Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE GRADO

Diseño e implementación de una maqueta de máquinas virtuales en red para simulación de ejercicios de ciberdefensa

Grado en Ingeniería Mecánica

ALUMNO: Víctor Romero Fernández

DIRECTORES: Belén Barragáns Martínez

Pablo Sendín Raña

CURSO ACADÉMICO: 2015-2016

Universidade Vigo

Centro Universitario de la Defensa
en la Escuela Naval Militar

TRABAJO FIN DE GRADO

Diseño e implementación de una maqueta de máquinas virtuales en red para simulación de ejercicios de ciberdefensa

Grado en Ingeniería Mecánica

Intensificación en Tecnología Naval

Infantería de Marina

Universidade Vigo

RESUMEN

En 2014 España fue el tercer país que más ciberataques sufrió y se prevé que el número de estos incidentes se seguirán incrementando en el tiempo. Estos episodios abarcan desde lo simplemente molesto a los actos de ciberguerra que ponen en riesgo la seguridad nacional. La formación en materia de ciberdefensa es una prioridad marcada en el plan de seguridad nacional. Los fundamentos teóricos son fácilmente impartibles en un aula, pero deben ser complementados con prácticas para conseguir el aprendizaje deseado. Sin embargo, la realización de ejercicios prácticos de ciberdefensa sobre sistemas en producción puede tener consecuencias catastróficas. En este trabajo se diseña e implementa una maqueta que proporcione un entorno aislado, seguro y realista en el cual llevar a cabo diversos ejercicios de ciberdefensa. La maqueta, que utiliza virtualización, implementa una arquitectura de red con tres zonas: Internet, DMZ e Intranet. En la DMZ se han instalado diferentes servicios comunes en las redes empresariales. En la Intranet se encuentran los equipos de los usuarios protegidos de las amenazas exteriores. La seguridad de la red corre a cargo de un cortafuegos, también virtualizado, que se encarga de hacer la separación entre las tres zonas así como el filtrado de paquetes en base a unas reglas de seguridad establecidas. La maqueta ha sido validada y se ha verificado que cumple con los requisitos iniciales.

PALABRAS CLAVE

Ciberdefensa, Virtualización, Servidores, Seguridad, Maqueta

AGRADECIMIENTOS

A mis padres y hermano, por apoyarme en todas mis decisiones aunque no siempre les sean agradables. Y por capitanear los primeros años de mi vida que me han hecho ser como soy.

A Marisma, por aportar su sonrisa a cada día de mi vida e iluminarlos sin importar cuán densa sea la oscuridad que los envuelve. Y por saber soportar estoicamente las ausencias que le hago sufrir.

A mis tutores, Belén y Pablo, por su extraordinaria labor de guiado sin la cual el trabajo se hubiese convertido ineludiblemente en pesadilla.

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Introducción a Internet

Si se trata de imaginar un día sin Internet, una mayoría pensará que el planeta probablemente se paralizaría. A lo largo de la historia, revoluciones tecnológicas han cambiado la sociedad y la economía del mundo. Ejemplos como el descubrimiento de la penicilina o la invención de la máquina de vapor demuestran cómo la tecnología y la ciencia marcan las pautas para la evolución de la sociedad.

Sin duda, en el siglo XX se ha desarrollado un cambio drástico en la forma de vivir de los habitantes de casi todos los rincones del mundo a raíz de la invención de Internet. Algunos investigadores creen que Internet puede incluso marcar el inicio de una nueva edad histórica: la edad de las comunicaciones y la información, dándole a la invención de Internet la misma trascendencia que tuvo la invención de la imprenta o la revolución francesa.

En 1960, J.C.R. Licklider comprendió la necesidad de una red mundial, según consta en su documento de enero de 1960, *Man-Computer Symbiosis* [1].

En los años posteriores se desarrollaron los primeros estudios sobre interconexión de computadores y conmutación de paquetes por parte de diferentes agencias gubernamentales y militares de EEUU. La primera implementación, ARPANET, transmitió sus primeros paquetes en 1969.

Han pasado menos de 50 años e Internet ha experimentado un crecimiento viral hasta hacerse imprescindible a día de hoy. Las cifras lo demuestran. En el año 2015 había casi 4.000 millones de usuarios en Internet; 3.000 millones de cuentas de usuarios únicos en redes sociales y alrededor de 1.000 millones de páginas webs activas en la Internet indexada [2].

La repercusión en la economía también es trascendental: en 2014 se realizaron 60 millones de transacciones monetarias a través de la red. Las grandes empresas de Internet manejan cifras impresionantes como, por ejemplo, los 89.000 millones de dólares que factura Amazon en un año (2015) o los 17.000 millones de dólares que factura Google. Internet no solo queda para los grandes magnates que basan su negocio en esta tecnología. Hoy en día, una de las máximas de los publicistas es “Quien no está en Internet, no existe”, y se aplica a empresas de todos los tamaños.

Además del impacto en la economía mundial, Internet proyecta su sombra en la vida de todos. Es muy probable que Internet influya en todos los aspectos de nuestra vida, desde el trabajo hasta nuestras relaciones sociales. Como se escribía en la primera línea de este documento, un día sin Internet supone un grave problema mundial. No es necesario imaginar el desastre de un colapso global de Internet. Simplemente analizar qué sucede cuando una persona no tiene acceso a la red en ninguna de sus

formas. No podría recibir el pronóstico del tiempo en su *smartphone*, leer el periódico en su *tablet* al levantarse, no podría escribir a su pareja por *whatsapp*, no sería capaz de consultar el estado de su cuenta bancaria ni hacer operaciones en ella, ni siquiera podría sacar dinero en un cajero o pagar con una tarjeta de crédito.

Por otro lado, lo realmente sorprendente de Internet es la información propiamente dicha, sobre todo la cantidad. No hay estudios certeros que puedan determinar cuanta información hay en la red de redes. Sin embargo, expertos como el director de Google, Eric Smith, sostienen que en el año 2015 en la red había 5ZB (ZettaByte) de datos [3]. La mente humana no tiene capacidad para imaginar esa cantidad de información. Para intentarlo hay que pensar primero en que todas las páginas indexadas por el buscador de Google corresponden al 0,004% de esta cantidad.

Entre estas cifras tan abultadas de datos se encuentra información de toda índole e importancia, desde los documentos con mayor clasificación de seguridad de un gobierno hasta contenido de entretenimiento público. Además hay que tener presente que entre los 5 ZettaByte que ocupa Internet probablemente haya datos personales como fotos, información bancaria o correos electrónicos de todos los usuarios que en algún momento han navegado por Internet.

1.2 Amenazas

Pocos pueden encontrarse cómodos sabiendo que sus datos se encuentran tan expuestos. Sin embargo, que los datos personales se encuentren en Internet, o mejor dicho, accesibles desde Internet, no significa que sea información pública o que esté disponible para todas las personas que están conectadas a la red. Los avances de la informática y de la criptografía han permitido dotar a la red de una cierta seguridad. Los ordenadores y servidores pueden protegerse tras *firewalls*, y los datos se pueden encriptar antes de transmitirse o almacenarse. Sin embargo, Antonio Ramos, conocido *hacker ético* y profesor de diferentes masters y posgrados en seguridad informática, sostiene que “La seguridad total en Internet no existe, o tendría un coste infinito” [4].

No se puede obviar que a Internet también están conectadas algunas de las infraestructuras críticas de los estados como pueden ser las centrales eléctricas, incluidas las nucleares, o las infraestructuras de transporte de combustibles.

En este entorno tan amplio y relevante que ha terminado por llamarse “ciberespacio” también hay delincuentes. La ciberdelincuencia es el conjunto de actividades ilícitas en las que se utiliza Internet y un dispositivo conectado a ella. El espectro de actividades es muy amplio y abarca desde la invasión de la intimidad personal o el robo de información sensible a estafas o extorsiones.

El ciberespacio proporciona un medio donde los ciberdelincuentes pueden llevar a cabo ataques muy rentables. Esto se debe a la sencillez de los medios que requieren los atacantes para llevar a cabo sus actividades. Y, en principal medida, a la dificultad para rastrear un ataque y poder conocer su autoría.

La ciberguerra es el término acuñado para hacer referencia a un conflicto de carácter bélico, cuyo campo de batalla sea el ciberespacio. El especialista en seguridad informática del gobierno estadounidense Richard Clarke cree que la guerra cibernética comprende las acciones llevabas a cabo por un estado para penetrar en las redes u ordenadores de otro estado que tengan la finalidad de causar perjuicio o alteración [5].

Las actividades ilícitas llevadas a cabo a través de la red se encuentran en un vertiginoso aumento desde el año 2005. En octubre de 2015, España había interceptado 68 ataques a infraestructuras críticas, el mismo número que todo 2014; según señala el periódico El Mundo en su noticia “63 'ciberataques' en lo que va de año contra infraestructuras críticas del Estado” de 26 de octubre. Sin embargo, las cifras son más alarmantes si ampliamos nuestro campo de visión fuera de las infraestructuras definidas como críticas por el estado. El total de los ataques detectados por el Instituto Nacional de Ciberseguridad (INCIBE) asciende en 10 meses a más de 36.000. Estos ataques tenían

como objetivo usuarios particulares, empresas o corporaciones, e incluso la red de educación e investigación científica RedIRIS, y tenían objetivos diversos como pueden ser la denegación de servicio o el robo de datos. El INCIBE señala entre los principales atacantes a grupos terroristas, miembros del crimen organizado y estados potencialmente adversos, aunque también es cierto que cualquier persona con conocimientos suficientes puede perpetrar ataques en solitario. Es reseñable el hecho de que el 60% de los ataques provenga de personal interno a la organización perjudicada. [6]

Este negro panorama se lleva gestando más de una década y no ha pasado desapercibido por los gobiernos, quienes conscientes de la importancia de proteger y protegerse en el espacio cibernético han incluido éste en los planes de seguridad y defensa de más alto nivel.

1.3 Ciberseguridad y ciberdefensa

La importancia que tiene en todos los aspectos de la sociedad actual la informática, y su creciente inseguridad son un problema que se debe abordar. Si nos remontamos en la historia, ya desde los inicios de Internet existía un interés en proteger a los usuarios y servicios.

Actualmente hay dos términos diferenciados: *ciberdefensa* y *ciberseguridad.* Aunque ambos hacen referencia a la protección del espacio cibernético, sus objetivos son diferentes. Por una parte, la *Ciberdefensa* es el conjunto de iniciativas, actividades y tecnologías con las cuales un estado se protege en el mundo cibernético. Este término está ligado a la c*iberguerra*, es decir, su objetivo es contribuir a la defensa nacional mediante actividades en las redes de comunicaciones.

Por otro lado, la *ciberseguridad* es un tema más amplio, que se extiende fuera de la defensa nacional hasta todos y cada uno de los ciudadanos que dispongan de un terminal con acceso a la red. En muchas ocasiones, el estado puede llevar a cabo iniciativas de ciberseguridad, pero no es cometido suyo exclusivamente. Al igual que la seguridad ciudadana, la ciberseguridad es cosa de todos y cada uno de los ciudadanos. En esta materia, además de las medidas e iniciativas estatales, se incluyen las acciones que toman las empresas y organizaciones para protegerse.

1.4 Objetivos del TFG

En este trabajo de fin de grado se plantea como objetivo principal la creación de una herramienta informática con la finalidad de colaborar en algunas de las líneas de actuación marcadas en el Plan Nacional de Seguridad. La herramienta proporcionará un entorno controlado en el cual desarrollar ejercicios y futuras líneas de investigación en las materias de ciberdefensa y ciberseguridad, contribuyendo así a la formación del personal, la investigación de vulnerabilidades,y su corrección y, lo que es más importante, a la creación de una conciencia colectiva de ciberseguridad.

Para ello se propone la construcción de una maqueta basada en la virtualización, en la cual se puedan configurar y simular redes completas ya sean reales o teóricas. La virtualización permitirá llevar a cabo las mismas pruebas o ejercicios que se pueden ejecutar en una red real con una inversión económica menor y sin el peligro inherente a realizar ataques sobre infraestructuras reales.

La maqueta constará de una arquitectura de red dividida en tres zonas: Internet, Zona Desmilitarizada (*DMZ,* por sus siglas en inglés) y red interna. En cada una de las zonas se configurarán los servidores y puestos de trabajo típicos. Para la arquitectura de red, se utilizarán elementos de red virtuales como adaptadores de red, enrutadores y cortafuegos.

1.5 Organización de la memoria

En el primer capítulo se ha realizado una introducción al TFG. Se ha comenzado por un análisis de la importancia que Internet ha cobrado en la vida diaria de todas las personas. También se han presentado las principales amenazas a las que está expuesto cualquier individuo u organización en la

red, como base para justificar la importancia que se le está dando a la ciberseguridad desde hace unos años. Por último, se han presentado los objetivos generales buscados en el trabajo.

En un segundo capítulo, se hace un análisis del contexto en el que se realiza el trabajo. Se analizan las amenazas que están presentes en el ciberespacio y cómo pueden afectar de diferente forma a las personas, empresas y naciones. Para ello, se hace uso de diferentes ejemplos históricos y actuales de ataques. Se presenta también el proceso por el cual la ciberdefensa comienza a ser un tema de importancia para los países, tanto España como otros de la comunidad internacional, y la normativa que recoge esta preocupación de los gobiernos. Posteriormente, se presentan diferentes alternativas para asegurar una red. Por último, se introduce el concepto de virtualización y se analizan las ventajas e inconvenientes de algunas de las herramientas de virtualización disponibles en el mercado; este proceso también se lleva a cabo con los simuladores de red. Estos análisis comparativos del estado del arte tienen como resultado la elección de las herramientas con las que luego se desarrollará el TFG.

En el capítulo tres se desarrolla todo el proceso de implementación de la maqueta. Se ha diseñado una arquitectura de red en tres zonas, de cuya separación se encarga un cortafuegos de tres patas. El modelo imita configuraciones y servicios que son habituales en cualquier empresa. El proceso se ha documentado mediante capturas de pantalla, siendo explicadas cada una de ellas.

En el cuarto capítulo se realiza una validación, para la cual se han llevado a cabo una serie de pruebas que tienen como objetivo mostrar que la maqueta es funcional y, al mismo tiempo, que su configuración de seguridad es realista. Las pruebas, realizadas desde Internet y desde la Intranet, han tenido un resultado satisfactorio.

Por último, en el capítulo cinco se presentan las conclusiones finales tras el desarrollo de este TFG. Estas conclusiones son relativas a los objetivos propios del trabajo, a los conocimientos adquiridos durante su realización, y al posible futuro de esta línea de investigación.

2 ESTADO DEL ARTE

2.1 Introducción

En este apartado de la memoria se realizará un análisis del estado del arte actual. Este análisis comenzará con una aproximación a las amenazas presentes en el ciberespacio, que abarcará desde las amenazas a un país hasta las amenazas a una persona.

Posteriormente, se analizarán las iniciativas que han tenido las diferentes organizaciones internacionales, países y organismos para mitigar los efectos de la ciberguerra y las ciberamenazas. En este subapartado se incluyen acciones concretas y organismos creados en España y sus cometidos en el ámbito citado.

Se finalizará el análisis de documentación introduciendo las diferentes técnicas informáticas en las que se basará este trabajo, y junto con ellas, serán explicados los aspectos más relevantes del software que las implementa. En cuanto al software, se presentarán varias opciones para cada tecnología y se realizará una selección del más adecuado en base a criterios de idoneidad y economía.

2.2 Amenazas en el ciberespacio

Es usual hacer la primera clasificación de las amenazas existentes en la red en función de si existe modificación o no de los datos que pasan por la red. En base a esta clasificación existen ataques pasivos, cuando el atacante solo “escucha” y posteriormente procesa los datos que circulan por la red; y ataques activos, en los cuales el atacante no se limita a “escuchar” la red, si no que transmite información a través de ella.

Dentro de los ataques pasivos se encuentran el s*niffing* y los ataques de ingeniería social. A pesar de que puedan parecer más inofensivos, los ataques pasivos pueden ser muy dañinos y tener consecuencias graves, como el robo de credenciales para suplantación de identidad o pérdida de confidencialidad en comunicaciones de carácter sensible.

Por otra parte, los ataques activos pueden tener finalidades muy variadas entre las cuales se destacan las siguientes por ser las más comunes.

- *Spoofing*: Se llama así a una técnica de suplantación de identidad, en la cual el atacante se hace pasar por un servidor o un dispositivo de la topología de la red, adueñándose así del tráfico de la víctima que tenía como destino ese servicio.
- *Phising*: Esta práctica suele llevarse a cabo por e-mail. El atacante se hace pasar por una organización o persona de confianza y pretende que las víctimas accedan a un servidor malicioso o descarguen código malicioso en sus máquinas.

- *Alteración de mensajes*: Se refiere tanto a mensajes de correo electrónico u otro tipo de comunicaciones entre personas como a mensajes de control entre infraestructuras, por ejemplo, los mensajes que controlan la parada y arranque de las centrales eléctricas. El atacante consigue interceptar un mensaje real y variar su contenido sin que el receptor lo perciba, creando así caos y desconfianza.
- *Code Injection*: La versión más extendida se denomina *SQLInjection* por la tecnología a la cual ataca. El atacante explota vulnerabilidades en aplicaciones o servicios que se encuentran en ejecución en el servidor para poder inyectar código malicioso que será procesado por éste. Puede tener como objetivo modificar una página web, modificar tablas de bases de datos, o ser el punto de partida para una escalada de privilegios en el servidor.
- *Denial of service (DoS)*: El objetivo de este ataque es saturar un determinado servicio para impedir su uso a los usuarios legítimos. En su versión más dañina, *Distributed Denial of Service*, se usan múltiples ordenadores (hasta millones de ellos) para atacar simultáneamente al mismo servidor, o a sus réplicas.

Además de estas amenazas, hay otro tema que preocupa en gran medida a los expertos. La *Deep web* es el nombre que se le ha dado a todo el conjunto de páginas webs que no son indexadas por los buscadores, bien porque sus propietarios no lo desean, o bien porque los propios buscadores deciden no indexarlas. La forma de acceder a esta sección de la red es mediante el uso de la herramienta *TOR (The Onion Router)* [7] cuyo nombre hace analogía a la forma en que la información se articula en capas dentro de la web profunda. De esta forma, el usuario va accediendo a las páginas en cascada y su dirección IP queda oculta. Se hace así imposible la identificación de las personas que navegan por este tipo de páginas.

Es en este entorno de confidencialidad en el que han encontrado su guarida una gran multitud de delincuentes. A día de hoy en la web profunda se da cabida a la actividad criminal tradicional; como por ejemplo tráfico de drogas, tráfico de armas, tráfico de personas, venta de pornografía infantil, venta de documentación robada e incluso asesinos a sueldo. Este tipo de servicios, normalmente de pago, se adquieren con monedas virtuales como *Bitcoin,* que no pueden ser rastreadas por los gobiernos. Sin embargo, la web profunda es también lugar de encuentro de *hackers* y de personas con deseos de perpetrar un ataque pero sin los conocimientos adecuados. Se ha creado así un lugar en el cual se pueden intercambiar técnicas y conocimientos informáticos de todos los niveles. A diferencia de los delitos tradicionales que se han instalado en la web profunda, el intercambio de conocimientos suele ser gratuito.

Una vez descritas en líneas generales, se van a clasificar las amenazas en función de la entidad de la víctima. Se analizarán los ataques a los que pueden estar sometidas naciones, empresas y personas. Pero antes es necesario citar quienes son los actores en este contexto de ciberataques [8]:

- Estados. El espionaje clásico se extiende ahora a esta dimensión.
- Ciberdelincuentes. Personas con una alta formación, cuyo objetivo es el beneficio económico.
- Hacktivistas. Personas o grupos más o menos organizados cuyo objetivo es promover su causa o provocar movimientos políticos, económicos o sociales.
- Terroristas. No se conoce su nivel de formación, pero en los últimos años los ataques se están volviendo más sofisticados y cada vez están más cerca de sus objetivos: causar terror.
- Cibervándalos. Se encuentran cibervándalos con niveles de conocimientos técnicos muy distintos. Su objetivo es demostrar a la comunidad que son capaces de realizar un ataque determinado.
- *Script Kiddies*. Son personas con pocos conocimientos que usan herramientas creadas por otras personas a modo de desafío. Normalmente no son conscientes de las consecuencias de sus actos.

- Ciberinvestigadores. Son personas bien formadas que persiguen el descubrimiento de vulnerabilidades en hardware y software. Sus acciones pueden tener consecuencias cuando las vulnerabilidades son publicadas, ya que otras personas las pueden aprovechar.
- Organizaciones privadas. Motivadas por el interés económico pueden llevar a cabo acciones de espionaje industrial. Normalmente son ataques sencillos, los ataques más complejos pueden ser encargados a ciberdelincuentes que venden estos servicios en la *Deep web*.
- Actores internos. Los actores internos son personas que han tenido o tienen relación con la organización atacada. Pueden realizar ellos mismos los ataques motivados por diferentes causas (poder, dinero, información) o ser aprovechados de forma inconsciente por espías, ciberdelincuentes, hacktivistas o terroristas para iniciar un ataque contra su organización.

2.2.1 Amenazas a la Seguridad Nacional

Tal y como se detalla en [9], el hecho de que el ciberespacio se cite como una fuente de amenazas en el Plan de Seguridad Nacional es demostrativo de que las amenazas informáticas pueden llegar a producir daños a niveles muy altos en la organización de los países.

En documentos emanados de diferentes organizaciones internacionales [10] [11] se pone de relieve la necesidad de contemplar el ciberespacio como un elemento militar. Por lo tanto, a un ciberataque se le puede dar carácter de actividad militar, e incluso de ataque armado contra el estado [12].

La percepción sobre el ciberespacio comenzó a cambiar tras los sucesos de Estonia durante el verano de 2007. “Tres semanas de ciberataques masivos dejó claro que las sociedades de los países de la OTAN adolecían de una elevada vulnerabilidad digital” se puede leer en la revista OTAN [13]. Posteriormente, en 2008 una memoria USB consiguió infectar un portátil del ejército americano en una base de oriente medio; un programa espía se propagó por sistemas clasificados y no clasificados robando así miles de archivos que fueron transferidos a servidores bajo control extranjero. En este momento nació el término de *Ciberespionaje*. Estados Unidos volvió a sufrir un ataque de ciberespionaje en el cual se vieron afectadas 72 empresas, incluyendo 22 oficinas gubernamentales y 13 contratistas de defensa.

La *Ciberguerra*, como se llama al uso de ataques cibernéticos de manera similar a las armas convencionales, en el marco de un conflicto internacional y con unos objetivos determinados, se puso de manifiesto durante el conflicto entre Rusia y Georgia. Durante el desarrollo de este conflicto, el gobierno georgiano recibió ataques masivos continuados sobre sus servidores. Si bien estos ataques no provocaron un daño físico, consiguieron debilitar al citado gobierno durante una fase crítica del conflicto y afectar a la capacidad de comunicar con sus ciudadanos y el resto del mundo.

Otro caso de estudio es del gusano llamado STUXNET [14]. Este gusano podría parecer uno más si no se le analiza en detalle. Sin embargo, ha sido descrito como “prototipo funcional y aterrador de un arma cibernética que conducirá a la creación de una nueva carrera armamentística mundial" por Kaspersky Lab. Este gusano es extrañamente sofisticado y dirigido. Su medio megabyte de código se encarga de tomar el control de ciertos sistemas de control industriales (PLC) del fabricante Siemens. El gusano se ha extendido por millones de ordenadores, pero solo tiene efectos en los que cumplen una serie de características. Ha afectado en concreto a plantas nucleares de Irán, el cual se cree que podría ser el objetivo último del *malware*. El virus explota vulnerabilidades *0-day* (vulnerabilidades recientes que aún no tienen disponible un parche para solucionarlas), pero además está firmado por certificados digitales auténticos obtenidos de alguna manera de autoridades de certificación de confianza.

El ataque de STUXNET hace reflexionar sobre la capacidad que tienen los atacantes de poder influir en infraestructuras tan críticas como pueden ser las nucleares. Es la primera vez que se ve que los efectos de ciberataques pueden producir daños graves fuera del ciberespacio. Algunos expertos, como la agencia china Xinhua, clasifican este ataque dentro de la Ciberguerra, acusando directamente

a Estados Unidos. Sin embargo, es cierto que en el ciberespacio no es necesario ser tan poderoso como el gobierno de una nación para llevar a cabo ataques tan graves. Un grupo de personas o una organización podrían haber sido los causantes de este ataque, clasificándose entonces como *ciberterrorismo* o *hacktivismo*, en función de la finalidad última que pretendiese este grupo.

En estas últimas categorías (*ciberterrorismo* y *hacktivismo*) no se puede determinar con certeza los ataques que se han producido, pues como ya se ha mencionado anteriormente, en el ciberespacio es muy difícil rastrear la autoría de un ataque.

A modo de resumen, las principales amenazas que pueden afectar a la seguridad nacional se recogen en la Tabla 2-1.

Fuente de la amenaza	Motivacion	Acciones
Hacker, cracker	• Desafío • Ego • Rebelion	• *Hacking* • Ingenieria social • Intrusion en los sistemas, robos • Acceso no autorizado al sistema
Delincuente informatico	• Destruccion de información • Divulgacion de información • Ganancias económicas • Alteracion no autorizada de datos	• Delitos informáticos • Acciones fraudulentas • Soborno • Spoofing • Intrusion en los sistemas
Terrorista	• Chantage terrorista • Destruccion • Explotacion • Venganza	• Bomba- terrorismo • Guerra de la información • Ataque a los sistemas (por ejemplo la denegación de servicio distribuido) • Penetracion en los sistemas • Manipulacion de los sistemas
Espionaje industrial (empresas, gobiernos extranjeros, otros intereses del gobierno)	• Ventaja competitiva • Espionaje económico	• Explotacion económica • Robo de la información • Intrusion en la intimidad personal • Ingenieria social • Penetracion en los sistemas • Acceso no autorizado a los sistemas (acceso a información clasificada, propietaria, y/o relacionadas con la tecnología)

Tabla 2-1: Resumen de amenazas (extraída de [9])

2.2.2 Amenazas a empresas y organizaciones

En el anterior apartado se trataba la dimensión de la ciberdelincuencia, que podía afectar a la Seguridad Nacional, hasta la ciberguerra. Sin embargo, los estados no son los únicos objetivos para los atacantes. En el punto de mira de los atacantes están las empresas y organizaciones, sobre todo las de mediano y gran tamaño.

Un informe del CCN-CERT (Centro Criptológico Nacional – *Computer Emergence Response Team*) [8] identifica las siguientes amenazas detectadas durante 2014 que han tenido como objetivo

empresas españolas. Se clasifican por su peligrosidad, teniendo en cuenta el origen y la probabilidad de que ocurra la amenaza, así como las herramientas existentes para defenderse de ella.

Tienen un riesgo **alto** las siguientes:

- Sustracción, publicación o venta de información
- Interrupción o toma de control de los sistemas
- Ciberespionaje proveniente de otros gobiernos

Como amenazas con un riesgo **medio** se clasifican las siguientes:

- Manipulación de información
- Interceptación de comunicaciones
- Venta de información

Como amenazas con una peligrosidad **baja** se clasifican las siguientes**:**

- Espionaje industrial
- Publicación de información
- Desfiguración de páginas web.

Es necesario comprender que esta clasificación no es hermética, y que la catalogación de una amenaza como de peligrosidad baja no quiere decir que sus efectos sean limitados. Cada organización tiene unas características únicas, pero todas están expuestas a amenazas de distinta índole. Son, por tanto, las propias organizaciones quienes deben analizar su presencia en el ciberespacio y tomar las medidas oportunas para mitigar las posibilidades de sufrir un ataque con éxito.

En cuanto al origen de las amenazas, las más graves provienen de profesionales del ciberdelito, hacktivistas, cibervándalos y actores internos. Las de nivel medio están generalmente perpetradas por otras naciones y profesionales del ciberdelito. Las restantes son las iniciadas por otras organizaciones privadas, ciberinvestigadores y ciberterroristas.

2.2.3 Amenazas a individuos

Si bien la huella digital de una persona es mucho menor que la de un estado o una empresa, es posible encontrarla en el ciberespacio. Además hay que tener en cuenta que, como norma general, una persona tiene menos capacidad de defensa ante un ataque que una empresa o nación [8]. Por estas razones debemos tener en cuenta que los ciberdelincuentes pueden encontrar en una persona particular un objetivo rentable. Esta rentabilidad se dispara cuando la persona es una persona importante en una organización, pertenece a la estructura del gobierno de una nación, o es una persona famosa. Los ataques que tienen como objetivo una persona suelen ser ataques más limitados a primera vista, pero que pueden tener consecuencias nefastas.

Normalmente son los ciberdelincuentes profesionales los que realizan ataques a personas, con el objetivo de conseguir un beneficio económico. Estos ataques suelen estar dirigidos a la información personal de los atacados, como fotografías, información bancaria o credenciales. El impacto de un robo de información varía mucho de una a otra persona, pero puede llegar a traducirse en un robo monetario o la destrucción de su imagen personal y reputación. Es común que los ciberdelincuentes chantajeen a los atacados pidiendo un rescate a cambio de no publicar su información personal, o a cambio de la devolución de la información sustraída.

Aunque no es común, los usuarios pueden ser objeto de ciberespionaje por parte de organizaciones nacionales, ya sean extranjeras o no, o privadas. Estos ataques normalmente están dirigidos a altos directivos de empresas y sus efectos están más cercanos a las amenazas a empresas descritas anteriormente.

2.3 Iniciativas en el ámbito de la ciberseguridad y ciberdefensa

2.3.1 Ámbito internacional

Estados Unidos, como referente en ciberdefensa a nivel mundial, publicó la *Estrategia Nacional para asegurar el Ciberespacio* [15] del presidente George W. Bush en 2003. Posteriormente, en 2006, se publicó el *Plan Nacional de Protección de Infraestructuras* [16] y la *Iniciativa Nacional de Ciberseguridad Integral* [17] en 2008. En todas ellas se señala la ciberdefensa y la ciberseguridad como unos de los pilares fundamentales en la defensa de la nación.

Tras los ataques de Estonia en 2007, la OTAN entiende que los ciberataques deben considerarse un elemento más de los conflictos. Tras la cumbre de Bucarest de 2008, la OTAN firma la *Política de ciberdefensa* y el *Concepto de ciberdefensa*. Además se aceleró el proceso para dotar de la capacidad de respuesta adecuada al NCIRC (*NATO Computer Incidents Response Capability Technical Centre)* que es un centro en el que se agrupan un centro de apoyo y coordinación y un centro técnico. Tiene como objetivo generar la respuesta de forma conjunta a un ciberataque grave sufrido por alguno de los estados miembros. En 2011, la OTAN pone a disposición de los socios la capacidad de respuesta y lleva a cabo actividades en el ámbito de la coordinación y asesoramiento, así como investigación y formación. Sin embargo, ha reseñado que la responsabilidad de la ciberdefensa recae en cada uno de los estados miembros [18].

En febrero de 2013, la Unión Europea (UE) aprueba el documento *Estrategia de Ciberseguridad de la Unión Europea: un ciberespacio abierto, seguro y protegido* [19]. En este documento se marcan las líneas de actuación de los países miembros y el objetivo de conseguir un ciberespacio en el que los ciudadanos europeos, las empresas y los países puedan desarrollar su actividad de forma segura.

2.3.2 Ámbito nacional

En España, el *Plan de Seguridad Nacional* (PSN) de 2009 [20], en su capítulo tercero *Los riesgos y amenazas para la Seguridad Nacional*, describe los riesgos y amenazas que afectan singularmente a la seguridad nacional: los conflictos armados, el terrorismo, las amenazas cibernéticas, el crimen organizado, la inestabilidad económica y financiera, la vulnerabilidad energética, la proliferación de armas de destrucción masiva, los flujos migratorios irregulares, el espionaje, las emergencias y catástrofes, la vulnerabilidad del espacio marítimo y la vulnerabilidad de las infraestructuras críticas y los servicios esenciales; colocando a la ciberdefensa y ciberseguridad en un primer plano entre las amenazas para la seguridad nacional.

El cuarto capítulo del citado plan, *Líneas de acción estratégicas*, expone en el área de seguridad cibernética un objetivo: garantizar un uso seguro de las redes y sistemas de información a través del fortalecimiento de nuestras capacidades de prevención, detección y reacción frente a los ataques cibernéticos. Para ello, traza diferentes líneas de acción estratégicas que se citan a continuación:

- Incremento de la capacidad de prevención, detección, investigación y respuesta ante las ciberamenazas, con apoyo en un marco jurídico operativo y eficaz.
- Garantía de la seguridad de los sistemas de información y las redes de comunicaciones e infraestructuras comunes a todas las Administraciones Públicas.
- Mejora de la seguridad y resiliencia de las tecnologías de la información y la comunicación (TIC) en el sector privado a través del uso de las capacidades de los poderes públicos.
- Promoción de la capacitación de profesionales en ciberseguridad e impulso a la industria española a través de un plan de I+D+i.
- Implantación de una cultura de ciberseguridad sólida. Se concienciará a los ciudadanos, profesionales y empresas de la importancia de la seguridad de la información y del uso responsable de las nuevas tecnologías y de los servicios de la sociedad del conocimiento.
- Intensificación de la colaboración internacional.

La *Estrategia Nacional de Ciberseguridad* [21], publicada por Presidencia del Gobierno en 2013, desarrolla en mayor profundidad estas líneas de actuación y marca unas pautas a seguir, y unos objetivos a alcanzar.

Se han asignado las competencias de ciberdefensa y ciberseguridad al Ministerio de Defensa y al Instituto Nacional de Ciberseguridad (INCIBE) respectivamente. En el caso de las Fuerzas Armadas se ha dado respuesta a esta competencia mediante la creación del Mando Conjunto de Ciberdefensa (MCCD) el 19 de febrero de 2013 (Orden Ministerial 10/2013). Este mando conjunto depende del Jefe del Estado Mayor de la Defensa (JEMAD).

Se están llevando a cabo también colaboraciones con universidades y empresas nacionales en estas materias, lo que demuestra la importancia otorgada por el gobierno a ellos. Un ejemplo es la financiación del Proyecto SACO [22] llevado a cabo por INDRA, la Universidad Carlos III y la Universidad de Málaga. El más reciente es el acuerdo promovido por el MCCD para realizar una colaboración en el ámbito de la ciberdefensa con la Universidad Politécnica de Madrid [23].

2.4 Alternativas para configurar redes de forma segura

La capacidad de Internet para interconectar cualquier ordenador con otro en cualquier parte del mundo puede ser muy útil para algunas personas y, sin embargo ser muy peligrosa para otras. Normalmente aquellos que más incómodos se sienten con el hecho de que alguien al otro lado del mundo pueda conectarse con su máquina son las empresas y organizaciones. En una red de este tipo puede haber información confidencial, que en manos de personas inadecuadas puede provocar graves daños a la organización. Además, estas redes con información sensible deben protegerse de los peligrosos ciberataques que pueden dejarlas fuera de servicio o dañadas.

El compromiso entre una arquitectura de red completamente aislada de Internet, y por lo tanto muy segura, y una completamente expuesta e insegura, se consigue mediante un elemento de red: el *firewall*. Los *firewall* o cortafuegos funcionan de la misma forma que un foso aislaba un castillo medieval, dejando una única entrada en la que los paquetes son analizados y solo se les permite el paso a los que cumplen las reglas de acceso [24].

2.4.1 Internet, DMZ e Intranet

La estructura típica que toma la red de una organización le debe permitir estar, por una parte, protegida y aislada de Internet, sin perder por otra parte la capacidad de tener ciertos servicios accesibles desde el exterior. Para este cometido se configuran los cortafuegos de forma que dejen tres zonas diferenciadas.

La primera zona, Internet, es la zona que está conectada directamente a la red, y en la que no se encuentra nada más que el router de acceso. La frontera de esta zona puede ser un cortafuegos o el mismo router, si está configurado para hacer filtrado de IP. Sin embargo, esta última configuración no proporciona una adecuada protección.

La segunda zona, que se encuentra a continuación de la frontera de Internet, se denomina DMZ (*DeMilitarized Zone).* En esta zona de la red se sitúan los servicios que deben estar accesibles desde Internet.

La última zona es la Intranet, en la que se encuentran conectados los equipos de la organización que deben ser aislados de Internet, como, por ejemplo, la maquinaria industrial y los equipos de trabajo de los trabajadores de la empresa.

Hay tres formas de conseguir esta configuración de tres zonas.

1. Usando un solo cortafuegos y un router con filtrado IPSEC (*Internet Protocol SECurity*) (véase Figura 2-1). Esta configuración es la que menos recursos necesita, pero también es la

que menos seguridad proporciona, ya que los servicios en la DMZ no tienen tanta protección como si estuviesen tras un cortafuegos.

2. Usando dos cortafuegos (véase Figura 2-2). Mediante el uso de dos cortafuegos, se consigue proteger completamente tanto los servidores en la DMZ como los equipos de la Intranet. El aumento de seguridad entre la configuración de *Router-firewall* y la de *2-firewall* corresponde a la mayor cantidad de reglas y la configuración más robusta de un cortafuegos en comparación con un router.
3. Usando un cortafuegos de *3 patas* (véase Figura 2-3). Ésta es una configuración de compromiso, que consigue asemejarse en seguridad a la configuración anterior, pero evitando el coste de adquirir y configurar dos cortafuegos diferentes. En esta arquitectura, el *firewall* tiene más de dos adaptadores de red, y crea reglas diferentes para cada uno de ellos.

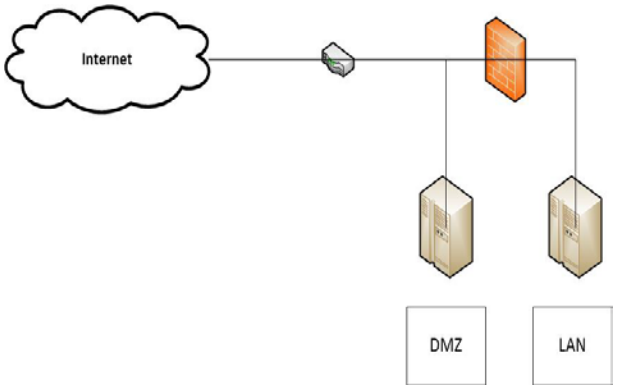

Figura 2-1: Arquitectura con un cortafuegos y router

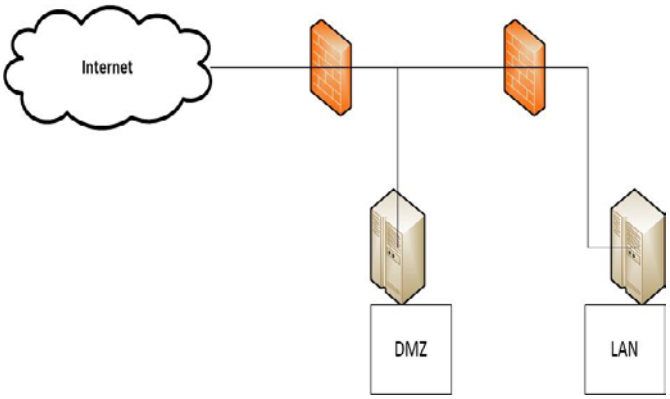

Figura 2-2: Arquitectura con dos cortafuegos

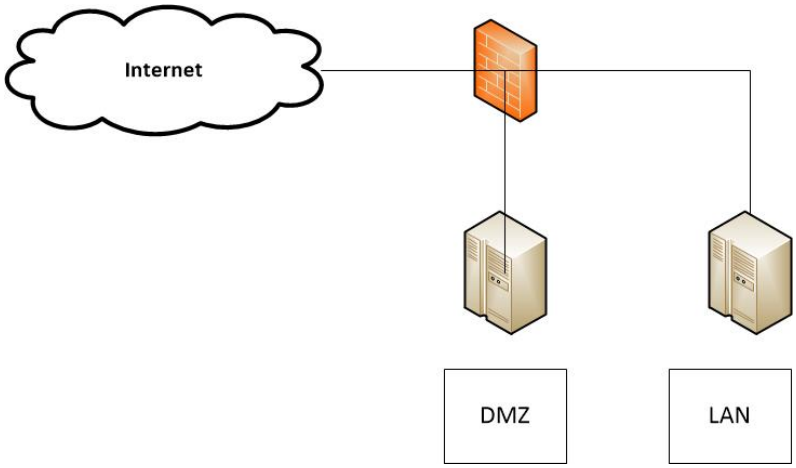

Figura 2-3: Arquitectura con *firewall* de tres patas

2.4.2 Servicios y servidores

Los servicios y servidores de una organización, que se colocan en la DMZ, son específicos de cada una. Estos servicios pueden servir a los usuarios internos de la organización, a usuarios de Internet o a ambos. Los servicios más típicos que suelen encontrarse en la zona desmilitarizada de una organización son servidores *web*, compartición de archivos, resolución de nombres (DNS), bases de datos, correo electrónico, etc.

2.5 Virtualización

El concepto de virtualización ya era manejado por IBM en los años 60; sin embargo, se desarrolló tal como se conoce hoy en día en los años 90. La virtualización toma importancia cuando el avance de los microprocesadores los hace tan potentes que son infrautilizados, pues sobraban ciclos de reloj.

La virtualización (en inglés se puede encontrar como “v12n”) en el ámbito de la informática se refiere a la abstracción de los recursos de una computadora para la recreación de un recurso tecnológico. Explicado de otra forma, se crea una capa de abstracción entre el hardware de la máquina real (*host* o anfitrión) y el sistema operativo de la máquina virtual. Esta capa de abstracción es manejada por el hipervisor, que es el software encargado de gestionar la asignación de los recursos a las diferentes máquinas virtuales que puede tener configuradas [25].

La virtualización proporciona la capacidad de mantener en funcionamiento un número de máquinas determinado por las capacidades del hardware del anfitrión, imprescindible para este trabajo. Cada una de las máquinas virtuales se ejecutará sobre un hardware virtual determinado por el administrador, que se encuentra perfectamente aislado del de las demás máquinas virtuales. Esto quiere decir que un fallo en el sistema operativo o en las aplicaciones que corren en una máquina virtual, no afectará al funcionamiento del anfitrión ni de las otras máquinas virtuales en ejecución. Este aislamiento también proporciona seguridad ante ataques informáticos, pues desde una máquina virtual determinada no es una tarea trivial acceder a la información de las demás, aunque se ejecuten sobre el mismo hardware realmente.

2.5.1 Tipos de virtualización

La virtualización puede clasificarse en varios tipos, en función de las características de la capa de abstracción. Estas características son definidas por el tipo de hipervisor utilizado. Existen dos tipos de hipervisor principalmente [26]:

1. *Bare metal*. La traducción literal “metal desnudo” hace referencia a la inexistencia de un sistema operativo entre el hardware y el hipervisor. También son llamados de tipo I. En el esquema de la Figura 2-4 se puede ver cómo trabajan este tipo de hipervisores.

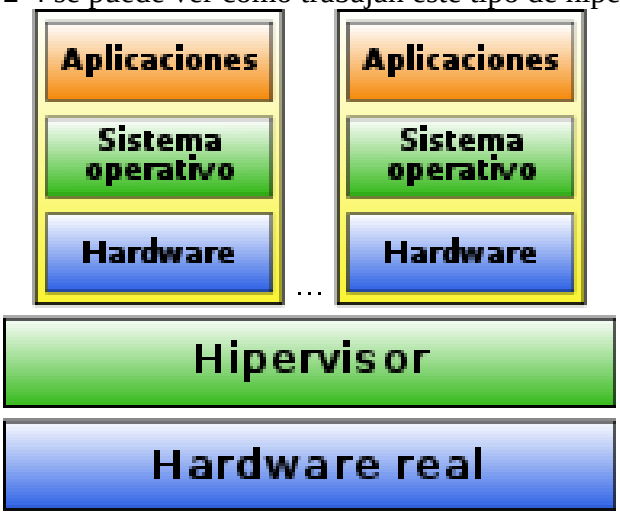

Figura 2-4: Arquitectura de un hipervisor tipo I [27]

El hipervisor incorpora los drivers necesarios para controlar el hardware sin necesidad de un sistema operativo. El hipervisor se carga antes que ninguno de los sistemas operativos y controla todas las interacciones directas con el hardware.
Los software de virtualización más potentes actualmente, como son Microsoft Hyper-V [28], Citrix XEN Server [29] y Vmware ESX-Server [30], utilizan este esquema.

Los hipervisores de tipo I se pueden dividir a su vez en dos tipos, en función del hardware sobre el que corren sus máquinas virtuales [31].

i) Monolíticos: Son hipervisores que emulan el hardware para sus máquinas virtuales. El hardware emulado debe ser lo suficientemente potente como para soportar los drivers del sistema operativo huésped.
   A su vez, el hipervisor tiene que hacer una gran cantidad de operaciones y cambios de contexto para intercomunicar el driver del hardware emulado con el driver que controla el hardware real.
ii) De Micro-*kernel*: En esta visión, el hipervisor únicamente se encarga de particionar el sistema, pero los drivers no son suyos. En la primera de las máquinas virtuales, llamada *parent* (padre), debe cargarse un sistema operativo con los drivers necesarios para controlar el hardware real. En las sucesivas máquinas virtuales se cargarán drivers que no son más que punteros hacia los drivers del sistema operativo padre.

En los gráficos de la Figura 2-5 se puede ver la arquitectura de los dos tipos de hipervisor de tipo I descritos anteriormente.

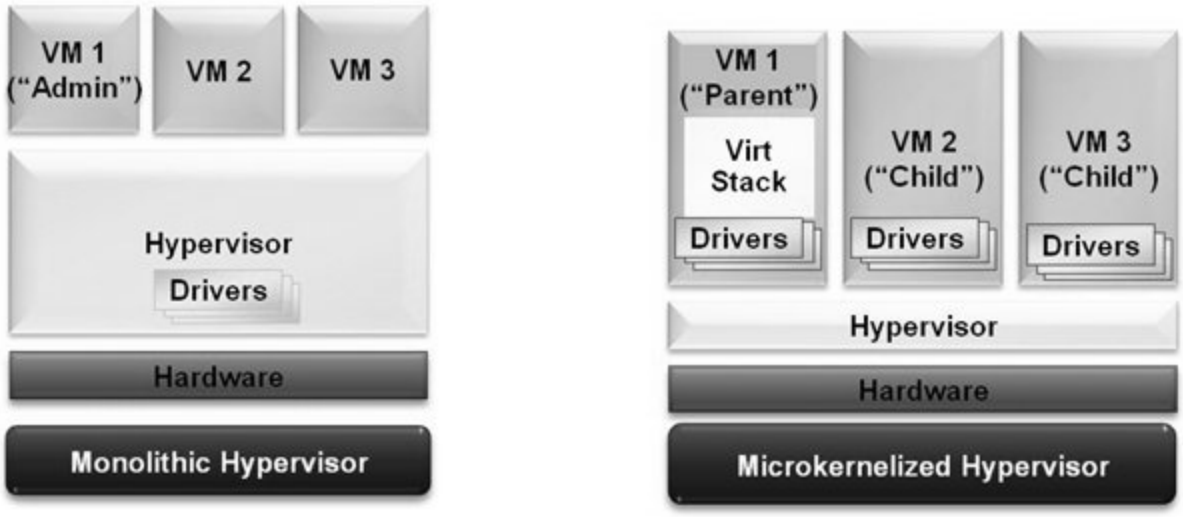

Figura 2-5: Comparativa entre hipervisor monolítico y de micro-*kernel* [27]

2. *Hosted*: En este tipo, también llamados hipervisores de tipo II, la capa de abstracción es para el sistema anfitrión una aplicación más. Es decir, en el hardware real se instala un sistema operativo normal (Linux o Windows generalmente) que gestiona los recursos y ejecuta una aplicación. Esta aplicación es la encargada de crear los contenedores con el hardware virtual sobre los que se instalan los sistemas operativos virtuales. La principal característica es que los sistemas operativos virtuales no tienen acceso al mismo hardware que el hipervisor, si no a uno específicamente preparado para este sistema operativo. Esta característica permite instalar sistemas operativos en máquinas que no serían compatibles, y también proporciona un perfecto aislamiento entre las diferentes máquinas virtuales. Sin embargo, el rendimiento del sistema virtualizado se verá disminuido debido a las operaciones de "traducción" que tiene que realizar el hipervisor durante su ejecución. El gráfico de la Figura 2-6 permite tener una idea más clara del funcionamiento por capas de un hipervisor de tipo II.

Figura 2-6: Arquitectura de un hipervisor de tipo II [27]

Existen casos de hipervisores de tipo II en los cuales las máquinas virtuales pueden interactuar directamente con el sistema operativo anfitrión y, por tanto, controlar el hardware real. Se les llama *hipervisores híbridos*.

Este tipo de virtualización es la más extendida y existen multitud de programas que usan esta tecnología, entre ellos se encuentran: VirtualBox [32], Vmware [33] (player, server y Workstation), QEMU [34], KVM [35], XEN [36], Microsoft Virtual PC [37] y Microsoft Hyper-V Server [28] entre otros.

La virtualización también puede hacer referencia a la virtualización de recursos, de aplicaciones o escritorios. Estos conceptos se engloban dentro de la filosofía *Cloud Computing* y son ampliamente utilizados en el mundo empresarial. Sin embargo, no son objeto de estudio en este trabajo.

2.5.2 Software de virtualización

El gran auge en el que se encuentra la filosofía de *Cloud Computing* y la virtualización ha propiciado el desarrollo de numerosas herramientas, orientadas a diferente público y bajo todo tipo de licencias. De entre todas ellas se van a introducir las más importantes, en función de la utilidad para este trabajo.

Se han elegido para comparar las herramientas de virtualización de las compañías Oracle, *Open Virtualization Alliance* (KVM), XEN y Vmware sobre las cuales versarán los siguientes subapartados. En ellos se pretende introducir de manera general la herramienta, así como sus principales características y los requisitos mínimos.

2.5.2.1 VirtualBox

VirtualBox [38] es un software que nace con el lanzamiento del denominado VirtualBox OSE en 2007, y que es la primera versión de la herramienta que no se distribuyó bajo licencia de código privativo. Destinado a la virtualización, englobado dentro de los hipervisores de tipo II, la aplicación VirtualBox puede ejecutarse sobre Windows, Linux, Solaris OS o Mac OS, y permite la creación de máquinas virtuales para sistemas operativos concretos como *Windows 8.1*, Ubuntu, SolarisOS, etc. o la creación de una máquina virtual genérica en la cual se puede cargar prácticamente cualquier sistema operativo. Es distribuido bajo licencia *GNU General Public License (GPL)*.

La forma de trabajar de este software se basa en tratar de ejecutar tanto código del sistema invitado en el procesador nativo como sea posible. También incorpora un recompilador dinámico para traducir las instrucciones que no sean soportadas por el procesador anfitrión, basado en QEMU.

VirtualBox no tiene limitación sobre la cantidad de máquinas virtuales que se pueden crear o ejecutar al mismo tiempo, siempre y cuando el anfitrión tenga potencia suficiente.

Para poder hacer funcionar correctamente VirtualBox se necesita:

- Procesador: Cualquier procesador con arquitectura x86 Intel o AMD lo suficientemente potente como para ejecutar los sistemas operativos virtualizados y el anfitrión a la vez.
- Memoria: Dependiendo de los sistemas operativos invitados que se desea ejecutar, se necesitarán al menos 512 MB de RAM. Sin embargo, lo recomendado asciende a la suma de lo necesario para que todos los sistemas huéspedes se ejecuten con normalidad.
- Disco duro: Para la instalación, se necesitan 30 MB de espacio. Sin embargo, cada máquina virtual ocupará en el disco duro al menos tanto como ocupe su sistema operativo instalado.

Las características más reseñables de VirtualBox son las que se enumeran a continuación:

- Portabilidad. Las máquinas virtuales pueden ejecutarse aunque cambie la arquitectura del anfitrión.
- No requiere virtualización por hardware.
- Carpetas compartidas, integración de ventanas y acelerador de gráficos 3D virtualizado (cuando se instala el software adicional, *Guest additions* en el huésped).
- Soporte a multiprocesador virtual.
- Posibilidad de uso de USB en la máquina virtual.
- Capacidad de escritorio remoto con soporte para *USB over RDP (Remote Desktop Protocol).*
- Es gratuito.

2.5.2.2 KVM

KVM [35] es el nombre que recibe una solución para realizar una virtualización completa sobre Linux. Son las siglas de máquina virtual basada en el núcleo (*kernel-based Virtual Machine*). El software se compone de módulo para el *kernel* (KVM.ko) y herramientas para la gestión desde el entorno de usuario. La totalidad del software se distribuye bajo licencia GPL, y el módulo del núcleo se incluye en el *kernel* de Linux desde la versión 2.6.20. La organización encargada de su desarrollo y mantenimiento es OVA (*Open Virtualization Alliance).*

KVM realiza virtualización completa, es decir, ejecuta instalaciones de sistemas operativos sin modificar. Cada máquina virtual necesita una imagen de disco y se ejecuta en su propio hardware virtualizado.

Los requisitos necesarios para ejecutarlo son los siguientes:

- Procesador x86 o x86_64 con soporte VT/SVM.
- Instalación de cualquier distribución de Linux con *kernel* superior a 2.6.20.
- Suficiente memoria RAM como la suma de la que necesiten los sistemas operativos virtualizados para ejecutarse correctamente

La característica más reseñable es que permite el *overcommit*, que es el uso de la memoria RAM excediendo de la memoria física del anfitrión. Su uso es gratuito.

2.5.2.3 The Xen Project

El hipervisor de Xen Project [36] es un hipervisor de tipo I que permite ejecutar varias instancias de un sistema operativo o varios diferentes en paralelo sobre un único hardware. El hipervisor de XEN es un proyecto bajo licencia *Open Source*. Su versión actual es la 4.0.

Este software es de tipo microkernel, por lo cual necesita la instalación de la máquina virtual padre (*Dom0*) con los drivers necesarios para gestionar el hardware real.

Los requisitos para ejecutar XEN 4.0 son los siguientes:

- Procesador Intel o AMD x86 con capacidad PAE, o x86_64.
- Al menos 512MB de RAM por cada máquina virtual en ejecución.
- Suficiente espacio en disco duro para la instalación de todas las máquinas virtuales.

Las principales características de XEN son las siguientes:

- El hipervisor consta únicamente de 150,000 líneas de código (1MB).
- La mayoría de las distribuciones de Linux puede usarse como sistema para el *Dom0.*
- Aislamiento de drivers. Si un driver ejecutándose en una máquina virtual se corrompe, el hipervisor tiene la capacidad de reiniciar la máquina sin afectar a las demás máquinas en ejecución ni al anfitrión.
- Paravirtualización. Puede ejecutar una versión optimizada de los sistemas operativos huésped para conseguir mayor rendimiento del que se obtiene con la virtualización por hardware.
- Es gratuito.

2.5.2.4 Vmware

Vmware [33] es una empresa que se dedica desde el año 1998 a la virtualización. Tras sus 17 años de experiencia ha creado multitud de aplicaciones gratuitas y de pago. En la actualidad apuesta por el desarrollo en el campo de *Cloud Computing* y es el fabricante de software de virtualización líder en el mundo empresarial. Ha creado además un sistema de certificaciones a las cuales optan los técnicos que consigan demostrar sus conocimientos en el software de esta marca, y que se valoran muy positivamente en el mundo empresarial. Los productos más importantes de los que dispone actualmente son los siguientes [39]:

- Vmware *vCloud Air*
- Vmware *vRealize Suite*
- Vmware *Workspace Suite*
- Vmware *EVO:RAIL*
- Vmware *Fusion*
- Vmware *vSphere*
- Vmware *vSphere Hypervisor*

Estas herramientas, con una calidad de nivel profesional, proporcionan un entorno de trabajo adecuado para una gran empresa. Por lo tanto, son herramientas que tienen la capacidad de ser fácilmente actualizables (dentro de la propia marca) para conseguir más potencia o más características. A su vez, la marca proporciona una asistencia técnica muy eficiente y personalizada. Al mismo tiempo, el software es muy estable. Todas estas características lo harían el software ideal, de no ser por su coste. Las licencias para las herramientas más avanzadas llegan a los 3.800 € por CPU(Vmware *vSphere OM Enterprise plus*) y el servicio de asistencia técnica para la misma, desde 800 € al año.

Los elevados precios de las herramientas Vmware pueden ser amortizados por una empresa de grandes dimensiones, pero no por un centro universitario para su uso en un trabajo de fin de grado. Es

por esta razón por la que nos hemos fijado únicamente en las herramientas gratuitas de la marca. Vmware ofrece las siguientes herramientas gratuitas:

- *vSphere Hypervisor*
- *vCenter Converter*
- *Software Manager*

La herramienta *vSphere Hypervisor* será la única introducida a continuación debido a que las demás herramientas de Vmware no son gratuitas, o no tienen utilidad para este trabajo.

Vmware *vSphere Hypervisor 6.0* [40] es la última versión disponible, anteriormente se conocía como Vmware *ESXi* (versión gratuita de Vmware *ESX*). Es una plataforma de virtualización a nivel de centro de datos, aunque en la versión gratuita solo es posible administrar un único servidor físico. La aplicación consiste en un hipervisor de tipo I compuesto por un sistema operativo basado en *Red Hat Enterprise Linux* en cuyo *kernel* se ha incrustado el código del hipervisor. Utiliza la arquitectura de microkernel, y en las últimas versiones incorpora capacidades de paravirtualización.

Los requisitos de hardware para ejecutarlo son los siguientes:

- CPU Intel o AMD x86_64 de 2 núcleos (se recomiendan varias CPUs con más de 4 núcleos por CPU).
- 256 MB de HD (mas el espacio ocupado por las máquinas virtuales).
- RAM necesaria para ejecutar los sistemas operativos huésped.

Las características más reseñables de este producto son las siguientes:

- Nº de CPU físicas: Ilimitado
- Nº de CPU lógicas: 8 por cada máquina virtual.
- Hipervisor con el mayor número sistemas operativos soportados como huésped del mercado.
- RAM limitada a 32 GB por máquina virtual.

2.5.3 Selección.

Según los datos mostrados en la Tabla 2-2, todos los software de virtualización comparados cumplen los requisitos para poder albergar las máquinas virtuales necesarias para la maqueta de este trabajo. En primer lugar, se ha descartado *vSphere Essentials* debido a su precio. El segundo en ser descartado ha sido XEN debido a que es un hipervisor de tipo *Bare metal,* lo cual se ha identificado como una desventaja para trabajar de forma remota sobre el anfitrión.

La elección ha sido utilizar VirtualBox debido a que es un software gratuito, que cumple los requisitos necesarios para este trabajo y presenta una mayor facilidad de uso y configuración que KVM. Además, es un software con el que ya se ha trabajado en otras materias del grado, por lo que la curva de aprendizaje es más eficiente.

Característica	VirtualBox	KVM	XEN	vSphere Essentials
Compañía	Oracle	Red Hat	The Linux Foundation	Vmware
Perfil de uso	Empresa mediana Empresa pequeña Corporaciones	Empresa mediana Empresa pequeña Doméstico	Corporaciones	Corporaciones
Hipervisor	Tipo II	Tipo II	Tipo I	Tipo I
Tipo de virtualización	Asistida por hardware Paravirtualización	Completa Asistida por hardware Paravirtualización	Asistida por hardware Paravirtualización	Completa Asistida por hardware Paravirtualización
RAM (por MV)	1024GB	No limitada	1000GB	32GB
Virtual CPU (por MV)	32 VCPU	-	512 VCPU	-
Controladores de red (NIC) por *Host*	Max 32 NIC	No limitado	Max 500 NIC	Max 512 NIC
Precio	Gratuito	Gratuito	Gratuito	445€ + 60€/año
Facilidad de uso	Alta	Media	Baja	Alta

Tabla 2-2: Tabla comparativa de software de virtualización

2.6 Simuladores de red

En informática, un simulador es un software capaz de reproducir las condiciones de un determinado experimento mediante el uso de un ordenador. Más concretamente, un simulador de redes es una herramienta ampliamente utilizada por cualquier persona que tenga intención de montar una red de mediano o gran tamaño. El simulador de redes permite crear una red reproduciendo los dispositivos que la formarán y sus conexiones, y probarla antes de hacer una inversión.

Aunque éste es el uso más típico de estas herramientas, sus capacidades permiten crear una red completamente funcional, en la que diferentes máquinas virtuales se interconectarán entre sí, e incluso con el exterior a través de una tarjeta de red física.

Esta capacidad de crear redes totalmente funcionales es la que será explotada en este trabajo, con la finalidad de interconectar las máquinas virtuales y sus adaptadores de red a través de una red virtual que represente la infraestructura de una red empresarial.

Hay una gran variedad de herramientas de este tipo, con diferentes niveles de especialización y desarrollo. A continuación se realizará una reseña de las más conocidas.

2.6.1 Cisco Packet Tracer

El software *Packet Tracer* [41] es un conjunto de herramientas desarrolladas por la compañía Cisco que proporciona la capacidad de crear redes y experimentar con su comportamiento. Está orientado a la simulación de redes diseñadas con hardware de la propia compañía para probarlas y posteriormente implementarlas. Soporta enrutamiento básico y permite una simulación completa del sistema operativo Cisco IOS.

En sus herramientas incluye herramientas de prueba como *Ping* o *Traceroute*. Y además una opción en la cual se puede ver cómo circulan los paquetes por la red. Este software es propiedad de Cisco y su licencia solo permite su uso para actividades de formación y a personas registradas en las diferentes academias certificadas por Cisco. Su interfaz gráfica puede verse en la Figura 2-7.

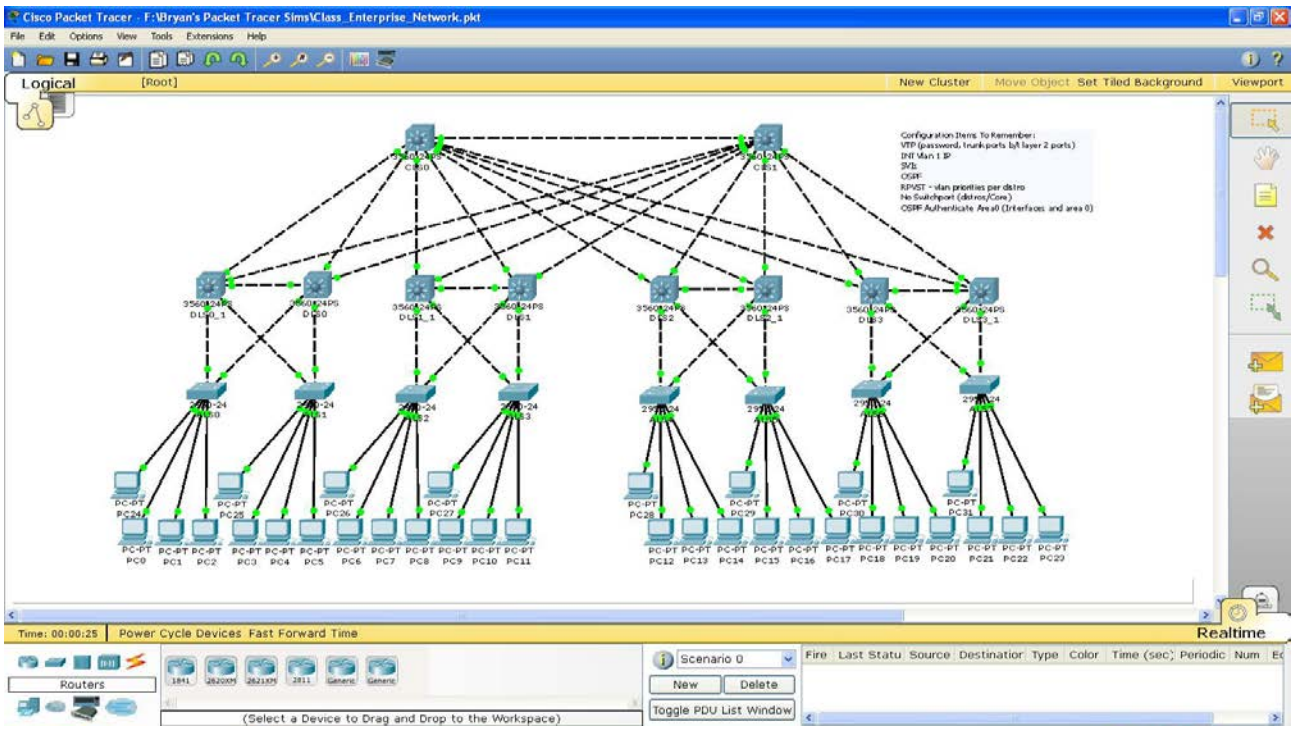

Figura 2-7: Interfaz de *Cisco Packet Tracer* [41]

2.6.2 Graphical Network Simulator

Graphical Network Simulator 3 (GNS3) [42] es un software destinado a la simulación de redes de ordenadores complejas. El software se desarrolla bajo licencia GPL.

Realmente GNS3 es más un emulador que un simulador, pues en casi la totalidad de los dispositivos que simula es capaz de reproducir condiciones idénticas a las de funcionamiento sobre su hardware real. Para ello integra en el programa los siguientes módulos:

- *Dynamips*. Es un emulador que permite ejecutar imágenes del sistema operativo Cisco IOS.
- *QEMU* y VirtualBox. Permite virtualizar elementos de red más complejos, como *firewalls*.
- *VPCS*. Es un emulador de PC capaz de ejecutar funciones básicas de redes.
- *IOU*. Compilaciones especiales de sistemas Cisco IOS preparadas para funcionar sobre sistemas UNIX.

La principal característica de GNS3 es que permite interactuar con los interfaces de red presentes en el ordenador. Esto permite conectar la red virtual a Internet y a máquinas virtuales u otros ordenadores. Incluye herramientas para el análisis del estado de la red y la captura de paquetes.

Es un software multiplataforma que está disponible en Windows, Linux y MacOS. Sin embargo, la versión de Linux tiene características que no están disponibles en las otras versiones, como el soporte nativo IOU (*IOS On UNIX)* que permite ejecutar el sistema operativo de *Cisco* con mayor rendimiento.

La Figura 2-8 muestra el interfaz gráfico del programa.

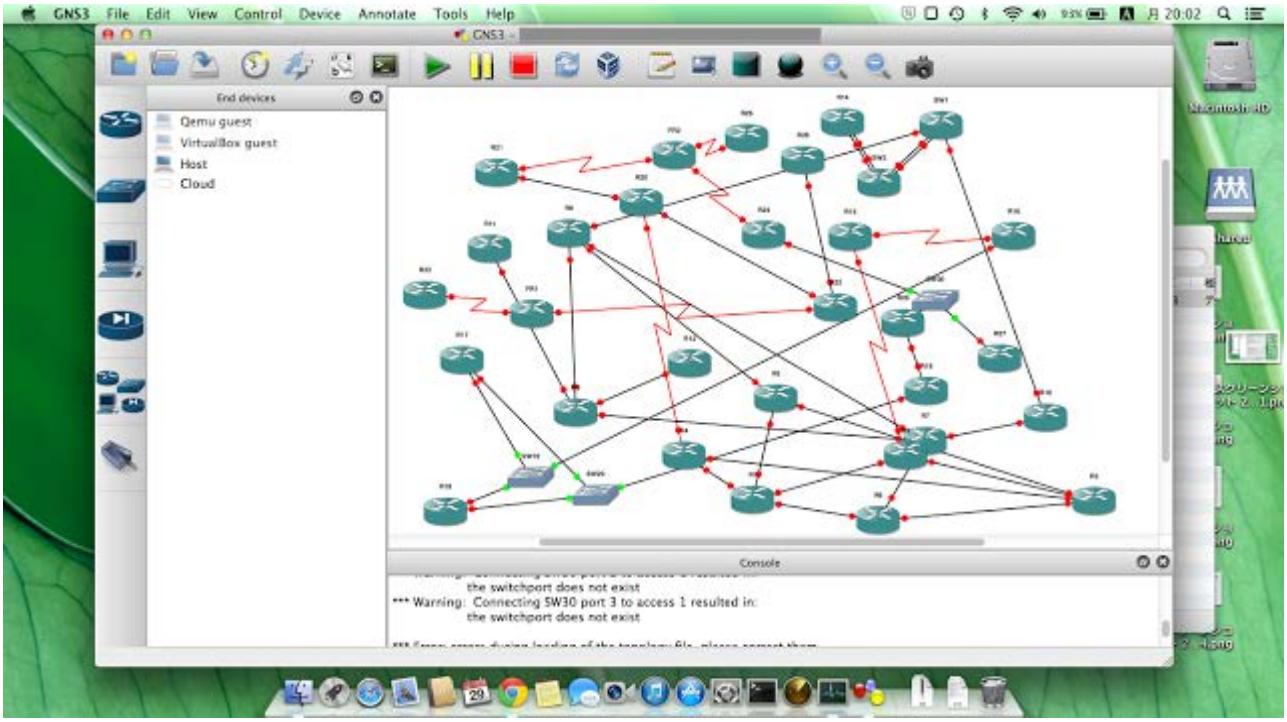

Figura 2-8: Interfaz de GNS3 sobre OSX [43]

2.6.3 Netgui

Netgui [44] es un proyecto de la Universidad Rey Juan Carlos que consiste en la creación de una interfaz gráfica para el sistema Netkit. Esta interfaz gráfica permite crear redes mediante su diagrama, arrancar las máquinas virtuales y dispositivos de red e interactuar con sus consolas.

Netkit es un entorno software que permite realizar experimentos con redes de ordenadores virtuales. Para ello ejecuta los sistemas operativos de las máquinas usando las librerías de *User Mode Linux* como máquinas virtuales dentro de un entorno Linux. No permite la interacción con los interfaces reales de red.

En la Figura 2-9 se puede ver el aspecto que presenta este software.

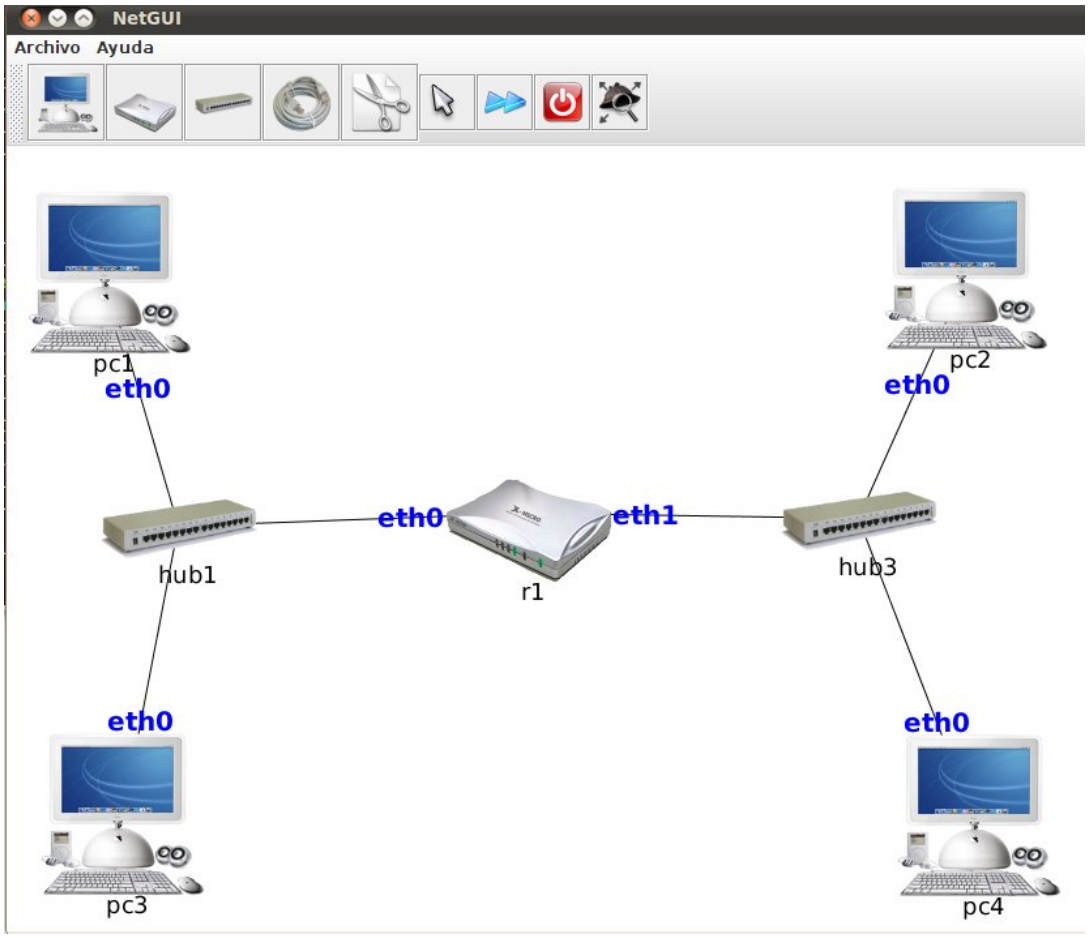

Figura 2-9: Interfaz de *Netgui*. [45]

2.6.4 Selección

De entre las herramientas descritas, por ser la que más características proporciona y distribuirse bajo licencia GPL, se ha decidido utilizar GNS3 para este trabajo. Ha sido decisiva la capacidad para comunicarse con el hardware de red existente, además de la fiabilidad con la que reproduce los sistemas, que le dan carácter de emulador y permitirán que los posteriores ejercicios que se ejecuten en la red virtual sean más reales.

3 DESARROLLO DEL TFG

En este apartado se comenzará por presentar el entorno de trabajo en el que se desarrollará el proyecto. Posteriormente se describirán las características buscadas en la maqueta y su diseño. También se tratarán los temas relativos a su implementación y configuración.

3.1 Preparación del entorno de trabajo.

3.1.1 Hardware

3.1.1.1 Servidor

El servidor es la plataforma física sobre la que se ejecutará la maqueta a desarrollar en este trabajo. El servidor debe contar con los recursos necesarios para poder ejecutar todas las máquinas virtuales que conformaran la maqueta al mismo tiempo, además del software auxiliar empleado para la simulación.

En nuestro caso se trata de un servidor *Dell Poweredge R530* con los siguientes recursos:

- Procesador: *Intel Xeon E5-2620v3*
  - 12 procesadores lógicos (6 núcleos físicos)
  - Velocidad de reloj 2,4 GHz
  - Cache: 15MB
  - Litografía: 22nm
- Memoria RAM: 16 GB DDR4
- Disco duro:
  - 2x SAS 300GB (RAID 1)
  - 2x SATA 1TB (RAID1)
- 4 Adaptadores de red *Gigabit Ethernet*

El servidor tiene un formato de carcasa de *Rack 2U de 19 pulgadas,* por lo que ha sido instalado en la sala de servidores del Centro Universitario de la Defensa. En las figuras 3-1y 3-2 se puede ver el interior y el frontal del servidor respectivamente.

Su conexión a la red se ha realizado mediante dos de sus interfaces: Uno de ellos conectado a la red pública (Internet) y otro a la red local de las aulas del CUD, llamada *LABORATORIOS.*

A este servidor se le ha bautizado con el nombre de *Dunquerque*. Su nombre de dominio es *dunquerque.cud.uvigo.es.*

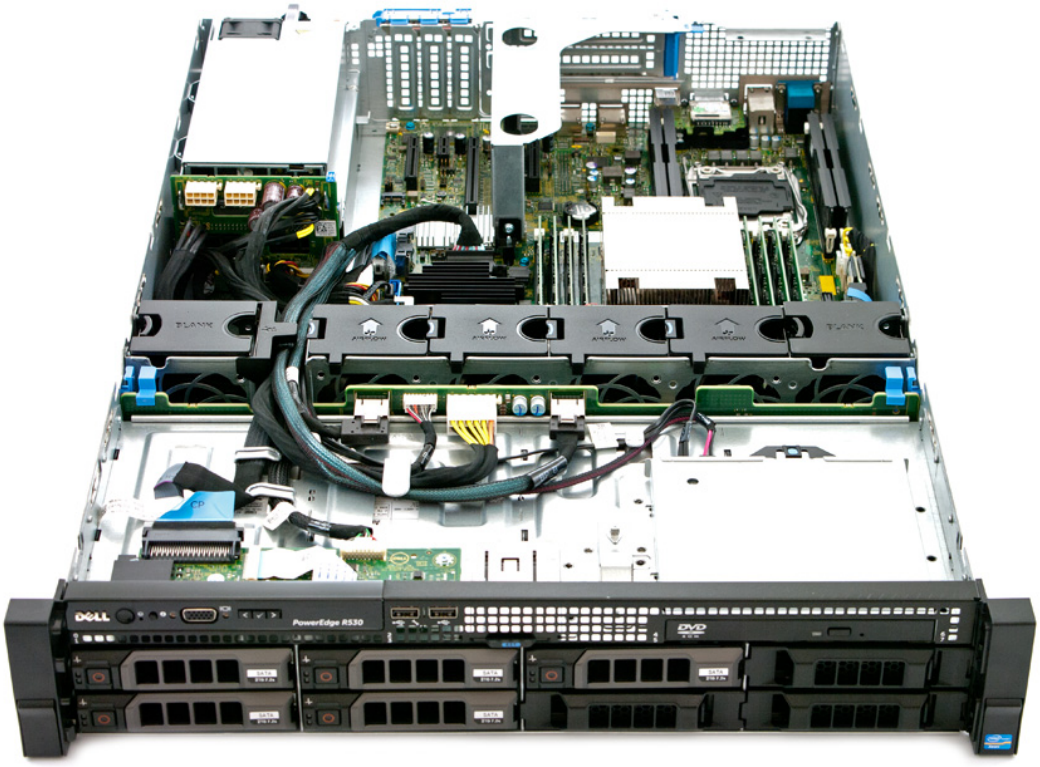

Figura 3-1: Vista interior del servidor *Dell Poweredge R530* (extraído de [46])

Figura 3-2: Frontal del servidor *Dell Poweredge R530* (extraído de [46])

3.1.1.2 Estación de trabajo (ordenador portátil)

Aunque el servidor será la plataforma hardware en la que se ejecutará la maqueta una vez consumado el trabajo, es necesario disponer de otra plataforma para poder llevar a cabo la implementación de la maqueta.

La estación de trabajo será un ordenador portátil *Asus U31SDK* con las siguientes características de hardware

- Procesador: *Intel Core i5-2410M.* 4 núcleos a 2.3GHZ
- Memoria RAM: 6GB
- Disco duro: SATA 500GB
- Tarjeta gráfica: *Nvidia GT520M 1GB*
- Interfaz de red *Ethernet* y *Wireless*

3.1.2 Software

3.1.2.1 Sistemas operativos

Tanto en el servidor *Dunquerque* como en el ordenador de trabajo se han instalado sistemas operativos *Linux*. En concreto, en *Dunquerque* se encuentra instalado *Ubuntu Server 14.04 LTS* [47], y en el ordenador portátil, *Open SUSE Leap 42.1* [48]. Ambos sistemas operativos son software libre y se distribuyen de manera gratuita en sus páginas oficiales.

En el ordenador de trabajo también se encuentra instalada una distribución especializada en *pentesting* llamada *Kali Linux*, que se utilizará para pruebas.

El sistema operativo anfitrión de la maqueta, *Ubuntu Server 14.04 LTS*, se ha instalado en el servidor *Dunquerque*. Este sistema operativo no incluye por defecto entorno gráfico, por lo que antes de iniciar el proyecto se ha instalado el conjunto de software llamado *Xfce* que proporciona un sistema de ventanas y escritorios completo. Además, se ha configurado la herramienta *xrdp* para que el servidor *Dunquerque* pueda ser gestionado utilizando el protocolo de escritorio remoto RDP.

3.1.2.2 VirtualBox

La instalación de VirtualBox es muy sencilla, se realiza desde una terminal de comandos.

El primer paso es añadir a la lista de repositorios de software del sistema operativo el repositorio de VirtualBox. Es importante añadir el repositorio oficial o uno de los autorizados para evitar la descarga de software malintencionado. Para añadir el repositorio oficial, se ejecuta el comando

```
$ echo "deb http://download.VirtualBox.org/VirtualBox/debian trusty contrib" | sudo tee /etc/apt/sources.list.d/VirtualBox.list
```

Con el repositorio añadido a la lista de repositorios del sistema operativo se realiza la instalación mediante el gestor de paquetes *apt-get*, con los siguientes comandos.

```
$ sudo apt-get update
```

```
$ sudo apt-get install VirtualBox-5.0
```

Tras finalizar el proceso de instalación se habrán instalado los servicios y aplicaciones correspondientes a VirtualBox en el sistema. El programa que permite gestionar las máquinas virtuales con un interfaz gráfico, *Oracle VM* VirtualBox *Administrador*.

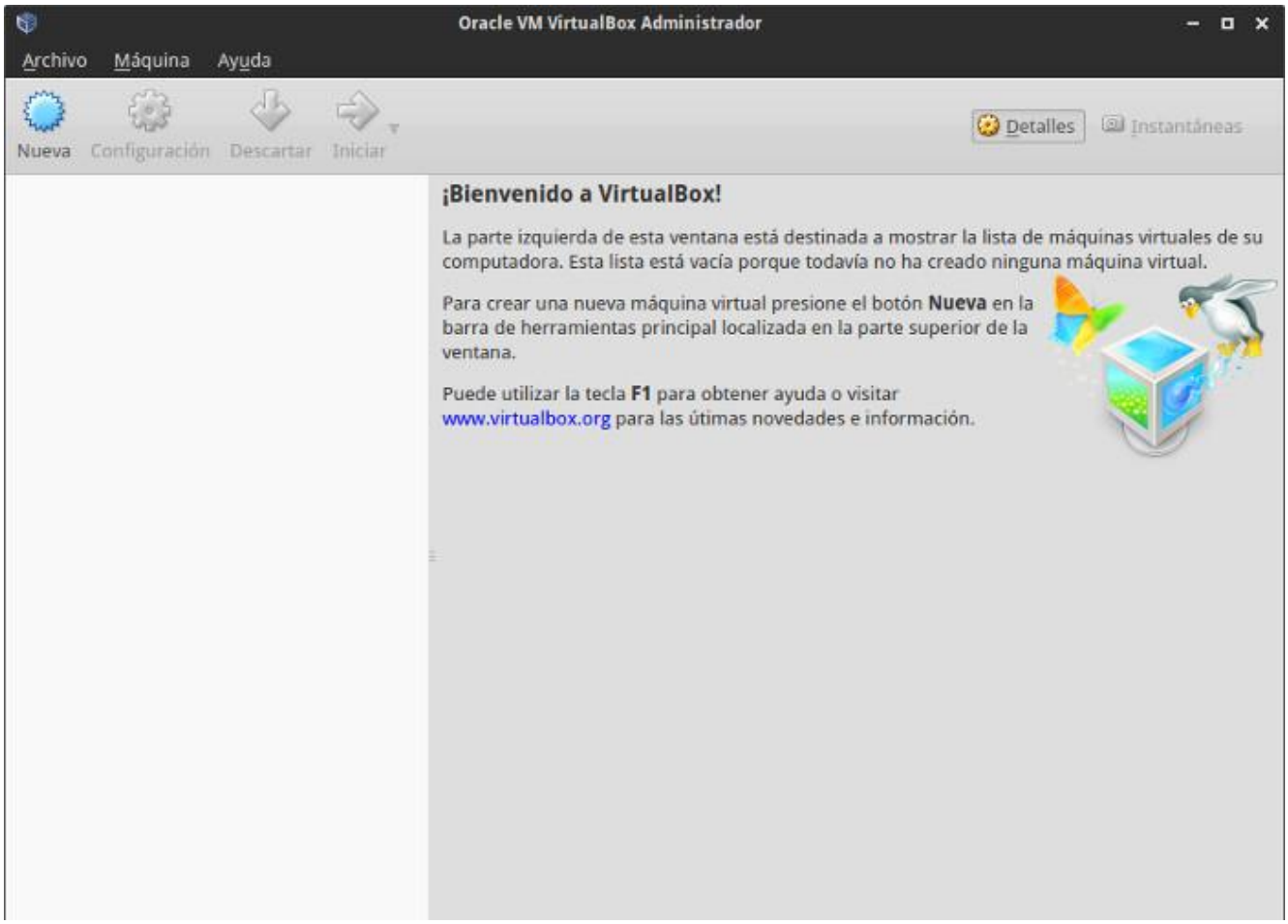

Figura 3-3: Ventana de inicio de VirtualBox

En el ordenador de trabajo la instalación es si cabe más sencilla, pues el repositorio de VirtualBox está incluido de serie entre los repositorios de confianza de *Open SUSE*, por ello para instalarlo basta con ejecutar *sudo zypper install* VirtualBox.

3.1.2.3 GNS3

Para instalar el software GNS3 que se va a utilizar para realizar la simulación de la arquitectura de red se siguen pasos similares a los que se siguieron para la instalación de VirtualBox.

En el servidor *Dunquerque* se ejecutan los siguientes comandos para añadir el repositorio y posteriormente instalar el programa:

```
$ sudo add-apt-repository ppa:gns3/ppa
$ sudo apt-get update
$ sudo apt-get install gns3-*
```

Es necesario prestar atención al asterisco en el último comando que indica al instalador que debe instalar todos los paquetes cuyo nombre empiece por *gns3-*, lo cual es necesario debido a que el programa se distribuye en paquetes separados y para este trabajo son necesarios varios de ellos.

La instalación en el ordenador de trabajo es más tediosa debido a que no se distribuyen paquetes de GNS3 para *Open SUSE*, por lo cual es necesario compilar las fuentes del programa e instalarlo. Esta instalación se explicará de forma menos exhaustiva, pero se encuentra en completamente documentada en [49]. Para instalar GNS3 en *Open SUSE* desde las fuentes, se siguen los siguientes pasos.

1. Instalar los paquetes correspondientes al lenguaje de programación *python* en el cual está escrito el programa.

```
$ sudo apt-get install python3-dev python3-setuptools python3-pyqt5
python3-pyqt5.qtsvg python3-pyqt5.qtwebkit python3-ws4py python3-
netifaces install python3-pip
```

2. Instalar dependencias necesarias para *Dynamips*, que es una dependencia fundamental de GNS3.

```
$ sudo apt-get install cmake uuid-dev libelf-dev libpcap-dev
```

3. Descargar el archivo comprimido con las fuentes (*sources* en inglés) de la página web oficial de GNS3 [42]. Descomprimirlo en una carpeta.

4. Descomprimir, compilar e instalar *Dynamips.* Desde la carpeta anterior ejecutar:

```
$ unzip dynamips-0.2.14.zip
$ cd dynamips-0.2.14
$ mkdir build
$ cd build
$ cmake ..
$ make
$ sudo make install
$ sudo setcap cap_net_admin,cap_net_raw=ep /usr/local/bin/dynamips
```

5. Descomprimir, compilar e instalar GNS3 y GNS3-*server:*

```
$ unzip GNS3-server-1.4.0rc1.zip
$ cd GNS3-server-1.4.0rc1
$ sudo python3 setup.py install
$ cd ..
$ unzip GNS3-gui-1.4.0rc1.zip
$ cd GNS3-gui-1.4.0rc1
$ sudo python3 setup.py install
$ cd ..
```

6. Instalar dependencias de *IOU*, que es uno de los módulos de GNS3 que permite simular enrutadores:

```
$ sudo apt-get install libssl1.0.0:i386
$ sudo ln -s /lib/i386-linux-gnu/libcrypto.so.1.0.0
/lib/libcrypto.so.4
$ sudo apt-get install bison flex git
$ git clone http://github.com/ndevilla/iniparser.git
$ cd iniparser
$ make
$ sudo cp libiniparser.* /usr/lib/
$ sudo cp src/iniparser.h /usr/local/include
$ sudo cp src/dictionary.h /usr/local/include
$ cd ..
```

7. Compilar e instalar *IOU:*

```
$ unzip iouyap-0.95.zip
$ cd iouyap-0.95
$ sudo make install
$ sudo cp iouyap /usr/local/bin
$ cd ..
```

8. Instalar el software de apoyo a GNS3 adicional.

```
$ sudo apt-get install cpulimit qemu wireshark
```

9. Descomprimir, compilar e instalar *VPCS*.

```
$ unzip vpcs-0.6.1.zip
$ cd vpcs-0.6.1/src
$ ./mk.sh
$ sudo cp vpcs /usr/local/bin/
$ cd ../..
```

Una vez instalado el software GNS3 en el servidor *Dunquerque*, es necesario configurarlo para poder aceptar conexiones como servidor.

Para ello se accede al servidor mediante una terminal remota usando el comando *ssh*, como se pude ver en la Figura 3-4

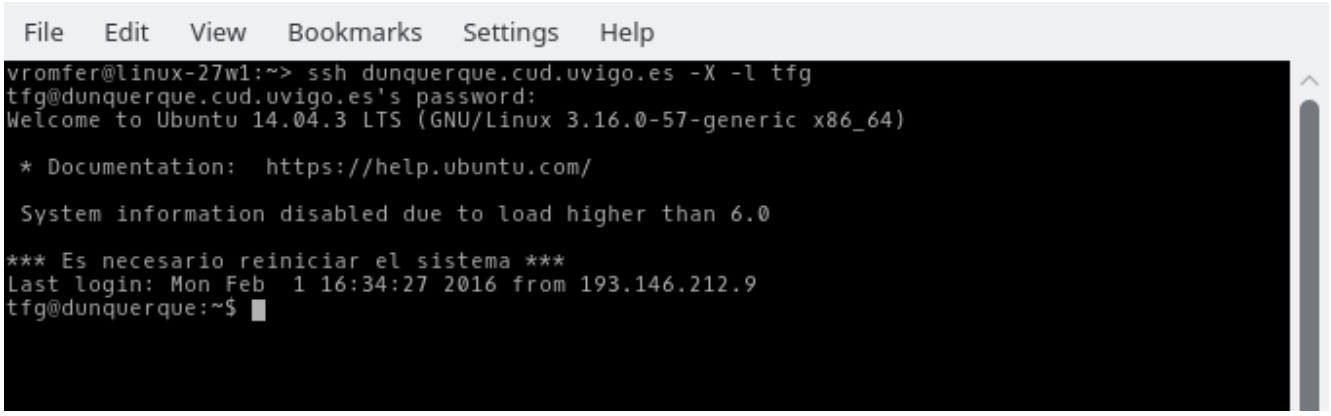

Figura 3-4: Acceso a *Dunquerque* mediante SSH

Una vez realizada la autenticación, se modifica el archivo de configuración de GNS3 Server, que se encuentra en la ruta *$HOME/.config/*GNS3*/gns3_server.conf*. Para editar este archivo se puede utilizar cualquier editor de texto para terminal, por ejemplo *nano*, como se puede ver en la Figura 3-5.

En el archivo de configuración se modifica la sección [Server] en la cual hay que indicarle al programa la IP externa del servidor y el puerto en el que debe escuchar conexiones. En este caso es la IP 193.146.212.33 y el puerto 8000. También se activa la autenticación y se configura el nombre de usuario y contraseña que usará posteriormente el cliente para conectarse con el servidor de GNS3.

Los demás parámetros han sido configurados automáticamente por el instalador, y normalmente no es necesario modificarlos.

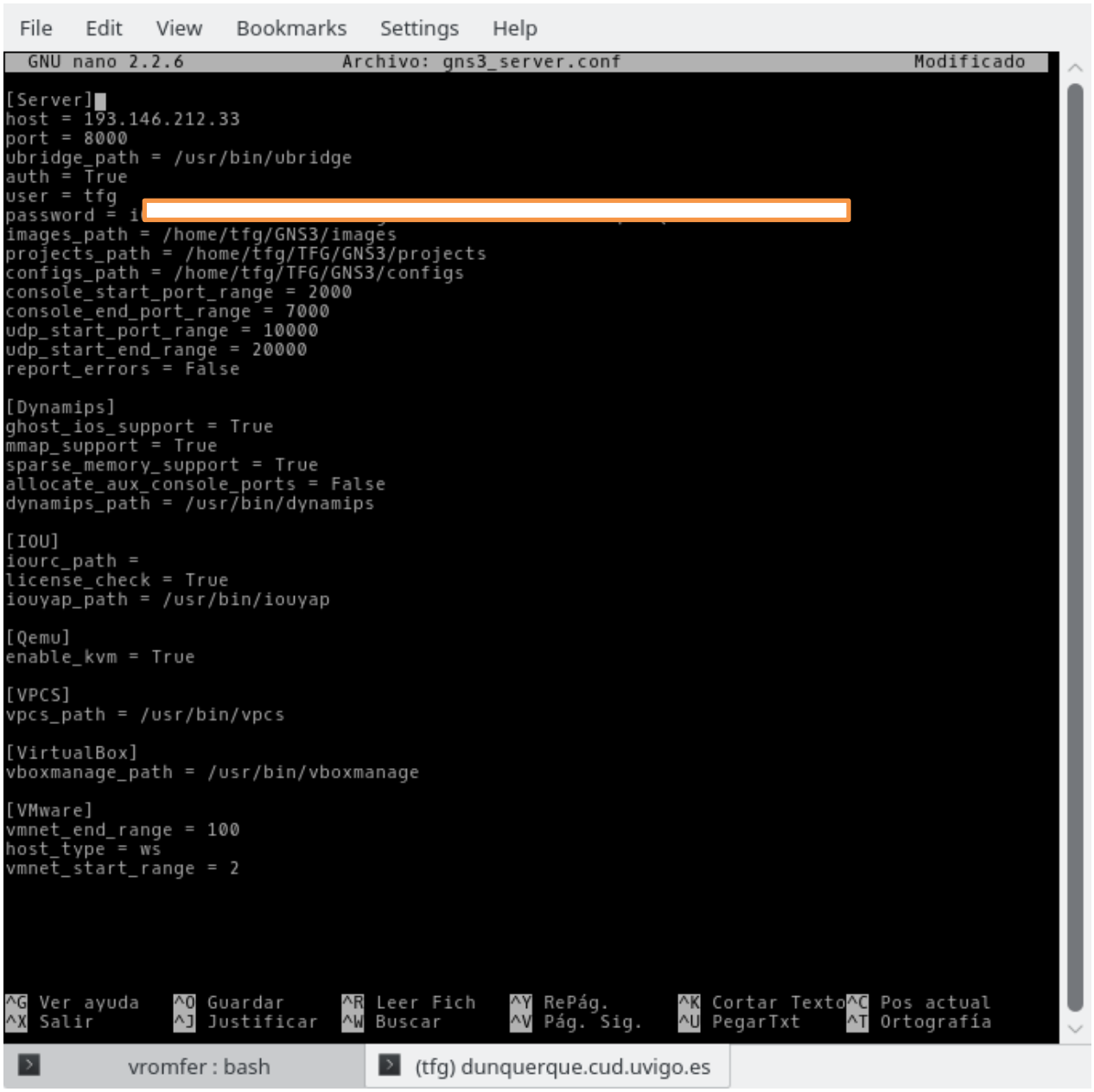

Figura 3-5: Archivo de configuración GNS3 Server

Una vez que el archivo de configuración del servidor de GNS3 ha sido actualizado con la información necesaria, se puede ejecutar el comando *gns3server*, que inicia el servidor y se mantiene a la escucha en el puerto asignado. Si el programa no encuentra ningún error, mostrará en el terminal la salida que se observa en la Figura 3-6. Al ejecutar este servidor de esta forma, se está ejecutando como si se tratase de un programa, y no un servicio, por lo que es necesario mantener la sesión del terminal remoto abierta. Se puede ejecutar como servicio si deseamos que se mantenga abierto una vez cerremos la sesión remota añadiendo el parámetro *--daemon* al comando. Este procedimiento presenta la desventaja de no proporcionar información de depuración que nos puede ayudar a encontrar errores, por lo tanto, no será utilizado hasta una fase posterior del trabajo.

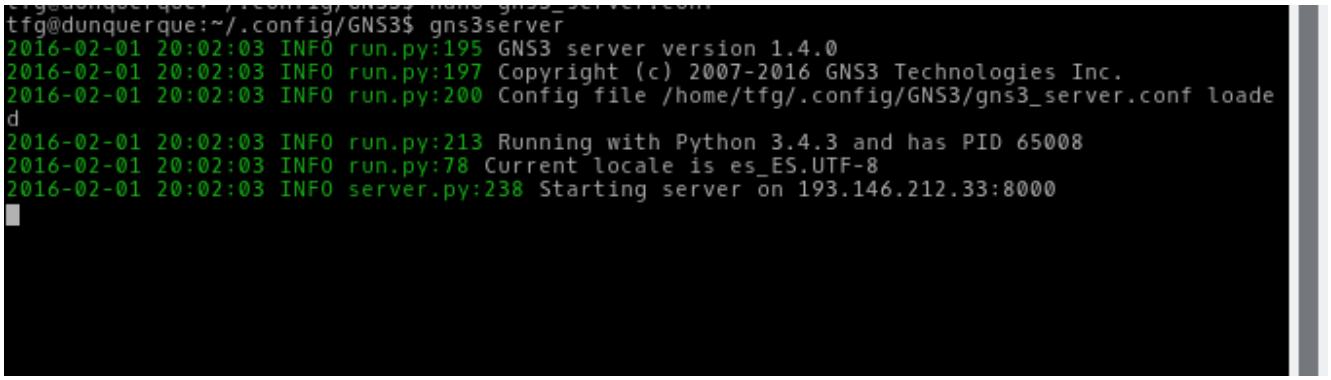

Figura 3-6: GNS3 ejecutándose en el terminal

Una vez funcionando correctamente el servidor de GNS3 en *Dunquerque*, se ejecutará el cliente GNS3 en el ordenador de trabajo, mediante el comando *gns3*. Este cliente es un entorno gráfico que, en primera instancia, intenta ejecutar y conectar con un servidor de GNS local. Es necesario añadir el servidor que se está ejecutando en *Dunquerque* a la lista de servidores. Para ello, como ilustra la Figura 3-7, en la ventana de *Preferences* nos dirigimos a la sección *Server*, desde la cual podremos desactivar el servidor local, y al mismo tiempo añadir a la lista de servidores remotos a *Dunquerque*. Es necesario recordar el nombre de usuario y contraseña que se configuraron anteriormente.

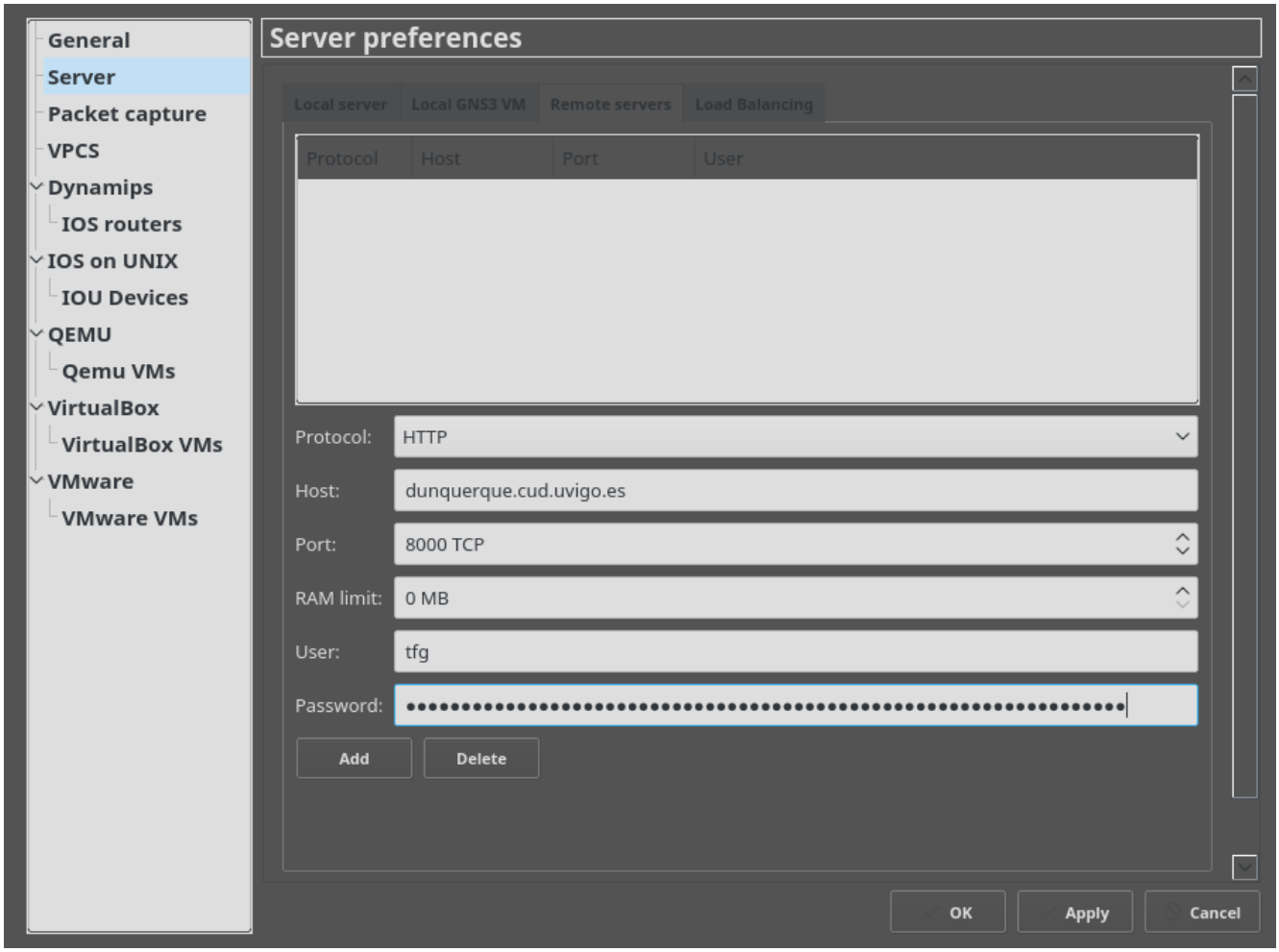

Figura 3-7: Configuración de servidor remoto en GNS3

Al guardar la configuración, el cliente conectará con el servidor y se autenticará. A partir de este momento, cuando se añada un dispositivo a la topología de red, el cliente preguntará sobre qué servidor queremos que se ejecute la simulación de este dispositivo, como puede verse en la Figura 3-8.

Se pueden añadir tantos servidores como se deseen mediante este procedimiento, lo que permitiría balancear la carga y ejecutar simulaciones de topologías de red mucho mayores. Se puede comprobar que la conexión entre cliente y servidor es correcta observando la terminal en la que se ejecuta el servidor, que deberá mostrar las conexiones entrantes y los dispositivos que está añadiendo o modificando el cliente.

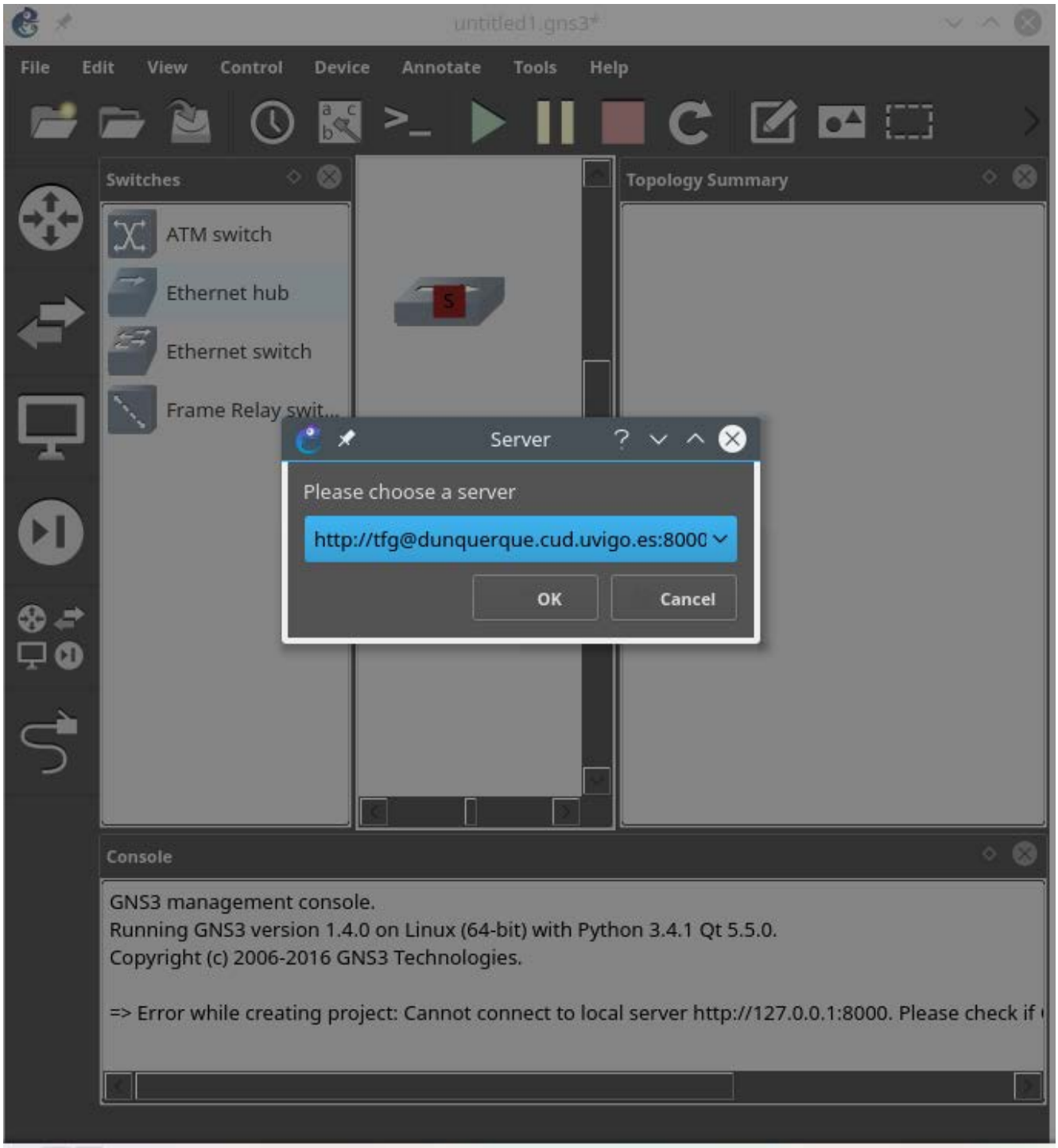

Figura 3-8: Añadir un dispositivo que se ejecuta en un servidor remoto

3.1.2.4 Otras herramientas.

Aunque los programas principales en los cuales se basa la maqueta son VirtualBox y GNS3, es necesario introducir otras herramientas que se han utilizado para poder realizar este trabajo.

- ***Filezilla***

  Filezilla es un cliente de FTP con funciones avanzadas, que permite conectarse como cliente SFTP al puerto 22. Se utilizará para realizar las transferencias de archivos entre el servidor *Dunquerque* y el ordenador de trabajo, y viceversa. Se instala en el ordenador de trabajo con *sudo apt-get install filezilla*. Este software se distribuye de manera gratuita bajo licencia GNU.

- **Cliente KRDP**

  KRDP es un cliente para conectarse mediante el protocolo de escritorio remoto (*Remote Desktop Protocol)* a otros ordenadores. Esta aplicación está preinstalada en la versión de *Open SUSE* que se ha instalado en el ordenador de trabajo. Se utilizará para acceder al servidor *Dunquerque* mediante este protocolo y también a cada una de las máquinas virtuales de la maqueta mediante el puerto RDP que activa VirtualBox.

- **SSH**

  SSH son las siglas de *Secure SHell*, que es un protocolo de red que sirve para acceder a máquinas remotas en forma de una terminal segura. De igual manera se llama el programa que implementa el protocolo. El cliente se encuentra instalado en la mayoría de las distribuciones de *Linux* y se ejecuta desde la terminal. Se utiliza para acceder de forma remota y segura a un terminal de comandos. Tambien se puede redirigir la salida grafica hacia el cliente, haciendo uso del parámetro *–X*.

3.1.3 Metodología de trabajo (gestión remota)

Se quiere implementar una maqueta que funcione de forma autónoma sobre el servidor *Dunquerque*, pero en las fases de desarrollo la maqueta estará dividida entre el servidor y el ordenador de trabajo. Además no se ejecutará durante todo el tiempo. Para trabajar con la maqueta se siguen los pasos siguientes.

1. Desde el ordenador de trabajo se abren dos sesiones remotas al servidor *Dunquerque* mediante SSH
   ```
   $ ssh Dunquerque.cud.uvigo.es -l tfg
   ```

2. En una de las sesiones remotas se ejecuta el servidor de GNS3, la otra sesión se mantiene abierta para poder ejecutar comandos de control u otros que sean necesarios, ya que la que ejecuta el servidor GNS3 queda ocupada y muestra sus salidas.
   ```
   $ gns3server
   ```

3. En una terminal del ordenador de trabajo se lanza el cliente de GNS3.
   ```
   $ gns3
   ```

4. Desde el cliente de GNS3 se carga el proyecto con la arquitectura de red y se pulsa el botón *play* para lanzar las máquinas virtuales.

5. Con el cliente KRDP, en el cual se han configurado los accesos a las máquinas virtuales como marcadores, se abre una sesión de escritorio remoto sobre la máquina virtual con la que queramos trabajar en cada momento.

Para finalizar la sesión de trabajo, se paran las máquinas virtuales desde GNS3 y posteriormente se cierra el programa y se para el servidor. Por último, se cierran las sesiones remotas.

3.2 Diseño de la arquitectura

En este apartado se va a introducir el modelo de maqueta que se quiere implementar, servirá como punto de partida y base para el desarrollo de las posteriores secciones del proyecto.

3.2.1 Descripción general

El escenario más común donde se reciben ataques cibernéticos es en las redes empresariales. Estas redes además de ser el objetivo más rentable, suelen ofrecer servicios al público y, por tanto, están más expuestas. La maqueta de este trabajo va a basarse en una red que podría pertenecer a una corporación de tamaño medio. Sin embargo, los recursos disponibles en el servidor que va a ejecutar la maqueta son limitados, por lo que no se podrá simular en la maqueta toda la arquitectura de red corporativa.

La maqueta se va a basar en el modelo de red en tres zonas; *Internet, zona desmilitarizada y red de usuarios*, también llamadas WAN, DMZ y LAN, respectivamente.

La zona de la red que más carga supondría para la maqueta es la de usuarios. Una corporación de tamaño medio, que usase una red como la que se va a implementar en la maqueta, tendría al menos cincuenta puestos de trabajo conectados a la red en esta zona. La ejecución de este elevado número de máquinas virtuales consumiría elevados recursos en el servidor *Dunquerque*, hasta el punto de no poder soportar la carga. Además, la simulación de cada uno de los puestos de trabajo no aporta nada a la maqueta, ya que todos presentan las mismas características y vulnerabilidades de cara a un ataque cibernético.

Debido a lo expuesto anteriormente, se ha decidido introducir una artificialidad en la maqueta. Mientras que la zona de servicios de la red se implementará completamente, la zona de usuarios se verá reducida a un número más lógico de estaciones de trabajo.

3.2.2 Servicios

En la maqueta se van a implementar ciertos servicios que normalmente son necesarios para el funcionamiento de la empresa. Estos servicios en algunos casos también se ofrecerán para los clientes, o usuarios de fuera de la red. Aunque no se pueden generalizar los servicios que ofrecen las redes de una organización, pues cada una es diferente a las demás, en esta maqueta se van a implementar los que creemos son comunes a la mayoría. Los servicios que se quieren ofrecer en la maqueta son los siguientes:

- Portal web de la organización
- Servidor de resolución de nombres (DNS)
- Servicio de intercambio de archivos
- Correo electrónico corporativo.

Para satisfacer estas necesidades de servicios, se implementarán cinco servidores, y sobre ellos las aplicaciones correspondientes. El paradigma en estos momentos nos dicta separar servicios por servidores, que pueden ser o no máquinas físicas.

1. **Servidor de páginas web.** Será el encargado de alojar las páginas web de la empresa y servirlas a los usuarios que necesiten visitarlas. Estará disponible desde el exterior y desde el interior. El servidor de páginas web que se instalará será *Apache* [50] Sobre él se instalarán las siguientes aplicaciones:
    a. ***Joomla*** [51]**,** un gestor de contenidos utilizado para crear el portal de la organización y organizar su contenido. El uso de un gestor de contenidos en lugar de una página web

tradicional facilita la actualización de la información contenida y además eleva la opinión creada de la organización a través de su página web.

b. ***Rainloop*** [52]**,** un cliente de webmail que se configurará para que los usuarios con cuenta de correo corporativo puedan consultarlo desde cualquier dispositivo, indistintamente si es desde dentro o fuera de la red corporativa.
c. ***Phpmyadmin*** [53], aplicación web utilizada para gestionar el servidor de bases de datos de la organización. Aunque este servidor puede gestionarse sin esta aplicación, es una práctica bastante común hacerlo desde ella, ya que se considera más seguro que permitir conexiones directamente al servidor de bases de datos.

2. **Servidor de bases de datos.** Se trata de un servidor auxiliar en el que se alojarán las bases de datos necesarias para las aplicaciones de la organización. En esta maqueta en particular será utilizado por el gestor de contenidos, el servidor de correo electrónico, el cliente webmail y el gestor de bases de datos. Cada una de estas aplicaciones usará una base de datos dedicada y accederá con su usuario particular. Se va a implementar un servidor de bases de datos con *Mysql* [54].
3. **Servidor de FTP.** Este servidor permitirá la compartición de archivos entre los usuarios de la organización, y también con el exterior. Su objetivo es compartir y distribuir archivos que no sean de carácter sensible, por lo que su seguridad deberá ser excesivamente elevada. El software encargado del servidor FTP será *VSFTP (Very Secure FTP Daemon)* [55].
4. **Servidor de resolución de nombres (DNS).** Este servidor proveerá a los usuarios del interior de la red corporativa la resolución de nombres. Disponer de este servicio en el interior de la red corporativa eleva su nivel de seguridad y hace más difícil que los usuarios sufran un ataque de *DNS Spoofing*. El servidor DNS que se configurará es el servidor DNS de *Windows Server 2008.*
5. **Servidor de correo electrónico.** El servidor de correo electrónico será el encargado de gestionar las cuentas de correo corporativo que se determinen. Este servidor de correo electrónico debe permitir el envío y la recepción de mensajes desde el exterior, así como el intercambio de mensajes internos. Para las labores de servidor de correo electrónico se ha elegido *hMailserver* [56].

3.2.3 Seguridad

La seguridad de la red de la maqueta vendrá dada por un cortafuegos de tres patas que realizará la separación de las tres zonas de la red. Este cortafuegos deberá estar correctamente configurado para permitir el acceso a los servicios que deban ser accesibles desde cada una de las zonas, y al mismo tiempo que proporcione la seguridad necesaria a los servicios que no sean accesibles. Además, será el encargado de ocultar la topología de la red al exterior. La zona más protegida será la LAN, mientras que la DMZ será la zona de la red más expuesta a los posibles ataques exteriores, sin llegar a ser vulnerable. El *firewall* que se va a implementar es *pfSense*. Su elección se ha basado en la gran cantidad de características y opciones disponibles, su gran estabilidad y a que es gratuito.

3.2.4 Esquema

Con los datos descritos en los apartados 3.2.1, 3.2.2 y 3.2.3 el esquema de partida para la realización de la maqueta es el que se puede ver en la Figura 3-9

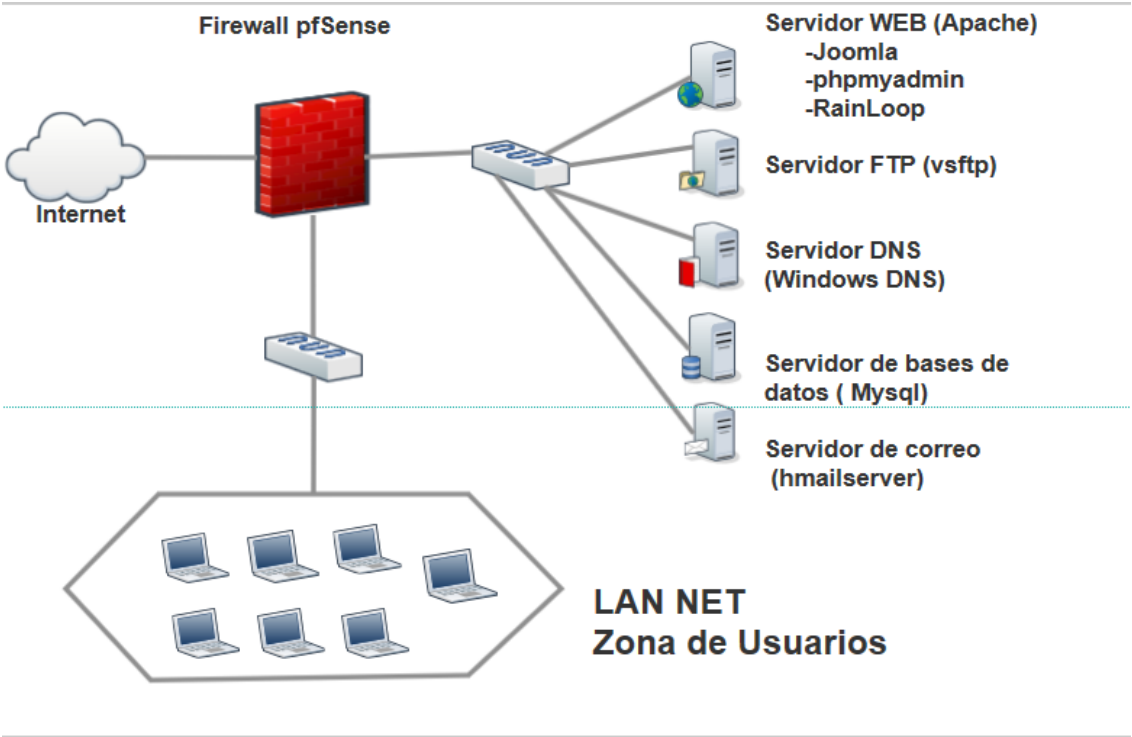

Figura 3-9: Arquitectura de red propuesta de la maqueta

3.3 Implementación de la arquitectura

3.3.1 Configuración de máquinas virtuales

Para crear una máquina virtual, VirtualBox dispone de un asistente, en el cual se asigna un nombre, y se indica el sistema operativo que va a ser instalado en ella.

Las máquinas virtuales pueden crearse en el ordenador de trabajo por comodidad, y luego ser transferidas al servidor *Dunquerque*, gracias a la independencia del anfitrión que proporciona VirtualBox.

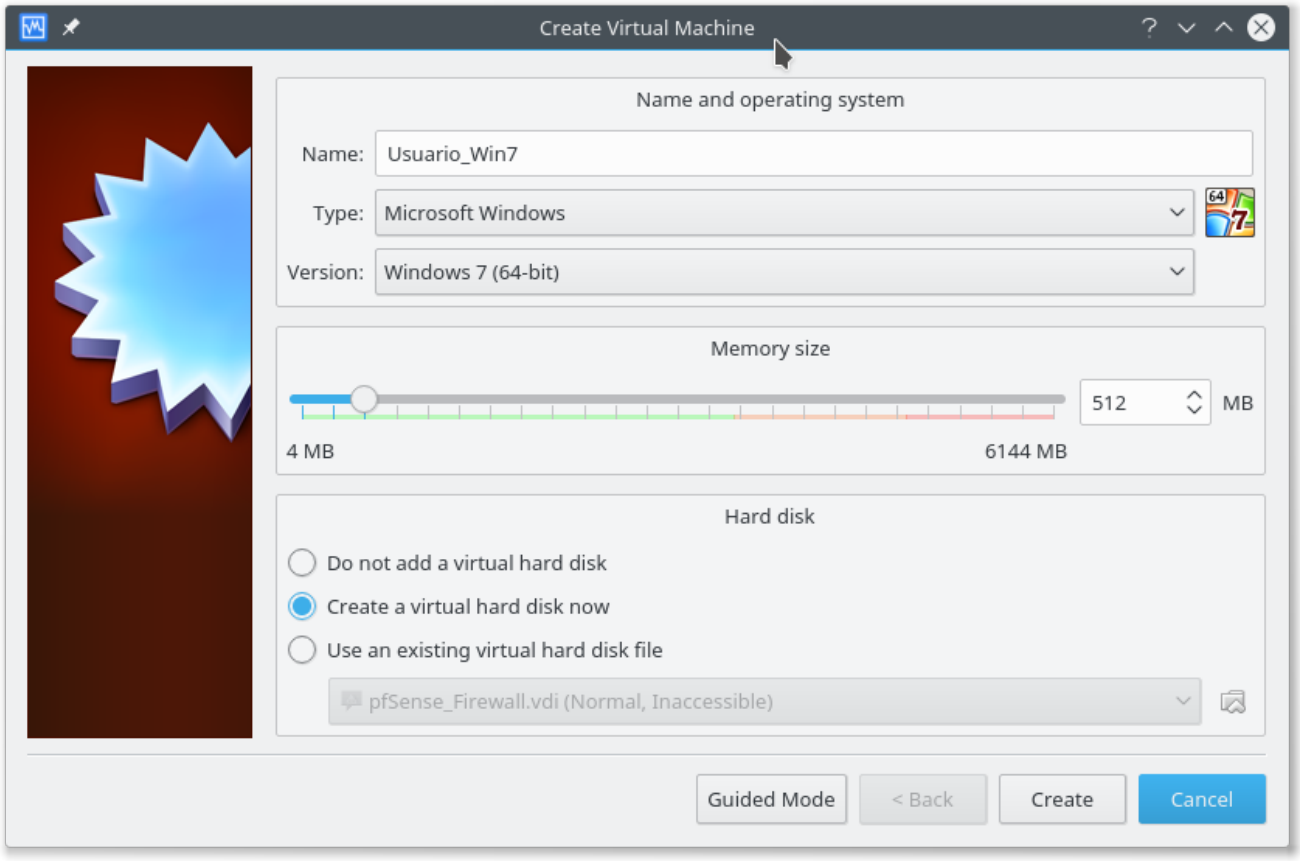

Figura 3-10: Asistente de creación de máquinas virtuales con VirtualBox

En el siguiente paso del asistente debemos indicar donde guardar el archivo de disco duro virtual, que contendrá todos los datos de la máquina virtual, así como su formato y el tamaño máximo del que dispondrá la máquina virtual.

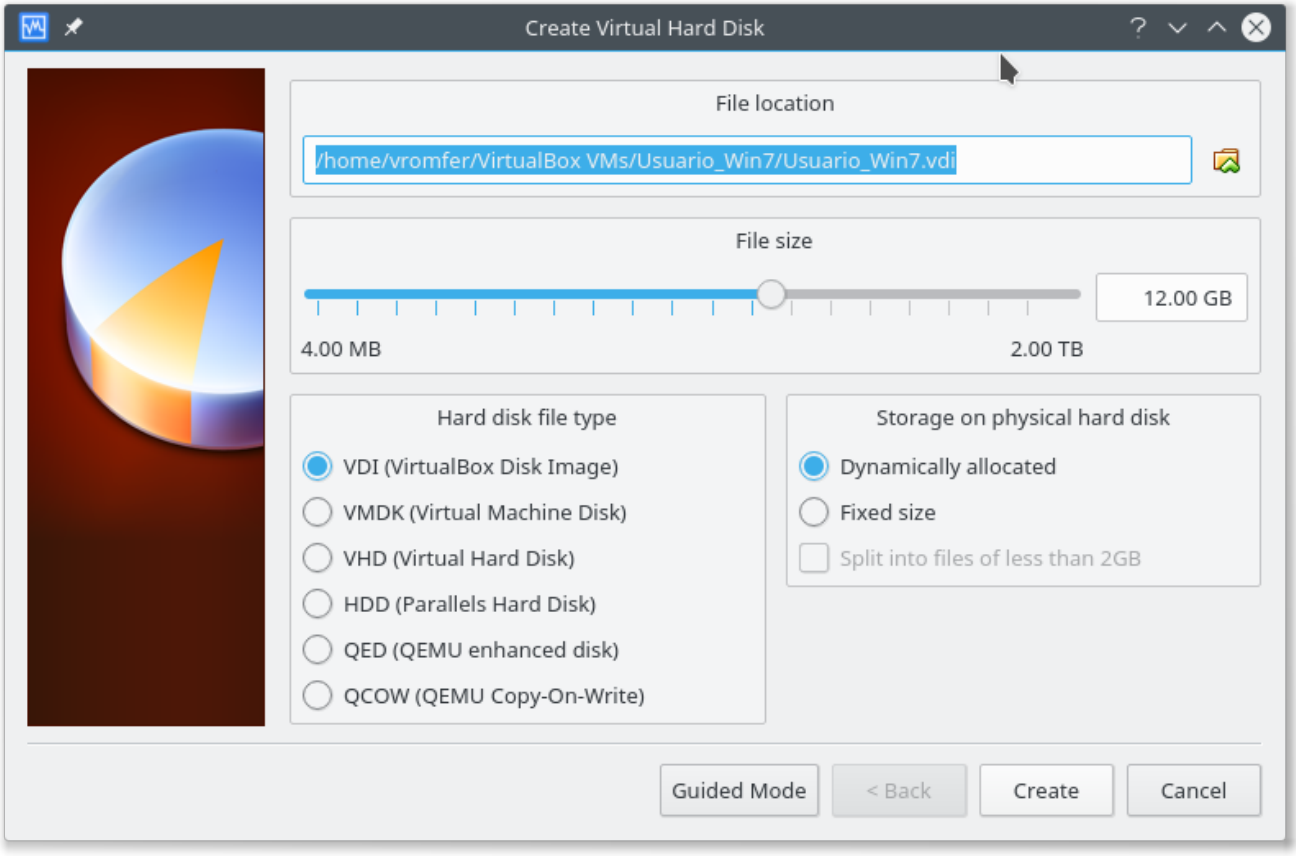

Figura 3-11: Creación de disco duro virtual

Siguiendo estos pasos se han creado cinco máquinas virtuales, que corresponden a los diferentes sistemas operativos que se van a utilizar en la arquitectura de red a simular. Las máquinas virtuales creadas tienen las características que muestra la Tabla 3-1.

Nombre	Sistema Operativo	RAM	Disco duro máximo
USER_WIN7	Microsoft Windows 7	512MB	12GB
USER_WIN8.1	Microsoft Windows 8.1	512MB	12GB
SERVER_UBUNTUS	Ubuntu Server 14.04	512MB	16GB
SERVER_WIN2008S	Microsoft Windows Server 2008	512MB	25GB
pfSense	BSD64bit (*firewall* pfSense)	256MB	3GB

Tabla 3-1: Características de las máquinas virtuales I

Una vez creadas las máquinas virtuales, es necesario configurar los adaptadores de red. Si necesitamos conexión a Internet durante la instalación de los sistemas operativos utilizaremos *NAT*. Si no es necesaria la conexión, seleccionaremos *Not Attached*.(véase Figura 3-12) Todas las máquinas virtuales se han configurado con un adaptador de red, excepto la correspondiente al cortafuegos *pfSense* que tiene tres.

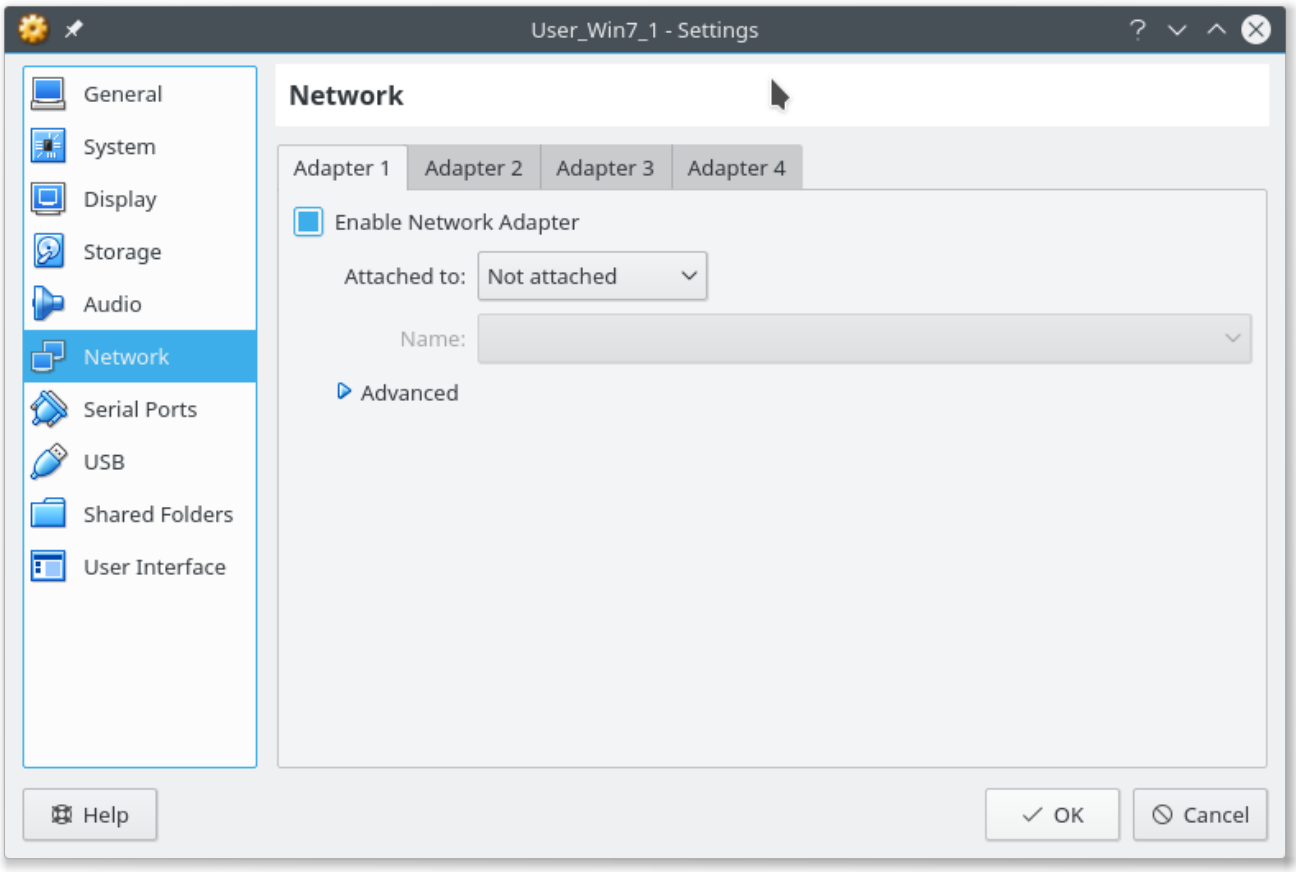

Figura 3-12: Configuración de un adaptador de red

Con las máquinas virtuales configuradas el siguiente paso es instalar los sistemas operativos huéspedes siguiendo las instrucciones que figuran en el Anexo I:

Las máquinas virtuales con el sistema operativo instalado se transfieren al servidor *Dunquerque* usando el programa *Filezilla*, que es un cliente de FTP con capacidades para transmitir la información sobre SSH (SFTP). Para realizar esta operación realizaremos la conexión al servidor mediante el puerto 22, en lugar del 21 correspondiente al FTP normal, y con los mismos datos de autenticación que se utilizan para iniciar una sesión remota en el servidor.

Cada máquina virtual consta de varios archivos, uno de ellos corresponde a la configuración de la máquina virtual, con extensión *.vbox;* y otros con la extensión *.vdi* que corresponden al disco duro virtual de la máquina. Para transferir una máquina virtual a otro ordenador basta con copiar ambos archivos en una misma carpeta, y posteriormente agregarla a VirtualBox. También podría haberse utilizado el asistente de importación y exportación de máquinas virtuales.

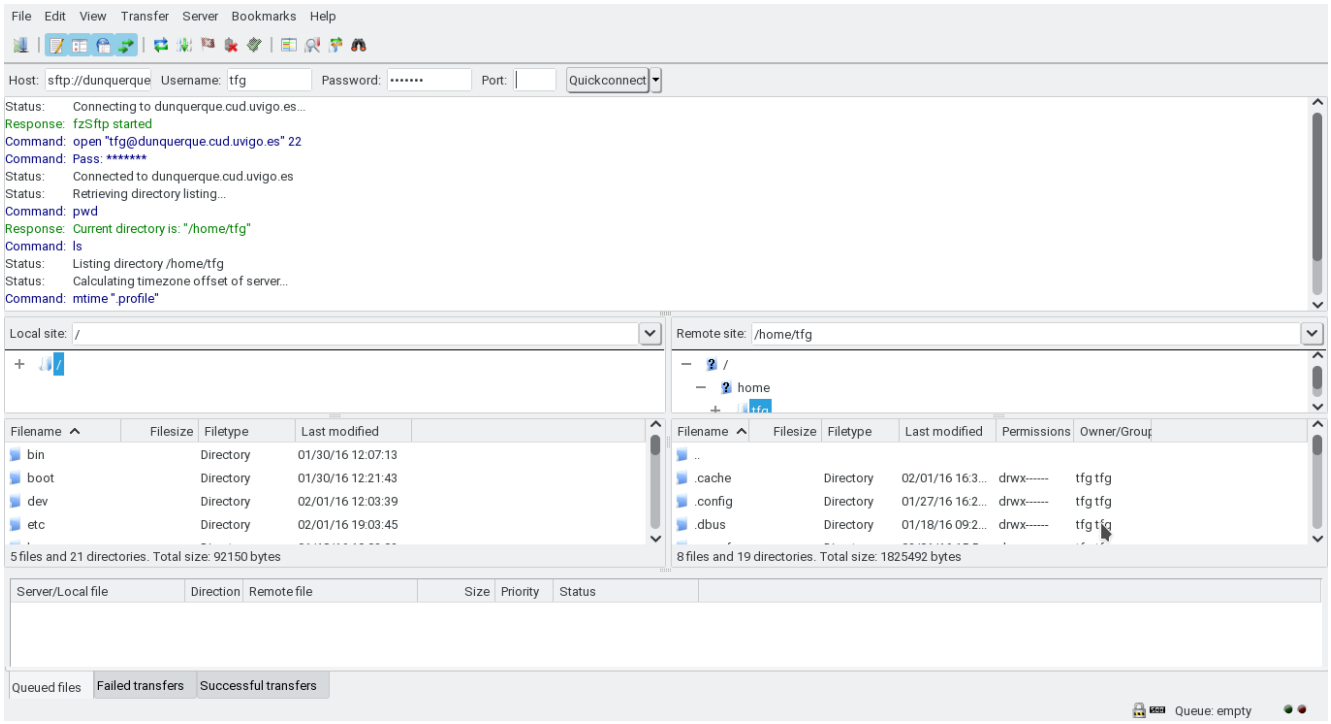

Figura 3-13: Conexión SFTP con *Filezilla* a *Dunquerque*

Con todas las máquinas virtuales transferidas al servidor *Dunquerque*, se inicia sesión en el mismo mediante escritorio remoto para agregarlas al programa VirtualBox. Una vez agregadas, se realizan las actualizaciones de configuración necesarias para adaptarlas al hardware disponible en el servidor, que es diferente al que tenían disponible en el ordenador de trabajo. Las modificaciones de configuración que se realizaron fueron las siguientes:

- Asignar correctamente el número de procesadores disponibles y el límite de uso de los mismos.
- Configurar todos los adaptadores de red como *Not attached* o No conectado.
- Desactivar el audio.
- Desactivar el USB 2.0 por problemas de compatibilidad.

Cuando las máquinas virtuales están correctamente configuradas y se pueden ejecutar sin problemas, se procede a clonarlas para poder usar cada una de ellas más de una vez de manera simultánea. El propio software dispone de un asistente de clonado de máquinas virtuales. El tipo de clon elegido es *Linked Clone* o "Máquina enlazada", el cual no copia de nuevo el disco duro virtual completo, si no que guarda *Snapshots* con el estado de ejecución de cada uno de los clones, y utiliza el mismo disco virtual como base para ejecutar la máquina. Es importante seleccionar la opción de *Reinicializar la dirección MAC de todos los adaptadores de red* (véase Figura 3-14) para evitar problemas posteriores cuando se conecten las máquinas en la misma red local.

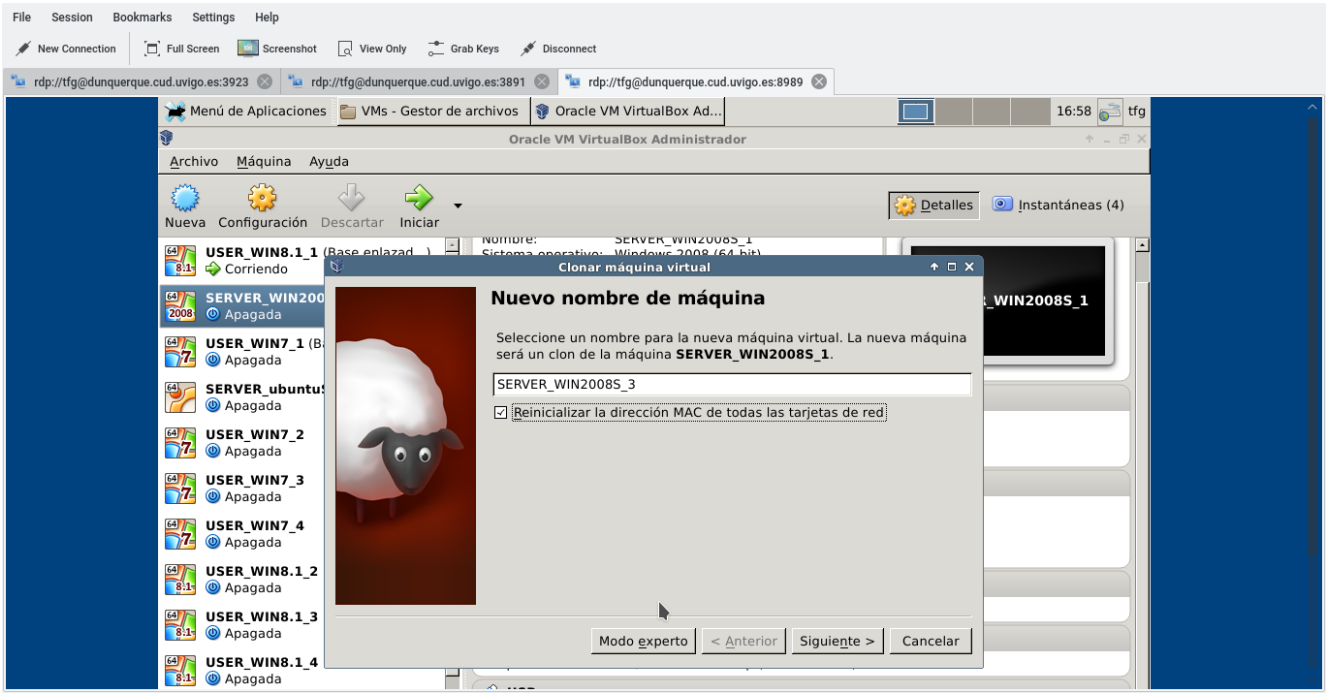

Figura 3-14: Asistente de VirtualBox para clonar una máquina virtual

La última modificación a la configuración de las máquinas virtuales corresponde a la activación del acceso mediante escritorio remoto, en la cual debe asignarse un puerto diferente a cada una de las máquinas virtuales. Esta acción permitirá posteriormente la conexión mediante escritorio remoto directamente a la máquina virtual, evitando tener que acceder a las máquinas virtuales a través del servidor *Dunquerque*, lo que proporciona una mayor comodidad y velocidad a la hora de trabajar. En la Figura 3-15 se ilustra cómo realizar esta acción. Es necesario reseñar que habilitar un servidor de escritorio remoto hacia una máquina virtual de esta forma, sin autenticación, es inseguro y supone la creación de una puerta trasera expuesta a Internet. Esta puerta trasera es inexistente para los sistemas operativos instalados en los equipos de la maqueta ya que se encuentra en un nivel superior, el hipervisor; sin embargo, su descubrimiento y explotación durante un ataque al propio servidor *Dunquerque* proporcionarían al atacante la capacidad de estar, virtualmente, sentado delante de las máquinas e interactuar con ellas.

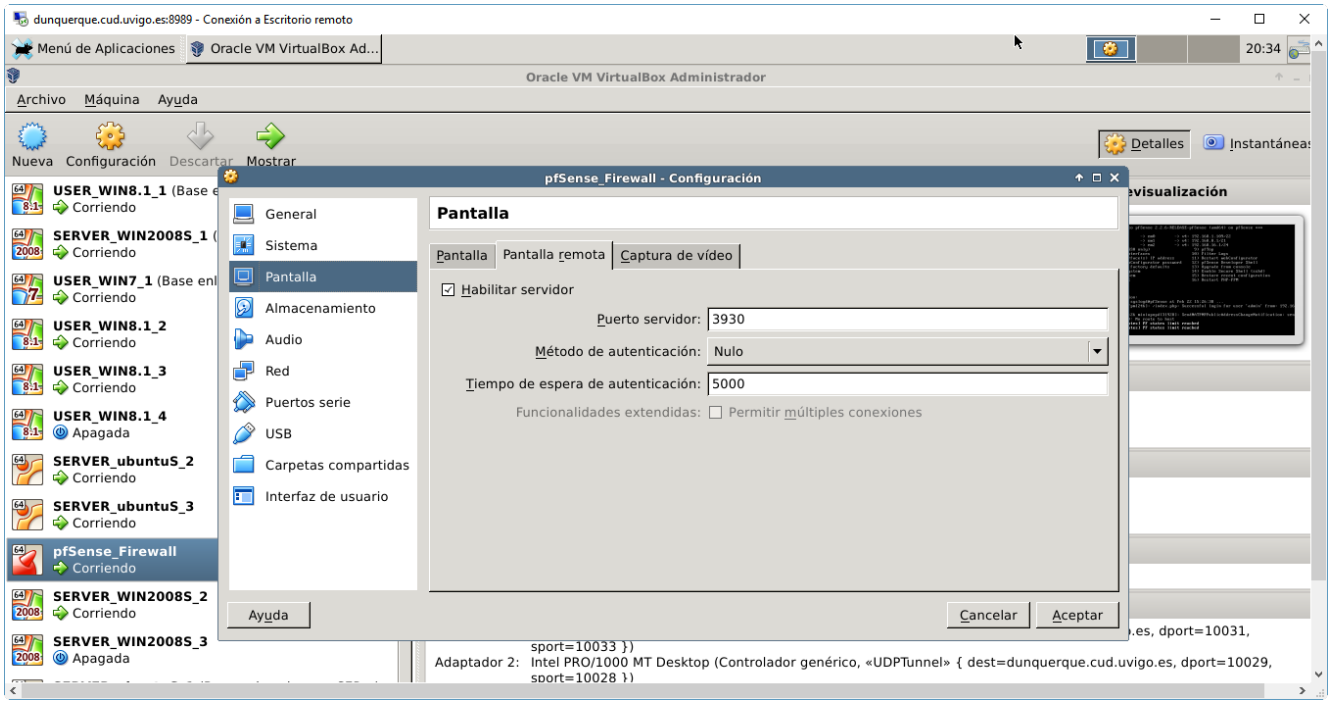

Figura 3-15: Apertura de un puerto para escritorio remoto para una máquina virtual.

A modo de resumen la configuración de las máquinas virtuales queda como se muestra en la Tabla 3-2.

Nombre	S.O.	Nº CPU y uso máximo	RAM	HD	Nº Interfaces Red	Puerto escritorio remoto
USER_WIN8.1_1	WIN8.1_x64	1@100%	2048MB	12GB	1	3891
USER_WIN8.1_2	WIN8.1_x64	1@50%	2048MB	12GB	1	3892
USER_WIN8.1_3	WIN8.1_x64	1@50%	2048MB	12GB	1	3893
USER_WIN7_1	WIN7_x64	1@50%	2048MB	12GB	1	3901
SERVER_WIN2008S_1	WIN Server 2008R2 (x64)	1@100%	1024MB	25GB	1	3911
SERVER_WIN2008S_2	WIN Server 2008R2 (x64)	1@100%	1024MB	25GB	1	3912
SERVER_UBUNTUS_1	Ubuntu Server 14.04 (AMD64)	1@75%	512MB	15GB	1	3921
SERVER_UBUNTUS_2	Ubuntu Server 14.04 (AMD64)	1@75%	512MB	15GB	1	3922
SERVER_UBUNTUS_3	Ubuntu Server 14.04 (AMD64)	1@75%	512MB	15GB	1	3923
pfSense	BSD_x64 (pfSense)	1@50%	1024MB	2GB	3	3930

Tabla 3-2: Características de las máquinas virtuales II

3.3.2 Configuración de la red

En el subapartado 3.3.1 se configuraron las máquinas virtuales que van a formar la arquitectura de red. Estas máquinas virtuales, que se ejecutan sobre VirtualBox, serán controladas directamente por el simulador GNS3, siendo este último el encargado de encenderlas, apagarlas y realizar sus conexiones de red.

GNS3 integra un módulo de control de máquinas virtuales de VirtualBox. Para poder utilizarlo hay que añadir las máquinas virtuales como dispositivo final al programa. Esto se realiza desde el apartado *VirtualBox VMs* dentro de las preferencias de GNS3.

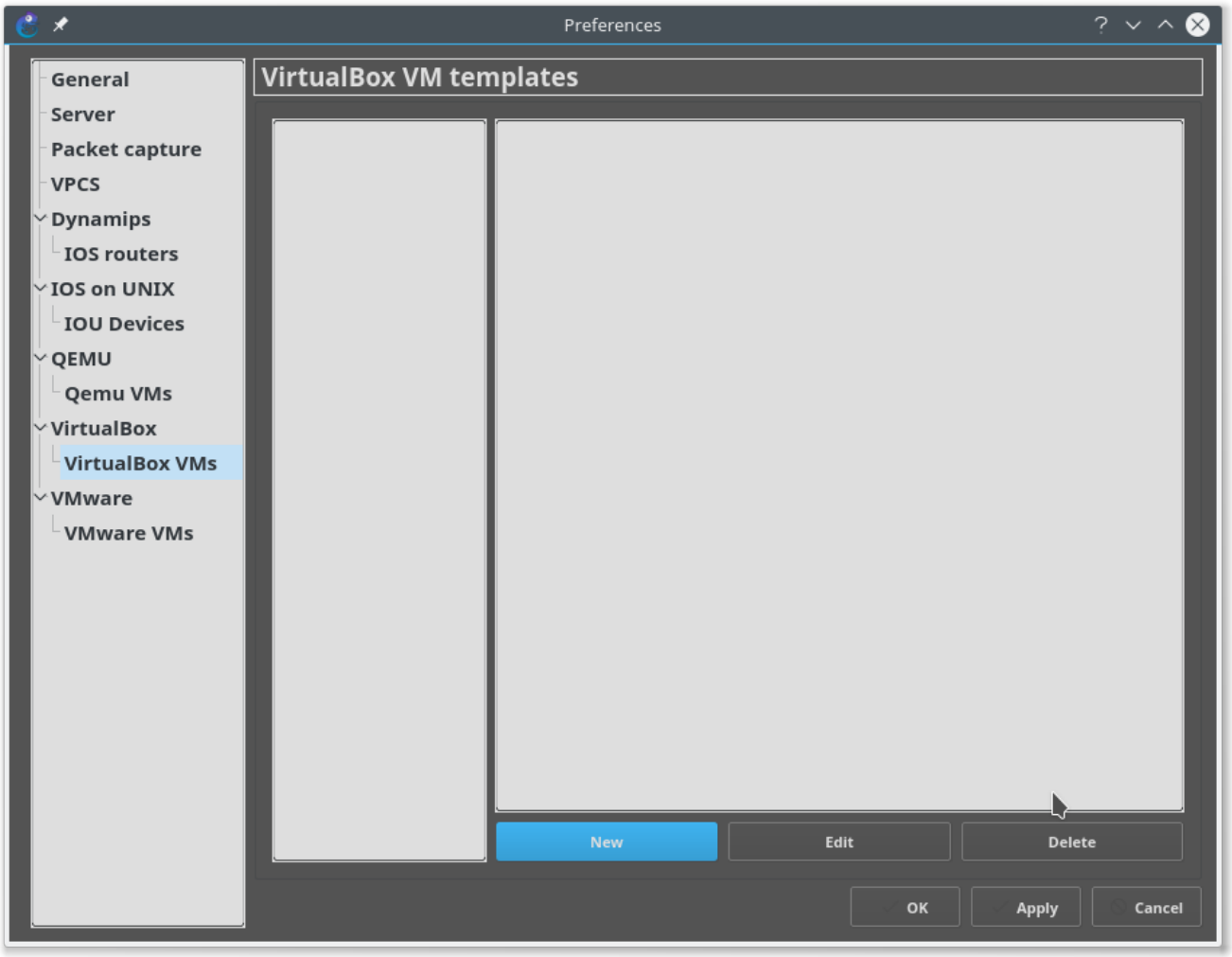

Figura 3-16: Añadir una máquina de VirtualBox a GNS3

Con el botón *New* que aparece en la Figura 3-16 se abre el asistente para esta tarea. Es necesario seleccionar el servidor en el que se encuentran las máquinas virtuales que vamos a agregar.

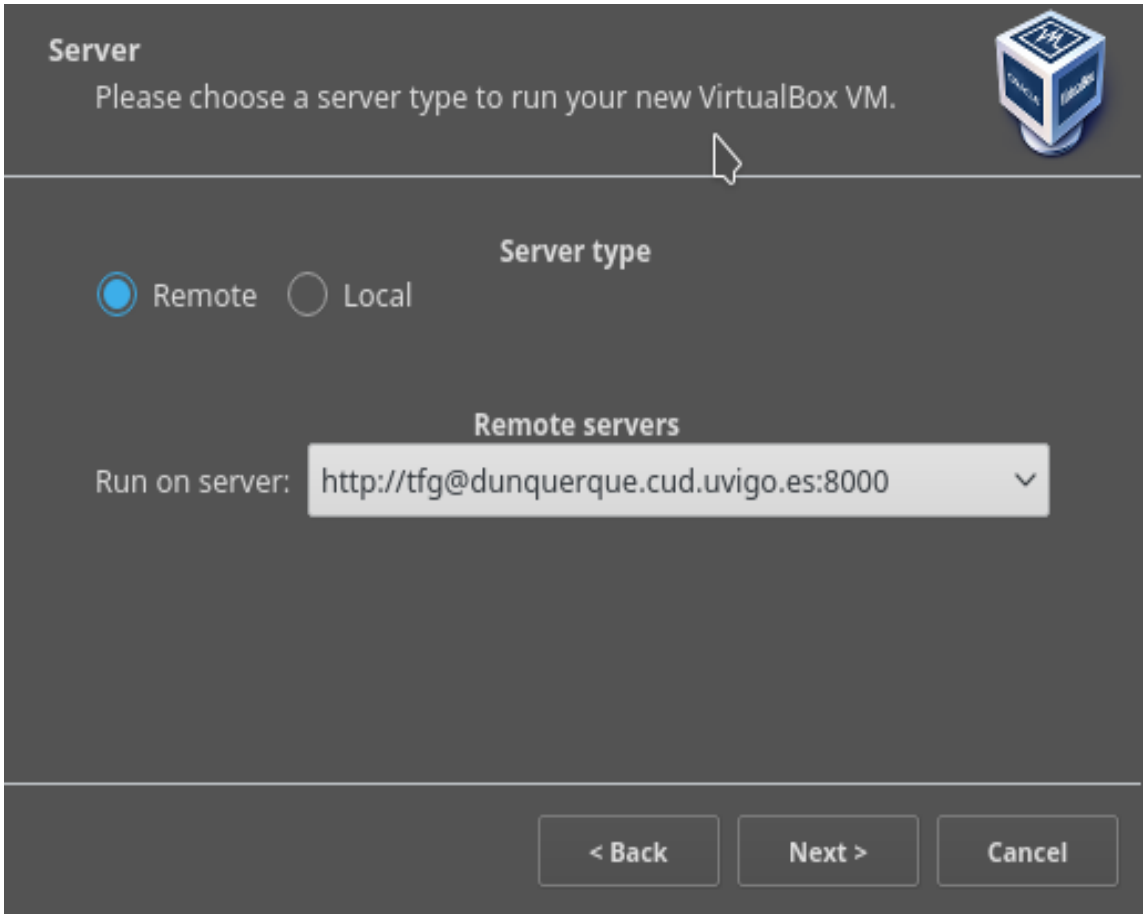

Figura 3-17: Selección del servidor que aloja las VM

Tras seleccionar el servidor, el programa conecta con el servicio de VirtualBox y lista todas las máquinas virtuales cargadas en el sistema anfitrión.

Una vez finalizado el asistente, la máquina virtual se agrega a la lista de máquinas de GNS3. En su configuración es necesario activar la opción de *Start VM in headless mode* para que la máquina virtual se inicie en segundo plano (ver Figura 3-18).

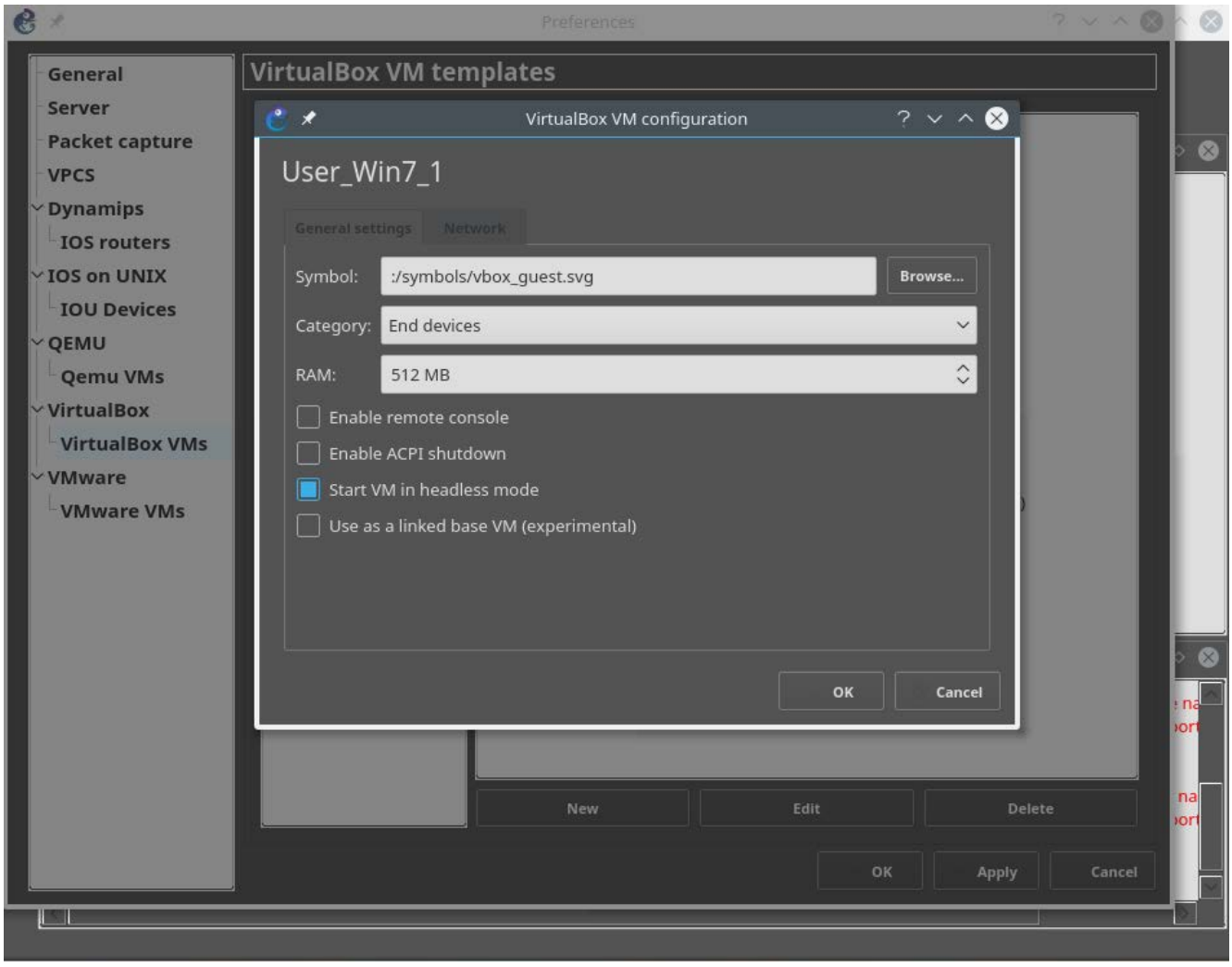

Figura 3-18: Configuración de una máquina virtual de VirtualBox en GNS3

Se repiten estos pasos con todas las máquinas virtuales que se vayan a utilizar en la simulación. En nuestro caso, la configuración es la mostrada en la Figura 3-19.

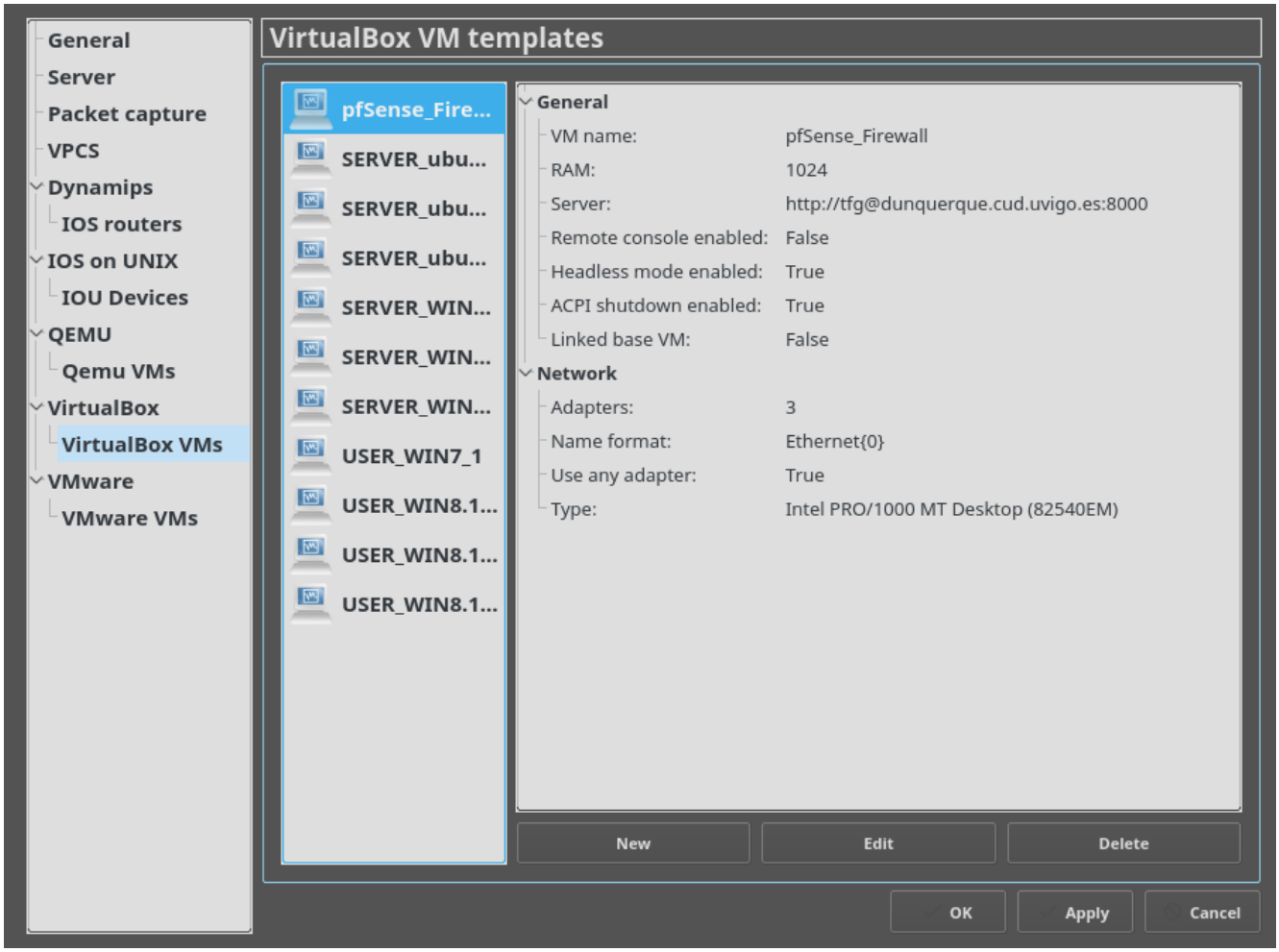

Figura 3-19: Maquinas virtuales en GNS3

Con las máquinas virtuales integradas en GNS3 disponemos de todo lo necesario para crear la topología de red propuesta. Para ello buscamos los equipos necesarios en la lista de dispositivos y los arrastramos a la pantalla de trabajo. Posteriormente, se interconectan usando la herramienta de conexión.

Para nuestra topología son necesarios los siguientes dispositivos:

- 1 Máquina virtual *firewall* (con *pfSense*)
- 2 Conmutadores de *Ethernet*
- 5 Máquinas virtuales de tipo Servidor (2 con *Windows Server 2008*, 3 con *Ubuntu Server 14.04*)
- 4 Máquinas virtuales de tipo Usuario (1 con *Windows* 7, 3 con *Windows* 8.1)
- 1 Nube

El dispositivo especial Nube simboliza una conexión con un interfaz físico del servidor *Dunquerque*. En esta fase del proyecto se ha configurado para que se asocie al interfaz de red principal mediante NAT, con lo cual proporciona acceso a Internet a la topología de red, aunque no permite que las máquinas sean accesibles desde Internet. En una fase posterior, se habilitará un interfaz dedicado que permitirá el acceso desde el exterior a la red virtual.

Tras la realización de los enlaces con la herramienta de conexiones, la topología de red queda como se aprecia en la Figura 3-20.

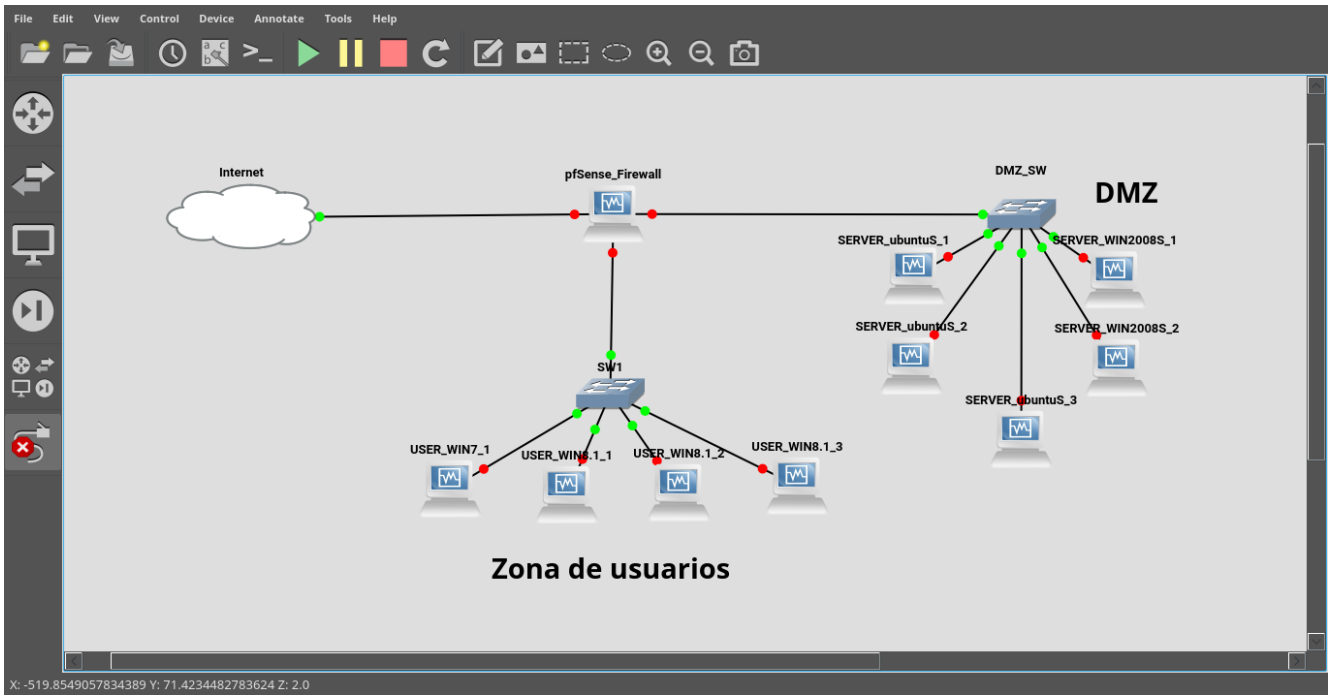

Figura 3-20: Topología de red de la maqueta

Con todas las máquinas virtuales enlazadas al programa, y la topología de red configurada correctamente, al pulsar *Play* se inicia la simulación. El programa enviará los comandos necesarios al servidor para configurar los adaptadores de red de las máquinas virtuales, y posteriormente las irá ejecutando.

3.3.3 Instalación del firewall pfSense.

El *firewall* elegido es *pfSense*, basado en BSD (*Berkeley Software Distribution*) pero se distribuye como si de un sistema operativo se tratase, por lo que se puede instalar directamente sobre la máquina virtual. Es necesario descargar la imagen de disco desde su página oficial y montarla en la unidad de DVD-ROM virtual de la máquina. Para esto, se conecta mediante escritorio remoto a *Dunquerque* y se configura en VirtualBox.

Cuando la máquina virtual arranca desde la imagen de disco, se presenta el menú que se ve en la Figura 3-21.

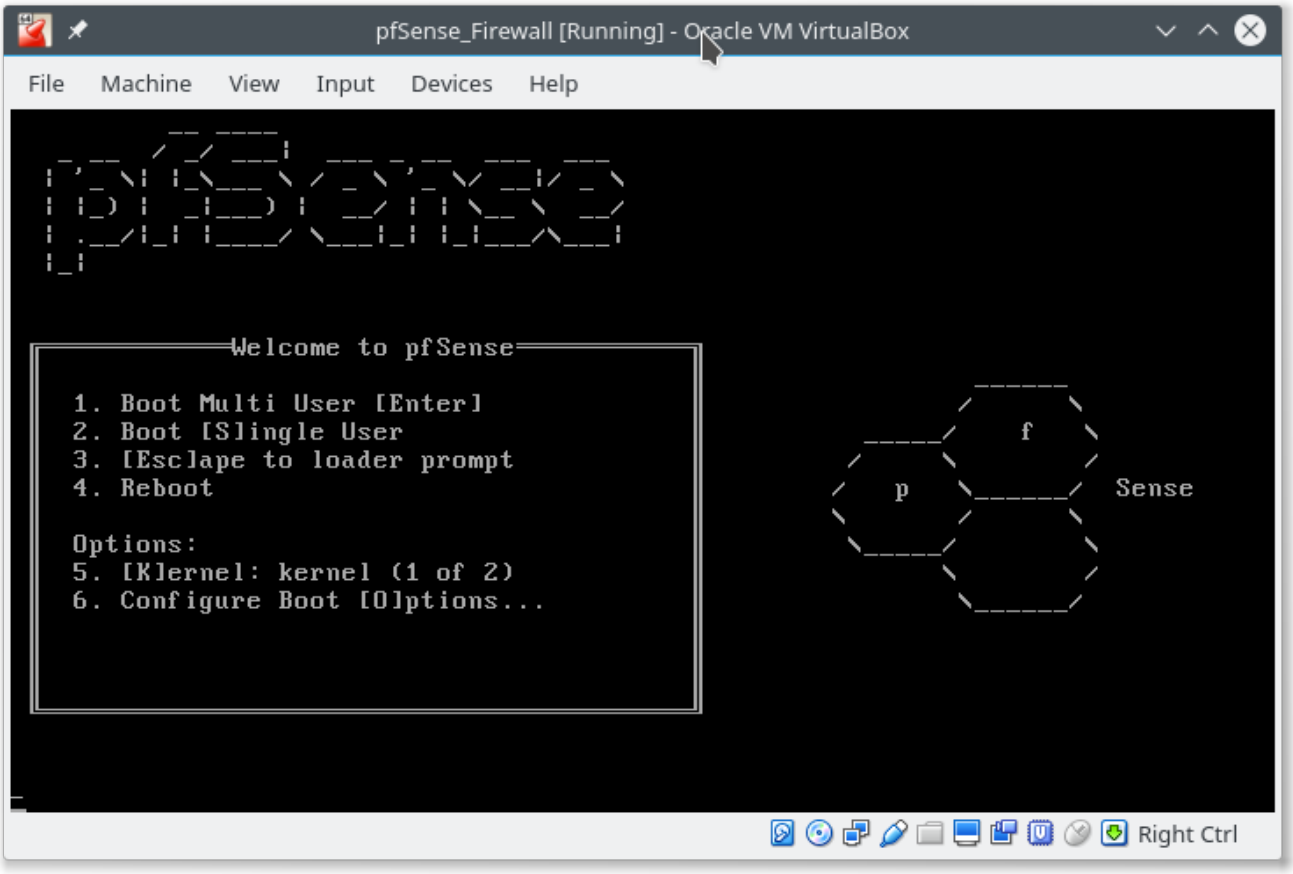

Figura 3-21: Boot-menu de *pfSense*

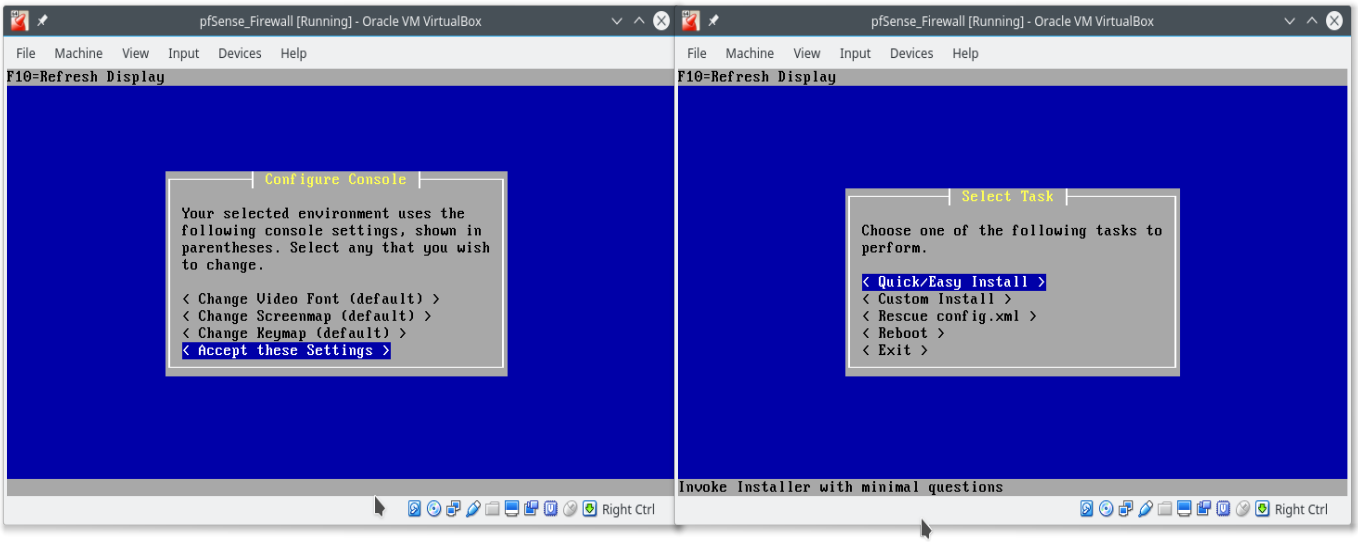

Figura 3-22: Instalador de *pfSense*

Una vez realizado el arranque, se carga el instalador directamente. El instalador es un asistente textual (ver Figura 3-22) en el cual se presentan las opciones configuradas por defecto y la posibilidad de cambiar alguna de ellas si se desea. En este caso, se va a realizar una instalación por defecto.

Tras la instalación, la máquina virtual se reinicia. Aunque *pfSense* dispone de un configurador basado en web, la configuración inicial se debe realizar desde la consola. La pantalla de inicio de *pfSense* (Figura 3-23) es un menú numérico que nos permite realizar las configuraciones necesarias.

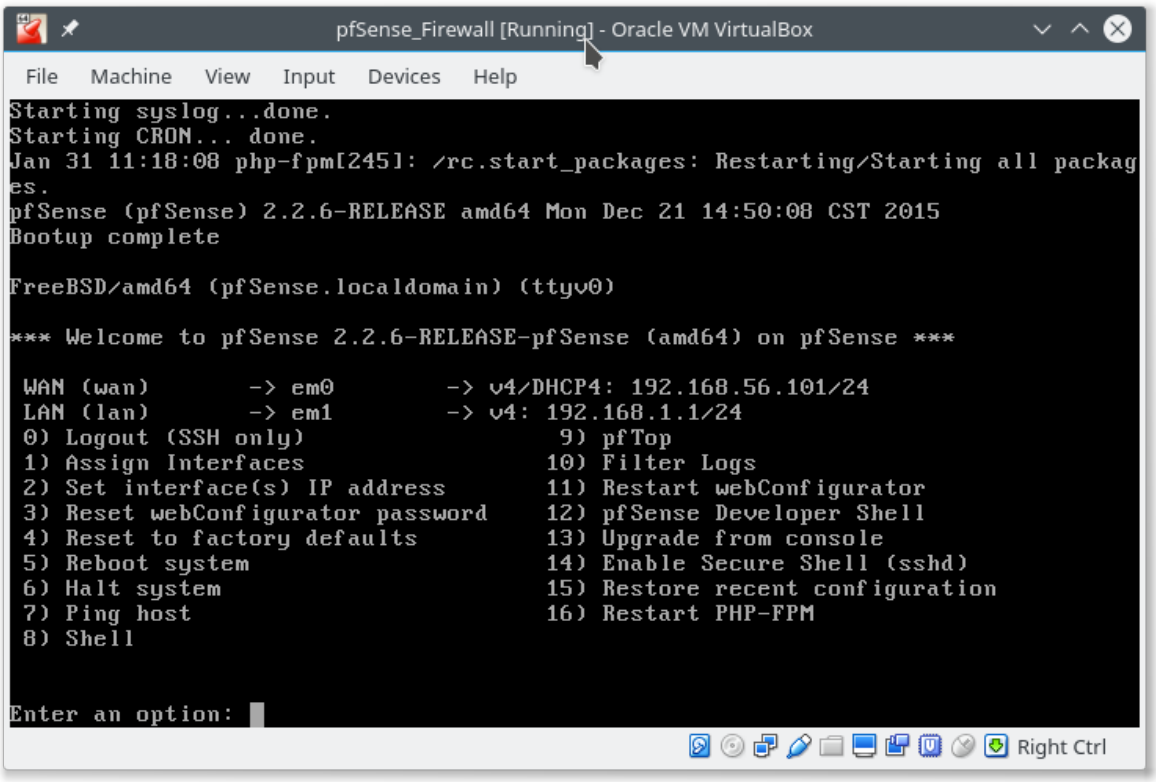

Figura 3-23: Pantalla de inicio de *pfSense*

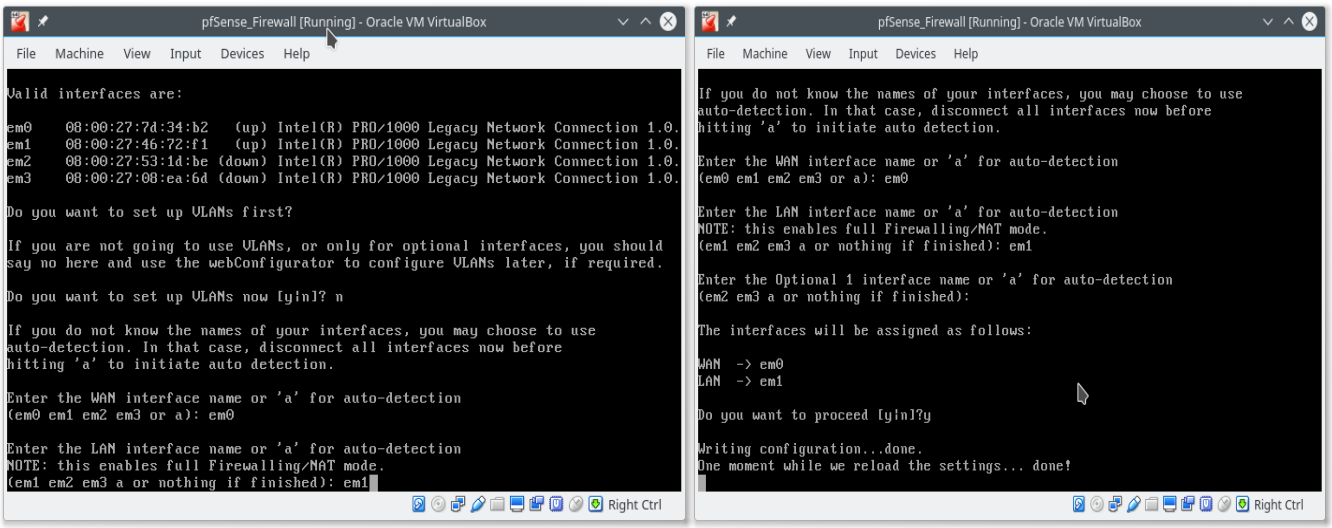

Figura 3-24: Asignar interfaces *pfSense*

En primer lugar, mediante la opción 1 asignaremos los interfaces de red a las redes WAN y LAN, según están conectados a Internet y la red interna, respectivamente. En este paso, no asignaremos el interfaz correspondiente a la DMZ, pues solo se pretende configurar lo mínimo para poder acceder al

configurador web del *firewall* para configurarlo con mayor comodidad. En la Figura 3-24 se pueden ver los pasos seguidos para realizar la asignación de los interfaces a LAN y WAN

Posteriormente, es necesario configurar las direcciones IP que usará cada interfaz, mediante la opción 2.

Se han asignado las siguientes direcciones IP (ver Figura 3-25) a los adaptadores, aunque posteriormente serán modificadas para adecuarlas a la red que se va a crear.

- WAN: 10.10.10.2/16; Puerta de enlace: 10.10.10.1
- LAN: 192.168.16.1/16

Es necesario reseñar que se ha asignado una IP interna al interfaz WAN cuando en realidad debería tener una IP pública, porque se encuentra conectado de manera virtual a Internet, a través de la conexión del servidor *Dunquerque*.

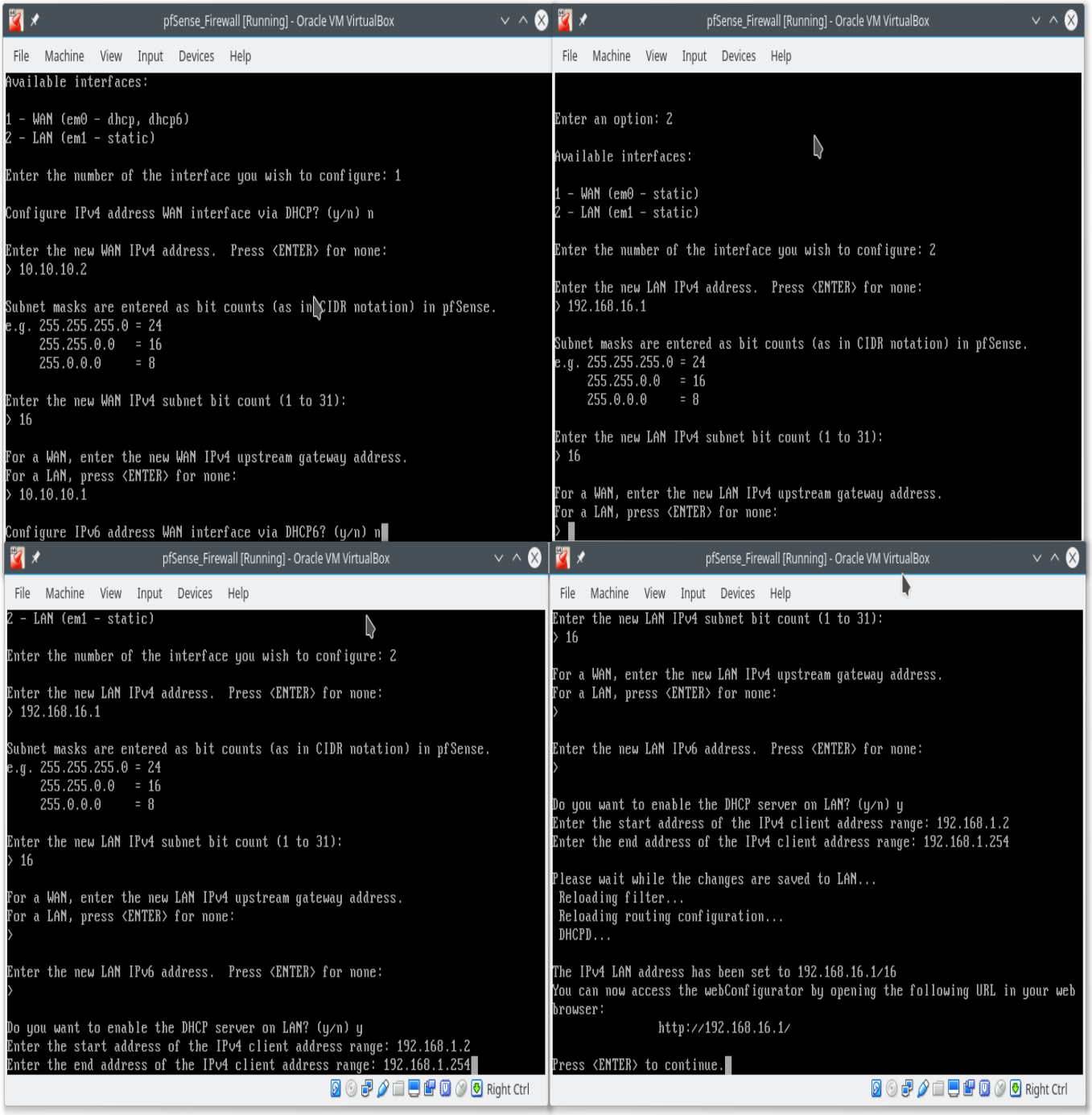

Figura 3-25: Asignación de IP a los interfaces de pfSense

Una vez asignadas las direcciones IP, activamos el servidor DHCP para la conexión LAN y asignamos el rango de IP que podrán asignarse a esta red.

Con la configuración mostrada en la Figura 3-25 ya se puede acceder al configurador web del *firewall* (ver Figura 3-26). Para ello es necesario usar una máquina virtual conectada a la LAN e introducir en el navegador la dirección IP del cortafuegos

La primera vez que se accede al configurador web se inicia un asistente que ayuda a realizar la configuración inicial. Mediante este asistente se configuran datos básicos como el dominio en el que se encuentra la máquina y los DNS que usará la red (véase Figura 3-26)

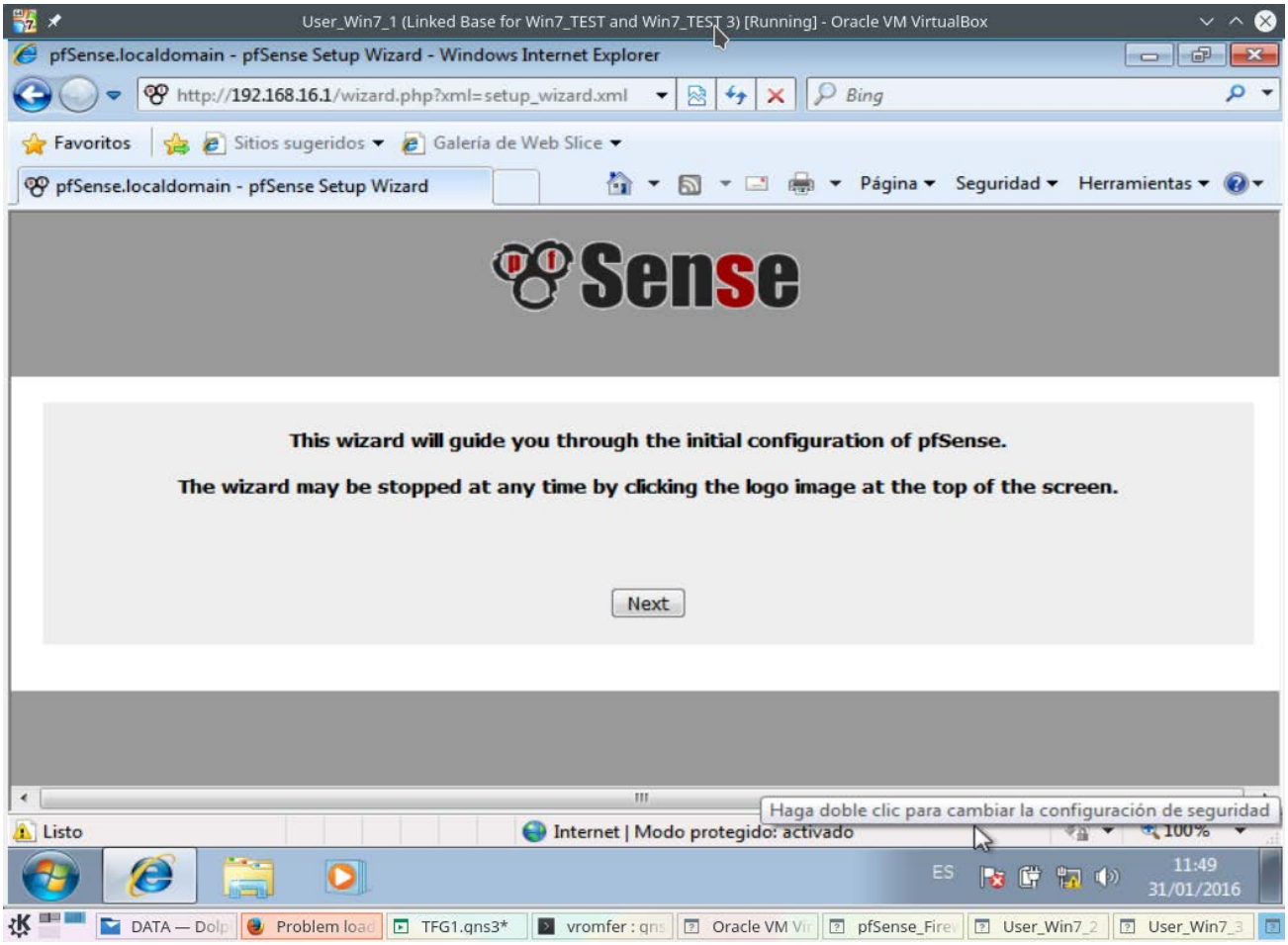

Figura 3-26: Asistente inicial del configurador web pfSense

Desde el configurador web, se activa la interfaz correspondiente a la zona desmilitarizada y se modifican las configuraciones necesarias en cada uno de los menús. Las modificaciones que se llevaron a cabo en este punto fueron:

- Establecer el dominio *tfg.dunquerque.cud.uvigo.es*.
- Usar el DNS local que se instalará a continuación 192.168.16.20.
- Activar y asignar el interfaz de DMZ. Establecer su IP como 192.168.16.1/24 (ver Figura 3-27).
- Cambiar la IP de LAN a 192.168.15.1/16.
- Configurar el servidor DHCP para que solo actúe en la red LAN y establecer su rango de IP de 192.168.1.2 a 192.168.15.254.
- Crear una regla en el *firewall* que permita el tráfico en todos los puertos hacia todos los interfaces, esta regla es únicamente para comodidad durante el desarrollo, se desactivará posteriormente.

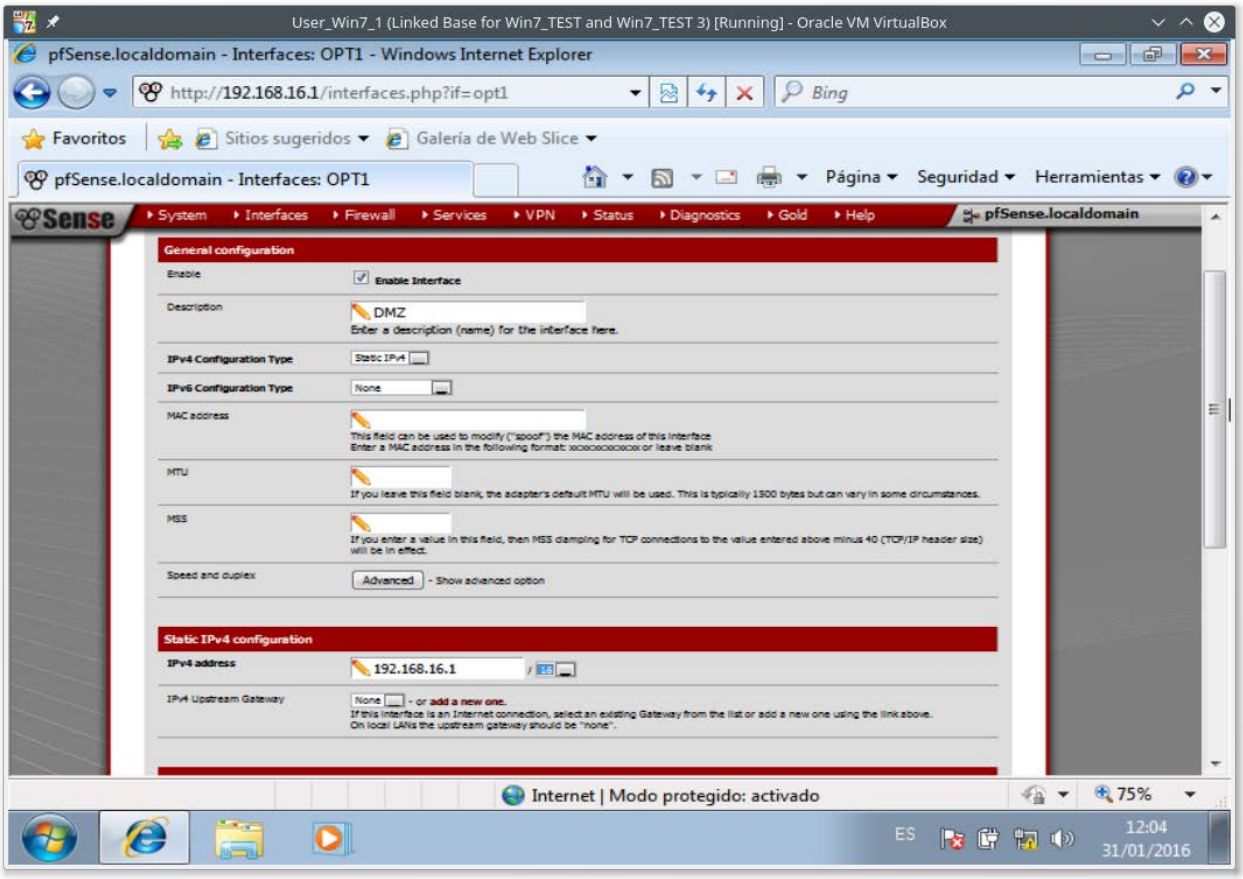

Figura 3-27: Activar interfaz DMZ

Con esta configuración, el *firewall* se encuentra funcionando aunque de manera insegura. En este momento cumple las funciones de router y de servidor DHCP.

3.3.4 Instalación de servidores

3.3.4.1 Servidor DNS

El primero de los servicios a implementar de los que se incluyen en la arquitectura de red a simular es el servidor DNS. Este servidor se va a configurar sobre la máquina virtual SERVER_WIN2008S_1 y tendrá la IP 192.168.16.20.

En primer lugar, partiendo de una máquina virtual con Windows Server 2008 instalado como se indica en el Anexo I:, es necesario configurar los datos relativos al nombre de la máquina, dominio y dirección IP. En este momento, los servidores DNS configurados son externos para permitir el acceso a Internet de esta máquina (véase Figura 3-28).

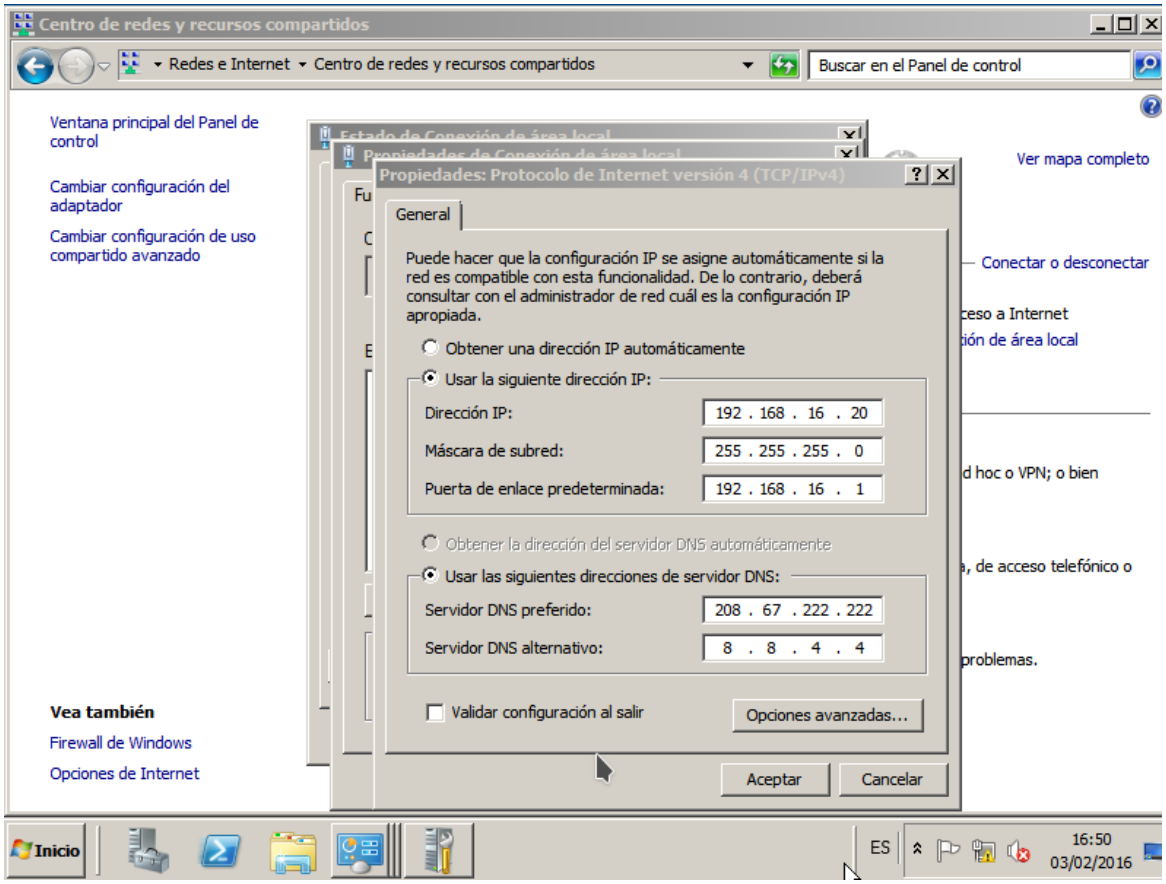

Figura 3-28: Configuración IP de la máquina servidor DNS

En Windows Server 2008 el servicio de servidor DNS está asociado al rol de servidor *Active Desktop*, por lo que en primer lugar habrá que realizar la instalación y configuración del citado rol. Esta instalación se inicia desde el panel de administración del servidor, con la opción de agregar una nueva función. Seleccionaremos únicamente la de *Servicios de dominio de Active Directory*.(ver Figura 3-29) Posteriormente se instalará el servidor DNS.

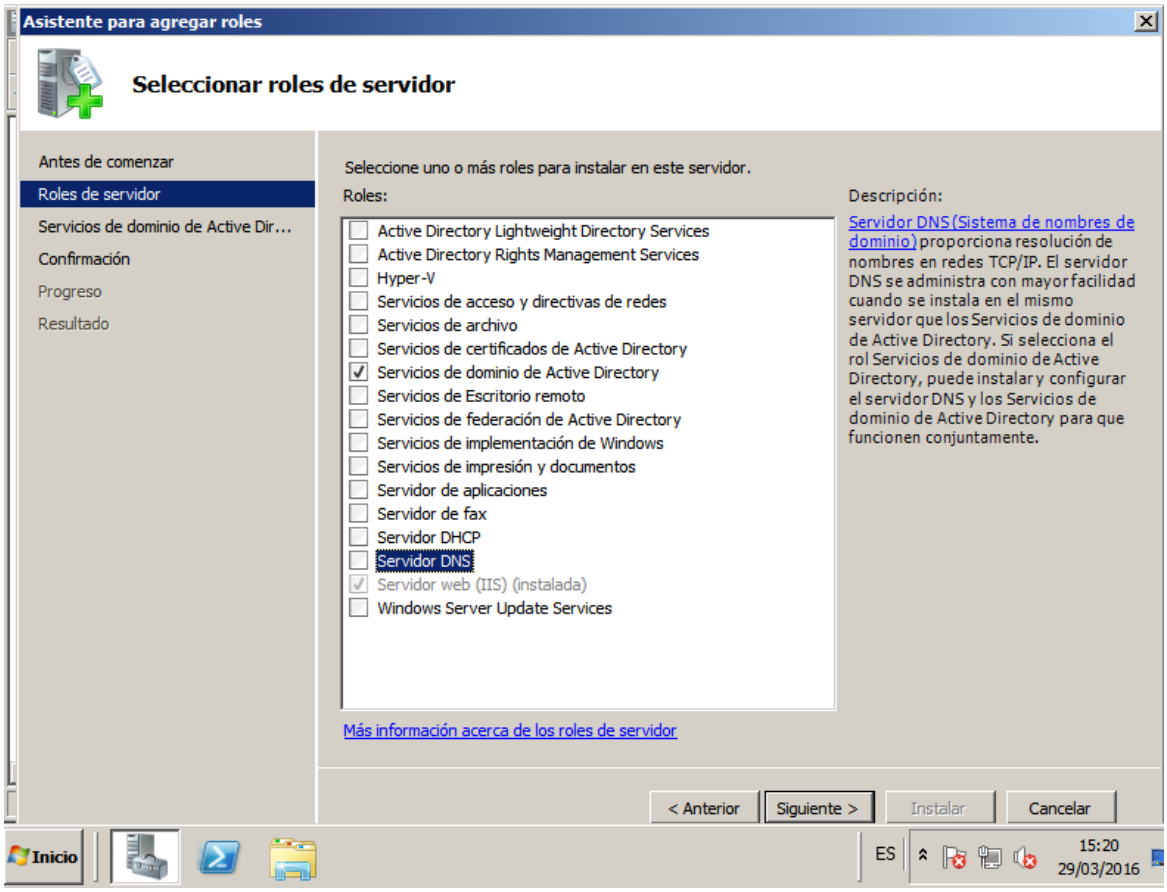

Figura 3-29: Instalación del servicio *Active Directory*

Durante la instalación se explican las características adicionales y actualizaciones obligatorias que va a llevar a cabo el asistente de manera automática. Cuando la instalación acaba, aparece una nueva función que se puede administrar en el servidor.

El dominio elegido es *tfg.dunquerque.cud.uvigo.es*, que como no existe será creado y administrado por esta máquina. Para ello abrimos el asistente de configuración de *Active Directory* mediante el comando *dcpromo.exe* (ver Figura 3-30).

No se desea integrar este dominio con los que pudieran existir en la red del Centro Universitario de la Defensa, por lo que se crea el contenedor de nivel superior *Bosque* y se administra desde esta máquina virtual.

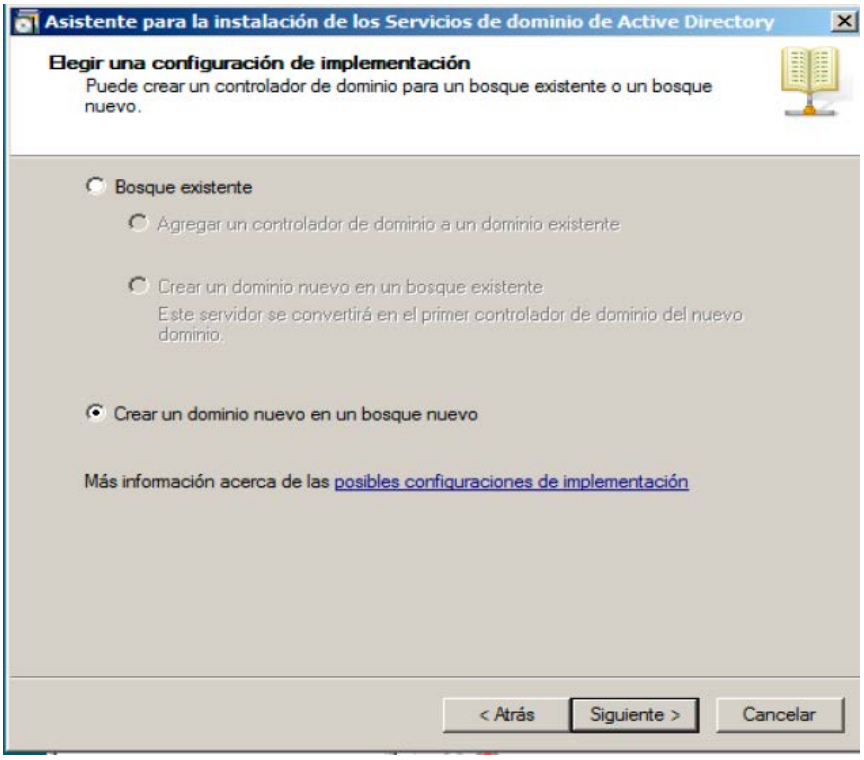

Figura 3-30: Creación de un nuevo bosque

Tras introducir el nombre FQDN del domino, seleccionar el nivel funcional del bosque (*Windows Server 2008* en este caso), indicarle al asistente el lugar dónde se desean guardar los archivos de base de datos y configurar la contraseña de recuperación del dominio; el asistente muestra un resumen de las acciones que va a llevar a cabo. Una de ellas es instalar el rol de servidor DNS, ya que es un requisito que la máquina administradora del bosque sea un servidor DNS.

Cuando finaliza la instalación es necesario reiniciar la máquina virtual. El próximo inicio de sesión ya será dentro del dominio configurado.

La configuración del servidor DNS se hace desde el panel de administración del servidor. Habrá aparecido el rol de servidor DNS, que podemos administrar.

El primer paso es crear las zonas de búsqueda. Para ello nos desplazamos en el árbol hasta los registros globales y añadimos una nueva zona de búsqueda directa, y posteriormente inversa. El proceso se realiza con un asistente (véase Figura 3-31). Las zonas se configurarán como principales, ya que no disponemos de otro servidor DNS en el dominio, además, las actualizaciones deberán ser seguras. Al crear la zona de búsqueda inversa, el identificador de red será *192.168.16*, ya que son los tres primeros octetos del segmento de red en el que se encuentra la DMZ.

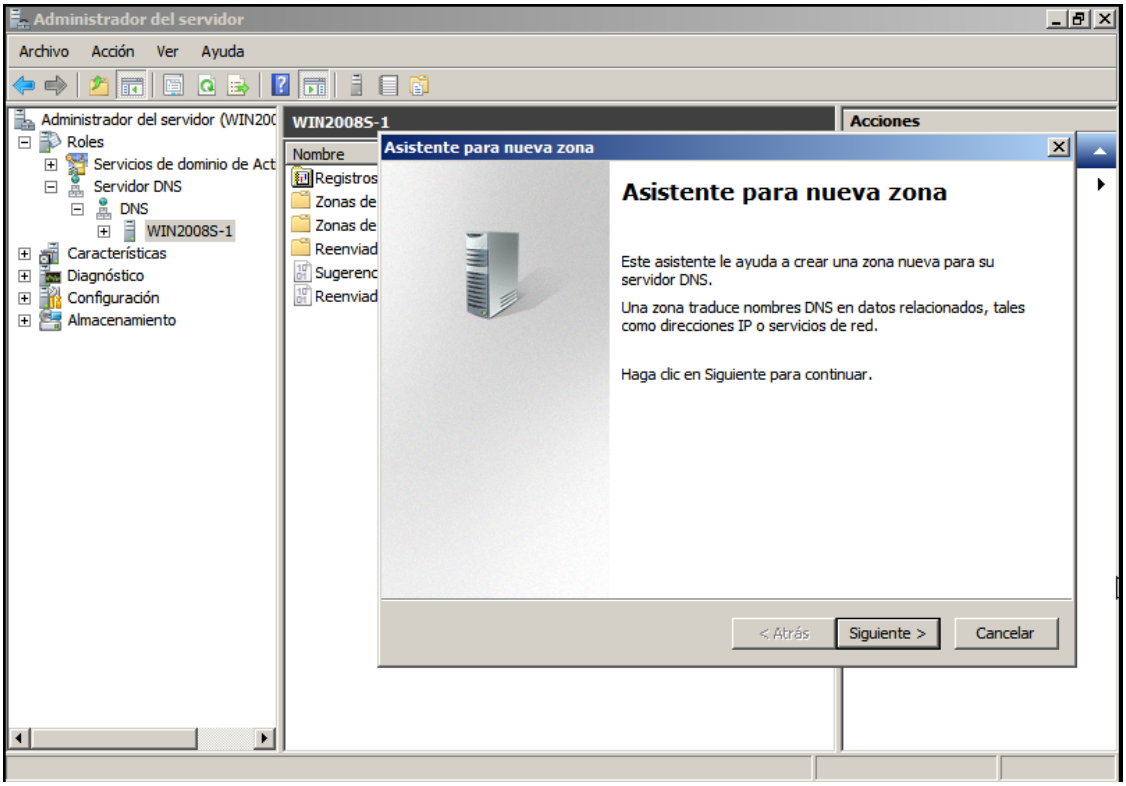

Figura 3-31: Asistente para nueva zona de búsqueda

Una vez creadas las zonas de búsqueda directa e inversa, es el momento de añadir los registros que declaran los servicios existentes en la topología de red. Los diferentes tipos de registros a añadir son:

- HOST: Asigna un nombre a una dirección IP.
- CNAME: Es un alias, asigna este nombre a un HOST.
- MX: Define un servicio de intercambio de correo, necesario para recibir correos externos en un servidor de correo.

Los registros creados para la topología de red descrita anteriormente han sido los que se muestran en la Tabla 3-3. Para ello se procede como se indica en la Figura 3-32.

Tipo	Dirección	Nombre
HOST	192.168.16.10	Ubuntu-1
HOST	192.168.16.11	Ubuntu-2
HOST	192.168.16.12	Ubuntu-3
HOST	192.168.16.21	Win2008S-2
CNAME	*Ubuntu-1.tfg.dunquerque.cud.uvigo.es*	WWW
CNAME	*Ubuntu-2.tfg.dunquerque.cud.uvigo.es*	FTP
CNAME	*Ubuntu-3.tfg.dunquerque.cud.uvigo.es*	MYSQL
CNAME	*win2008s-2.tfg.dunquerque.cud.uvigo.es*	MAIL
MX	*win2008s-2.tfg.dunquerque.cud.uvigo.es*	

Tabla 3-3: Registros de búsqueda de DNS

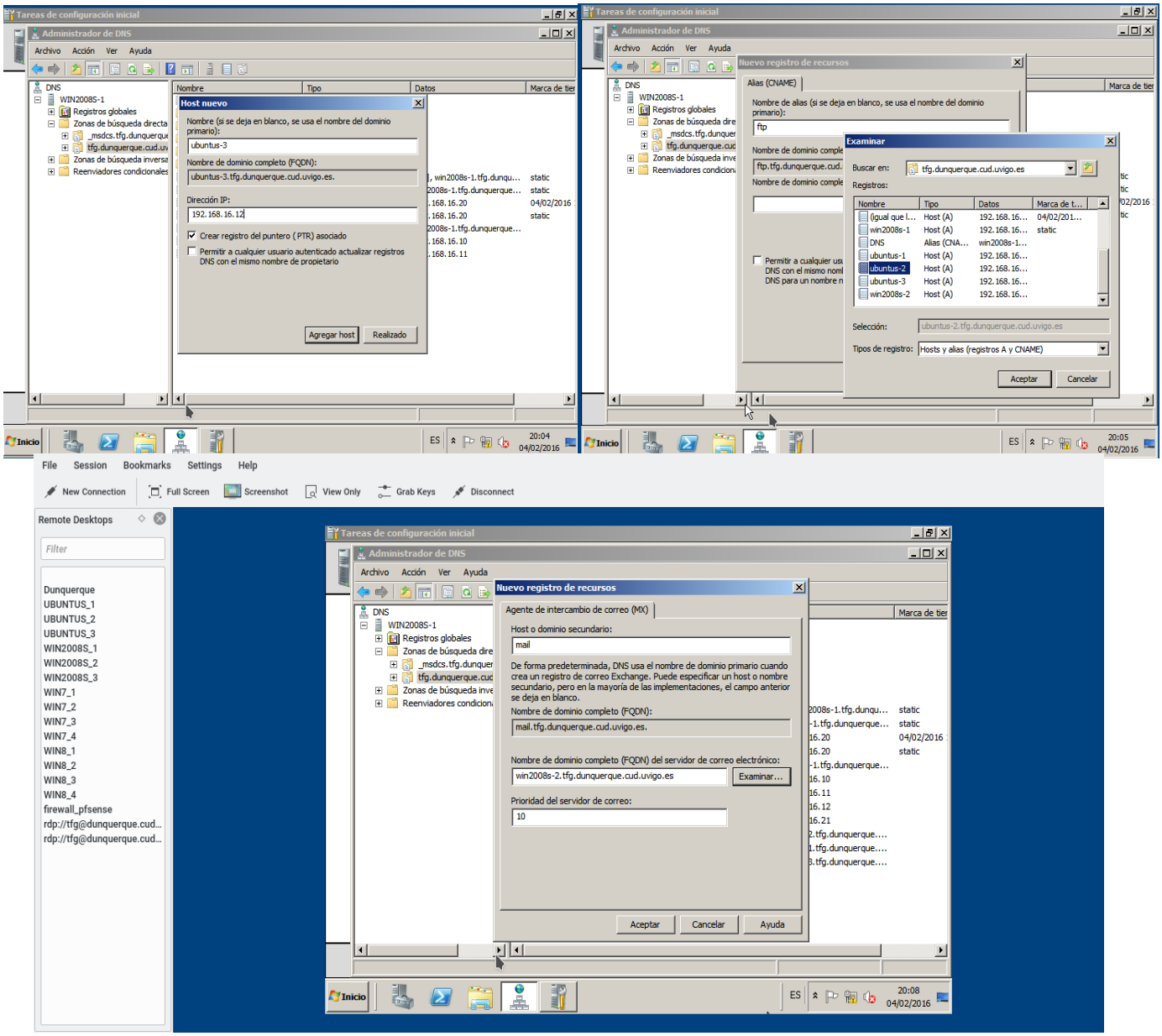

Figura 3-32: Creación de diferentes tipos de registro DNS

Una vez que el servidor DNS se encuentra configurado y en funcionamiento, es necesario modificar la configuracion IP del mismo, para indicar que el servidor DNS principal es él mismo (ver Figura 3-33). El DNS configurado como secundario será el que resuelva los nombres que no se puedan encontrar en los registros locales.

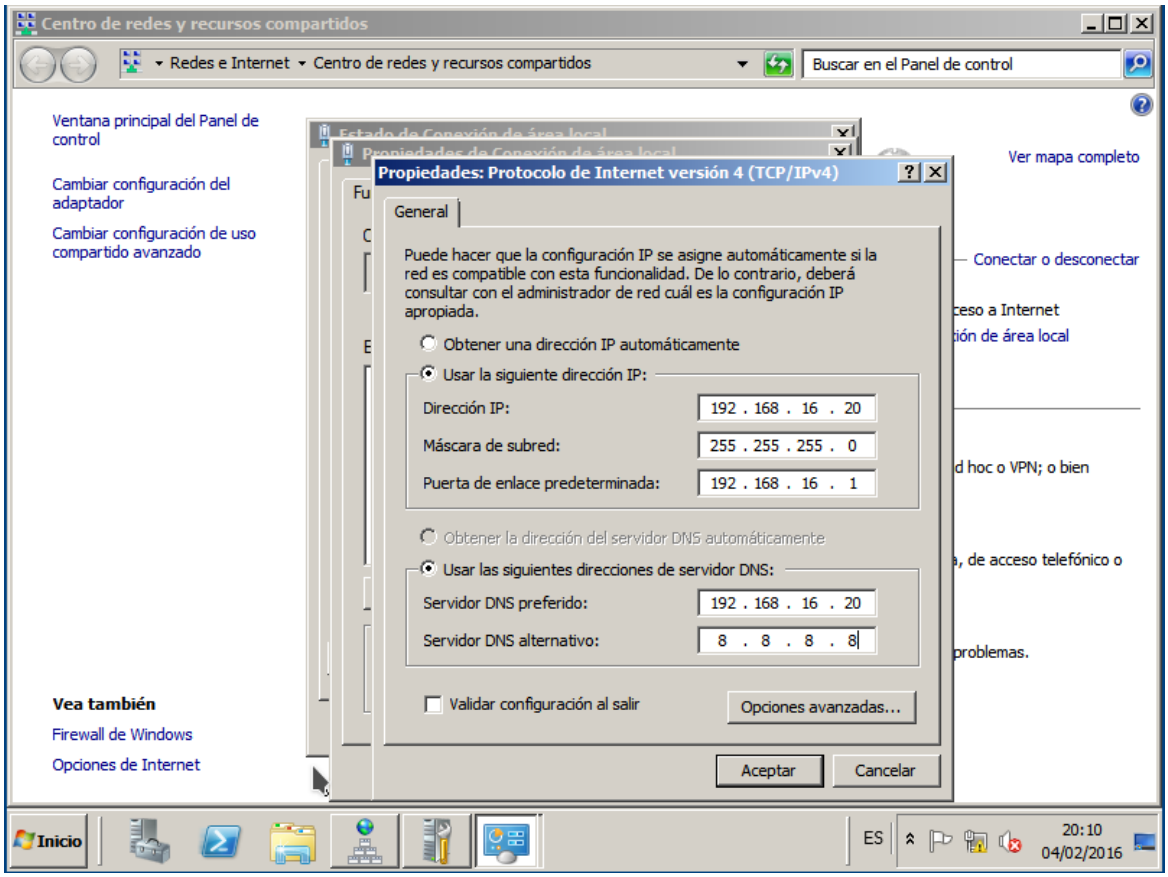

Figura 3-33: Actualización de la configuración IP

Se puede comprobar el funcionamiento del servidor DNS con el comando *nslookup* desde el mismo servidor DNS o desde alguno de los equipos conectados a la red.

3.3.4.2 Servidor de base de datos (MySQL)

En este apartado se va a explicar el procedimiento de instalación de un servidor de bases de datos. En este caso, el motor de bases de datos elegido es *MySQL* y será instalado sobre *Ubuntu server 14.04 LTS* en la máquina virtual SERVER_UBUNTUS_3

El servidor de bases de datos *MySQL* se distribuye como un paquete para la mayoría de los sistemas operativos *Linux*. Para instalarlo, basta con ejecutar como administrador el comando:

```
$ apt-get install mysql-server
```

Una vez finalizada la instalación, para permitir conexiones entrantes al servidor, es necesario modificar el archivo *my.cnf* que se encuentra en */etc/mysql/my.cnf*. En este archivo, que se puede editar con cualquier editor de texto, es necesario eliminar la marca de comentario de la línea *bind_address* y colocar la IP en la cual el servidor *MySQL* estará escuchando, tal y como se puede ver en la Figura 3-34.

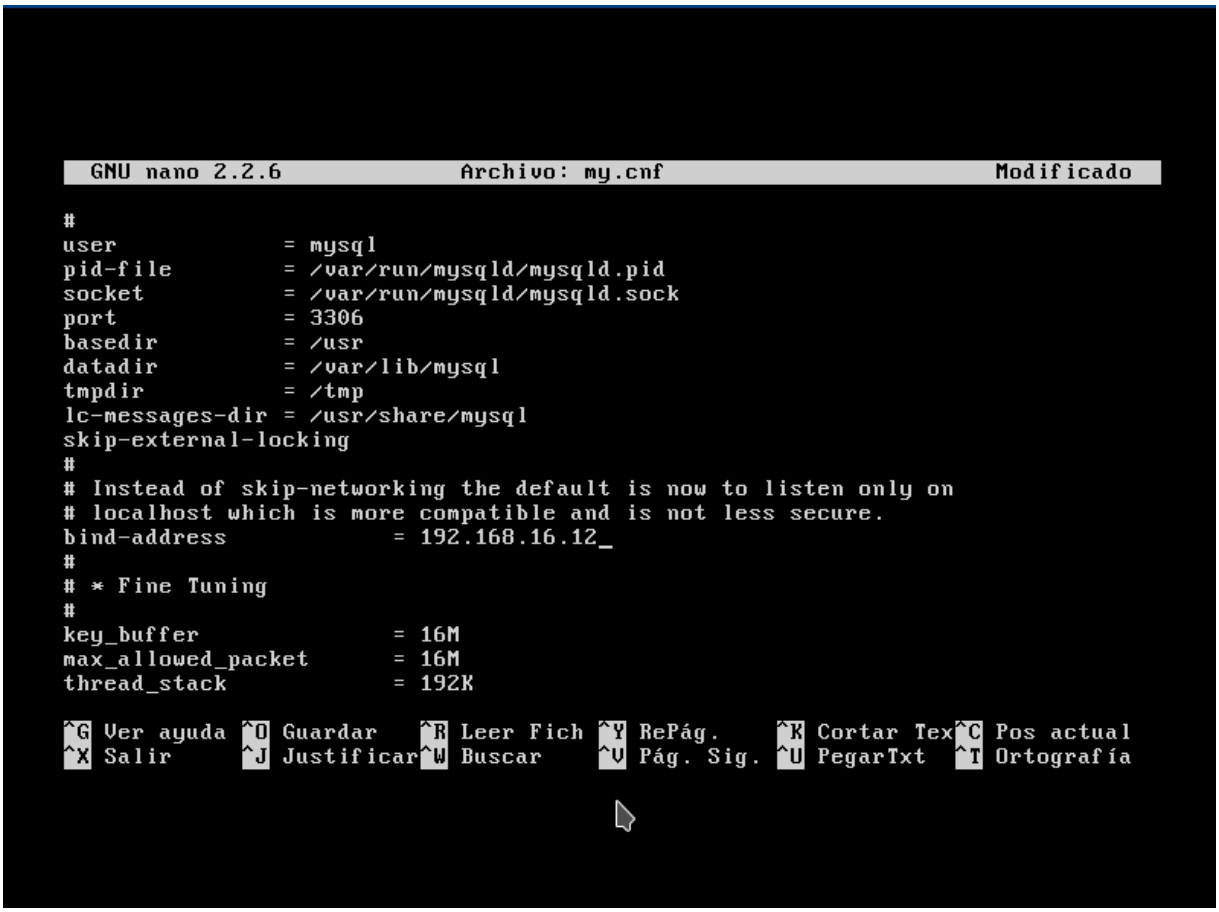

Figura 3-34: Edición de *my.cnf*

Tras reiniciar el servidor, se aplica la nueva configuración y el servidor se encuentra preparado para recibir conexiones en el puerto 3306. La contraseña del usuario administrador del servidor, *root*, se estableció antes de completar la instalación. Es la contraseña que se usará para gestionar las bases de datos y los demás usuarios (ver Figura 3-35).

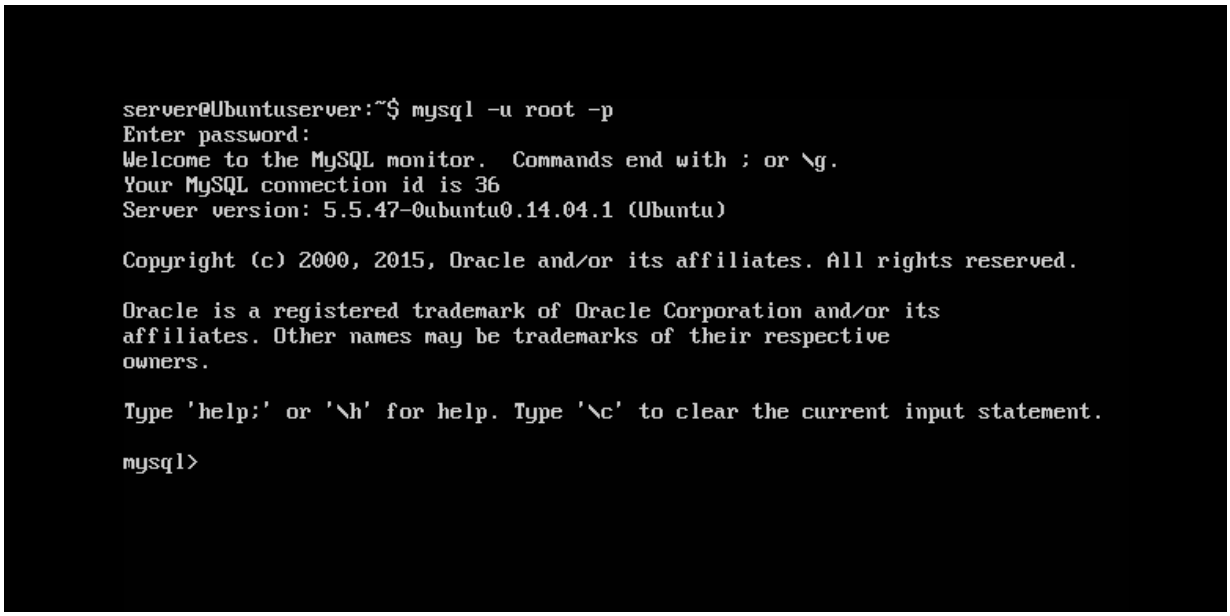

Figura 3-35: Usuario root autenticado en servidor *MySQL*

3.3.4.3 Servidor web (*Apache*)

El servidor web cumple la función de alojar las páginas web y servirlas a los clientes que se conecten al mismo desde Internet o desde la red local.

En nuestro caso, se ha elegido *Apache* como servidor web. Este servidor se instalará sobre *Ubuntu server 14.04 LTS* en la máquina virtual SERVER_UBUNTUS_1. Sobre él se configurarán posteriormente los siguientes sitios web:

- Gestor de contenidos (CMS). En concreto, el portal *Joomla.*
- Cliente gestor de bases de datos *phpmyadmin.*
- Cliente de correo electrónico web (*webmail*) *Rainloop.*

Estos servicios utilizan el lenguaje de programación PHP, con lo cual es necesario instalar también los paquetes que implementan el soporte de este lenguaje en *Apache.*

Al igual que ocurría con el servidor de bases de datos, *Apache* se distribuye en forma de paquete para el sistema operativo que se va a utilizar, por lo que para instalarlo basta con ejecutar como administrador el comando

```
$ apt-get install apache2
```

Una vez finalizada la instalación el servidor web, se inicia automáticamente y comienza a escuchar en el puerto por defecto de HTTP, el puerto 80. Además, accediendo a la dirección IP de esta máquina, o a la dirección *www.tfg.dunquerque.cud.uvigo.es* desde el navegador de cualquier equipo conectado a la red, se presenta la página de prueba de *Apache*, que demuestra que el servidor funciona correctamente, como se observa en la Figura3-36.

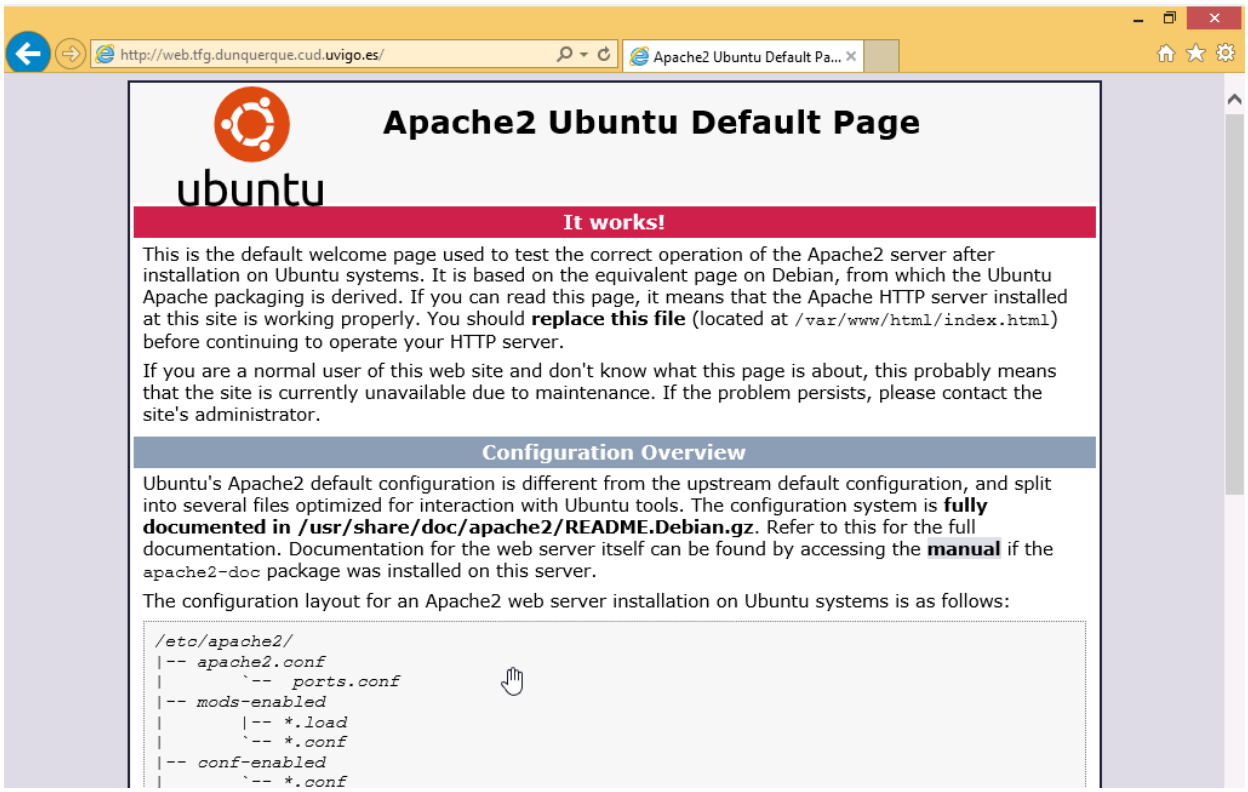

Figura3-36: Página de prueba de *Apache*, vista desde la MV USER_WIN8.1_1

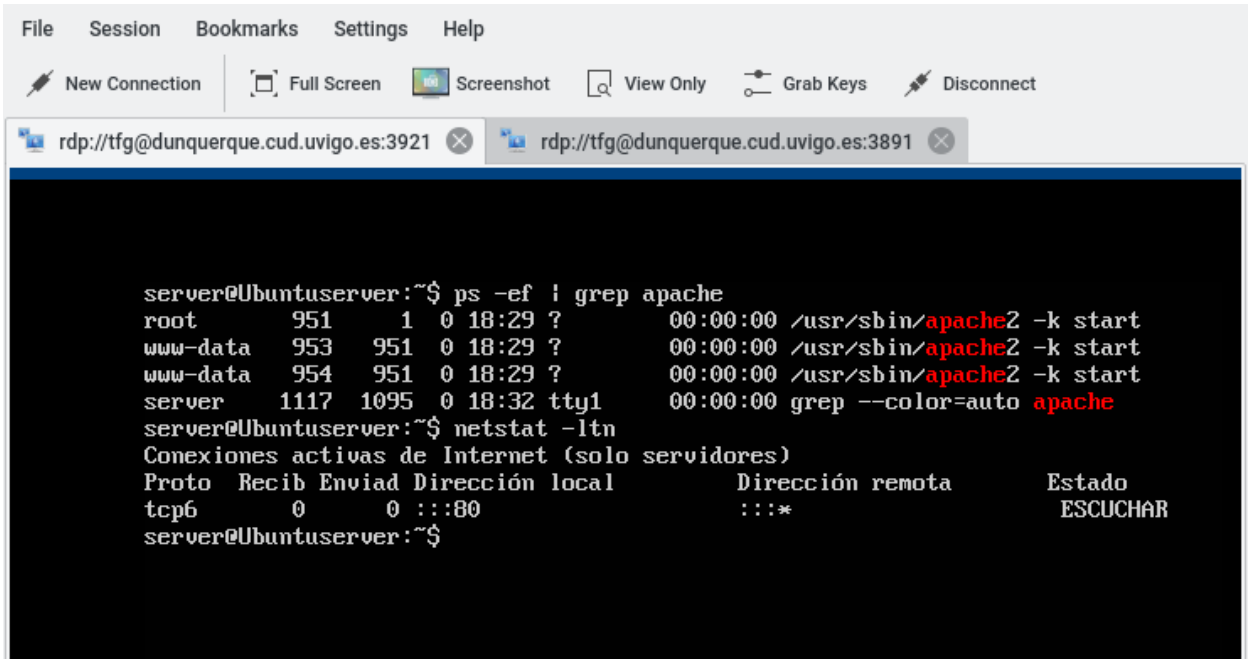

Figura 3-37: Servidor *Apache* ejecutándose y escuchado en el puerto 80

Una vez el servidor *Apache* está en funcionamiento, comprobado como se muestra en la Figura 3-37, se instalan las librerías de PHP. PHP es un lenguaje de programacion que permite crear páginas web con contenido dinámico y dispone de numerosas librerías.

La instalación de estas librerías también se realiza mediante la herramienta de gestión de paquetes *apt-get*. Se instalan en dos pasos, en primer lugar, el lenguaje de programacion y, posteriormente, las librerías requeridas:

```
$ apt-get install libapache2-mod-php5 php5 php5-mcrypt

$ apt-get install php5-mysql php5-curl php5-gd php5-idn php-pear php5-imagick php5-imap php5-mcrypt php5-memcache php5-ming php5-ps php5-pspell php5-recode php5-snmp php5-sqlite php5-tidy php5-xmlrpc php5-xsl
```

En este momento es necesario reiniciar el servidor *Apache* para que funcione con soporte para PHP

3.3.4.3.1 phpmyadmin

El primero de los sitios web a instalar sobre el servidor *Apache* es *phpmyadmin*, una aplicación programada en PHP que permite gestionar la base de datos *MySQL* desde un navegador web.

Se instala con el comando *apt-get install phpmyadmin* y el instalador es un asistente textual en el que el primer paso consiste en seleccionar el servidor de páginas web que vamos a usar, en nuestro caso, *Apache2* (ver Figura 3-38).

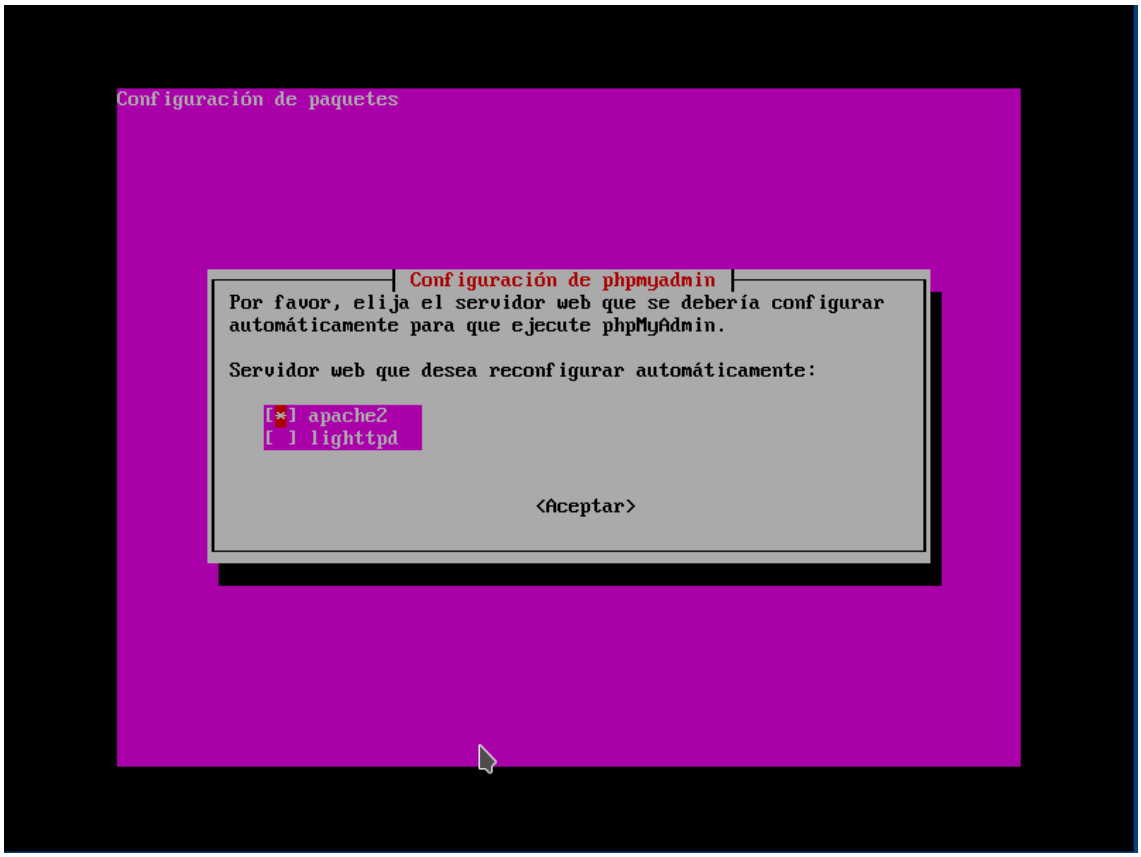

Figura 3-38: Instalador de *phpmyadmin*

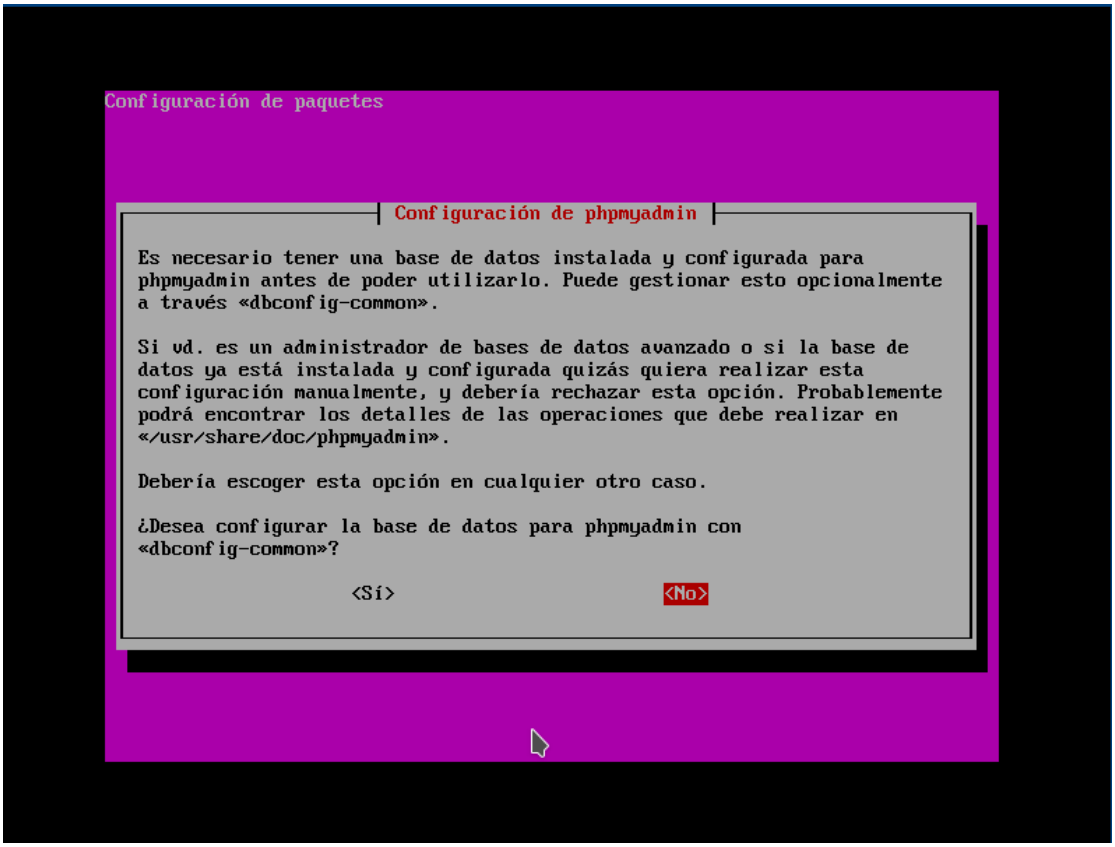

Figura 3-39: Asistente de instalación de *phpmyadmin*

Como se puede ver en la Figura 3-39, el instalador nos ofrece configurar automáticamente la base de datos a usar por *phpmyadmin.* Sin embargo, en esta ocasión deberemos rechazar la ayuda del asistente, ya que está configurado para conectarse con una base de datos en el mismo equipo que el servidor web en lugar de para conectarse con un servidor *MySQL* externo, como es nuestro caso.

Para configurar *phpmyadmin* de forma que utilice una base de datos en un servidor que no sea el local, editaremos el archivo */etc/dbconfig-common/phpmyadmin.conf* con los datos relativos a nuestro servidor *MySQL*, como se puede ver en la Figura 3-40.

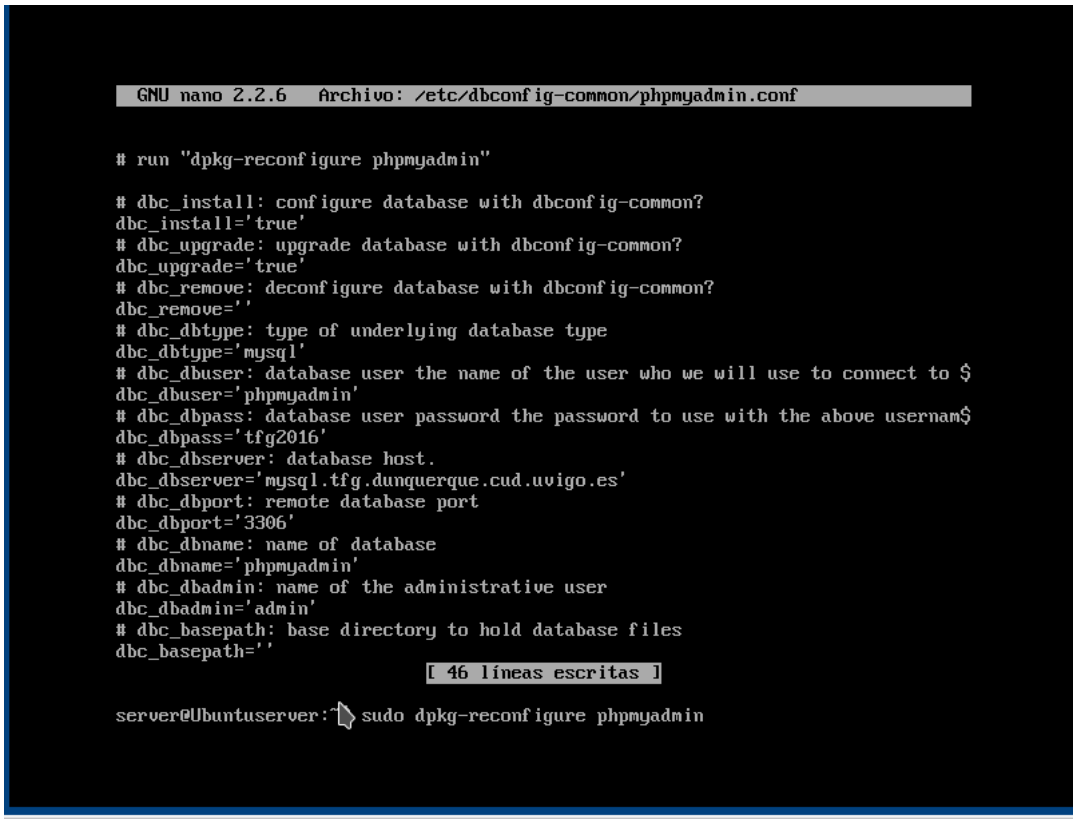

Figura 3-40: Archivo *phpmyadmin.conf*

Una vez se ha actualizado el archivo *phpmyadmin.conf* con los datos relativos al servidor de bases de datos *MySQL* que va a gestionar el programa, se ejecuta el configurador con el comando *dkpg-reconfigure phpmyadmin.*(ver Figura 3-41)

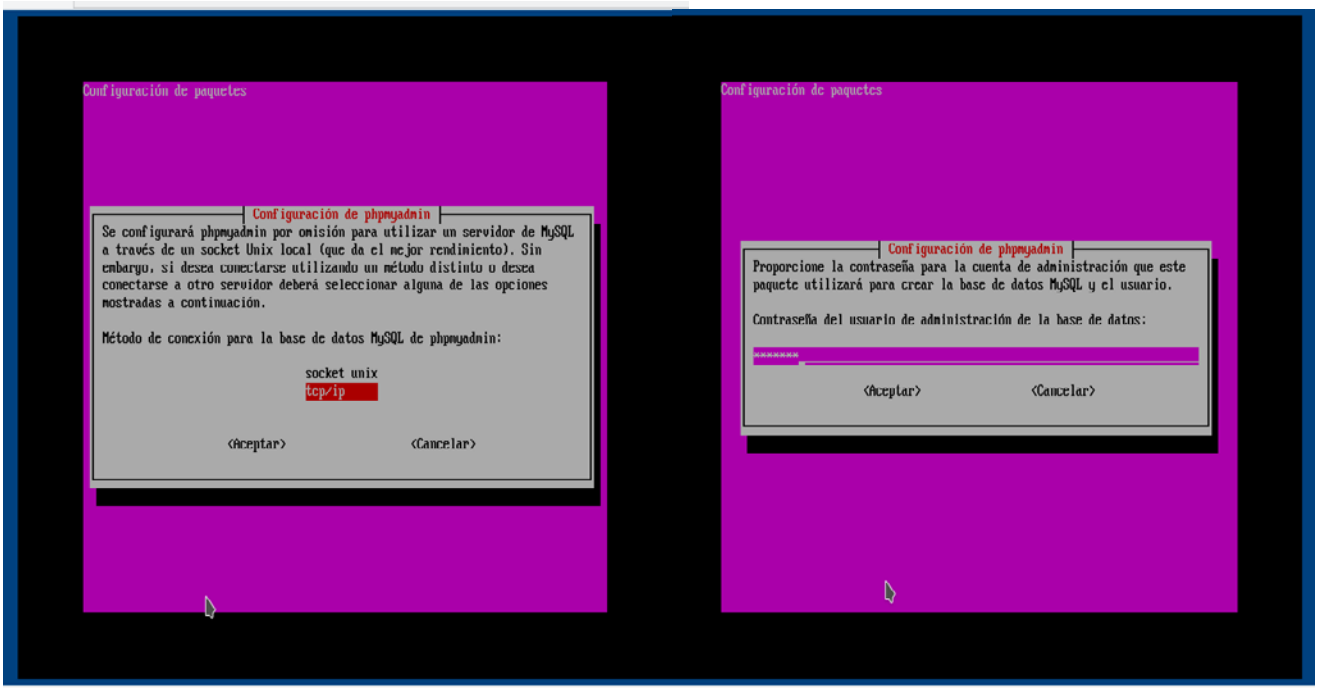

Figura 3-41: Configurador de base de datos *phpmyadmin*

El asistente de configuración en este momento pedirá alguna información relativa al servidor de bases de datos (el tipo de conexión a realizar, la contraseña del usuario de administración de la base de datos, etc).

Para finalizar el asistente, elegiremos la opción de “Instalar la versión del responsable del paquete” (como se muestra en la Figura 3-42) para que el instalador sobrescriba el archivo de configuración anterior.

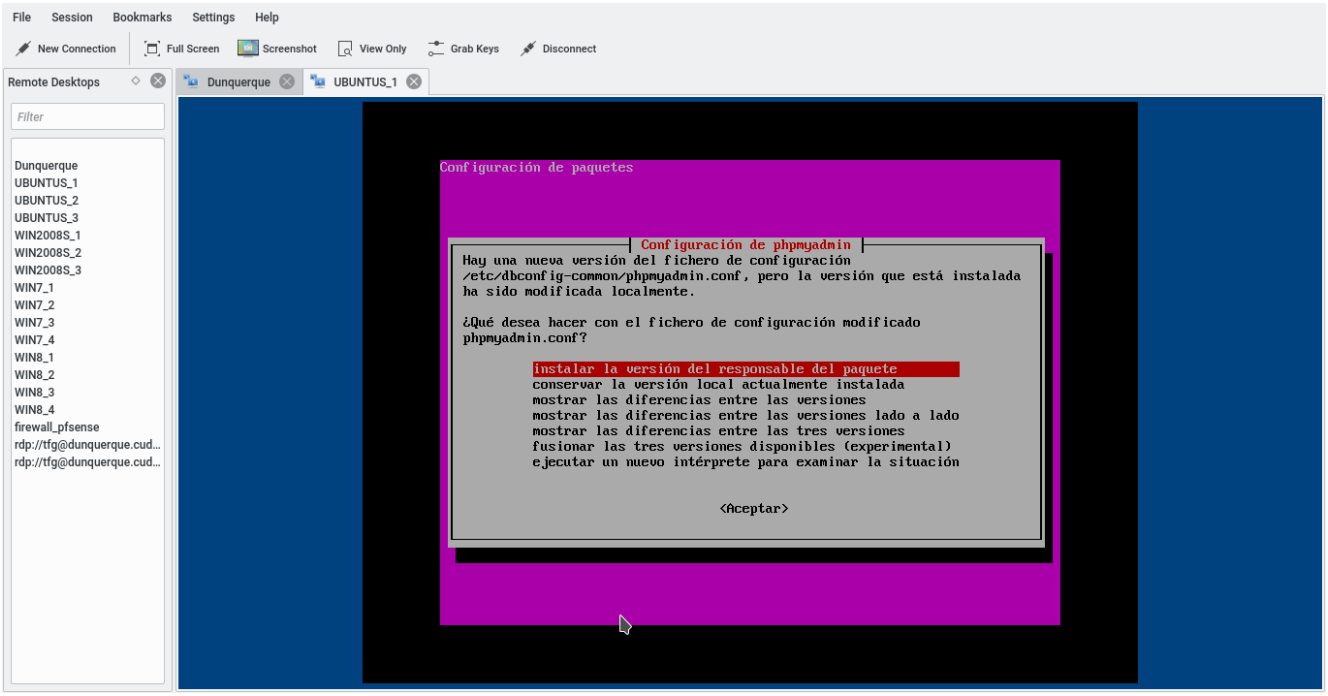

Figura 3-42: Configurador de base de datos de *phpmyadmin*

Para activar el acceso a *phpmyadmin*, el servidor web tiene que cargarlo como una de las páginas web publicadas por él. Para que *Apache* reconozca de esta forma a *phpmyadmin*, se edita el archivo */etc/apache2/httpd.conf* y se le agrega la línea *Include /etc/phpmyadmin/apache.conf* como se indica en la Figura 3-43)

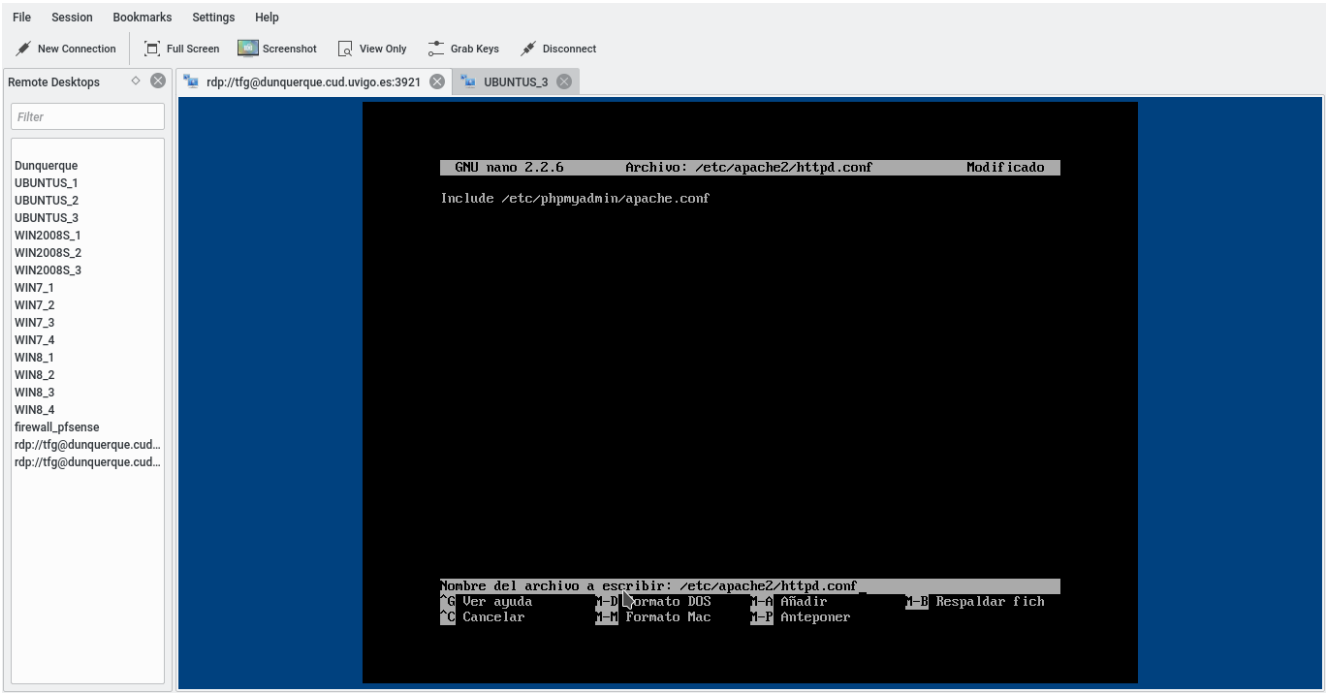

Figura 3-43: Archivo *httpd.conf*

Tras reiniciar el servidor *Apache*, desde cualquier ordenador de la red se puede abrir en el navegador la dirección *https://www.tfg.dunquerque.cud.uvigo.es/phpmyadmin* desde la cual se puede gestionar de manera gráfica el servidor de bases de datos instalado en el apartado 3.3.4.2.

En la Figura 3-44 se puede ver el funcionamiento de esta herramienta, abierta desde uno de los ordenadores en la red LAN. Se observan bases de datos correspondientes a aplicaciones que se detallarán posteriormente.

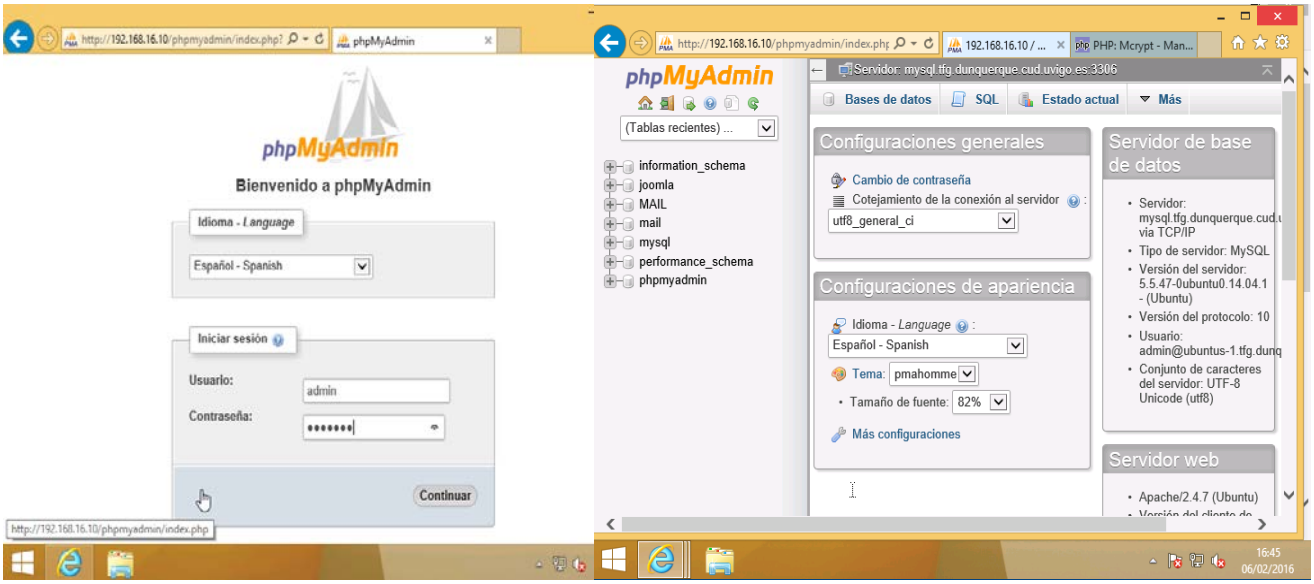

Figura 3-44: *phpmyadmin* desde máquina virtual USER_WIN8.1_1

3.3.4.3.2 Gestor de contenidos Joomla

Un gestor de contenidos es un software que crea un entorno web en el cual el administrador puede crear, organizar y modificar el contenido y el diseño. Es sobre todo aplicable a portales web, donde su utilidad es muy alta, ya que permite la creación de páginas dinámicas fácilmente personalizables y editables.

En este caso se ha elegido *Joomla*, un gestor de contenidos para páginas web programado en PHP y distribuido bajo licencia GNU.

El primer paso para la instalación del gestor de contenidos es la descarga del mismo desde su repositorio oficial. *Joomla* se distribuye en forma de archivo comprimido que deberá ser descomprimido en la raíz del directorio de páginas web de nuestro servidor web. En el caso de *Apache*, este directorio se encuentra en */var/www/html*. Para la descarga, se puede, por ejemplo, utilizar usar el comando *wget*. En la Figura 3-45 se puede ver cómo se descarga y descomprime el paquete de *Joomla*.

Figura 3-45: Descarga del paquete *Joomla*

Al descomprimir el paquete, se establece como propietario de los archivos descomprimidos al usuario que llevó a cabo la descompresión. *Apache*, por seguridad, solo permite acceder a los archivos que tengan permisos para ser gestionados por su usuario *www-data;* por lo tanto, es necesario asignarle de nuevo los permisos y el propietario a los archivos de *Joomla.* Para esto, se utilizan los comandos *chown* y *chmod,* tal como se puede ver en la Figura 3-46.

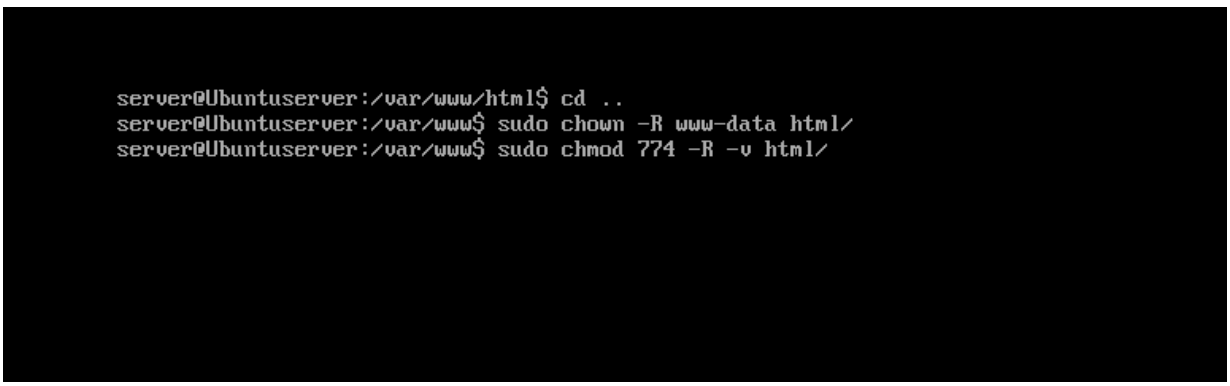

Figura 3-46: Asignación de permisos a archivos de *Joomla*

A partir de este momento, la instalación de *Joomla* continúa en otro ordenador de la red. Para abrir el instalador, basta con acceder a la dirección del servidor *Apache*. Sin embargo, antes de continuar

con la instalación hay que realizar las siguientes operaciones en el servidor de bases de datos, desde *phpmyadmin*:

- Creación de un usuario *joomlacore* con permiso para acceder desde 192.168.16.10, sin privilegios.
- Creación de una base de datos *joomla*
- Asignar todos los privilegios sobre la base de datos *joomla* al usuario *joomlacore*.

Una vez preparada la base de datos, se puede comenzar a rellenar los campos que pide el asistente de instalación de *Joomla*. En el primer paso, se introducirán datos relativos al sitio y su administrador (véase la Figura 3-47).

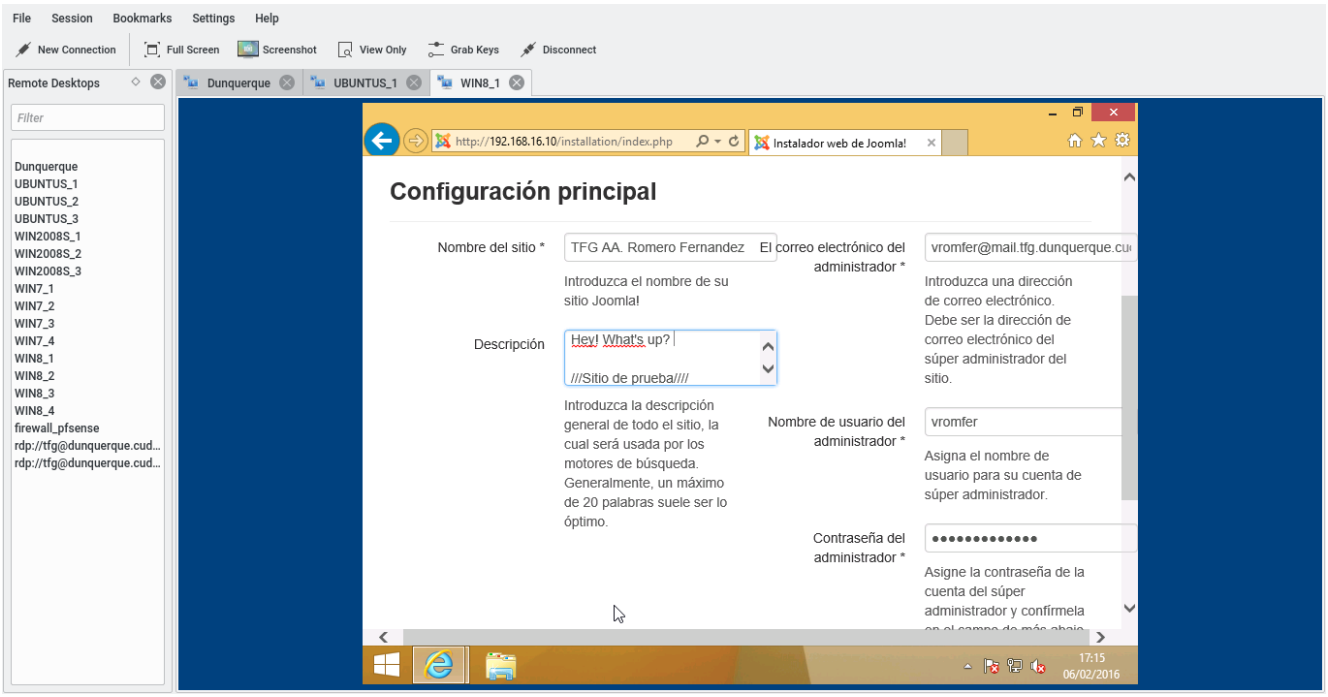

Figura 3-47: Instalador *Joomla* (I)

En el segundo paso se introducen los datos relativos a la base de datos que va a usar el gestor de contenidos para guardar su información (ver Figura 3-47). En este paso se introducen los datos definidos previamente en la base de datos. *Joomla* pedirá que se le asigne un prefijo para sus tablas. Esta opción es importante únicamente en el caso de bases de datos compartidas. Sin embargo, como en nuestro caso *Joomla* dispondrá de una base de datos en exclusiva, el prefijo no tiene importancia.

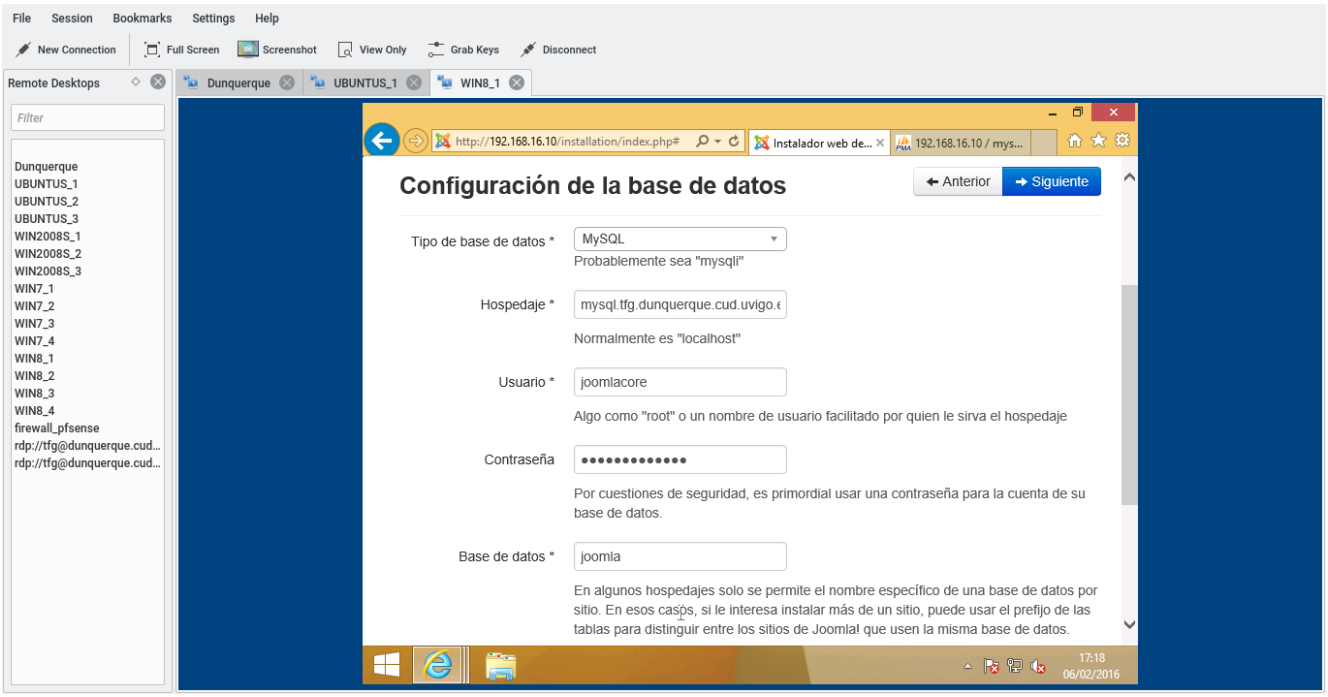

Figura 3-48: Instalador de *Joomla* (II). Base de datos

Con los datos introducidos, antes de completar la instalación se realiza una comprobación de los parámetros del servidor y la base de datos. En el caso de no pasar completamente la comprobación, aparecerían características en rojo, que deberían solventarse antes de la instalación (ver Figura 3-49).

Si todo es correcto, se puede continuar la instalación. *Joomla* ofrece la posibilidad de rellenar el gestor de contenidos con datos de prueba o ejemplo. En un caso real, se declinaría la oferta de rellenar el gestor de contenidos, para posteriormente crear los contenidos deseados por el administrador de páginas web. En este caso, como no se van a crear contenidos reales, se ha pedido al instalador que instale los datos de prueba. Estos datos incluyen un ejemplo de cada uno de los módulos y posibilidades de las que dispone el gestor de contenido en inglés.

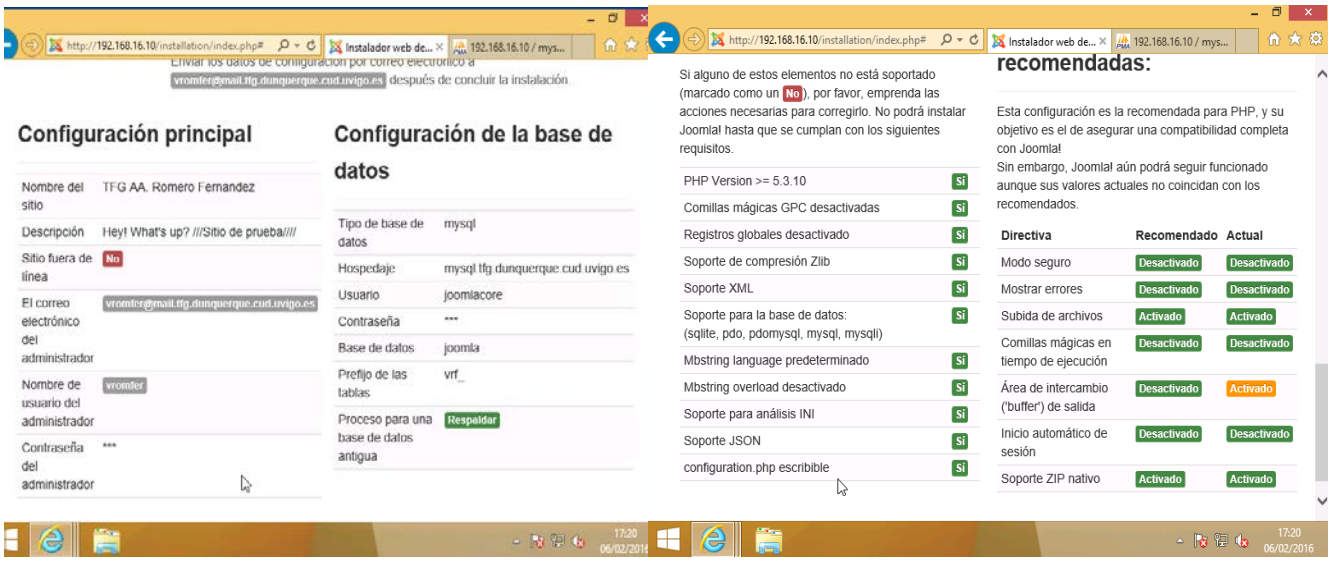

Figura 3-49: Comprobación antes de instalar

Al finalizar la instalación, se pide que eliminemos la carpeta de instalación antes de usar el gestor de contenidos (ver Figura 3-50). Debido a los permisos configurados no se puede hacer desde el

navegador, por lo que ejecutaremos en la máquina que aloja los archivos el comando *rm -R installation/* desde la carpeta */var/www/html* y con privilegios de administrador.

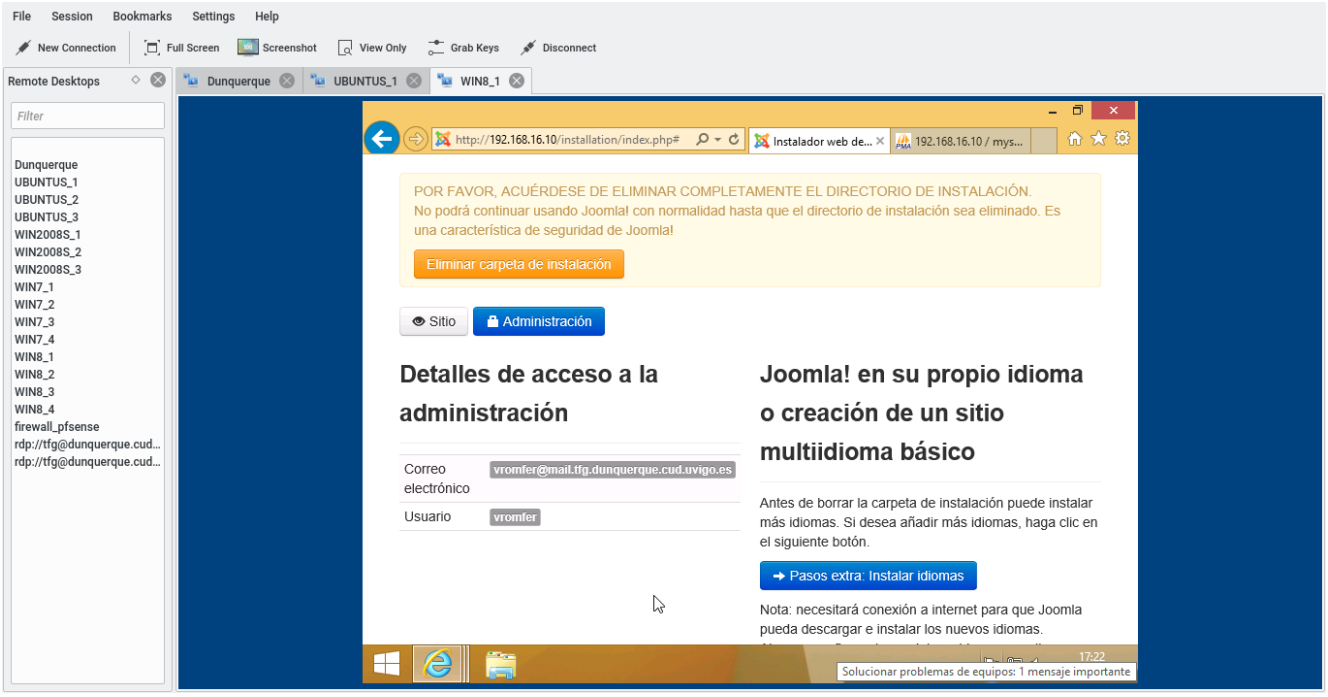

Figura 3-50: Instalación de *Joomla* finalizada

El gestor de contenidos instalado correctamente puede accederse ahora desde cualquier equipo de la red, introduciendo la dirección *www.tfg.dunquerque.cud.uvigo.es* en el navegador. La página principal, con los datos de ejemplo, tiene el aspecto mostrado en la Figura 3-51. En los menús laterales puede accederse a las diferentes funciones y apartados que el gestor de contenidos tiene implementadas.

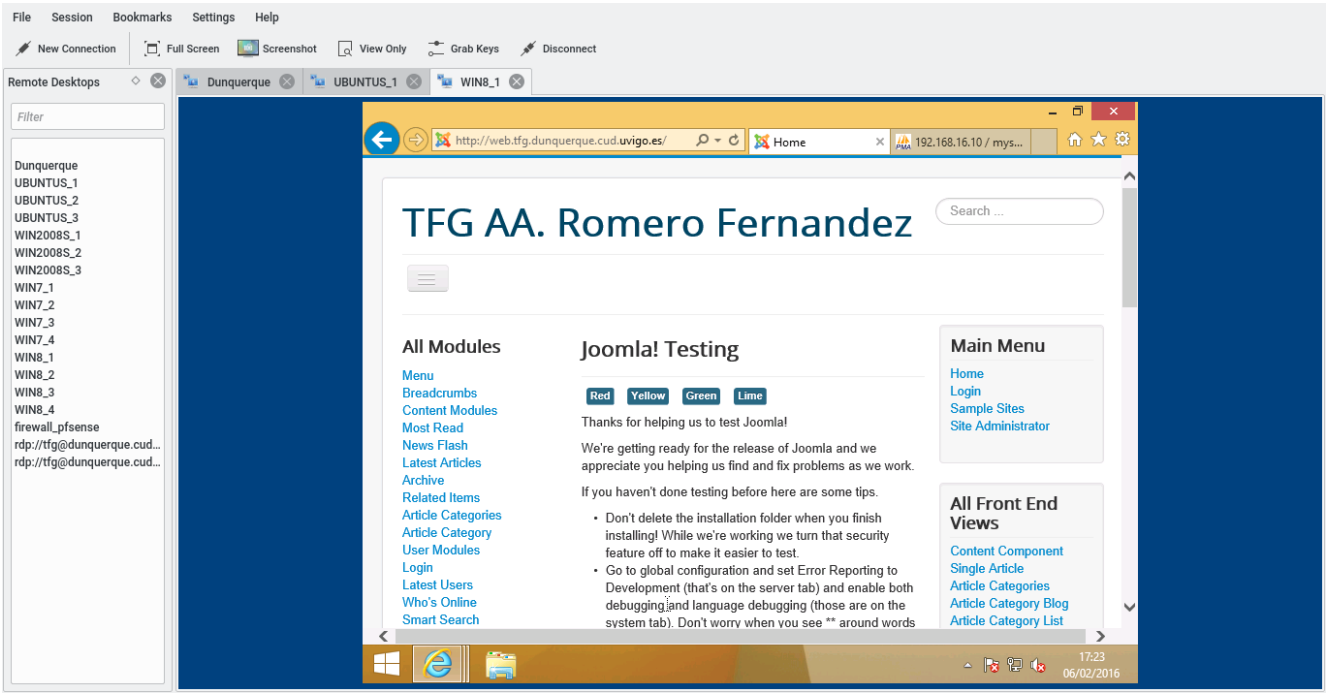

Figura 3-51: Página de inicio de *Joomla*

3.3.4.3.3 Cliente Webmail

El último servicio que se va a instalar sobre el servidor web es un cliente *Webmail*, que permite a los usuarios consultar su correo corporativo desde el propio navegador. Para poner en funcionamiento este servicio es necesario tener instalado un servidor de correo electrónico, que se detalla en el apartado 3.3.4.4 de esta memoria.

Se ha elegido como cliente *webmail* el software *Rainloop*, que se distribuye de manera gratuita para aplicaciones no empresariales.

De manera similar a como se hacía con el gestor de contenidos, es necesario descargar el paquete desde el repositorio oficial y descomprimirlo. En este caso, se ha descomprimido en la ruta */var/www/html/webmail*, para que esté accesible añadiendo el directorio *webmail* a la dirección del servidor web.

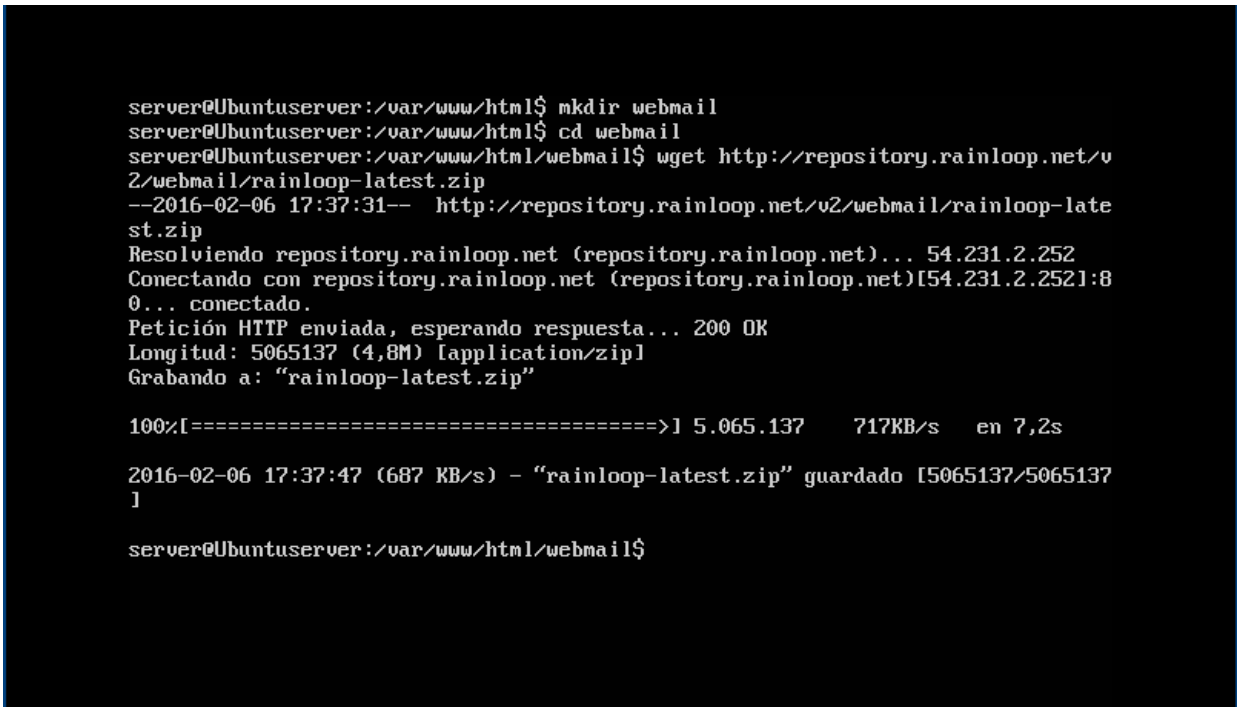

Figura 3-52: Descarga y descompresión de *Rainloop*

Al igual que se hacía con *Joomla*, es necesario ajustar los permisos de los archivos creados. *Rainloop* necesita unos permisos determinados en función de cada archivo, por ello dispone de unos archivos auxiliares que ayudan a la configuración. Para configurar correctamente los permisos de los archivos de *Rainloop*, se ejecutan los siguientes comandos, que buscan los archivos auxiliares y siguen sus instrucciones.

```
$ find . -type f -exec chmod 644 {} \
```

```
$ find . -type d -exec chmod 755 {} \
```

A continuación, se utiliza el comando *chown* para asignar a *www-data* como propietario de los archivos.

La configuración se completa desde otro ordenador de la red. En primer lugar, se crea un usuario y una base de datos en el servidor *Mysql*, usando la herramienta *phpmyadmin* de la misma forma que se hizo antes de la instalación de *Joomla* (ver Figura 3-53).

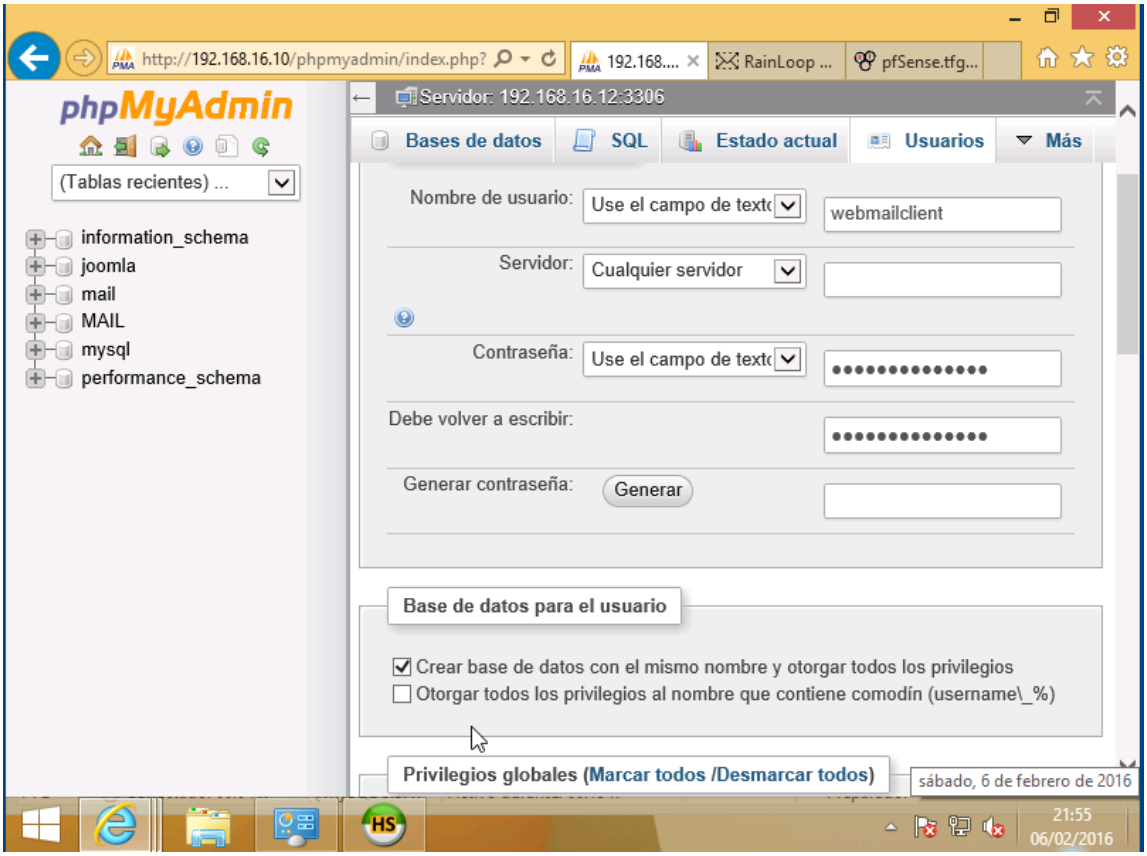

Figura 3-53: Creación de usuario con *phpmyadmin*

Para acceder al panel de administración, se abre la dirección *http://www.tfg.dunquerque.cud.uvigo.es/webmail/?admin y* se usan las credenciales por defecto. (*admin* y *12345)* (ver Figura 3-54), que deberán cambiarse tras acceder la primera vez (como se muestra en la Figura 3-55).

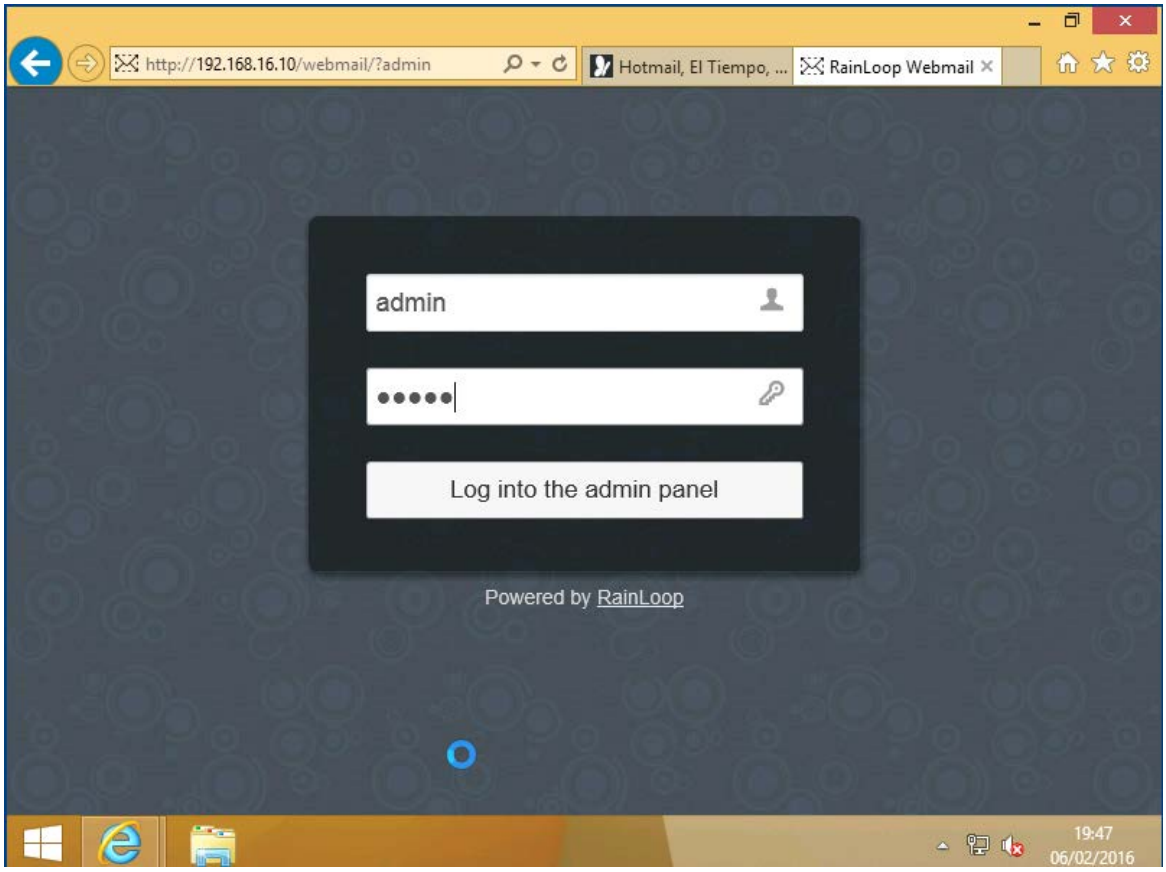

Figura 3-54: Acceso al panel de administración de *Rainloop*

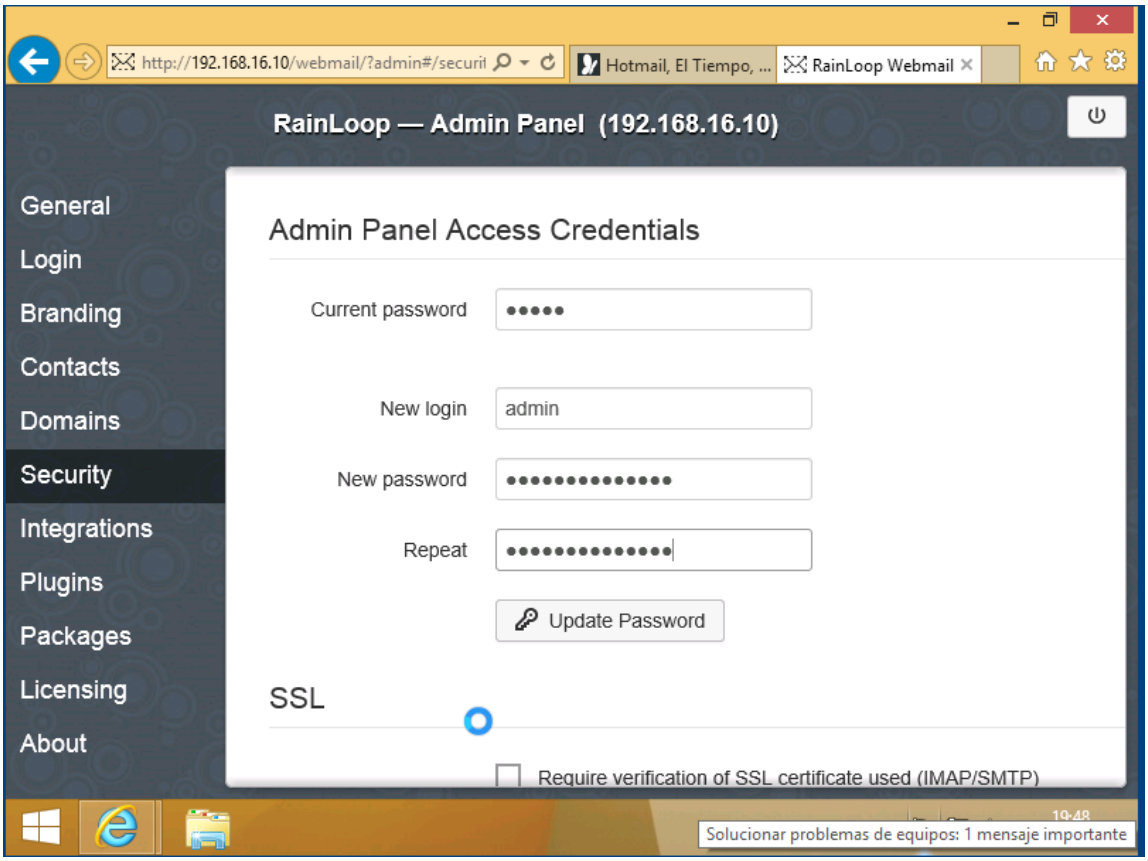

Figura 3-55: Cambio de la contraseña de administrador de *Rainloop*

En la pestaña *Contacts* se configuran los datos de la base de datos que se creó anteriormente. Esta base de datos se utilizará para guardar los contactos de cada uno de los usuarios que utilicen el cliente de correo (ver Figura 3-56).

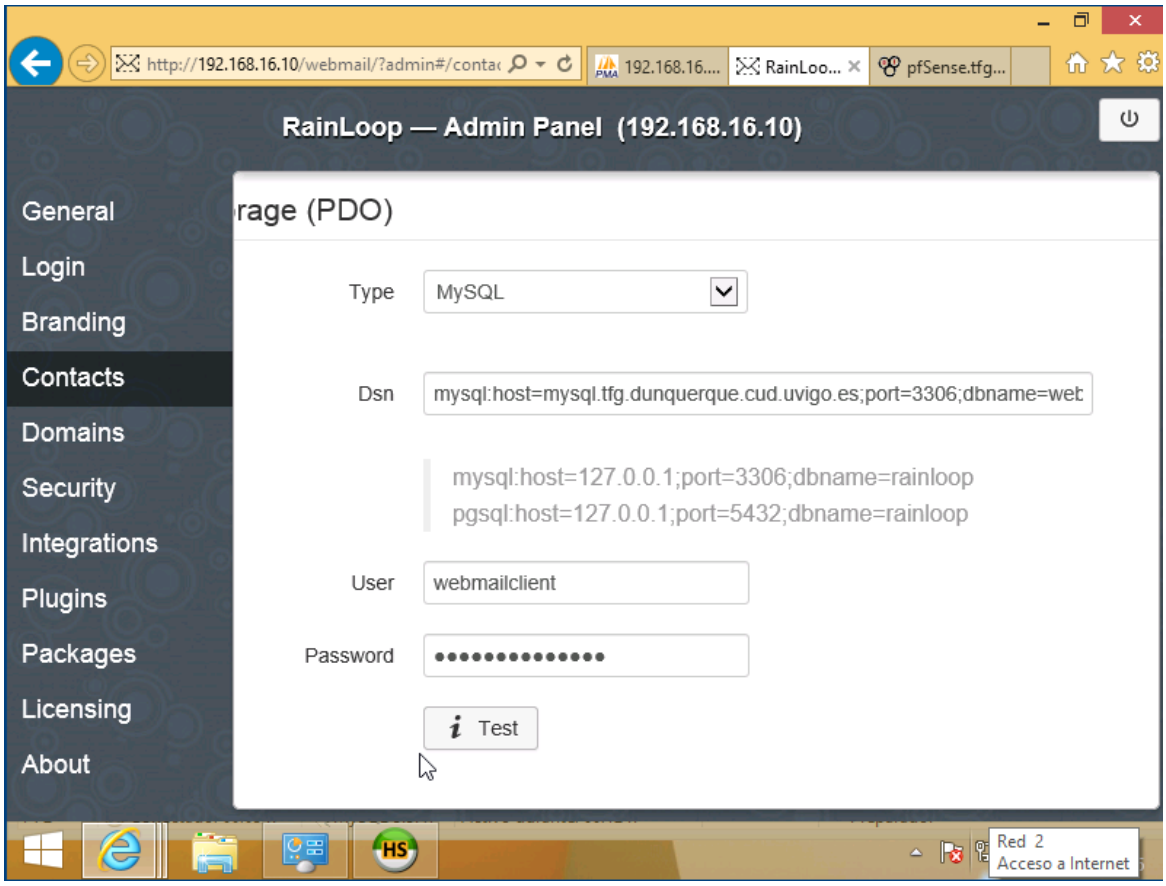

Figura 3-56: Configuración de la base de datos para *Rainloop*.

Por último, se configura en la pestaña *Domains* los datos relativos al servidor de correo electrónico con el que queremos que trabaje el cliente y el nombre del dominio de correo al que pertenece, como se observa en la Figura 3-57. Antes de aceptar esta configuración, el servidor de correo electrónico indicado tiene que estar en funcionamiento.

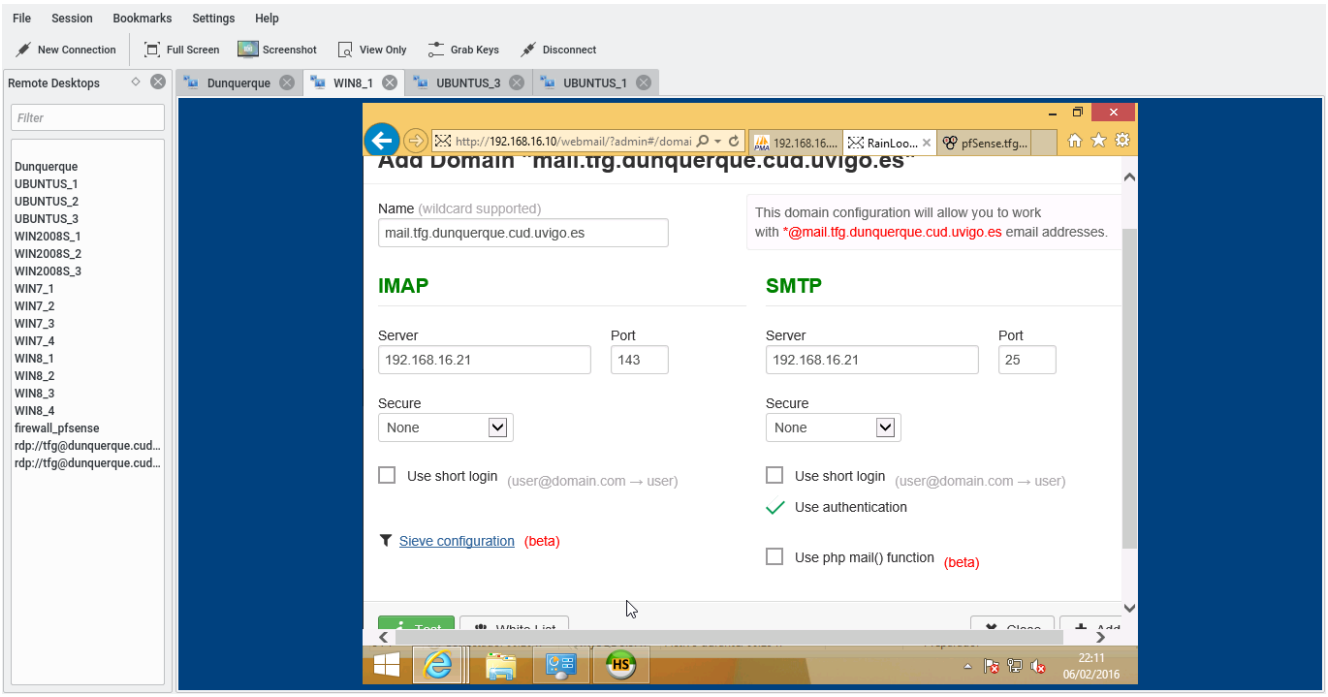

Figura 3-57: Configuración del dominio de correo

3.3.4.4 Servidor de correo electrónico (*hMailserver*).

El servidor de correo electrónico es el software que se encarga de enviar y recibir los correos electrónicos correspondientes a los usuarios del dominio.

En este caso, se ha decidido instalar el servidor de correo *hMailserver* sobre *Windows Server 2008* en la máquina virtual SERVER_WIN2008S_2.

El sistema operativo se ha instalado en la máquina virtual y su configuración de direcciones IP se ha establecido de la siguiente forma:

- IP: 192.168.16.21
- Máscara de subred: 255.255.255.0
- Puerta de enlace: 192.168.16.1
- DNS: 192.168.16.20

Además de la configuración de direcciones IP, la máquina se ha agregado al dominio de *Active Directory* creado con anterioridad y gestionado por la máquina virtual que aloja al servidor DNS (tal y como se puede ver en la Figura 3-58).

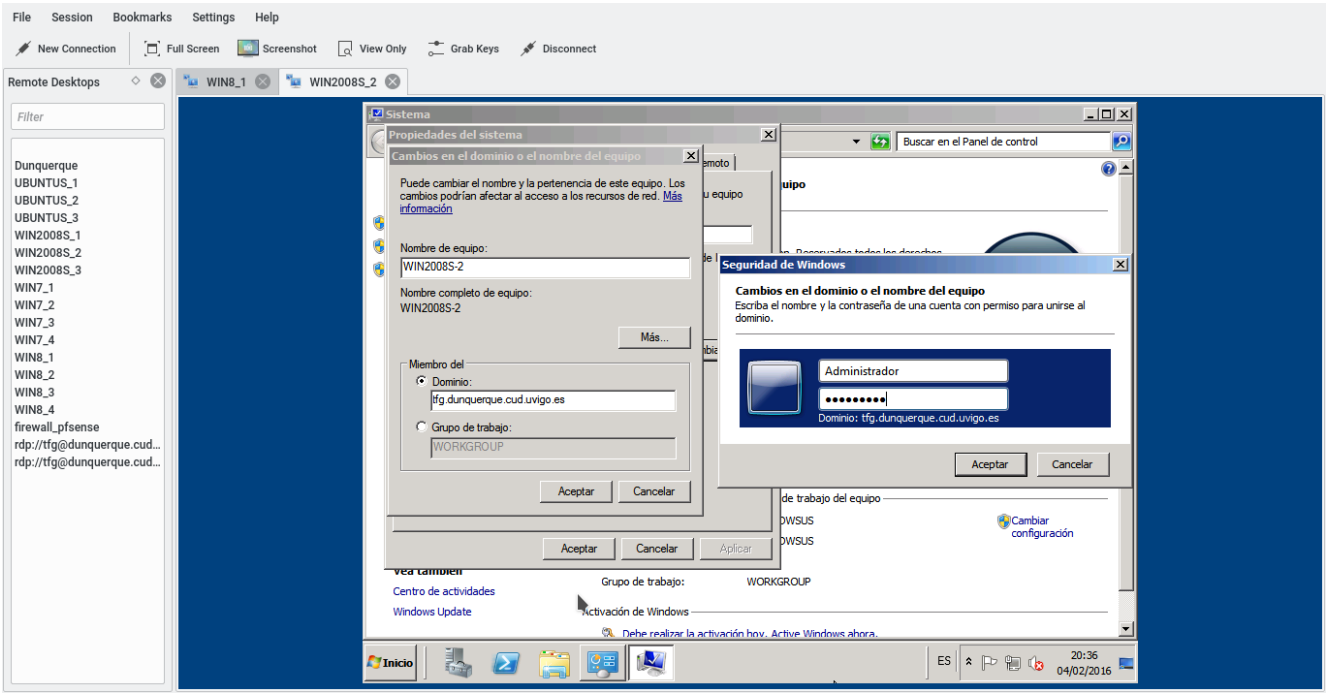

Figura 3-58: Añadir equipo al dominio

El software *hMailserver* puede descargarse desde su página oficial en forma de instalador ejecutable para Windows.

La información del servidor de correo será guardada en una base de datos dentro del servidor *MySQL*. Para ello hay que introducir los datos relativos al mismo en el asistente (ver Figura 3-59 yFigura 3-60)

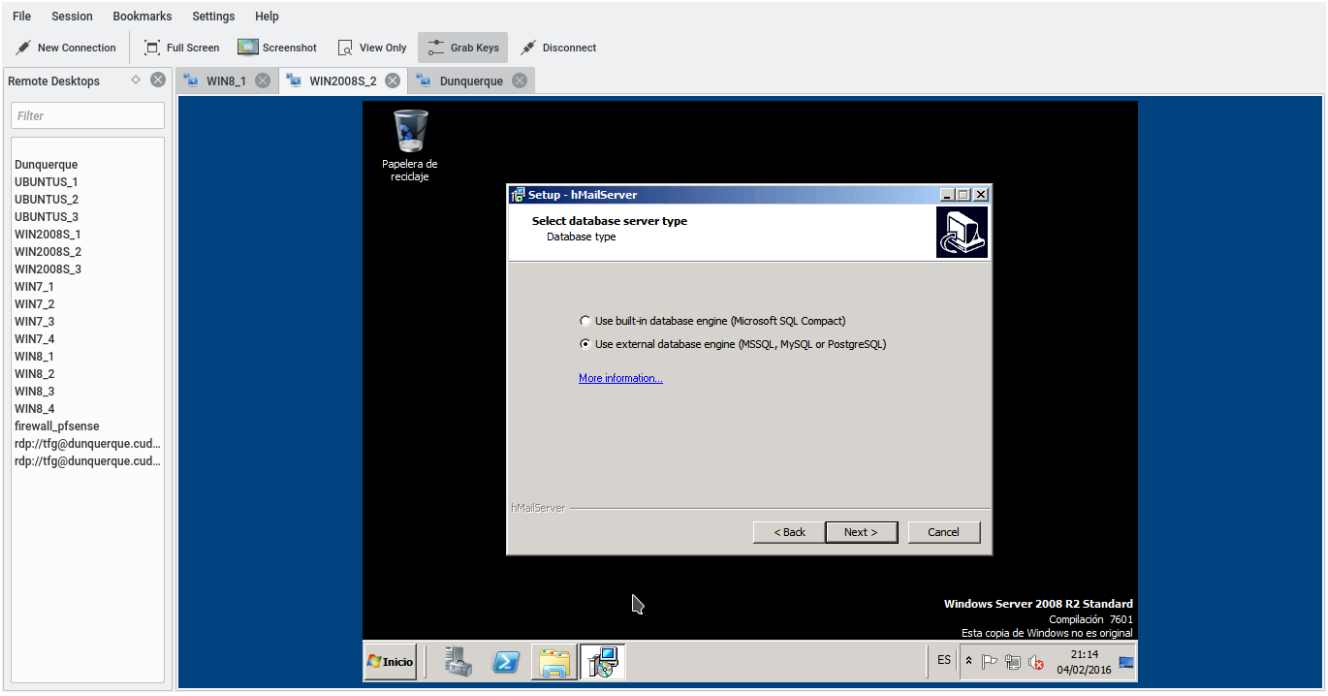

Figura 3-59: Asistente de instalación de *hmailserver*

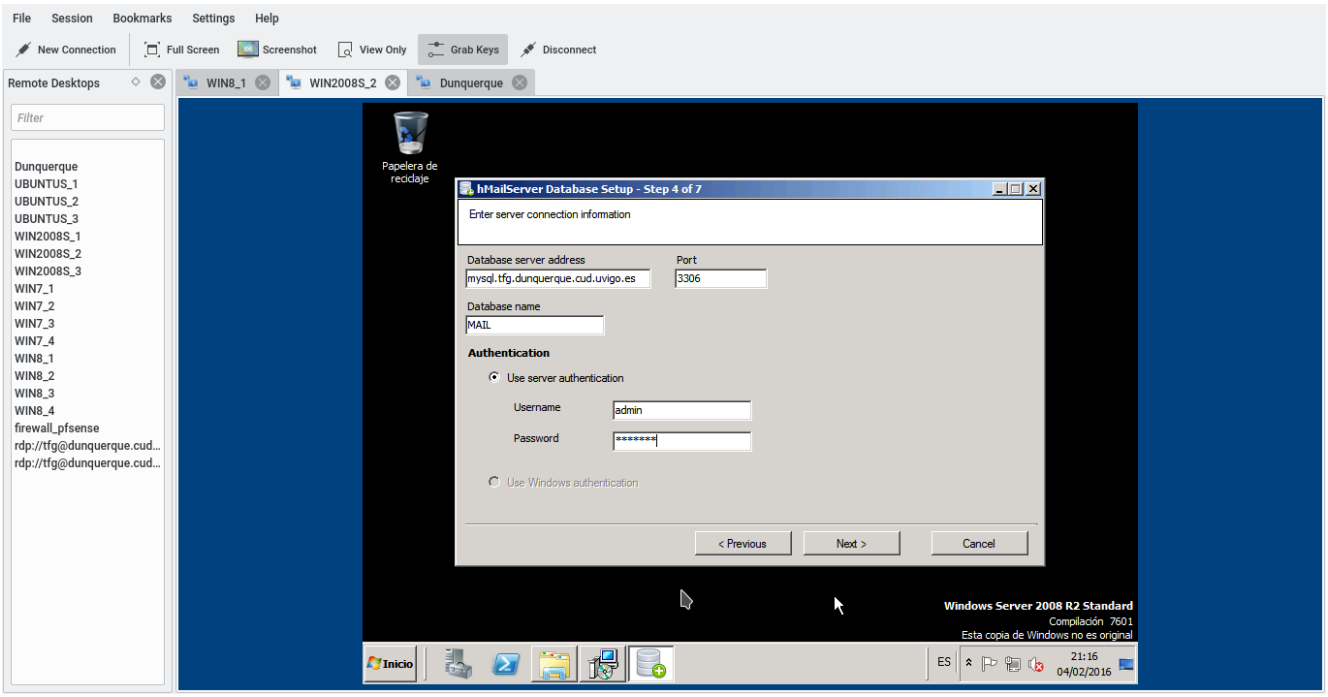

Figura 3-60: Configuración de base de datos

Cuando la instalación finaliza, abrimos el programa de administrador, y el primer paso es configurar un dominio. El dominio configurado será la parte posterior al "@" en la dirección de correo de los usuarios, y para que se puedan recibir mensajes desde el exterior, tiene que estar definido como intercambiador de correo en el DNS, mediante un registro MX.

Como se puede ver en la Figura 3-61, el dominio elegido para las direcciones de correo es *mail.tfg.dunquerque.cud.uvigo.es*. El servidor puede gestionar más de un dominio de correo si se configuran correctamente.

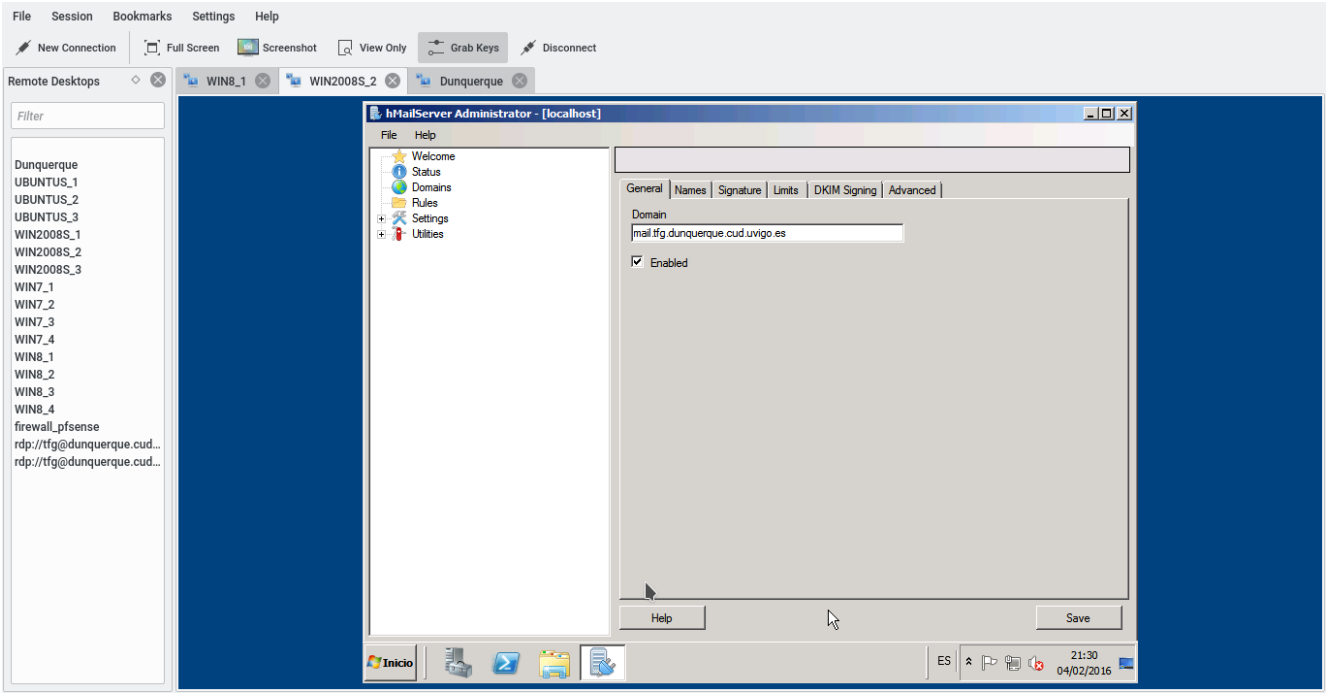

Figura 3-61: Definir dominio de correo

Con el dominio configurado, el siguiente paso es crear las cuentas de usuario que estarán disponibles en el mismo (véase Figura 3-62).

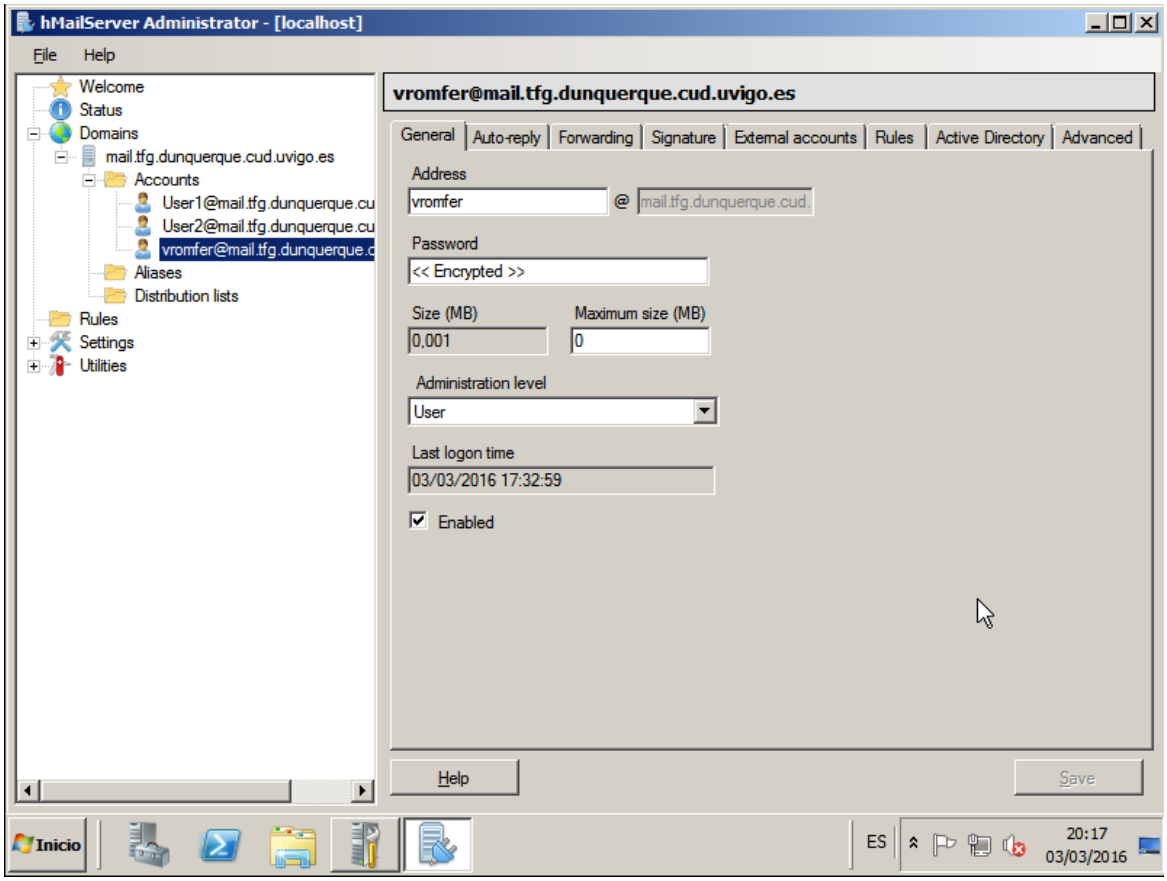

Figura 3-62: Añadir usuarios al dominio de correo

Por último, se activan en el servidor los servicios de SMTP, POP3 e IMAP (ver Figura 3-63) para poder acceder al correo electrónico con los clientes de correo tradicionales. Se van a usar los puertos por defecto de estos servicios y no se configura la conexión segura con cifrado SSL ya que no se dispone de un certificado firmado por una autoridad de certificación. Podría generarse un certificado SSL auto firmado y usarlo, sin embargo, esta opción hará que los clientes de correo muestren advertencias de seguridad e incluso que rechacen la conexión debido a un certificado inválido.

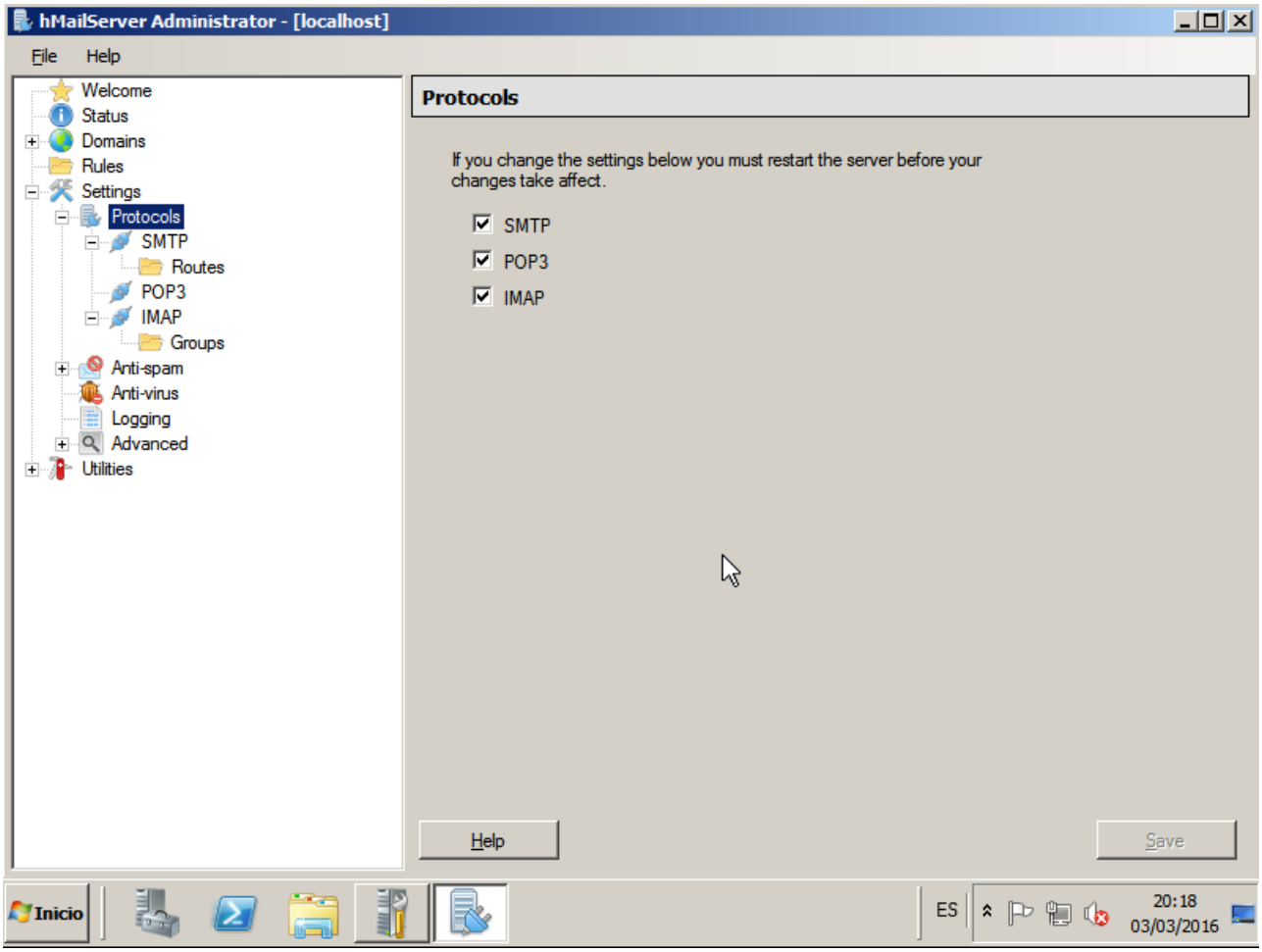

Figura 3-63: Activación de SMTP, POP3 e IMAP

Para comprobar que el servidor funciona correctamente, la opción *Server sendout* nos permite enviar un mensaje a todas las cuentas de correo configuradas (como se indica en la Figura 3-64).

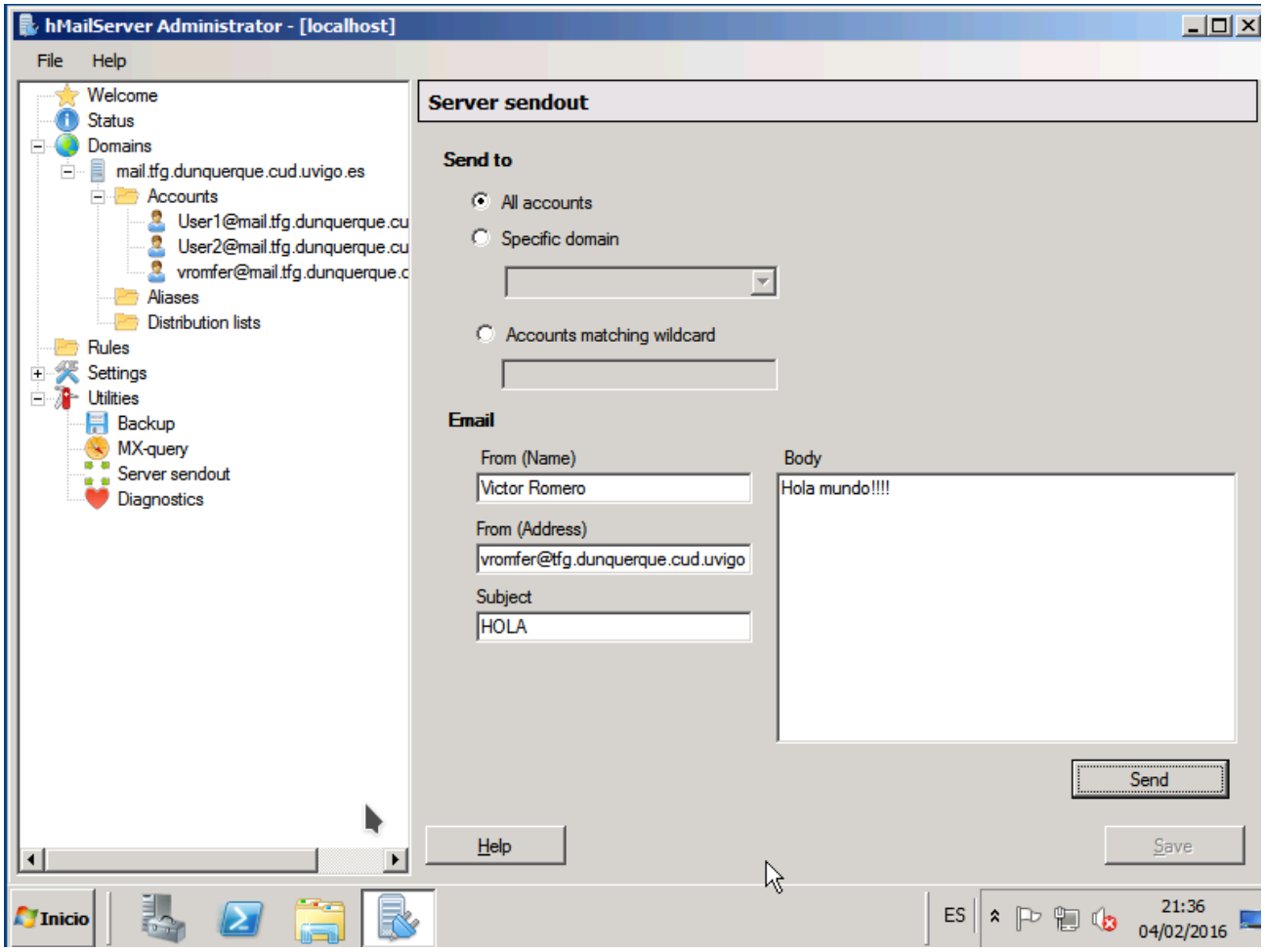

Figura 3-64: Mensaje a todos con *hMailserver*

Accediendo a la cuenta desde cualquier cliente de correo, en otro ordenador de la red, comprobamos que, efectivamente, el servidor de correo electrónico está funcionando correctamente (véase Figura 3-65)

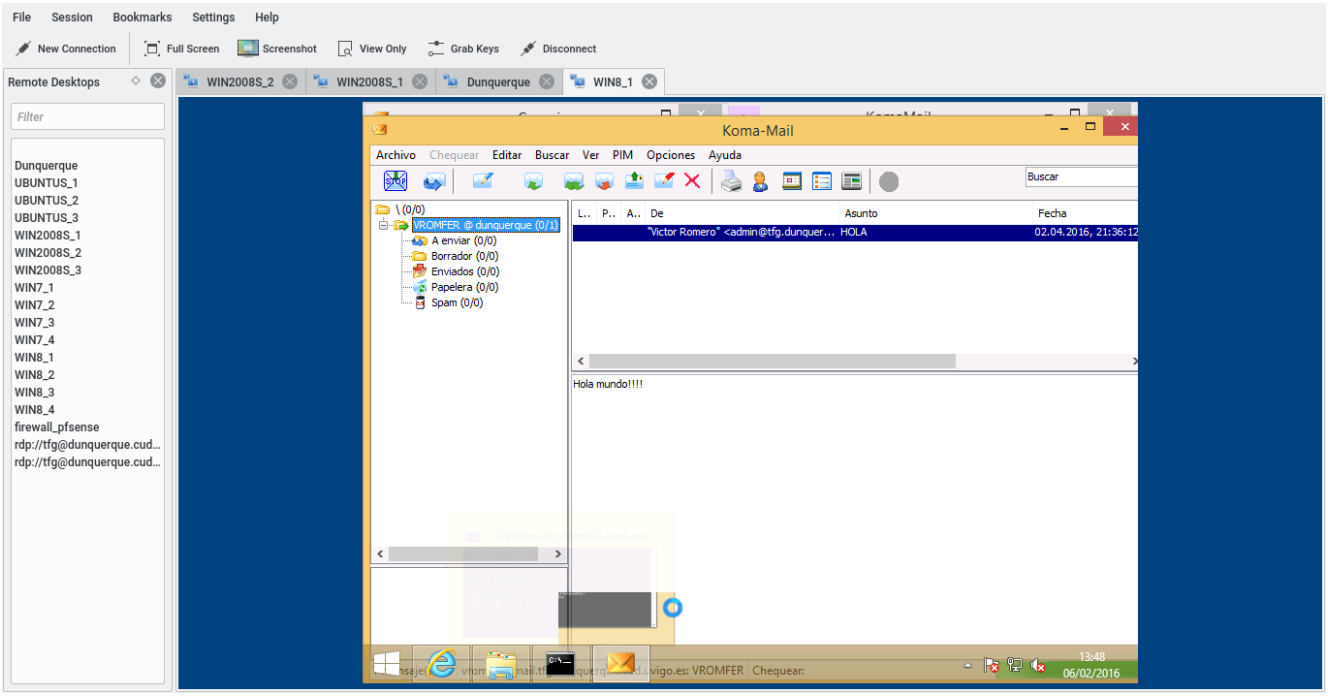

Figura 3-65: Mensaje de correo recibido en un equipo de la LAN

3.3.4.5 Servidor FTP

El servidor FTP es un protocolo que permite el acceso a ficheros de forma remota. Para ello, el servidor dispone de una carpeta a la que podrán acceder los usuarios a los cuales se le dé permiso para utilizar el servidor. El servidor FTP está accesible desde Internet y desde LAN.

Aunque el servidor FTP puede configurarse de manera segura y controlar qué carpetas pueden ser accesibles para cada uno de los usuarios, se ha decidido implementar el servidor FTP únicamente como medio para compartir información no sensible entre personas internas y externas de la organización. Por ello se ha elegido implementar un servidor FTP que acepte conexiones anónimas y sin separación de usuarios por carpetas.

El servidor FTP se implementará sobre *Ubuntu Server* en la máquina virtual SERVER_UBUNTUS_2. El software servidor FTP elegido es *Very Secure File Transfer Protocol Daemon*, normalmente llamado VSFTP.

Para realizar la instalación de este software, se hace uso de la herramienta de instalación de paquetes ya mencionada con anterioridad:

```
sudo apt-get install vsftpd
```

Una vez instalado el software, para modificar su configuración se hace uso del archivo */etc/vsftpd/vsftpd.conf* en el cual se pueden configurar diversas opciones relativas a las conexiones y a la seguridad.

Cuando el archivo esté configurado de acuerdo a nuestras necesidades, es necesario reiniciar el servidor para aplicar la configuración.

El servidor FTP puede ser accedido desde cualquier equipo en la red LAN o Internet, únicamente es necesario escribir un email que quedará almacenado en los registros del servidor.

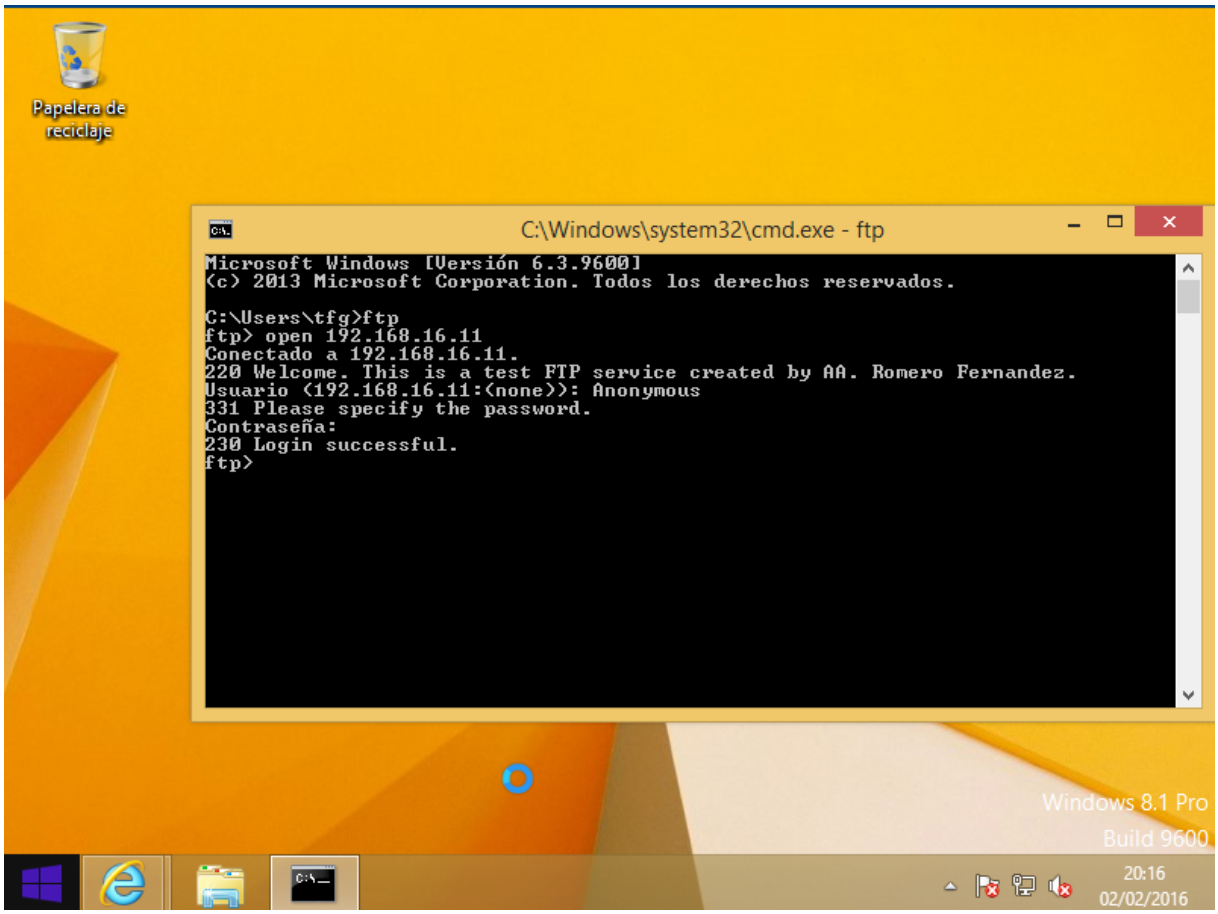

Figura 3-66: Sesión iniciada en servidor FTP

3.3.5 Configuración del firewall

En este momento, todos los servicios presentes en la topología de red se encuentran funcionando correctamente, pero están desprotegidos. En el apartado 3.3.3 se explicaba la instalación del software de cortafuegos *pfSense*. Sin embargo no se definía ninguna regla de filtrado, de modo que el cortafuegos permitía todas las conexiones desde todas las zonas a todos los puertos. En este apartado se van a configurar las reglas necesarias para permitir el tráfico de datos hacia los servidores que se encuentran en la DMZ, y bloquear todo lo demás.

Es necesario explicar que las reglas de *firewall* se comprueban en orden, hasta que el paquete cumple una de ellas. Además se aplican a cada interfaz de entrada, por lo tanto, cuando un paquete ha cumplido una regla de permiso de su interfaz de entrada podrá salir por cualquiera de los otros interfaces. Si un paquete no cumple ninguna de las reglas, será bloqueado.

Las reglas de cortafuegos en *pfSense* se configuran desde el configurador web.

3.3.5.1 Reglas de la zona desmilitarizada

En el adaptador de la zona desmilitarizada se bloquea el tráfico que tenga como dirección la red LAN, y se permite el tráfico hacia la red WAN a los servicios que desde la red DMZ necesitan acceso a Internet. Estos servicios son email (POP3, IMAP y SMTP), FTP, DNS y HTTP.

Las reglas se detallan en la Tabla 3-4 y su configuración sobre *pfSense* se puede ver en la Figura 3-67.

Nº	Regla	Acción
1	Todos los paquetes con destino LAN	Bloquear
2	Paquetes TCP con destino WAN en puerto 143 (IMAP)	Permitir
3	Paquetes TCP con destino WAN en puerto 25 (SMTP)	Permitir
4	Paquetes TCP con destino WAN en puerto 110 (POP3)	Permitir
5	Paquetes UDP/TCP con destino WAN en puerto 53 (DNS)	Permitir
6	Paquetes TCP con destino WAN en puerto 21 (FTP)	Permitir
7	Paquetes TCP con destino WAN en puerto 80 (HTTP)	Permitir
8	Paquetes TCP con destino WAN en puerto 443 (HTTPS)	Permitir
9	Paquetes ICMP con destino WAN	Permitir

Tabla 3-4: Reglas de cortafuegos en la DMZ

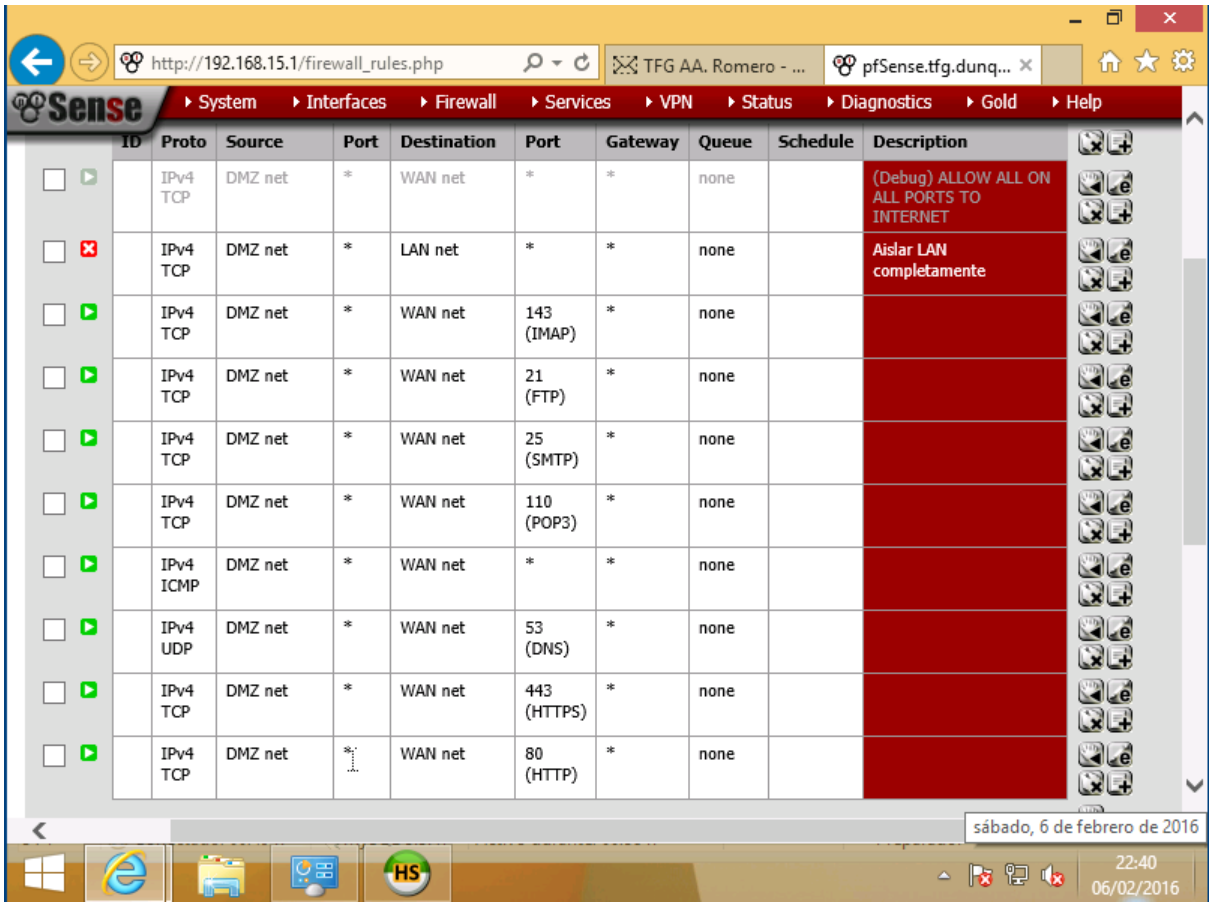

Figura 3-67: Reglas de cortafuegos para interfaz DMZ

3.3.5.2 Reglas de la red interna

En el adaptador de la red interna se permite el tráfico a los servicios que se le permite utilizar a los usuarios de esta red. Estos servicios son email (POP3, IMAP y SMTP), FTP, DNS, HTTP y MySQL. Además se permite el trafico ICMP hacia cualquier destino.

Las reglas se detallan en la Tabla 3-5 y su configuración sobre *pfSense* se puede ver en la Figura 3-68.

Nº	Regla	Acción
	Paquetes TCP con destino DMZ en puerto 3306 (MySQL)	Permitir
2	Paquetes TCP en puerto 21 (FTP)	Permitir
3	Paquetes TCP en puerto 25 (SMTP)	Permitir
4	Paquetes TCP en puerto 110 (POP3)	Permitir
5	Paquetes UDP/TCP en puerto 53 (DNS)	Permitir
6	Paquetes TCP en puerto 143 (IMAP)	Permitir
7	Paquetes TCP en puerto 80 (HTTP)	Permitir
8	Paquetes TCP en puerto 443 (HTTPS)	Permitir
9	Paquetes ICMP	Permitir

Tabla 3-5: Reglas para red interna

Figura 3-68: Reglas de cortafuegos para red interna

3.3.5.3 Reglas de la red externa

En el adaptador de la red WAN (acceso a Internet) se permite el tráfico a los servicios de la DMZ que deben estar disponibles desde Internet. Estos servicios son email (POP3, IMAP y SMTP), FTP, DNS y HTTP. Además se bloquea expresamente el tráfico que tenga como destino la red LAN u otro puerto de la red DMZ. No se permite tráfico ICMP desde Internet hacia ninguna de las redes internas.

Las reglas se detallan en la Tabla 3-6 y su configuración sobre *pfSense* se puede ver en la Figura 3-69

Nº	Regla	Acción
1	Paquetes con destino LAN	Bloquear
2	Paquetes TCP con destino DMZ en puerto 21 (FTP)	Permitir
3	Paquetes TCP con destino DMZ en puerto 25 (SMTP)	Permitir
4	Paquetes TCP con destino DMZ en puerto 110 (POP3)	Permitir
5	Paquetes UDP/TCP con destino DMZ en puerto 53 (DNS)	Permitir
6	Paquetes TCP con destino DMZ en puerto 143 (IMAP)	Permitir
7	Paquetes TCP con destino DMZ en puerto 80 (HTTP)	Permitir
8	Paquetes TCP con destino DMZ en puerto 443 (HTTPS)	Permitir
9	Paquetes con destino DMZ	Bloquear

Tabla 3-6: Reglas de Internet (WAN)

Figura 3-69: Reglas de cortafuegos para interfaz WAN

3.3.5.4 Traductor de direcciones de red (NAT)

Para permitir el acceso desde Internet hacia los servidores que se encuentran en la zona desmilitarizada, es necesario configurar el servicio NAT además de haber permitido el tráfico en esos puertos con el cortafuegos. Esto es debido a que un usuario de Internet solo conocerá nuestra dirección IP externa, y todas las peticiones a cada uno de los servidores las hará hacia la misma dirección. Por lo tanto, el sistema NAT es el encargado de dirigir cada paquete a la dirección interna adecuada para que el servidor pueda responderlo. Para determinar qué servidor es el encargado de atender cada paquete, el servicio NAT usa el puerto de destino del paquete.

Los servicios que estarán accesibles desde el exterior de la red son el servidor web, servidor de correo, servidor FTP y servidor DNS.

Las reglas de redirección configuradas en el NAT son las que pueden verse en la Tabla 3-7 y la Figura 3-70.

Origen	Puerto origen	Destino	Puerto destino
Cualquier dirección WAN	25 (SMTP)	192.168.16.21	25
Cualquier dirección WAN	143 (IMAP)	192.168.16.21	143
Cualquier dirección WAN	110 (POP3)	192.168.16.21	110
Cualquier dirección WAN	21 (FTP)	192.168.16.11	21
Cualquier dirección WAN	53 (DNS)	192.168.16.20	53
Cualquier dirección WAN	80 (HTTP)	192.168.16.10	80
Cualquier dirección WAN	433 (HTTPS)	192.168.16.10	433

Tabla 3-7: Reglas de redirección NAT

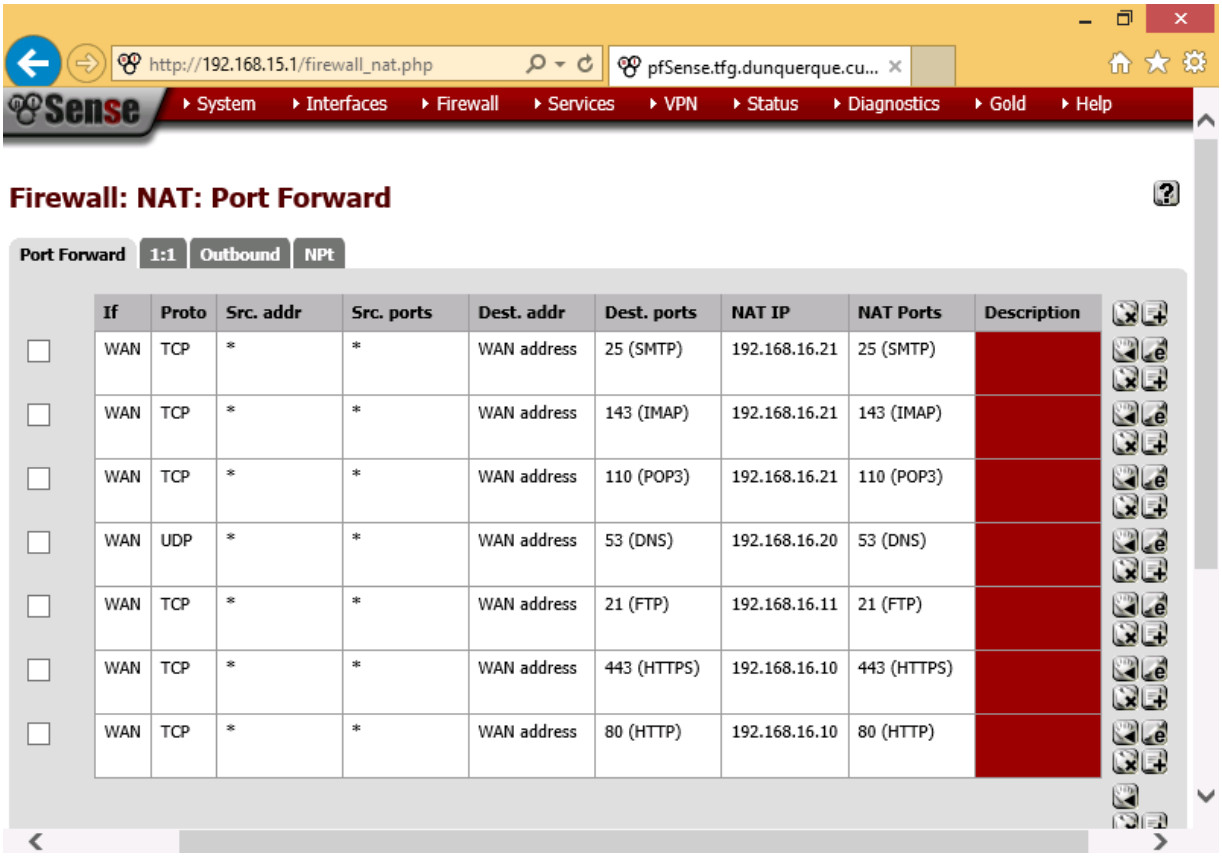

Figura 3-70: Reglas de NAT

3.3.6 Conexión a Internet

En el apartado 3.3.5 se terminó de configurar la arquitectura de la red, que se encuentra funcionando correctamente. Sin embargo, esta arquitectura está aislada de Internet debido a que su conexión con la red real se estaba realizando a través de una red virtual.

En las condiciones anteriormente mencionadas, los equipos de la maqueta podían navegar por Internet, pero no eran accesibles desde el exterior, ya que los paquetes que tenían como destino el servidor *Dunquerque* no atravesaban el túnel que comunicaba la maqueta de máquinas virtuales con el servidor.

La forma de conectar la maqueta realmente a Internet, de forma que esté accesible desde el exterior es asignándole un interfaz de red físico, en lugar de un túnel de red. Al asignar un interfaz a la maqueta este interfaz quedará inutilizable por el servidor *Dunquerque* mientras la maqueta esté en funcionamiento. Debido a esto no es posible asignarle a la maqueta el interfaz que se usa para administrar el servidor, las conexiones a escritorio remoto y el servidor de GNS3. Por lo tanto, la solución es conectar otro interfaz de red a Internet, para poder usarlo de forma dedicada por la maqueta, sin perder el control del servidor.

Se ha decidido conectar el nuevo interfaz (em2*)* a la red “Laboratorios” en lugar de a Internet directamente por motivos de seguridad. De esta forma, la maqueta estará disponible únicamente desde los ordenadores de los diferentes laboratorios del centro. La administración remota del servidor *Dunquerque* sigue accesible desde Internet.

La configuración de direcciónes IP asignadas por el administrador de la red para el nuevo interfaz es la siguiente

```
IFACE em2
INET STATIC
IP: 192.168.3.50
NETMASK:255.255.252.0
GATEWAY:192.168.1.1
```

Una vez está conectado y configurado correctamente el nuevo interfaz de red, es el momento de actualizar la configuración de GNS3. Añadiremos el interfaz *em2* como interfaz del tipo *Linux Ethernet NIO* (como se muestra en la Figura 3-71). Para ello hay que eliminar el dispositivo tipo *nube* que se estaba usando anteriormente y agregar uno nuevo.

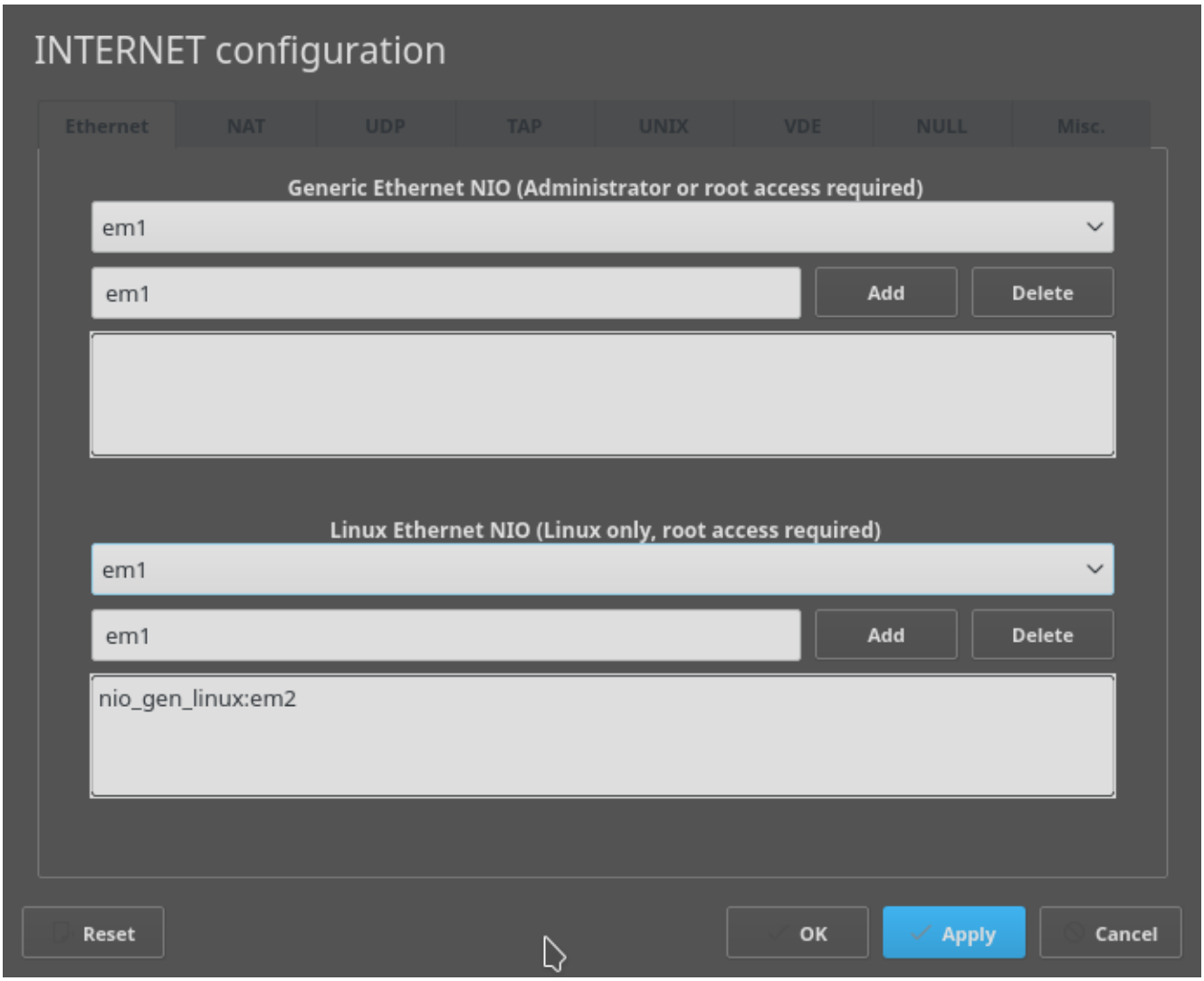

Figura 3-71: Configuración del dispositivo *Nube* INTERNET

Cuando el nuevo dispositivo tipo *nube* llamado INTERNET esté configurado para utilizar el interfaz *em2* lo conectaremos con la máquina virtual del cortafuegos *pfSense*, que es el que hace las funciones de enrutador en nuestra arquitectura de red.

En este momento nos encontramos con un problema, la máquina y el dispositivo nube son ambos tarjetas de red Ethernet, por lo que no pueden ser conectadas entre sí sin un cable cruzado de Ethernet. Como GNS3 no permite el uso de cables cruzados, se ha solucionado el problema intercalando un concentrador (HUB) con dos puertos Ethernet.

La topología de red final puede verse en la Figura 3-72.

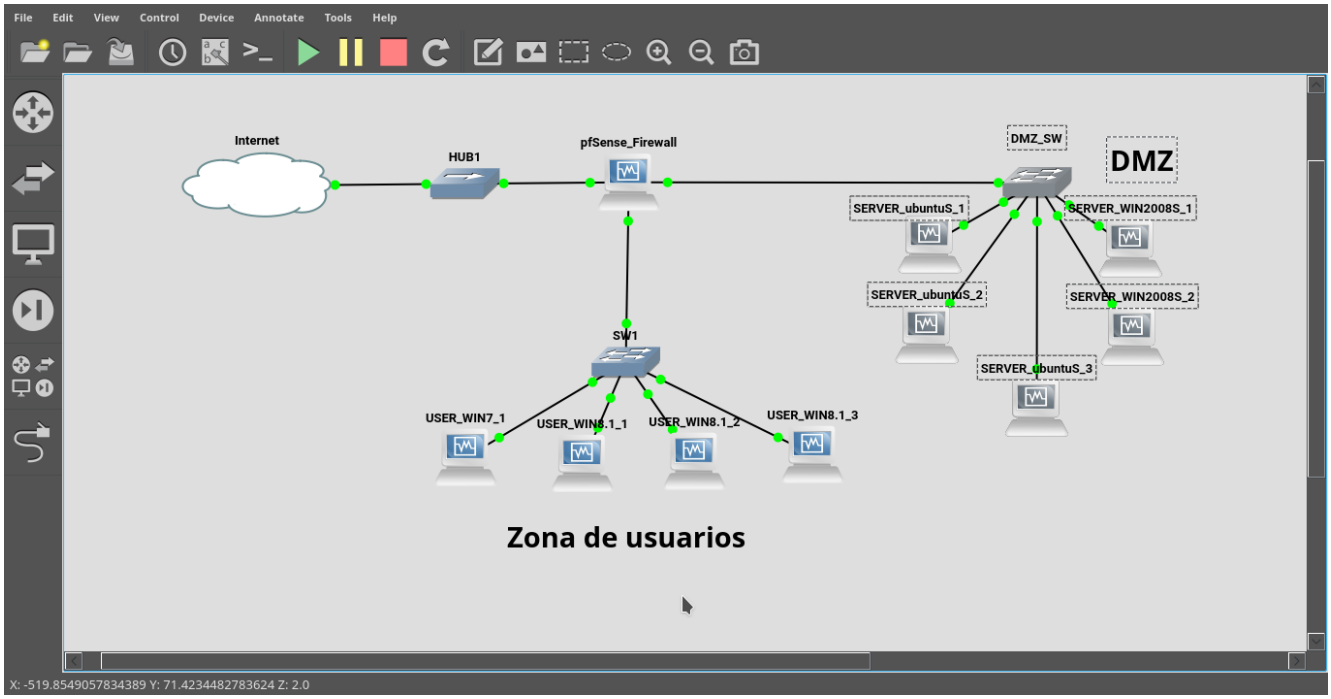

Figura 3-72: Topología de red para conexión a Internet, en GNS3

En el caso de que el interfaz *em2* estuviese conectado a Internet y tuviese una IP pública en lugar de estar conectado a una red local (la red de *laboratorios*), la maqueta estaría ya configurada y conectada correctamente.

Debido a la artificialidad de haber conectado el interfaz WAN de *pfSense* a una red local, y por coincidencia la red *wan*, y la red *lan* están superpuestas en el mismo segmento de red. Es necesario por lo tanto ajustar la configuración de direcciones IP de *pfSense* para evitar que las dos redes estén en el mismo segmento de direcciones.

La red *laboratorios* o *wan* (en el entorno de la maqueta), es una red de la universidad, por lo que no se puede modificar. Esta red está asignada al segmento *192.168.1.0/22.*

Accediendo a la máquina virtual de *pfSense* mediante su puerto de escritorio remoto se configuran los interfaces WAN y LAN con las siguientes opciones:

- WAN (ver Figura 3-73)
  IPv4: 192.168.3.50
  Netmask: 255.255.252.0 (22)
  Gateway: 192.168.1.1
  Ipv6: DISABLE

- LAN(ver Figura 3-74)
  IPv4: 192.168.8.1
  Netmask: 255.255.248.0 (21)
  Gateway: None
  IPv4 DHCP server: ACTIVE
  DHCP IPv4 Range: 192.168.8.2 → 192.168.15.254
  IPv6: DISABLE

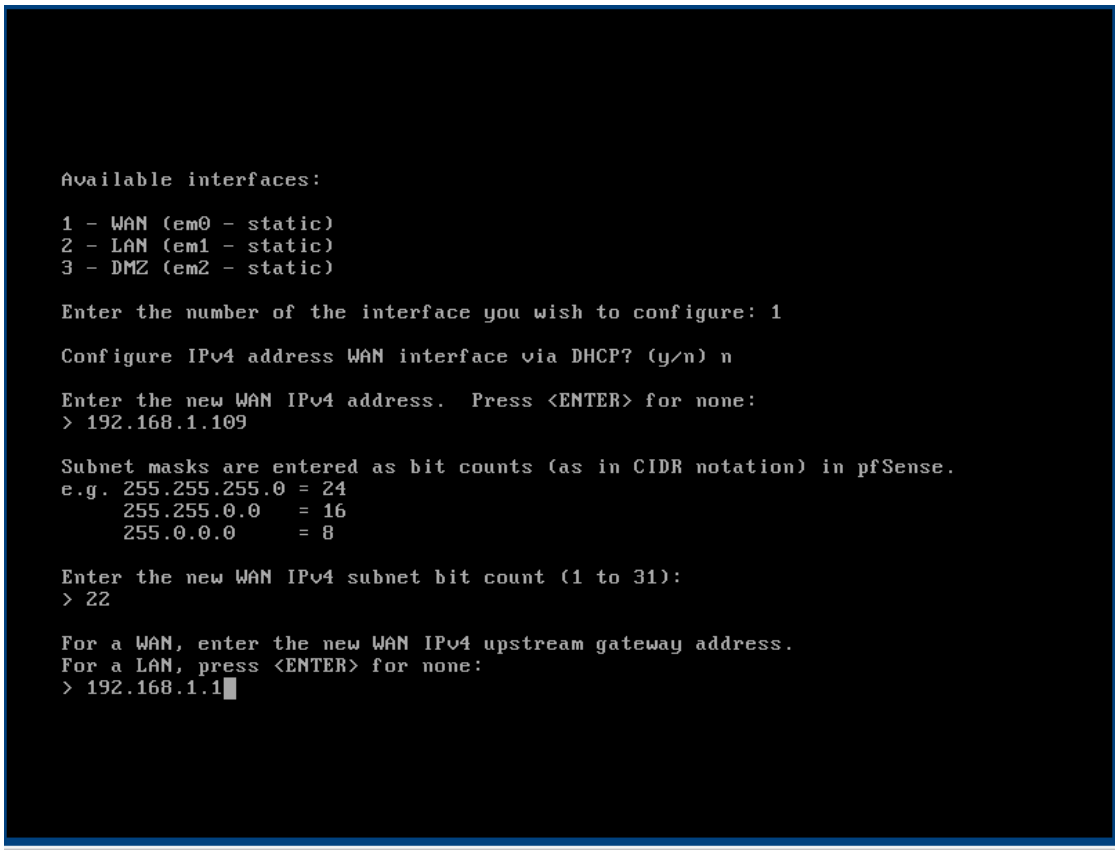

Figura 3-73: *pfSense*, configuración de interfaz WAN

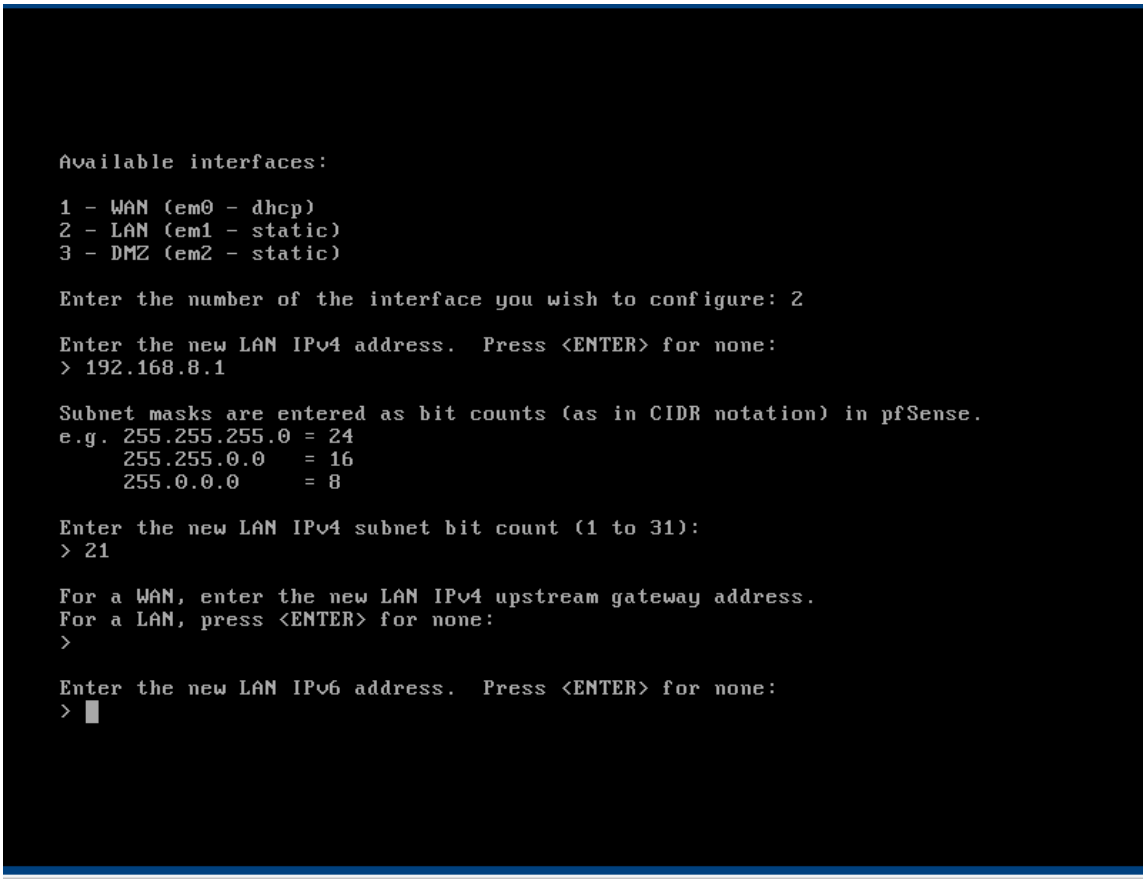

Figura 3-74: *pfSense*, configuración de interfaz LAN

3.3.7 Funcionamiento autónomo

Con la maqueta correctamente implementada y configurada, en este apartado se pretende dejar de lado la forma de trabajo que se usaba hasta ahora (explicada en el apartado 3.1.3). De esta forma, la maqueta puede ejecutarse de manera independiente sobre el servidor *Dunquerque* sin necesidad de estar conectado ni ejecutando ningún programa el ordenador de trabajo. Además, a partir de este momento, la maqueta comenzará a comportarse como un conjunto de servidores reales que permanecen disponibles en todo momento.

Las máquinas virtuales ya se encontraban en el servidor *Dunquerque*, por lo tanto no será necesario modificar sus configuraciones y datos.

Lo único que será necesario migrar es el proyecto de GNS3 con la topología de red, que se encontraba en el ordenador de trabajo. Para ello, se transfiere utilizando el servicio SFTP el archivo *TFG2.gns3* que contiene esta información. Se guarda en el servidor *Dunquerque* en la ruta */home/tfg/TFG/*GNS3*/projects/TFG2.gns3.*

En este momento se va a dejar de ejecutar el proyecto de GNS3 desde el ordenador portátil. Hay dos posibilidades para llevar a cabo esta tarea, desactivar el servidor de GNS3 y ejecutar el proyecto como local, o mantenerlo activo y configurar el cliente GNS3 en *Dunquerque*. Se ha decidido mantener el servidor activo, ya que así el servidor *Dunquerque* puede recibir conexiones y ejecutar otras simulaciones de arquitecturas de red en un futuro, al mismo tiempo que mantiene activa esta maqueta. Por lo tanto, se configura el cliente de GNS3 en *Dunquerque* de la misma manera que en el apartado 3.1.2.3 se configuraba en el ordenador de trabajo.

Activaremos el autoarranque en el archivo del proyecto de GNS3 para que nada más abrir el programa, arranquen las máquinas virtuales de la maqueta. Para ello, con un editor de texto abrimos el archivo *TFG2.gns3* y en la segunda línea establecemos el parametro *auto_start* como *true* (tal como se muestra en la Figura 3-75).

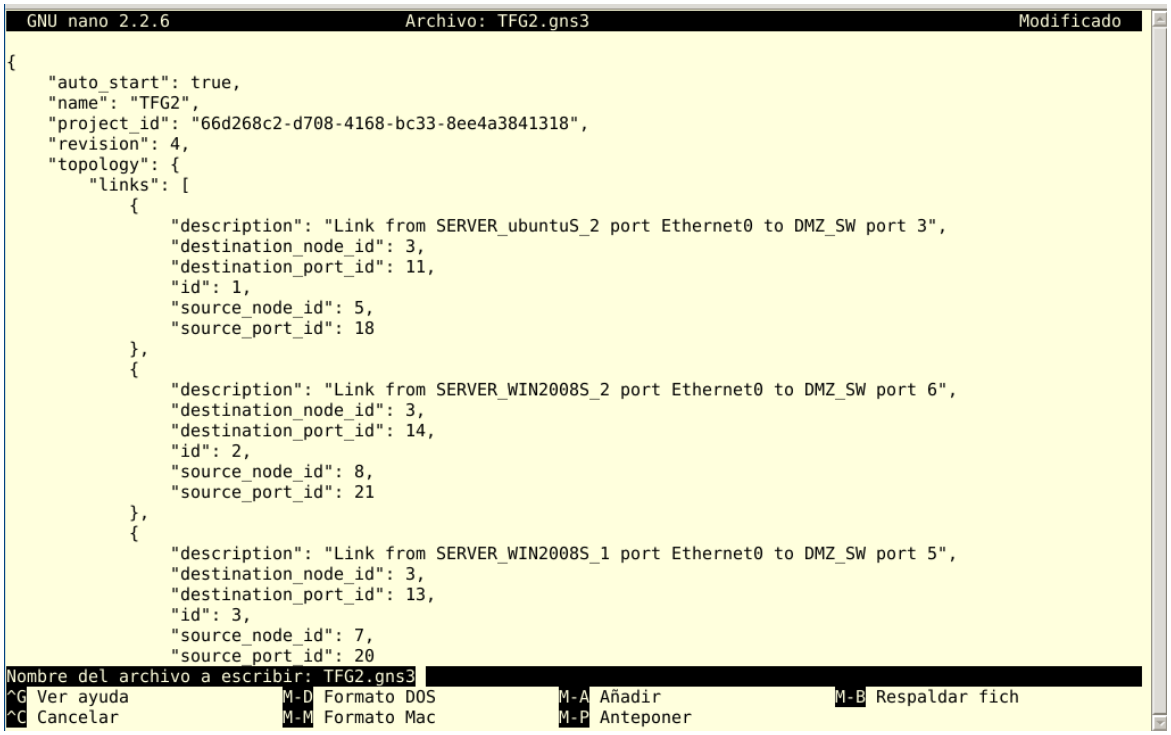

Figura 3-75: Archivo de proyecto de GNS3

Para ejecutar la maqueta es necesario arrancar tanto el servidor de GNS3 como su cliente, con el archivo de proyecto. En éste caso, se ejecutarán las tareas en segundo plano, para posteriormente indicar con el comando *disown* que estas tareas deben mantenerse activas cuando se cierre la sesión remota. Ejecutaremos la maqueta desde una terminal en el servidor *Dunquerque* mediante escritorio remoto como se ve en la Figura 3-76, con los comandos:

```
$ gns3server --daemon & disown
$ gns3 /home/tfg/TFG/GNS3/projects/TFG2.gns3 & disown
```

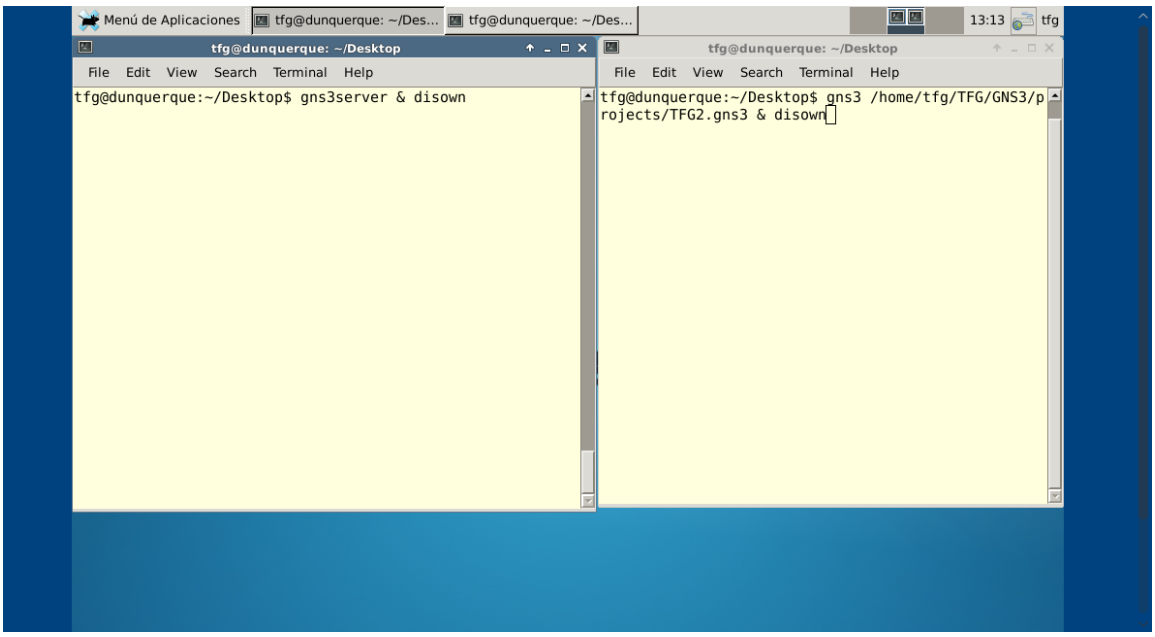

Figura 3-76: Ejecución de la maqueta

Tras unos minutos, la maqueta se encontrará en ejecución (como se muestra en Figura 3-77). Las terminales donde se han ejecutado los comandos pueden cerrarse.

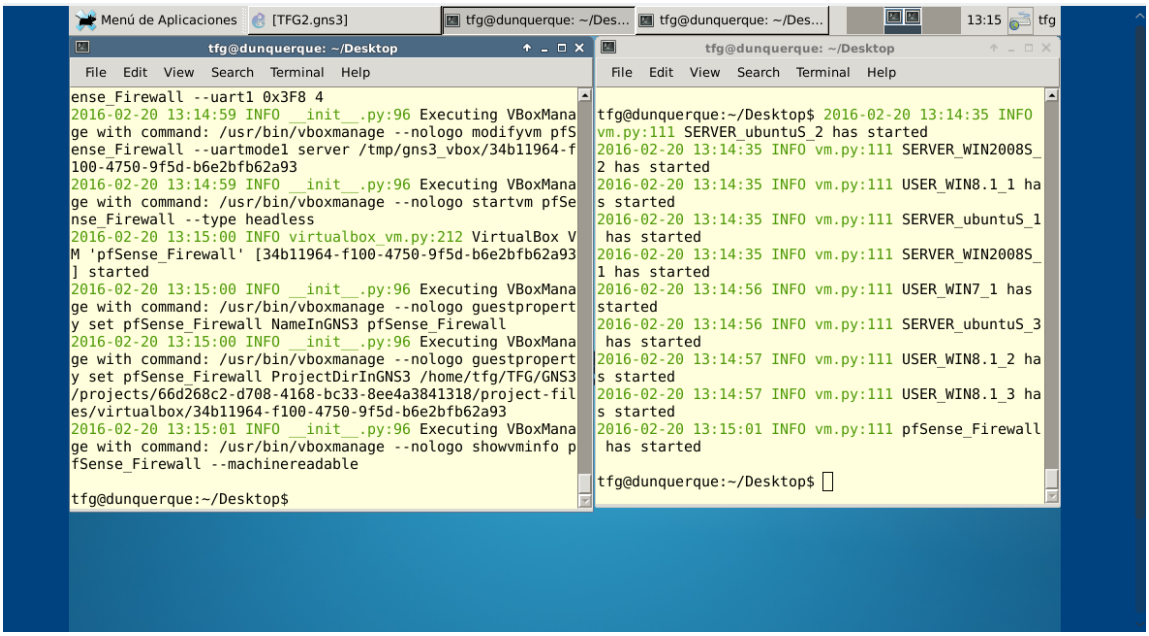

Figura 3-77: Maqueta en ejecución (I)

Con la ayuda del comando *ps* podemos comprobar que las aplicaciones siguen abiertas tras cerrar las consolas. También, con VirtualBox se puede comprobar que las máquinas virtuales de la maqueta están en ejecución.

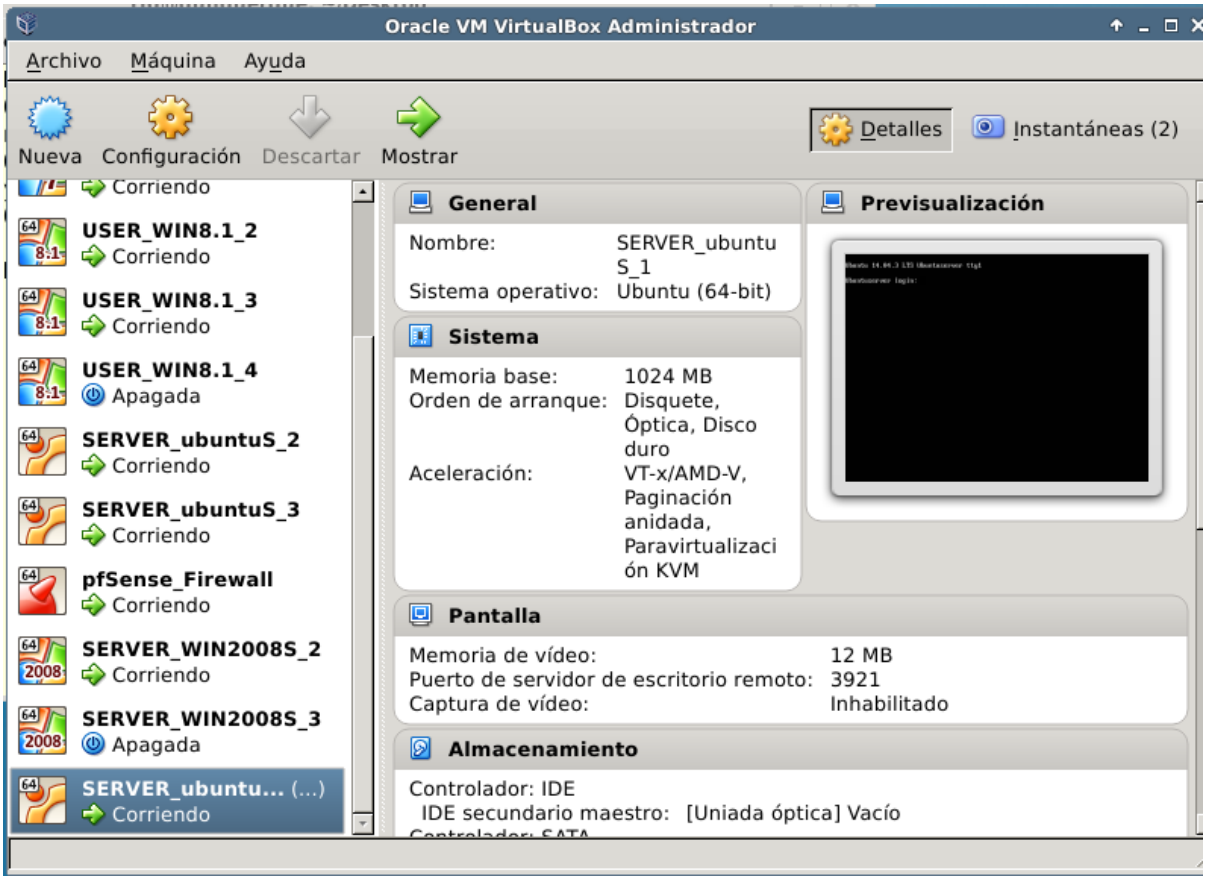

Figura 3-78: Maqueta en ejecución (II)

En este momento se puede cerrar la sesión de escritorio remoto y la maqueta queda lista para su utilización, accesible en modo usuario desde la red de *laboratorios* del CUD, en la dirección *192.168.3.50*. La Figura 3-79 demuestra que la maqueta funciona y se puede acceder a ella desde los ordenadores de los laboratorios del CUD.

Figura 3-79: Página principal del servidor web de la maqueta desde un ordenador del laboratorio

4 VALIDACIÓN DEL MODELO Y PRUEBAS

En este apartado se va a validar la maqueta de máquinas virtuales. Para ello se van a realizar dos pruebas. La primera de ellas es una demostración de servicios, en la cual se comprobará que los servicios están funcionando y se puede acceder a ellos. La segunda es un análisis de vulnerabilidades que pretende validar que la configuración de seguridad que tiene la maqueta es la que se pretendía. Ambas pruebas se realizarán desde el punto de vista de un atacante o usuario en la red interna, y en la red externa.

4.1 Demostración de servicios.

4.1.1 Desde LAN

Recordando el modelo propuesto en el apartado 3.2, desde la red interna de la maqueta deben estar disponibles los siguientes servicios:

- Servidor web.
  - Gestor de contenidos
  - *Phpmyadmin*
  - Cliente de webmail
- Servidor FTP
- Servidor DNS
- Servidor de Correo electrónico.

Para acceder al servidor web utilizamos la dirección *http://www.tfg.dunquerque.cud.uvigo.es.* En las Figuras 4-1, 4-2 y 4-3 se muestra respectivamente el acceso a los servicios del servidor web desde una máquina de la red interna.

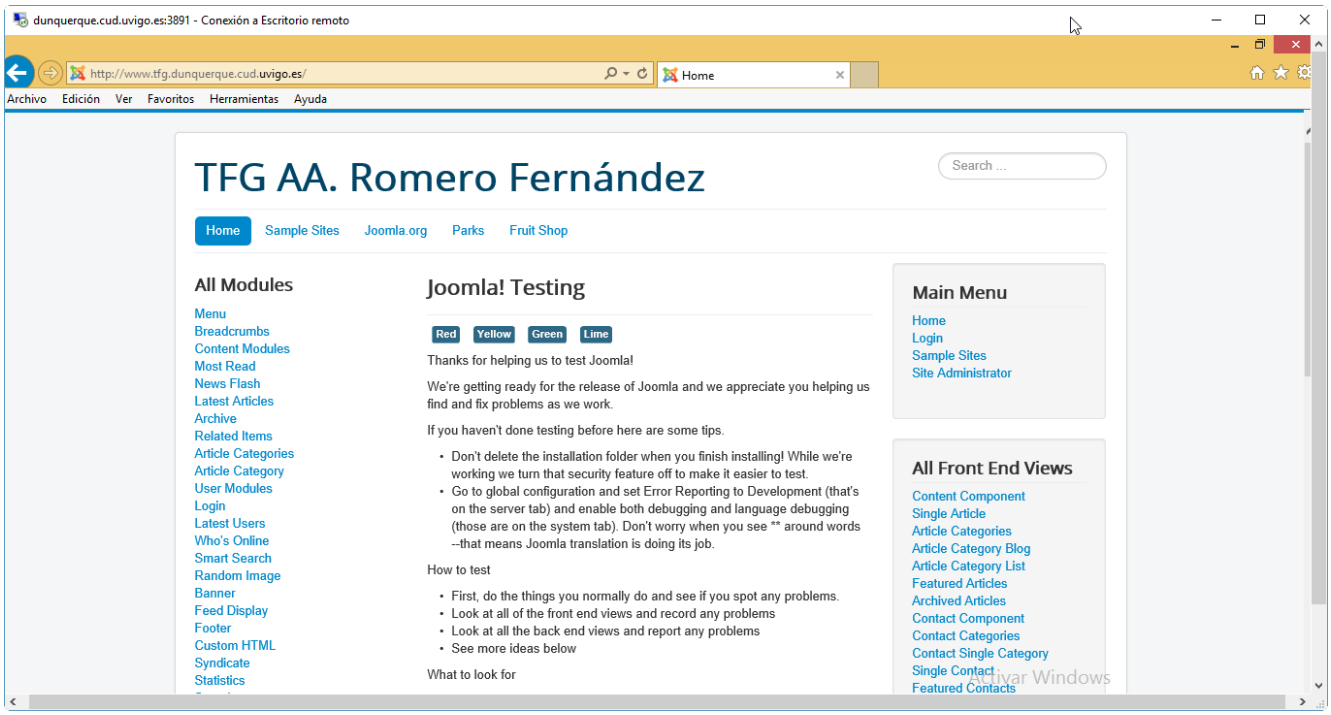

Figura 4-1: Gestor de contenidos desde MV USER_WIN8.1_1

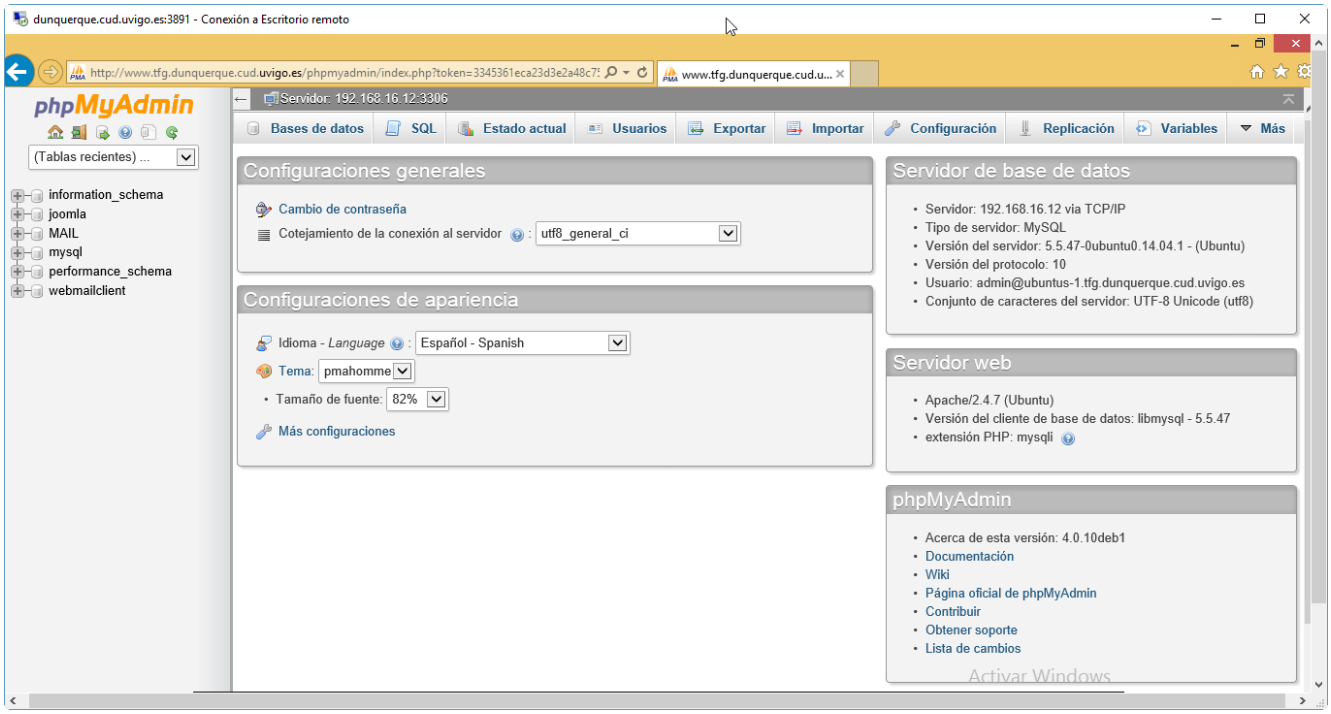

Figura 4-2: *Phpmyadmin* desde MV USER_WIN8.1_1

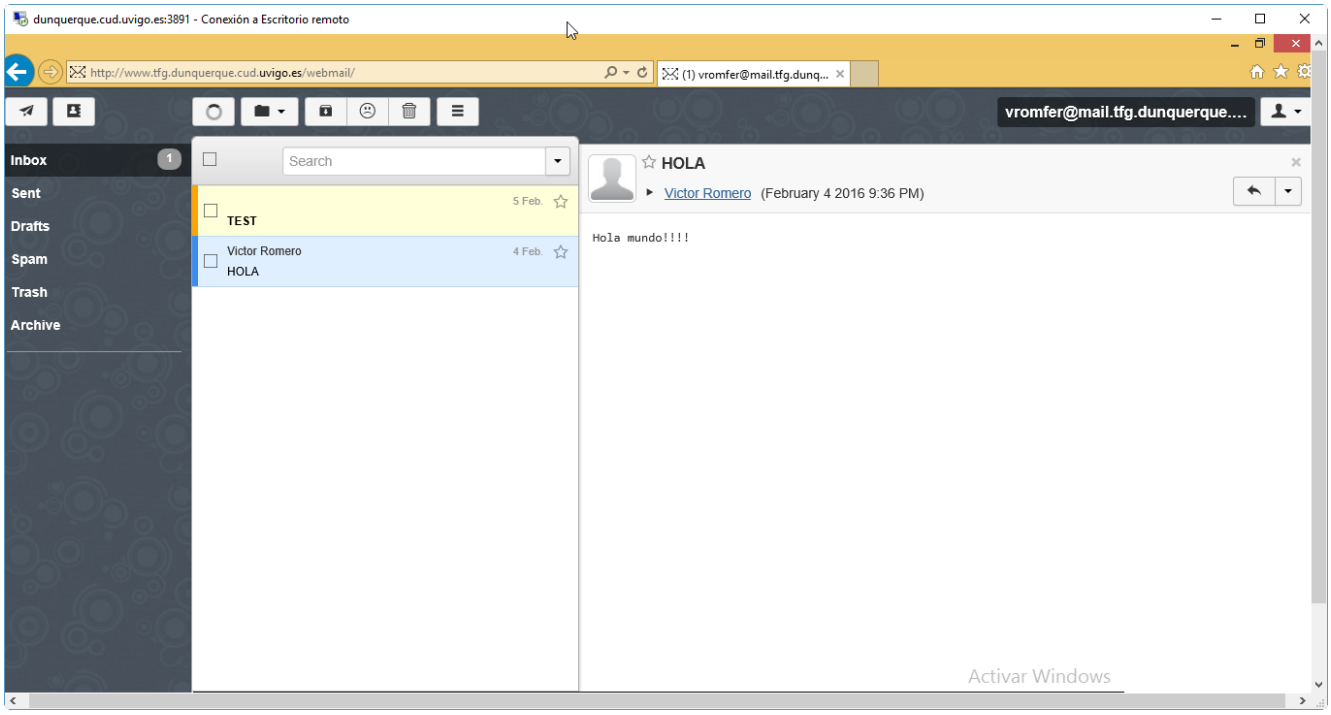

Figura 4-3: Cliente Webmail desde MV USER_WIN8.1_1

El servidor FTP se encuentra en la dirección IP *192.168.16.11*. En la Figura 4-4 se ilustra cómo es posible acceder a él desde la utilidad *ftp* de la línea de comandos de *Windows*.

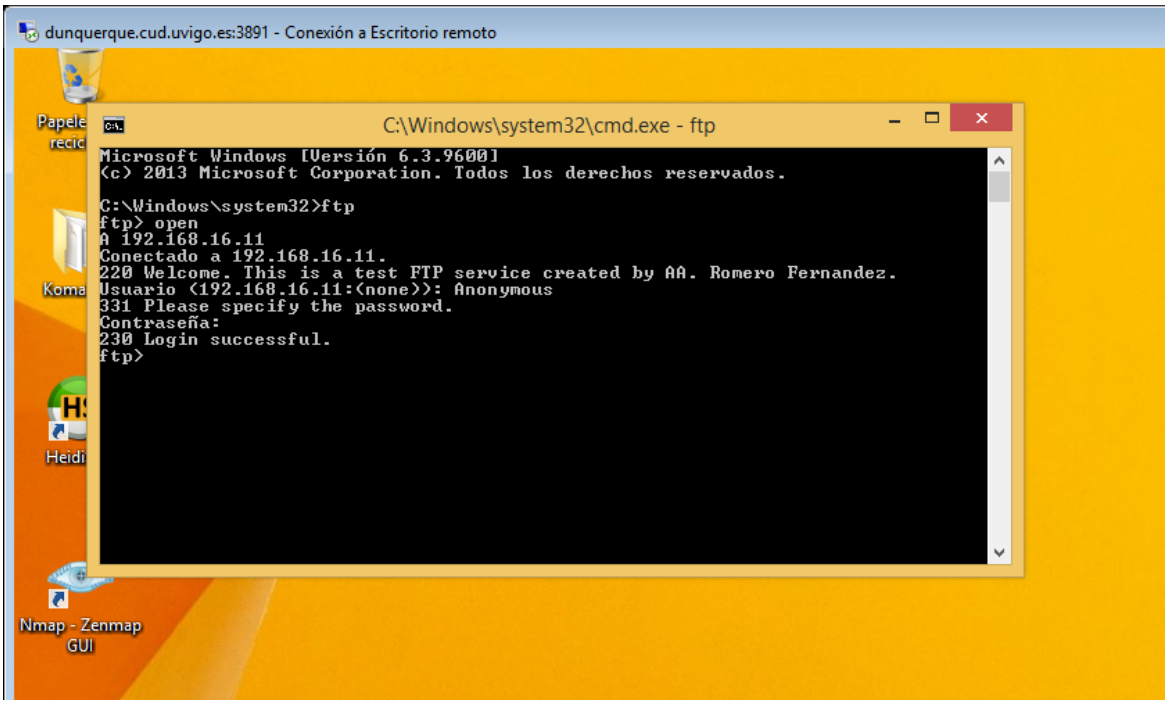

Figura 4-4: Login en servidor FTP desde MV USER_WIN8.1_1

El servidor DNS tiene la dirección IP *192.168.16.20*. En la Figura 4-5 se puede observar la respuesta del servidor DNS a una petición realizada con la herramienta *nslookup*.

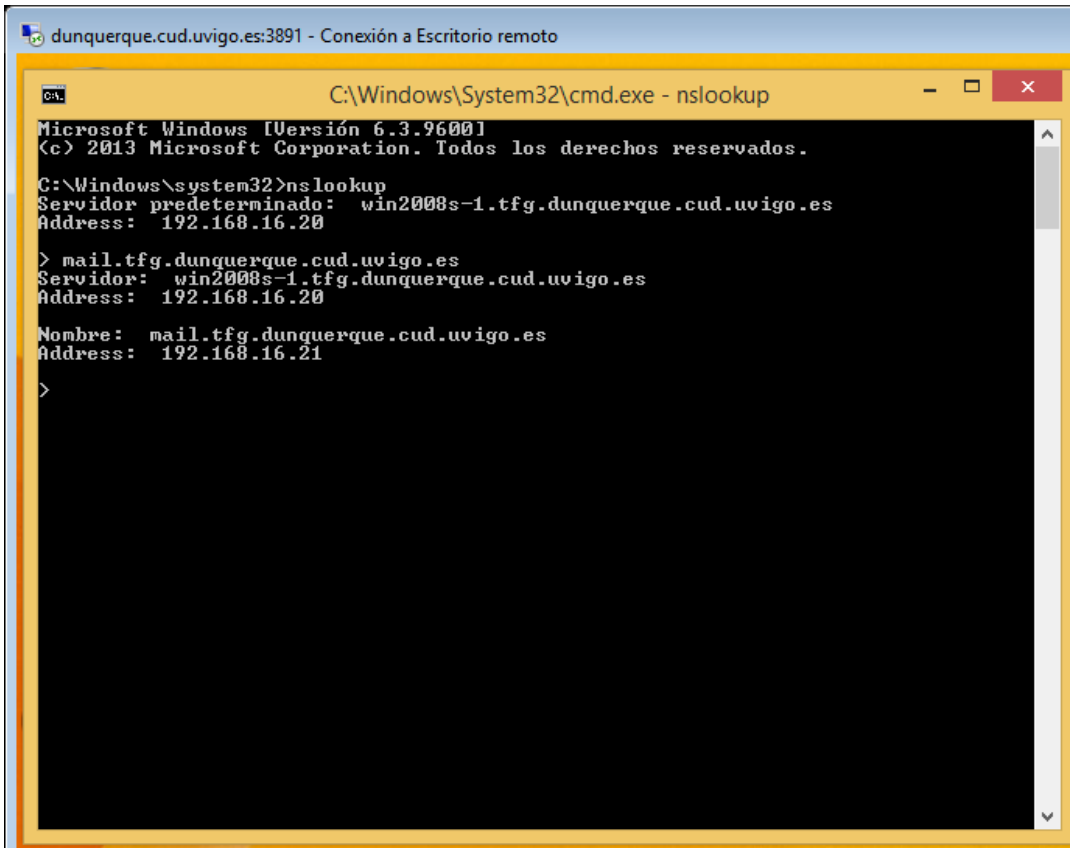

Figura 4-5: Resolución de una búsqueda DNS desde MV USER_WIN8.1_1

El servidor de correo electrónico, con dirección IP *192.168.16.21*, proporciona los servicios IMAP, POP3 y SMTP; por lo tanto, puede consultarse el correo desde cualquier aplicación cliente de correo electrónico, además del cliente *Webmail*. En la Figura 4-6 se puede ver cómo el cliente de correo electrónico *Koma-Mail* puede consultar el correo electrónico del servidor de correo con IMAP.

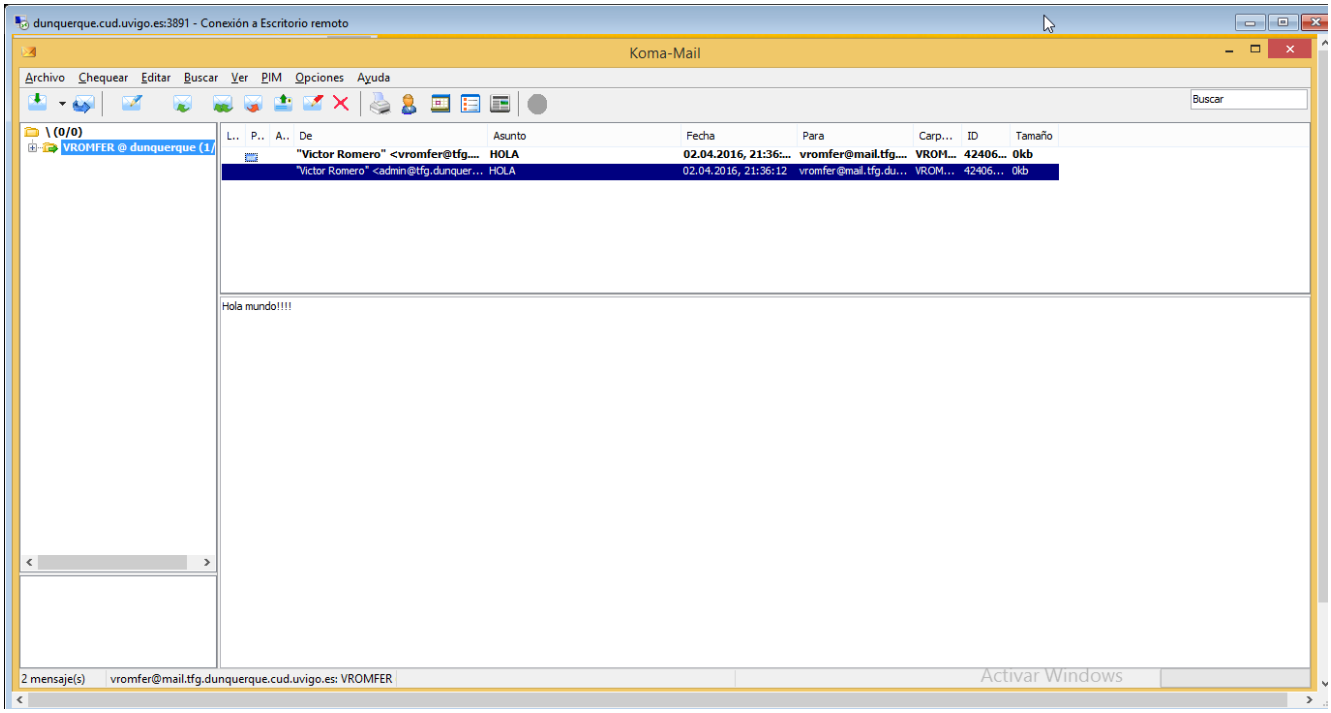

Figura 4-6: Acceso a servidor de correo electrónico desde MV USER_WIN8.1_1

4.1.2 Desde el exterior.

Según el modelo propuesto en el apartado 3.2, los servicios a los que los usuarios deberían poder acceder desde el exterior de la maqueta son los siguientes:

- Servidor web.
  - Gestor de contenidos
  - *Phpmyadmin*
  - Cliente de webmail
- Servidor FTP
- Servidor DNS
- Servidor de correo electrónico.

El acceso a todos los servicios de la maqueta desde el exterior se realiza a través de la dirección IP *192.168.3.50*. Los puertos utilizados para cada servicio son los siguientes.

- Servidor web: 80 y 433 (para las paginas seguras, como *phpmyadmin*)
- Servidor FTP: 21
- Servidor DNS: 53
- Servidor de correo electrónico: 25, 110 y 143.

Las Figuras 4-7, 4-8 y 4-9 ilustran, respectivamente, el acceso desde el ordenador portátil de trabajo, conectado a la red de laboratorios, a los servicios web de la maqueta.

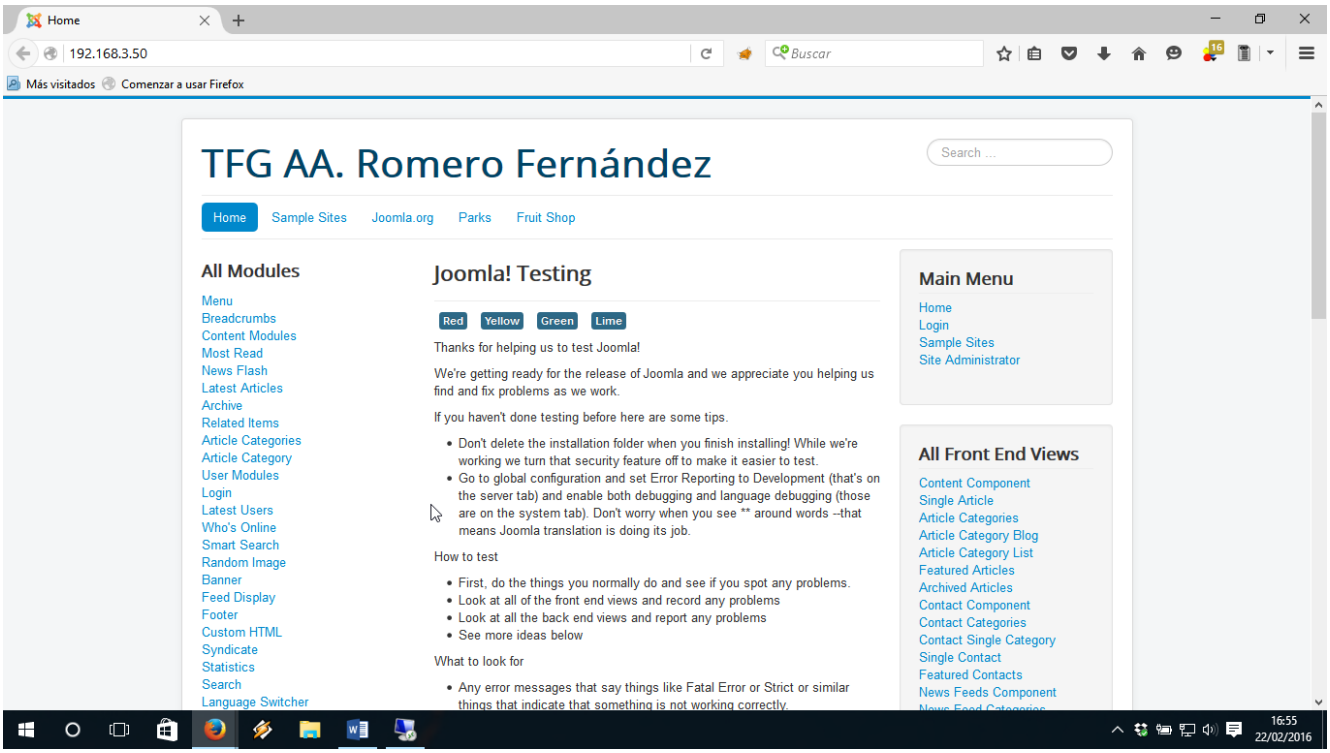

Figura 4-7: Gestor de contenidos desde ordenador conectado a la red de laboratorios

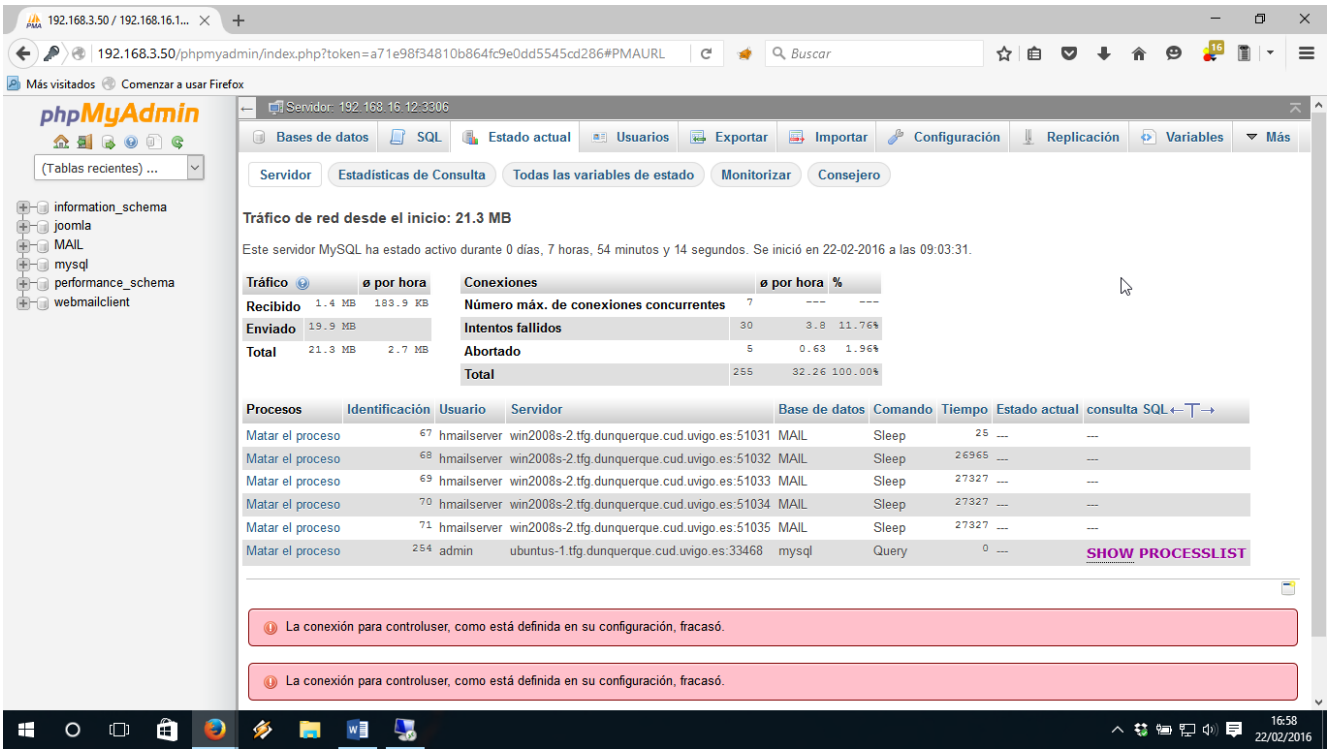

Figura 4-8: *Phpmyadmin* desde ordenador conectado a la red de laboratorios

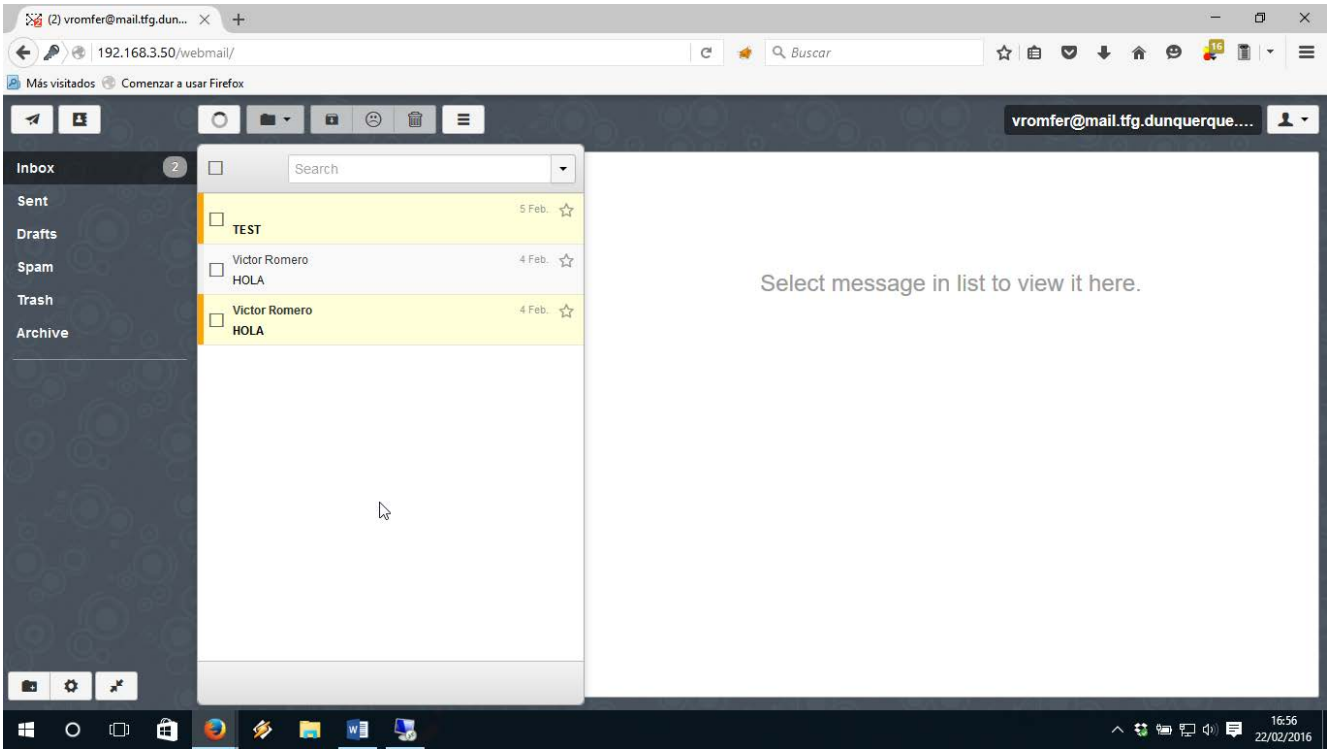

Figura 4-9: Cliente webmail desde ordenador conectado a la red de laboratorios

En la Figura 4-10, se demuestra que el servidor FTP puede ser accedido desde la red de laboratorios.

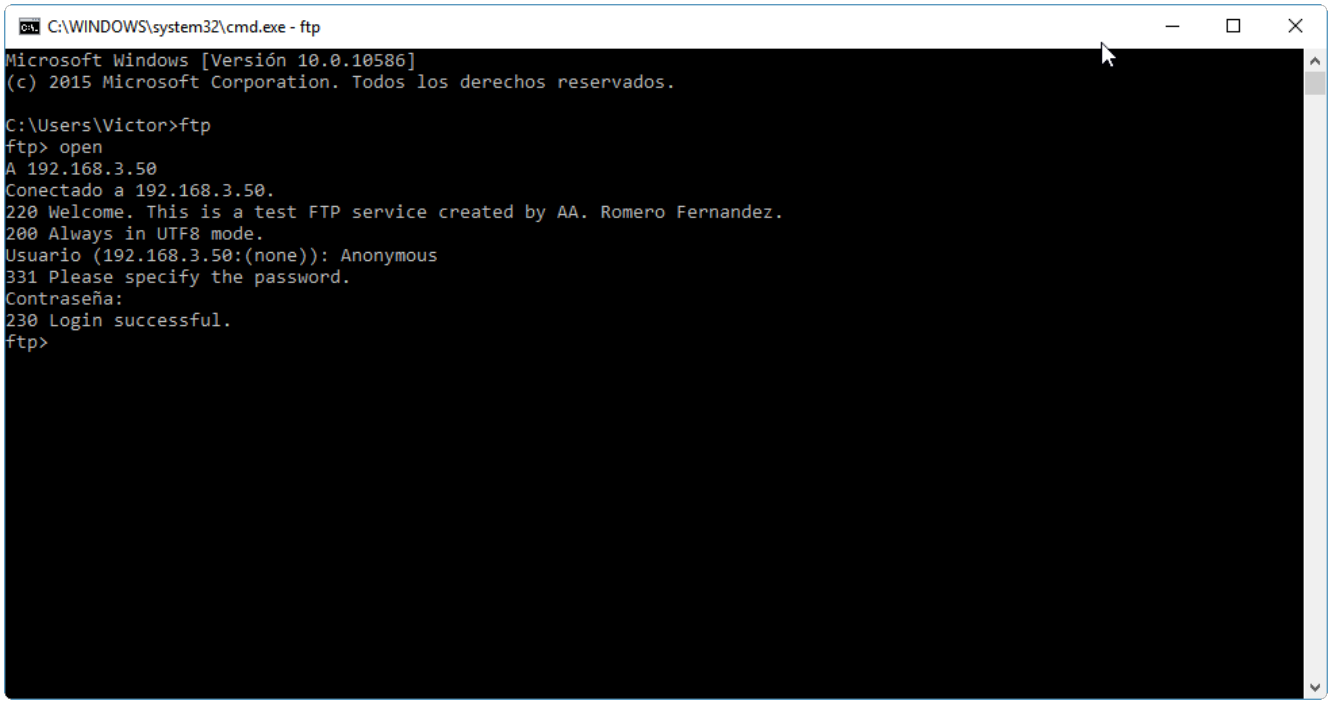

Figura 4-10: Login en servidor FTP desde ordenador conectado a la red de laboratorios

La Figura 4-11 muestra una petición de resolución de nombres realizada al servidor DNS de la maqueta. Aunque el servidor responde adecuadamente, sus respuestas no tienen interés fuera de la red local, ya que las direcciones que devuelve no son accesibles desde el exterior.

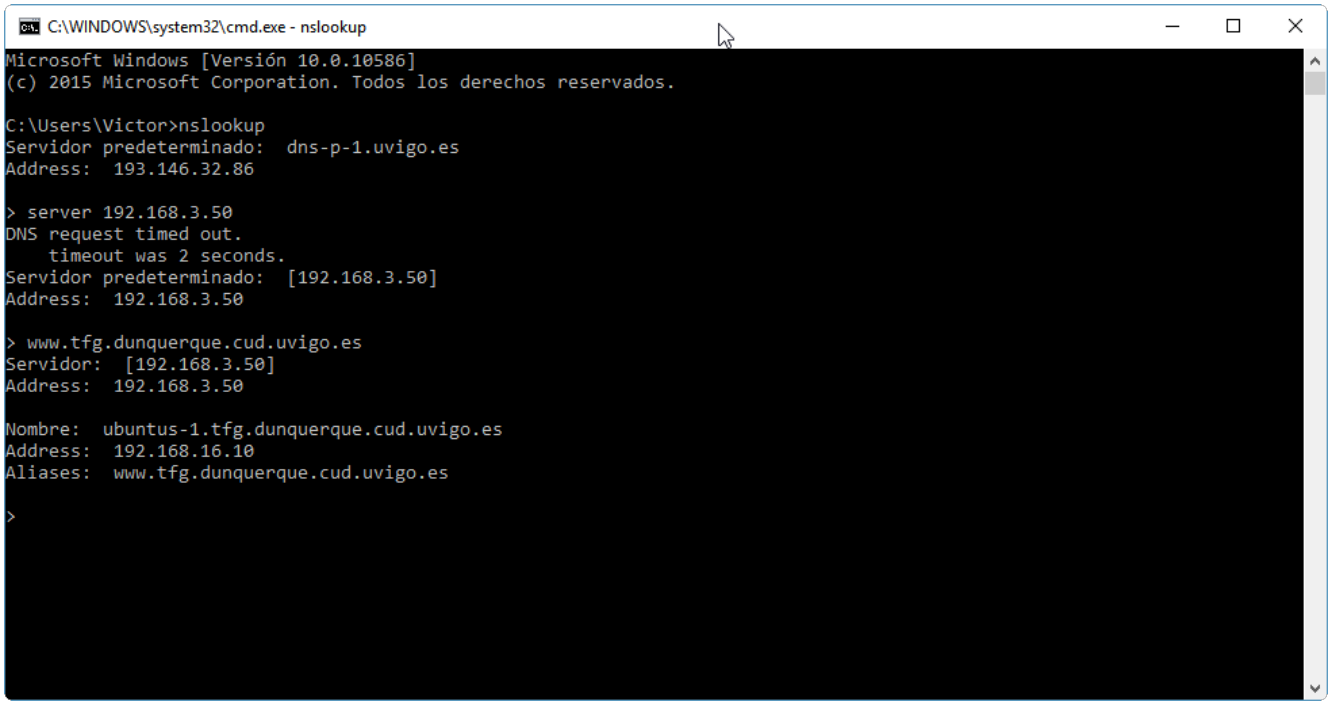

Figura 4-11: Resolución DNS desde ordenador conectado a la red de laboratorios

Al igual que desde la red interna, el servidor de correo puede ser consultado desde el exterior usando cualquier cliente de correo electrónico con soporte para IMAP, POP3 o SMTP. En la Figura 4-12 se puede ver al cliente *Koma-Mail* consultando el correo desde la red de laboratorios. En este caso, es necesario tener en cuenta que el DNS de la red de laboratorios no dispone de las direcciones

de la maqueta, por lo cual el dominio de la cuenta de correo electrónico debe ser sustituido por la dirección IP *192.168.3.50* correspondiente a la maqueta.

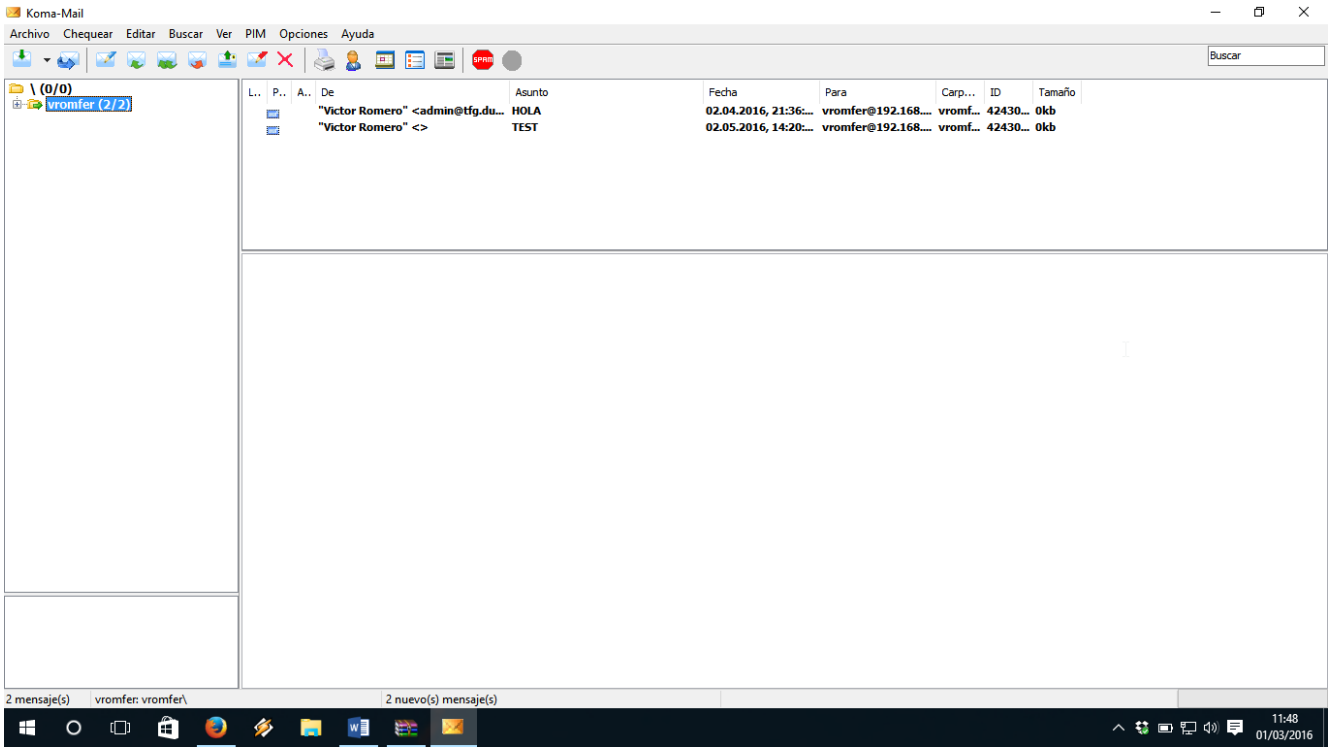

Figura 4-12: Acceso a servidor de correo electrónico desde ordenador conectado a la red de laboratorios

4.2 Seguridad

La prueba de seguridad consistirá en la ejecución de una pequeña batería de pruebas de seguridad desde la red interna y la red externa. Las pruebas se llevaran a cabo desde *Kali Linux*, una distribución de Linux especializada en análisis de seguridad de redes. Esta batería de pruebas estará compuesta por las siguientes pruebas:

- Descubrimiento con *nmap*.
- Ataque *Hail Mary* con *Armitage*.

El descubrimiento con *nmap* se realizará con la interfaz gráfica *Zenmap*. Se lanzarán los escaneos *Quick Scan y Slow Comprenhensive Scan*.

El ataque *Hail Mary* consiste en analizar los servicios que están ejecutándose en los objetivos y posteriormente lanzar todos los ataques posibles sobre esos servicios. Para ello, en primer lugar, se importan los escaneos realizados por *nmap*. A continuación, se buscan los servicios en ejecución y sus posibles *exploits* y se lanza el ataque.

4.2.1 Desde el exterior

El descubrimiento realizado con *nmap* dio como resultado la información que puede verse en la Figura 4-13 y los puertos que aparecen en la Figura 4-14. Es necesario reseñar que el programa no ha conseguido identificar correctamente el sistema operativo que se ejecuta en la máquina cortafuegos, tampoco la ha conseguido atravesar y revelar la topología interna de la red de la maqueta. El puerto correspondiente a HTTPS aparece como bloqueado, sin embargo, está abierto y se utiliza sin problema, por ejemplo, al acceder a *Phpmyadmin*, por lo que puede considerarse un falso positivo.

Nmap proporciona más información que no se presenta en las capturas de pantalla y puede ser útil para continuar un ataque. Los archivos de salida del programa se adjuntan en el disco que acompaña

este trabajo, pueden ser abiertos con la interfaz gráfica *Zenmap* para el estudio de los resultados del escaneo.

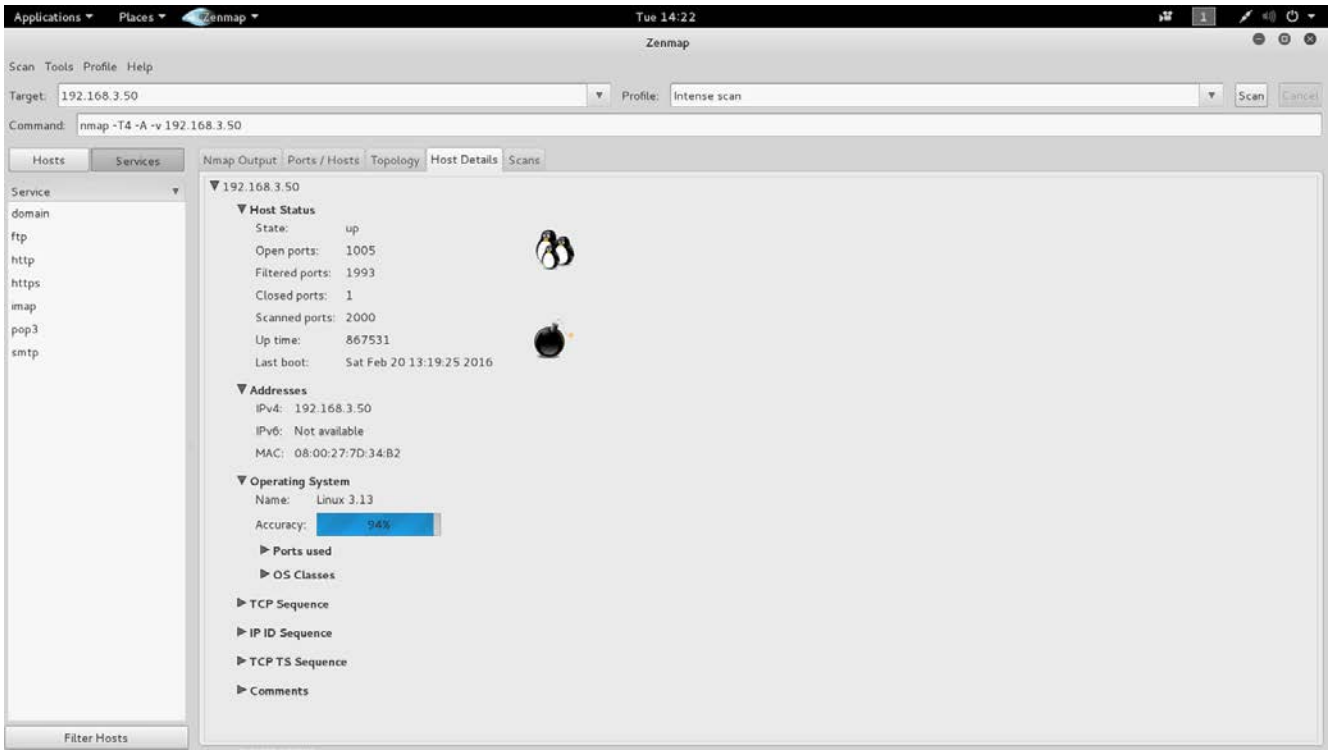

Figura 4-13: *Nmap*: datos relativos al *Host*

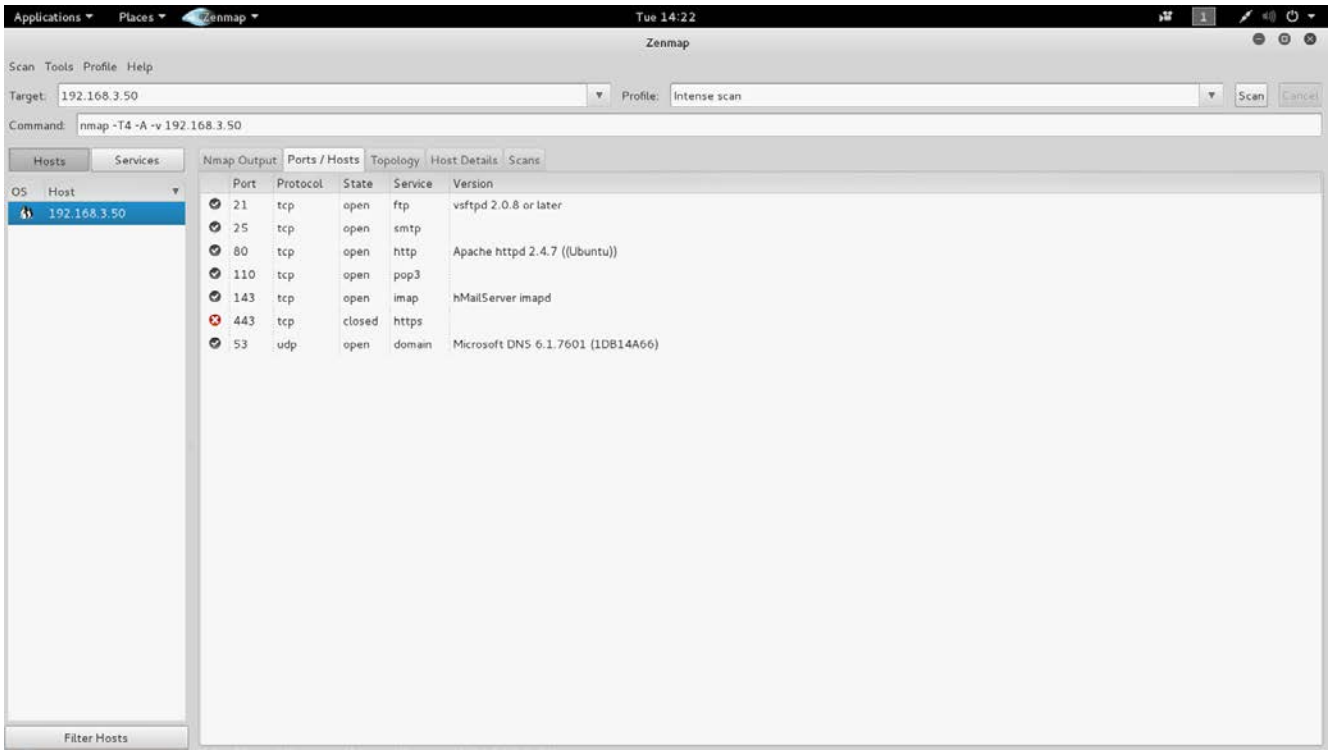

Figura 4-14: *Nmap*, puertos abiertos

Con los análisis de *nmap* importados en *Armitage*, y una vez realizados los análisis específicos de este programa, se obtiene información relativa a los servicios que se ejecutan (véase Figura 4-15). Esta información coincide con la mostrada por *nmap*. Se lanza el ataque *Hail Mary*, cuya finalidad es explotar alguna vulnerabilidad para abrir una sesión remota en el objetivo. El ataque no tiene éxito, como se puede ver en la Figura 4-16.

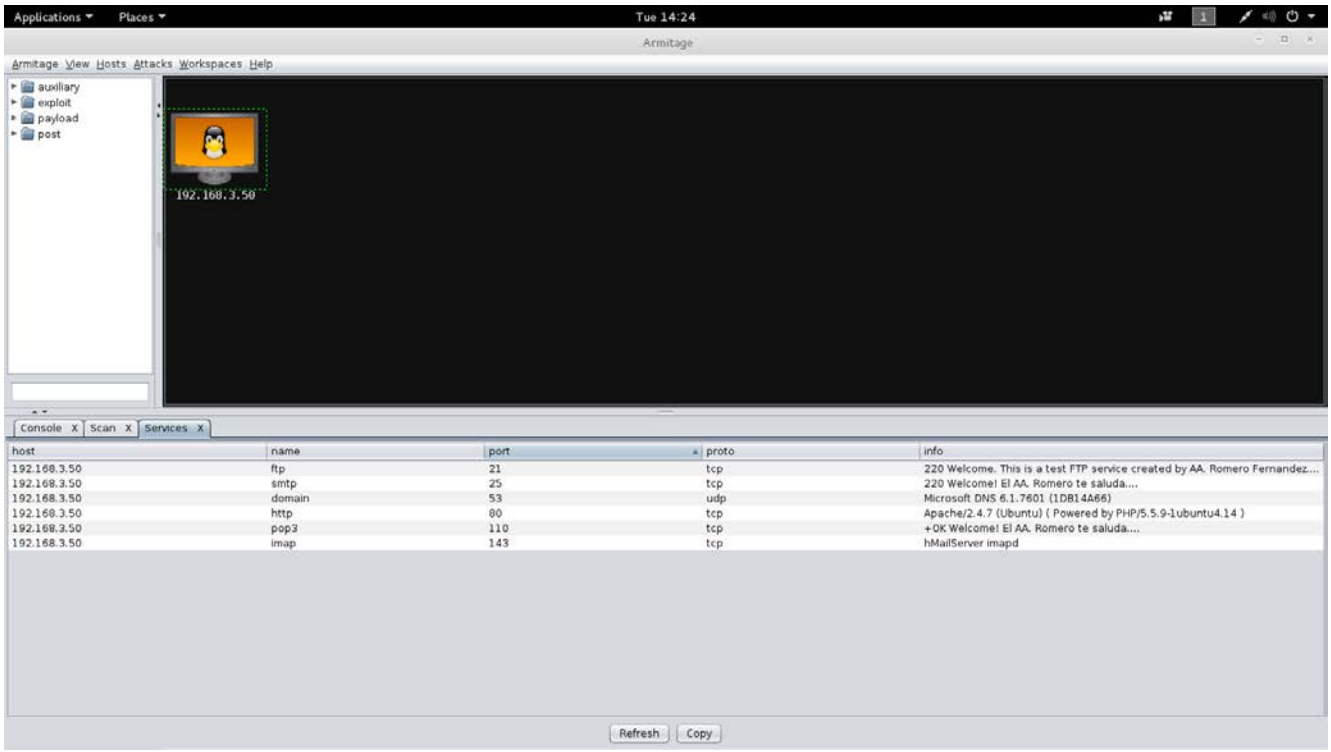

Figura 4-15: *Armitage*: objetivo y servicios identificados

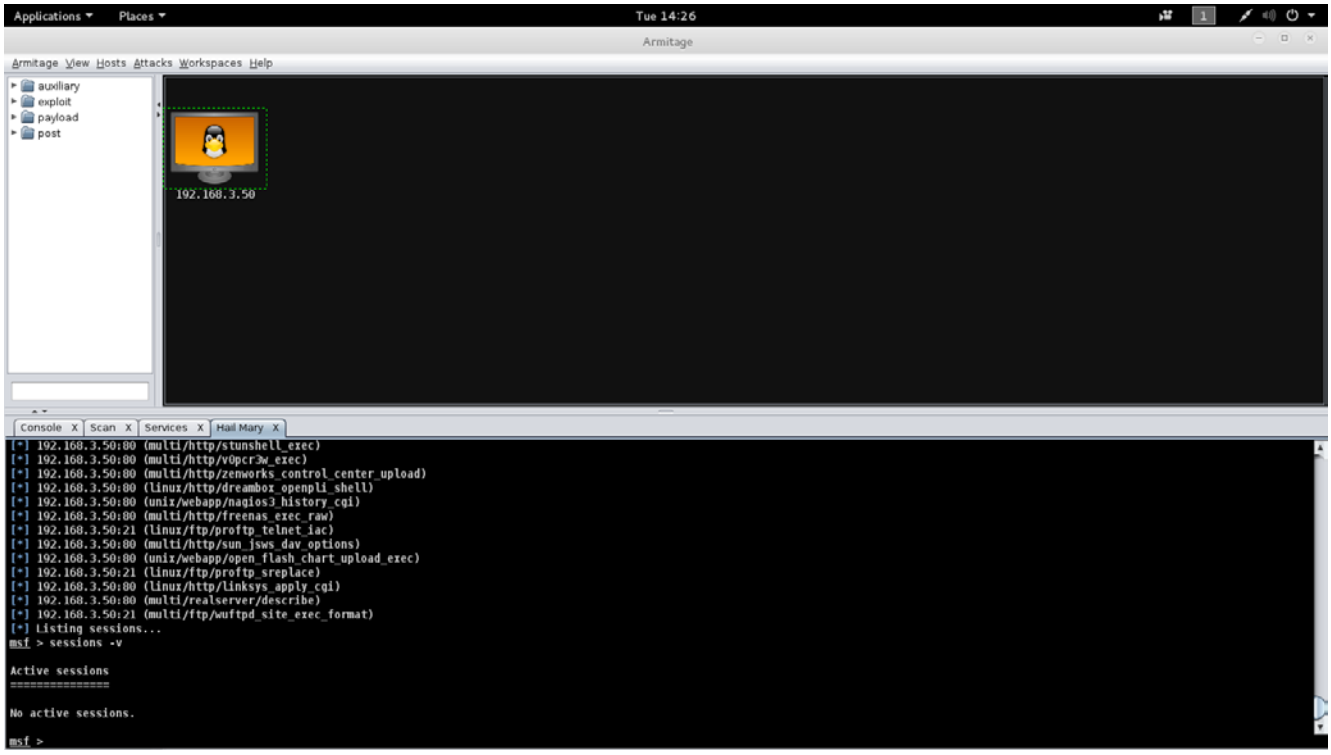

Figura 4-16: *Armitage:* Ataque fallido.

4.2.2 Desde LAN

La exploración con *nmap* y el posterior ataque con *Armitage* desde la red interna se han realizado arrancando la máquina virtual USER_WIN8.1_3 con un disco de *Kali Linux* en modo *Live*.

La exploración ha resultado más fructífera que la realizada desde fuera de la red local. En esta ocasión *nmap* ha encontrado más servicios en funcionamiento y puertos abiertos. Además, ha sido capaz de reconocer los diferentes sistemas operativos que ejecuta cada máquina. Sin embargo, la topología de red que presenta *nmap* no es correcta (como se muestra en la Figura 4-17).

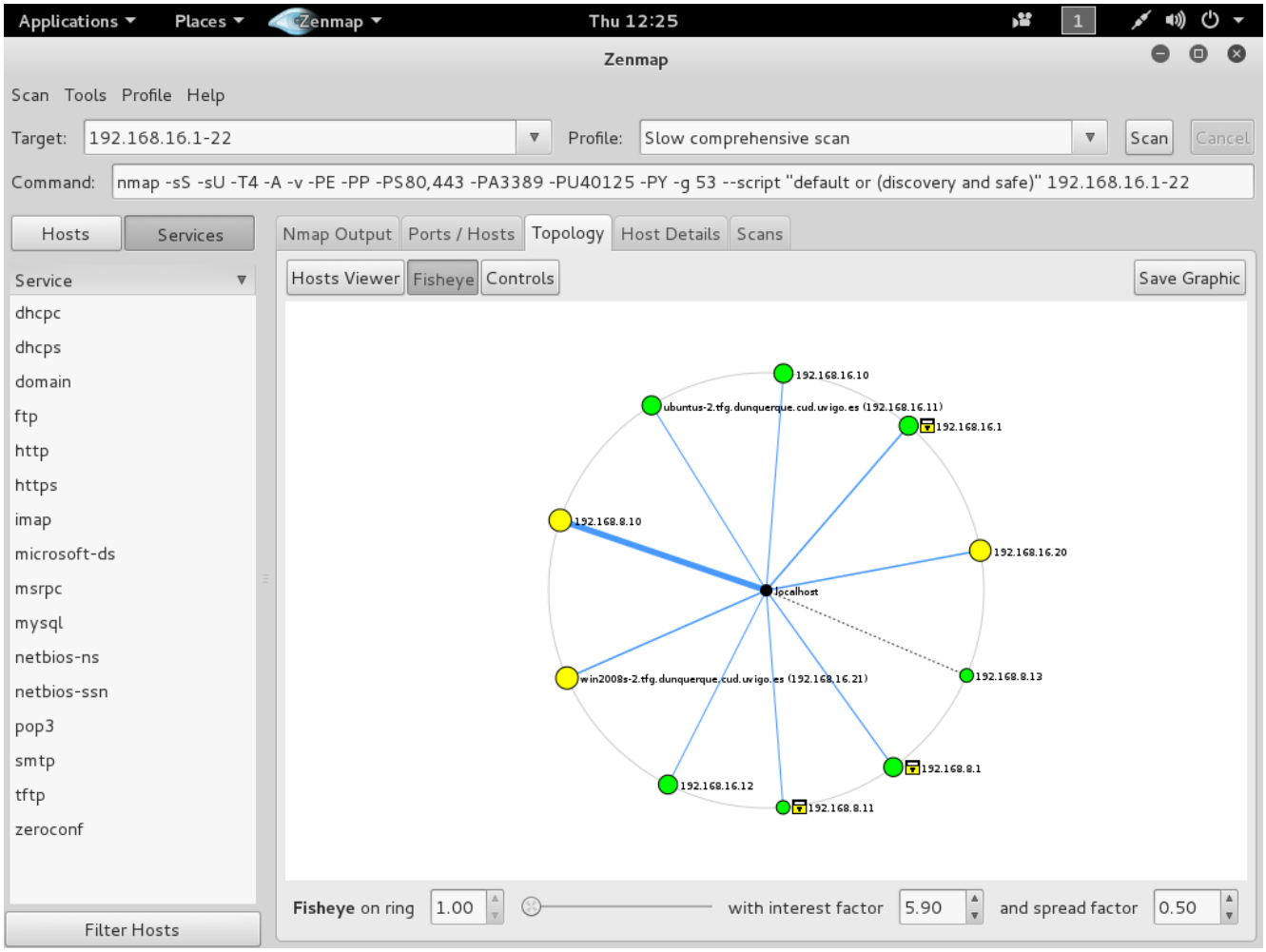

Figura 4-17: Topología de la red con *nmap*, resultado incorrecto

Debido a que la topología de red detectada por NMAP no es correcta con los análisis realizados anteriormente, se ha añadido a la lista de análisis uno del tipo *Quick traceroute*, con el cual el programa sí es capaz de detectar correctamente la topología (ver Figura 4-18).

Figura 4-18: Topología de la red con *nmap*, resultado correcto

El análisis de *nmap* ejecutado desde la red interna muestra considerablemente más información que el ejecutado desde el exterior, señal inequívoca de que el cortafuegos está realizado su labor correctamente. En las Figuras 4-19, 4-20 y 4-21 se puede ver respectivamente la información obtenida de cada servicio en funcionamiento y datos relativos a la máquina cortafuegos. En este caso, *nmap* sí ha podido identificar correctamente el sistema operativo del cortafuegos. Los archivos de salida de *nmap* se adjuntan en el disco que acompaña al trabajo.

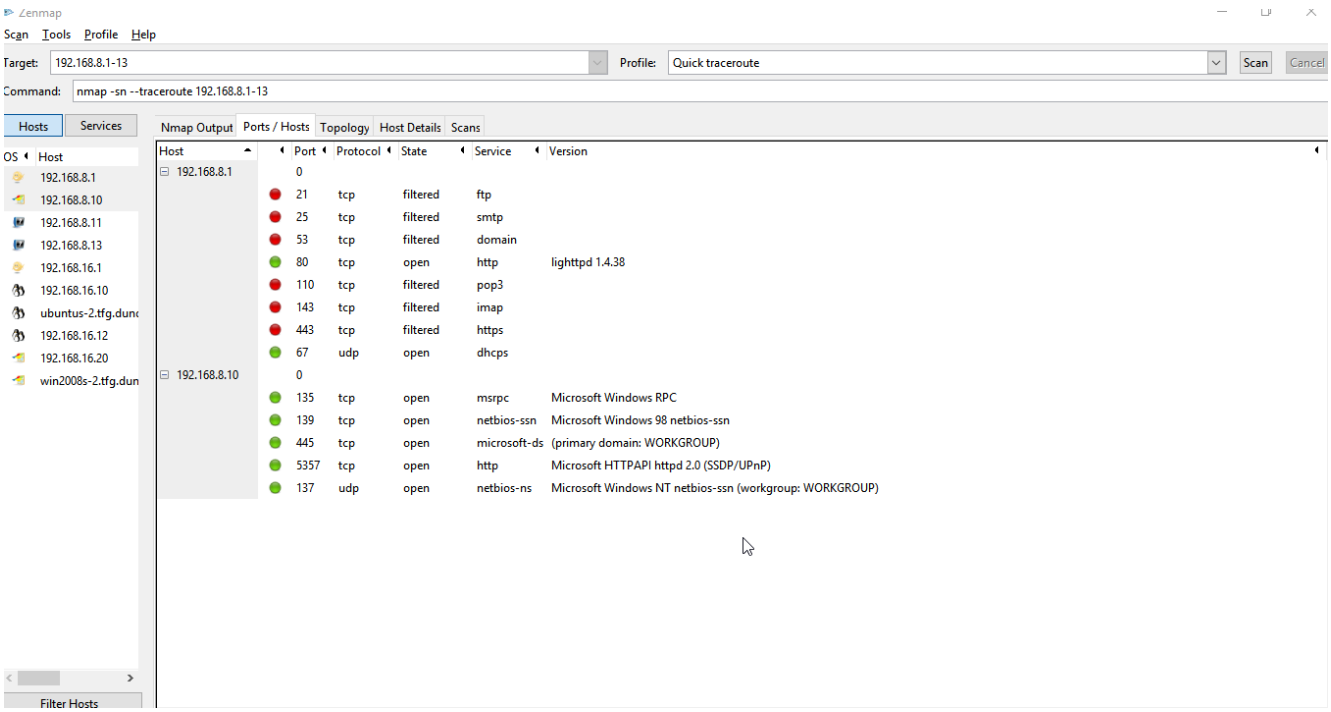

Figura 4-19: Puertos abiertos por cada *Host* I

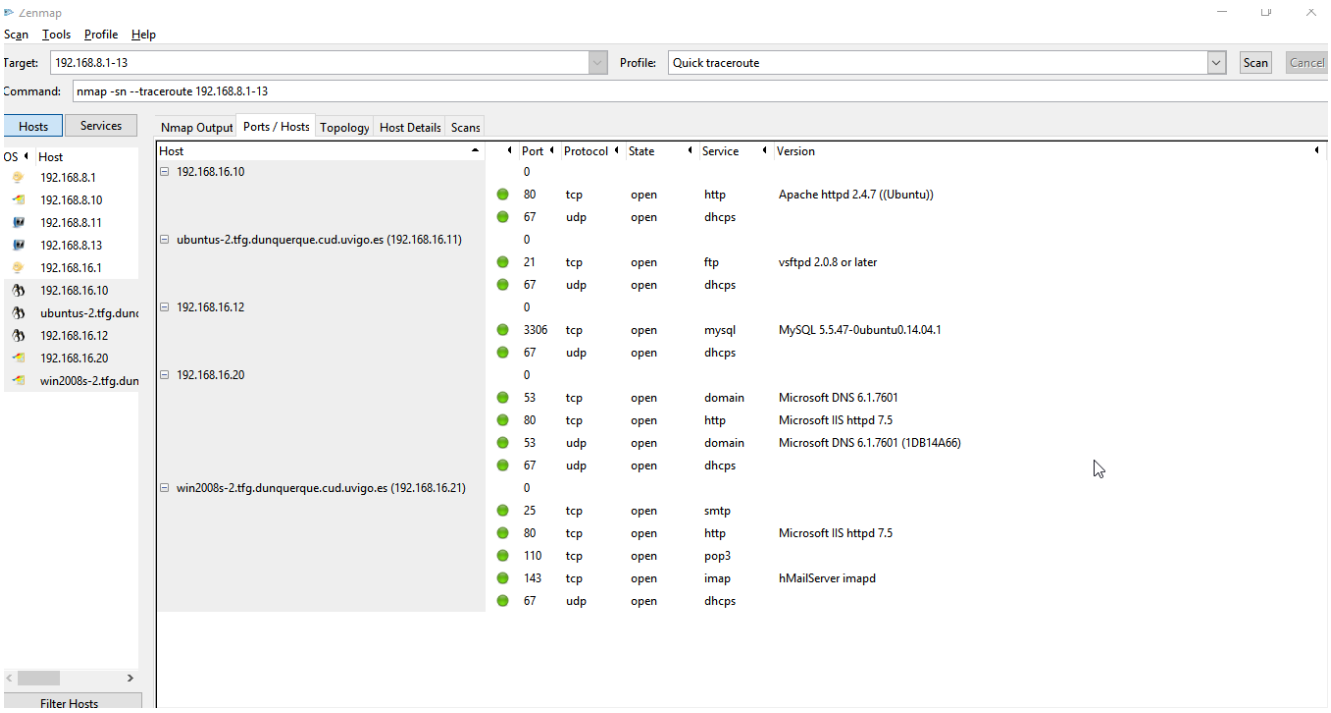

Figura 4-20: Puertos abiertos por cada *Host* II

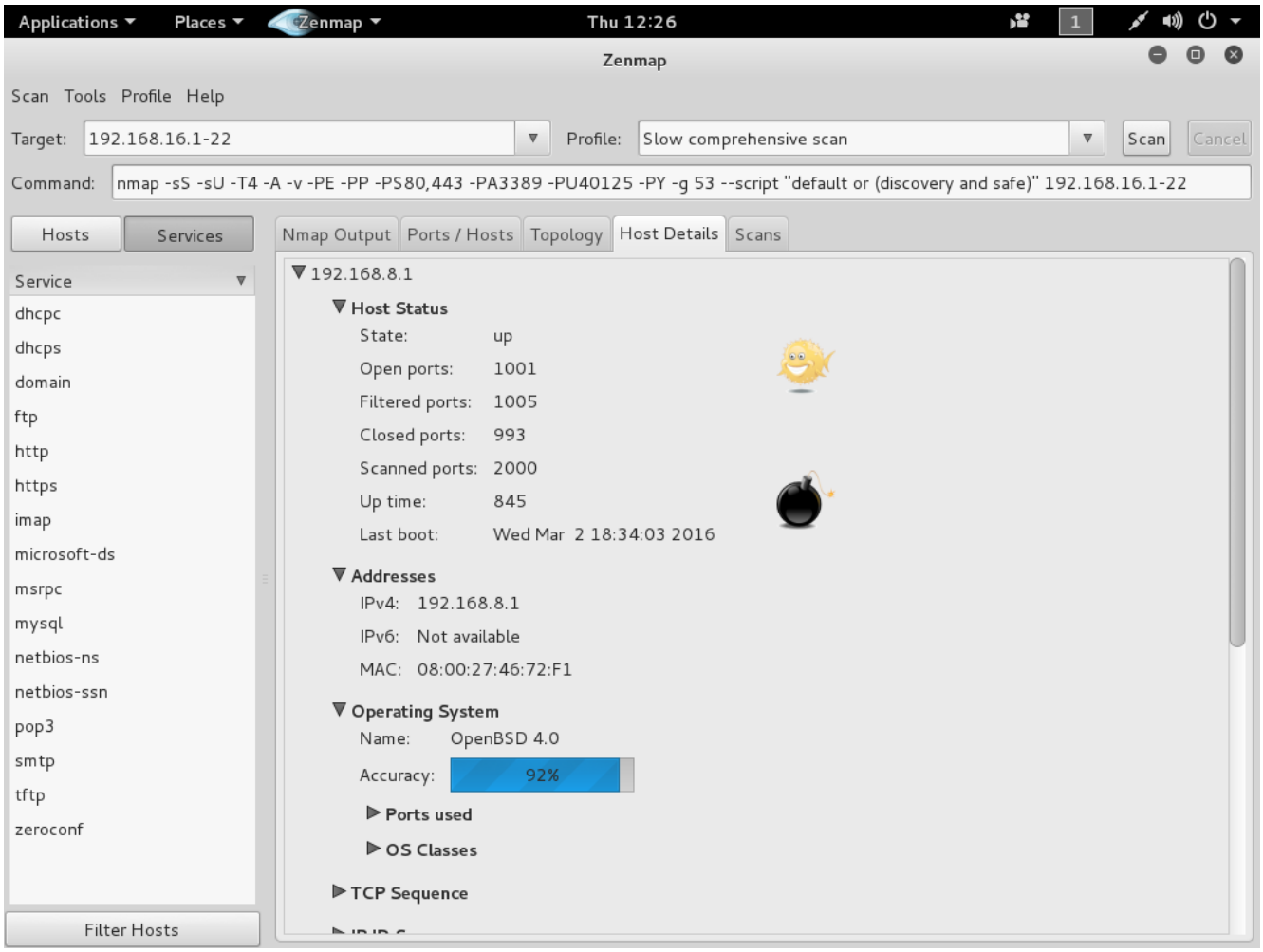

Figura 4-21: Información relativa a la máquina cortafuegos

Con la información obtenida con *nmap*, se procede a hacer el análisis con *Armitage* (ver Figura 4-22) para el posterior ataque *Hail Mary*. A pesar de disponer de abundante información y de que *Armitage* haya obtenido numerosos datos de su análisis, el ataque resulta fallido y, como se observa en la Figura 4-23, no conseguimos abrir ninguna sesión remota con las máquinas de la red.

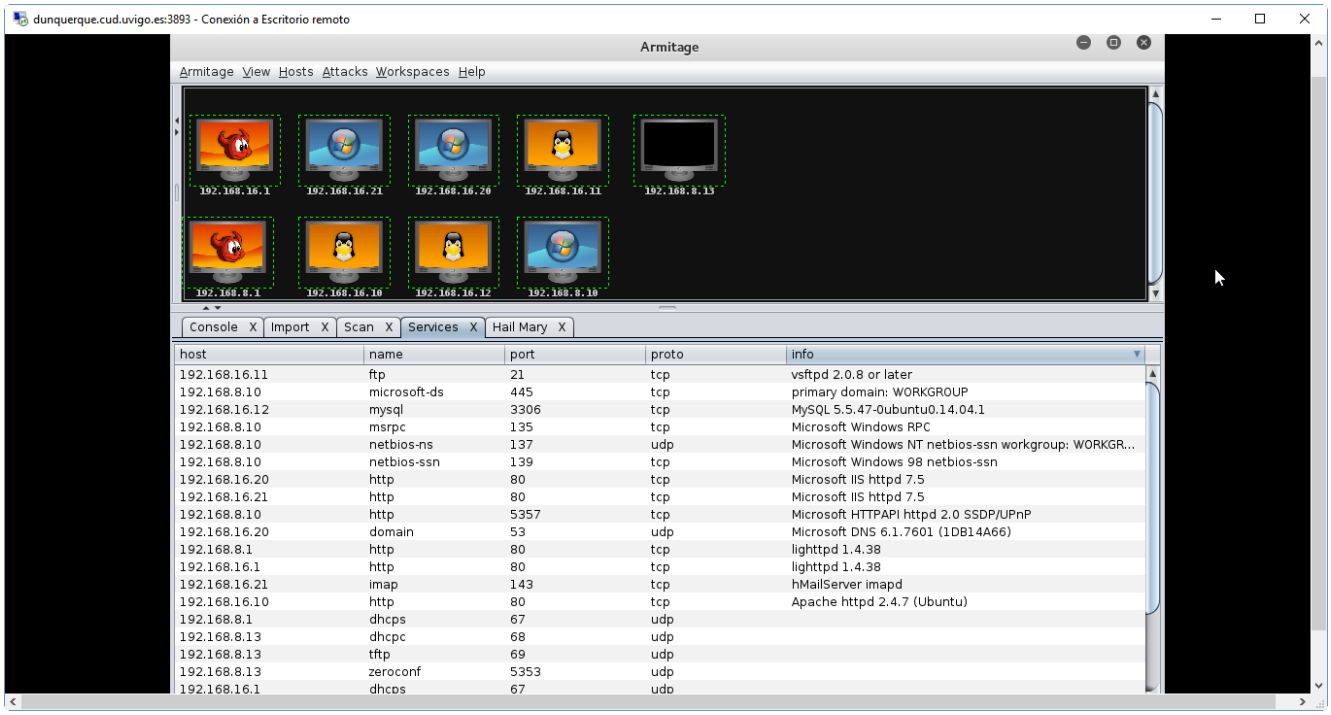

Figura 4-22: Servicios identificados por *Armitage*

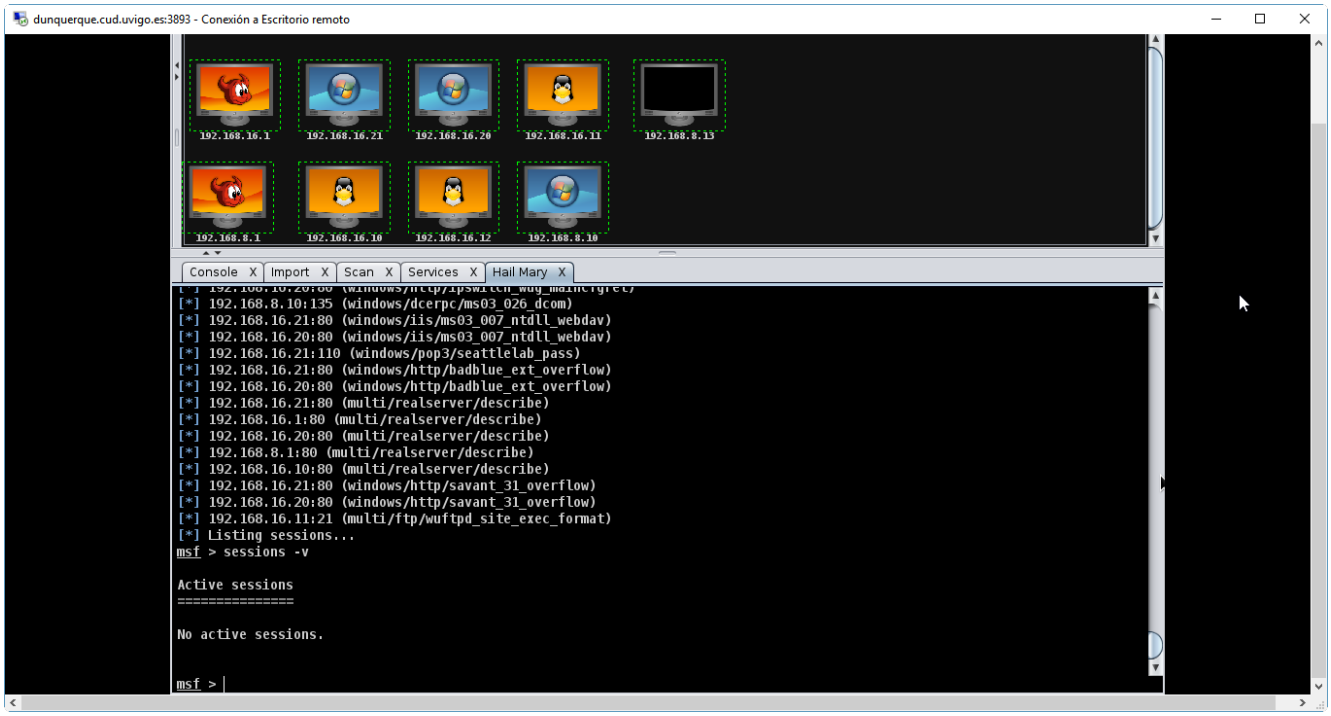

Figura 4-23: Ataque *Hail Mary* con *Armitage*

5 CONCLUSIONES Y LÍNEAS FUTURAS

Tras la realización del proyecto y analizando los resultados obtenidos es interesante presentar algunas conclusiones, así como proponer posibles líneas futuras de investigación.

5.1 Conclusiones

De los objetivos presentados en el apartado 1.4 se puede afirmar que se han cumplido la totalidad de ellos. En primer lugar, el desarrollo de la maqueta que se planteaba como objetivo principal ha tenido como resultado la implementación de la misma, que se encuentra correctamente funcionando. Las pruebas indican que el producto creado cumple con las especificaciones de ser una maqueta segura y estable, aunque es necesario realizar una auditoría de seguridad completa y mejorar las carencias encontradas para hacerla completamente segura. Durante las pruebas realizadas ha demostrado soportar la ejecución de diferentes herramientas de *pentesting* y no muestra diferencias con el comportamiento obtenido en una red real, por lo que la maqueta brinda la oportunidad de la realización de ejercicios en un entorno controlado y contenido, sin perder realismo.

Sería de gran satisfacción para el desarrollador su uso para la formación en técnicas de ciberdefensa y ciberataque de los futuros alumnos.

Como finalidad secundaria se proponía la contribución a la creación de una conciencia colectiva de ciberseguridad. Aún es pronto para poder determinar si la maqueta cumplirá el objetivo de concienciar a los que sean sus futuros usuarios, de que la red es un campo de batalla en el cual debemos protegernos continuamente para que nuestros datos no acaben en las manos de un ciberdelincuente. Por mi parte, sí puedo reseñar que durante la realización de este trabajo he adquirido la citada conciencia de ciberseguridad, o de inseguridad. El conocimiento de las técnicas necesarias para asegurar una red y del trabajo que esto acarrea me inclina a no menospreciar el trabajo de los técnicos de sistemas de informáticos y, por otra parte, a pensar que no es difícil que algo haya podido escapárseles. Por este motivo, considero que cualquier precaución es poca cuando estamos lidiando con una amenaza tan heterogénea como la que se presenta en Internet. Creo que no debemos dejar el trabajo de asegurar nuestros datos solamente en manos de los administradores de las redes, si no poner cada uno de nosotros una capa de protección que le ponga las cosas más difíciles a un posible atacante.

Además de lo anteriormente analizado, durante el desarrollo de este trabajo se han obtenido importantes conocimientos relativos al diseño e implementación de las arquitecturas de red más habituales en las corporaciones que creo necesario especificar en este documento. Se han obtenido conocimientos y experiencia en los campos relativos a la configuración de servidores web, FTP, de bases de datos, de resolución de nombres y de correo electrónico, que considero útiles y con grandes posibilidades de aplicación en un futuro próximo.

En la misma línea que el párrafo anterior, es una importante experiencia la configuración de un cortafuegos y la adquisición del conocimiento de su forma de trabajar. Bajo mi punto de vista, son un pilar fundamental en el funcionamiento de una red que tenga intención de ser medianamente segura. Además, una mala configuración de un cortafuegos puede proporcionar una falsa sensación de seguridad, más peligrosa si cabe que la ausencia de estos dispositivos.

En el campo de la seguridad informática, se ha obtenido conciencia de que es necesario prestar atención y tomar medidas para asegurar nuestros datos en la red, sin perder la capacidad de aprovechar los avances que las nuevas tecnologías nos brindan.

La experiencia rebate el falso mito que gira en torno a la virtualización, presente al menos fuera del entorno más especializado, de que no se obtiene buen rendimiento con sistemas virtualizados. Creo necesario reseñar que la pérdida de rendimiento experimentada al trabajar sobre máquinas virtuales ha sido baja y no ha afectado a la usabilidad.

También es reseñable la experiencia de administrar un servidor de forma remota y sus dificultades. En este aspecto toma especial relevancia el conocimiento del uso de la línea de comandos, ya que las conexiones no siempre permiten el trabajo mediante escritorio remoto.

5.2 Líneas futuras

Aunque se ha obtenido un prototipo funcional como resultado de este trabajo, dista mucho de estar completamente desarrollado. Las siguientes líneas de investigación proponen funcionalidades cuyo desarrollo no ha podido tener lugar en este trabajo pero son útiles o necesarias para obtener un producto final completamente desarrollado.

1. Diseño e implementación de un conjunto de herramientas que permita auditar la red en tiempo real, de forma que el director de un ejercicio tenga información de los avances del mismo.
2. Creación de otros escenarios, por ejemplo, una maqueta de la red corporativa del Ministerio de Defensa.
3. Diseño e implementación de un entorno gráfico que permita la configuración de la maqueta y su administración de una forma más amigable para el usuario.
4. Diseño e implementación de software que permita simular una utilización real de los recursos de la maqueta; ya que actualmente la maqueta tiene los servicios disponibles pero no hay tráfico real en la red.
5. Diseño de un entorno que agrupe las funcionalidades anteriores una vez desarrolladas para obtener una herramienta completa que permita el diseño, ejecución y observación de ejercicios de ciberseguridad y ciberdefensa.

6 BIBLIOGRAFÍA

[1] J. C. R. Licklider, Man-Computer Simbiosis, 1960.

[2] Internet World Stats, [En línea]. Available: http://www.internetworldstats.com. [Último acceso: 2016 01 26].

[3] M. Jasra, «Webanalyticsworld.net» 03 11 2010. [En línea]. Available: http://www.webanalyticsworld.net/2010/11/google-indexes-only-0004-of-all-data-on.html. [Último acceso: 2016 02 26].

[4] A. R. Varon, «Antonio Ramos, hacker y experto en seguridad informática de StackOverflow» *Emprendedores.es,* 9 6 2015.

[5] R. A. Clarke y R. K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It,* Ecco, 2011.

[6] V. Martínez, «63 'ciberataques' en lo que va de año contra infraestructuras críticas del Estado,» *El Mundo.es,* vol. http://www.elmundo.es/economia/2015/10/26/562cf6c0e2704e21798b45bb.html, 26 10 2015.

[7] *The Onion Router, «Tor project»* [En línea]. Available: https://www.torproject.org/. [Último acceso: 23 02 2016].

[8] *Computer Emergence Response Team* - Centro Criptologico Nacional (CCN-CERT), CCN-CERT IA-09/15: Ciberamenazas 2014, tendencias 2015. Resumen ejecutivo, 2015.

[9] Centro Superior de Estudios de la Defensa Nacional (CESEDEN), El ciberespacio. Nuevo escenario de confrontación, 2012.

[10] NATO, *«Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization»* Lisboa, 2010.

[11] Comité Internacional de la Cruz Roja; Federación Internacional de sociedades de la Cruz Roja y Media Luna Roja, «Informe de la XXXI Conferencia Internacional de la Cruz Roja y la Media Luna Roja» Ginebra, 2011.

[12] C. A. Elias y A. P. V. Ortiz, «La ciberdefensa y sus dimensiones global y específica en la estrategia de seguridad nacional española» *Icade. Revista cuatrimestral de las facultades de*

Derecho y Ciencias Económicas y Empresariales, nº 92, pp. 48-77, Agosto 2014.

[13] La revista de la OTAN, «Nuevas amenazas: el ciberespacio,» 2011.

[14] L. O'Murchu, «*Last-minute paper: An indepth look into Stuxnet*» VirusBulletin, 2010. [En línea]. Available https://www.virusbulletin.com/conference/vb2010/abstracts/indepth-look-stuxnet: [Último Acceso: 2016 03 29].

[15] The White House, *The national strategy to secure the cyberspace* Washington, 2003. [En línea]. Available: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf [Último Acceso: 2016 03 29].

[16] U.S Department of Homeland Security, *National Infrastructure Protection Plan*, 2006. [En línea]. Available: https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf[Último Acceso: 2016 03 29].

[17] The White House, *The Comprehensive National Cybersecurity Initiative*, 2008. [En línea]. Available: https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative [Último Acceso: 2016 03 29].

[18] Ministerio de Defensa, «Documento informativo del IEEE 09/2011: Nuevo concepto de ciberdefensa de la OTAN (Marzo 2011)» 2011. [En línea]. Available: http://www.ieee.es/Galerias/fichero/docs_informativos/2011/DIEEEI09-2011ConceptoCiberdefensaOTAN.pdf [Último Acceso: 2016 03 29].

[19] Unión Europea, Estrategia de Ciberseguridad en la Union Europea: un ciberespacio abierto, seguro y protegido, 2013. [En línea]. Available: http://www.consilium.europa.eu/es/policies/cyber-security/ [Último Acceso: 2016 03 29].

[20] Gobierno de España, Plan Nacional de Seguridad, 2013. [En línea]. Available: http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf

[21] Presidencia del Gobierno, Gobierno de España, Plan Nacional de Ciberdefensa, 2013. [En línea]. Available: http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf [Último Acceso: 2016 03 29].

[22] Indra company (Proyecto SACO), [En línea]. Available: http://www.indracompany.com/en/sostenibilidad-e-innovacion/proyectos-innovacion/saco-simulador-avanzado-para-la-ciberdefensa-organi. [Último Acceso: 2016 03 29].

[23] Ministerio de Defensa, «Resolución 420/38007/2016,» de *Boletín Oficial del Estado num.19*, vol. III. Otras disposiciones, 2016, p. 5944.

[24] A. S. Tanenbaum y D. J. Wetherall, *Computer Networks 5th edition*, Pearson , 2011, .

[25] Irochka, Virtualizacion corporativa con VMware, Torredembarra: lulu.com, 2009.

[26] T. M. Jones, «*IBM Bluemix*» [En línea]. Available: http://www.ibm.com/developerworks/ssa/library/l-hypervisor/index.html. [Último acceso: 21 01 2016].

[27] Blog *DesdeLinux*: Usemos *Linux* para ser libres.[En línea]. Available: http://blog.desdelinux.net. [Último acceso: 2016 01 26].

[28] Microsoft Hyper V Server, [En línea]. Available: https://www.microsoft.com/OEM/es/PRODUCTS/servers/Pages/hyper_v_server.aspx#fbid=NUfwWalzsnC. [Último Acceso: 2016 03 29].

[29] Citrix, [En línea]. Available: https://www.citrix.es/products/xenserver/overview.html. [Último Acceso: 2016 03 29].

[30] Vmware, [En línea]. Available: https://www.vmware.com/es/products/esxi-and-esx/overview. [Último Acceso: 2016 03 29].

[31] B. S. Ramirez Sierra, *Cloud Computing GRID*, Universidad del Quindio, 2014.

[32] Oracle VirtualBox, [En línea]. Available: https://www.virtualbox.org/. [Último Acceso: 2016 03 29].

[33] Vmware, [En línea]. Available: https://www.vmware.com/es/products/. [Último Acceso: 2016 03 29].

[34] QEMU, [En línea]. Available: http://wiki.qemu.org/Main_Page. [Último Acceso: 2016 03 29].

[35] Linux-KVM, [En línea]. Available: http://www.linux-kvm.org/page/Main_Page. [Último Acceso: 2016 03 29].

[36] Xen Project, «*Xen Project Beginners Guide*» 2015. [En línea]. Available: http://wiki.xenproject.org/wiki/Xen_Project_Beginners_Guide. [Último acceso: 21 01 2016].

[37] Microsoft, [En línea]. Available: https://www.microsoft.com/en-us/download/details.aspx?id=3702. [Último Acceso: 2016 03 29].

[38] Oracle, Virtualbox user manual, 2016.

[39] VMware, *Guide to New Product and Service Names*, https://www.vmware.com/files/pdf/products/vmware-guide-to-new-product-and-service-names.pdf ed. [Último Acceso: 2016 03 29].

[40] VMware, *VMware Vsphere 6.0 Release Notes*, https://www.vmware.com/support/vsphere6/doc/vsphere-esxi-vcenter-server-60-release-notes.html ed., 2015. [Último Acceso: 2016 03 29].

[41] *CISCO Networking Academy*, [En línea]. Available: https://www.netacad.com/about-networking-academy/packet-tracer/.[Último Acceso: 2016 03 29].

[42] *Graphical Network Simulator,* [En línea]. Available: https://www.gns3.com/.[Último Acceso: 2016 03 29].

[43] «*Infra engineering Blog*» [En línea]. Available: http://infra-engineering.blogspot.com. [Último acceso: 23 02 2016].

[44] NETGUI, [En línea]. Available: http://mobiquo.gsyc.es/netgui/LEEME. [Último Acceso: 2016 03 29].

[45] «Software Libre Blog,» [En línea]. Available: http://sw-libre.blogspot.es. [Último acceso: 23 02 2016].

[46] Storage Review.com, «*Dell Poweredge r530 review*» [En línea]. Available: http://www.storagereview.com/dell_poweredge_13g_r530_review. [Último acceso: 04 03

2016].

[47] Ubuntu, «*Ubuntu server 14.04 LTS Realse Notes*» [En línea]. Available: https://wiki.ubuntu.com/TrustyTahr/ReleaseNotes?_ga=1.160245629.1922354801.1455638121. [Último acceso: 2016 03 23].

[48] Open SUSE, «*Open SUSE: Leap portal*» [En línea]. Available: https://en.opensuse.org/Portal:Leap. [Último acceso: 2016 03 23].

[49] J. Neuman, «*GNS3 Support: Installing linux from sources*» [En línea]. Available: https://gns3.com/support/docs/installing-gns3-1-4-on-ubuntu-li. [Último acceso: 02 2016].

[50] Apache, «*Apache HTTP server project*» [En línea]. Available: https://httpd.apache.org/. [Último acceso: 2016 03 01].

[51] Joomla , «*Joomla project: The CMS trusted by millions for their websites.*» [En línea]. Available: https://www.joomla.org/. [Último acceso: 2016 03 01].

[52] RainLoop, «*RainLoop Webmai,*» [En línea]. Available: http://www.rainloop.net/. [Último acceso: 2016 03 01].

[53] Phpmyadmin, «*Phpmyadmin: Bringing MySQL to the web*» [En línea]. Available: https://www.phpmyadmin.net/. [Último acceso: 2016 03 01].

[54] MySQL, «*MySQL: The world's most popular open source database*» [En línea]. Available: https://www.mysql.com/. [Último acceso: 2016 03 01].

[55] C. Evans, «*vsftpd: Probably the most secure and fastest FTP server for UNIX-like systems.*» [En línea]. Available: https://security.appspot.com/vsftpd.html. [Último acceso: 2016 03 01].

[56] hMailserver, «*hMailserver: Free open source email server for Microsoft Windows*» [En línea]. Available: https://www.hmailserver.com/. [Último acceso: 2016 03 01].

Anexo I: Instalación de los diferentes sistemas operativos hospedados

En este anexo se incluye una guía para la realización de la instalación y la configuración inicial de los sistemas operativos usados en las máquinas virtuales de la maqueta.

A-I.1 Ubuntu Server 14.01 LTS

Una vez configurada la máquina virtual correspondiente, en el primer inicio, VirtualBox avisa de que no hay ningún dispositivo arrancable y permite seleccionar un archivo de imagen de disco ISO para ser montado en la unidad de DVD de la máquina virtual. La ISO de *Ubuntu Server 14.04* puede ser descargada de la página web oficial.

Con la ISO montada, la máquina virtual arranca y presenta el menú de la Figura A1-1.

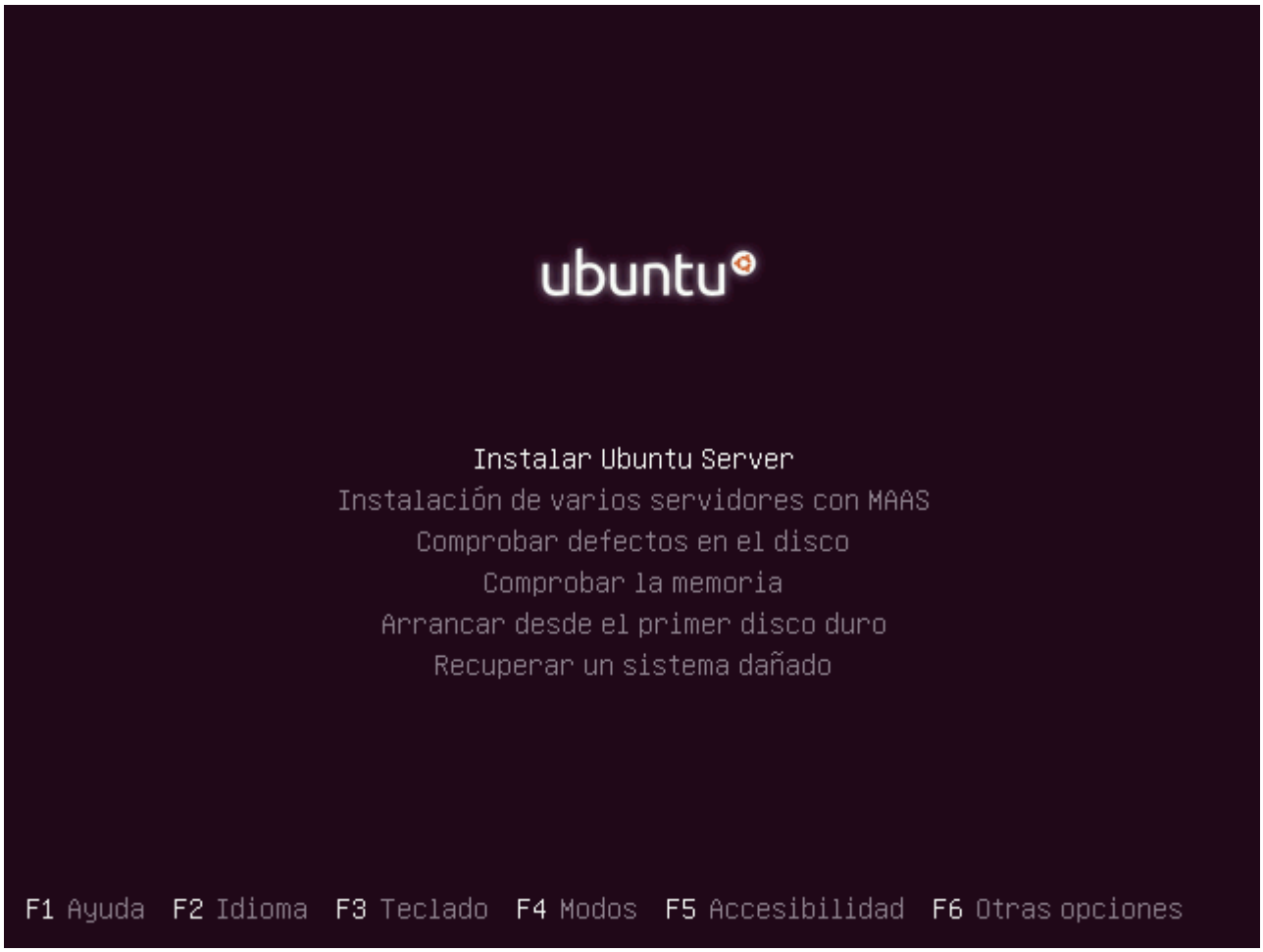

Figura A1-1: Menú de inicio del disco de *Ubuntu Server*

En los primeros pasos del asistente textual, se deben seleccionar las opciones relativas al idioma, la localización y la distribución del teclado (ver Figura A1-2).

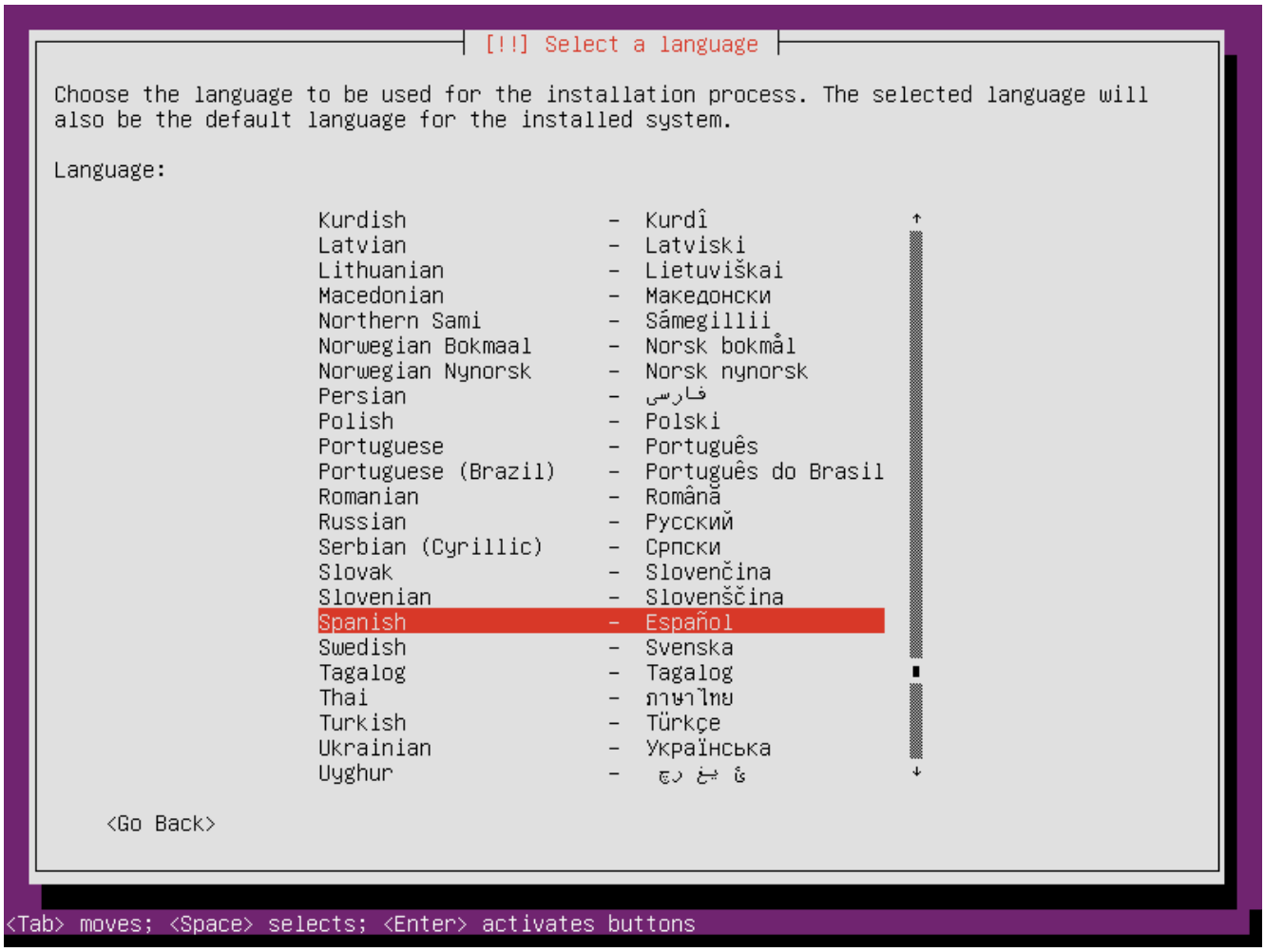

Figura A1-2: Elección de idioma de instalación de *Ubuntu Server*

Posteriormente se solicita la introducción del nombre de la máquina, el del usuario del sistema y su contraseña (véase Figura A1-3).

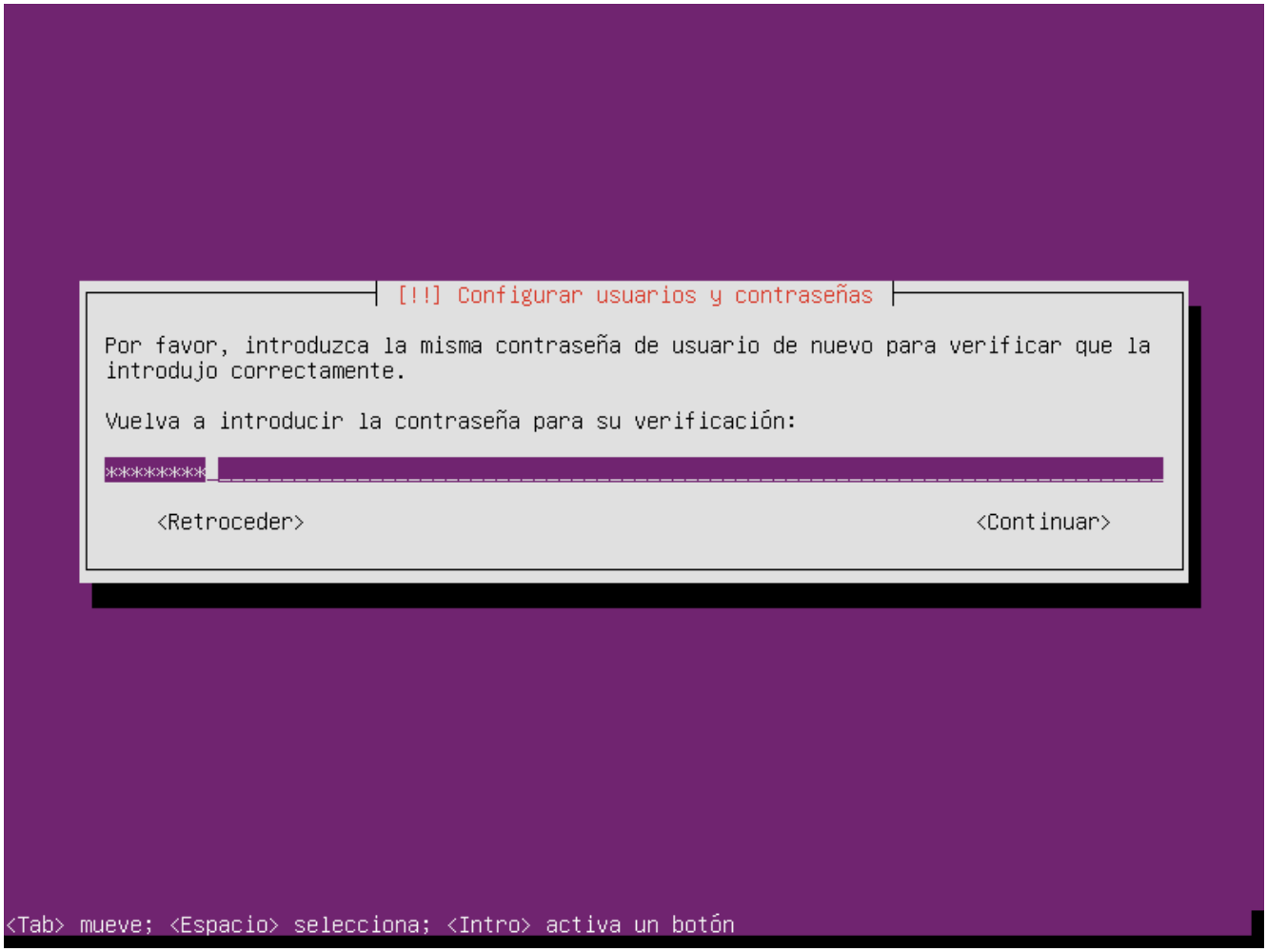

Figura A1-3: Introducción de contraseña para nuevo usuario

Avanzando en el asistente, se pedirá que confirmemos la zona horaria y que elijamos si queremos configurar el cifrado de la carpeta personal. A esta última pregunta responderemos *No*. Posteriormente el asistente presenta las opciones de particionado. Dado que estamos instalando el sistema operativo en una máquina virtual dedicada para él, el sistema operativo usará el disco duro completo, como se indica en la Figura A1-4.

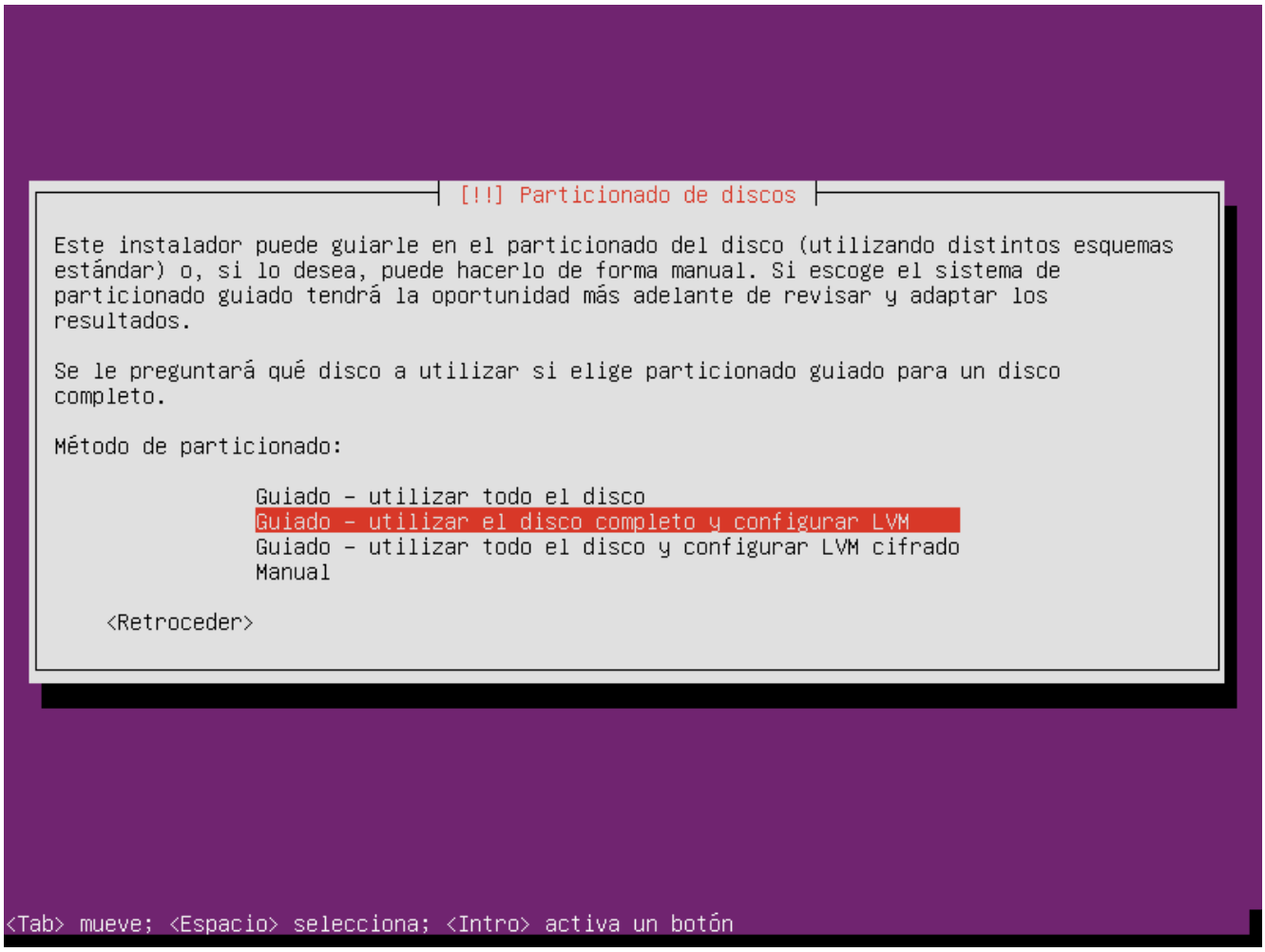

Figura A1-4: Selección de método de particionado

Se nos ofrecerá la configuración propuesta para las particiones, que aceptaremos (ver Figura A1-5).

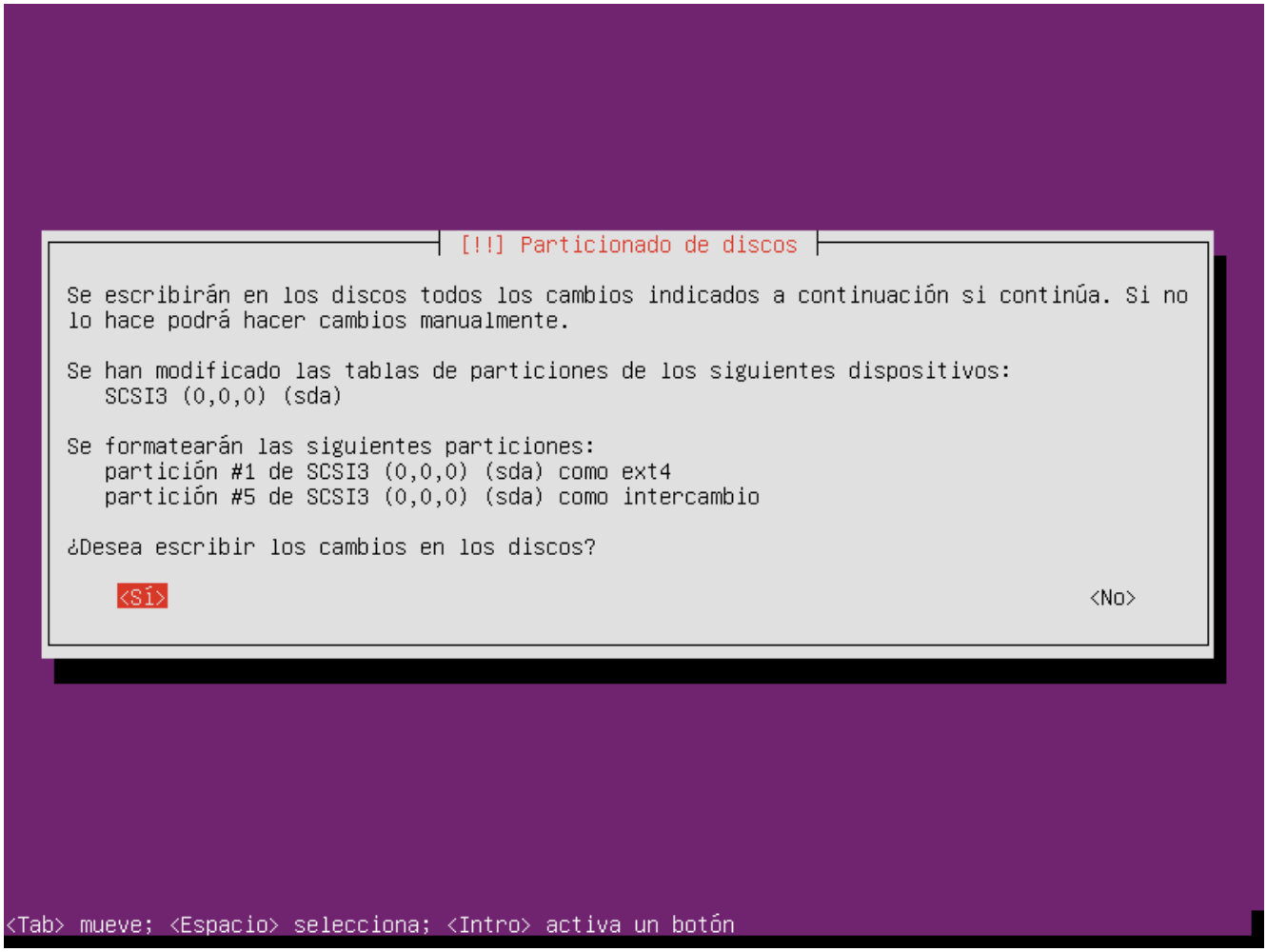

Figura A1-5: Resumen de particionado para *Ubuntu Server*

En este momento, el asistente preguntará por la configuración del proxy HTTP, que se dejará en blanco. También presentará varias opciones relativas a las actualizaciones automáticas. En este caso, se elige la opción *Sin actualizaciones automáticas.*

Tras finalizar la instalación del sistema operativo, se puede elegir instalar algunos servicios automáticamente. En este caso no se selecciona ninguno, ya que la máquina virtual será clonada para la instalación de diferentes servicios con posterioridad.

Por último, el asistente pide autorización para instalar el cargador de arranque (véase Figura A1-6).

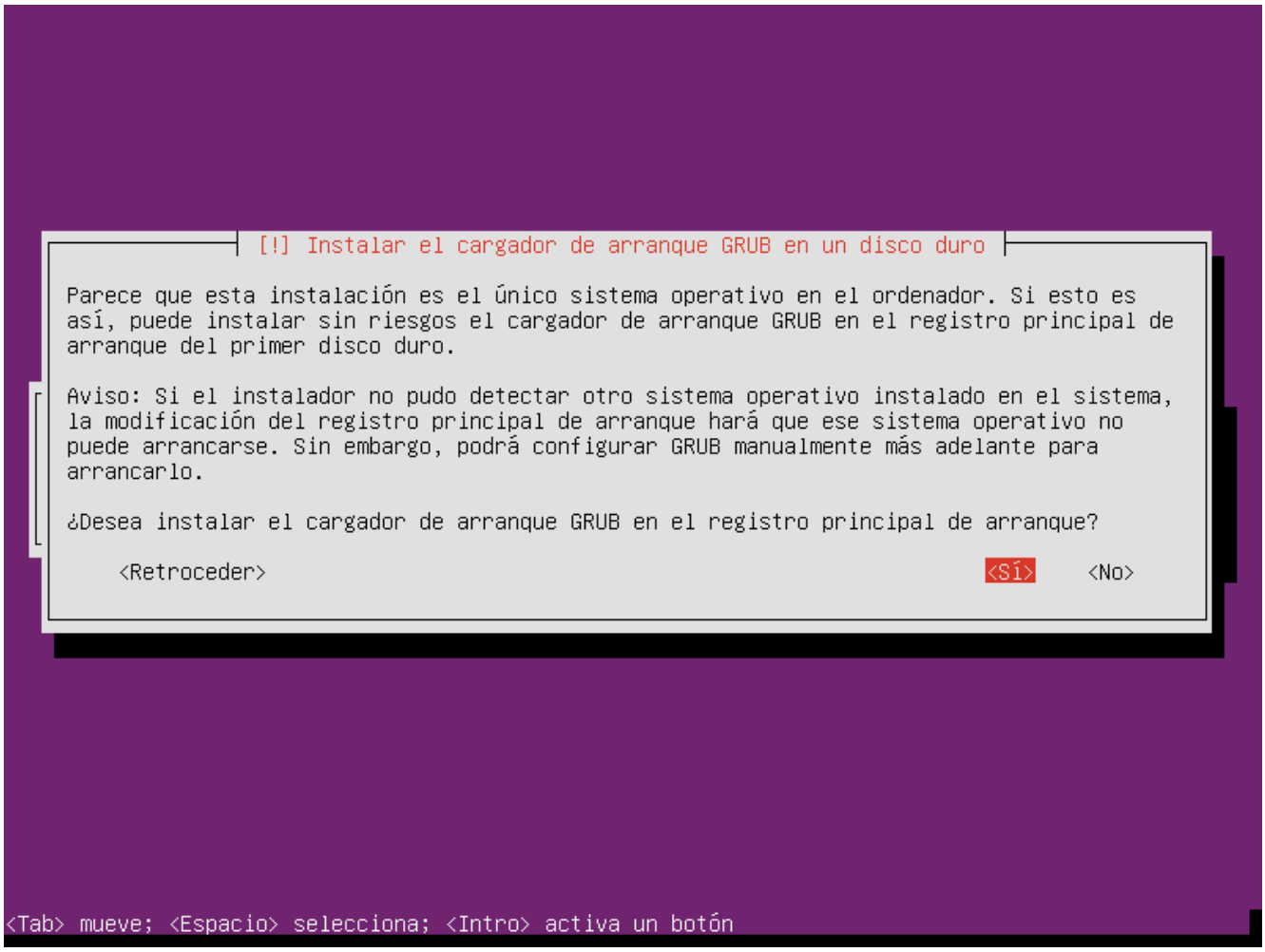

Figura A1-6: Instalación del cargador de arranque para *Ubuntu Server*

Cuando finaliza la instalación de GRUB, la imagen de disco se desmonta automáticamente. La máquina virtual se reinicia y el sistema operativo está instalado.

A-I.2 Windows Server 2008

Una vez configurada la máquina virtual correspondiente, en el primer inicio, VirtualBox avisa de que no hay ningún dispositivo arrancable y permite seleccionar un archivo de imagen de disco ISO para ser montado en la unidad de DVD de la máquina virtual. La ISO de *Windows Server 2008R2* ha sido proporcionada por la Universidad de Vigo que dispone de una licencia para uso corporativo.

Una vez montada la ISO, la máquina virtual arranca y carga el instalador gráfico de Microsoft. El primer paso del instalador es seleccionar el idioma y la distribución del teclado (ver Figura A1-7).

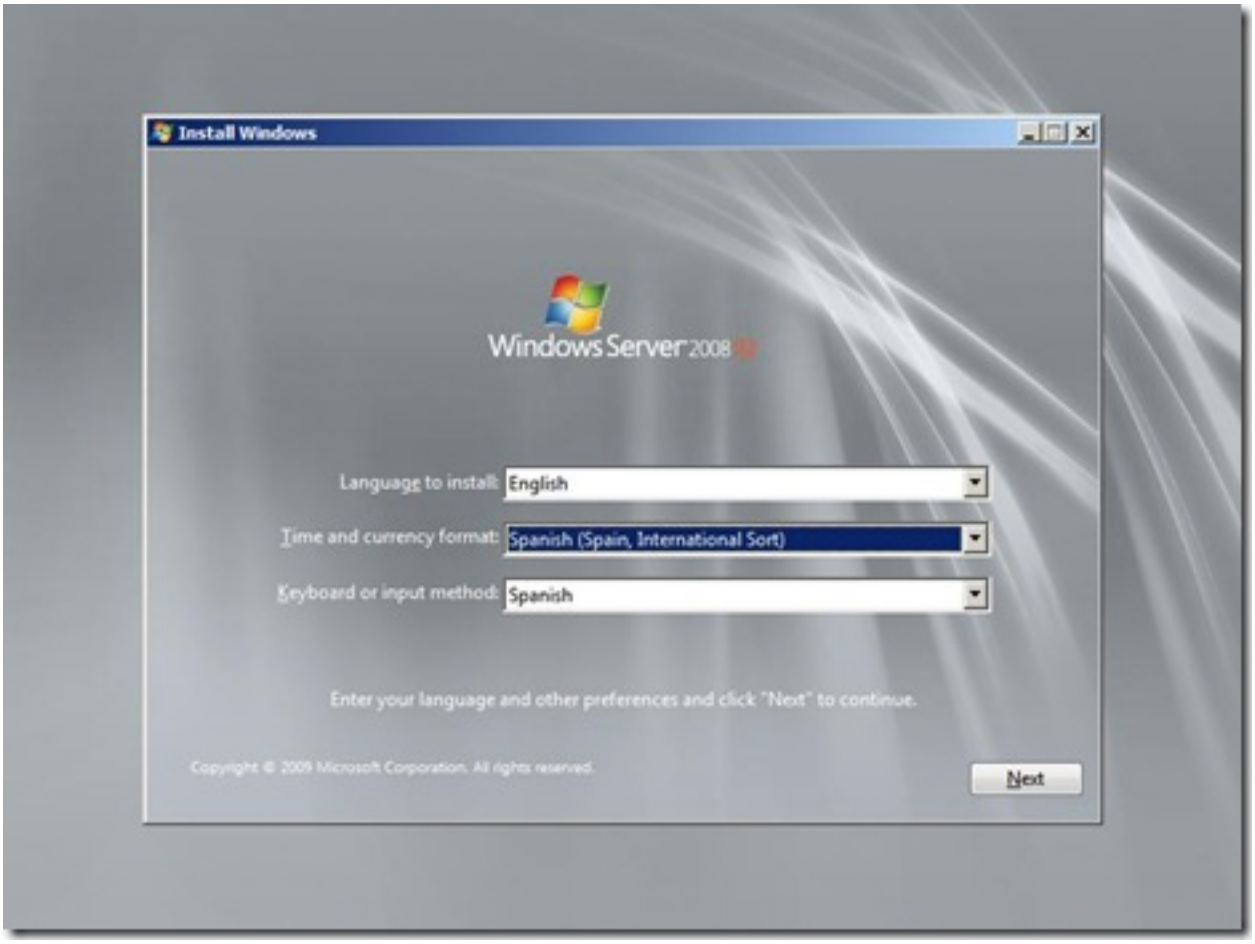

Figura A1-7: Selección de idioma y distribución de teclado para instalación de Windows Server

Una vez seleccionado el idioma es el momento de seleccionar la versión a instalar. En nuestro caso, se va a instalar la versión *Standard* de 64 bits (Figura A1-8).

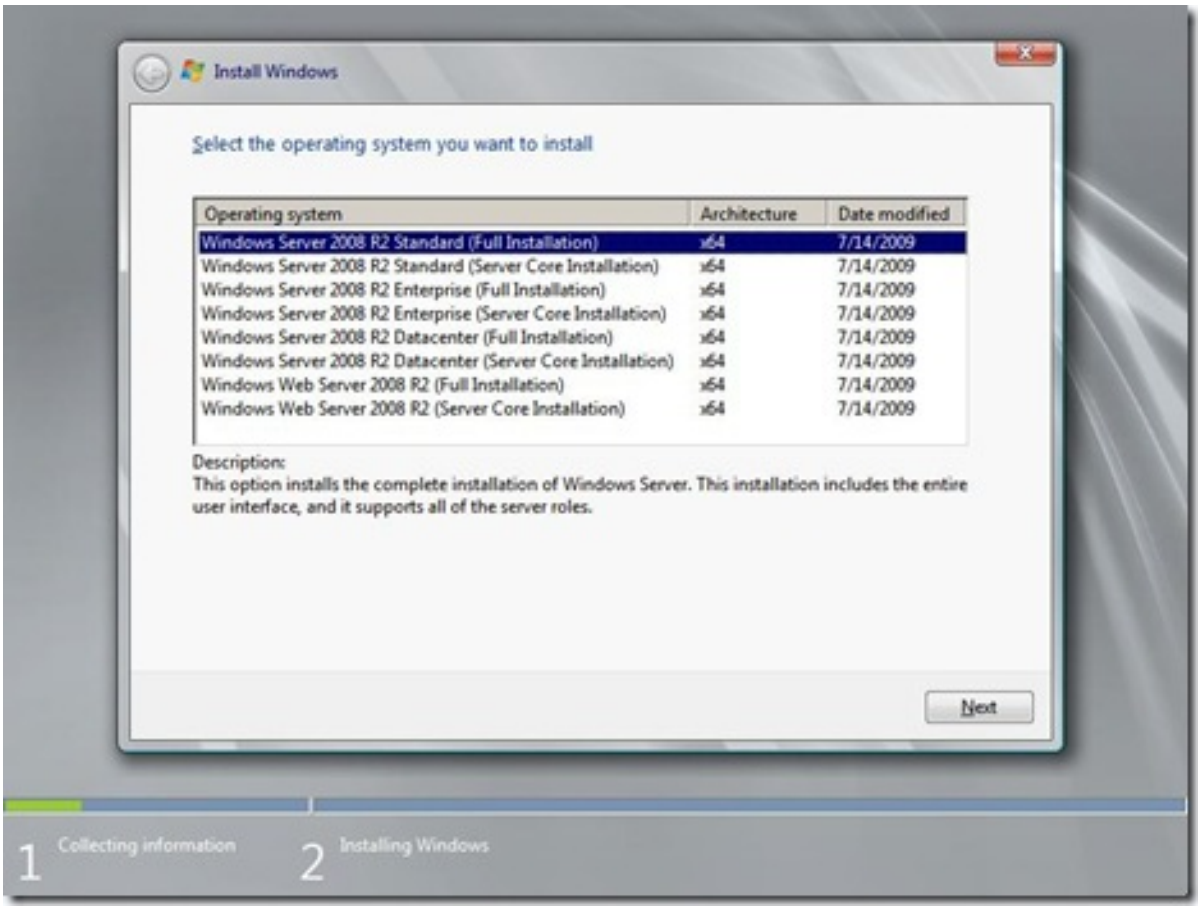

Figura A1-8: Selección de la versión de Windows Server a instalar

Tras aceptar los términos de la licencia, se elige la opción de instalación nueva y se selecciona el disco duro de la máquina virtual al completo (ver Figura A1-9).

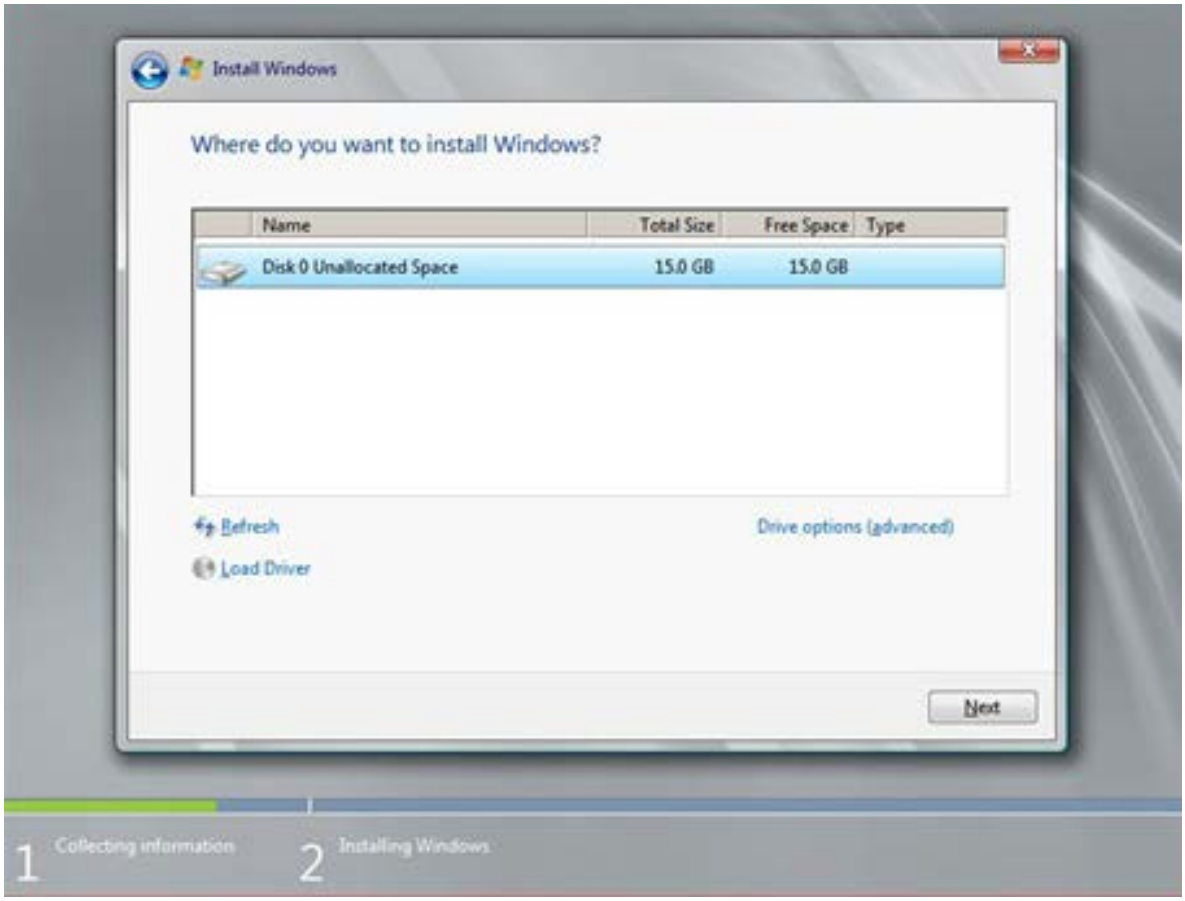

Figura A1-9: Particionado del disco duro

Tras esto comienza la instalación del sistema operativo, que finaliza con la petición para cambiar la contraseña de administrador (véase Figura A1-10). Debido a la política de seguridad de *Windows Server*, la contraseña debe contener letras, números y caracteres especiales.

Figura A1-10: Cambio de la contraseña de administrador

Un reinicio completa la instalación, tras la cual es necesario desmontar la imagen de disco de la unidad de DVD virtual.

A-I.3 Windows 8.1

Una vez configurada la máquina virtual correspondiente, en el primer inicio, VirtualBox avisa de que no hay ningún dispositivo arrancable y permite seleccionar un archivo de imagen de disco ISO para ser montado en la unidad de DVD de la máquina virtual. La ISO de *Windows 8* ha sido proporcionada por la Universidad de Vigo que dispone de una licencia para uso corporativo.

Una vez montada la ISO, la máquina virtual arranca y carga el instalador gráfico de Microsoft. El primer paso del instalador es seleccionar el idioma y la distribución del teclado (ver Figura A1-11).

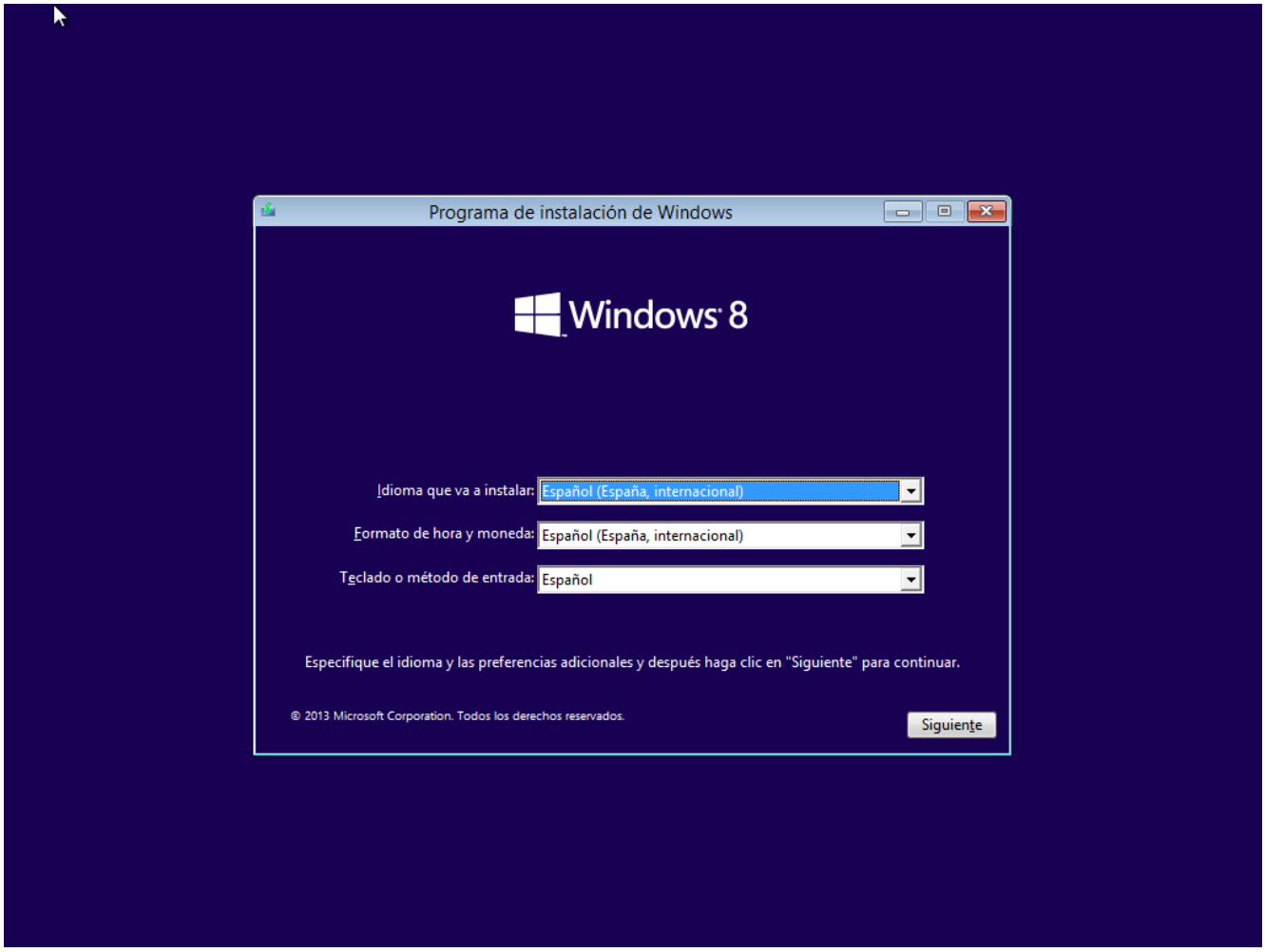

Figura A1-11: Inicio de la instalación de *Windows 8*

Tras seleccionar el idioma para la instalación y aceptar los términos de la uso de la licencia, se ofrecen dos opciones. Usaremos la avanzada para instalar una nueva copia del sistema operativo (véase Figura A1-12).

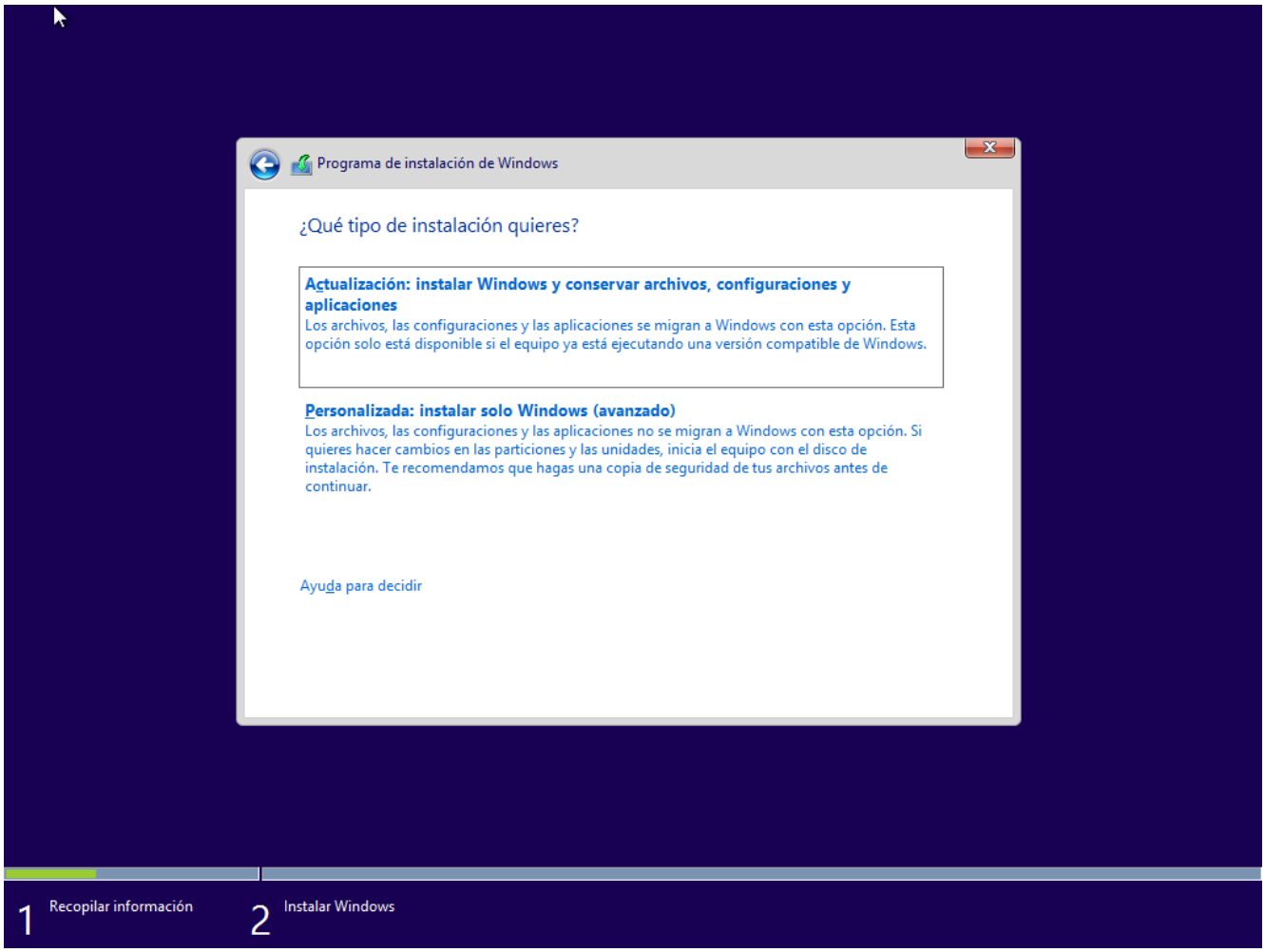

Figura A1-12: Selección del tipo de instalación

En el asistente de discos y particiones únicamente es necesario seleccionar el disco duro de la máquina virtual, que será utilizado al completo para el sistema operativo que se está instalando. Por lo tanto, no es necesario crear particiones de forma manual.

Al pulsar siguiente, el instalador realiza las demás acciones de manera automática (ver Figura A1-13). El proceso de instalación finaliza con un reinicio en el cual hay que desmontar la imagen ISO de la unidad virtual. Tras este reinicio, *Windows* necesitará que se configuren datos relativos a la zona horaria y las actualizaciones automáticas, así como datos relativos al usuario y administrador del sistema.

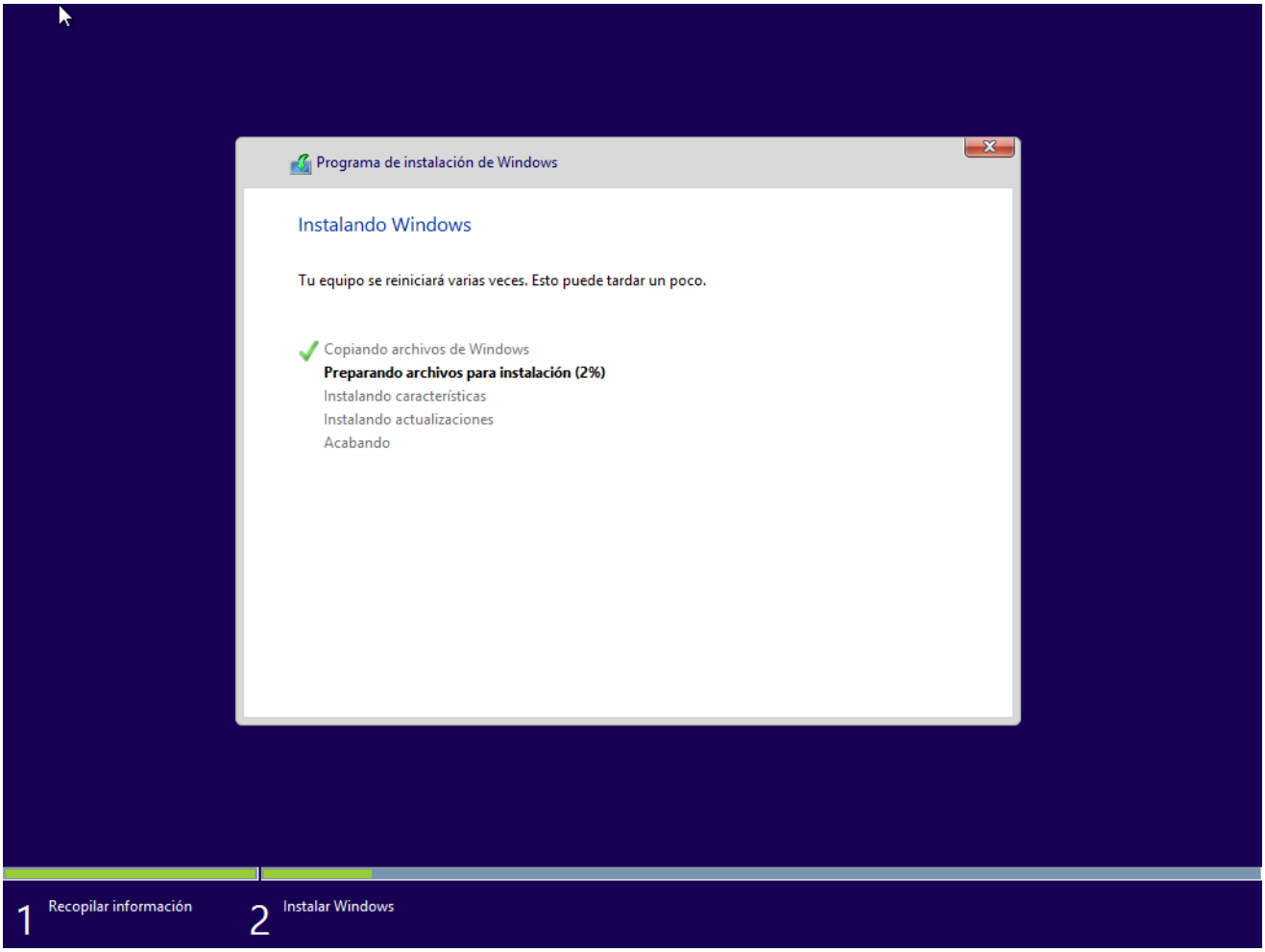

Figura A1-13: Instalación de *Windows 8* en proceso

A-I.4 Windows 7

De la misma manera que en los apartados anteriores, la instalación comienza con el montaje de la imagen de disco en la unidad de DVD de la máquina virtual.

Tras el arranque, se selecciona el lenguaje y la distribución del teclado para comenzar la instalación de *Windows* 7, como se ilustra en la Figura A1-14.

Figura A1-14: Configuración inicial del instalador de *Windows 7*

Se selecciona la opción de instalación avanzada, para que el programa de instalación instale una copia nueva del sistema operativo (ver Figura A1-15).

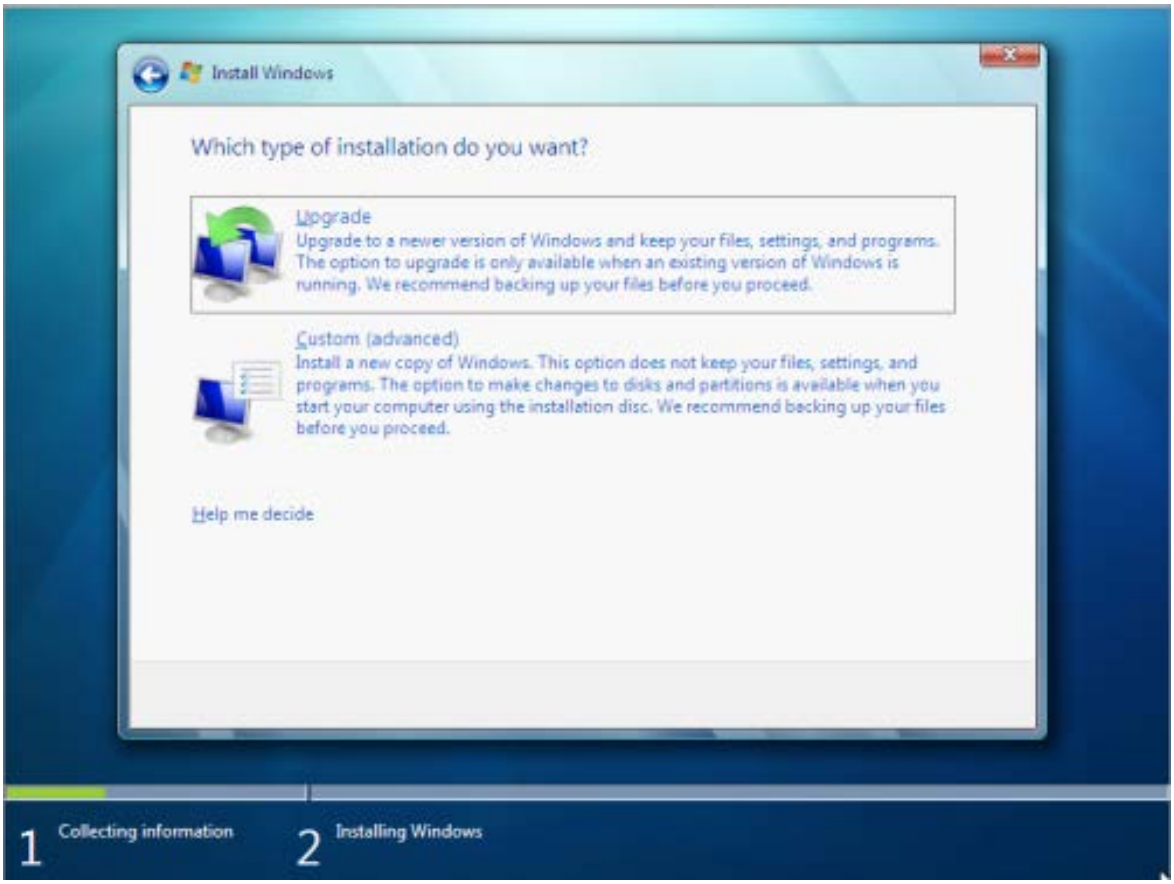

Figura A1-15: Selección del tipo de instalación

En el siguiente paso, es necesario seleccionar el disco duro de la máquina virtual, que será utilizado al completo para el sistema operativo. Por lo tanto, no es necesario particionarlo (véase Figura A1-16).

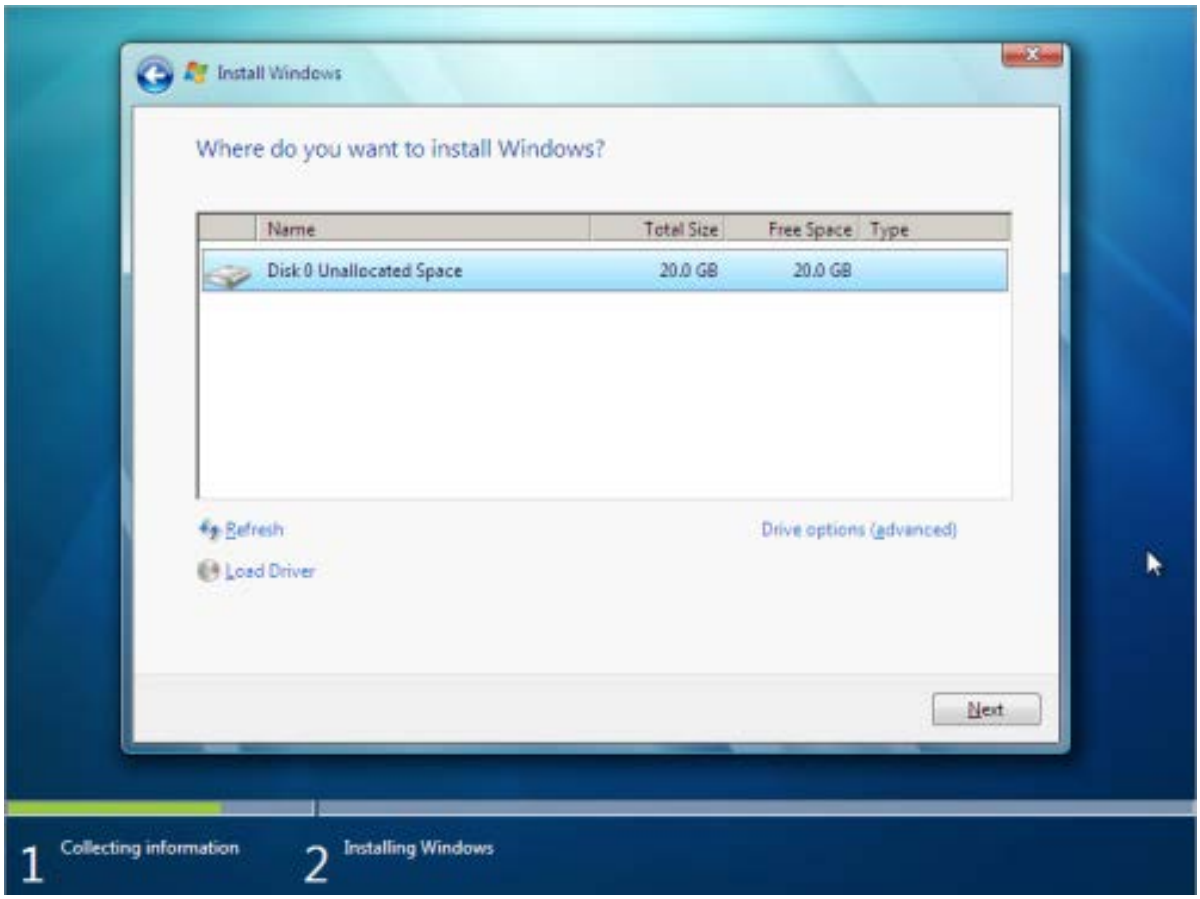

Figura A1-16: Asistente de particionado de discos

El asistente de instalación realizará las acciones restantes de forma automatica y reiniciará la maquina virtual cuando la instalación haya finalizado (ver Figura A1-17). En este momento, se desmonta la imagen de disco.

Tras el reinicio, es necesario realizar la configuracion inicial del sistema en la cual se introducen datos relativos a la zona horaria y a los usuarios del sistema.

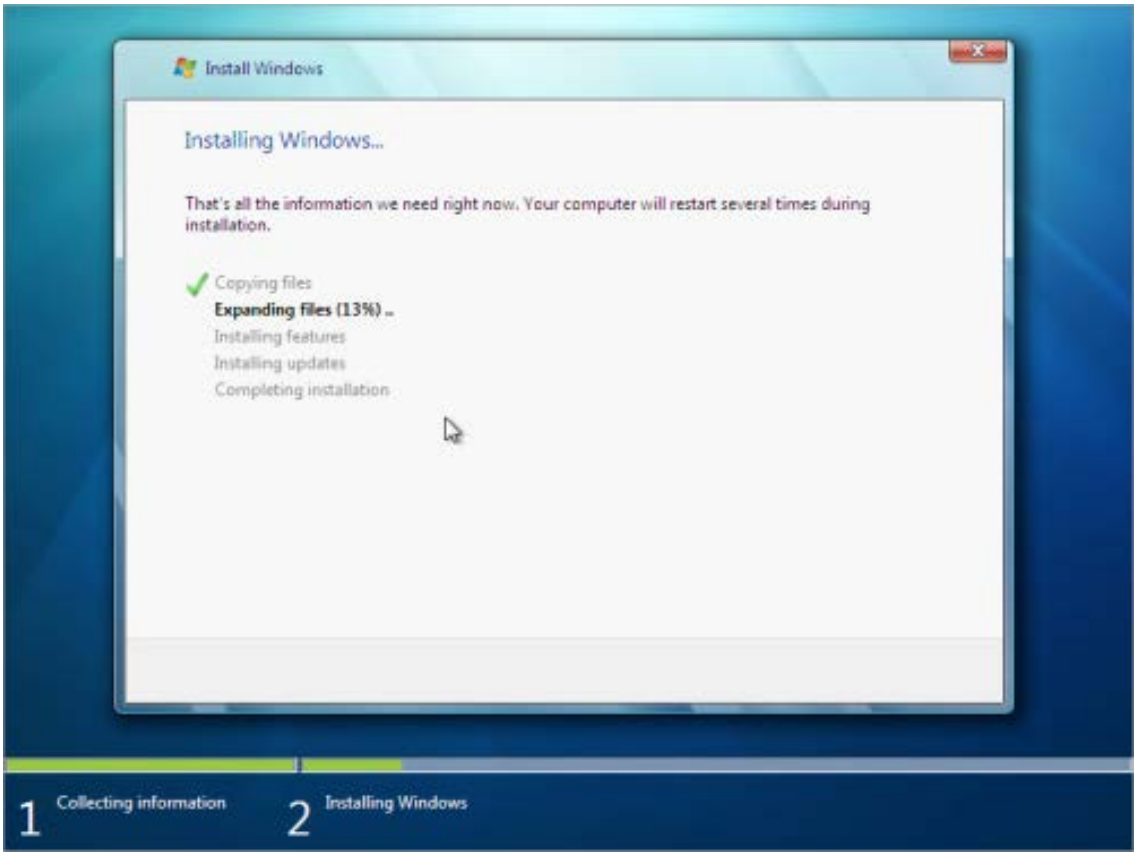

Figura A1-17: Instalación de Windows 7 en proceso