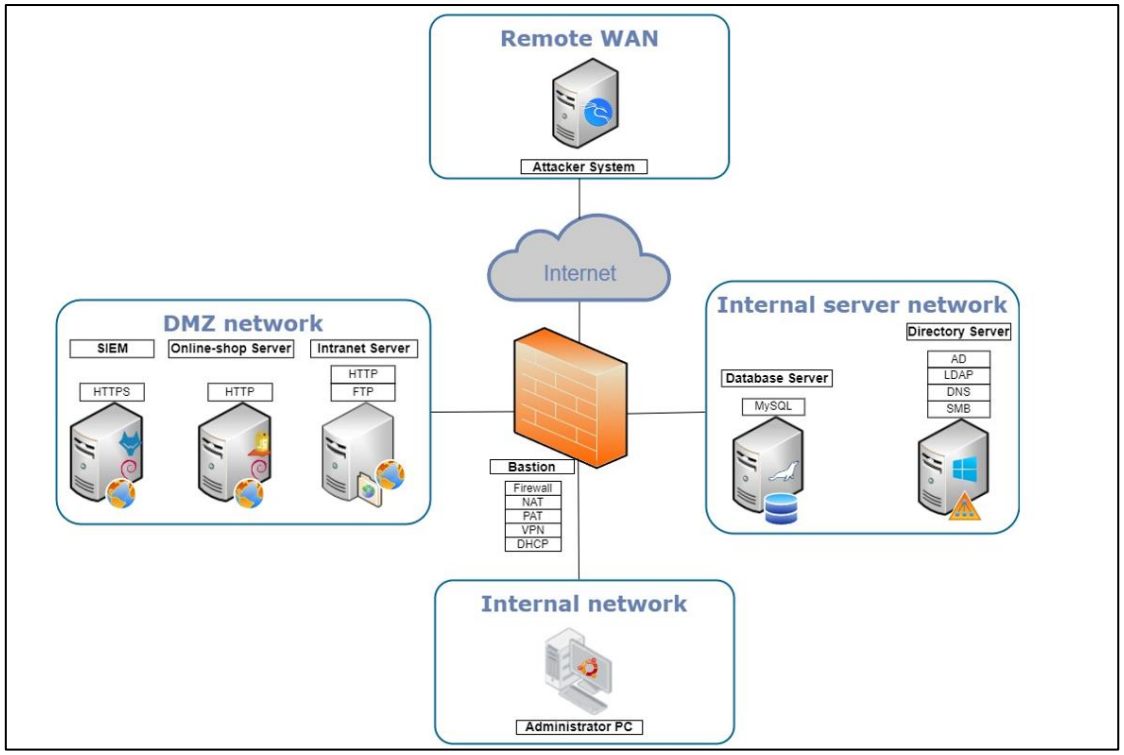


Como se puede ver en la imagen, la topología de la red de la simulación de SimHackCorp.lab se define a través de la segmentación realizada por el firewall bastión de la organización. Además, el esquema propuesto incluye un conjunto de redes enfocadas a la simulación de Internet.

La simulación contempla las siguientes redes:

- WAN1. Internet Access WAN. Esta red simula la conexión de la organización con un proveedor de servicios que le aprovisiona del acceso a Internet.
- WAN2. Attacker WAN. Esta red será utilizada durante el módulo 3 como red remota desde la que se producirá el ataque a la organización.
- LAN1. Internal network. Esta red simulará una red LAN corporativa. En ella solo se encontrarán los equipos de usuario.
- LAN2. DMZ network. Esta red simulará la zona desmilitarizada del firewall. Será la red desde donde se publiquen servicios hacia la WAN.
- LAN3. Internal Servers network. Esta red se corresponde con una zona donde encontraremos servidores que publicaran servicios de las redes corporativas. Estos servicios no serán accesibles desde la WAN.

4. Servicios y funcionalidades principales desarrolladas



En la imagen se puede ver el detalle de los elementos que componen el sistema y que son listados a continuación:

- Firewall bastión
  - Implementado sobre pfSense CE
  - Realizará las siguientes funciones:
    - Segmentación de la red en 4 zonas: WAN, LAN, DMZ, SERVERS
    - Publicación de servicios a Internet
    - Servidor VPN de acceso
    - Servidor DHCP para autoconfiguración de red

- SIEM Wazuh.
  - Implementado sobre Debian.
  - Ubicado en la DMZ
    - Realizará las siguientes funciones de centralización y correlación de los logs de los dispositivos de la red

- Servidor web tienda virtual simulada
  - Implementado sobre Debian.
  - Ubicado en la red DMZ.
  - Implementado con la plataforma juice-shop de OWASP Fundation
  - Ofrece un entorno CTF para formación en ciberseguridad especializada en vulnerabilidades en aplicaciones web.

- Servidor web intranet corporativa simulada
    - Implementado por una instancia del sistema Basic_Pentesting1 de VulnHub
    - Ubicado en la red DMZ
    - Ofrece un reto de boot2root enfocado en los servicios HTTP y FTP

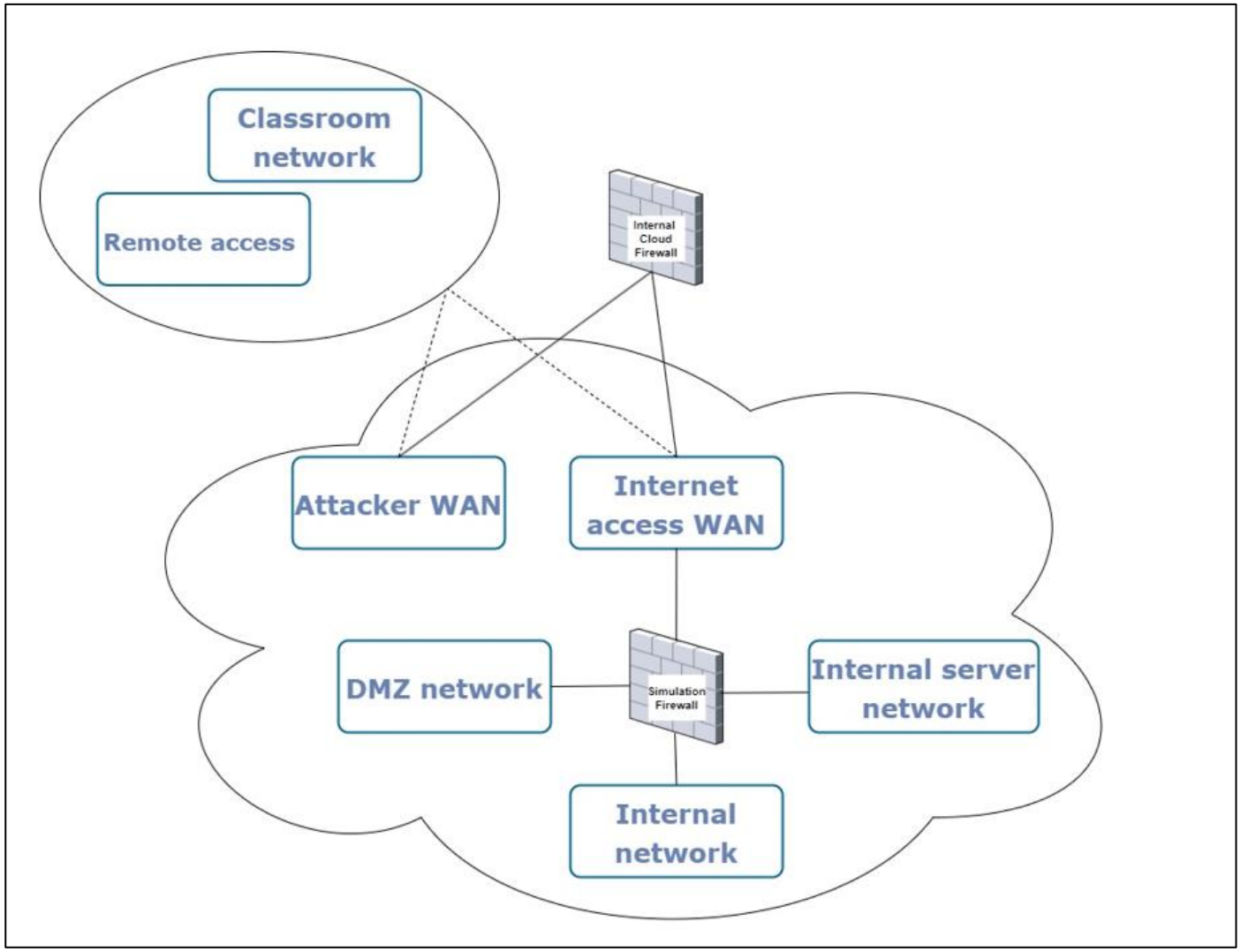
- Servidor de Directorio Activo corporativo
    - Implementado sobre Windows Server 2012 R2.
    - Ubicado en la red SERVERS
    - Ofrece los siguientes servicios:
        - Servicio de directorio activo.
        - Servicio LDAP
        - Servicio DNS
        - Servicio SAMBA

- Servidor de base de datos corporativo simulado
    - Implementado por una instancia del sistema PYEXP1 de VulnHub
    - Ubicado en la red SERVERS
    - Ofrece un conjunto de retos boot2root enfocados en el servicio MySQL

- Equipo cliente del administrador
    - Implementado sobre Ubuntu Desktop
    - Ubicado en la red LAN
    - Ofrece el acceso a las herramientas básicas de un administrador encargado de la seguridad de la organización

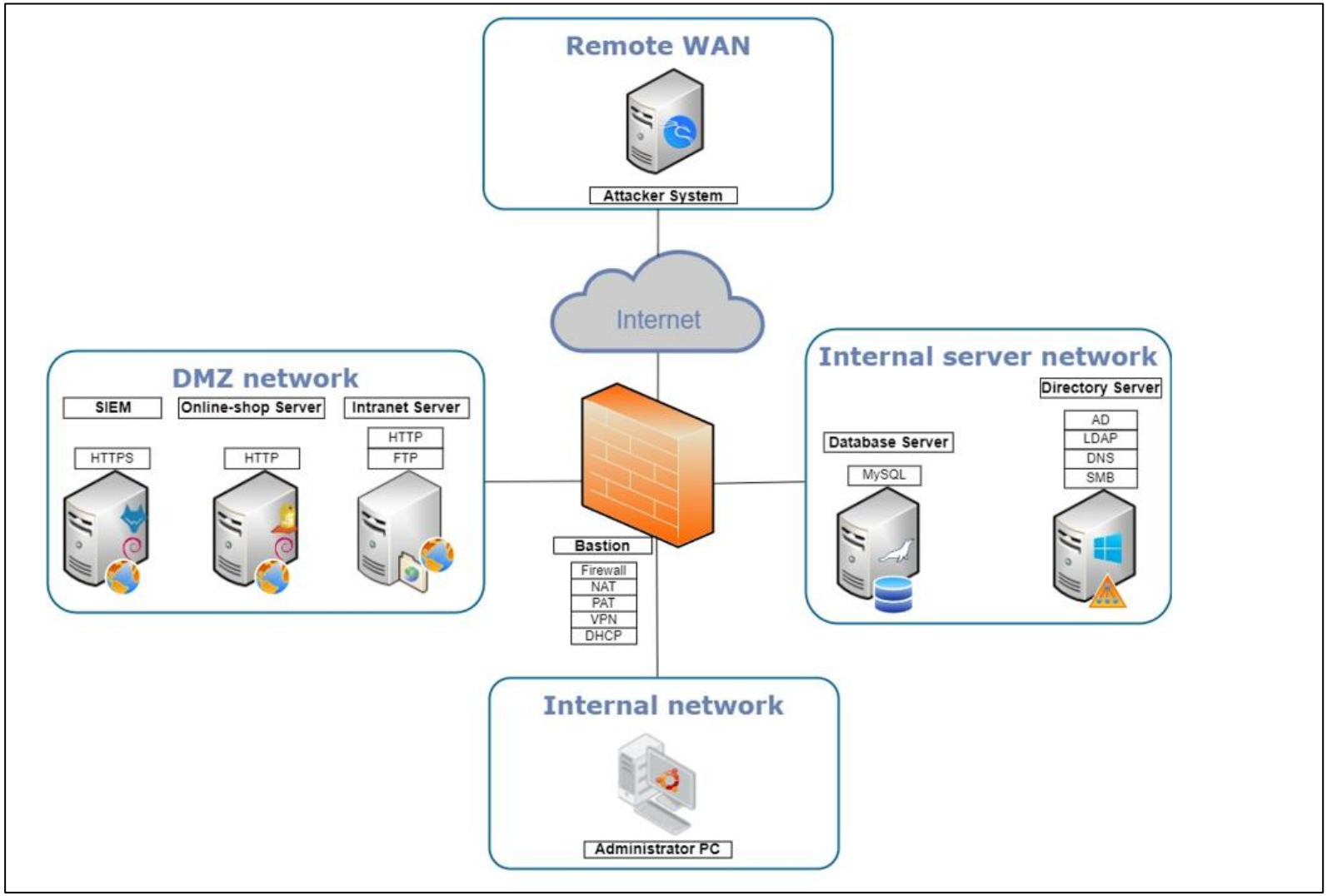
- Sistema atacante
    - Implementado sobre Kali Linux
    - Ubicado en la red remote WAN
    - Ofrece los recursos necesarios para realizar un ataque remoto a un sistema empresarial.

3. Esquemas de red y de la arquitectura de servicios



Esquema de red de la simulación

Esquema de la arquitectura de servicios red de la simulación



Proyecto: Desarrollo de un entorno de simulación como laboratorio de prácticas especializado en ciberseguridad

Procedimiento para la automatización del despliegue del sistema

Contenido

Historial de Versiones

Fecha	Versión	Autor	Organización	Descripción
06/04/2024	1.0	Jose García		

Información del Proyecto

Empresa / Organización	
Proyecto	*Desarrollo de un entorno de simulación como laboratorio de prácticas especializado en ciberseguridad*

Aprobaciones

Nombre y Apellido	Cargo	Departamento u Organización	Fecha	Firma

1. Propósito

El presente documento define el procedimiento establecido para realizar el despliegue de la simulación de red corporativa orientada en la formación en ciberseguridad. El objetivo del presente documento es ofrecer una guía para la realización del despliegue automatizado del entorno de la simulación mencionado. El propósito principal de este documento es asegurar la estandarización del proceso de despliegue facilitando la implantación del entorno tantas veces como sea necesario.

Siguiendo los pasos establecidos en este documento, creado específicamente para la configuración establecida en el sistema de cloud de la organización, y según la definición específica de los recursos que componen la simulación de la red empresarial que será utilizada como laboratorio especializado para el desarrollo de contenidos especializados en ciberseguridad.

2. Herramientas utilizadas

Para el despliegue se utilizará el software Terraform, que es una herramienta que tiene como principal característica la creación de infraestructura en sistemas de *cloud* de forma declarativa, es decir, definiendo una serie de objetos y recursos en una estructura de archivos que permiten definir las características y configuración de los despliegues. Por lo tanto, de forma general, el proceso de automatización del despliegue de un entorno basado en Terraform consiste en la creación de una estructura de directorios adecuada junto con un conjunto de archivos estructurados según el lenguaje HCL, lenguaje creado específicamente por HashiCorp (los desarrolladores del software), de forma que la aplicación los interpreta y aplica las configuraciones adecuadas sobre un entorno de *cloud*, ya sea público o como es nuestro caso un *cloud* privado.

3. Procedimiento

3.1. Preparación del Entorno

La preparación del entorno de cloud para realizar el proceso de despliegue que será abordado en este documento consiste en la preparación de todas las plantillas de los distintos sistemas que compondrán la infraestructura final de la simulación. Además, será necesario establecer tantos conjuntos de VLANs como versiones del entorno quieran hacerse convivir. Finalmente, estos parámetros tendrán que ser incluidos en el archivo de variables que será tratado posteriormente.

3.2. Configuración de Terraform

El uso de Terraform como herramienta para la automatización de despliegues en sistemas de *cloud* es bastante sencillo, aunque requiere conocer el funcionamiento de la herramienta y estructurar correctamente el sistema de archivos que soportara la solución.

```
wget -O- https://apt.releases.hashicorp.com/gpg | sudo gpg --dearmor -o
/usr/share/keyrings/hashicorp-archive-keyring.gpg

echo "deb [signed-by=/usr/share/keyrings/hashicorp-archive-keyring.gpg]
https://apt.releases.hashicorp.com $(lsb_release -cs) main" | sudo tee
/etc/apt/sources.list.d/hashicorp.list

sudo apt update && sudo apt install terraform
```

El primer paso para poner en funcionamiento la aplicación es realizar la instalación. Este proceso para un sistema Debian, que es nuestro caso, se realiza con el procedimiento estándar de instalación, mediante la inclusión de las fuentes adecuadas en el archivo sources.list y el comando apt. A continuación, se puede observar la secuencia de comandos realizada extraída desde la web de los desarrolladores:

Una vez instalada la herramienta es necesario estructurar los directorios de la aplicación en función de los procesos de despliegue que se realizarán. En nuestro caso se ha creado una estructura de directorios de tres niveles. El último nivel que se corresponde con los procesos de despliegue que se realizarán, en nuestro caso se desplegará infraestructura al inicio del módulo 2 y del módulo 3. Este tercer nivel, contiene los ficheros que permiten definir la configuración del entorno que se quiere realizar. A continuación, se muestra la estructura completa realizada:

```
/terraform
       /sinhackcorp
              /module2
                     /main.tf
                     /provider.tf
                     /tf.tfvars
                     /variables.tf
              /module3
                     /main.tf
                     /provider.tf
                     /tf.tfvars
                     /variables.tf
```

Los archivos que se han definido y que permiten automatizar el despliegue para varias infraestructuras son los siguientes:

- `provider.tf`: este primer archivo proporciona a la aplicación la información referente al proveedor de *cloud* que se utilizará y los parámetros de conexión con el entorno.

```
terraform {
  required_providers {
    opennebula = {
      source = "OpenNebula/opennebula"
      version = "~> 1.4"
    }
  }
}
provider "opennebula" {
  endpoint  = "http://localhost:2633/RPC2"
  username  = "username"
  password  = "Your_Secure.Password"}
```

- `main.tf`: este archivo es el que contiene la definición de los recursos que se desplegarán durante la ejecución. Para poder realizar el despliegue de varias arquitecturas hay que generalizar por medio de variables los distintos parámetros que no serán comunes para cada arquitectura. A continuación, se incluye como ejemplo una versión reducida de ejemplo del main.tf del módulo 2. Esta versión sólo incluye un recurso a modo de ejemplo, pero generaliza el proceso de despliegue para varios sistemas utilizando la estructura de variables y la asignación de valores creada en los archivos `varibales.tf` y `tf.tfvar` respectivamente, que serán comentados posteriormente.

```
resource "opennebula_virtual_machine" "pfSense_SimHackCorp" {
  count       = length(lab_sets)
  name        = "Pfsense.SimHackCorp.lab_${count.index}"
  template_id = 59
  group       = var.lab_sets[count.index].group_name
  permissions = "600"

  context = {
    USER_NAME  = var.lab_sets[count.index].user_name
    GROUP_NAME = var.lab_sets[count.index].group_name
  }
  nic {
    network_id = var.lab_sets[count.index].network_id_wan
  }
  nic {
    network_id = var.lab_sets[count.index].network_id_lan
  }
  nic {
    network_id = var.lab_sets[count.index].network_id_dmz
  }
  nic {
    network_id = var.lab_sets[count.index].network_id_servers
  }}
```

- `varibales.tf`: este tercer archivo declara las variables que serán utilizadas en el archivo main para generalizar su ejecución para varias arquitecturas.

```
variable "lab_sets" {
  description = "List of sets"
  type = list(object({
    user_name         = string
    group_name        = string
    network_id_wan    = string
    network_id_lan    = string
    network_id_dmz    = string
    network_id_servers = string
  }))
}
```

- `tf.tfvar`: Finalmente el último archivo que utilizaremos durante el despliegue permite definir los valores para las distintas variables de cada uno de los sets de recursos que se corresponderán con las distintas arquitecturas que coexistirán de forma simultánea en el entorno.

```
lab_sets = [
  {
    user_name         = "username"
    group_name        = "groupname"
    network_id_wan    = "93"
    network_id_lan    = "244"
    network_id_dmz    = "245"
    network_id_servers = "248"
  },
  {
    user_name         = "other_username"
    group_name        = "other_ groupname"
    network_id_wan    = "92"
    network_id_lan    = "234"
    network_id_dmz    = "235"
    network_id_servers = "238"
  }
]
```

3.3. Descripción de los comandos

La ejecución del despliegue se realiza por medio de 3 comandos, estos comandos deben ser ejecutados desde la ruta establecida para cada uno de los módulos definidos en la estructura de directorios. A continuación, se detallan los comandos que realizaran el despliegue, así como una breve descripción de los parámetros específicos definidos para nuestro entorno:

```
terraform init
```

Este primer comando prepara el proceso de despliegue inicializando el directorio de trabajo que contiene los archivos de configuración.

```
terraform plan -var-file="tf.tfvars" -parallelism=2 -out module2.out
```

Este segundo comando planifica el despliegue de la infraestructura. El parámetro -out permite generar la planificación de la infraestructura que se va a generar y se almacena en un archivo que servirá posteriormente para realizar el despliegue según las especificaciones indicadas por plan.

Finalmente, el tercer comando realiza el despliegue basándose en la información generada

```
terraform apply -parallelism=2 “module2.out”
```

durante la planificación del comando anterior. Cabe destacar que, en ambos casos, este comando y el anterior, se ha utilizado el parámetro `-parallelism=2` que define el número de instancias o tareas de despliegue que serán ejecutadas de forma simultánea

El proceso de eliminación de un despliegue se realiza mediante la ejecución de un único comando. El comando `terraform` con el modificador `destroy` realizará la comprobación del entorno e informará de las acciones que llevarán a cabo durante el despligue. Tras una confirmación procederá a la eliminación de los sistemas que componen el despliegue según el directorio desde donde sea ejecutado.

Por otro lado, la aplicación también dispone del siguiente comando que permite realizar la eliminación del entorno.

```
terraform destroy -var-file="tf.tfvars" -parallelism=4
```

Este comando también debe ir acompañado de un archivo de variables y permite establecer el número de tareas de eliminación que se ejecutarán de forma simultánea sobre el entorno de cloud.

3.4. Proceso de despliegue

Según lo visto hasta ahora y partiendo de la correcta definición de la estructura de directorio y archivos, se procede a detallar los comandos que realizaran el despliegue del entorno de forma adecuada para nuestro sistema:

Despliegue del entorno del módulo 2:

```
cd /terraform/sinhackcorp/module2
terraform init
terraform plan -var-file="tf.tfvars" -parallelism=2 -out module2.out
terraform apply -parallelism=2 “module2.out”
```

Despliegue del entorno del módulo 3:

```
cd /terraform/sinhackcorp/module3
terraform init
terraform plan -var-file="tf.tfvars" -parallelism=2 -out module3.out
terraform apply -parallelism=2 “module3.out”
```

Eliminación del entorno del módulo 2:

```
cd /terraform/sinhackcorp/module2
terraform destroy -var-file="tf.tfvars" -parallelism=4
```

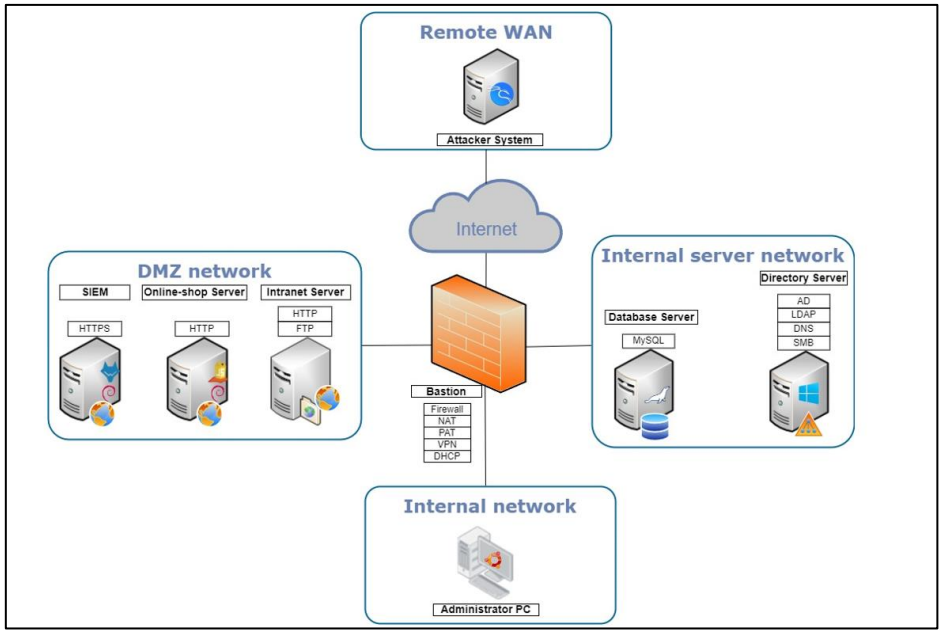
Eliminación del entorno del módulo 3:

```
cd /terraform/sinhackcorp/module3
terraform destroy -var-file="tf.tfvars" -parallelism=4
```

Documentación de la configuración de los distintos elementos que componen la simulación

Contenido

Arquitectura del sistema



Descripción de las instancias que componen la arquitectura

Code name	DNS name	OS	Network	IP	Procesadores	Memoria (MB)
PfSenseBastion	pfsense.simhackcorp.lab	pfSense OS 2.7.2	WAN LAN DMZ SERVERS	DHCP 192.168.1.1 192.168.10.1 192.168.20.1	1	512
DebianWazuh	wazuhserver.simhackcorp.lab	Debian11	DMZ	192.168.10.50	2	8192
DebianNessus	nessusserver.simhackcorp.lab	Debian11	SERVERS	192.168.20.61	4	4096
juice-shop	online-shop.simhackcorp.lab	Debian11	DMZ	192.168.10.60	1	2048
Basic_Pentesting	intranet.simhackcorp.lab	-	DMZ	192.168.10.61	2	4096
Adserver	adserver.simhackcorp.lab	Windows Server 2012 R2	SERVERS	192.168.20.50	1	4096
Pyexp	ddbbserver.simhackcorp.lab	-	SERVERS	192.168.20.62	2	2048
UbuntuDesktop	systemadmin.SimHackCorp.lab	Ubuntu Desktop 2204	LAN	192.168.1.23	2	4096
Kali	-	Kali OS	RemoteWAN	DHCP	2	4096

1. Firewall bastión

Despliegue de la instancia básica de pfSense con cuatro interfaces conectadas a las siguientes redes del sistema de *cloud* en el orden siguiente: WAN94, LAN146, LAN147 y LAN150:

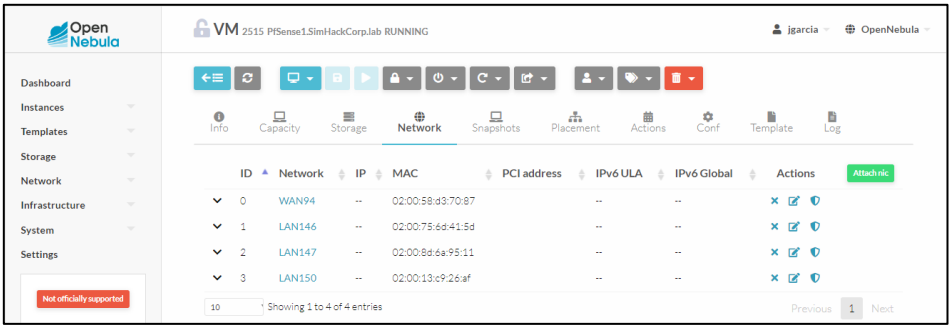


Figura 41. Asignación de redes del firewall bastión

Tras el despliegue inicial del sistema se le aplicarán las siguientes configuraciones:

- Configuración de la red.

Zona	IP	Tipo de direccionamiento
WAN	10.3.194.XX/24	Dinámico (DHCP del cloud)
LAN	192.168.1.1/24	Estático
DMZ	192.168.10.1/24	Estático
SERVERS	192.168.20.1/24	Estático

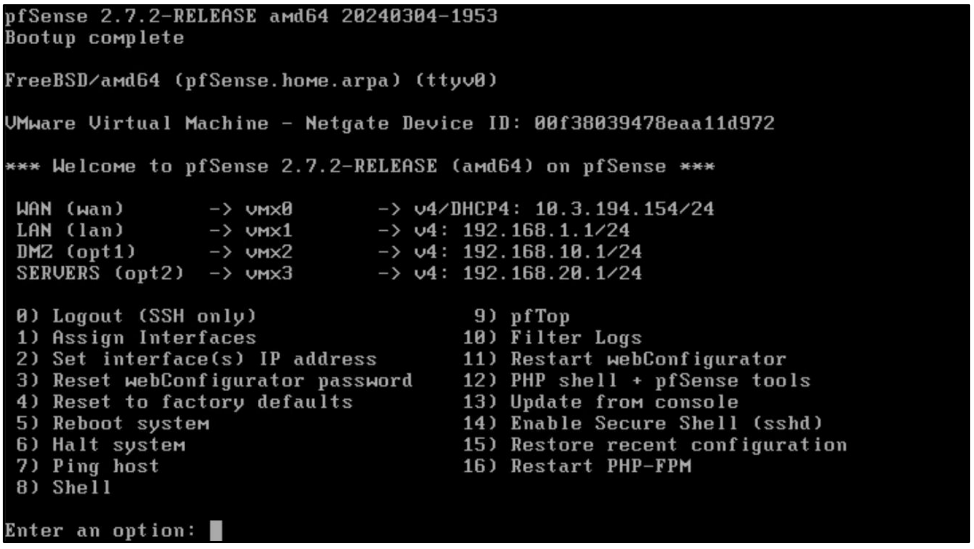


Figura 42. Configuración IP del firewall

- Instalación del paquete de pfSense OpenVPN Agent configuration

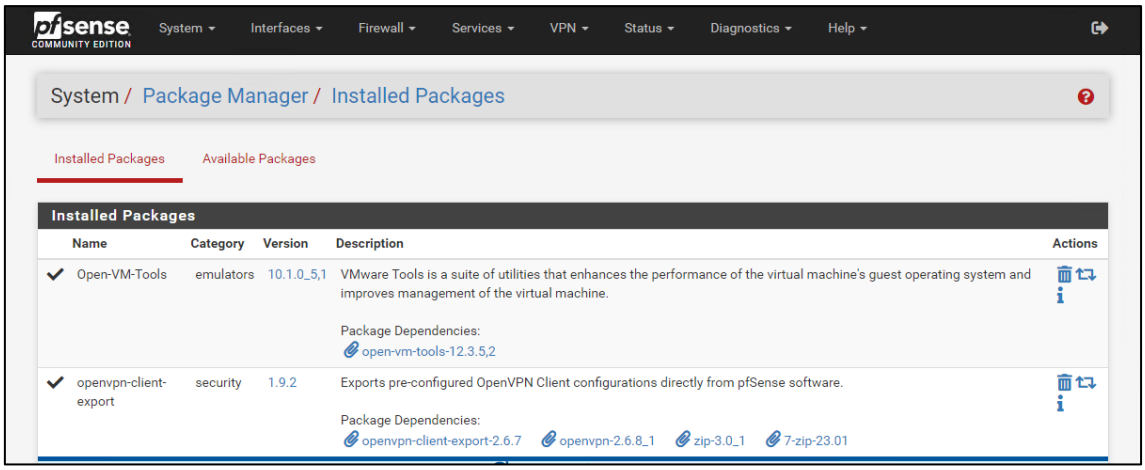


Figura 43. Instalación del paquete *openvpn-client-export*

- Creación del usuario sysadmin para la VPN

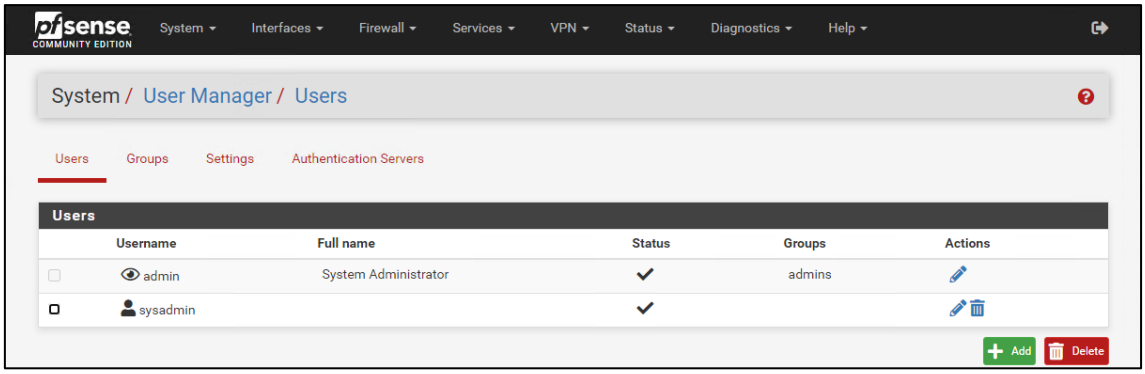


Figura 44. Usuario creado en el firewall para el acceso VPN

- Configuración del servicio de VPN con OpenVPN.

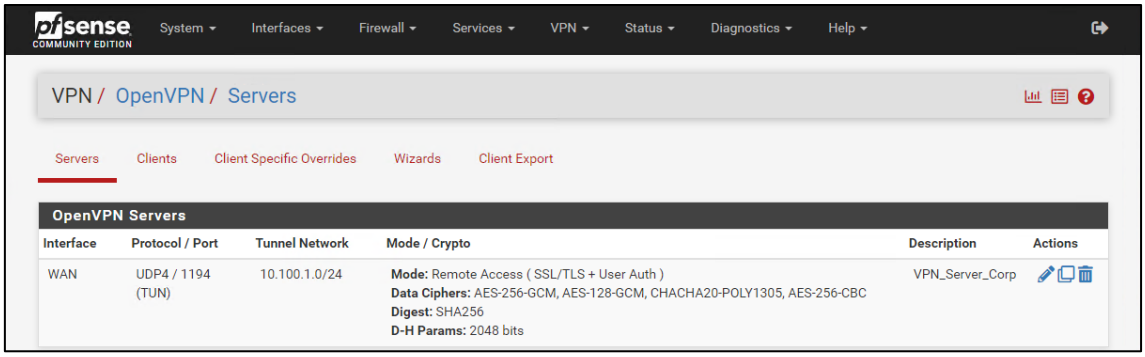


Figura 45. Parámetros de configuración del servidor VPN

- Configuración del paquete de generación de configuración del cliente
- Configuración de direcciones IP virtuales para la publicación de servicios:
  - 10.3.194.60
  - 10.3.194.61
  - 10.3.194.62

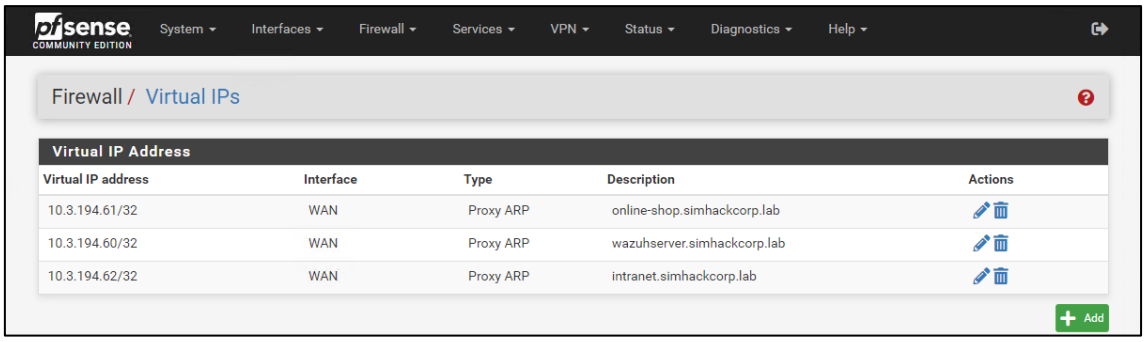


Figura 46. Asignación de IPs virtuales

- Configuración de NAT 1:1 de los servicios publicados por el firewall

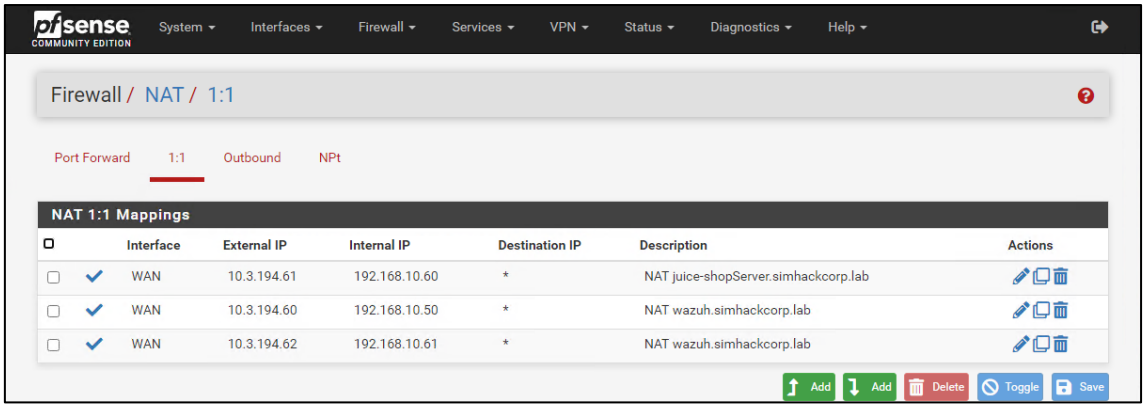


Figura 47. Configuración de NAT 1:1 para la publicación de servicios

- Creación de reglas de acceso para todas las zonas del firewall

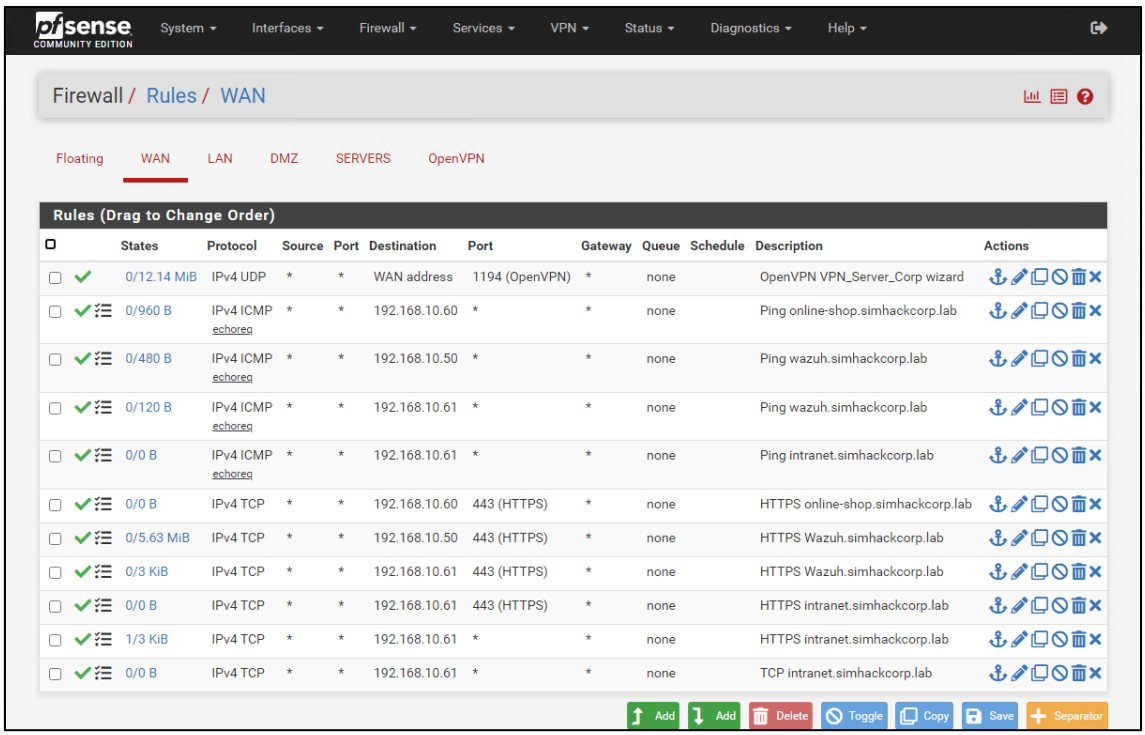


Figura 48. Conjunto de reglas definido en la zona WAN del firewall

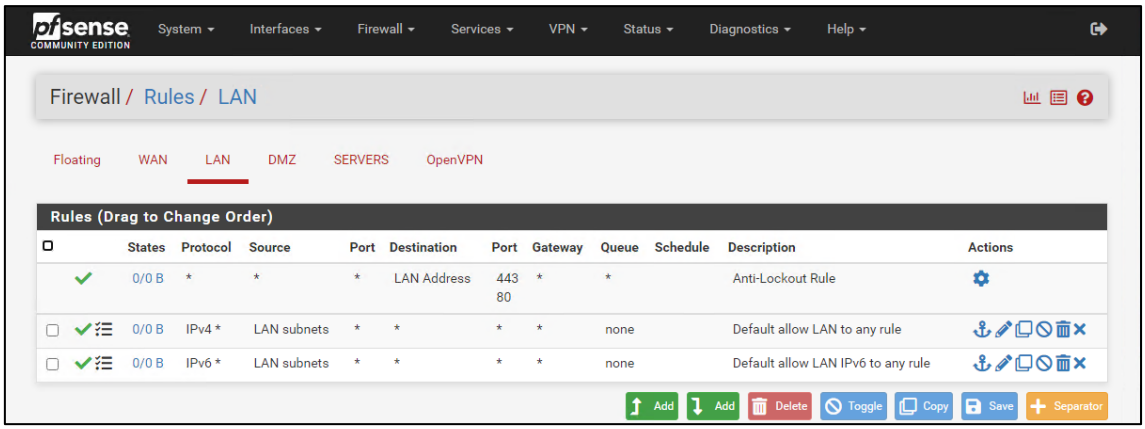


Figura 49. Conjunto de reglas definido en la zona LAN del firewall

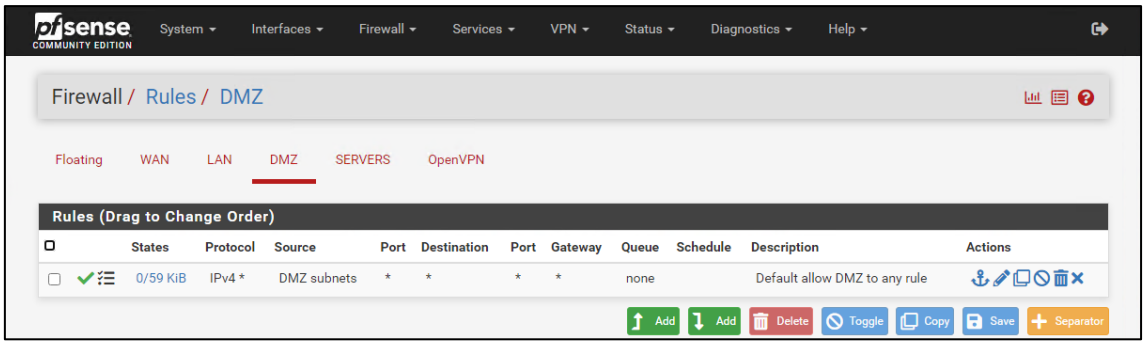


Figura 50. Conjunto de reglas definido en la zona DMZ del firewall

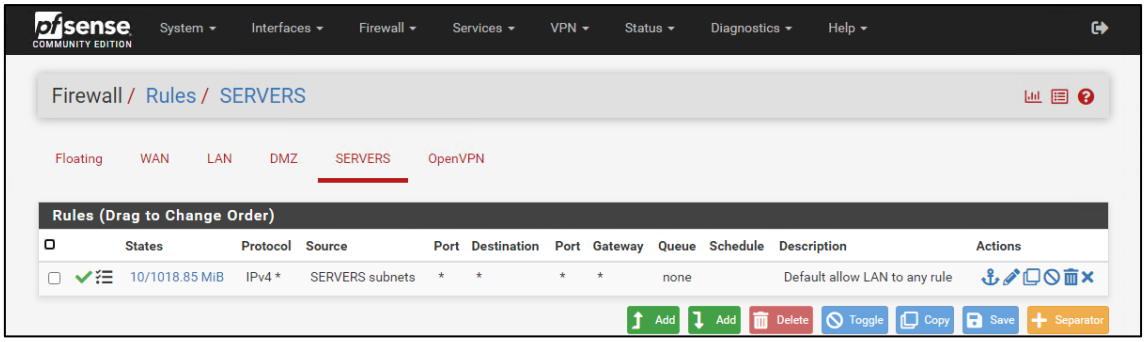


Figura 51. Conjunto de reglas definido en la zona SERVERS del firewall

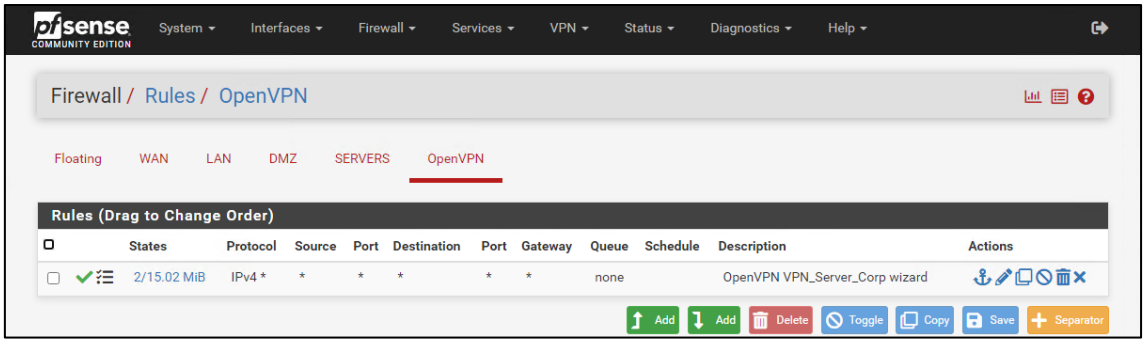


Figura 52. Conjunto de reglas definido en el firewall para el túnel VPN

2. Servicio de directorio

Despliegue de una instancia básica de Windows Server 2012 con una interfaz conectada a la LAN150 del entorno de *cloud*. Tras su despliegue se completa el proceso de sysprep y se le configura una contraseña al usuario administrador del sistema. El resto de la configuración de este sistema se basa en la ejecución de un script de PowerShell que realiza la siguiente configuración de forma automática del sistema:

- Configuración de la red asignando la dirección IP 192.168.20.50 adecuada para la red SERVERS, establece el firewall como puerta de enlace y como DNS el 8.8.8.8 administrado por Google.
- Instalación y configuración de los servicios de DNS y Active Directory
- Se crean las entradas en el servicio DNS de todos los sistemas que forman parte del entorno.
- Se habilita la transferencia de zona para simhackcorp.lab en el servicio DNS.
- Se incluyen las flags que permitirán la implementación del proceso de gamificación que será tratado en detalle en el apartado 7.6.
- Instalación del agente de Wazuh.

3. Servidor de seguridad

Despliegue de una instancia básica de Debian 11 con una interfaz de red conectada a la LAN147:

- Configuración de la red de forma adecuada para ajustarse al direccionamiento utilizado en la red DMZ. Para ello se configura la IP 192.168.10.50 de forma estática y la puerta de enlace será la 192.168.10.1 correspondiente al firewall de la red. El servicio DNS que utilice este sistema para la resolución será el que proporciona el servidor del Directorio Activo a la red interna de la organización.
- Instalación del servicio Wazuh mediante el proceso all-in-one según las especificaciones realizadas por el desarrollador.

4. Servidor de auditorías

Despliegue de una instancia básica de Debian 11 con una interfaz de red conectada a la WAN94

- La configuración de red se realizará automáticamente por el DHCP del entorno de *cloud*.
- Instalación del software Nessus Essential según la documentación oficial del desarrollador. Queda en manos del alumno la realización del registro de la licencia y la inicialización del software.

5. Servidor de bases de datos interno

Despliegue de una instancia de máquina virtual del sistema “PYEXP: 1” del repositorio de retos de ciberseguridad vulnhub, con una interfaz de red conectada a la LAN150:

- Configuración de la red de forma adecuada para ajustarse al direccionamiento utilizado en la red SERVERS. Para ello se configura la IP 192.168.20.62 de forma estática y la puerta de enlace será la 192.168.20.1 correspondiente al firewall de la red. El servicio DNS que utilice este sistema para la resolución será el que proporciona el servidor del Directorio Activo a la red interna de la organización.
- Se incluyen las flags que permitirán la implementación del proceso de gamificación posteriormente.

6. Servidor Web tienda virtual

Despliegue de una instancia básica de Debian 11 con una interfaz de red conectada a la LAN147:

- Configuración de la red de forma adecuada para ajustarse al direccionamiento utilizado en la red DMZ. Para ello se configura la IP 192.168.10.60 de forma estática y la puerta de enlace será la 192.168.10.1 correspondiente al firewall de la red. El servicio DNS que utilice este sistema para la resolución será el que proporciona el servidor del Directorio Activo a la red interna de la organización.
- Cambio del nombre de host a juice-shop.
- Ejecución del script de Bash InstallJuiceShop.sh que realiza el proceso de instalación de la aplicación juice-Shop.

7. Servidor Web de la intranet

Despliegue de una instancia de máquina virtual del sistema "BASIC PENTESTING: 1" del repositorio de retos de ciberseguridad Vulnhub, con una interfaz de red conectada a la LAN147:

- Configuración de la red de forma adecuada para ajustarse al direccionamiento utilizado en la red DMZ. Para ello se configura la IP 192.168.10.61 de forma estática y la puerta de enlace será la 192.168.10.1 correspondiente al firewall de la red. El servicio DNS que utilice este sistema para la resolución será el que proporciona el servidor del Directorio Activo a la red interna de la organización.
- Se generan de forma manual, las flags que permitirán la implementación del proceso de gamificación posteriormente.

8. Equipo atacante

Despliegue de una instancia del sistema Kali en la WAN03:

- La configuración de red se realizará automáticamente por el DHCP del entorno de *cloud*. Queda en manos del alumno, durante el proceso de aprendizaje su actualización y personalización.

6. Memoria de integración del sistema con los contenidos didácticos

Proyecto: Desarrollo de un entorno de simulación como laboratorio de prácticas especializado en ciberseguridad

Descripción de los contenidos didácticos y propuesta de practicas

Contenido

Historial de Versiones

Fecha	Versión	Autor	Organización	Descripción
28/05/2024	1.0	Jose García		

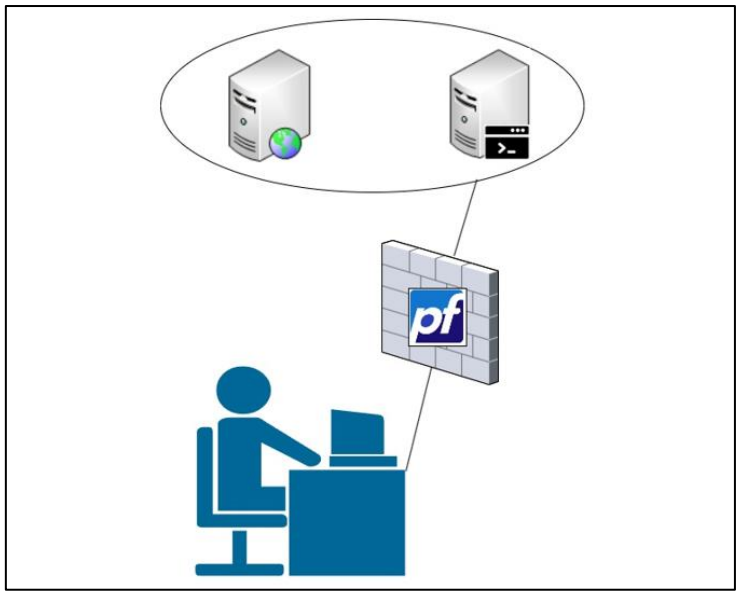
Información del Proyecto

Empresa / Organización	
Proyecto	*Desarrollo de un entorno de simulación como laboratorio de prácticas especializado en ciberseguridad*

Aprobaciones

Nombre y Apellido	Cargo	Departamento u Organización	Fecha	Firma

Módulo 1: Introducción al curso



Este primer módulo del curso realiza una introducción al curso y al entorno en el que se desarrollan los contenidos. Este módulo se divide en los siguientes capítulos:

7. Descripción del curso y sus contenidos.
8. Introducción al laboratorio de seguridad.
9. Implementación de una arquitectura básica de seguridad.

Para la realización de las prácticas de este módulo, será el propio alumno el que despliegue las instancias los distintos sistemas mediante las plantillas adecuadas. Para su desarrollo, se proporcionará al alumno los recursos necesarios para el despliegue, las credenciales de acceso al sistema, las plantillas de sistema operativo necesarias y el conjunto de redes requerido.

Tras el despliegue, cada una de las prácticas asociadas permitirán al alumno adquirir los conocimientos básicos del entorno de *cloud* mientras se trabajan contenidos muy básicos de seguridad informática pero que servirán de base para el desarrollo de los siguientes módulos.

Este módulo abordará la configuración básica de este tipo de arquitectura, reforzando los conceptos de zona de seguridad en un firewall bastión, y la caracterización que tiene cada tipo de zona, como por ejemplo el propósito de cada una o el nivel de seguridad que la caracteriza.

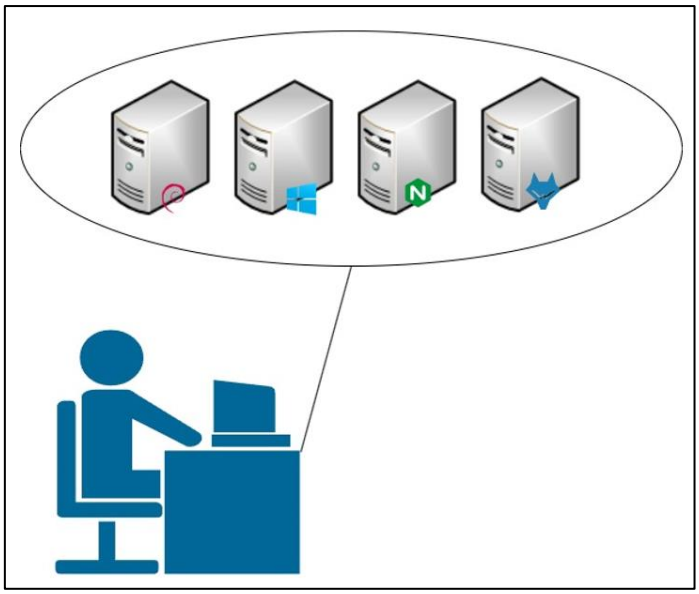
Finalmente, el módulo abordará el concepto de publicación de servicios en sus dos variantes, mediante la traducción de IP y la redirección de puertos. A continuación, se describe la propuesta de las prácticas que podrán ser realizadas durante el módulo 1:

Práctica 1. Despliegue de un firewall perimetral.	
Descripción:	Despliegue de una instancia de pfSense con tres interfaces que corresponden a zonas básicas de la configuración de un firewall perimetral, WAN, LAN y DMZ.
Objetivos:	• Conocer el entorno de *cloud*. • Introducir conceptos básicos de seguridad como un firewall o sus zonas de seguridad.
Resultados de aprendizaje:	• Adquirir las destrezas adecuadas para trabajar con el entorno de *cloud*. • Adecuar la estructura general de un firewall que realiza la función de bastión en una organización. • Habrán adquirido los conocimientos básicos para diferenciar las características de una red WAN, LAN y DMZ.

Práctica 2. Publicación de servicios: Port address translation (PAT).	
Descripción:	Despliegue de un sistema Debian en el cual se deberá instalar el servidor web Nginx y publicar el servicio SSH y HTTP a través de la ip del propio firewall utilizando la redirección de puertos (PAT).
Objetivos:	• Instalación de un servidor web. • Configuración de PAT sobre un firewall.
Resultados de aprendizaje:	• Instalación de un servicio web. • Configuración de reglas para la redirección de puertos. • Configuración de reglas de control de acceso en el firewall.

Práctica 3. Publicación de servicios: Network address translation (NAT).	
Descripción:	Despliegue de un sistema Debian en el cual se deberá instalar el servidor web Nginx y se publicarán los servicios SSH y HTTP a través del firewall por medio de una IP virtual de forma que todas las peticiones que reciba el firewall sean reenviadas al sistema Linux.
Objetivos:	• Configuración de IP virtuales en el firewall. • Configuración de NAT sobre el firewall.
Resultados de aprendizaje:	• Configuración de IP virtuales en el firewall. • Configuración de la traducción de direcciones de red (NAT). • Configuración de reglas de control de acceso en el firewall.

Módulo 2: Espacio de ejecución seguro



Este segundo módulo constituye una introducción al área técnica de la ciberseguridad desarrollando una serie de conceptos y recursos básicos desde la perspectiva de la seguridad informática para la implantación de sistemas informáticos con el objetivo de garantizar su protección. El segundo módulo se compone de los siguientes capítulos:

10. Estándares sobre sistemas de ejecución segura.
11. Bastionado de sistemas.
12. Sistemas de detección de vulnerabilidades.
13. Sistemas de gestión de eventos e información de seguridad.

Para el desarrollo de este módulo, se desplegará la arquitectura de la simulación completa, descartando los sistemas creados durante el primer módulo del curso y ofreciendo una primera visión básica del entorno desde el exterior de la red empresarial.

El desarrollo de las prácticas asociados a los contenidos didácticos de este segundo módulo se realizará sobre una infraestructura mixta. Por un lado, el alumno tendrá disponibles las plantillas básicas de sistema operativo necesarias para abordar los contenidos relacionados con el bastionado, junto con una instancia de un sistema Debian con la aplicación Nessus preinstalada que le permitirá realizar el análisis y evaluación de los equipos bastionados.

Por otro lado, se proveerá al alumnado de las credenciales de acceso al sistema Wazuh de la arquitectura final de la simulación. Este acceso se realizará por medio de la interfaz web del servidor Wazuh, publicada a través del firewall perimetral de la simulación.

Es importante mencionar que tanto el firewall de la simulación como el directorio activo están preconfigurados para integrarse con el sistema Wazuh. Por un lado, el firewall estará reenviando los logs que genera al servicio de syslog remoto de Wazuh. Por su parte, el directorio activo de la simulación ya lleva el agente de Wazuh preinstalado y configurado para conectarse al servicio. Esta configuración básica de los servidores de la red, permitirán que el alumno conozca el entorno de la aplicación Wazuh y haga la configuración básica del servicio.

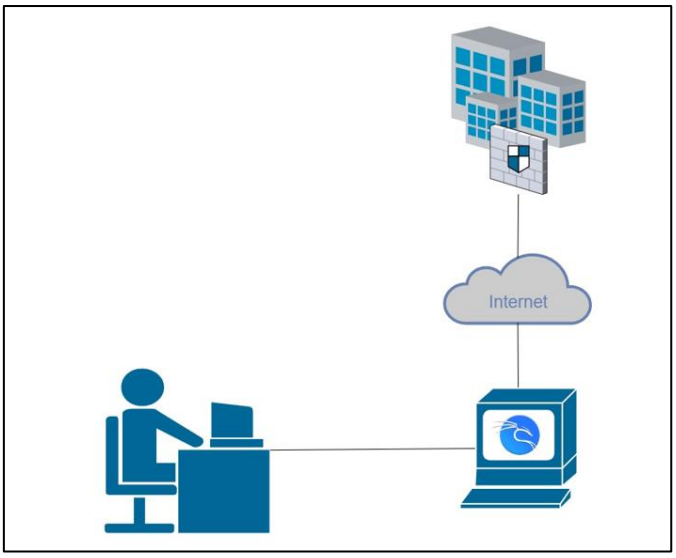
Práctica 1. Bastionado de un OS	
Descripción:	Realizar el bastionado de un sistema operativo en base a la documentación obtenida de fuentes confiables en este ámbito como por ejemplo las guías proporcionadas por el Centro criptográfico nacional (CCN-CERT).
Objetivos:	• Realizar el bastionado de un sistema operativo.
Resultados de aprendizaje:	• Conocer el concepto de bastionado o fortificación de un sistema operativo. • Conocer fuentes de documentación adecuadas en el ámbito de la ciberseguridad.

Práctica 2. Bastionado de un servicio	
Descripción:	Ampliación del trabajo realizado en la práctica 1 incluye el bastionado de un servicio sobre un sistema operativo ya fortificado.
Objetivos:	• Definir el concepto de servicio frente al de sistema operativo • Implementar las medidas adecuadas para realizar el bastionado del servicio basado en la documentación aportada por una fuente de información confiable.
Resultados de aprendizaje:	• Distinguir el concepto de servicio y sistema operativo. • Conocer los mecanismos de fortificación de un servicio

Práctica 3. Uso de herramientas de detección de vulnerabilidades: NESSUS	
Descripción:	Introducción al uso de herramientas de detección de vulnerabilidades y la generación automática de informes de seguridad.
Objetivos:	• Configurar una herramienta de detección de vulnerabilidades. • Definir un proceso de escaneo utilizando la herramienta Nessus. • Generar un informe de vulnerabilidades.
Resultados de aprendizaje:	• Aprender a configurar una aplicación de escaneo de vulnerabilidades. • Conocer el proceso para realizar un escaneo de vulnerabilidades automatizado. • Generación de un informe de resultados automatizado.

Práctica 4. Configuración básica SIEM: Wazuh	
Descripción:	Configuración básica de un SIEM que permita centralizar y analizar los logs de seguridad de una red.
Objetivos:	• Introducir conceptos básicos como SIEM o logs. • Conocer la herramienta Wazuh. • Realizar la configuración básica de agentes en el sistema. • Realizar la configuración básica para permitir la recepción de logs a través de la red.
Resultados de aprendizaje:	• Conocer el concepto de SIEM y XDR. • Aprender a realizar la configuración básica de un sistema de centralización de logs.

Módulo 3: Hacking ético.



Este módulo se centra en el desarrollo de los contenidos relacionados con las auditorías de seguridad, así como el conjunto de técnicas y herramientas utilizadas en el proceso de pentesting. Su desarrollo queda dividido en los siguientes capítulos:

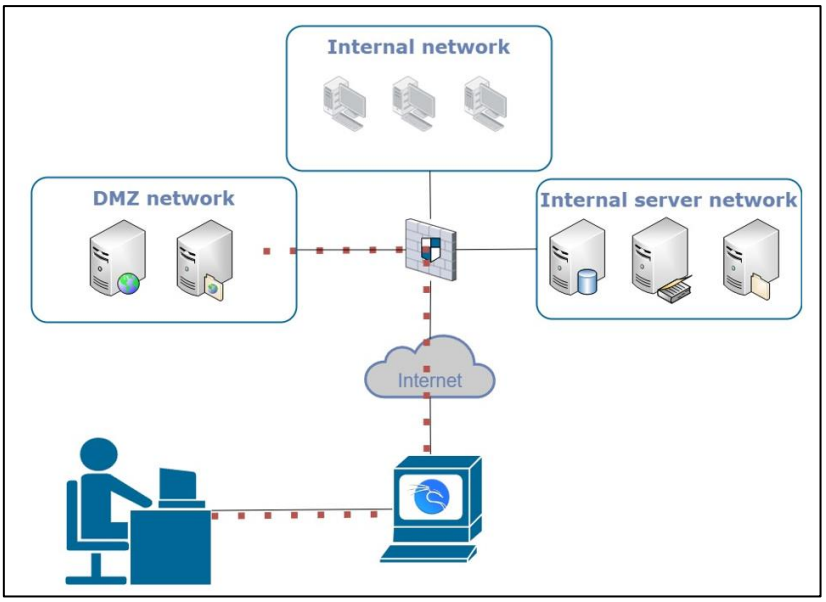
11. Introducción al hacking ético: Fases, alcance, tipos de auditoría.
12. Recopilación de información
13. Análisis de vulnerabilidades
14. Herramientas y técnicas de ataque
15. Documentación de la auditoría

Práctica 1. OSINT	
Descripción:	Aprender los conceptos necesarios y técnicas básicas en la recolección de información de fuentes públicas (OSINT).
Objetivos:	• Conocer el concepto de OSINT. • Conocer el concepto de fuentes públicas de información. • Aprender técnicas y herramientas de recolección de información de fuentes públicas.
Resultados de aprendizaje:	• Conocer el concepto de OSINT. • Conocer el concepto de fuentes públicas de información. • Aprender técnicas y herramientas de recolección automatizadas.

Práctica 2. Vulnerabilidades web	
Descripción:	Utilizar técnicas de ataque especializadas para extraer información y atacar sistemas informáticos basados en entorno web.
Objetivos:	• Conocer las principales vulnerabilidades de entorno web. • Extraer información de las técnicas de recolección de información focalizando el objetivo en la tienda virtual de la simulación.
Resultados de aprendizaje:	• Aprender a identificar y explotar las principales vulnerabilidades web. • Aplicar técnicas de recolección de información en entornos web.

Práctica 3. Análisis de vulnerabilidades. Nmap, NESSUS	
Descripción:	Aprender a utilizar herramientas de análisis de vulnerabilidades como Nmap y Nessus.
Objetivos:	• Conocer el funcionamiento de las herramientas Nmap y Nessus • Realizar escaneos de red y vulnerabilidades personalizadas sobre sistemas operativos.
Resultados de aprendizaje:	• Aprender a identificar vulnerabilidades utilizando las herramientas y técnicas adecuadas según el entorno • Interpretar los resultados de los escaneos extrayendo la información adecuada. • Aprender a generar informes automatizados de los resultados obtenidos tras un escaneo de vulnerabilidades

Práctica 4. Explotación inicial. Metasploit	
Descripción:	Utilizar el framework Metasploit como herramienta para la explotación de vulnerabilidades en sistemas operativos.
Objetivos:	• Conocer el entorno de Metasploit y sus componentes principales. • Conocer y poner en práctica las técnicas de ataque que permitan explotar vulnerabilidades y tomar el control o acceder a áreas del sistema operativo no autorizadas.
Resultados de aprendizaje:	• Identificar entre un conjunto de vulnerabilidades aquellas que permitan definir una estrategia de ataque adecuada. • Configurar adecuadamente los distintos elementos que requiere la ejecución de un *exploit* sobre Metasploit, como por ejemplo la selección de script adecuado para una vulnerabilidad, parámetros asociados y *payload* adecuado según la necesidad del ataque



Práctica 5. Post-explotación 1. Movimiento lateral	
Descripción:	Realizar actividades de post-explotación enfocadas al reconocimiento de la red interna y el movimiento lateral dentro de la red objetivo.
Objetivos:	• Conocer las distintas técnicas que permiten realizar el reconocimiento de la red interna del objetivo (axfr). • Aplicar técnicas para encadenar ataques para alcanzar zonas internas de la red (Proxychains)
Resultados de aprendizaje:	• Utilizar el DNS interno como fuente de información de la estructura interna de la red. • Configurar correctamente el encadenamiento de ataques por medio de la herramienta Metasploit.

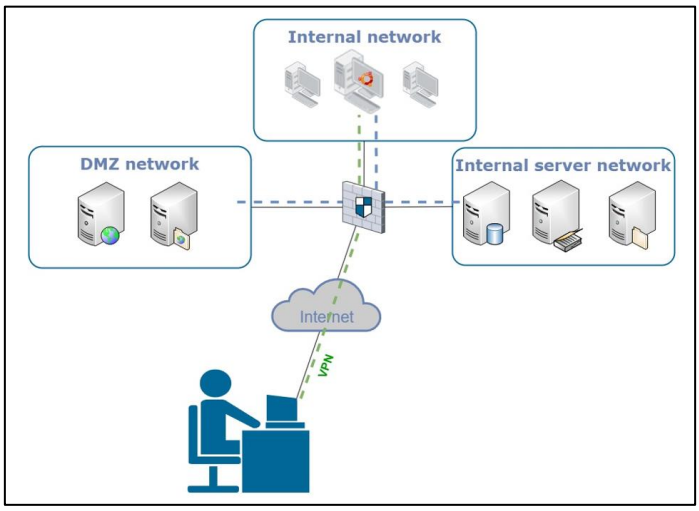
Práctica 6. Post-explotación 2. Servicios internos	
Descripción:	Ampliar el conjunto de técnicas de ataque visto en la fase de explotación mediante la integración de técnicas de ataque sobre servicios internos como bases de datos bases de datos o el servicio de directorio.
Objetivos:	• Conocer las vulnerabilidades y técnicas de explotación de servicios internos. • Realizar ataques dirigidos a bases de datos o servicios vinculados al directorio activo, como SMB o LDAP.
Resultados de aprendizaje:	• Identificar servicios internos de una red • Realizar técnicas de ataque específicas para explotar vulnerabilidades en servicios internos.

Módulo 4: Gestión y respuesta ante incidentes

El cuarto módulo del curso ofrece los conocimientos y habilidades relacionadas con la gestión y respuesta ante incidentes de seguridad.

5. Fuentes de información de amenazas
6. Fases del ciclo de vida de un incidente

6.1. Preparación ante incidentes
6.2. Detección y análisis de incidentes
6.3. Contención, mitigación y recuperación.
6.4. Tratamiento post-incidente: Informe y notificación.



Práctica 1. Detección de Incidentes	
Descripción:	Acceder a los logs centralizados en el SIEM para identificar patrones de comportamiento sospecho o anómalo que sirvan para identificar incidentes de seguridad.
Objetivos:	• Aprender a identificar amenazas y clasificar incidentes de seguridad.
Resultados de aprendizaje:	• Conocer el entorno y las características de un SIEM • Aprender a crear filtros y reglas de búsqueda de eventos • Aprender a identificar y clasificar incidentes de seguridad

Práctica 2. Análisis Forense	
Descripción:	Realizar el análisis forense de los sistemas vulnerados en el desarrollo del módulo 3 para aprender a rastreara el origen y la cadena de eventos que llevaron al compromiso del sistema.
Objetivos:	• Aprender técnicas de análisis forense básicas.
Resultados de aprendizaje:	• Aprender los conceptos básicos del análisis forense de un sistema informático. • Adquirir las capacidades necesarias para rastrear y reconstruir la cadena de eventos de seguridad que conlleva un incidente de seguridad. • Aprender y aplicar el concepto de correlación de eventos para obtener una visión completa de la sucesión de eventos que se producen en un incidente de seguridad.

Práctica 3. Contención, mitigación y recuperación	
Descripción:	Simulación de un ataque sobre uno de los sistemas vulnerables de forma que los estudiantes puedan aprender los procedimientos que se deben seguir para contener este tipo de amenazas.
Objetivos:	• Aprender a definir y aplicar un plan de respuesta ante incidentes. • Conocer medidas para contener o mitigar ataques.
Resultados de aprendizaje:	• Adquirir la capacidad para evaluar el impacto de ataque. • Conocer las acciones que se pueden ejecutar en el proceso de contención o mitigación de un incidente de seguridad.

Práctica 4. Creación de Reglas de Detección Personalizadas	
Descripción:	Los estudiantes aprenderán a crear reglas personalizadas en el servidor Wazuh para detectar tipos de ataques específicos y comportamientos anómalos concretos en el entorno de red de la simulación.
Objetivos:	• Aprender el proceso de creación personalizada de reglas sobre el SIEM.
Resultados de aprendizaje:	• Conocer el formato de reglas que permite personalizar el sistema. • Aprender a crear, implantar y probar reglas en el entorno de Wazuh.

Módulo 5: Seguridad con new generation firewall.

Este último módulo aborda las capacidades y mejoras que aportan los firewalls de nueva generación. Debido a que su realización se lleva a cabo con software propietario queda fuera de la propuesta actual.

7. Documentación de la gamificación del sistema

Proyecto: Desarrollo de un entorno de simulación como laboratorio de prácticas especializado en ciberseguridad

Definición del proceso de gamificación de la simulación de red empresarial

Contenido

Historial de Versiones

Fecha	Versión	Autor	Organización	Descripción
28/05/2024	1.0	Jose García		

Información del Proyecto

Empresa / Organización	
Proyecto	*Desarrollo de un entorno de simulación como laboratorio de prácticas especializado en ciberseguridad*

Aprobaciones

Nombre y Apellido	Cargo	Departamento u Organización	Fecha	Firma

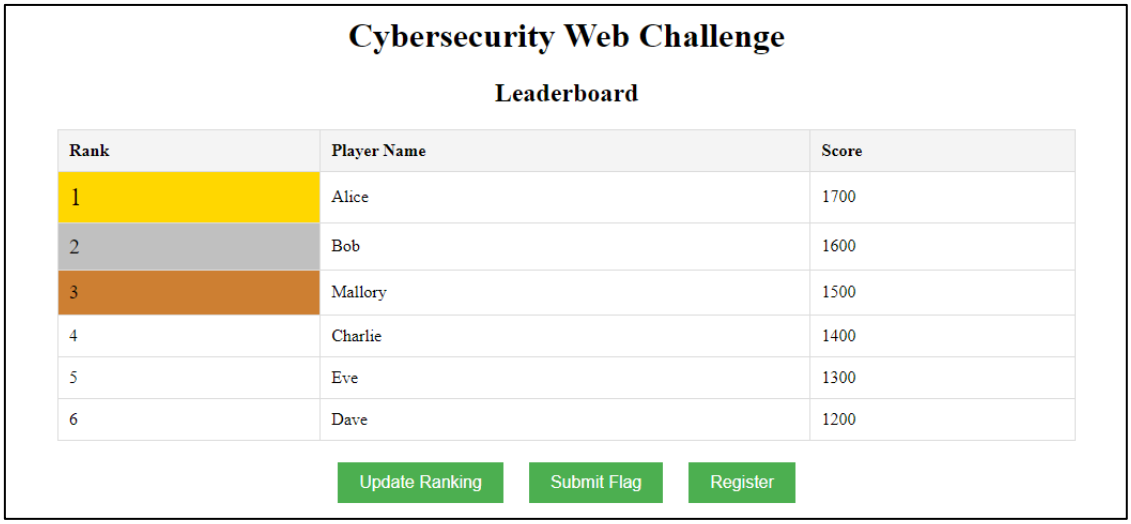
1. Propósito

El propósito del presente documento es definir el proceso de gamificación implementado en el entorno de aprendizaje en ciberseguridad desarrollado como una simulación de red empresarial. Este documento detallará el proceso de gamificación, los componentes del mismo, así como una descripción de la situación de las distintas banderas. Toda esta información debe servir a los docentes que imparten el curso para comprender el funcionamiento del proceso, así como la ubicación y el propósito de cada uno de los elementos que lo componen. Por lo tanto el objetivo final de este documento es facilitar la implantación del proceso que mejore el aprendizaje y sirva como elemento motivador para los estudiantes.

2. Descripción del proceso

El proceso de gamificación del entorno propuesto se basa en una práctica habitual de los retos sobre ciberseguridad, el CTF (capture de flag). Este tipo de retos muy característico de los sistemas vulnerables que se suelen utilizar como entorno de aprendizaje orientados al pentesting, consiste en buscar determinadas "banderas" que se encuentran ocultas en los sistemas que se están vulnerando. Estas flags son secuencias de caracteres que deben ser encontradas por medio de la aplicación de distintas técnicas de ataque que permiten acceder a zonas del sistema o la aplicación que deberían estar protegidas. Este tipo de retos fomentan el interés ya que proporcionan un desafío adicional sobre el entorno y ayuda a que los estudiantes practiquen y refuercen sus habilidades en un contexto práctico y competitivo, incrementando así su motivación y compromiso con el aprendizaje.

En nuestra arquitectura, se ha implementado la gamificación como un reto de CTF a lo largo de toda la red, que se realizará en paralelo al desarrollo del contenido del módulo 3, Hacking ético. Al inicio de este tercer módulo del curso, se presentará el reto que consiste en encontrar un conjunto de banderas que se encuentran escondidas en distintos elementos de la red. Cada una de estas banderas tendrán asociada una puntuación que variará en función de la complejidad de su captura. El alumno podrá acceder a estas banderas atacando los distintos elementos que componen el sistema y con ello accediendo a la secuencia de caracteres que componen cada una de las flag.



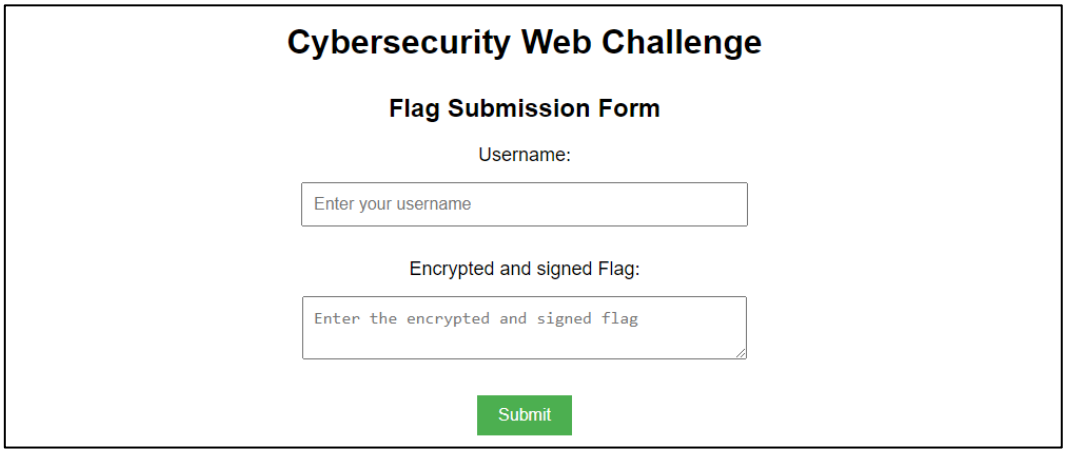
Como elemento adicional, el sistema proveerá un entorno web que ofrecerá un ranking basado en la puntuación obtenida por cada jugador. Este elemento se basará en un diseño que utilizará la criptografía asimétrica y generación de resúmenes de archivos (hash). Utilizando estos dos mecanismos criptográficos de forma adecuada, se consigue que la aplicación lleve el control de las puntuaciones, evitando el uso de contraseñas y asegurando el proceso de gestión de las banderas y asignación de las puntuaciones.

Para implementar estos mecanismos de autenticación y validación, inicialmente el servidor deberá almacenar un archivo con los hashes de las distintas flags así como la puntuación de cada una de ellas. Además, el servidor también generará una pareja de claves que serán utilizadas posteriormente durante el registro y el proceso de validación de

las banderas. La clave pública correspondiente al servidor deberá quedar accesible en la web para que los jugadores puedan descargarla en el momento que vayan a utilizarla.

Por su parte, previo al inicio del registro, el jugador deberá generar un par de claves propias. Posteriormente, al acceder al entorno web el jugador accederá al formulario de registro que le permitirá elegir su nombre de usuario y subir el archivo con su clave pública. El registro quedará completo una vez la aplicación vincule el nombre de usuario con la clave pública del jugador.

Este tipo de registro permite que el proceso de autenticación del jugador que quiera validar una bandera y adquirir la puntuación asociada se realice utilizando su clave privada como mecanismo de autenticación, añadiendo valor al sistema como prueba práctica de las posibilidades que ofrece la criptografía asimétrica. Basándonos en el funcionamiento de la criptografía de clave asimétrica, el diseño de la página de validación de bandera contendrá dos campos, el primero de ellos, un campo de texto donde el jugador deberá introducir su nombre de usuario. El segundo campo de texto se corresponderá con el espacio definido para que el jugador incluya la secuencia de caracteres correspondiente al cifrado y firma de la bandera. Para obtenerlo, el jugador tendrá que realizar un paso previo que consistirá en cifrar la bandera con la clave pública del servidor, que habrá descargado previamente, y firmarla utilizando su clave privada.



Según la mecánica definida, el jugador podrá ir acumulando puntos en su casillero del *ranking* adquiriendo las distintas banderas escondidas por la red. Una vez se capture una bandera, según lo comentado sobre el proceso de validación de bandera, el jugador deberá

acceder a la página del entorno web de validación y rellenar los campos solicitados: la cadena de caracteres correspondiente a su nombre y el bloque de texto que contendrá el cifrado y firma de la bandera. Tras realizar el envío, el sistema de puntuación validará mediante la clave pública del usuario que la firma se corresponde con la del jugador, realizando el proceso de autenticación. Posteriormente, se descifrará el contenido del mensaje mediante la clave privada del servidor. Por último, el servidor calculará el hash de la bandera proporcionada por el jugador y lo comparará con el listado de hashes que tiene almacenados correspondiente a las banderas registradas inicialmente en la aplicación. De esta forma el servidor comprobará que efectivamente el jugador ha enviado una de las *flags* y se acumulará la puntuación establecida para esa bandera a la puntuación total del jugador. Tras la asignación de la puntuación al usuario, se actualizará el *ranking* y el resto de los participantes podrán consultar el nuevo estado de la competición.

A continuación, se proporciona la ubicación concreta donde se han escondido banderas en el entorno:

- intranet.simhackcorp.lab
    - Se ha incluido una flag en la raíz del servidor web.
    - Se ha incluido una flag en el archivo robots.txt del servicio web.
    - Se ha incluido una flag en la raíz del servidor ftp.
    - Se ha incluido una flag en la carpeta del usuario root.
- ddbbserver.simhackcorp.lab
    - Se ha incluido una flag en la carpeta del usuario root del servidor.
    - El timestamp asociado a la decodificación del registro que se encuentra en la base de datos será considerado una key.
- ADserver.SimHackCorp.lab
    - Servidor DNS. Se ha creado un registro DNS de tipo txt que devuelve una cadena de caracteres. La bandera podrá ser alcanzada utilizando el ataque axfr que devolverá la copia completa de la zona DNS del servidor.
    - En la carpeta de documentos del administrador del sistema se ha añadido un archivo denominado flag.txt.

Se ha compartido una unidad de red oculta que tiene otro archivo flag.txt.