Centro Universitario de la Defensa
en la Escuela Naval Militar

TRABAJO FIN DE GRADO

Diseño e implementación de un ciberejercicio de ataque sobre una maqueta de máquinas virtuales en red

Grado en Ingeniería Mecánica

ALUMNO: Fernando Hernández de Armijo Casas

DIRECTORES: Belén Barragáns Martínez

Pablo Sendín Raña

CURSO ACADÉMICO: 2017-2018

Universidade Vigo

Centro Universitario de la Defensa
en la Escuela Naval Militar

TRABAJO FIN DE GRADO

Diseño e implementación de un ciberejercicio de ataque sobre una maqueta de máquinas virtuales en red

Grado en Ingeniería Mecánica

Intensificación en Tecnología Naval

Infantería de Marina

Universidade Vigo

RESUMEN

La importancia de la ciberseguridad ha crecido exponencialmente en los últimos años. Todas las organizaciones y organismos cuya expansión depende en parte de Internet pueden ser objetivo y, en consecuencia, víctimas de ciberataques. Nace así la necesidad de disponer de personal formado en este ámbito en la actualidad.

Con la finalidad de adiestrar al personal en el campo de la ciberseguridad, en este TFG se diseña e implementa un ejercicio de ciberataque. Para ello, se propone trabajar en un entorno controlado como el que nos ofrece una maqueta virtual resultado de un TFG anterior. Se pretende seguir la línea de trabajo de las diferentes plataformas de retos de ciberseguridad online que podemos encontrar en Internet y que son objeto de estudio en este trabajo.

El ciberejercicio abordará aspectos variados, como el estudio de paquetes de una red, el uso de la fuerza bruta para romper contraseñas, escaneo de puertos y servicios, la ingeniería social como medio de ataque informático, la esteganografía, etc. Para hacerlo más atractivo, el trabajo se ha ambientado en la investigación de una red yihadista, debido a la actualidad de este tipo de amenazas.

Posteriormente, se presenta la ejecución del ciberejercicio desde el punto de vista del alumno que lo realice, finalizando este documento con la presentación de una serie de conclusiones y líneas futuras.

PALABRAS CLAVE

Ciberdefensa, ciberataque, ciberejercicio, maqueta, virtual

AGRADECIMIENTOS

Después de unos meses intensos de trabajo, en los cuales mi tiempo libre ha pasado a estar, si no en un segundo, en un tercer plano, me gustaría agradecer a todas aquellas personas que, de una u otra forma, han contribuido en el desarrollo de este trabajo.

Empezar por mi familia y, en especial, por mis padres. Viendo el esfuerzo y la dificultad que estaba suponiendo para mí desarrollar un trabajo ambientado en una materia la cual no se estudia en profundidad en esta carrera, nunca dudaron de mí y siempre estuvieron ahí para animarme.

Agradecerle también a mi compañera de aventuras Mckenna Powers, cuyo apoyo me ha sido fundamental. Siempre supo entenderme y facilitarme el trabajo. No hubo día en el que no impusiese mis necesidades a las suyas, sacrificando sus prioridades para apoyarme.

Por supuesto, no podían faltar tampoco mis dos tutores: Belén y Pablo. Si bien el tiempo que yo he invertido me pudo llegar a parecer excesivo en algunos momentos, mis dos tutores, teniendo otras prioridades, otros trabajos y un gran número de TFG's, hicieron una labor extraordinaria. No sabría decir el tiempo que Pablo se mostró disponible para enseñarme, o el tiempo que Belén pudo dedicar al sinfín de memorias que le entregué para que me corrigiese. Ambos han conseguido lo que yo ya me esperaba en un inicio cuándo escogí este TFG, y es aumentar el interés que tenía por aprender algunas pinceladas de ciberdefensa. Gracias por no dudar en encarrilarme a tiempo cuándo las dudas me tenían bloqueado.

Para terminar, quiero agradecerle este TFG a mi gran amigo Antonio Moreno Amigo. Esta persona, teniendo también que realizar su propio trabajo y teniendo otras tareas a mayores por ser el número uno de la promoción, me ayudó cuando más lo necesitaba. Cuando peor iba y el agobio asomaba en mi día a día, cuando mi papel era el de jefe de la Cía. de Alumnos de IM y se me juntaban las tareas, cuando comenzamos a dedicar gran parte de nuestro tiempo a la operación anfibia, Antonio siempre cargó con la mayor parte del trabajo y me dejó liberado para ayudarme a avanzar en mi TFG. No cabe duda de que es el número uno de la promoción merecidamente.

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Introducción

Por lo general, existe una necesidad en nuestra vida diaria de proporcionar seguridad a aquello que creemos que la necesita. "Guarda el dinero en un lugar seguro" o "no dejes eso a la vista, que te lo roban" son frases que han acompañado a la gran mayoría de las personas a lo largo de su vida. Pero, ¿qué es lo que entendemos por *seguridad*?

Hoy en día el concepto de la seguridad se aplica a nuevos campos. El avance de las tecnologías y los sistemas informáticos han abierto un mundo diferente, un mundo capaz de recoger todo aquello de valor y hacerlo perdurable en el tiempo: fotografías y vídeos digitales capaces de compartirse infinidad de veces sin deteriorarse, dinero digital con el que comprar desde casa, datos privados almacenados en nuestro ordenador, y así, un sinfín de posibilidades que nos ofrece el mundo de Internet en la actualidad.

En las últimas décadas, una gran parte del mundo ha decidido invertir y confiar en las nuevas tecnologías. Y es que muchas personas no son capaces de imaginar sus vidas sin ellas. Lo que antes era pura imaginación, ahora es uno de los pilares de la sociedad. Y no hablamos solo de las personas. Empresas importantes de marketing y ventas, como es el caso de Amazon [1], viven de su expansión en la red. Y como ésta, otras miles.

Parece que Internet es una solución a muchos de los problemas de la vida cotidiana. Proporciona un canal de comunicación sencillo, económico, rápido y eficiente. Todo parece perfecto, excepto por un detalle. ¿Cómo proporcionar seguridad a los datos informáticos? En eso consiste la ciberseguridad.

Pero vayamos un poco más allá, ¿y si ya no hablamos de la seguridad en una compra por Internet, de tener a buen recaudo nuestros datos bancarios, de la privacidad de nuestros archivos…? ¿Y si hablamos de documentos de secreto de estado, de información sensible, de poder provocar/evitar guerras entre naciones? Éste es un campo dentro de la ciberseguridad, que hace referencia a la seguridad nacional de un país. Se conoce como ciberdefensa.

Cuando surgió Internet, no se imaginó el beneficio y las posibilidades que este nuevo mundo podría ofrecer. Es por ello que el concepto de la seguridad no fue uno de los factores primordiales, si no que se añadiría a posteriori. A medida que van apareciendo agujeros de seguridad y la situación nos lo exige, se van tapando: así es como se construye la seguridad en Internet. Esto nos lleva a una conclusión: "No existe la seguridad absoluta" [2].

En los últimos años, vista la importancia que está adquiriendo la red, su vulneración se está convirtiendo en el objetivo de determinadas personas conocidas como hackers, que se dedican a explotar la vulnerabilidad de la red para obtener así un beneficio. Este beneficio viene asociado a las intenciones de los propios hackers. Según INCIBE (Instituto Nacional de Ciberseguridad) estos ataques se clasifican en robo de dinero y extorsión cibernética, filtraciones o fuga de datos y ciberespionaje, ataques a servicios importantes y explotación de vulnerabilidades de plataformas, sistemas y protocolos ampliamente utilizados [3].

En 2016, tras los Estados Unidos y Reino Unido, España se convierte en el tercer país del mundo que más ciberataques ha sufrido: un 130% más que en 2015 [4], lo que lleva a pensar que la seguridad en la red es algo de actualidad, algo que a día de hoy sigue siendo un problema y que hay que trabajar en ello constantemente [5]. Comienza a aparecer entonces una necesidad: disponer del personal con la formación necesaria para garantizar seguridad dentro del ciberespacio.

La preocupación de las empresas, tanto públicas como privadas, de disponer de personal formado en conocimientos TIC (Tecnologías de la Información y Comunicaciones) a día de hoy crece exponencialmente. Cada vez son más las instituciones y organismos que viven, se expanden y se dan a conocer a través de Internet, o las empresas de telefonía que viven del mundo de las telecomunicaciones. Poco a poco, negocios extendidos mundialmente comienzan a crecer dentro de la red y, por consiguiente, a ampliar sus fronteras en el ámbito económico, como podría ser el caso de Inditex [6] entre muchos otros. Y es que en el ciberespacio se controlan y se mueven cantidades inimaginables de dinero diariamente. ¿Se imaginan las repercusiones que podrían tener sobre ellas cualquier ciberataque que les incapacitase para hacer un uso de la red? Probablemente ellas tampoco. Y no solo hablamos de organismos comerciales; el propio Estado de un país debe estar capacitado para controlar el ciberespacio dentro de aquello que le corresponde: redes eléctricas, líneas de transporte, centrales de energía… Un simple fallo debido a un ciberataque podría sumir en el caos a una nación.

Ésta es la razón principal por la cual todos los organismos y empresas prestan una atención especial al personal TIC, creando departamentos específicos en sus instituciones con las competencias requeridas para garantizar la seguridad informática. Y al igual que los ciberataques van evolucionando y siendo perfeccionados, los conocimientos en ciberseguridad también. En la actualidad, es continuo el interés y la inversión por parte de dichos organismos en la formación de este personal [7].

El propio Estado español cuenta con el CCN-CERT [8] (Centro Criptológico Nacional- *Computer Emergency Response Team*), organismo por excelencia que se encarga de la protección de las infraestructuras críticas dentro del ámbito informático.

También debemos mencionar al MCCD [9] (Mando Conjunto de CiberDefensa), que es el organismo responsable del planeamiento y la ejecución en lo que respecta a ciberdefensa en las redes y sistemas de información y telecomunicaciones del Ministerio de Defensa, así como de contribuir a la respuesta a ciberamenazas que pudiesen afectar a la Defensa Nacional. En este trabajo se le dará especial importancia al concepto de ciberdefensa y a la ciberguerra, ya que son estos ciberataques los que ocupan un mayor porcentaje [10] dentro de los calificados como ataques críticos.

1.2 Ciberdefensa

La ciberdefensa, dentro del campo de la ciberseguridad, hace referencia al conjunto de tecnologías, actividades e iniciativas de las que un Estado hace uso para la defensa dentro del mundo cibernético. Este término se encuentra en crecimiento exponencial. Junto con las facilidades y los usos que Internet y los sistemas informáticos nos ofrecen, viene la utilización de estos por parte de los Estados de las diferentes naciones. Podemos decir que hay una gran cantidad de datos críticos, gestiones, controles… que se encuentran en fuentes informáticas y cuya seguridad es fundamental, porque siempre existirá la posibilidad de que pudiesen ser explotados por personal no deseado y en beneficio de otras naciones.

Es por eso que el CCN-CERT, encargado de la defensa de las administraciones públicas de España contra las amenazas del ciberespacio, requiere de personal altamente cualificado y entrenado en los diferentes ámbitos de la ciberseguridad. Existen diferentes plataformas donde se diseñan ejercicios de ciberataques y ciberdefensa en los que el personal se puede entrenar. Destacar aquí la nueva plataforma llamada "Atenea" [11], del CCN y de carácter público, basada en los diferentes pilares de la ciberseguridad: seguridad básica, criptografía y esteganografía, exploiting, análisis forense, hacking web, análisis de tráfico y reversing. Como ella, existen otras plataformas muy diversas que serán comentadas en el capítulo dos.

1.3 Objetivos

Entre los numerosos objetivos que persigue este trabajo, destacamos como primordial la propia elaboración del ciberejercicio de ataque. Este ciberejercicio se implementará en una maqueta de máquinas virtuales, en concreto en la maqueta diseñada por el Tte. Romero Fernández en su correspondiente Trabajo de Fin de Grado [12], de modo que podamos trabajar en el entorno controlado y seguro que buscamos.

Otros objetivos secundarios de este trabajo son:

- Revisión del estado del arte de plataformas de pentesting para adiestramiento.
- Validación del correcto funcionamiento de la maqueta de máquinas virtuales en red con un mayor grado de fiabilidad.
- Introducción al pentesting y al estudio de páginas web para aquellas personas con unos conocimientos informáticos básicos.
- Otro objetivo implícito será la concienciación del personal en la importancia de la seguridad informática.

1.4 Estructura de la memoria

En este primer capítulo, se ha pretendido ilustrar el panorama actual en lo que respecta a la seguridad informática. Hacer ver la importancia y el impacto que tiene en el presente y en el futuro, y concienciar de la necesidad de disponer de un entorno seguro dentro de un ciberespacio lleno de amenazas. Se aborda también el concepto de ciberdefensa dentro de la ciberseguridad, de la importancia que se le ha de dar, así como de la importancia de la formación en este ámbito y de las posibilidades que se abren a un Estado capaz de controlar el ciberespacio.

En el segundo capítulo se hace una reseña de los ciberataques y ciberincidentes y su evolución. Además, se describen los principales organismos relacionados con la ciberseguridad nacional así como sus principales funciones dentro de este ámbito. Se realiza también un estudio de las plataformas de adiestramiento de ciberejercicios más populares. Por último, se hace una breve introducción a la arquitectura de red y, en relación con ésta, al software de virtualización empleado para virtualizar dicha arquitectura.

En el tercer capítulo, desarrollamos el ciberejercicio que constituye la base de este TFG. Lo diseñamos conforme a algunos de los diferentes aspectos del campo de la ciberseguridad, con el fin de familiarizar y fomentar en el alumno algunos conceptos básicos de las técnicas de pentesting. Se tratan temas como la esteganografía, el estudio de trazas de paquetes de una red, ataques por fuerza bruta, ingeniería social, escaneos de puertos y servicios y otros conceptos que hemos considerado interesantes incorporar.

En el cuarto capítulo, realizamos y validamos el diseño del ciberejercicio implantado en la maqueta de máquinas virtuales en red, planteando también su ejecución desde el punto de vista del alumno que lo desee realizar.

En el quinto y último capítulo, tras la finalización del trabajo, analizamos el grado de cumplimiento de los objetivos propuestos y exponemos unas conclusiones, así como unas líneas futuras que orienten este trabajo para futuras investigaciones y proyectos.

2 ESTADO DEL ARTE

2.1 Introducción

Este capítulo comienza presentando una introducción a las ciberamenazas y su clasificación. Dentro de este apartado analizaremos cuál es la tendencia actual y cuáles son los focos de mayor riesgo de sufrir estas ciberamenazas.

Realizaremos un estudio de los principales organismos nacionales encargados de la ciberseguridad en España y las características y funciones de cada uno de ellos.

Estudiaremos también, con una relación directa hacia este trabajo, de plataformas online diseñadas para realizar ejercicios de ciberseguridad y poner en prácticas los conocimientos en este campo.

Por último, y con relación a este tema, se hará una introducción al concepto de arquitectura de una red y al software de virtualización empleado en este TFG. Es sobre este tipo de simulaciones de red en el que se desarrollará el trabajo y se diseñará e implementará un ciberataque.

2.2 Ciberamenazas

Dentro del ciberespacio, se pueden identificar una serie de amenazas principales causantes de la gran mayoría de ciberataques. Estos ciberataques se pueden producir en los diferentes eslabones que componen un sistema informático: datos, aplicaciones, sistemas operativos, hardware, red, suministro de energía o incluso el entorno puede comprometer la ciberinformación [13].

Acceso físico a la máquina: en este caso, el atacante tendría acceso a la máquina de la víctima o a las instalaciones que se quieren atacar. Dentro de las diversas opciones que esto puede ofrecer, se destacan:

- Interrupción del suministro eléctrico.
- Apagado manual del equipo.
- Vandalismo.
- Apertura manual del equipo y robo del disco duro.
- Monitorización del tráfico de red.

Intercepción de las comunicaciones: en este caso, el atacante tendría acceso a las comunicaciones de la víctima con la capacidad de secuestrar una sesión, falsificar una identidad (*spoofing*) o también redireccionar y alterar mensajes de la red. Relacionados con este tipo de ataques están los *honeypots*, puntos de acceso falsos con el mismo ESSID (*Extended Service Set IDentifier*) que el punto al que pretenden replicar, con el fin de que la víctima se conecte a las falsas imitaciones. Esto le proporciona

al atacante la posibilidad de capturar el tráfico y obtener información sensible como usuarios y contraseñas.

Otro tipo de ataque muy extendido es conocido como MITM (*Man In The Middle*), que consiste en la colocación del atacante entre el punto de acceso y la víctima, siendo así el propio atacante un punto de paso del flujo entre punto de acceso y máquina. Permite al atacante capturar la información que él desee o modificarla e interactuar con ella. Hoy en día existen protocolos que intentan evitar este tipo de ataques, como HTTPS (*Hypertext Transfer Protocol Secure*), que es una variante del conocido HTTP, con la virtud de que cifra la información basándose en SSL/TLS (protocolos criptográficos). Este protocolo impide en gran medida [14] la interpretación de la información capturada por el atacante.

Denegación de servicio (DoS): estos ataques consisten en impedir e inutilizar el uso de un servicio. Por lo general, los ataques de denegación de servicio se pueden clasificar en dos tipos:

- Explotación de las debilidades del protocolo TCP/IP.
- Explotación de las vulnerabilidades del software del servidor.

En la actualidad, este tipo de ataques ha evolucionado hasta el punto de realizarse a través de miles o millones de ordenadores atacando a un mismo servidor. Este método emplea lo que se conoce en la *Deep Web* con el sobrenombre de redes zombi o *botnets*, pudiendo utilizar máquinas de usuarios anónimos infectadas con algún tipo de malware [15]. A este nuevo método de denegación de servicio se le conoce como DDoS (*Distributed Denial of Service*).

Intrusiones: este ataque consiste en explotar alguna vulnerabilidad para tener acceso a la red y llevar a cabo una monitorización del flujo de la red a través de una tarjeta de red en modo monitor (*sniffing*). Por lo general, este tipo de ataques conlleva un DoS que obligue a la víctima a conectarse de nuevo al servicio, lo que le permite al atacante capturar el *handshake* (primer paso para obtener la contraseña para acceder a la red). Este tipo de ataques tienen como finalidad:

- Análisis de puertos.
- Elevación de privilegios: este tipo de intrusión consiste en aprovechar una vulnerabilidad de alguna aplicación cuando ésta envía una solicitud específica (no planeada por su diseñador). Esto puede generar determinadas situaciones atípicas en las cuales el atacante puede acceder al sistema con derechos de aplicación. Un caso conocido en este tipo de ataques es el desbordamiento de la memoria intermedia (búfer). Un ejemplo es el caso del "Gusano Morris", un malware que aprovechó esta vulnerabilidad para averiguar contraseñas, otorgándole privilegios de *root* y reproducirse a otras máquinas [16].
- Ataques malintencionados: virus, troyanos, gusanos, etc.

Ingeniería social: éste es un concepto que hasta ahora no se había mencionado, y se trata de un ataque al eslabón más débil en la cadena de la ciberseguridad: el propio individuo. Muchas veces, ya sea por desconocimiento e ignorancia o por engaño, las personas generamos nuestras propias vulnerabilidades en el sistema otorgando de forma indirecta información crítica (como contraseñas) o abriendo archivos de origen desconocido (obra del atacante). Cuando esto sucede, ningún dispositivo puede proteger al usuario contra la falsificación; solo el sentido común, la razón y el conocimiento básico, obra de la cultura general acerca de la seguridad en la informática, pueden evitar este tipo de errores.

Puertas trampa: se trata de puertas traseras ocultas en algún programa de software que brindan acceso al diseñador en todo momento. Muchas veces estas puertas traseras no son intencionadas por parte del diseñador y su existencia se debe a errores de programación. Estas vulnerabilidades deben ser corregidas con rapidez nada más publicarse para evitar que alguna persona indeseada aproveche la situación. Queda en manos de los administradores el estar informado acerca de las actualizaciones de los programas para limitar el riesgo de este tipo de ataques.

2.2.1 Tendencias actuales en ciberataques

Dentro del panorama actual, las principales tendencias en ciberataques suelen incurrir en los siguientes principios:

2.2.1.1 Ciberespionaje

El ciberespionaje se considera la mayor amenaza para la seguridad nacional. El ciberespionaje más extendido se encuentra en el ámbito económico, dirigido principalmente a las industrias de los sectores de defensa, la industria de la fabricación y empresas dedicadas a la información, entre otras, como se puede ver en la Figura 2-1. El fin es el acceso a avances y desarrollo, teniendo su origen en Estados y empresas.

Se debe destacar también el ciberespionaje político y el de los servicios de inteligencia, que persiguen información política, económica o estratégica, como también planes de desarrollo y posiciones nacionales en torno a negociaciones.

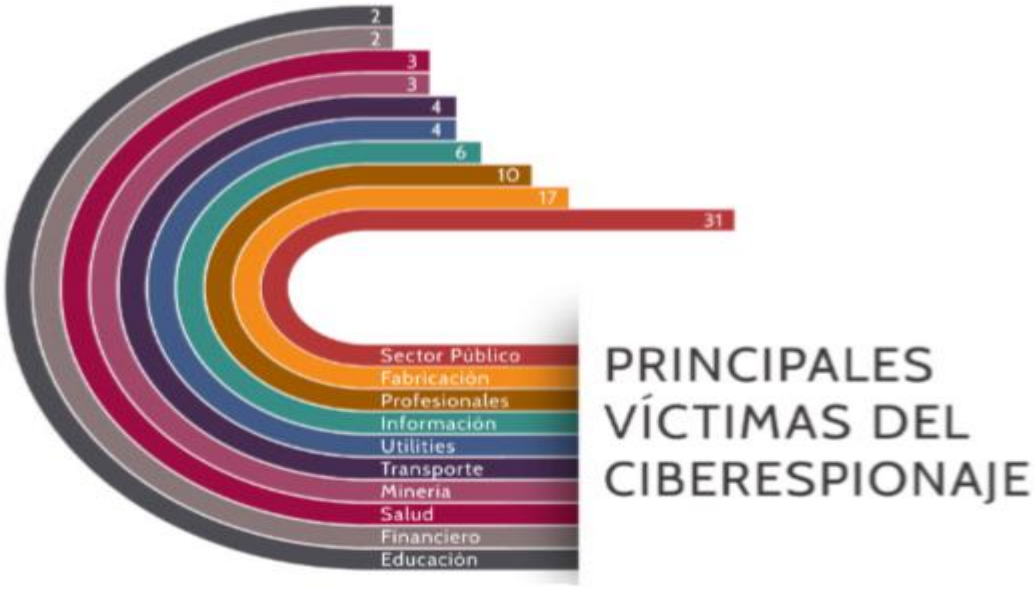


Figura 2-1 Principales víctimas del ciberespionaje en 2016 [17]

2.2.1.2 Ciberdelincuencia

La ciberdelincuencia continúa en crecimiento, llegando a superar incluso a la delincuencia tradicional en algunos países, según uno de los últimos informes de la Europol [18]. En algunos casos, incluso la población tiene más preocupación de sufrir cibercrimen que de sufrir de delincuencia física [19]. La ciberdelincuencia más común tiene su origen en diferentes aspectos:

- *Ransomware y cryptoware*: este tipo de ataque es el que tuvo un mayor crecimiento en 2016, afectando mayoritariamente a los sectores de energía, buscando interrumpir a los servicios gubernamentales, sanitarios y de telecomunicaciones. Este tipo de ataques se incrementó entre 2015 y 2016 más de un 375%, llegando a producirse aproximadamente 638 millones de ataques en ese último año [20].
- Publicidad dañina: se inserta este tipo de publicidad en páginas web conocidas y de confianza con el fin de engañar a las personas.
- Ataques a entidades financieras: estos ataques también se han incrementado con el fin de, a través de lo que se conoce como *phishing* (obtener credenciales e información personal por

medio del engaño y la astucia), de obtener información privada para ser vendida en la Internet profunda (*Deep Web*).

Se conoce como Internet profunda (véase en la Figura 2-2) al contenido de Internet que no está indexado por los motores de búsqueda convencionales debido a diversos factores. Es en esta parte de Internet donde se encuentra el mayor porcentaje de ciberdelincuencia, ciberterrorismo, pornografía infantil, venta de contenidos ilícitos, venta de armas, etc [21].

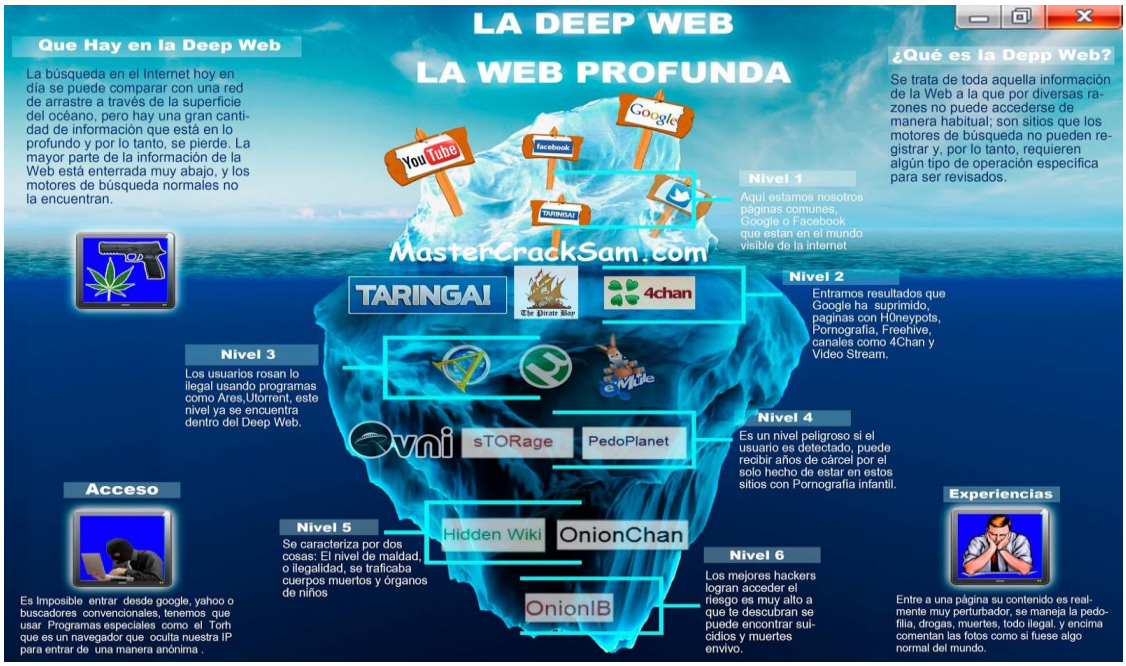


Figura 2-2 La *Deep Web* [22]

Sin embargo, no solo las empresas y los organismos más codiciados son víctimas de la ciberdelincuencia; los usuarios particulares también son objetivos muy comunes. En la Figura 2-3 podemos ver un gráfico a modo de resumen del porcentaje de ciberincidentes sufridos en 2017 por la población española.

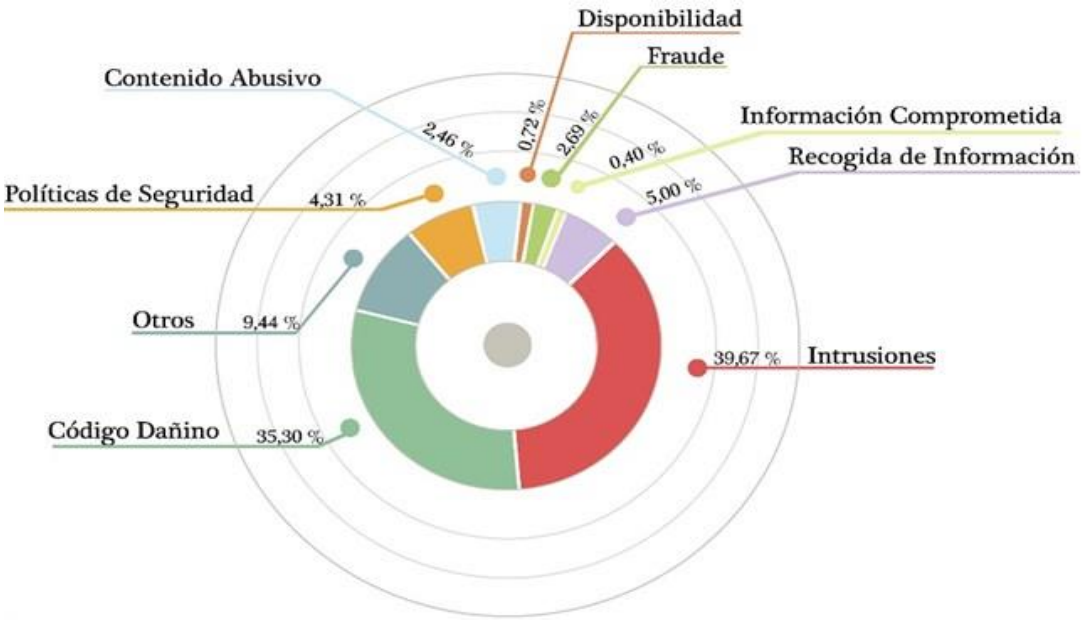


Figura 2-3 Ciberincidentes en España en 2017 [23]

2.2.1.3 Interrupción de sistemas

Hoy en día muchas de las instalaciones industriales con una configuración insegura en el campo de la informática, o conexiones a Internet sin la adecuada vigilancia, son las principales razones para que se lleven a cabo este tipo de ciberataques:

- Ataques de denegación de servicio: consiste, como ya se mencionó, en saturar un servicio con el fin de inutilizarlo. Impedir este tipo de ataques consume muchos recursos a las empresas y, muchas veces, los atacantes simplemente amenazan con realizar uno para conseguir un rescate económico a cambio de no llevar a cabo el ataque.
- Sabotaje digital: este tipo de delincuencia suele estar relacionado con el descontento de antiguos empleados de alguna empresa. Utilizan sus credenciales de acceso para eliminar información y destruir o deteriorar soportes de almacenamiento.
- Desfiguraciones: consiste en la desfiguración de las páginas web. Tienen su origen en motivos ideológicos o en la simple demostración pública de las capacidades de los atacantes.
- Infraestructuras críticas: los ataques a los Sistemas de Control Industrial (SCI) se consideran ataques críticos por las consecuencias que pueden conllevar. Los incidentes confirmados en estos casos son escasos, aunque se han detectado muchas instalaciones inseguras sin las conexiones a Internet con la vigilancia adecuada.

Como resumen a los ciberincidentes actuales, en la Tabla 2-1 podemos ver cómo el CCN-STIC (Centro Criptológico Nacional- Seguridad en Tecnologías de la Información y Comunicación) clasifica los ciberincidentes.

CLASIFICACIÓN DE LOS CIBERINCIDENTES	
Clase de ciberincidente	**Descripción**
Código dañino	Software cuyo objetivo es infiltrarse o dañar un ordenador, servidor u otro dispositivo de red, sin el conocimiento de su responsable o usuario y con finalidades muy diversas.
Disponibilidad	Ataques dirigidos a poner fuera de servicio los sistemas, al objeto de causar daños en la productividad y/o la imagen de las instituciones atacadas.
Obtención de información	Ataques dirigidos a recabar información fundamental que permita avanzar en ataques más sofisticados, a través de ingeniería social o de identificación de vulnerabilidades.
Intrusiones	Ataques dirigidos a la explotación de vulnerabilidades de diseño, de operación o de configuración de diferentes tecnologías, al objeto de introducirse de forma fraudulenta en los sistemas de una organización.
Compromiso de la información	Incidentes relacionados con el acceso y fuga (confidencialidad), modificación o borrado (integridad) de información no pública.
Fraude	Incidentes relacionados con acciones fraudulentas derivadas de suplantación de identidad, en todas sus variantes.
Contenido abusivo	Ataques dirigidos a dañar la imagen de la organización o a utilizar sus medios electrónicos para otros usos ilícitos (tales como la publicidad, la extorsión o, en general la ciberdelincuencia).
Política de seguridad	Incidentes relacionados por violaciones de usuarios de las políticas de seguridad aprobadas por la organización.
Otros	Otros incidentes no incluidos en los apartados anteriores.

Tabla 2-1 Clasificación de los ciberincidentes según CCN-STIC [24]

2.2.2 Costes de los ciberincidentes y su gestión

Los incidentes de seguridad tienen un alto coste global derivado de varios costes parciales, tales como: coste económico, coste de servicio, coste de imagen y reputación de una organización, coste por sanciones, etc.

Normalmente, los ciberincidentes llevados a cabo por personal con conocimientos informáticos acaban en algún tipo de rescate económico. De no ser así, las consecuencias podrían clasificarse según los costes más significativos: tiempo de inactividad (cortes de suministro de energía), costes económicos (derivados de la respuesta al ciberincidente), pérdida de datos (afecta a la reputación y a la intimidad de la empresa) y pérdida de vidas (ataques cibernéticos a hospitales, afectando los registros de los pacientes). El riesgo de los ataques puede medirse según se muestra en la Tabla 2-2.

CRITERIOS DE DETERMINACIÓN DEL NIVEL DE PELIGROSIDAD DE LOS CIBERINCIDENTES			
NIVEL	AMENAZA(S) SUBYACENTE(S) MÁS HABITUAL(ES)	VECTOR DE ATAQUE	CARACTERÍSTICAS POTENCIALES DEL CIBERINCIDENTE
CRÍTICO	Ciberespionaje	- APTs, campañas de malware, interrupción de servicios, compromiso de sistemas de control industrial, incidentes especiales, etc.	- Capacidad para exfiltrar información muy valiosa, en cantidad considerable y en poco tiempo. - Capacidad para tomar el control de los sistemas sensibles, en cantidad y en poco tiempo.
MUY ALTO	Interrupción de los Servicios IT / Exfiltración de datos / Compromiso de los servicios	- Códigos dañinos confirmados de Alto Impacto (RAT, troyanos enviando datos, rootkit, etc.) - Ataques externos con éxito.	- Capacidad para exfiltrar información valiosa, en cantidad apreciable. - Capacidad para tomar el control de los sistemas sensibles, en cantidad considerable.
ALTO	Toma de control de los sistemas / Robo y publicación o venta de información sustraída / Ciberdelito / Suplantación	- Códigos dañinos de Medio Impacto (virus, gusanos, troyanos). - Ataques externos – compromiso de servicios no esenciales (DoS / DDoS). - Tráfico DNS con dominios relacionados con APTs o campañas de malware. - Accesos no autorizados / Suplantación / Sabotaje. - Cross-Site Scripting / Inyección SQL. - Spear phising / pharming	- Capacidad para exfiltrar información valiosa. - Capacidad para tomar el control de ciertos sistemas.
MEDIO	Logro o incremento significativo de capacidades ofensivas / Desfiguración de páginas web / Manipulación de información	- Descargas de archivos sospechosos. - Contactos con dominios o direcciones IP sospechosas. - Escáneres de vulnerabilidades. - Códigos dañinos de Bajo Impacto (adware, spyware, etc.) - Sniffing / Ingeniería social.	- Capacidad para exfiltrar un volumen apreciable de información. - Capacidad para tomar el control de algún sistema.
BAJO	Ataques a la imagen / menosprecio / Errores y fallos	- Políticas. - Spam sin adjuntos. - Software desactualizado. - Acoso / coacción / comentarios ofensivos. - Error humano / Fallo HW-SW.	- Escasa capacidad para exfiltrar un volumen apreciable de información. - Nula o escasa capacidad para tomar el control de sistemas.

Tabla 2-2 Criterios de determinación de peligrosidad de ciberincidentes [25]

2.2.3 Responsables de los ciberataques

Los actores de los ciberataques pueden dividirse en diferentes grupos, en función del objetivo del ciberataque y de los conocimientos de los que disponen [17]:

- Estados: mejorar su posición geopolítica o estratégica.
- Organizaciones criminales: beneficio económico (directo o indirecto).
- Organizaciones privadas: ciberespionaje, obtención de información de valor.
- Ciberterroristas: alterar el orden social, aterrorizar a la población, influir en política.
- Ciberyihadistas: propaganda, reclutamiento.
- Ciberactivismo: ideologías.
- Cibervándalos y *script kiddies*: evidenciar vulnerabilidades, piratería. Diversión, retos.
- Actores internos: venganza, beneficio económico, motivos ideológicos.
- Ciberinvestigadores: evidenciar debilidades, autoafirmación.

2.3 Organismos nacionales de ciberseguridad

El mundo de los ciberataques está en auge y, a la par, debe estarlo el de la ciberseguridad. Los hackers saben que los agujeros de seguridad existen y tratan de explotarlos en su beneficio. Debido a la importancia que está cobrando el mundo TIC, el nivel de daño y las ganancias económicas cada vez son mayores debido a ciberataques. La ocultación y la no exposición del atacante a la hora de delinquir son factores importantes que juegan en beneficio de los hackers cuando se realiza un ciberataque.

Ésta es una problemática que viene solucionándose disponiendo de personal con conocimientos TIC y formación adecuada en seguridad informática, de modo que tengan las capacidades de responder a estos ciberataques y anularlos. De ahí el interés, mencionado en la introducción, de las empresas y organizaciones en disponer de este personal y en invertir dinero para su formación. En la Figura 2-4, podemos ver una gráfica que representa el aumento de ciberataques en los últimos años en España.

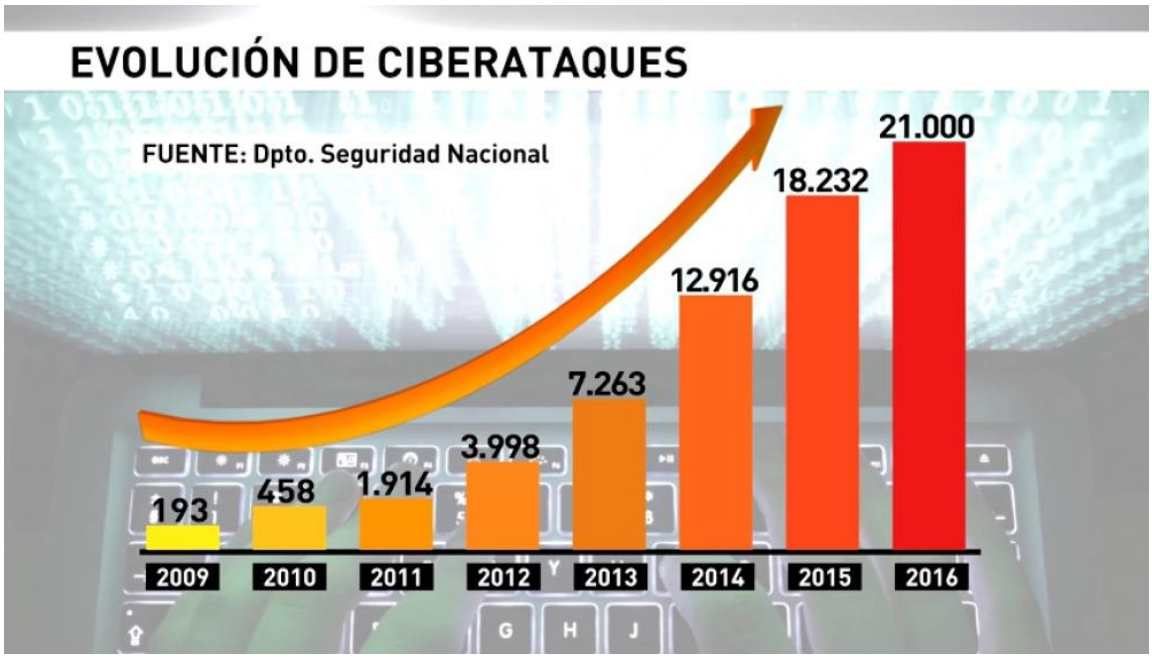


Figura 2-4 Evolución de ciberataques entre 2009-2016 [26]

A pesar de que esta gráfica no siga una proporción a escala, se puede ver cómo a principios de 2009 los ciberataques se duplicaban año tras año. Sin embargo, a partir de 2015, aunque el mundo de las ciberataques sigue en aumento, se puede apreciar que la intensidad con la que crecen ya no es la misma; esto se debe a la inversión en seguridad y a la preocupación de las organizaciones y organismos por este tema de actualidad.

2.3.1 CCN-CERT

El CCN-CERT es un organismo español que nace en 2006 en el seno del CCN (Centro Criptológico Nacional), que se encuentra adscrito al CNI (Centro Nacional de Inteligencia) [27]. Este organismo ostenta la capacidad de respuesta a incidentes de seguridad de la información del CCN.

De acuerdo a la normativa (Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y el RD 3/2010, de 8 de enero, regulador del ENS (Esquema Nacional de Seguridad), modificado por el RD 951/2015, de 23 de octubre) que rige al CCN-CERT, éste se encarga de los ciberincidentes que afecten a sistemas del sector público, a empresas y organizaciones de interés estratégico y de cualquier sistema clasificado. Su misión es la de mejorar la ciberseguridad española y responder rápida y eficientemente a los ciberataques y ciberamenazas. El resultado será un ciberespacio más seguro y confiable [28].

Debemos destacar también la Estrategia de Ciberseguridad Nacional 2013 [29], proveniente del DSN (Departamento de Seguridad Nacional) [30], que delimita el entorno del ciberespacio, fija principios, objetivos y líneas de acción para el logro de la ciberseguridad nacional. Además fija la cooperación de los organismos con responsabilidades en ciberseguridad, en especial entre el CCN-CERT, el MCCD y el CERT de Seguridad e Industria.

Es continúa la renovación de información de este organismo. Cada día aparecen informes y noticias nuevas acerca de la ciberseguridad y de las cuales el CCN-CERT se hace cargo [31]. También difunde avisos de los últimos ciberataques, consejos de carácter público para aumentar la ciberseguridad o, incluso, cursos de ciberseguridad para personal interesado en esta materia [32]. Además, el CCN-CERT cuenta con una serie de herramientas para evaluar la ciberseguridad a nivel técnico de una red como podría ser la herramienta *CLARA*, o con plataformas de desafíos de seguridad informática para la realización de ejercicios, con el fin de entrenar, motivar y fomentar el interés por el mundo de la ciberseguridad, como podría ser la plataforma *ATENEA*.

Más adelante se hará referencia a este tipo de plataformas, ya que el estudio de las mismas constituye uno de los objetivos de este TFG.

2.3.2 INCIBE

Se trata del Instituto Nacional de Ciberseguridad [33]. Fue fundado en 2006 con el nombre de Instituto Nacional de Tecnologías de la Comunicación y pasó a denominarse como INCIBE el 28 de octubre de 2014. El objetivo de INCIBE es desarrollar la Sociedad de la Información mediante el desarrollo de proyectos e innovaciones que tienen su centro de atención en la ciberseguridad tanto nacional como internacional [34].

En la Figura 2-5, podemos ver un organigrama de cómo se estructura el INCIBE.

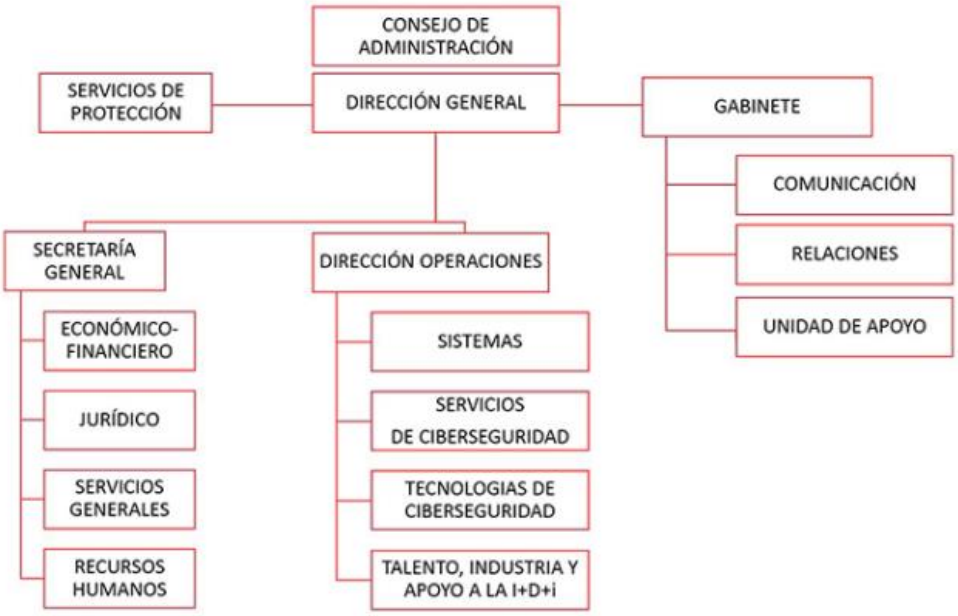


Figura 2-5 Organigrama de INCIBE [35]

El CERT de Seguridad e Industria, centro de respuesta a incidentes de ciberseguridad operado por INCIBE, trabaja para mejorar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de ciberincidentes, aumentar el diseño de medidas preventivas para atender a las necesidades de la sociedad en general y a las necesidades de seguridad de las infraestructuras críticas, de apoyo en la investigación y lucha frente a ciberdelitos y ciberterrorismo [36].

2.3.3 MCCD

La Directiva de Defensa Nacional de 2012 establece que el Ministerio de Defensa participe en el impulso de la ciberseguridad, en el marco de los principios que se establecen en la Estrategia de Ciberseguridad Nacional. Esto requiere que el Ministerio de Defensa contribuya a la ciberseguridad nacional, no solo en el ámbito militar. Por ello y debido al carácter crítico de la información que procesan los sistemas de información y telecomunicaciones, su múltiple dependencia, complejidad técnica, cantidad y dispersión geográfica de sus infraestructuras, se requiere la creación de un MCCD que dirija y coordine las acciones de las Fuerzas Armadas en este ámbito [37].

El MCCD es el órgano de la estructura operativa que, subordinado al JEMAD (Jefe de Estado Mayor de la Defensa), se encarga del planeamiento y ejecución de las acciones con relación a la ciberdefensa en las redes y sistemas de información y telecomunicaciones del Ministerio de Defensa (como se indicó en la sección 1.1).

Dentro de sus cometidos, destacan [38]:

- Garantizar el libre acceso al ciberespacio con la finalidad de cumplir las misiones de las FAS.
- Garantizar integridad, disponibilidad y confidencialidad de la información.
- Garantizar el funcionamiento de los servicios críticos de los sistemas de información y telecomunicaciones de las FAS.
- Obtener, analizar y explotar la información sobre ciberataques y ciberincidentes.
- Ejercer la respuesta oportuna, legítima y proporcionada en el ciberespacio en el ámbito de la Defensa Nacional.
- Dirigir y coordinar en materia de ciberdefensa los diferentes centros de respuesta de los Ejércitos y la Armada y el de operaciones de seguridad de la información del Ministerio de Defensa.
- Representar al Ministerio de Defensa en materia de ciberdefensa en el ámbito nacional e internacional.
- Cooperar en materias de ciberdefensa con otros centros nacionales de respuesta, según lo que determinen las estrategias y políticas de ciberseguridad en vigor.
- Definir, dirigir y coordinar la concienciación, la formación y el adiestramiento especializado en materia de ciberdefensa.

A día de hoy, el MCCD sigue trabajando e invirtiendo en ciberdefensa con el fin de reforzar a las FAS y al propio Gobierno en la lucha contra las ciberamenazas. Se tiene previsto en 2018 crear un cuerpo de ciberdefensa que dependa del MCCD [39].

2.4 Plataformas de ejercicios de ciberseguridad

Como parte de los objetivos de este TFG, a continuación mencionaremos algunas de las plataformas en las que los usuarios pueden realizar diferentes ejercicios de ciberseguridad. Estos ejercicios tienen como fin fomentar y desarrollar el interés por el ámbito de la ciberseguridad, entrenar al personal que así lo requiera para poder actuar en el marco de la ciberseguridad o, incluso, motivar e incentivar mentes para la superación de retos y ejercicios con la finalidad de hacer del ciberespacio un lugar más seguro. En todo momento, estas plataformas tienen un carácter ético para formar, lo que comúnmente se denomina como ‘hacker ético’: personal con conocimientos de hackactivistas pero con una finalidad completamente diferente: buscan la mejora de la ciberseguridad.

Para hacer más atractivo este tipo de plataformas, generalmente cuentan con algún tipo de ranking. No hay mejor manera de involucrar al personal que cuando se le hace competir unos contra otros por un puesto en una clasificación. Cada plataforma tiene sus criterios de puntuación y valora en función del tiempo invertido y del desafío que se resuelva.

Muchas de estas plataformas son de carácter público, en las que cualquiera puede registrarse con acceso libre y gratuito. Sin embargo, hay otras plataformas exclusivamente de pago para la realización de este tipo de ejercicios, como puede ser la plataforma iPhalanx, perteneciente a Indra [40]. No serán éstas objeto de análisis de este apartado, por el simple hecho de que las plataformas gratuitas nos ofrecen unas capacidades similares sin coste alguno, a pesar de que algunas de las siguientes plataformas que estudiaremos no sean enteramente públicas.

2.4.1 Atenea

Atenea [11] (véase Figura 2-6) se presentó el 13 de diciembre de 2017 [41] y es la plataforma oficial de desafíos de seguridad informática del CCN-CERT. Está compuesta de distintos retos que abarcan diferentes campos como criptografía y esteganografía, exploiting, análisis forense, networking y reversing, entre otros. Es gratuita y de carácter público. Los objetivos que persigue son:

- Concienciar al personal TIC sobre los riesgos de la seguridad informática.
- Involucrar al personal con experiencia en seguridad TIC.
- Mostrar al público con menos experiencia en el campo de la ciberseguridad que los retos son divertidos y que no se trata de una ciencia oculta imposible de comprender.

Como muchas de las plataformas, la resolución de los ejercicios exige una serie de normas que deben de cumplirse para conseguir la puntuación correspondiente de cada reto. En concreto, Atenea impone las siguientes normas:

- Cada desafío tendrá una puntuación. Los tres primeros en resolver el reto figurarán en el panel de puntuaciones con las medallas de oro, plata y bronce, respectivamente. El resto de concursantes obtendrán los puntos correspondientes.
- Si se han consumido todos los intentos para resolver un reto, existe la posibilidad de seguir intentándolo, pero sin recibir ningún punto.
- No están permitidos los ataques de denegación de servicio.
- No están permitidos los escaneos automatizados contra la plataforma.
- No están permitidos ataques destructivos (no se podrá modificar ningún desafío ya que se perjudicaría el juego de otros jugadores).
- Es preciso mantener el objetivo en los puntos que están indicados para ello.
- Si aun así se encuentra una vulnerabilidad en su infraestructura o algún atajo para resolver un desafío con mayor facilidad; debe informarse de ello. De esta forma se obtendrá un mayor reconocimiento y puntos de bonificación.
- Las reglas pueden ser cambiadas por los organizadores en el transcurso del desafío.
- En algunas ocasiones, y en función del número de jugadores y el tiempo utilizado para resolver un desafío, se podrá proporcionar alguna pista adicional.
- Los jugadores que no acepten estas reglas podrán ser penalizados o, según el caso, expulsados de forma permanente de la plataforma.

Figura 2-6 Logo de la plataforma Atenea [11]

2.4.2 CTF365

CTF365 [42] (véase Figura 2-7) a diferencia de la plataforma Atenea, no es exclusivamente gratuita. Para hacer uso de ella hay que registrarse, lo que permite tener acceso a todos los servicios que se ofrecen durante un total de 30 días. Una vez cumplido el plazo, la plataforma ofrece diferentes planes de contratación [43] con distintos precios:

- *Student*: 15 $ usuario/mes

  Este tipo de contratación ofrece acceso a todos los servidores de la plataforma.

- *Professional*: 46 $ usuario/mes

  Este tipo de contratación ofrece acceso a todos los servidores de la plataforma y a ejercicios que exigen mayor profesionalidad.

- *Enterprise*: 37 $ usuario/mes

  En esta contratación se tiene acceso a todos los servidores. Además, se puede hacer uso de tres servidores privados virtuales y hay un apartado destinado exclusivamente a ver las estadísticas de las actividades del grupo de personas que lo haya contratado y otro destinado a informes personales.

- *Corporate*: El precio se negocia en el contrato con el colectivo que opte por esta modalidad.

  Este último modelo de contratación cuenta con todos los privilegios del modo *Enterprise* y, a mayores, se añaden: uso interno de la plataforma, punto de acceso, una interfaz privada, una red privada de CTF365, una tabla de clasificación y servicio de atención al cliente con disponibilidad las 24 horas.

Figura 2-7 Logo de la plataforma CTF365 [42]

2.4.3 OverTheWire

OverTheWire [44] (véase Figura 2-8) es una plataforma pública en la que no hay opción para registrarse, por lo tanto, no existe un ranking de puntuaciones ni un registro de los retos completados. Sin embargo, ofrece un servicio de ayuda al público en uno de sus servidores, por si alguna persona tuviese dudas o quisiese contactar con los administradores para obtener información, por medio de IRC (*Internet Relay Chat*) (irc.overthewire.org).

Cada desafío tiene un usuario correspondiente dentro del servidor y para acceder a los retos hay que hacer uso del protocolo SSH (*Secure SHel*). La contraseña del usuario del siguiente reto, y en consecuencia del siguiente nivel, se encuentra en el reto anterior, de manera que no se puede acceder al siguiente desafío si no se supera el anterior. Los retos de esta plataforma son, ante todo, instructivos. Los principales tópicos son: seguridad en las webs, programación, exploiting, vulnerabilidades en códigos y reversing, además de una serie de ‘juegos’ basados en ciberseguridad.

Esta plataforma, al ser expresamente gratuita, se sostiene gracias a donaciones de personas que, sin ánimo de lucro, realizan donaciones para mantener activa la plataforma [45].

Figura 2-8 Logo de la plataforma OverTheWire [44]

2.4.4 Hacking-Lab

Hacking-Lab [46] (véase Figura 2-9) es una plataforma en la que el registro y el acceso a los retos son gratuitos. Sin embargo, cuenta con una opción de pago de 49 €/año en la que el usuario pasa a tener la categoría de miembro de la plataforma. Esta opción de pago otorga al usuario una serie de privilegios como:

- Acceso a eventos especiales.
- Descuentos en eventos de novedad.
- Participación en el ranking de retos.

Para participar en los retos es necesario tener instalado en el equipo personal VirtualBox o VMware y cargar en uno de estos programas el *LiveCD* [47] que se puede descargar en la propia página de Hacking-Lab. El segundo paso sería conectarse a la VPN (*Virtual Private Network*) de Hacking-Lab y acceder a la cuenta de registro desde el buscador *Mozilla Firefox* de la máquina virtual.

Una vez conectados, sería cuestión de escoger un reto, llegar a la solución correcta, demostrar la vulnerabilidad y explicarla. Los ejercicios de esta plataforma [48] son variados y están centrados en pruebas de penetración de redes, respuesta a incidentes, análisis forense digital y entrenamientos de seguridad. Esta plataforma también cuenta con un chat público en el que las personas pueden comentar libremente dudas e intercambiar información con otros usuarios.

Figura 2-9 Logo de la plataforma Hacking-Lab [46]

2.4.5 Pwnable.kr

Pwnable.kr [49] (véase Figura 2-10) es una plataforma no comercial que ofrece varios desafíos de pwn (en la jerga del *script kiddie*, pwn hace referencia a tomar el control de otra computadora, sitios web, dispositivo de puerta de enlace o aplicación [50]) con respecto a la explotación del sistema. El objetivo principal de esta plataforma es la diversión. A su vez, durante la superación de retos, una persona puede aprender/mejorar las habilidades de hackear un sistema.

Para llegar a las soluciones de los retos hacen falta algunos conocimientos básicos de: programación, ingeniería inversa, explotación de errores, conocimiento del sistema y criptografía. Cada desafío tiene la solución prevista del autor, sin embargo hay muchas soluciones alternativas. Los desafíos de esta plataforma se dividen en cuatro categorías:

- *Toddler's Bottle*: desafíos muy simples con errores muy simples.
- *Rookies*: desafíos típicos de explotación de errores para novatos.
- *Grotesque*: estos desafíos requieren de una mayor experiencia y conocimientos en el campo de la informática.
- *Hacker's Secret*: es el conjunto de desafíos de mayor complejidad y para llegar a una solución hace falta aplicar técnicas concretas y especiales de cada campo de la informática.

Esta plataforma tiene un servicio de contacto al administrador como el resto de plataformas con el fin de obtener más información de la misma. Además ofrece la oportunidad de registrarse y competir en el ranking de retos de forma totalmente gratuita.

Figura 2-10 Logo de la plataforma Pwnable.kr [49]

2.4.6 IO

IO [51] (véase Figura 2-11) es una plataforma de retos de ciberseguridad que pertenece a los creadores de netgarage.org. Éste fue un proyecto comunitario fundado en 2002 con el objetivo de compartir conocimientos e intereses acerca de códigos, seguridad, tecnología, fuentes abiertas, inteligencia artificial, comercio automatizado, realidad virtual, interfaces informáticas y diversión.

Es también la plataforma principal de los retos de ciberseguridad IO, ya que estos retos no dejan de actualizarse y existen diferentes versiones de radare2 y gdb tales como IO64, IOarm o IO07, siendo IO el principal apartado.

Para conectarse al servidor y a los diferentes retos, hay diferentes usuarios: ha de hacerse a través del protocolo SSH. Es de carácter gratuito y no ofrece un servicio de registro de usuario, pero como el resto de plataformas, proporciona un servicio de ayuda a través de IRC (irc.netgarage.org).

Figura 2-11 Logo de la plataforma IO [51]

2.4.7 SmashTheStack

SmashTheStack [52] (véase Figura 2-12) es una plataforma de retos de ciberseguridad abierta al público y de carácter gratuito, cualquier persona con nuevas ideas o retos es bien recibida para contactar con los administradores. No ofrece servicio de registro y, puesto que es gratuita, está abierta a donaciones públicas para poder seguir activa.

Esta plataforma ofrece nuevamente un servicio de ayuda a través de IRC (irc.smashthestack.org). Para acceder a los retos ha de accederse a través del protocolo SSH, ubicándose cada reto en un usuario diferente del servidor. A medida que se van obteniendo las respuestas de los diferentes niveles, se nos proporciona la contraseña del usuario para realizar el siguiente reto.

SmashTheStack, IO y OverTheWire [53] son plataformas íntimamente ligadas entre sí. Las tres son de carácter gratuito y no ofrecen registro de usuarios. Todas ellas tienen disponibles los retos en servidores a los cuales hay que acceder a través del protocolo SSH. Además, al tratarse de plataformas públicas, comparten retos y desafíos entre ellas, ofreciendo estos servicios al público.

El tipo de retos de esta plataforma sigue la línea de sus dos compañeras: romper códigos, programación, vulnerabilidades de códigos, seguridad de la web, reversing, exploiting, etc.

Figura 2-12 Logo de la plataforma SmashTheStack [52]

2.4.8 Microcorruption

Microcorruption [54] es una plataforma en la cual los diferentes retos están orientados a un único juego: encontrar vulnerabilidades en códigos. Este juego es conocido en la web como "*Capture the flag*" y consiste en explotar vulnerabilidades de los diferentes sistemas que se le proporcionan al usuario e ir obteniendo unas claves para abrir "puertas" y llegar así hasta el último nivel, en el cual el usuario "captura la bandera".

Este juego comienza con una dificultad muy baja en el cual cualquier usuario que se registre y participe, con los conocimientos adquiridos de Wikipedia sabría comenzar a jugar. La propia web incita a probar el desafío partiendo de conocimientos básicos [55]. El registro es gratuito y, como tal, esta plataforma tiene a disposición de quien lo desee un servicio de donación de dinero.

Ofrece además un servicio de ayuda y de obtención de información para cualquiera que lo solicite mediante: email (support@microcorruption.com), twitter (#uctf @tqbf @n0nst1ck) e IRC (irc.freenode.net #uctf).

2.4.9 Reversing.kr

Reversing.kr [56] es una plataforma gratuita con servicio de registro para cualquier usuario. Está especializada en retos acerca del *cracking* y la ingeniería inversa. A diferencia de otras plataformas, reversing.kr no tiene retos de actualidad ya que la última actualización fue en diciembre de 2014, sin embargo, ofrece la oportunidad de realizar retos específicos de los diferentes sistemas operativos [57].

Su servicio de ayuda se lleva a cabo mediante email: gogil@reversing.kr.

2.4.10 HackThisSite

HackThisSite [58] (véase Figura 2-13) es una plataforma de entrenamiento gratuita, segura y legal en la que los hackers éticos pueden ampliar sus habilidades en el ámbito de la ciberseguridad. Se trata también de una comunidad bastante activa con muchos proyectos en desarrollo, con una amplia selección de retos y un foro donde los usuarios pueden hablar sobre tópicos de la piratería informática, la seguridad de la red, etc.

Esta plataforma es una de las plataformas de ciberseguridad con mayor impulso, debido a que la filosofía de ésta no sigue la línea del resto de plataformas. Mientras la finalidad del resto de plataformas era incrementar los conocimientos en ciberseguridad y la diversión del usuario, HackThisSite orienta su página a un movimiento contra la injusticia social. Esta plataforma, si bien no alienta ni participa en actividades ilegales, defiende la piratería y el hacktivismo como medio de lucha para combatir la opresión, la desigualdad o la censura. Anima a sus usuarios a compartir esta línea de pensamiento siempre y cuando se hagan responsables de sus actos. Como dato curioso, el fundador de esta página web, Jeremy Hammond, fue detenido en 2005 por el FBI debido a que un grupo de hackers pertenecientes a HackThisSite se infiltraron en la base de datos de una organización y obtuvieron información de tarjetas de crédito que, posteriormente, se utilizaron para robar dinero y donarlo a una serie de organizaciones sin ánimo de lucro [59].

Los retos son diseñados y subidos a esta plataforma por los usuarios más experimentados, y los tópicos de estos retos son: retos básicos para principiantes, hackeo de aplicaciones, desafíos de esteganografía, vulnerabilidades de JavaScript, programación, exploiting, etc.

Para contactar con los administradores de la plataforma se puede hacer por mail (irc@hackthissite.org). Esta página web no solo dispone de una plataforma para actividades de hacking, sino que también cuenta con servicios como una tienda online, destinada a la venta de ropa o artículos de adorno.

Figura 2-13 Logo de la plataforma HackThisSite [58]

2.4.11 W3Challs

W3Challs [60] es una plataforma de entrenamiento de pruebas de penetración que apareció en mayo de 2009, pero fue en junio de 2010 cuando comenzó a funcionar. Ofrece varios desafíos informáticos relacionados con la seguridad: piratería, crackeo, análisis forense, criptografía, esteganografía y programación.

El objetivo de esta plataforma es ofrecer desafíos realistas sin simulación. Ofrece la oportunidad de probar las habilidades de hacking resolviendo los retos e incluso reta al usuario a hackear la propia plataforma. Sin embargo, acciones como fuerza bruta o ataques de denegación de servicio están prohibidos.

Para acceder a los desafíos hay que registrarse como usuario gratuitamente. Es una plataforma pública y no cuenta con servicio de pago. Ésta es una plataforma que, nuevamente, establece un ranking y una valoración de puntos en función de los desafíos que se hayan completado. Al igual que el resto de plataformas gratuitas, esta web está abierta a todo tipo de sugerencias y retos que los usuarios se presten a proporcionar.

El servicio de ayuda establecido es mediante mail (awe@w3challs.com).

2.5 Arquitectura de las redes

La arquitectura de una red consiste en el diseño de una red de comunicaciones y, en función de ello, se define el grado de seguridad de dicha red. Calificaremos como red segura a aquella cuya exposición a Internet sea mínima y, por el contrario, como red expuesta y vulnerable a aquella que se encuentre directamente en Internet. El elemento que definirá la relación entre una red e Internet se

denominará firewall. Más concretamente, este firewall es la parte del sistema de una red que bloquea los accesos no autorizados y permite las comunicaciones autorizadas.

Por lo general, las redes de las empresas se estructuran según tres partes: Internet, DMZ (*DeMilitarized Zone*) e intranet. Estas redes deben, por un lado, estar seguras de las ciberamenazas que se encuentran en el exterior, entendiendo éste como la zona de Internet, y por otro lado, deben ofrecer servicios al público a los que se puedan acceder desde el exterior. A continuación se explicará en más detalle cómo funciona este tipo de arquitectura de red:

Internet: entendiendo el firewall como el límite de una red privada, Internet es todo aquello que hay de puertas a fuera a partir de dicho firewall, siempre y cuando éste se encargue de hacer un filtrado de IP's del exterior que se disponen a entrar en nuestra red privada.

DMZ: es una zona insegura que se encuentra entre Internet e intranet, perteneciendo a la sección de la red privada (recordemos que el firewall dividía en dos secciones: Internet e Intranet). En esta zona insegura es donde se sitúan los diferentes servicios de la red privada que están a disposición del público [61].

Intranet: ésta es la base de la red privada. En ella se encuentran los equipos conectados y debe ser una zona aislada de Internet mediante el firewall.

La configuración más común es la que se puede observar en la Figura 2-14, pero hay otras posibilidades de arquitectura de red en las que se aísla la DMZ con el router y la intranet con el firewall, o casos en los que se hace uso de dos firewalls, uno para aislar la DMZ y otro para aislar la intranet.

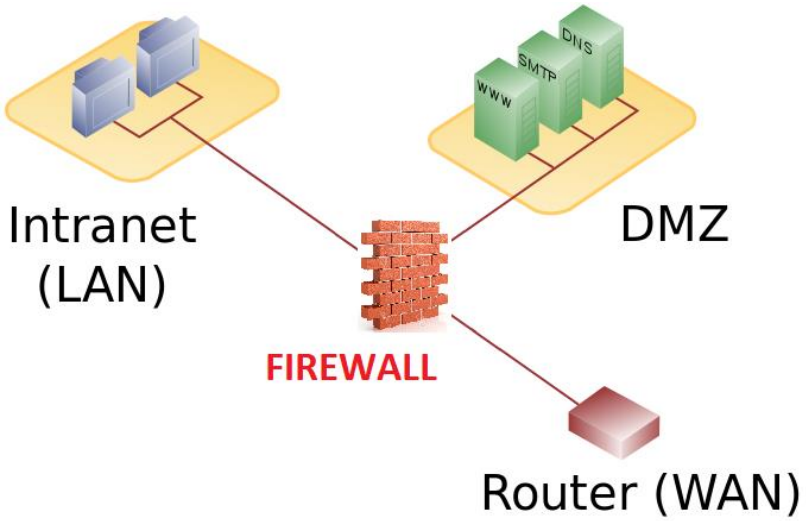


Figura 2-14 Arquitectura de red estándar [62]

2.6 Virtualización

En informática, llamamos virtualización a la versión virtual de algún recurso tecnológico, ya sea un sistema operativo, una plataforma de hardware, un dispositivo de almacenamiento, la simulación de una red, etc. Explicado de otra forma, puede decirse que la virtualización es la abstracción de los recursos de una computadora de manera que se cree una capa entre el hardware de la máquina física y el sistema operativo de la máquina virtual [63].

Dentro de la virtualización, existen diferentes formas para hacer uso de ella: virtualizar el hardware del servidor, virtualizar el software del servidor, virtualizar aplicaciones y, el concepto que mayor interés tendrá para este proyecto, crear máquinas virtuales y redes. Esto se debe a que la implementación y diseño del ataque de ciberdefensa que se desarrollará posteriormente, se hará sobre una serie de máquinas virtuales en una red privada.

Dentro de las ventajas que ofrece la virtualización, podemos destacar:

- Optimizar y reutilizar el hardware existente de una máquina.
- Reducir costes de espacio y consumo en proporción a lo que una máquina física nos demandaría.
- Administración global centralizada y simplificada.
- Mayor facilidad para la creación de entornos de test que permiten poner en marcha nuevas aplicaciones sin impactar a la producción, agilizando el proceso de las pruebas.
- Aislamiento: un fallo general de sistema de una máquina virtual no afecta al resto de máquinas virtuales.
- Reduce los tiempos de parada.
- Migración de máquinas virtuales de un servidor a otro sin pérdida de servicio, eliminando así paradas planificadas debido al mantenimiento de un servidor.
- Contribución al medio ambiente por menor consumo de energía en servidores físicos.

En relación con este trabajo, la virtualización ha supuesto un avance en el concepto de ciberataques y ciberseguridad. Cuando antes estas prácticas debían llevarse a cabo en redes y equipos reales, cualquier incidente o problema tenía repercusiones importantes, por lo que ninguna empresa quería prestarse voluntaria para realizar estas prácticas sobre sus equipos. Con la innovación de la virtualización, esto ya no supuso un problema. Como se ha comprobado en la sección 2.4, la gran mayoría de plataformas para practicar ejercicios de pentesting cuentan con servidores virtuales, donde la mayor amenaza que puede haber es que un ciberataque haga caer el servidor virtual, sin suponer esto grandes problemas.

Dentro del software de virtualización, podemos destacar los siguientes programas: VirtualBox, KVM, XEN y VMware vSphere Essentials. Para una revisión detallada de estos programas, remitimos al capítulo 2 del TFG del Tte Romero Fernández [12].

A continuación veremos algunas de las características de VirtualBox, ya que es este software sobre el que implementaremos la maqueta de máquinas virtuales en red y sobre el que trabajaremos.

2.6.1 VirtualBox

VirtualBox [64] es un software gratuito destinado a la virtualización que trabaja como una aplicación más dentro de un hardware real con su propio sistema operativo. La principal característica de este tipo de hipervisores es la no interactuación entre los sistemas operativos de las máquinas virtuales y el hardware de la máquina real, consiguiendo además un completo aislamiento entre las máquinas virtuales. Los sistemas operativos que puede soportar VirtualBox son: Windows, Linux, Solaris OS y Mac OS.

VirtualBox no tiene capacidad límite para soportar máquinas virtuales. La única restricción que tiene es la potencia del cliente que esté ejecutando dicha aplicación, siendo éste el factor condicionante del rendimiento del software.

3 DISEÑO Y DESARROLLO DEL CIBEREJERCICIO

3.1 Introducción

En este capítulo se diseñará e implementará un ciberejercicio de ataque que tiene por finalidad adiestrar a quien lo ejecute en determinadas técnicas que describiremos más adelante. Para hacer más atractiva la ejecución del ejercicio, hemos decidido ambientarlo en el yihadismo ya que se trata de un tema de actualidad. Dicho de otro modo, el ciberejercicio consistirá en localizar una red yihadista a partir del estudio de una web de una ferretería online. Una vez localizada dicha red, deberemos ir infiltrándonos, empezando por el control de uno de los servidores de la DMZ y terminando con el acceso del usuario administrador de la red local. En la cuenta de este último usuario, encontraremos información clasificada de la que podremos extraer un plan de un atentado terrorista.

3.1.1 Ciberejercicio

El ciberejercicio se diseñará e implementará sobre una maqueta de máquinas virtuales en red [12] ya diseñada y estructurada, resultado del TFG del Tte. Romero Fernández. Este escenario virtual nos permitirá actuar en un entorno controlado el cual iremos modelando en función de la dificultad que queramos establecer en dicho ciberejercicio. La idea es crear un escenario en el cual obliguemos al alumno que realice el ciberejercicio a familiarizarse con algunos de los diferentes campos de la ciberseguridad. Por ello, a lo largo del próximo ciberejercicio se tratarán diversos temas como: la esteganografía, el estudio de paquetes de red, ataques de fuerza bruta, la importancia de la ingeniería social, etc. En la Figura 3-1 se puede ver a rasgos generales los pasos que el alumno deberá seguir durante el ciberejercicio.

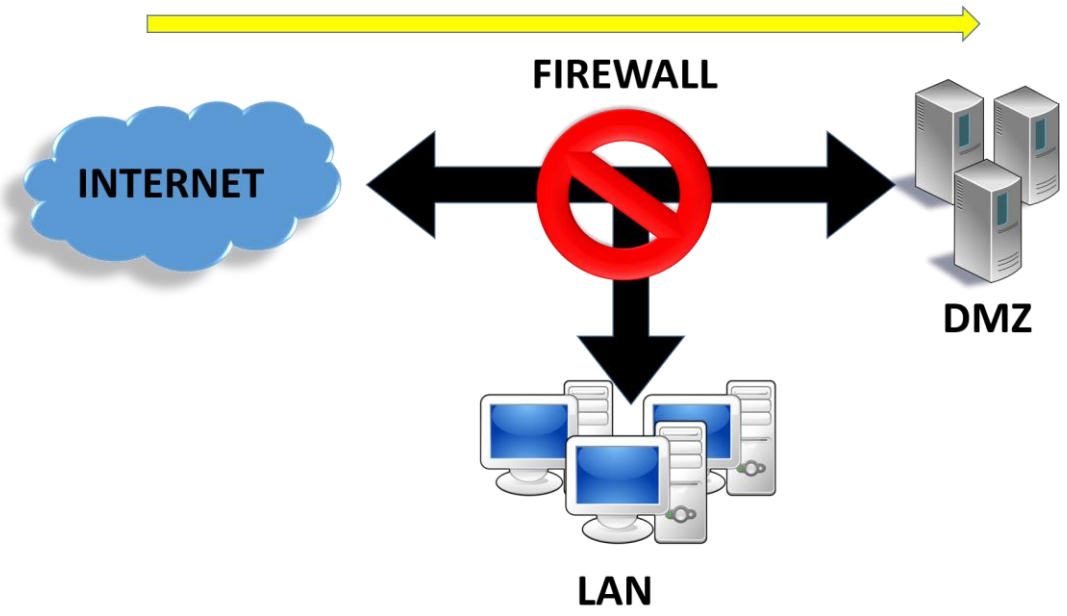


Figura 3-1 Acceso a la DMZ

Tras proporcionarle al alumno la entrada a la DMZ desde el exterior, se le irá guiando para acceder a la red LAN de la maqueta. Para ello, como muestra la Figura 3-2, deberá modificar el firewall de la red.

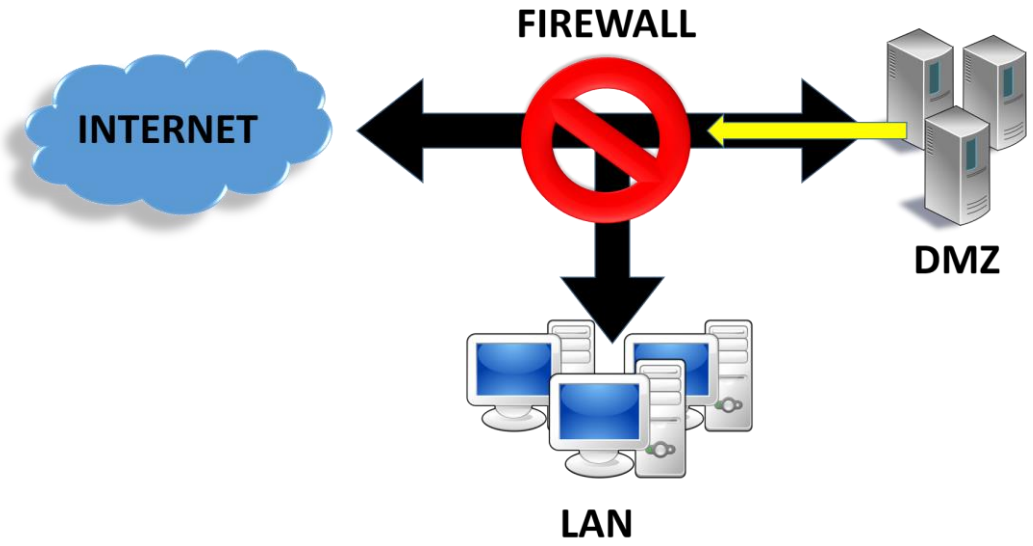


Figura 3-2 Modificación del firewall

Una vez las reglas del firewall sean modificadas, como se ve en la Figura 3-3, el alumno deberá conseguir introducirse en uno de los equipos de la red LAN y obtener la información que necesita.

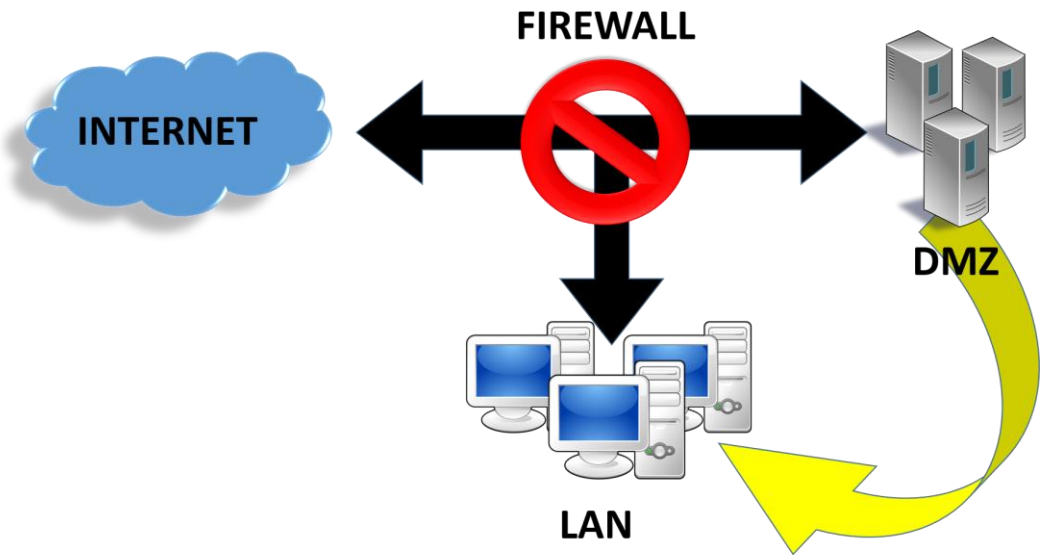


Figura 3-3 Acceso a la LAN

El nivel de dificultad del ciberejercicio se categorizará como un nivel medio/bajo destinado a personal con pocos conocimientos informáticos.

3.2 Herramientas del entorno hardware

3.2.1 Ordenador portátil (estación de trabajo)

Como se puede ver en la Figura 3-4, se trata de un ordenador portátil de la marca *Lenovo* desde el cual trabajaremos en el diseño del ciberejercicio. A través de este ordenador nos conectaremos al servidor donde se encuentra cargada la arquitectura de red de nuestra maqueta virtual, la cual controlaremos desde nuestra estación de trabajo. No es necesario utilizar un ordenador de elevadas prestaciones.

Las características de esta máquina son:

- Ordenador portátil: *Lenovo 80EW*
- Procesador: *Intel® Core™ i3-5010U CPU @* 2.10GHz, 2100 MHz, 2 procesadores principales, 4 procesadores lógicos.
- Memoria RAM: 4,00 GB
- Tarjeta gráfica: *Intel® HD Graphics 5500 2GB*

Figura 3-4 Ordenador Lenovo [65]

3.2.2 Ordenador portátil (análisis de seguridad)

Para la comprobación del ciberejercicio diseñado, se utilizará un ordenador que cubra las necesidades de un usuario medio. Éste es un ordenador de la gama HP. Algunas de sus características son:

- Ordenador portátil: *HP EliteBook 8470p*
- Procesador: *Intel® Core™ i5-3210M CPU* @ 2.50GHz, 2500 MHz x 4
- Memoria RAM: 4,00 GB
- Tarjeta gráfica: *Intel® 3ª gen. Core™ processor Graphics Controller*

3.2.3 Servidor

Como se aprecia en la Figura 3-5, el servidor es la plataforma física a través de la cual trabajaremos. El servidor deberá tener la suficiente capacidad para poder ejecutar todas las máquinas virtuales que compongan nuestra maqueta virtual de simulación de red. En este caso, se tratará del servidor *Dell Poweredge R530*.

Este servidor se encuentra en la sala de servidores del CUD (Centro Universitario de la Defensa). Su conexión a la red se ha realizado mediantes dos de sus interfaces: una conectada a la red pública y otra, identificada como LABORATORIOS, conectada a la red local del CUD. Este servidor se llama *dunquerque* y su dominio es *dunquerque.cud.uvigo.es.*

Sus especificaciones son las siguientes:

Procesador: *Intel Xeon E5-2620v3*

- 12 procesadores lógicos (6 núcleos físicos)
- Velocidad de reloj 2,4 GHz
- Caché: 15 MB

Memoria RAM: 16 GB DDR4

Disco duro:

- 2x SAS 300GB (RAID 1)
- 2x SATA 1TB (RAID 1)

4 Adaptadores de red *Gigabit Ethernet*

Figura 3-5 Servidor dunquerque [12]

3.3 Herramientas del entorno software

3.3.1 Ordenador portátil (estación de trabajo)

Actualmente, la estación de trabajo personal tiene creada una partición del disco duro en la que se han instalado dos sistemas operativos. En una de ellas, se encuentra el sistema operativo del ordenador por defecto, *Windows 10*, y en la otra partición, se encuentra instalada una distribución de Linux, en

concreto *Ubuntu 16.04*. Este último sistema operativo será el utilizado para interactuar con la maqueta virtual y con el que se trabajará.

3.3.1.1 VirtualBox

VirtualBox [64] (ver Figura 3-6) será el software utilizado para la simulación tanto de las máquinas de la red virtual como de las máquinas que crearemos en nuestro cliente para después incorporarlas a la maqueta virtual. Se ha elegido este software porque es el utilizado por las máquinas que conforman la arquitectura de red virtual.

Para su instalación simplemente deberemos escribir en el terminal lo siguiente:

$ sudo apt-get install virtualbox

La versión de VirtualBox con la que trabajaremos será la versión 5.2.6.

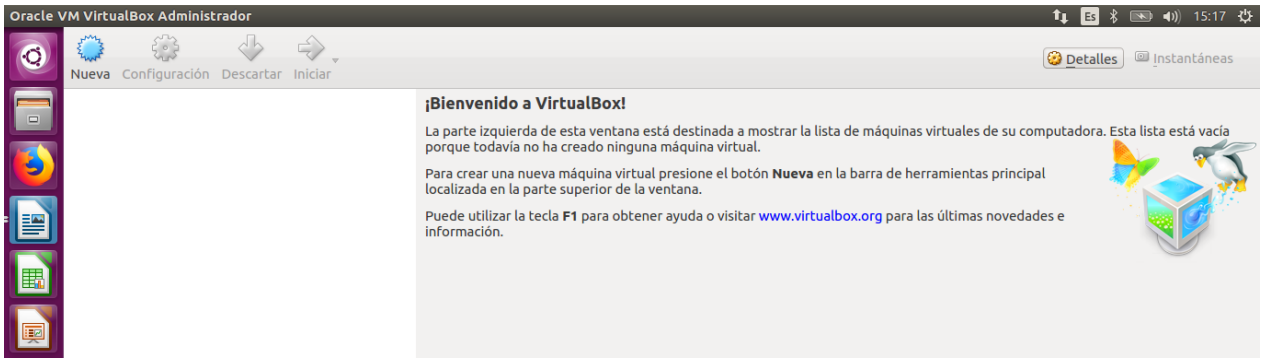


Figura 3-6 Inicio de VirtualBox

3.3.1.2 GNS3

GNS3 [66] es un simulador gráfico de red que permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellas.

Para instalar GNS3, deberemos adaptarnos a la versión de GNS3 que se encuentra instalada ya en el servidor dunquerque. En este caso, instalaremos la versión 1.4.0. Para ello deberemos instalar primero un nuevo repositorio.

$ sudo apt-get install python3-pip

Y seguidamente instalaremos los paquetes de GNS3.

$ sudo pip3 install gns3-gui==1.4.0

3.3.1.3 KRDC

KRDC [67] (ver Figura 3-7) nos permitirá trabajar por escritorio remoto tanto con el servidor dunquerque como con las máquinas virtuales. Este método de trabajo podría llevarse a cabo mediante una conexión *SSH* y el comando –X, el cual nos ofrecería una interfaz gráfica de la conexión. Sin embargo, debido a prestaciones de velocidad del servicio, utilizaremos KRDC (*KDE Remote Desktop Connection*). Se instalará desde la línea de comandos.

$ sudo apt-get install krdc

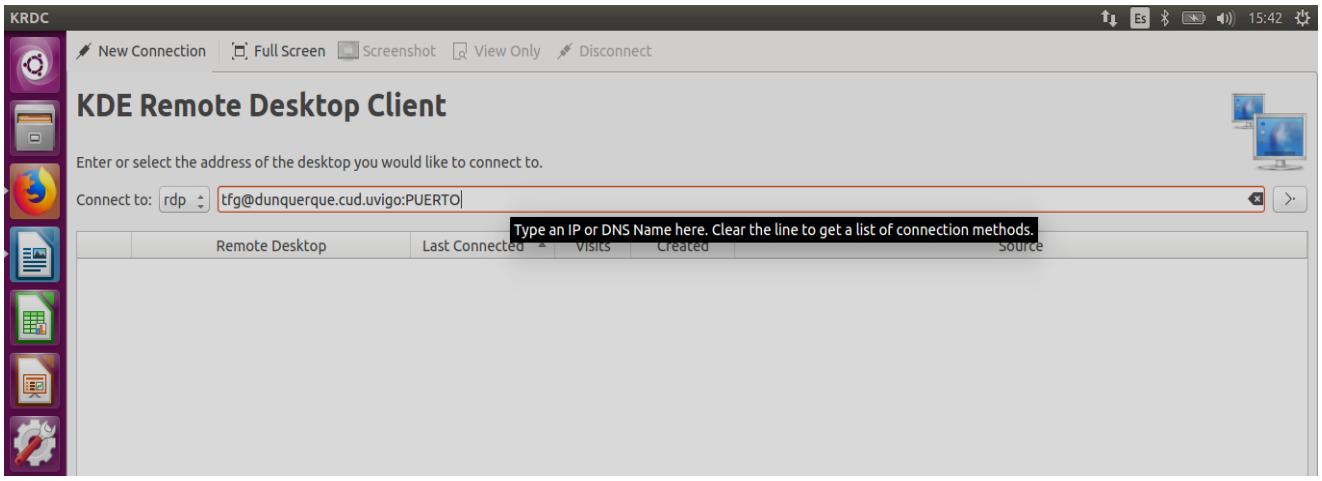


Figura 3-7 KRDC

3.3.1.4 Filezilla

Filezilla [68] será utilizado para la transferencia de archivos entre las máquinas virtuales/servidor dunquerque con nuestra estación de trabajo. Lo utilizaremos principalmente para transferir máquinas virtuales entre el servidor y el cliente y para transferir a nuestra estación de trabajo la arquitectura de red, ya que este proyecto es necesario abrirlo con GNS3-cliente para cargar la arquitectura de red. Lo instalaremos desde el propio repositorio de Ubuntu.

$ sudo apt-get install filezilla

3.3.1.5 SSH

SSH [69] es utilizado para conectarse a un servidor de forma remota de manera segura. Permite el control del servidor mediante un intérprete de comandos y trabaja en el puerto TCP 22 por defecto. Además nos permite copiar datos de forma segura, gestionar claves RSA (*River, Shamir, Adleman*) y redirigir el tráfico para poder ejecutar programas gráficos de manera remota. Se puede instalar desde el repositorio de Ubuntu mediante el siguiente comando.

$ sudo apt-get install ssh

3.3.2 Ordenador portátil (análisis de seguridad)

Este ordenador tiene instalado como sistema operativo la versión 2018.1 de Kali Linux. Este sistema operativo está orientado al uso de herramientas que estudian la ciberseguridad. Dentro de las herramientas de este software, nosotros utilizaremos Nmap, Hydra, Wireshark, Wpscan y Websploit.

Nmap (Zenmap la versión gráfica) [70] es una herramienta que permite a un usuario escanear los equipos de una red y así obtener información sobre estos, concretamente información sobre los puertos y los servicios activos en dichos equipos. Para ello, Nmap envía paquetes definidos a otros equipos y analiza sus respuestas. Este software posee varias funciones para sondear redes de ordenadores, incluyendo detección de equipos, servicios y sistemas operativos.

Hydra [71] es una herramienta destinada a la fuerza bruta. Permite el uso de diccionarios que, a base de prueba y error, descifran los usuarios y las claves de diferentes servicios.

Wireshark [72] es una herramienta utilizada para realizar análisis y solucionar problemas en redes de comunicaciones, para el desarrollo de software y protocolos, y como herramienta didáctica. Cuenta con las características de un analizador de protocolos y permite filtrar y organizar la información capturada. De este modo, permite ver todo el tráfico que pasa a través de una red, estableciendo la configuración de la interfaz de red en modo promiscuo.

Wpscan [73] es una herramienta especializada para escanear páginas web sobre Wordpress. Define la versión utilizada de Wordpress y las vulnerabilidades a las que está expuesta la web. También incluye un módulo de fuerza bruta para hacer frente a la interfaz de administración de Wordpress.

Websploit [74] es una herramienta dedicada a la explotación de vulnerabilidades y ataques en red. Contiene un total de dieciséis módulos divididos en módulos web, red, explotación y wifi. Para la utilización de esta herramienta solo es necesario cargar el módulo deseado, introducir los parámetros necesarios y ejecutar la acción.

3.3.3 Servidor

En el servidor dunquerque se encuentra instalado un sistema operativo Linux, en concreto la distribución *Ubuntu Server 14.04 LTS*. Este sistema operativo es gratuito y se puede descargar directamente de la página oficial de Linux [75].

Este sistema operativo no dispone de entorno gráfico por defecto, por lo que posteriormente a su instalación, se llevó a cabo la instalación de un conjunto de software llamado *Xfce*, que proporciona un sistema de ventanas y escritorio completo. Además, también fue configurada la herramienta *xrdp* para que el servidor pueda ser gestionado desde el protocolo de escritorio remoto RDP (*Remote Desktop Protocol*).

Se encuentra instalado también el software GNS3-server. En el próximo apartado explicaremos el método de trabajo para enlazar GNS3-cliente y GNS3-server.

3.4 Puesta en funcionamiento de la maqueta

3.4.1 GNS3

En el servidor dunquerque se encuentra disponible la maqueta de redes virtuales sobre la que crearemos nuestro escenario para el diseño del ciberejercicio. Para ejecutar la maqueta, será necesario ejecutar GNS3-cliente en nuestro ordenador personal con la arquitectura de red y las máquinas virtuales de la maqueta, y GNS3-server, que se encontrará instalado en el servidor dunquerque y será el encargado de ejecutar la maqueta. De esta manera conseguiremos ejecutar la arquitectura de red sobre el servidor dunquerque en el que se encuentran las máquinas virtuales controlándola desde nuestra estación de trabajo.

Para poder realizar este proceso, primero deberemos configurar el GNS3-cliente y enlazarlo con el GNS3-server del servidor. De esta manera, podremos controlar la arquitectura de red. Para que GNS3-server esté a la escucha en el puerto 8000 del servidor dunquerque, deberemos inicializarlo con el comando:

$ gns3server

Si no quisiésemos iniciarlo cada vez que cerrásemos la conexión, podríamos inicializar GNS3-server como demonio y el comando *disown*:

$ gns3server –daemon disown

A continuación, veremos cómo es el proceso para enlazarlo con el GNS3 del servidor. Lo primero que deberemos hacer es entrar en el diente en *Edit>Preferences>Server* y configurarlo como se muestra en la Figura 3-8.

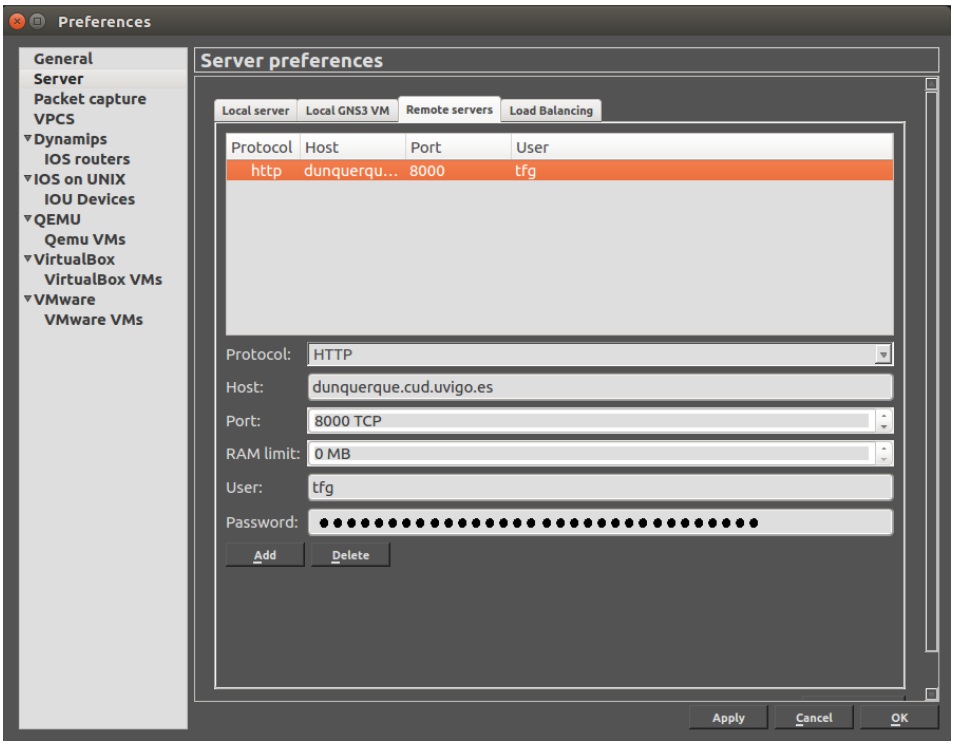


Figura 3-8 Configuración de GNS3

Esto permitirá la conexión al servidor dunquerque y cargar las máquinas virtuales con el asistente. Tampoco debemos olvidar desactivar la opción por defecto de *Enable local server*, ya que nos conectaremos a un servidor remoto.

Para incorporar las máquinas virtuales, deberemos utilizar *Help>Setup Wizard* y, a continuación, seguir los pasos reflejados en la Figura 3-9, Figura 3-10, Figura 3-11 y Figura 3-12, respectivamente.

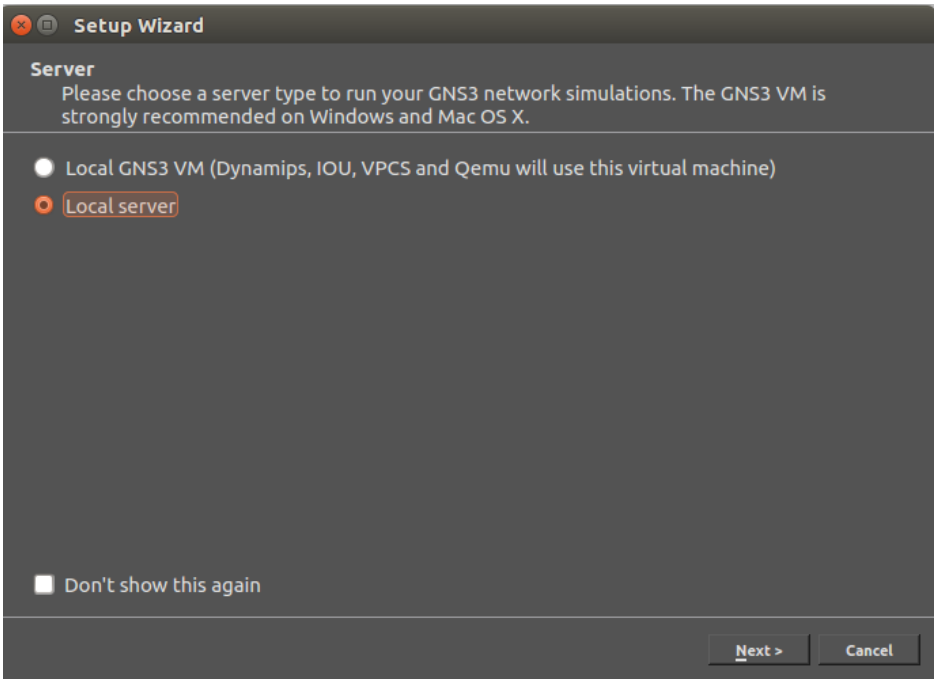


Figura 3-9 *Setup Wizard 1*

En la Figura 3-9, elegiremos dónde deseamos ejecutar la simulación. A continuación, como se puede ver en la Figura 3-10, deberemos indicar que queremos cargar en la arquitectura las máquinas virtuales de VirtualBox.

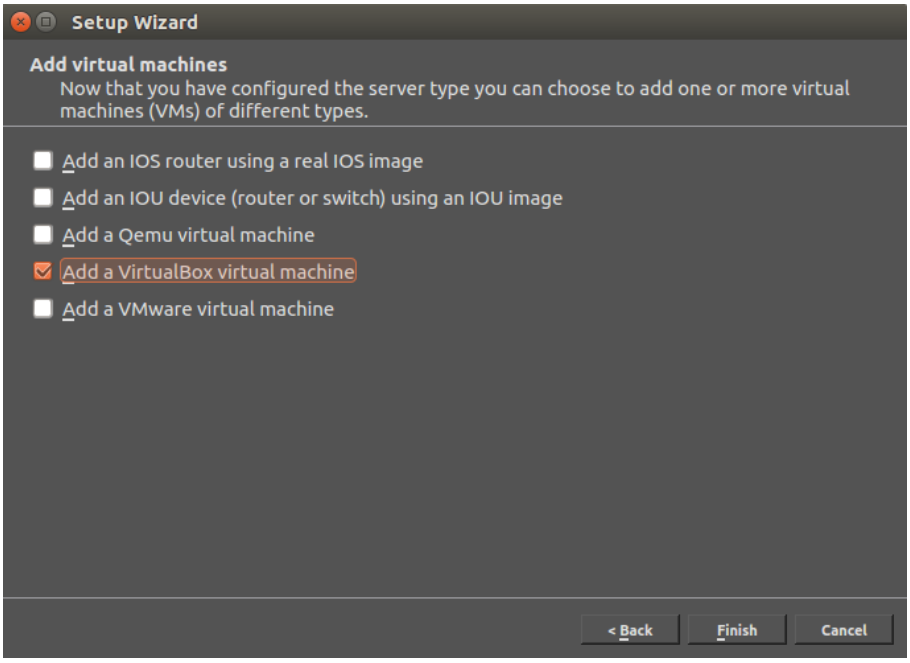


Figura 3-10 ***Setup Wizard 2***

Como se ve en la Figura 3-11, deberemos indicar la ubicación de las máquinas virtuales. En este caso, deberemos indicar que se encuentran en el servidor dunquerque.

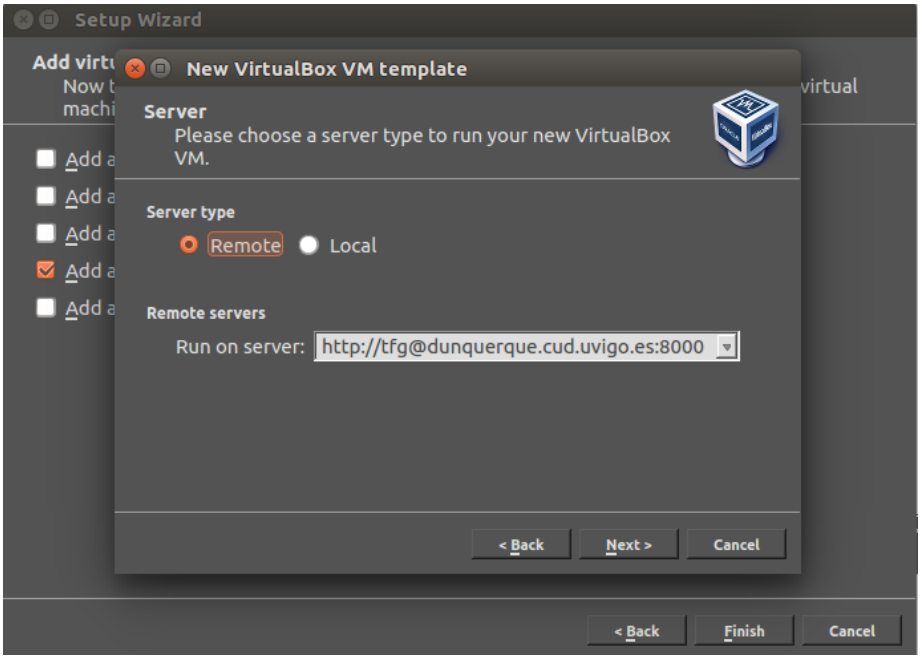


Figura 3-11 ***Setup Wizard 3***

Y por último, como se puede ver en la Figura 3-12, solo quedaría ir cargando de una en una las máquinas del servidor dunquerque. Ya solo faltaría cargar el archivo *TFG2.gns3*, archivo en el cual se encuentra configurada la arquitectura de red que se diseñó en el TFG del Tte Romero Fernández, y dar al botón *play* para lanzar las máquinas virtuales con su arquitectura ya definida.

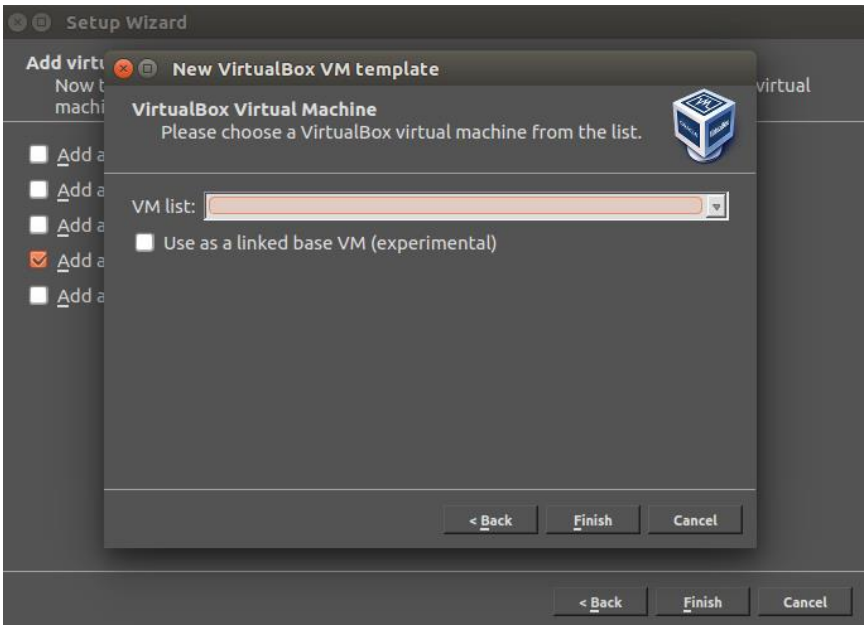


Figura 3-12 ***Setup Wizard 4***

El resultado se puede observar en la Figura 3-13. Aquí ya se pueden ver las conexiones funcionando y la arquitectura de la maqueta de la red virtual.

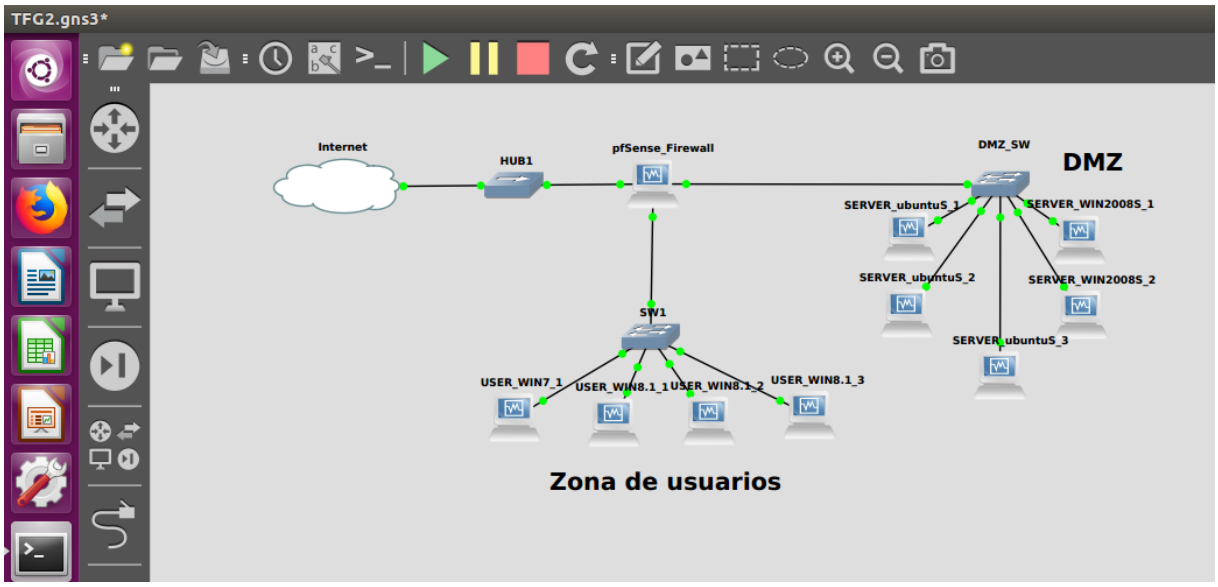


Figura 3-13 Arquitectura inicial de la red virtual

La red inicialmente estará configurada con las máquinas virtuales según se indica en la Tabla 3-1.

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 3-1 Configuración de las máquinas virtuales de la maqueta de red [12]

3.4.1.1 Dificultades asociadas a GNS3

Durante este procedimiento se han encontrado algunas dificultades que no han permitido conectar la arquitectura de red correctamente. A continuación hablaremos de ellas y de cómo se han solucionado.

La primera de ellas se debió a un problema en algunos módulos del kernel [76]. Estos módulos son fragmentos de código que pueden ser cargados y eliminados del núcleo bajo demanda. Algunas veces, estos códigos interfieren con VirtualBox produciendo, como se puede ver en la Figura 3-14, un problema en el software. Para solventarlo y poder hacer uso de VirtualBox en el servidor, donde se cargan las máquinas virtuales, es necesario eliminar y volver a cargar dichos módulos.

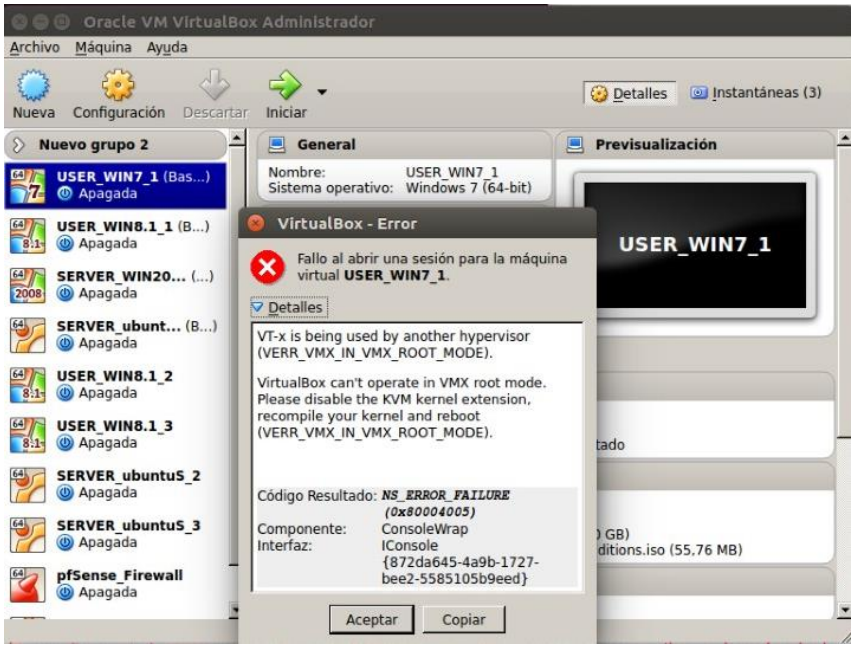


Figura 3-14 Problema en la carga de VirtualBox

El segundo de los problemas, como se puede ver en la Figura 3-15, fue debido a un error en lo que respecta a versiones diferentes entre GNS3-cliente y GNS3-server. La versión actual para descargar GNS3 es la 2.1.3 y la versión que había en el servidor dunquerque era la 1.4.0. Para solucionarlo fue necesario cargar en la estación de trabajo la misma versión que GNS3-server.

$ sudo apt-get install python3-pip

$ sudo pip3 install gns3-gui==1.4.0

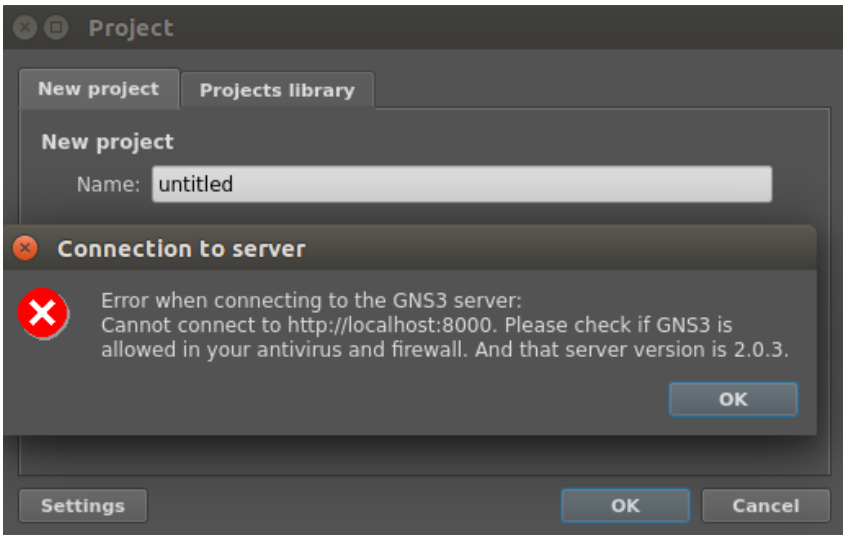


Figura 3-15 Problema con las versiones de GNS3-cliente y GNS3-server

Una vez cargadas las mismas versiones, como se puede ver en la Figura 3-16, apareció un tercer problema, y se debía a uno de los paquetes de *dynamips* de la versión 1.4.0 que hubo que modificar. Para solucionarlo, bastó con instalar la versión compatible de *dynamips* y GNS3-server en el servidor, aunque también se podría haber modificado el paquete de *dynamips* de la versión GNS3-cliente de la siguiente forma.

$ sudo apt-get install libelf-dev

$ sudo apt-get install libpcap0.8-dev

$ git clone git://github.com/GNS3/dynamips.git

$ cd dynamips

$ mkdir build

$ cd build

$ cmake ..

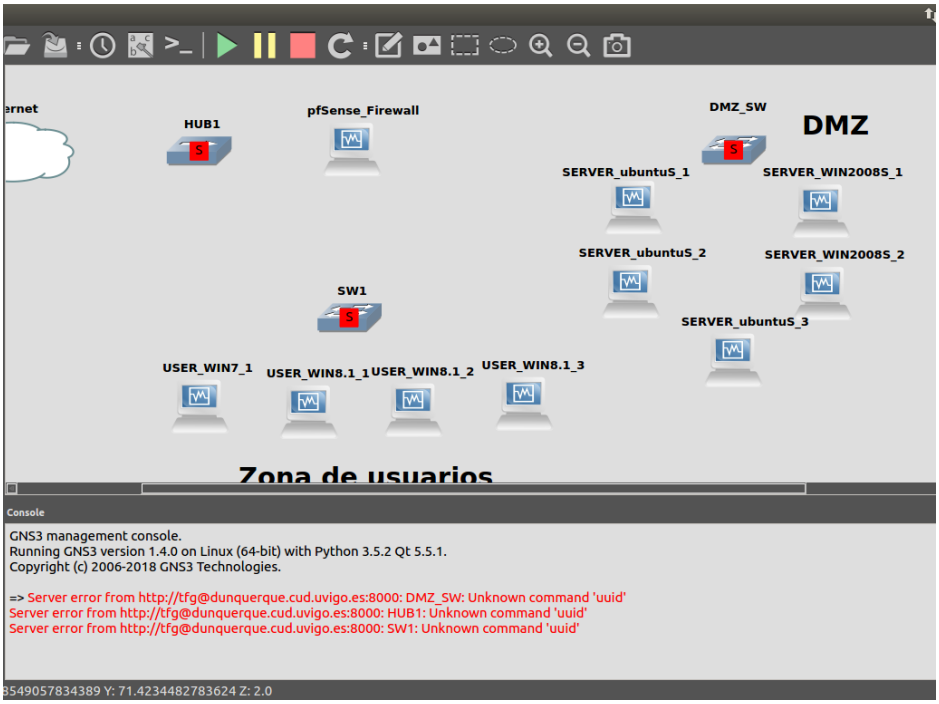


Figura 3-16 Problema en el paquete *dynamips*

El último problema por solucionar, como se puede ver en la Figura 3-17, se debió al paquete de *dynamips* que instalamos en el servidor dunquerque. Este problema causó que hubiese enlaces entre máquinas virtuales, pero no conexión con la nube para la conexión a Internet. Para solucionarlo, hubo que dar permisos de *root* a dicho paquete.

$ chmod root:root dynamips

$ chmod +s dynamips

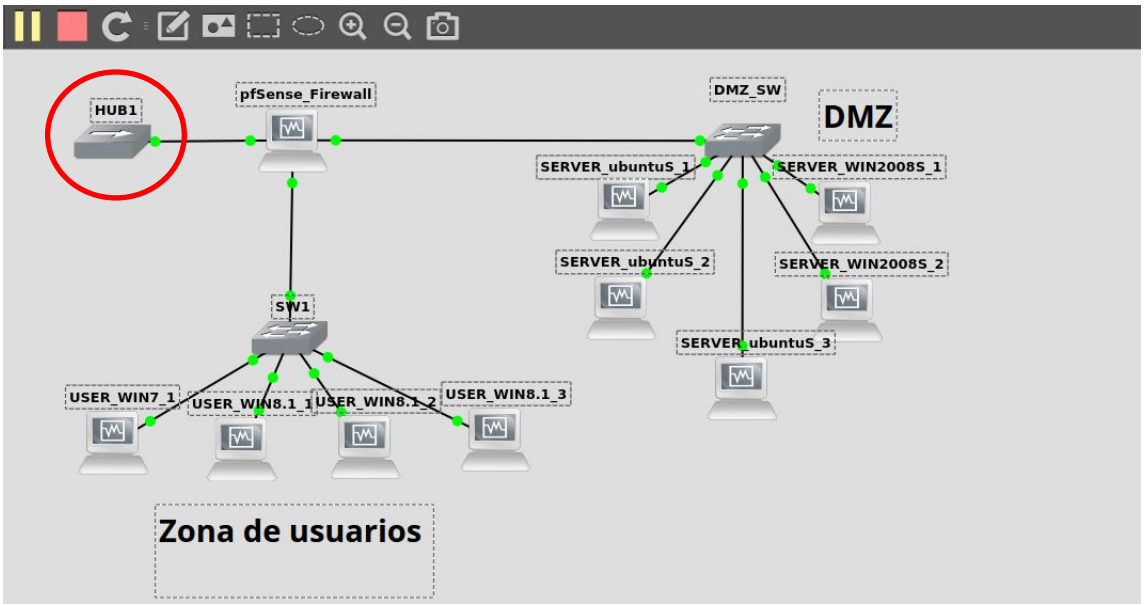


Figura 3-17 Problema en los permisos del paquete *dynamips*

Una vez solucionados todos estos errores, como se puede ver en la Figura 3-18, conseguimos hacer uso de la maqueta virtual desde la red de LABORATORIOS del CUD.

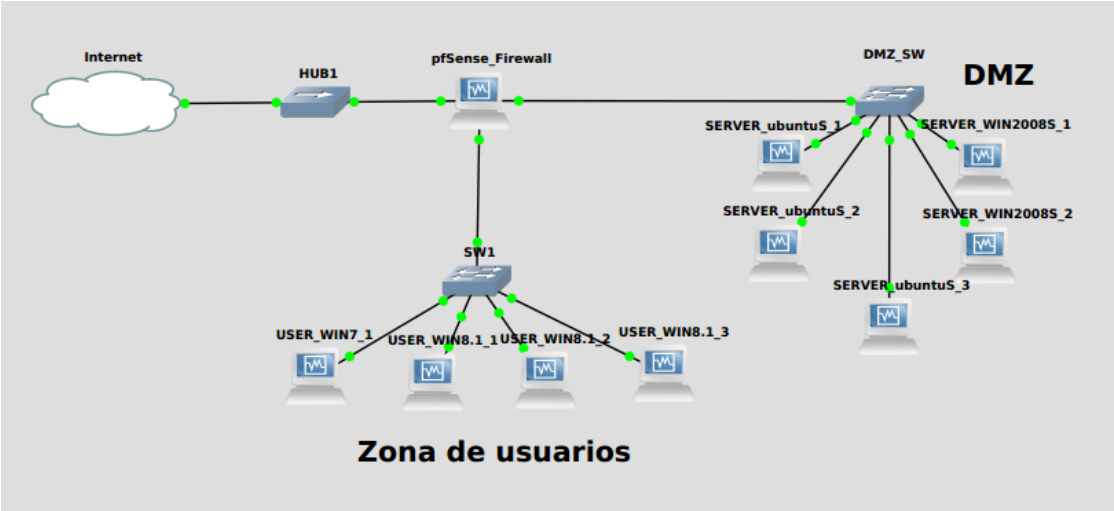


Figura 3-18 Maqueta de máquinas virtuales en red en funcionamiento

3.4.2 Transferencia de ficheros con Filezilla

Para poder cargar la arquitectura de red en nuestra estación de trabajo, deberemos primero transferir el proyecto de GNS3 a través de Filezilla del servidor dunquerque a nuestro equipo. El proyecto, como se puede ver en la Figura 3-19, se encuentra dentro del servidor en *TFG/GNS3/projects/TFG2.gns3*. El puerto en el cual escuchará el servidor dunquerque será el puerto 22.

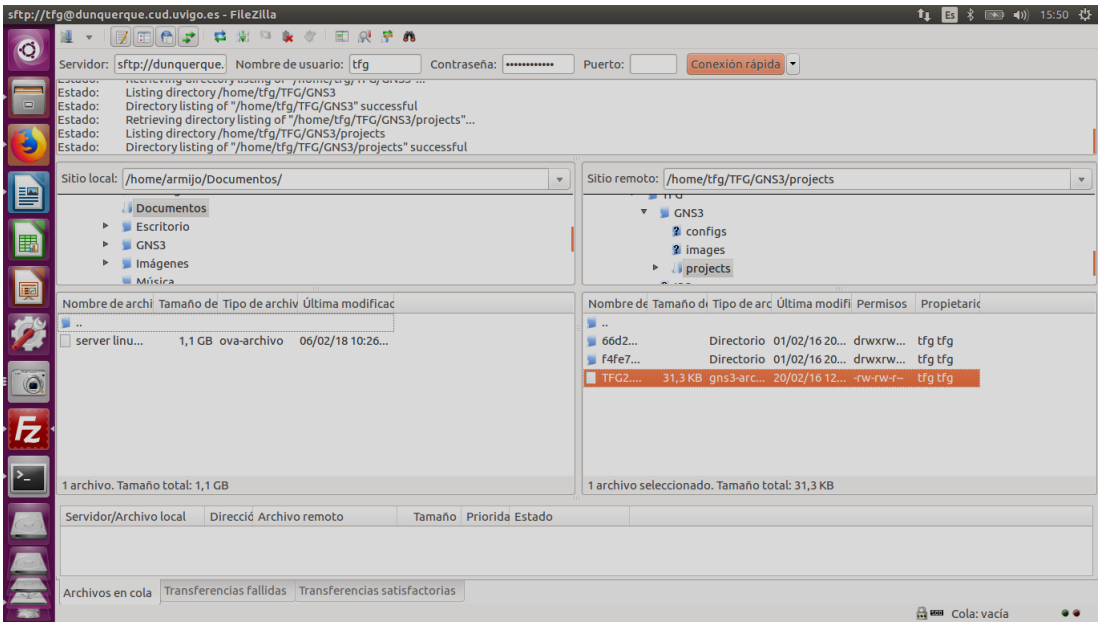


Figura 3-19 Conexión con dunquerque a través de Filezilla

3.4.3 Conexión al servidor

A través del protocolo SSH, como se puede ver en la Figura 3-20, podremos conectarnos desde una terminal al servidor dunquerque. Utilizaremos el comando -X para indicar que la salida gráfica se redirija hacia el cliente. Por defecto nos conectaremos al puerto 22; si quisiéramos conectarnos a través de otro puerto, utilizaríamos el comando –p.

$ sudo ssh tfg@dunquerque.cud.uvigo.es -X

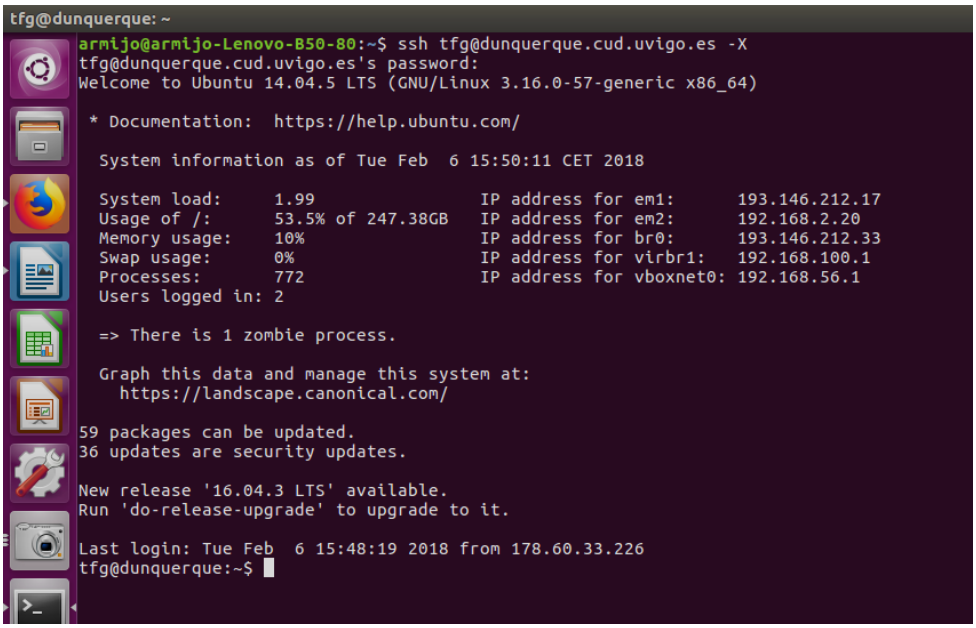


Figura 3-20 Conexión por SSH al servidor

Por lo general trabajaremos a través de escritorio remoto, exceptuando aquellas veces que necesitemos reiniciar tanto el GNS3-server como el software de VirtualBox en el que corren las máquinas virtuales de la red virtual.

3.5 Implementación del ejercicio propuesto en la maqueta

Antes de comenzar el ciberejercicio planteado, crearemos una máquina virtual con el sistema operativo *Ubuntu Server 14.04*, el cual usaremos como servidor web para que sirva de partida como escenario del ciberataque que se va a llevar a cabo. La plataforma elegida para configurar la página web es Wordpress [77], uno de los gestores de contenidos más utilizados en la actualidad. Las razones por las que hemos elegido este software son dos: su alto historial de vulnerabilidades y el gran número de actualizaciones al que ha tenido que hacer frente esta plataforma para ofrecer el nivel de seguridad adecuado. Al tratarse de una plataforma tan extendida a nivel mundial, se ha convertido en uno de los principales objetivos de los ciberatacantes. La versión actual de Wordpress es la 4.9.2. En nuestro caso, instalaremos una de las versiones anteriores, la versión 2.5.1.

Una vez configurada la máquina virtual, deberemos instalar algunos paquetes de software necesarios, conocidos como LAMP (Linux, Apache, MySQL y phpmyadmin), para la instalación de Wordpress.

3.5.1 Apache

Apache [78] es un servidor web HTTP de código abierto que tendrá como función alojar nuestras páginas web, en este caso la que diseñemos con el software de Wordpress. Al igual que ocurrirá con la base de datos de MySQL, Apache podrá ser instalado directamente desde el repositorio de Ubuntu a través de la siguiente línea de comandos.

$ apt-get install apache2

Una vez instalado, para evitar el error "*Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message*" deberemos editar el fichero *apache2.conf*, como se puede ver en la Figura 3-21, y escribir al final del archivo *ServerName localhost* [79].

$ sudo nano /etc/apache2/apache2.conf

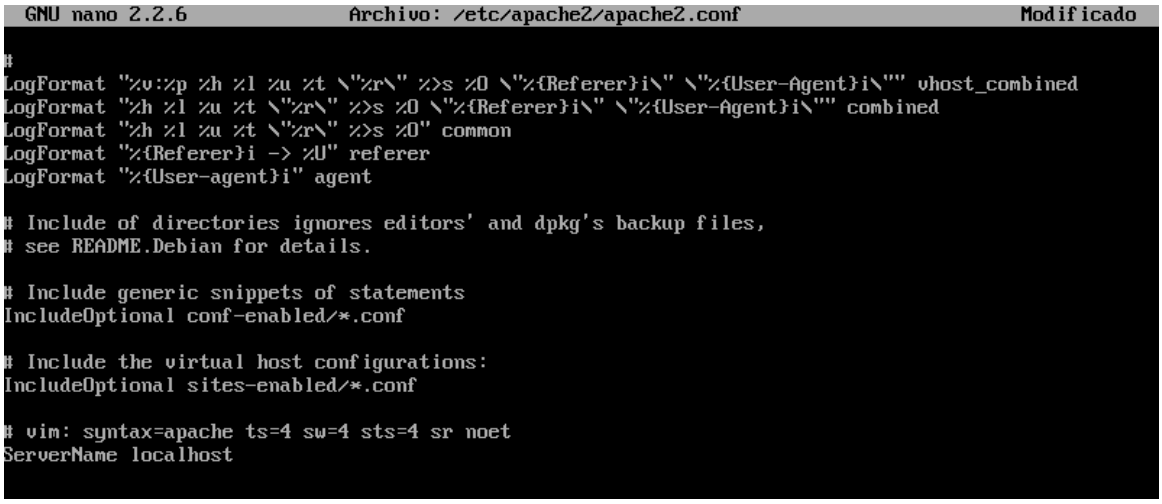


Figura 3-21 Solución del error *ServerName*

Para confirmar la correcta instalación y el funcionamiento de este servidor, bastará con dirigirnos en la web a nuestro dominio (localhost) y, como se ve en la Figura 3-22, deberá aparecer la página de inicio de Apache.

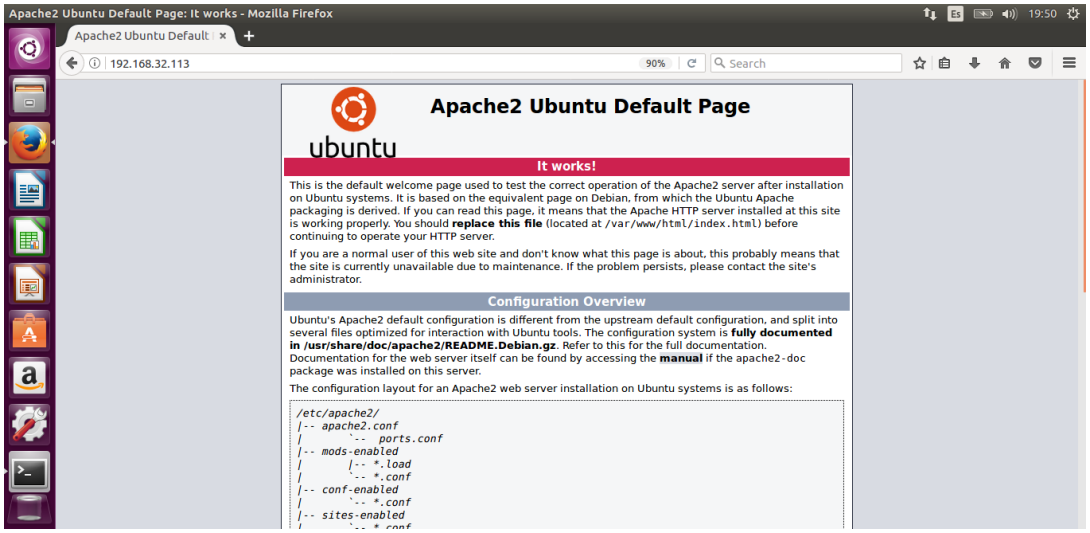


Figura 3-22 Página de Apache en localhost

3.5.2 MySQL

MySQL [80] es un sistema de gestión de bases de datos necesario para gestionar las diferentes bases de datos de nuestro servidor. Una de estas bases de datos será la utilizada por Wordpress. Para su instalación basta con utilizar directamente el repositorio de Ubuntu.

$ apt-get install mysql-server

A continuación, tras el comienzo de la instalación, como se ve en la Figura 3-23, nos pedirá indicar una contraseña de administración que posteriormente deberemos confirmar.

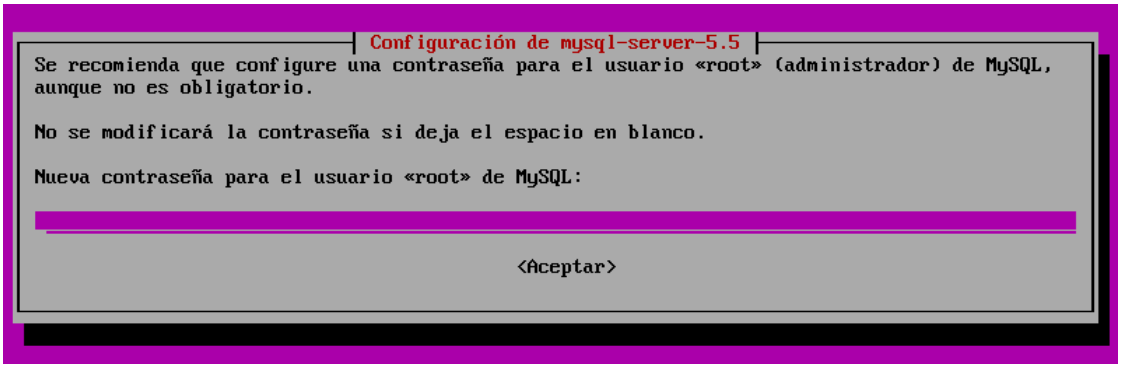


Figura 3-23 Instalación de MySQL

A continuación veremos cómo se configura esta base de datos desde la herramienta phpmyadmin.

3.5.3 Phpmyadmin

Phpmyadmin [81] es una herramienta escrita en PHP con la intención de manejar, administrar y configurar MySQL a través de una interfaz web. Actualmente permite: crear y eliminar bases de datos, crear, eliminar y alterar tablas, borrar, editar y añadir campos, ejecutar cualquier sentencia SQL, administrar claves en campos, administrar privilegios y exportar datos en varios formatos.

Para instalarlo en el servidor de Ubuntu deberemos ir a la consola.

$ apt-get install phpmyadmin

Como vemos en la Figura 3-24, deberemos seleccionar la opción de Apache2.

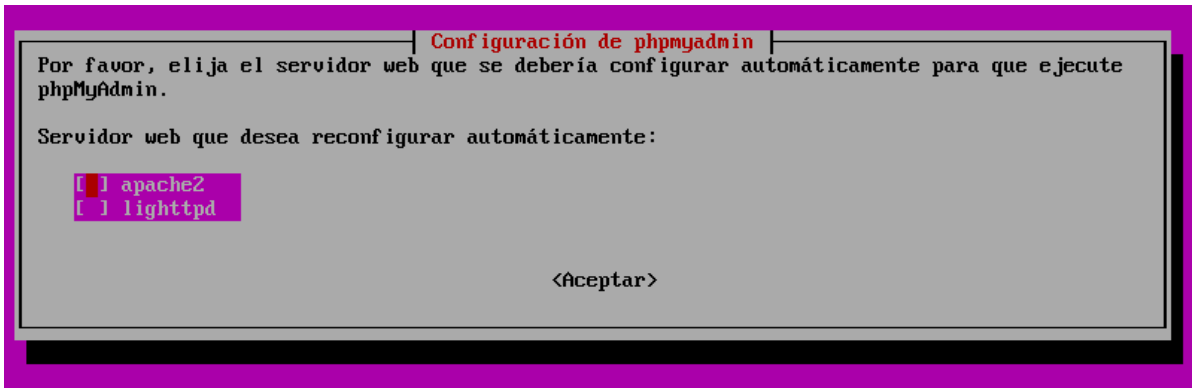


Figura 3-24 Elección de servidor web

Posteriormente, deberemos elegir para el usuario *root*, una contraseña con la que acceder a la base de datos MySQL desde phpmyadmin.

Como MySQL se ejecutará en el propio servidor, al igual que en la Figura 3-25, elegiremos la opción de configurar la base de datos a través de *dbconfig-common*.

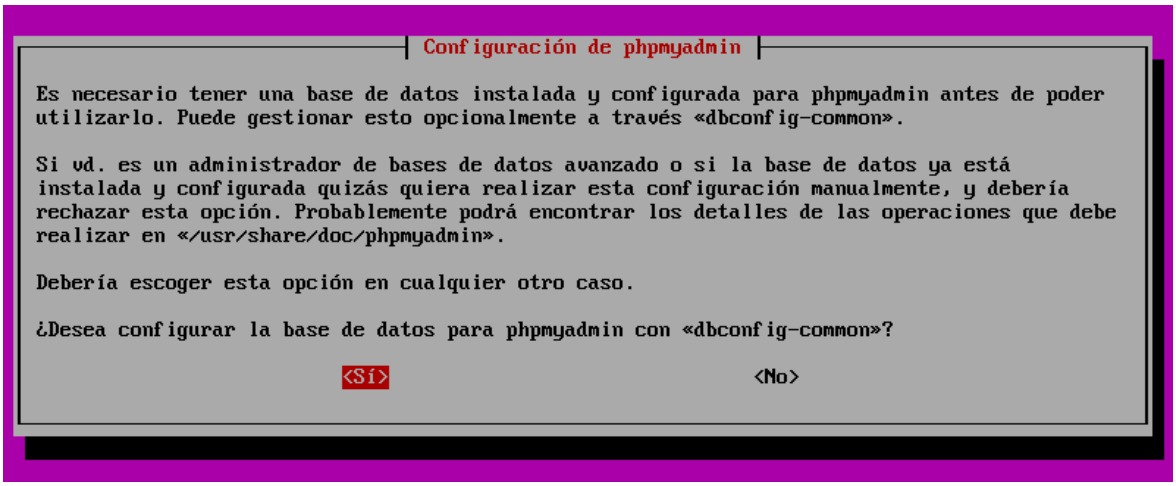


Figura 3-25 Configurar a través de *dbconfig-common*

Por último, para definir el acceso a phpmyadmin, deberemos ejecutar en la consola los siguientes comandos:

$ cd /var/www/html/

$ sudo ln –s /usr/share/phpmyadmin

De esta manera habremos creado un vínculo de la carpeta phpmyadmin al directorio desde el cual Apache sirve las páginas web. Antes de arrancar correctamente phpmyadmin, debemos reiniciar apache.

$ sudo service apache2 restart

Si la configuración se ha realizado correctamente, al ingresar en el buscador *http://localhost/phpmyadmin*, deberá aparecer algo similar a lo que se presenta en la Figura 3-26.

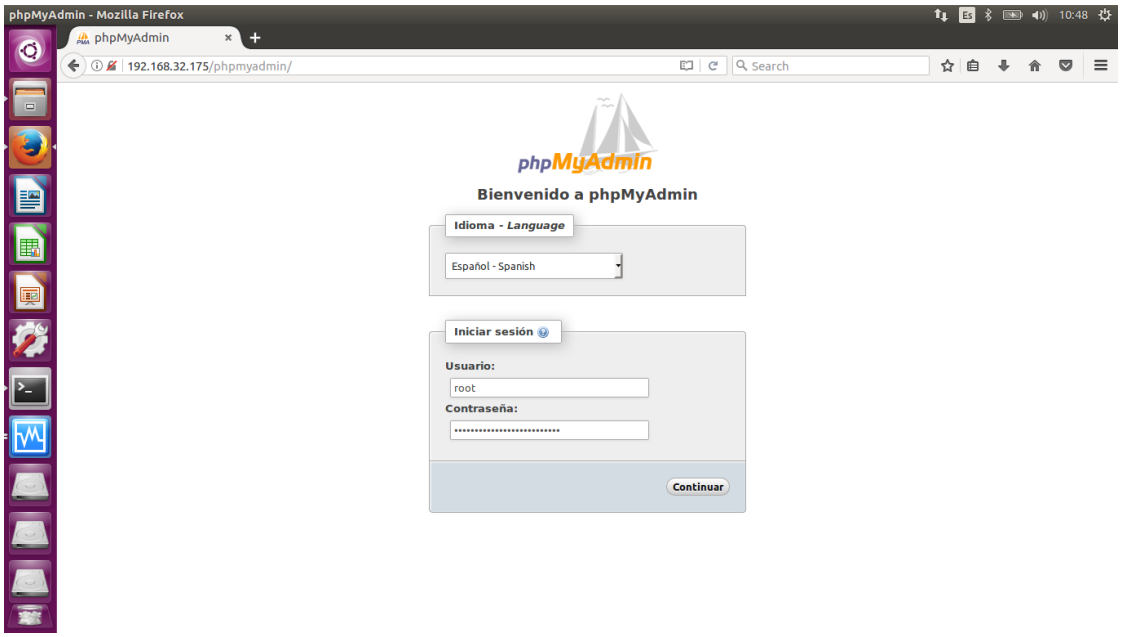


Figura 3-26 Phpmyadmin en localhost

A través de esta página y mediante el usuario *root* y la contraseña que hayamos configurado en los pasos anteriores, accederemos a nuestra base de datos de MySQL y realizaremos en ella las

modificaciones que consideremos. En nuestro caso, como se puede ver en la Figura 3-27, crearemos una nueva base de datos llamada 'Wordpress'.

Figura 3-27 Creación de base de datos Wordpress

A su vez crearemos un usuario llamado "Wordpress". Como se puede ver en la Figura 3-28, es importante otorgarle a este nuevo usuario de la base de datos que utilizará Wordpress los respectivos permisos necesarios.

Figura 3-28 Permisos del usuario Wordpress

3.5.4 Instalación de Wordpress

Una vez configurados los diferentes paquetes de software LAMP de nuestro servidor, es momento de instalar Wordpress 2.5.1

Para ello, primero deberemos descargar y descomprimir los paquetes necesarios.

$ cd /var/www/html/

$ sudo wget http://es.wordpress.org/wordpress-2.5.1-es_ES.zip

$ sudo unzip wordpress-2.5.1-es_ES.zip

$ sudo rm wordpress-2.5.1-es_ES.zip

A continuación, accederemos a la nueva carpeta descomprimida de Wordpress y veremos cómo, en dicha ubicación, tenemos todos los archivos necesarios. Como se puede ver en la Figura 3-29, es recomendable copiar el archivo *wp-config-sample.php*.

$ sudo cp wp-config-sample.php wp-config.php

```
server@server:/var/www/html/wordpress$ ls
index.php      wp-atom.php            wp-cron.php        wp-pass.php       wp-trackback.php
licencia.txt   wp-blog-header.php     wp-feed.php        wp-rdf.php        xmlrpc.php
license.txt    wp-comments-post.php   wp-includes        wp-register.php
readme.html    wp-commentsrss2.php    wp-links-opml.php  wp-rss2.php
wp-admin       wp-config-sample.php   wp-login.php       wp-rss.php
wp-app.php     wp-content             wp-mail.php        wp-settings.php
server@server:/var/www/html/wordpress$ sudo cp wp-config-sample.php wp-config.php
server@server:/var/www/html/wordpress$ _
```

Figura 3-29 Archivos de Wordpress

Deberemos abrir con el editor de textos el archivo *wp-config.php* y configurarlo con los datos de la base de datos y el usuario que creamos anteriormente a través de phpmyamin en MySQL (Figura 3-30).

```
  GNU nano 2.2.6                    Archivo: wp-config.php

<?php
// ** Configuracion de MySQL ** //
define('DB_NAME', 'wordpress');     // el nombre de la base de datos
define('DB_USER', 'wordpress');     // tu nombre de usuario de MySQL
define('DB_PASSWORD', [redacted] // ...y tu contraseña
define('DB_HOST', 'localhost');     // hay un 99% de probabilidades de que no necesites cambiar esto
define('DB_CHARSET', 'utf8');
define('DB_COLLATE', '');

// Define tu clave secreta (SECRET_KEY) con una frase especial. No tendrás que recordarla más,
// así que utiliza una larga y complicada.  Puedes visitar http://api.wordpress.org/secret-key/1.0/
// para conseguir una clave secreta generada automáticamente o inventarte una.
define('SECRET_KEY', 'pon aquí tu frase especial'); // Cambia esto por tu frase especial.

// Cambia el prefijo si deseas instalar multiples blogs en una sola base de datos.
$table_prefix  = 'wp_';   // Solo números, letras y guiones bajos

// Cambia lo siguiente para traducir el WordPress.  El correspondiente archivo MO
// del lenguaje elegido debe encontrarse en wp-content/languages.
// Por ejemplo, instala ca_ES.mo copiándolo a wp-content/languages y define WPLANG como 'ca_ES'
// para traducir WordPress al catalán.
define ('WPLANG', 'es_ES');

/* No edites desde aqui */

define('ABSPATH', dirname(__FILE__).'/');
require_once(ABSPATH.'wp-settings.php');
?>
```

Figura 3-30 Configuración de datos de Wordpress

Una vez configurado Wordpress, deberemos darle permisos de escritura al directorio */var/www/html/wordpress/wp-content* para poder instalar temas, plugins, actualizaciones, etc.

$ sudo chmod –R 775 wp-content/

Ya solo faltaría la propia instalación de Wordpress como página web. Para ello, como vemos en la Figura 3-31, accederemos a través de un buscador web a *https://localhost/wordpress/wp-admin/install.php*.

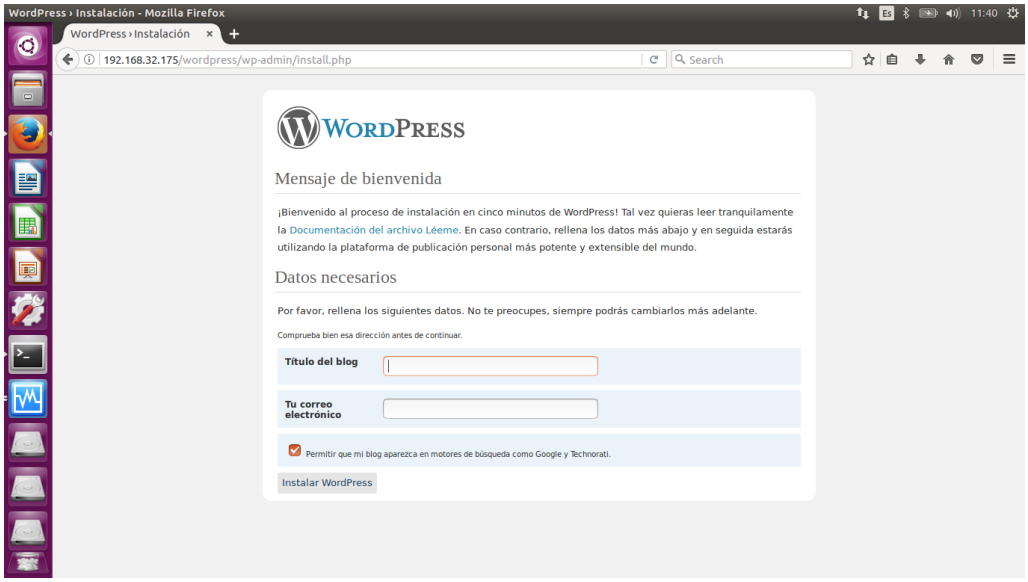


Figura 3-31 Inicio del proceso de instalación de Wordpress

Como podemos ver en la Figura 3-32, para finalizar la instalación, Wordpress nos facilita por defecto el usuario admin y una contraseña que deberemos modificar cuando accedamos a la página web por primera vez.

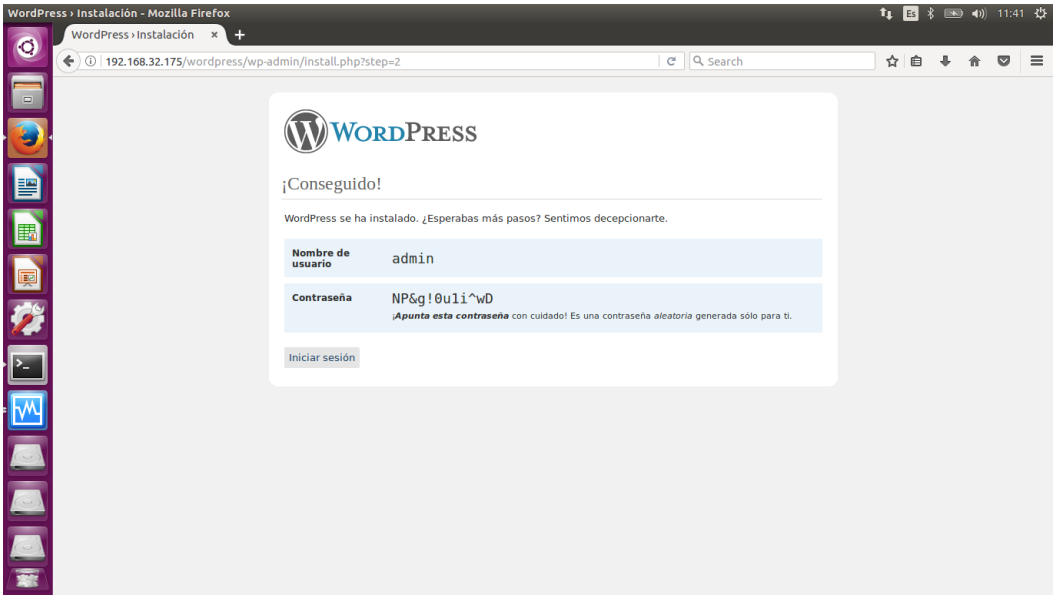


Figura 3-32 Finalización de instalación de Wordpress

3.5.5 Configuración de Wordpress

3.5.5.1 Zona pública

Tras la instalación de Wordpress, configuraremos un diseño sencillo. Este servidor servirá como introducción al ejercicio de ciberataque. Simularemos, como se puede ver en la Figura 3-33, un blog asociado a una ferretería online. Sin embargo, esta página web pertenecerá a una red yihadista la cuál será investigada por el CNI. A raíz de este descubrimiento, deberemos infiltrarnos en la red LAN yihadista y obtener información clasificada.

Para darle un poco de realismo, se han añadido algunos enlaces a páginas web de ferreterías online. Además, se han añadido dos entradas publicitarias que a simple vista no parecen tener nada especial.

Figura 3-33 Página principal de la ferretería online

En la web que hemos creado anteriormente hay dos imágenes públicas que hemos preparado para que la persona que está desarrollando el ciberejercicio las explote en busca de información. A ojos de una persona que carezca de conocimientos informáticos podrían pasar desapercibidas, sin embargo, por medio de la esteganografía, hemos ocultado un mensaje en una de ellas.

- Primero, como vemos en la Figura 3-34, hemos elegido el mensaje que queremos ocultar.

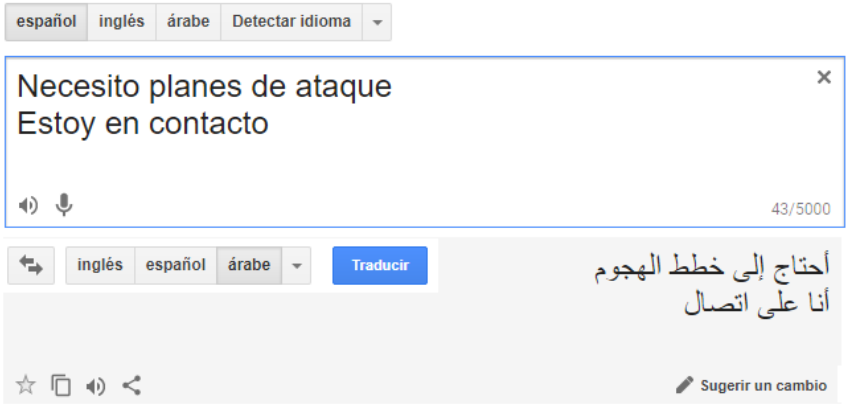


Figura 3-34 Traducción del mensaje al árabe [82]

Es importante traducir el mensaje a la inversa para asegurarnos de que es traducido correctamente por el traductor de idiomas [82]. Hemos elegido el árabe como idioma de comunicación del terrorista.

- Seguidamente, como podemos ver en la Figura 3-35, deberemos escribir un mensaje en un editor de texto, para lo cual nosotros hemos escogido el editor *nano*.

Figura 3-35 Mensaje de la fotografía

- Escogemos la fotografía en la cual queremos esconder el mensaje mediante esteganografía. La imagen elegida, como se ve en la Figura 3-36, aparecerá en una de las entradas de nuestra página web de la ferretería online.

Figura 3-36 Imagen elegida

- A continuación, haremos uso de una de las muchas herramientas orientadas a la esteganografía en la actualidad. En este caso, utilizaremos *Steghide* [83] debido a su facilidad e interpretación de los resultados. Esta herramienta nos permitirá ocultar un mensaje en formato *.txt* en una imagen *.jpg*. Para instalarla, lo haremos desde el repositorio de Ubuntu.
    - *$ sudo apt-get install steghide*

- Guardando el archivo de texto al cual hemos denominado ‘arabe.txt’ y la fotografía de la ferretería denominada ‘ferretería.jpg’ en la misma ubicación, ejecutamos los siguientes comandos.

- *$ sudo steghide embed –cf ferreteria.jpg -ef arabe.txt*

El resultado será el propio archivo imagen de la ferretería con el archivo de texto oculto en ella. En la Figura 3-37 se puede ver la secuencia que se ha seguido. Como se puede observar, el propio programa nos da la oportunidad de cifrar el archivo de texto dentro de la imagen con una contraseña. Puesto que no contiene información relevante, hemos decidido no cifrarlo. De este mensaje se debe sacar una conclusión clara: dentro de esta red se espera que alguien enlace con el fin de mandar un plan terrorista.

```
armijo@armijo-VirtualBox: ~/Escritorio
armijo@armijo-VirtualBox:~/Escritorio$ ls
arabe.txt  ferreteria.jpg
armijo@armijo-VirtualBox:~/Escritorio$ steghide embed -cf ferreteria.jpg -ef arabe.txt
Anotar salvoconducto:
Re-ingresar salvoconducto:
adjuntando "arabe.txt" en "ferreteria.jpg"... hecho
armijo@armijo-VirtualBox:~/Escritorio$
```

Figura 3-37 Esteganografía

3.5.5.2 Zona privada

Hasta ahora, nos hemos dedicado a la apariencia pública de nuestra página web, no sin antes ocultar un mensaje que nos permita identificar el objetivo que queremos conseguir con el ciberataque.

A continuación, nos centraremos en la parte privada de nuestra web de la ferretería online, aquella en la cual solo administradores y personal registrado puede acceder. Esta zona del blog la configuraremos acorde a publicaciones y entradas privadas con ideas claramente partidarias del yihadismo. Como podemos ver en la Figura 3-38, dentro de la sección de enlaces de nuestro sitio web, donde en principio solo había enlaces públicos a las diferentes secciones de una ferretería, hemos añadido algunos enlaces privados con información sobre el yihadismo.

Nombre	URL	Categorías	rel	Visible
Electrónica Descuentos en electrónica	https://ferreteria.es/hogar/hoga...	Enlaces		Sí
Fontanería Descuentos en fontanería	https://bricomart.es/fontaneria....	Enlaces		Sí
Herramientas Descuentos en herramientas	https://ferreteria.es/ferreteria...	Enlaces		Sí
Isis	https://es.wikipedia.org/wiki/Es...	Enlaces		No
Islamismo	https://es.wikipedia.org/wiki/Is...	Enlaces		No
Jardinería Descuentos en jardinería	https://ferreteria.es/jardin.html	Enlaces		Sí
Venta de armas	https://tiendashoke.es/armeria-o...	Enlaces		No
Yihad	publico.es/internacional/violenc...	Enlaces		No

Figura 3-38 Enlaces públicos/privados

Además, también se han añadido algunas entradas privadas que solo se revelan en la página web al personal que dispone de una cuenta y que se ha logueado en la web. En este caso, como muestra la Figura 3-39, hemos elegido algunas fotos de Internet publicitando el movimiento yihadista.

Figura 3-39 Entrada privada

Por último, como muestra la Figura 3-40, hemos configurado una serie de usuarios dentro del blog yihadista. Dentro de estos usuarios podemos distinguir a población española como participantes del blog, y a un administrador de origen marroquí, el cual pretendemos hacer pasar por uno de los líderes terroristas. Dentro de la sección de correos, hemos utilizado el mismo correo para todos los usuarios excepto para el usuario marroquí, al cual le hemos asignado un correo con su propio nombre. Esto debe servir como indicio al alumno que realice el ciberejercicio de que este usuario tiende a utilizar su nombre de pila como nombre de usuario en diferentes campos: usuario de una página web, correo electrónico, nombre de usuario de un equipo, etc.

Nombre de usuario	Nombre	Correo electrónico	Rol	Entradas
Alvaro	Álvaro Armijo Fuentes	yihadismo2018@gmail.com	Suscriptor	0
Ignacio	Ignacio Sánchez Romero	yihadismo2018@gmail.com	Colaborador	0
Jesus	Jesús Castro Marcos	yihadismo2018@gmail.com	Editor	0
Juan	Juan García Rossi	yihadismo2018@gmail.com	Administrador	2
Juansito	Juan Carlos Crespo Gómez	yihadismo2018@gmail.com	Autor	0
Marcos	Marcos López Gerente	yihadismo2018@gmail.com	Autor	0
Qutaybah	Qutaybah Mohammed	Qutaybah@gmail.com	Administrador	2

Figura 3-40 Usuarios del blog yihadista

Para que nuestro alumno pueda acceder a la información de los usuarios, hemos configurado un segundo usuario de origen español como administrador de la web. Más adelante, simularemos una

intrusión del CNI en la red yihadista y una captura de tráfico por parte de éste en la que se podrán encontrar las credenciales necesarias para entrar como usuario administrador en la web.

3.5.5.3 Imagen privada

La zona privada se denomina así porque el contenido de ésta debe ser de acceso exclusivo para los usuarios registrados. En este caso, la zona privada contiene imágenes a las que solo los usuarios de Wordpress tendrán acceso.

Entre las diferentes imágenes privadas que hemos subido a la web yihadista, hemos modificado una con GIMP [84]. Esta herramienta es un editor de imágenes que hemos descargado desde su página oficial [85] y que hemos utilizado para añadir información clasificada a la imagen privada. En la Figura 3-41 podemos ver la imagen original.

Figura 3-41 Imagen original [86]

Lo que se ha pretendido simular con esta acción es recrear una situación muy conocida en el mundo de la ciberseguridad [87], en la cual, durante una entrevista a los funcionarios que emiten las alertas de misil en Hawái, se toma una fotografía donde posa un funcionario y, de fondo, puede verse un *post-it* con la contraseña de uno de los equipos. En la Figura 3-42 se puede ver la imagen original de la entrevista.

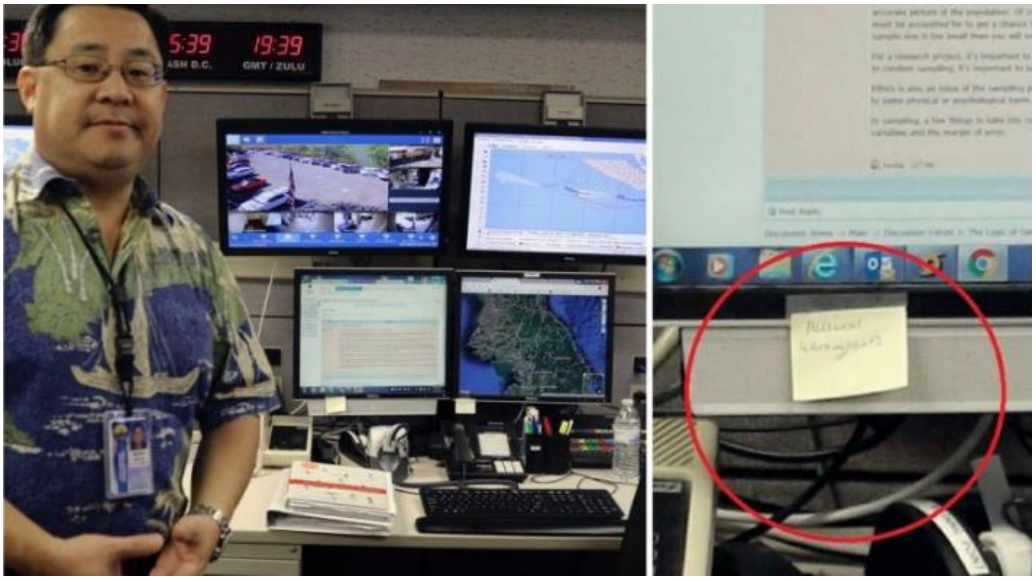


Figura 3-42 Entrevista en Hawái [87]

Para editar nuestra imagen ha sido necesario, en primer lugar, una fotografía de un *post-it* en el que hemos escrito un usuario y una contraseña. En la Figura 3-43 podemos ver la imagen del *post-it*.

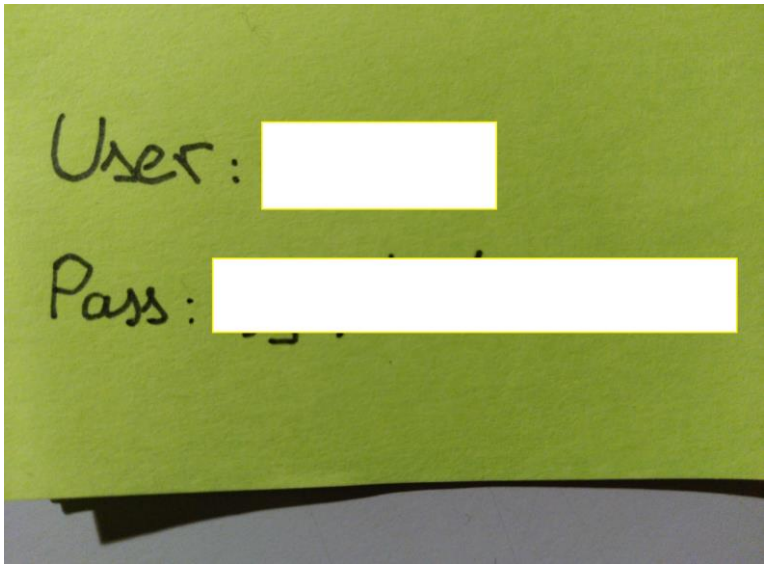


Figura 3-43 *Post-it* con información clasificada

A continuación, con el uso del GIMP hemos recortado la imagen del *post-it* de manera que diese la impresión de encontrarse en el mismo plano del espacio que el ordenador de la imagen yihadista original y le hemos aplicado algunos filtros para adaptar el color del *post-it* a la imagen yihadista. En la Figura 3-44 se puede ver el resultado de la imagen del *post-it*.

Figura 3-44 Filtros aplicados a la imagen del *post-it*

Posteriormente, hemos superpuesto la imagen del *post-it* sobre la imagen yihadista. Para dar sensación de realidad, hemos establecido un efecto en la fotografía ya editada y le hemos dado a la imagen del *post-it* un leve efecto de sensación de profundidad para aumentar el realismo. Como resultado final, en la Figura 3-45 podemos distinguir un *post-it* en la carcasa del ordenador en el que se pueden apreciar las credenciales del usuario de la fotografía. En este caso, la persona simula ser uno de los usuarios de la red LAN de la red yihadista que estamos configurando.

Figura 3-45 Imagen editada de la zona privada de la web

Para concluir hemos subido a la zona privada de la web la imagen editada, con intención de que el alumno, cuando acceda a la zona privada y navegue entre las diferentes imágenes, se percate del error que han cometido los miembros de la web subiendo la fotografía de este usuario de la red LAN.

3.5.6 Configuración del servidor

La idea será que nuestro alumno consiga obtener los nombres de los diferentes usuarios de la página web yihadista y los utilice para acceder al servidor web a través del protocolo SSH, el cual habremos dejado abierto para permitir conexiones, y así tomar el control de uno de los equipos de la DMZ de la red yihadista. Para hacer esto posible debemos:

- Instalar el servicio ssh-server en el servidor.
    - *$ sudo apt-get install openssh-server*
    - Puesto que vamos a permitir la entrada por el puerto 22 al servidor de la DMZ, es importante configurar el servicio SSH para evitar un ataque de fuerza bruta de gran magnitud y así obligar al ciberatacante a reducir las combinaciones de usuarios y contraseñas al máximo. De este modo forzaremos al ciberatacante a buscar información en la web antes de atacar directamente al servidor. Para ello, como muestra la Figura 3-46, estableceremos un tiempo de espera por cada combinación errónea introducida en el puerto 22 del servidor.

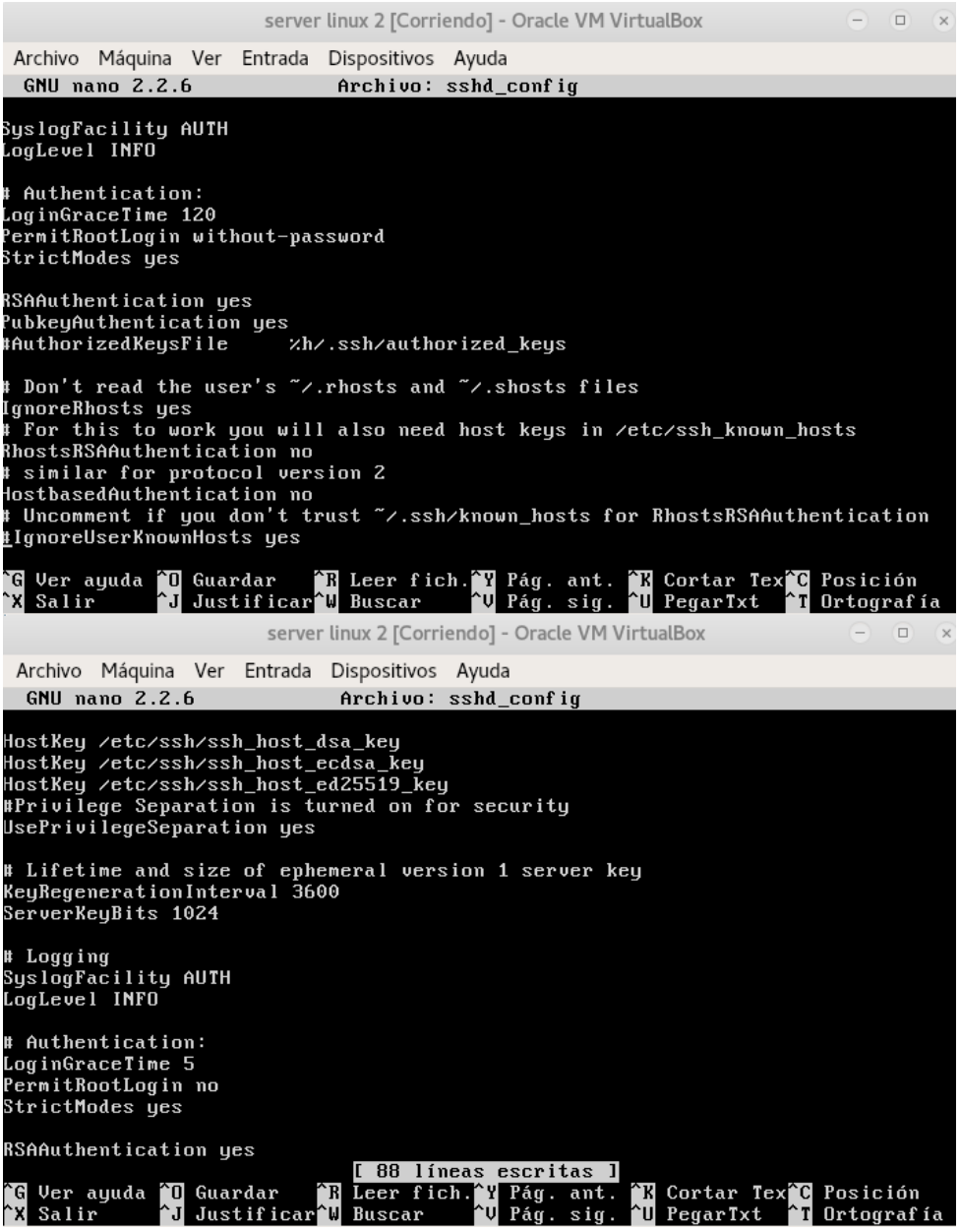


Figura 3-46 Configuración del servicio SSH antes / después

- Editaremos el archivo */etc/ssh/sshd_config* y cambiaremos los parámetros de *LoginGraceTime 120* a *LoginGraceTime 5* y estableceremos la opción *PermitRootLogin without-password* como *PermitRootLogin no.*

- Desactivar el firewall del servidor para permitir el acceso remoto y el escaneo de puertos del servidor. El firewall de Linux que por defecto viene instalado es UFW (*Uncomplicated FireWall*). Esto no sería estrictamente necesario, solo lo desactivamos por posibles reglas que pudiesen añadirse en algún momento al firewall y que interfiriesen en la conexión por SSH.
  - *$ sudo ufw disable*

- Configurar el nombre de usuario del servidor que aloja la web yihadista y su contraseña acorde a datos que podamos extraer fácilmente.

Se trata de aprovechar la ingeniería social como medio de ataque y, en este caso, de aprovechar el nombre del usuario administrador marroquí.

Cambiaremos el nombre del usuario administrador del servidor, que hasta ahora era 'server', y configuraremos una contraseña fácil de romper a través de diccionarios para que, a través de aplicaciones de Kali Linux, se pueda conseguir descifrar rápidamente y se pueda tener el control del servidor en el que se aloja la página web. Para modificar las credenciales del servidor deberemos hacer uso de los siguientes comandos.

$ sudo usermod –l 'nuevo_nombre' 'nombre-antiguo'

$ sudo passwd 'usuario'

****

****

3.5.6.1 Configuración de direcciones

Por el momento, el servidor está configurado para mostrar en *http://localhost/* la página principal de Apache y, que desde ésta, se pueda acceder tanto a nuestra página de Wordpress como a nuestra base de datos de phpmyadmin utilizando las siguientes URL's:

- Wordpress: *http://localhost/wordpress*
- Phpmyadmin: *http://localhost/phpmyadmin*

Cuando incorporemos el servidor virtual a la maqueta de red y le proporcionemos una URL (*www.tfg.dunquerque.cud.uvigo.es*) a través del servidor DNS de la DMZ de la maqueta, queremos que esta URL, asociado a la IP 192.168.16.10, futura IP de nuestro servidor virtual, nos redirija a nuestra web de Wordpress y no a la página principal de Apache.

Para ello deberemos modificar el archivo */etc/apache2/sites-available/000-default.conf* y cambiar *DocumentRoot /var/www/html* por *DocumentRoot /var/www/html/wordpress.* En la Figura 3-47 se puede ver el resultado final.

```
  GNU nano 2.2.6 Archivo: ...ache2/sites-available/000-default.conf

<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port t$
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html/wordpress

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        ErrorLog ${APACHE_LOG_DIR}/error.log
                                [ 31 líneas leídas ]
^G Ver ayuda ^O Guardar    ^R Leer fich.^Y Pág. ant. ^K Cortar Tex^C Posición
^X Salir     ^J Justificar^W Buscar     ^V Pág. sig. ^U PegarTxt  ^T Ortografía
```

Figura 3-47 Configuración de ruta

Una vez hemos indicado que queremos que nuestra web de Wordpress se encuentre en la ruta de nuestra IP local, deberemos mover el directorio de phpmyadmin dentro del directorio de Wordpress para poder encontrarlo de nuevo en la ruta *http://localhost/phpmyadmin.* Para ello nos dirigimos a

/var/www/html y ahí se encontrarán los directorios de phpmyadmin y de Wordpress. Solo deberemos mover phpmyadmin ejecutando lo siguiente.

$ sudo mv /var/www/html/phpmyadmin /var/www/html/wordpress

3.5.6.2 Incorporación del servidor Wordpress a la maqueta de red

Para transferir el servidor yihadista al servidor dunquerque lo podemos hacer empleando dos métodos:

- Extraer el servidor yihadista virtual como un archivo *.ova* y, a través de Filezilla, transferirlo al servidor dunquerque y cargarlo en el VirtualBox de este último servidor.
- Transferir al servidor dunquerque los dos archivos principales que constituyen nuestro servidor virtual y, una vez en dunquerque, guardarlos en la misma carpeta. Estos archivos son los archivos *.vbox* (se corresponde a la configuración de la máquina virtual) y *.vdi* (se corresponde con el disco duro virtual del servidor).

Hemos optado por esta segunda opción ya que, durante la primera opción, el VirtualBox del servidor dunquerque no era capaz de cargar correctamente el archivo *.ova*. Una vez transferido y cargado nuestro servidor yihadista en el VirtualBox de dunquerque, pasamos a modificar la arquitectura de red. Inicialmente, la DMZ de nuestra red virtual se compone de cinco servidores:

- Un servidor de base de datos.
- Un servidor DNS.
- Un servidor web.
- Un servidor de correo electrónico.
- Un servidor FTP.

El servidor que estamos configurando es un servidor web con su propia base de datos, por lo que sustituirá al servidor web inicial. Por ello, lo primero que debemos hacer es apagar el servidor web original. Una vez apagado, arrancaremos nuestro servidor yihadista y modificaremos el archivo */etc/network/interfaces* y definiremos su interfaz eth0 con la misma configuración que tenía el servidor web que acabamos de apagar. En la Figura 3-48 podemos ver el resultado de la interfaz modificada.

```
  GNU nano 2.2.6        Archivo: /etc/network/interfaces          Modificado

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface

auto eth0
iface eth0 inet static
address 192.168.16.10
netmask 255.255.255.0
gateway 192.168.16.1
dns-nameservers 192.168.16.20
_

^G Ver ayuda ^O Guardar   ^R Leer fich.^Y Pág. ant. ^K Cortar Tex^C Posición
^X Salir     ^J Justificar^W Buscar    ^V Pág. sig. ^U PegarTxt  ^T Ortografía
```

Figura 3-48 Interfaz de red modificada

En lugar de sustituir la máquina virtual por completo, lo que haremos será sustituir únicamente su disco duro, por lo que nos dirigiremos a la carpeta raíz de VirtualBox del servidor dunquerque y entraremos en la carpeta */home/tfg/TFG/VMs/SEVER_ubuntuS_1* y sustituiremos el archivo de extensión *.vmdk* (correspondiente al disco duro virtual del servidor web de la red) por el archivo *.vmdk* correspondiente a nuestro servidor yihadista. En la Figura 3-49 podemos ver cómo se transfiere el servidor yihadista al servidor dunquerque.

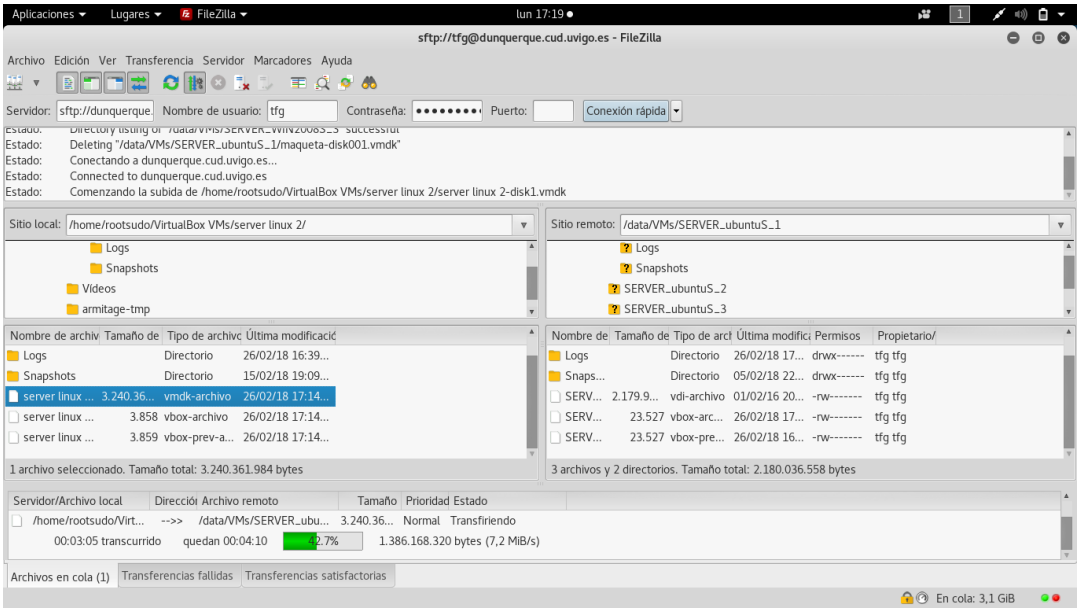


Figura 3-49 Transferencia al servidor dunquerque

Al iniciar el servidor web en el VirtualBox de dunquerque, deberemos asegurarnos de establecer la nueva ruta para que el servidor virtual arranque desde el disco duro virtual que acabamos de incorporar.

3.5.7 Captura de tráfico

Una de las evidencias que deberemos facilitar al alumno, será una traza de tráfico en la que haya información confidencial capturada. Con ello el alumno podrá poner en práctica el estudio de paquetes capturados por Wireshark. Esta traza se la daremos al alumno una vez haya investigado la zona pública de la ferretería online de la red yihadista y haya descubierto el mensaje oculto en una de las fotografías.

Para ello, simularemos ser el CNI y haber entrado de forma silenciosa en la red doméstica de nuestro usuario sospechoso, el cual nos ha llevado a investigar la página web de la ferretería. Este usuario será uno de los registrados en dicha página y el CNI capturará una traza en la cual se encuentran los datos de acceso del usuario.

3.5.7.1 Wireshark

Para capturar la traza de tráfico, abriremos la herramienta wireshark y capturaremos el tráfico de nuestra estación de trabajo (simulando ser el usuario que está bajo investigación) conectando con la ferretería online. Navegaremos por algunas páginas web de Internet y, entre ellas, accederemos a *http://www.tfg.dunquerque.cud.uvigo.es* y nos loguearemos para acceder a la zona privada. Hecho esto, puesto que nuestro servidor yihadista donde está instalada la página de Wordpress trabaja en el puerto 80, el tráfico capturado irá en claro. En la Figura 3-50 podemos ver la traza de tráfico en el proceso de captura de tráfico de wireshark.

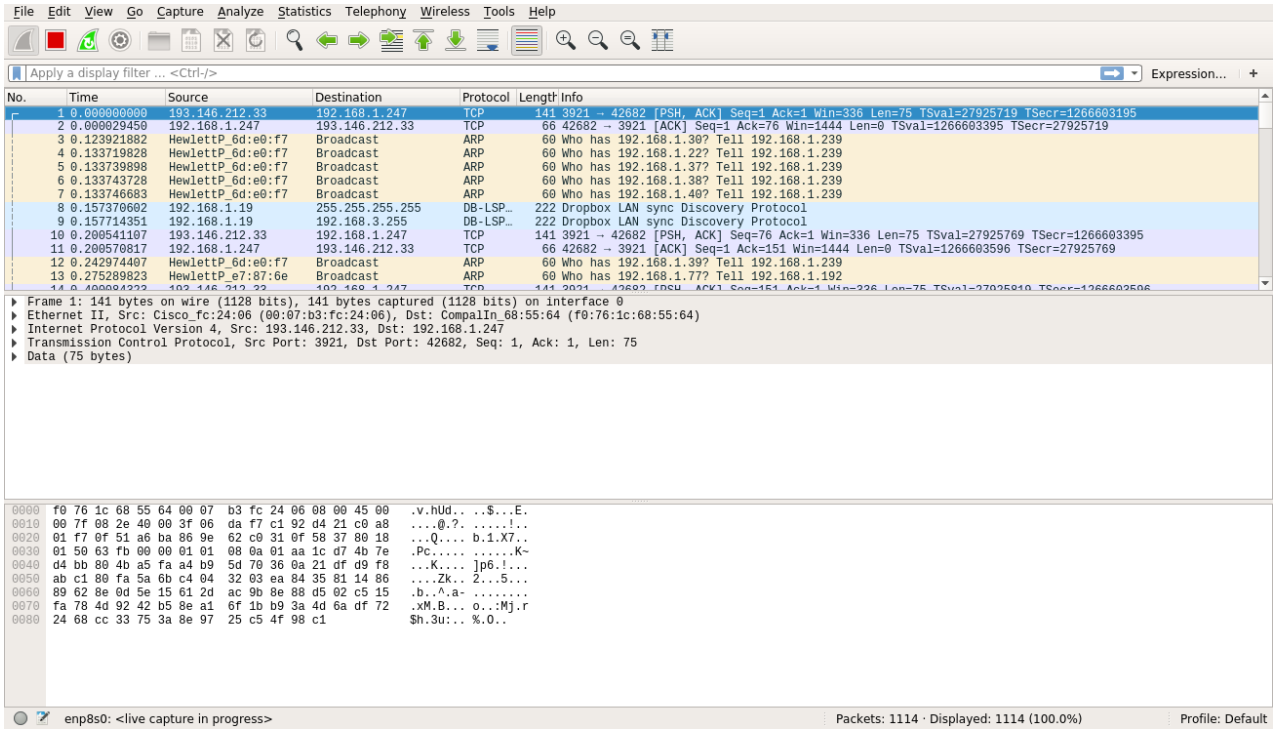


Figura 3-50 Captura de tráfico

Una vez tenemos la traza, paramos la captura de tráfico y guardamos la traza con extensión *.pcapng*. Este archivo se le proporcionará, como hemos indicado anteriormente, al alumno una vez haya confirmado actividad terrorista mediante el estudio de las imágenes públicas.

3.5.8 Configuración de Pfsense

Pfsense es el firewall que protege nuestra red virtual. Hasta el momento, las restricciones que mantenía eran muy severas, por lo que nos hemos visto obligados a modificarlas. Puesto que uno de los objetivos del ciberataque es tomar el control del servidor de la DMZ a través del puerto 22, debemos incorporar una nueva regla al firewall: permitir el paso del tráfico del exterior que circule por el puerto 22 y redireccionarlo a nuestro servidor web de Wordpress.

Lo primero que debemos hacer es acceder a la configuración del firewall Pfsense. Para ello, a través de KRDC, hemos accedido a uno de los equipos de la red LAN desde el cual hemos accedido al firewall a través de la IP 192.168.8.1. Hemos debido hacerlo así porque actualmente el firewall solo acepta tráfico desde la LAN y desde la DMZ. Una vez dentro de la configuración de Pfsense, nos dirigimos a *firewall/rules* y creamos una nueva regla.

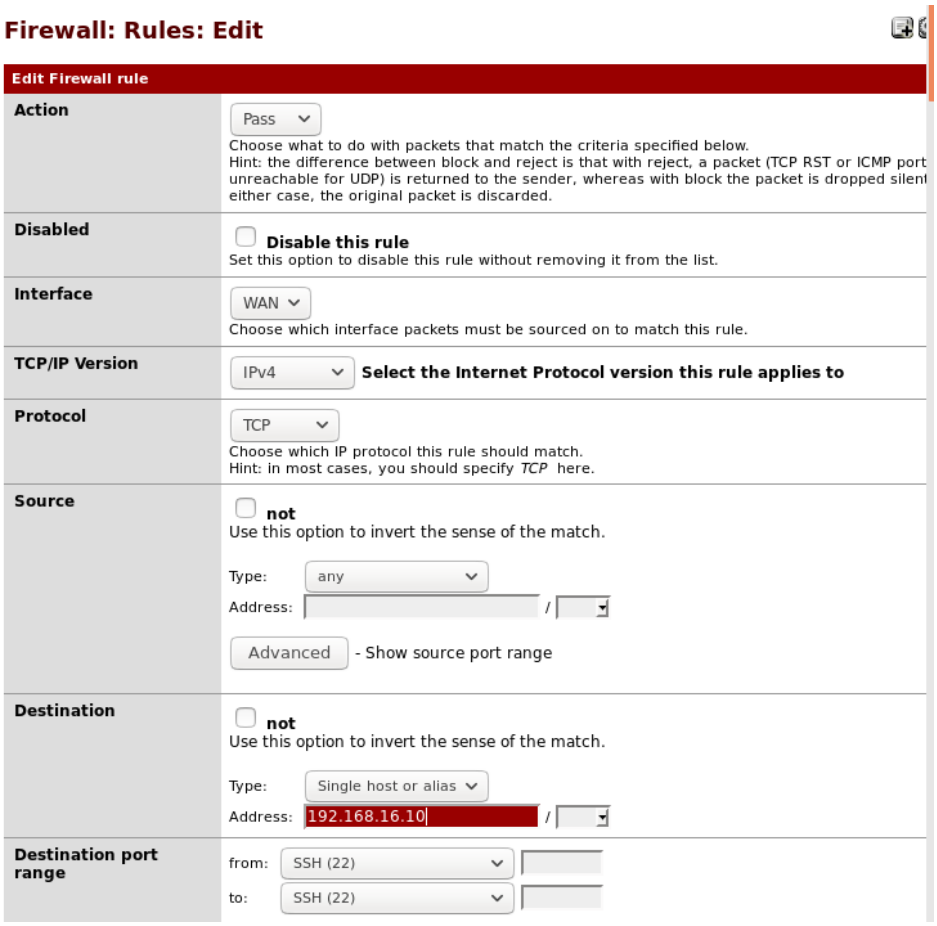


Figura 3-51 Nueva regla para el puerto 22

Como podemos ver en la Figura 3-51, permitiremos el paso del tráfico que provenga de la WAN (aquello que es externo a la red virtual que estamos configurando) por el puerto 22 y lo redireccionaremos al puerto 22 de la IP del servidor Wordpress 192.168.16.10. En la Figura 3-52 podemos ver la nueva regla añadida al final del resto de reglas de la DMZ del firewall. Además, también será necesario desactivar la regla de restricción indicada.

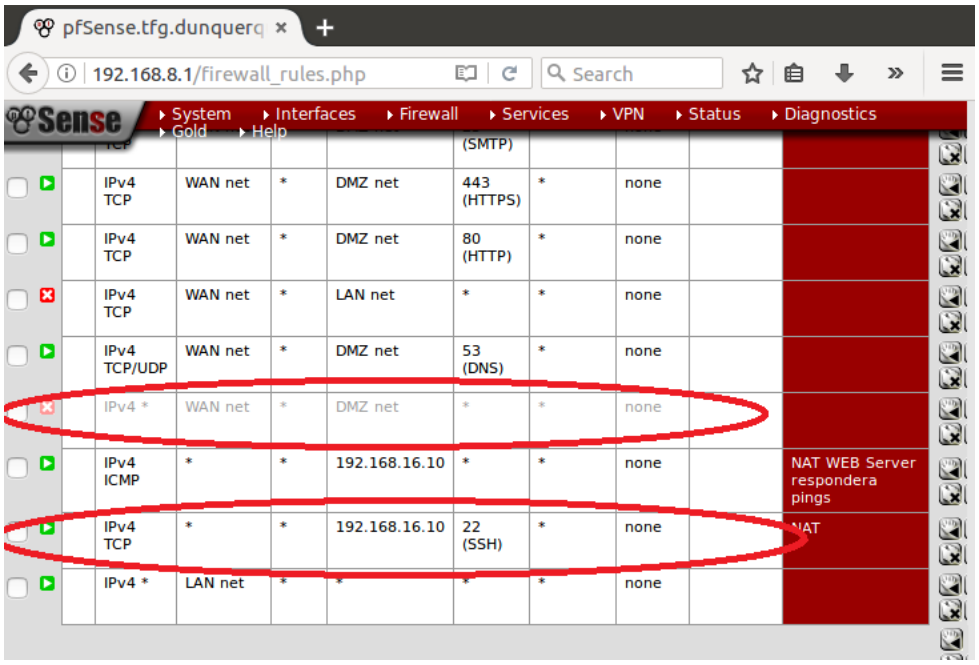


Figura 3-52 Regla del puerto 22 añadida a Pfsense

Actualmente, como muestra la Figura 3-53, Pfsense no permite el acceso a la LAN desde la DMZ. Esto es algo que nuestro alumno deberá modificar durante la realización del ciberejercicio.

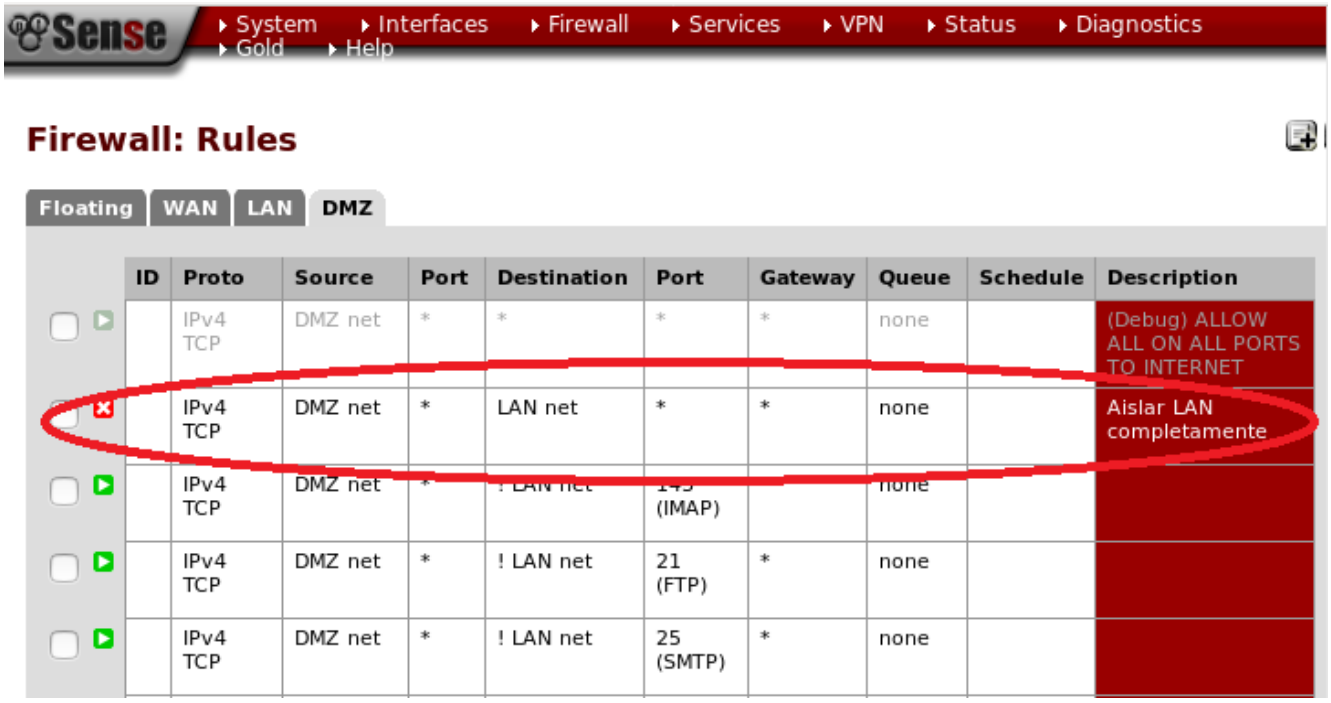


Figura 3-53 Prohibición de acceso a la LAN desde la DMZ

Por último, para que el alumno pueda acceder al firewall de la red, deberíamos configurar el usuario y contraseña y establecer las credenciales que vendrían por defecto. De esta manera, el alumno, con ayuda de información pública de Internet, podría obtener fácilmente el usuario y contraseña. Sin embargo, el firewall ya tenía establecida su configuración de usuario y contraseña por defecto (nótese que las personas no protegen con la seguridad adecuada aquello que prevén que es seguro), por lo que no lo modificaremos.

3.5.9 Configuración equipo LAN

Hasta ahora, la red LAN estaba configurada únicamente con equipos con diferentes distribuciones del sistema operativo Windows. Por razones de comodidad a la hora de trabajar con comandos y dar un poco de variedad a los equipos de la red LAN, lo que haremos será sustituir, al igual que hicimos con el servidor web de la arquitectura de red inicial, el disco duro virtual de un equipo de Windows, en concreto del equipo USER_WIN7_1, por un disco duro virtual llamado 'armijo' con la distribución de *Ubuntu 16.04*. En la Figura 3-54 puede verse cómo sustituimos el disco duro virtual de la máquina.

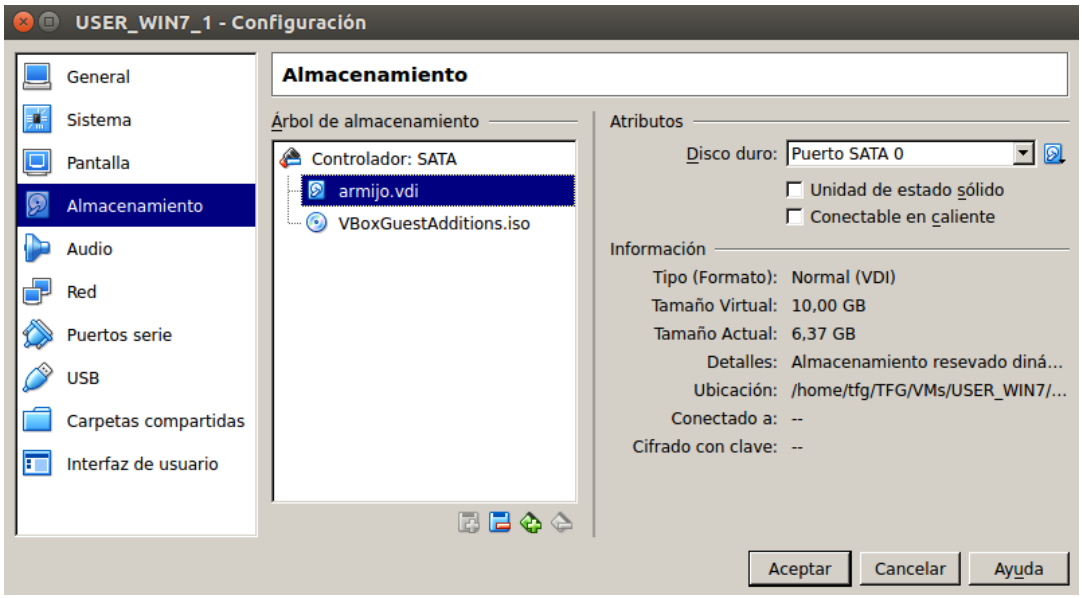


Figura 3-54 Sustitución de Windows por Ubuntu en la red LAN

También deberemos configurar su interfaz de red acorde al equipo al cual hemos suplantado dentro de la red LAN. En la Figura 3-55 se muestra su nueva configuración de red.

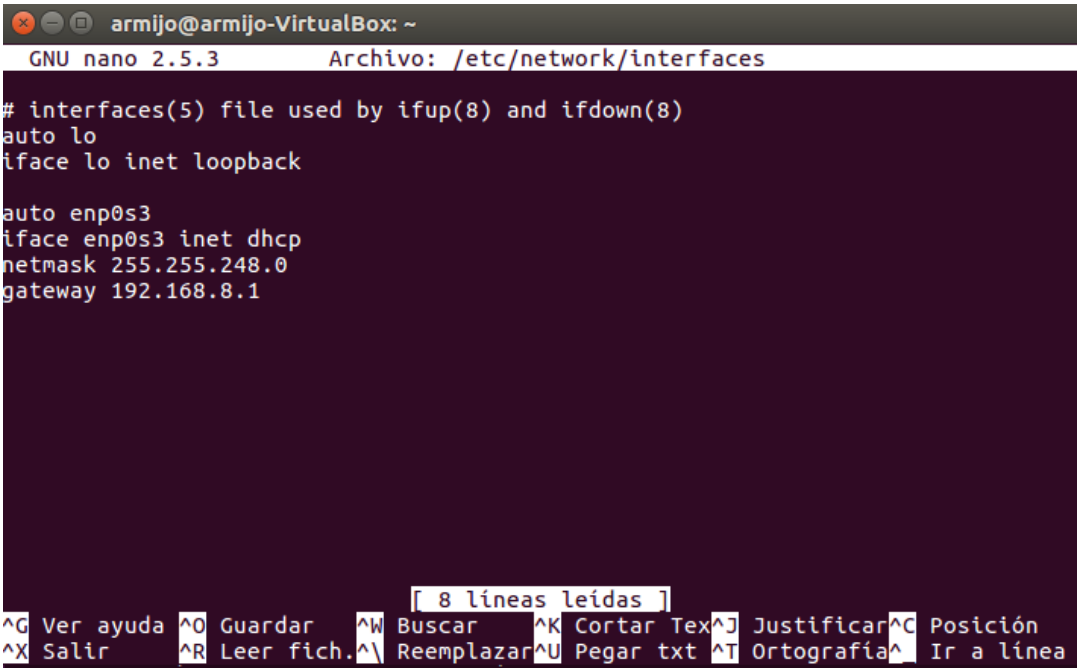


Figura 3-55 Interfaz de equipo de red LAN

A diferencia de la DMZ, en la red LAN las interfaces están configuradas según el protocolo DHCP (*Dinamic Host Configuration Protocol*) [88]. Este protocolo permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. En este caso se asigna una IP dentro del rango de IP's que se ha establecido para la red LAN: 192.168.8.1/21.

En este equipo se encontrará instalado un servidor SSH y dejaremos habilitado el puerto 22. También deberemos modificar el usuario y contraseña acorde al usuario y contraseña que dejamos como pista en la Figura 3-45.

3.5.9.1 Plan terrorista

Los documentos de formato *.docx* son la evolución del formato *.doc* y su principal ventaja es el espacio que ocupa este tipo de archivos: tienen una compresión sin pérdida incorporada. Por norma general, un archivo *.docx* tiene la mitad de tamaño que un archivo *.doc;* esto facilita el envío de documentos por correo electrónico o la realización de copias de seguridad. Todo esto es debido a que los archivos *.docx* son realmente archivos *.zip* compuestos por diferentes archivos [89]. Esta es la característica principal que explotaremos en este apartado.

Como se pude ver en la Figura 3-56, procederemos a crear un archivo *.docx* en el que simularemos una factura de la ferretería.

	CANTIDAD	PRECIO €	TOTAL €
Destornillador	40	6	240
Tornillos	500	0,20	100
Tuercas	500	0,20	100
Alambre	100 m	2	200
Cinta	400 m	0,5	200
Llave	30	8	240
TOTAL	-	-	1080

Figura 3-56 Factura

A continuación, como se ve en la Figura 3-57, cambiaremos la extensión de nuestro documento *.docx* a la extensión *.zip.* Accederemos a la ruta */Factura.zip/word/media* en la que se guardan las imágenes del documento y copiaremos unas imágenes que hemos descargado de Internet de la Puerta del Sol de Madrid, simulando ser éste el objetivo de un atentado. A mayores, añadiremos una imagen con datos clave como la hora y el día previstos del atentado, el lugar y el tipo de explosivo (Figura 3-58).

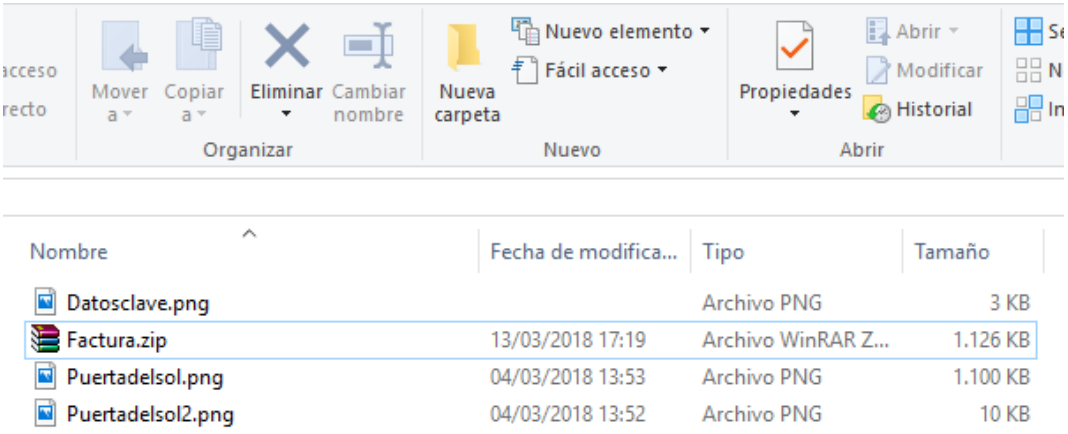


Figura 3-57 Documento *.zip*

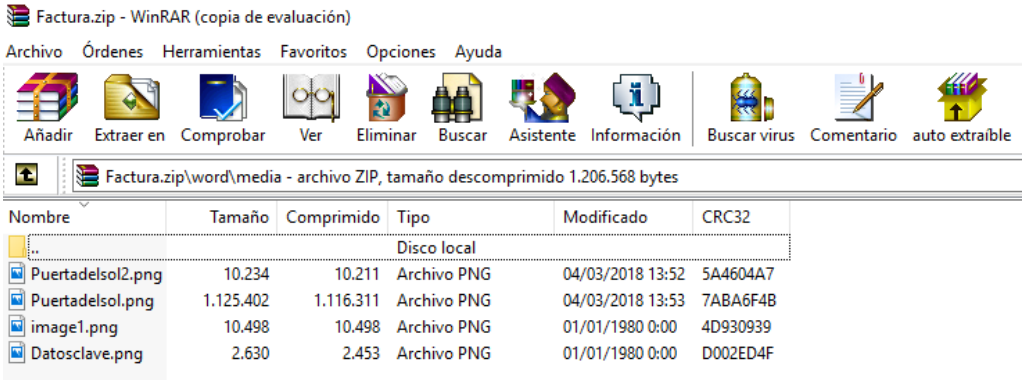


Figura 3-58 Plan terrorista

Una vez incorporadas las imágenes con los datos elegidos, volveremos a cambiar la extensión del documento a un documento *.docx*. Es importante incorporar los archivos en la ruta elegida y asegurarse de que son imágenes en formato *png* y que sus nombres no contienen espacios, de lo contrario, cuando intentemos abrir el documento *.docx*, nos aparecerá un error de lectura.

Para finalizar, transferiremos el archivo a la carpeta */Documentos* de la máquina de la red LAN cuyo acceso deberá conseguir el alumno que realice el ciberejercicio.

4 VALIDACIÓN DEL CIBEREJERCICIO

4.1 Introducción

En este capítulo llevamos a cabo una validación del ciberejercicio planteado. Definimos también un enunciado del ciberejercicio (el enunciado completo puede verse en el Anexo I: Enunciado del ciberejercicio) que consta de una serie de apartados, a los cuales les asignamos pistas en caso de que el alumno que lleve a cabo el ciberejercicio no supiese cómo continuar. Puesto que nosotros ya sabemos cómo resolverlo, nos ceñiremos a una resolución directa del ciberejercicio. Cabe mencionar que habría otras maneras de resolverlo, otro tipo de ciberataques, etc. Si no los hubiese, estaríamos afirmando que podríamos hacer un entorno con una seguridad absoluta. Para este capítulo, trabajaremos principalmente con el equipo HP con el sistema operativo Kali Linux.

4.2 Acceso a la zona pública

4.2.1 Enunciado

Se ha detectado a un usuario con antecedentes penales visitando algunas páginas de actividad ilegal dentro de la *Deep Web*. Tras varias semanas llevando a cabo una investigación en secreto sobre este usuario, podemos confirmar que visita diariamente la web *www.tfg.dunquerque.cud.uvigo.es*. Al parecer, no es más que una ferretería online. ¿Podrías investigar esta página y confirmar alguna actividad maliciosa?

Pista: Investigar imágenes.

4.2.2 Solución

Después de que el alumno investigue los diferentes enlaces, busque comentarios sospechosos, investigue las diferentes entradas de la página web, estudie el código HTML, etc., deberá llevar a cabo el estudio de las imágenes.

4.2.2.1 Estudio de imágenes

Para estudiar en profundidad una imagen, como muestra la Figura 4-1, lo primero que debemos hacer es descargarla a nuestro equipo personal.

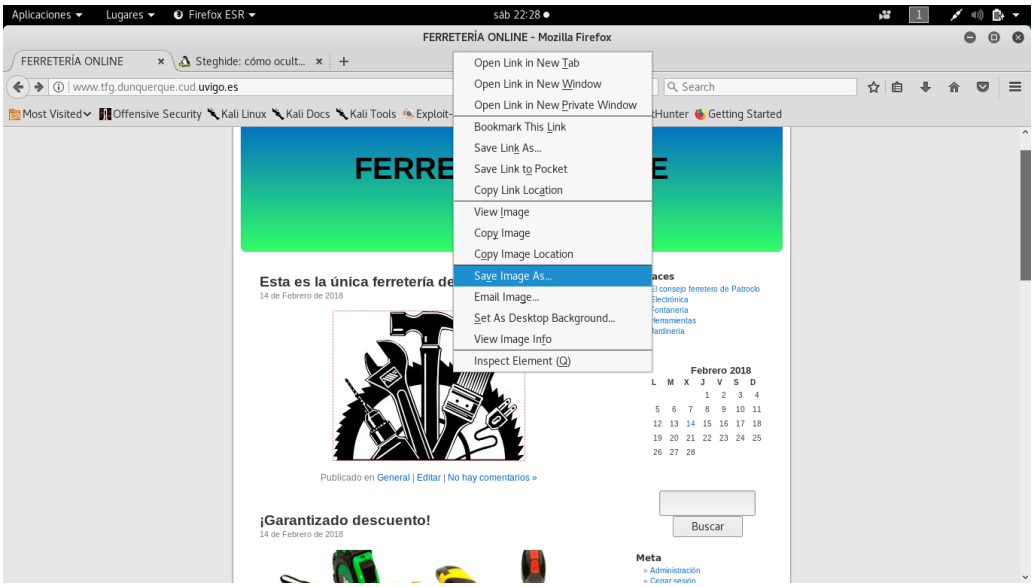


Figura 4-1 Descargar imagen sospechosa

Una vez podamos trabajar sobre ella, deberemos descargar alguna herramienta que permita la extracción de información mediante esteganografía. En este caso, trabajaremos con la misma herramienta que utilizamos en el apartado 3.5.5.1, *steghide*.

$ sudo apt-get install steghide

A continuación nos dirigimos al directorio donde se encuentra nuestra imagen descargada, en este caso, el escritorio. En dicha ubicación abrimos una terminal y ejecutamos *steghide* con los comandos indicados para la extracción de información de la imagen. En la Figura 4-2 podemos ver el resultado.

$ sudo steghide extract –sf ferreteria.jpg

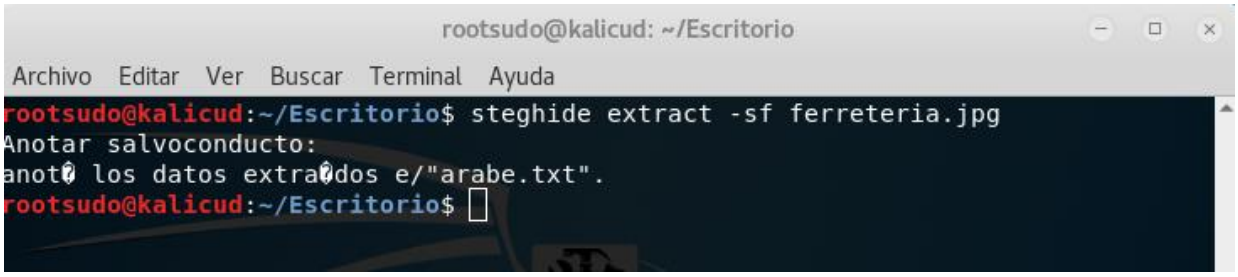


Figura 4-2 Extracción de información

Steghide nos pedirá una contraseña para desencriptar la información de la fotografía. En este caso decidimos no establecer ninguna, por lo que con dejar el espacio en blanco y pulsar *enter* es suficiente. En la Figura 4-3 podemos ver la fotografía y el fichero de texto llamado *arabe.txt*.

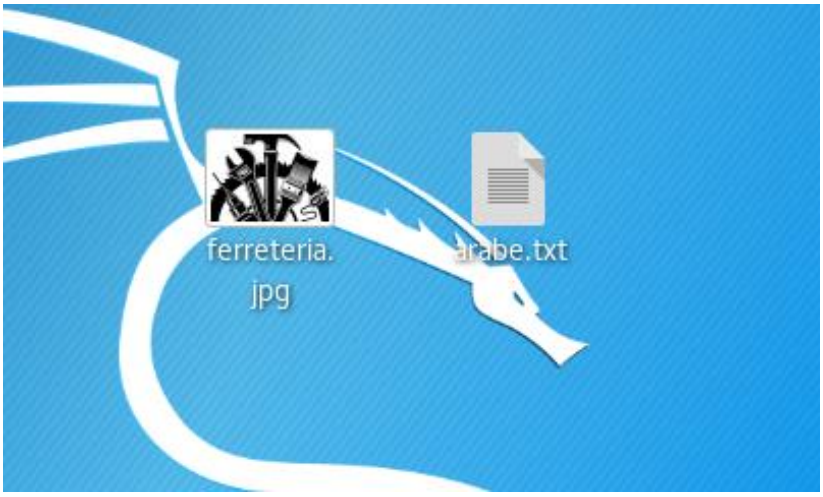


Figura 4-3 Imagen y fichero de texto extraído

En la Figura 4-4 podemos ver el contenido del archivo de texto.

Figura 4-4 Texto oculto

Para finalizar este apartado y confirmar actividad maliciosa, veamos en la Figura 4-5 lo que significa el mensaje en árabe.

Figura 4-5 Traducción del mensaje oculto

Con esto, el alumno acaba de confirmar el carácter malicioso de la ferretería online.

4.3 Acceso a la web yihadista

4.3.1 Enunciado

Muchas gracias por la información aportada. La confirmación de posibles actividades terroristas ha dado lugar a la autorización de un equipo del CNI a investigar en profundidad a nuestro sospechoso.

Por lo que parece, han conseguido capturar una traza de tráfico de su equipo personal. ¿Podrías obtener algún resultado analizando la traza?

Pista: Credenciales de autenticación, usuarios, imágenes…

4.3.2 Solución

Después de que el alumno reciba dicha traza de tráfico, deberá saber interpretarla analizando las diferentes peticiones del sospechoso y las diferentes respuestas del servidor, averiguando así en qué petición podría haber información importante. Una vez obtenga el usuario y contraseña de nuestro sospechoso, el alumno deberá autentificarse en la web y recopilar información: nombres de usuario, correos electrónicos y otros detalles que puedan ser de ayuda.

4.3.2.1 *Scan* del servidor

Lo primero que deberemos hacer es un *scan* con Zenmap de la página web yihadista para ver qué servicios tiene habilitados el servidor. En la Figura 4-6 podemos ver los resultados.

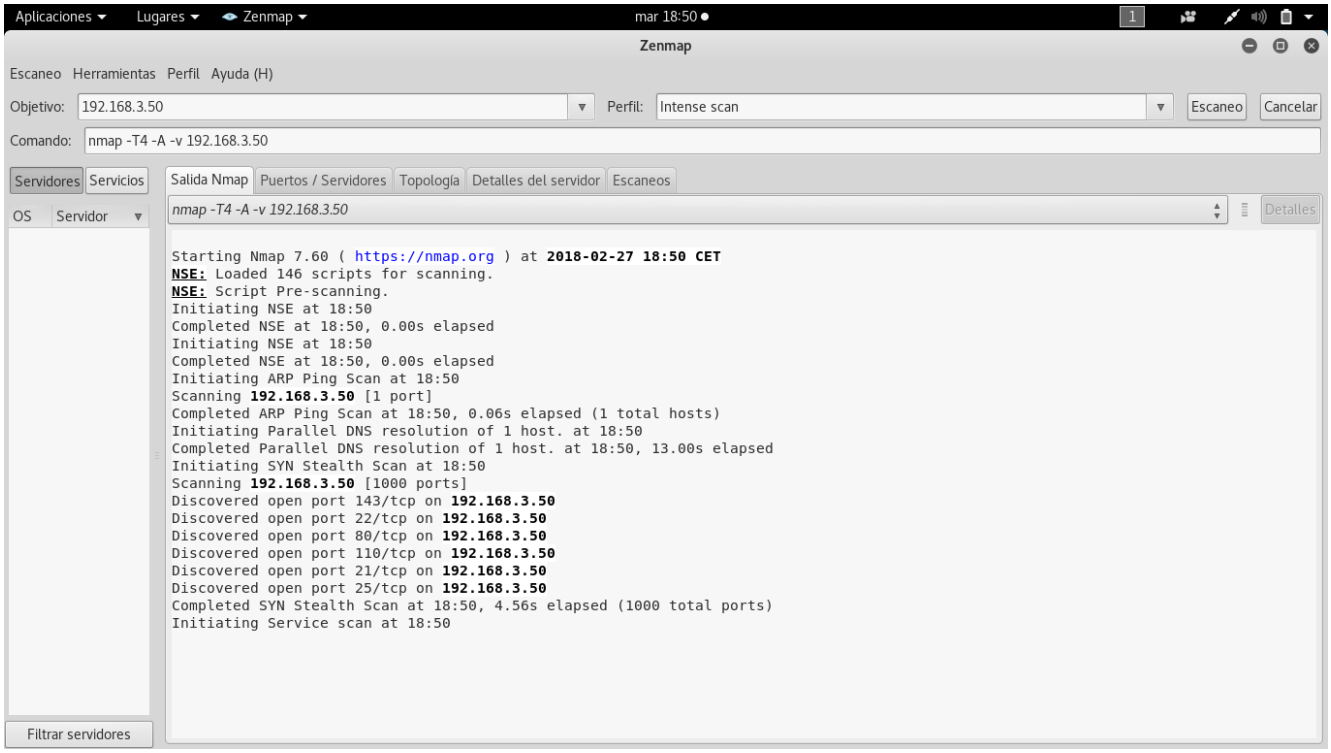


Figura 4-6 *Scan* del servidor yihadista

Zenmap nos indica qué puertos son los que mantiene abiertos el firewall para el paso de información. Sin embargo, como muestra la Figura 4-7, no nos muestra la arquitectura de red.

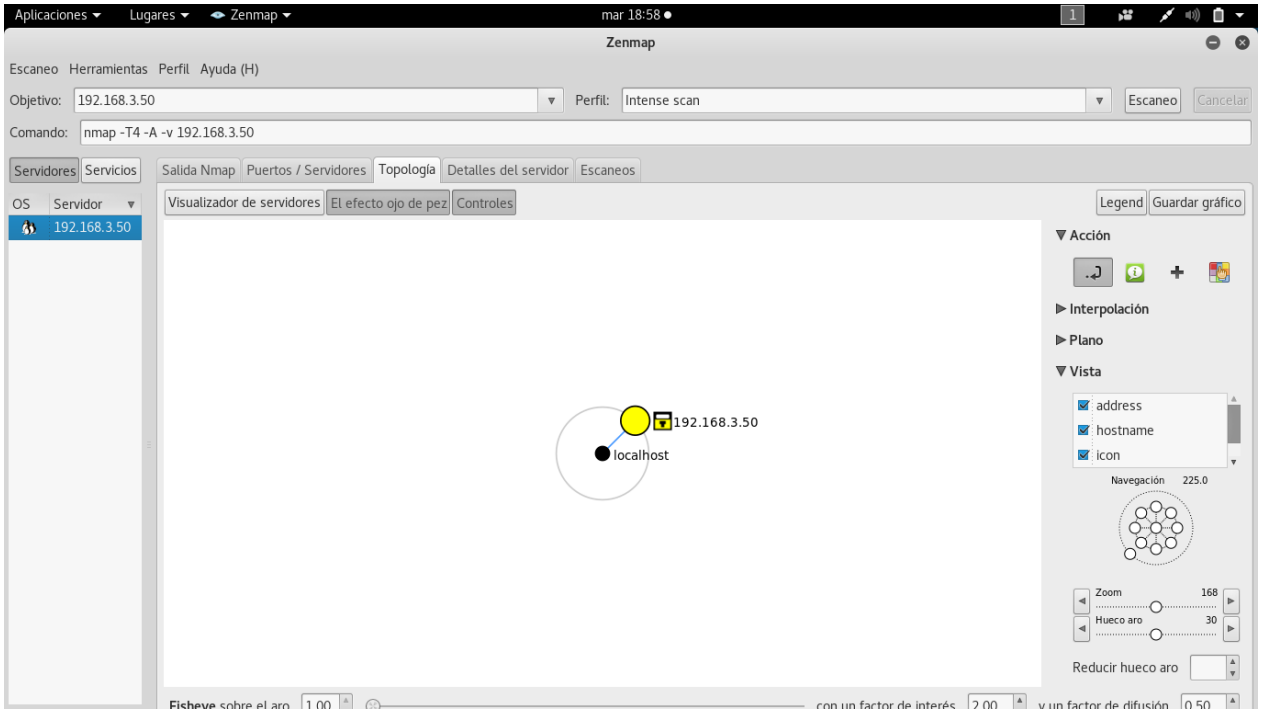


Figura 4-7 Arquitectura de red desde la WAN

En la Figura 4-8 podemos ver con detalle qué servicios son los que corren a través de cada puerto. Hay que destacar para futuros ciberejercicios sobre dicha maqueta, que el puerto 443, el cual se utiliza para HTTPS, se encuentra deshabilitado. Esto quiere decir que la información a nuestro servidor y la que vuelve no va cifrada, por lo que cualquier captura de tráfico o cualquier ataque basado en MITM podrían resultar muy eficaces a la hora de realizar alguna operación de 'esnifado'.

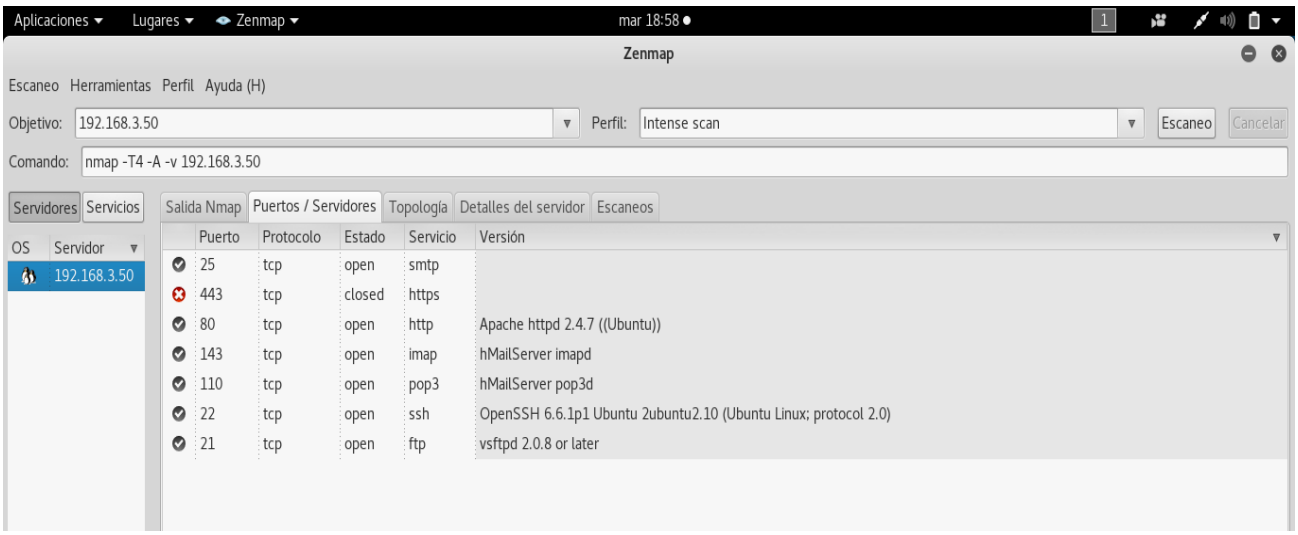


Figura 4-8 Servicios de la red

Otra herramienta muy útil contra páginas web construidas sobre Wordpress es Wpscan. Esta herramienta nos va a permitir escanear las vulnerabilidades a las que está expuesta la versión 2.5.1 instalada de Wordpress. Lo primero que haremos será abrir la herramienta y observar las diferentes opciones de las que dispone.

$ sudo wpscan –help

```
rootsudo@kalicud:~$ sudo wpscan --help
[sudo] password for rootsudo:

        WordPress Security Scanner by the WPScan Team
                         Version 2.9.3
          Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_

Help :

Some values are settable in a config file, see the example.conf.json

--update                          Update the database to the latest version.
--url       | -u <target url>     The WordPress URL/domain to scan.
--force     | -f                  Forces WPScan to not check if the remote site is running WordPress.
--enumerate | -e [option(s)]      Enumeration.
  option :
    u        usernames from id 1 to 10
    u[10-20] usernames from id 10 to 20 (you must write [] chars)
    p        plugins
    vp       only vulnerable plugins
    ap       all plugins (can take a long time)
    tt       timthumbs
    t        themes
    vt       only vulnerable themes
    at       all themes (can take a long time)
  Multiple values are allowed : "-e tt,p" will enumerate timthumbs and plugins
  If no option is supplied, the default is "vt,tt,u,vp"
```

Figura 4-9 Opciones de Wpscan

En la Figura 4-9 vemos que tiene una opción para escanear los usuarios, sin embargo, en la Figura 4-10 podemos ver como no es eficaz contra la página web.

$ sudo wpscan –url http://www.tfg.dunquerque.cud.uvigo.es –enumerate u

```
[+] Enumerating plugins from passive detection ...
[+] No plugins found

[+] Enumerating usernames ...
[+] We did not enumerate any usernames

[+] Finished: Sat Mar  3 16:36:37 2018
[+] Requests Done: 64
[+] Memory used: 32.223 MB
[+] Elapsed time: 00:00:03
rootsudo@kalicud:~$
```

Figura 4-10 Detección de usuarios

Sin embargo, sí podemos listar las vulnerabilidades de la versión 2.5.1 de Wordpress que hay hasta el momento. Esto es información muy interesante que puede ser útil a la hora de atacar una página web. En la Figura 4-11 se muestran algunas de las vulnerabilidades listadas.

$ sudo wpscan –url http://www.tfg.dunquerque.cud.uvigo.es

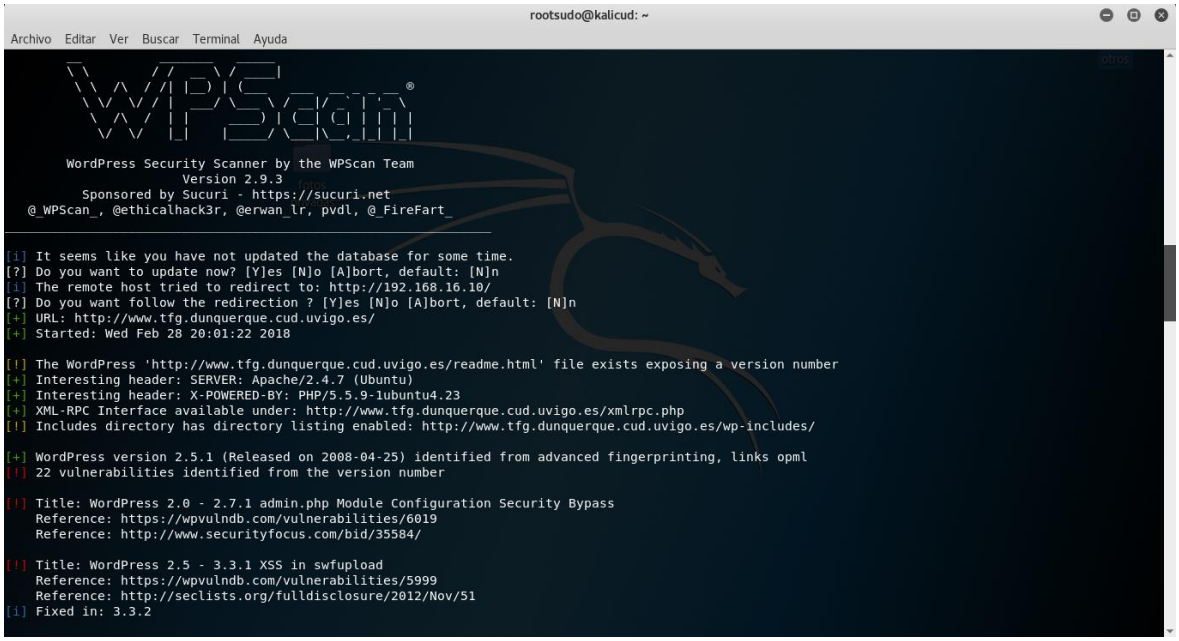


Figura 4-11 Análisis de Wordpress

Wpscan nos ha dado la opción de redirigirnos a la IP privada 192.168.16.10 (IP del servidor Wordpress). En este caso hemos elegido la opción N (No) ya que el *scan* debemos realizarlo desde la IP (192.168.3.50) donde se encuentra nuestra interfaz de red.

A continuación, haremos uso también de la herramienta Websploit. Es lógico pensar que, si hay una página web, también hay una base de datos; si hay una base de datos, es probable que para gestionarla se utilice alguna herramienta escrita en PHP. Para iniciar esta herramienta, debemos hacer lo siguiente:

$ sudo websploit

Wsf> show modules

En la Figura 4-12, debemos seleccionar uno de los módulos para identificar si nuestro servidor es gestionado mediante phpmyadmin. En este caso, utilizaremos *web/pma*.

Wsf> use web/pma

```
rootsudo@kalicud: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
Web Modules                    Description
-------------------            --------------------
web/apache_users               Scan Directory Of Apache Users
web/dir_scanner                Directory Scanner
web/wmap                       Information Gathering From Victim Web Using (Metasploit Wmap)
web/pma                        PHPMyAdmin Login Page Scanner
web/cloudflare_resolver        CloudFlare Resolver

Network Modules                Description
-------------------            --------------------
network/arp_dos                ARP Cache Denial Of Service Attack
network/mfod                   Middle Finger Of Doom Attack
network/mitm                   Man In The Middle Attack
network/mlitm                  Man Left In The Middle Attack
network/webkiller              TCP Kill Attack
network/fakeupdate             Fake Update Attack Using DNS Spoof
network/arp_poisoner           Arp Poisoner

Exploit Modules                Description
-------------------            --------------------
exploit/autopwn                Metasploit Autopwn Service
exploit/browser_autopwn        Metasploit Browser Autopwn Service
exploit/java_applet            Java Applet Attack (Using HTML)

Wireless / Bluetooth Modules   Description
-------------------            --------------------
wifi/wifi_jammer               Wifi Jammer
wifi/wifi_dos                  Wifi Dos Attack
wifi/wifi_honeypot             Wireless Honeypot(Fake AP)
wifi/mass_deauth               Mass Deauthentication Attack
bluetooth/bluetooth_pod        Bluetooth Ping Of Death Attack

wsf > use web/pma
```

Figura 4-12 Módulos de Websploit

A continuación, como puede verse en la Figura 4-13, seleccionamos nuestro objetivo (*target*).

Wsf: PMA> show options

Wsf: PMA> set TARGET http://www.tfg.dunquerque.cud.uvigo.es

```
wsf > use web/pma
wsf:PMA > show options

Options          Value
---------       --------------
TARGET          http://google.com

wsf:PMA > set TARGET http://www.tfg.dunquerque.cud.uvigo.es
TARGET =>  http://www.tfg.dunquerque.cud.uvigo.es
wsf:PMA >
```

Figura 4-13 Selección del objetivo

Para finalizar, como se ve en la Figura 4-14, con la herramienta Websploit, solo debemos lanzar el exploit seleccionado y esperar resultados.

Wsf: PMA> run

```
wsf:PMA > set TARGET http://www.tfg.dunquerque.cud.uvigo.es
TARGET =>  http://www.tfg.dunquerque.cud.uvigo.es
wsf:PMA > run
[*] Your Target : www.tfg.dunquerque.cud.uvigo.es
[*]Loading Path List ... Please Wait ...
[/phpMyAdmin/] ... [404 Not Found]
[/phpmyadmin/] ... [200 OK]
[/PMA/] ... [404 Not Found]
[/admin/] ... [404 Not Found]
[/dbadmin/] ... [404 Not Found]
[/mysql/] ... [404 Not Found]
[/myadmin/] ... [404 Not Found]
[/phpmyadmin2/] ... [404 Not Found]
[/phpMyAdmin2/] ... [404 Not Found]
[/phpMyAdmin-2/] ... [404 Not Found]
[/php-my-admin/] ... [404 Not Found]
[/phpMyAdmin-2.2.3/] ... [404 Not Found]
[/phpMyAdmin-2.2.6/] ... [404 Not Found]
[/phpMyAdmin-2.5.1/] ... [404 Not Found]
[/phpMyAdmin-2.5.4/] ... [404 Not Found]
[/phpMyAdmin-2.5.5-rc1/] ... [404 Not Found]
[/phpMyAdmin-2.5.5-rc2/] ... [404 Not Found]
[/phpMyAdmin-2.5.5/] ... [404 Not Found]
[/phpMyAdmin-2.5.5-pl1/] ... [404 Not Found]
[/phpMyAdmin-2.5.6-rc1/] ... [404 Not Found]
[/phpMyAdmin-2.5.6-rc2/] ... [404 Not Found]
[/phpMyAdmin-2.5.6/] ... [404 Not Found]
[/phpMyAdmin-2.5.7/] ... [404 Not Found]
[/phpMyAdmin-2.5.7-pl1/] ... [404 Not Found]
[/phpMyAdmin-2.6.0-alpha/] ... [404 Not Found]
[/phpMyAdmin-2.6.0-alpha2/] ... [404 Not Found]
[/phpMyAdmin-2.6.0-beta1/] ... [404 Not Found]
[/phpMyAdmin-2.6.0-beta2/] ... [404 Not Found]
[/phpMyAdmin-2.6.0-rc1/] ... [404 Not Found]
[/phpMyAdmin-2.6.0-rc2/] ... [404 Not Found]
[/phpMyAdmin-2.6.0-rc3/] ... [404 Not Found]
[/phpMyAdmin-2.6.0/] ... [404 Not Found]
```

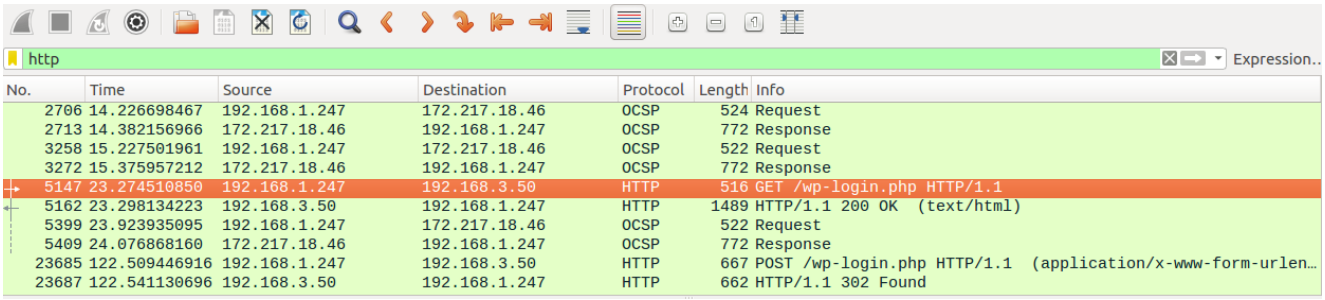
Figura 4-14 Exploit contra phpmyadmin

No solo confirmamos la presencia de phpmyadmin, sino que además tenemos localizada la ruta para acceder al portal: */phpmyadmin/*.

Con toda la información recopilada permitimos un abanico de posibilidades por las cuales el alumno puede obtener datos que le permitan acceder al servidor de la DMZ a través del puerto 22. Sin embargo, como hemos dejado ver, la razón por la que instalamos una versión más antigua de Wordpress es facilitar al alumno la explotación de vulnerabilidades en vista a desarrollar otro tipo de ciberejercicios en posteriores trabajos. En este ciberejercicio, puesto que el nivel elegido ha sido medio/bajo, le facilitaremos al alumno el fichero *.pcapng* que creamos en el apartado 3.5.7 y así fomentar la familiarización con el estudio de trazas de tráfico.

4.3.2.2 Estudio del tráfico de red

Una vez abrimos la traza que nos han dado, debemos buscar los paquetes que pueden interesarnos: en este caso, los paquetes de un flujo HTTP. Para ello filtramos este tipo de paquetes en la barra superior de búsqueda como muestra la Figura 4-15.



No.	Time	Source	Destination	Protocol	Length	Info
2706	14.226698467	192.168.1.247	172.217.18.46	OCSP	524	Request
2713	14.382156966	172.217.18.46	192.168.1.247	OCSP	772	Response
3258	15.227501961	192.168.1.247	172.217.18.46	OCSP	522	Request
3272	15.375957212	172.217.18.46	192.168.1.247	OCSP	772	Response
5147	23.274510850	192.168.1.247	192.168.3.50	HTTP	516	GET /wp-login.php HTTP/1.1
5162	23.298134223	192.168.3.50	192.168.1.247	HTTP	1489	HTTP/1.1 200 OK (text/html)
5399	23.923935095	192.168.1.247	172.217.18.46	OCSP	522	Request
5409	24.076868160	172.217.18.46	192.168.1.247	OCSP	772	Response
23685	122.509446916	192.168.1.247	192.168.3.50	HTTP	667	POST /wp-login.php HTTP/1.1 (application/x-www-form-urlen…
23687	122.541130696	192.168.3.50	192.168.1.247	HTTP	662	HTTP/1.1 302 Found

Figura 4-15 Paquetes HTTP filtrados

Una vez filtramos los paquetes, comenzamos a buscar los paquetes capturados entre nuestra víctima y la página de Wordpress, en este caso los paquetes correspondientes a la IP 192.168.3.50.

Como veremos a continuación en la Figura 4-16, podemos distinguir conexiones que podrían ser de gran interés:

- 192.168.1.247 > 192.168.3.50: HTTP: 516 GET /wp-login.php HTTP/1.1 (la víctima hace una petición de *login* a la página de Wordpress).
- 192.168.3.50 > 192.168.1.247: HTTP: 1489 HTTP/1.1 200 OK (el servidor recibe la petición y envía la página a la víctima).
- 192.168.1.247 > 192.168.3.50: HTTP: 667 POST /wp-login.php HTTP/1.1 (la víctima introduce sus datos de acceso y los envía al servidor).

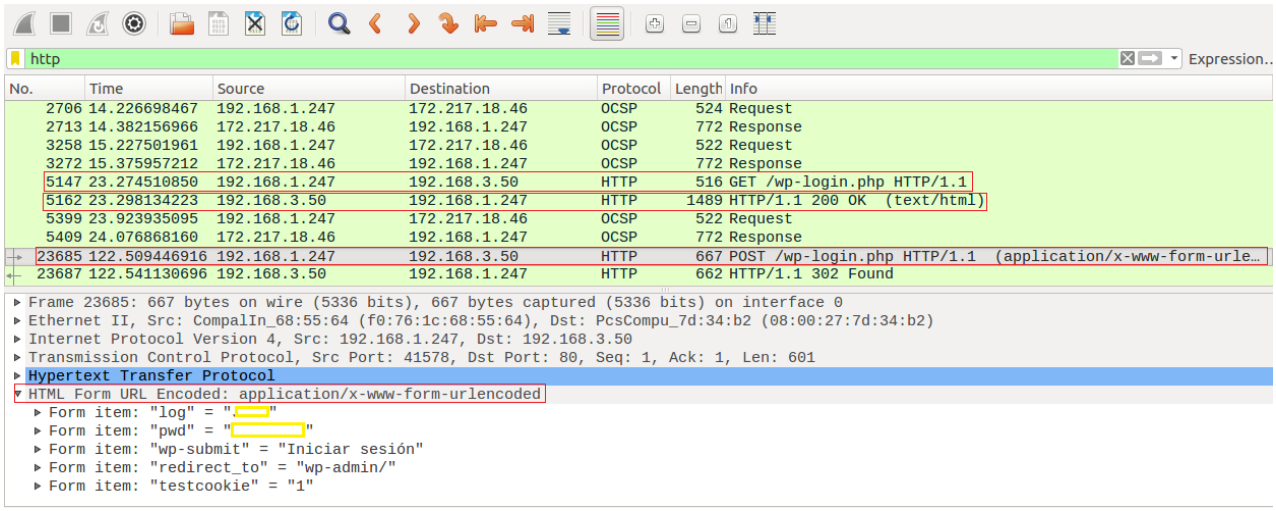


Figura 4-16 Usuario y contraseña en wireshark

Dentro de este último paquete, en la sección *HTML Form URL Encoded*, podemos distinguir en claro las credenciales de la víctima accediendo a la zona privada de Wordpress.

4.3.2.3 *Scan* de la web

Una vez obtenemos las credenciales del usuario de la web de la ferretería online, accedemos a través de la opción 'iniciar sesión' de la web a un portal de autenticación como el que muestra la Figura 4-17.

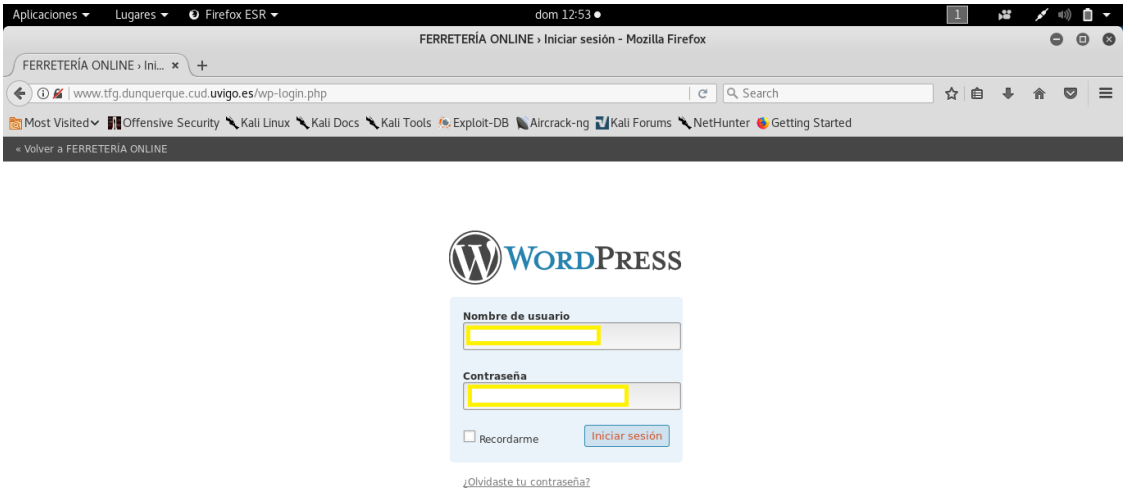


Figura 4-17 Acceso de usuario a la web

Dentro de todo lo que se puede observar en la zona privada de la web, podemos confirmar que se trata de un grupo activo yihadista. El alumno deberá recopilar información de los usuarios y detectar la

anomalía que presenta el usuario llamado Qutaybah. Este usuario es un usuario administrador que, como muestra la Figura 4-18, utiliza su nombre como usuario en el correo electrónico, en el usuario de la web, etc.

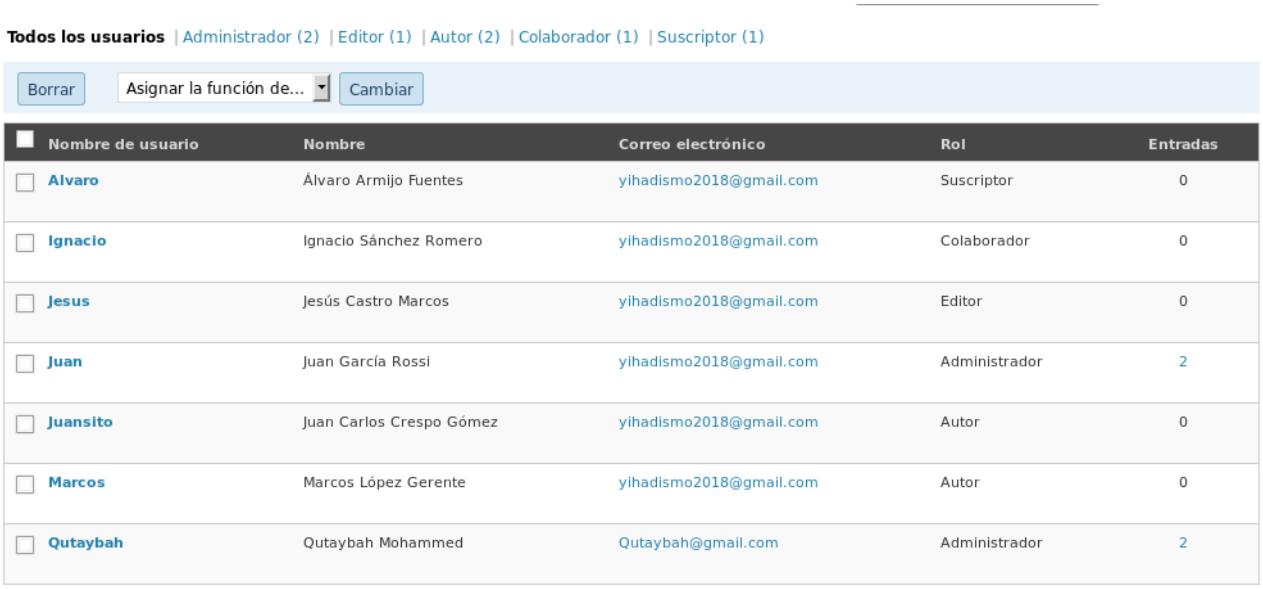


Figura 4-18 Usuarios de la web

Por último, dentro de la sección de entradas privadas a las que tenemos acceso tras haber accedido a la web como usuario, debemos observar una entrada característica y es, como se ve en la Figura 4-19, una entrada en la que se menciona al 'jefe' de una operación.

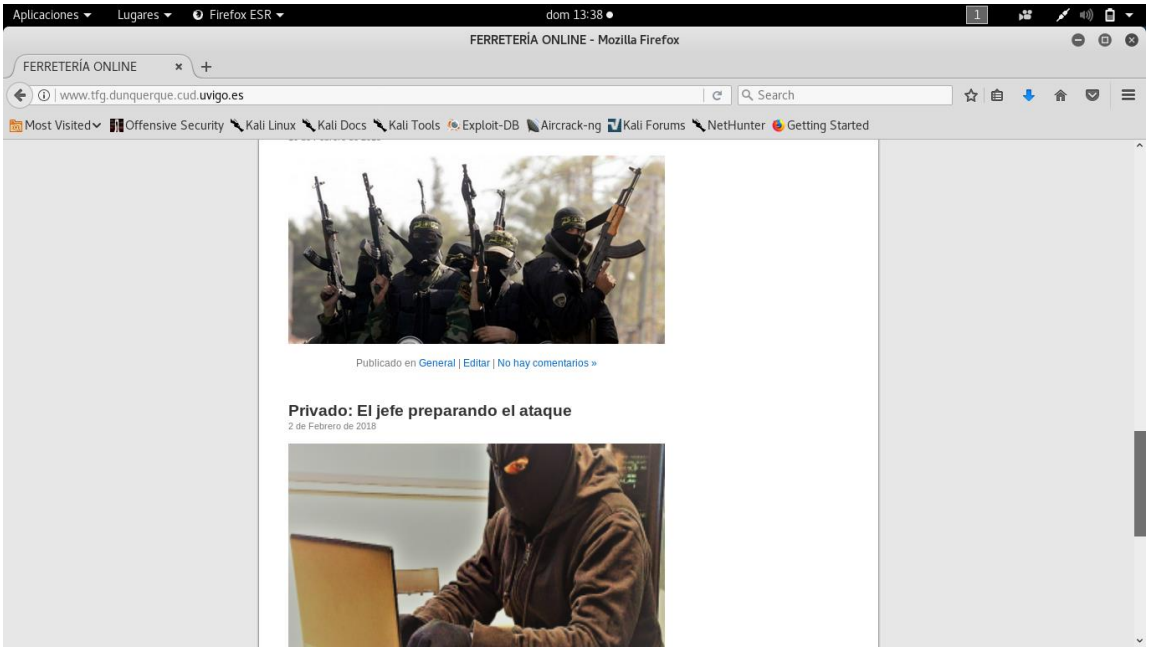


Figura 4-19 Entradas privadas

En la fotografía de dicha entrada se puede apreciar un pequeño *post-it* en el cual se dejan ver la contraseña y el usuario del llamado jefe. Si ampliamos la imagen de la Figura 4-20, podemos obtener información muy importante que entregarle al CNI.

Figura 4-20 Jefe de la operación

4.4 Acceso al servidor

4.4.1 Enunciado

Parece ser que las sospechas se confirman y se trata de una célula yihadista que se encuentra activa. La información que nos has ofrecido es muy valiosa, sin embargo parece que hemos levantado sospechas en el grupo terrorista y nos hemos visto obligados a detener nuestras acciones. ¿Podrías usar esta información para tener acceso a la red privada?

Pista: Accede y toma el control del servidor de la DMZ.

4.4.2 Solución

Una vez el alumno haya identificado y recopilado los nombres de usuarios, deberá identificar como usuarios importantes los usuarios administradores: Juan y Qutaybah. Sin embargo, el usuario Qutaybah, a diferencia del resto de usuarios, como hemos dicho anteriormente, tiende a usar su nombre para diferentes cuentas, correos, etc.

4.4.2.1 Ataque a servidor

Una de las herramientas de Kali Linux que vamos a utilizar a continuación es Hydra, ya mencionada en el apartado 3.3.2. Hasta ahora tenemos nombres de usuario y el servicio SSH corriendo en el puerto 22. Solo faltaría obtener la contraseña, y la obtendremos mediante un ataque de fuerza bruta.

Lo primero que debemos hacer es iniciar la herramienta Hydra y, como muestra la Figura 4-21, introducir los parámetros del objetivo.

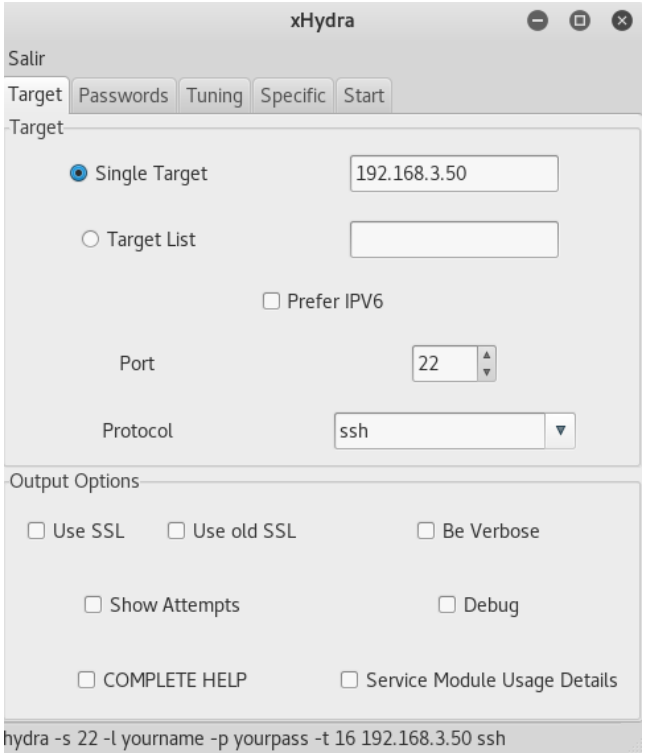


Figura 4-21 Opciones del objetivo

A continuación, en la Figura 4-22 definimos los parámetros para realizar el ataque. En este caso el usuario ya lo conocemos (de manera menos eficiente se podría crear un pequeño diccionario con el nombre de todos los usuarios de Wordpress) y, en la sección de *password*, elegiremos la opción *Password List*. En el caso de Kali Linux contamos ya con diccionarios bastante completos, aunque también hay varios enlaces en Internet: *https://www.renderlab.net/projects/WPA-tables/*.

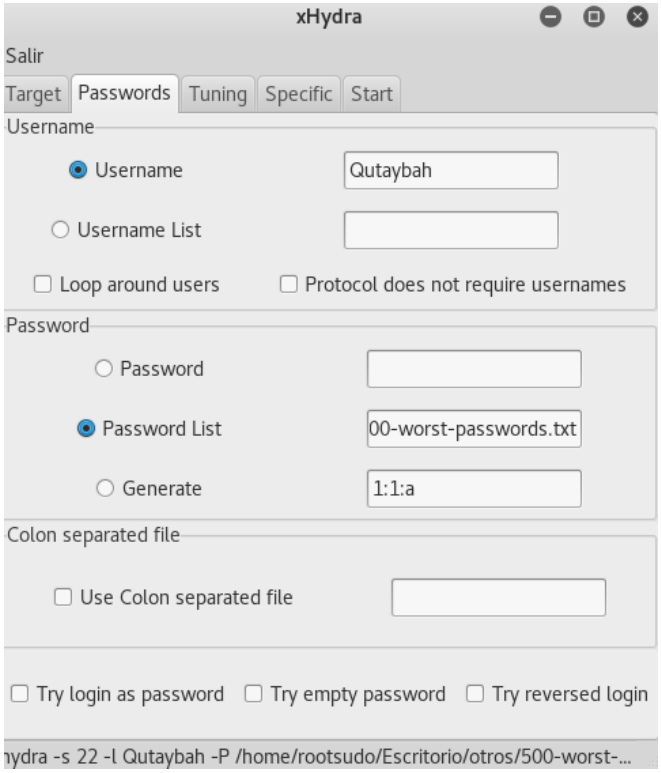


Figura 4-22 Parámetros de ataque

Por último, nos vamos a la sección *start* y comenzamos el ataque pulsando '*start*' en la esquina inferior izquierda del panel. En la Figura 4-23 podemos ver cómo, en poco segundos, el resultado es exitoso y obtenemos la clave del usuario Qutaybah.

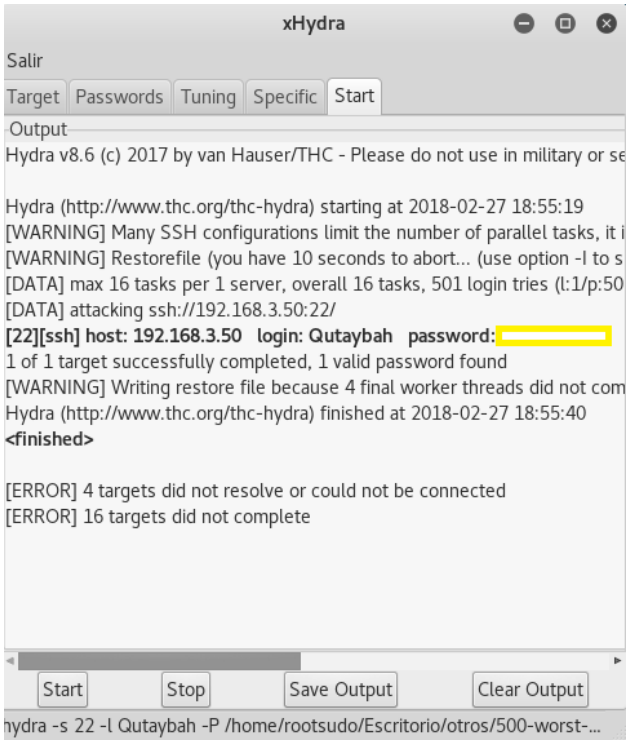


Figura 4-23 Resultado de ataque por fuerza bruta

4.4.2.2 Acceso al servidor

Una vez obtenemos la contraseña del usuario Qutaybah, basta con usar SSH para obtener acceso al servidor de la DMZ de la red yihadista. En la Figura 4-24 podemos ver el resultado con éxito.

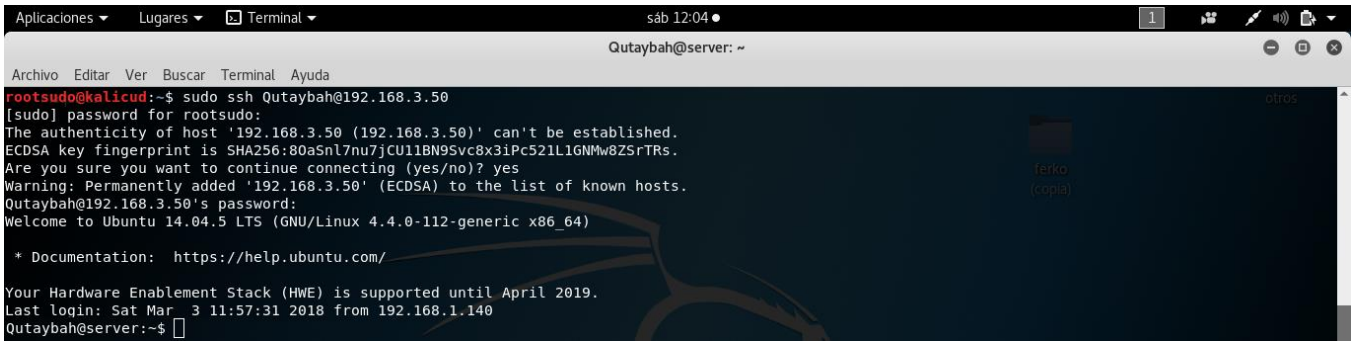


Figura 4-24 Acceso al servidor de la DMZ

4.5 Acceso al firewall

4.5.1 Enunciado

Nos han informado de que tienes acceso a uno de los servidores de la DMZ. ¡Fantástico! Sin embargo, no es suficiente. ¿Podrías acceder a la red LAN y obtener información crítica?

Pista: ¿Por qué no pruebas a acceder al firewall de la red?

4.5.2 Solución

Para que el alumno tenga acceso a la red LAN, primero deberá modificar las reglas del firewall de la red y habilitar el acceso a la LAN desde la DMZ. Para acceder al firewall, deberá usar el servidor

como puente: el firewall no permite la comunicación desde el exterior pero sí desde el interior de la red. El alumno deberá configurar el servidor para que, las peticiones que se manden al puerto 80 del servidor desde el exterior sean redirigidas al firewall y, a su vez, las contestaciones del firewall que se devuelvan al servidor sean redirigidas hacia el exterior a la máquina del alumno. Una vez modificado el firewall y configurado el acceso a la LAN desde la DMZ, el alumno deberá utilizar nuevamente la información que pudo obtener de la zona privada de la página de la ferretería online para acceder a un equipo de la LAN.

4.5.2.1 Configuración del servidor

Antes de acceder, veamos si podemos obtener información desde el servidor de la DMZ. Para ello, primero deberemos saber cuál es la puerta de enlace/pasarela (*gateway*) del servidor, ya que será esta la entrada, a través del firewall, del segmento de red en el que nos encontramos. Para ello, como muestra la Figura 4-25, usaremos el siguiente comando:

$ sudo route –n

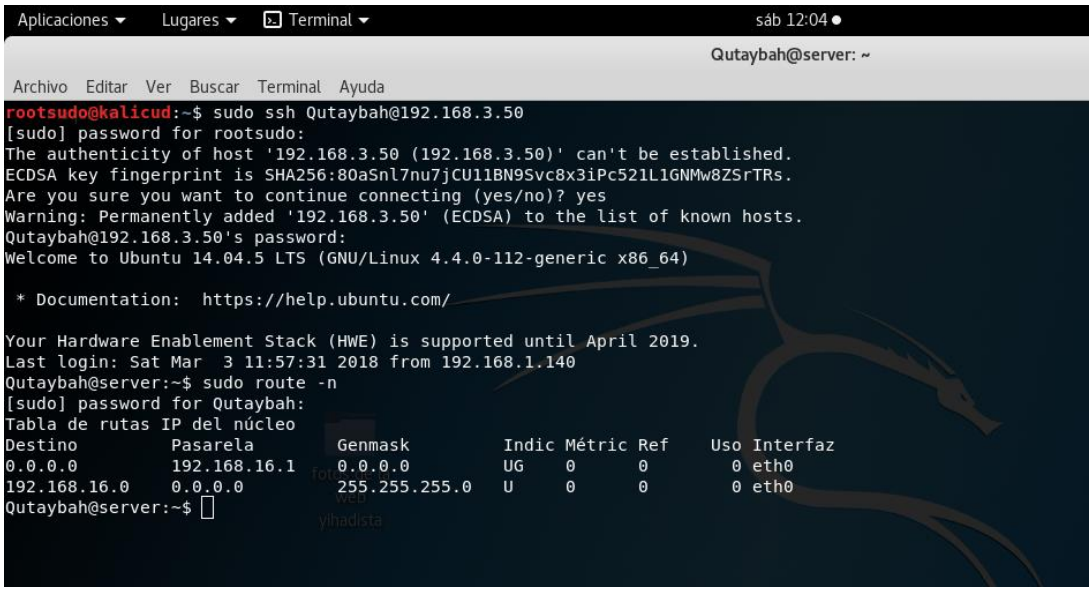


Figura 4-25 Pasarela al firewall

Una vez conocida la pasarela, analizamos los servidores que se encuentran en nuestro segmento de red. Analizaremos el siguiente rango de IP: 192.168.16.1/24. De las múltiples opciones hemos elegido la opción –PS20 ya que consiste en el descubrimiento de equipos, y la opción –O para analizar sistemas operativos. Los resultados son los siguientes:

$ sudo nmap –PS20 –O 192.168.16.1/24

- Servidor FTP (Figura 4-26).
- Servidor e-mail (Figura 4-27).
- Base de datos (Figura 4-28).
- Servidor DNS (Figura 4-29).

```
Nmap scan report for ubuntus-2.tfg.dunquerque.cud.uvigo.es (192.168.16.11)
Host is up (0.00061s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: 08:00:27:50:18:3D (Cadmus Computer Systems)
No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=6.40%E=4%D=3/3%OT=21%CT=1%CU=31472%PV=Y%DS=1%DC=D%G=Y%M=080027%TM
OS:=5A9AD3DD%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=10B%TI=Z%CI=I%TS=8)
OS:OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4
OS:ST11NW7%O6=M5B4ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)
OS:ECN(R=Y%DF=Y%T=40%W=7210%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%
OS:F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T
OS:5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=
OS:Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF
OS:=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40
OS:%CD=S)
Network Distance: 1 hop
```

Figura 4-26 Servidor FTP

```
Nmap scan report for win2008s-2.tfg.dunquerque.cud.uvigo.es (192.168.16.21)
Host is up (0.00051s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
143/tcp   open  imap
445/tcp   open  microsoft-ds
587/tcp   open  submission
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
MAC Address: 08:00:27:5C:E0:2C (Cadmus Computer Systems)
Device type: general purpose
Running: Microsoft Windows 2008|7
OS CPE: cpe:/o:microsoft:windows_server_2008::sp2 cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_8
OS details: Microsoft Windows Server 2008 SP2, Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, or Windows 8
Network Distance: 1 hop
```

Figura 4-27 Servidor e-mail

```
Nmap scan report for ubuntus-3.tfg.dunquerque.cud.uvigo.es (192.168.16.12)
Host is up (0.00064s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
3306/tcp open  mysql
MAC Address: 08:00:27:86:DA:9F (Cadmus Computer Systems)
No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=6.40%E=4%D=3/3%OT=3306%CT=1%CU=34866%PV=Y%DS=1%DC=D%G=Y%M=080027%
OS:TM=5A9AD3DD%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=10B%TI=Z%CI=I%TS=
OS:8)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5
OS:B4ST11NW7%O6=M5B4ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=712
OS:0)ECN(R=Y%DF=Y%T=40%W=7210%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S
OS:+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=
OS:)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%
OS:A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%
OS:DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=
OS:40%CD=S)
```

Figura 4-28 Base de datos

```
Nmap scan report for win2008s-1.tfg.dunquerque.cud.uvigo.es (192.168.16.20)
Host is up (0.00053s latency).
Not shown: 982 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
MAC Address: 08:00:27:B3:61:A0 (Cadmus Computer Systems)
Device type: general purpose
Running: Microsoft Windows 2008|7
OS CPE: cpe:/o:microsoft:windows_server_2008::sp2 cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_8
OS details: Microsoft Windows Server 2008 SP2, Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, or Windows 8
Network Distance: 1 hop
```

Figura 4-29 Servidor DNS

Los distintos puertos de los diferentes servidores caracterizan la función de cada servidor dentro de la DMZ. En algunos casos, podemos identificar también el sistema operativo de alguno de los servidores. En cualquier caso, un fallo claro de seguridad ha sido proporcionar un nombre a los servidores acorde al sistema operativo que tienen instalados. Lo que no hemos conseguido ha sido detectar otros segmentos de red, por lo que se deberá atacar el firewall para obtener más información, ya que en lo que respecta a este ciberejercicio, lo que buscamos es infiltrarnos en la red LAN.

Para permitir el acceso al firewall, modificaremos las iptables [90] del servidor. Las iptables son reglas individuales que funcionan como un firewall que viene integrado en el kernel de Linux. Recordemos que la pasarela por la que el firewall manda las peticiones a los servidores es a través de la IP 192.168.16.1. Lo que haremos será redirigir el tráfico que reciba el servidor web por el puerto 80 al puerto 80 del firewall y viceversa, de manera que el servidor funcione como 'puente'. Para ello, haremos uso de lo siguiente:

- Activar el funcionamiento de redireccionamiento del servidor y reiniciar el servicio.
    - *$ sudo sysctl –w net.ipv4.ip_forward=1*
    - *$ sudo sysctl –p*
- Configuramos la regla de direccionamiento. Es importante añadir la opción *–s 'IP del alumno'* para que el redireccionamiento solo ocurra desde nuestro equipo personal, de otra forma cualquier persona que accediese a la página web de la ferretería sería redireccionada al firewall de la red.
    - *$ sudo iptables –t nat –A PREROUTING –p tcp –s 'IP del alumno' –dport 80 –j DNAT –to-destination 192.168.16.1:80*
- Y por último, no debemos olvidarnos de indicar, con el siguiente comando, que el firewall reciba las peticiones como si fueran del servidor y no peticiones del exterior, de lo contrario no las aceptaría.
    - *$ sudo iptables –t nat –A POSTROUTING –j MASQUERADE*

En la Figura 4-30 se puede ver la secuencia completa.

```
Aplicaciones  Lugares  Terminal                    sáb 16:19
                                                   Qutaybah@server: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
rootsudo@kalicud:~$ sudo ssh Qutaybah@192.168.3.50
[sudo] password for rootsudo:
Qutaybah@192.168.3.50's password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-112-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

Your Hardware Enablement Stack (HWE) is supported until April 2019.
Last login: Sat Mar  3 16:11:40 2018 from 192.168.1.138
Qutaybah@server:~$ sudo route -n
[sudo] password for Qutaybah:
Tabla de rutas IP del núcleo
Destino         Pasarela        Genmask         Indic Métric Ref    Uso Interfaz
0.0.0.0         192.168.16.1    0.0.0.0         UG    0      0        0 eth0
192.168.16.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
Qutaybah@server:~$ sudo sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
Qutaybah@server:~$ sudo sysctl -p
Qutaybah@server:~$ sudo iptables -t nat -A PREROUTING -p tcp -s 192.168.2.16 --dport 80 -j DNAT --to-destination 192.168.16.1:80
Qutaybah@server:~$ sudo iptables -t nat -A POSTROUTING -j MASQUERADE
Qutaybah@server:~$
```

Figura 4-30 Configuración de iptables

4.5.2.2 Configuración del firewall

Cuando nos conectemos ahora al servidor desde el exterior, éste nos redireccionará al firewall de la red. Sin embargo, como puede verse en la Figura 4-31, el servidor DNS de la red parece detectar que la URL (*www.tfg.dunquerque.cud.uvigo.es*) correspondiente a la IP 192.168.16.10 de la página web, redirecciona a otro destino que no es la propia página web.

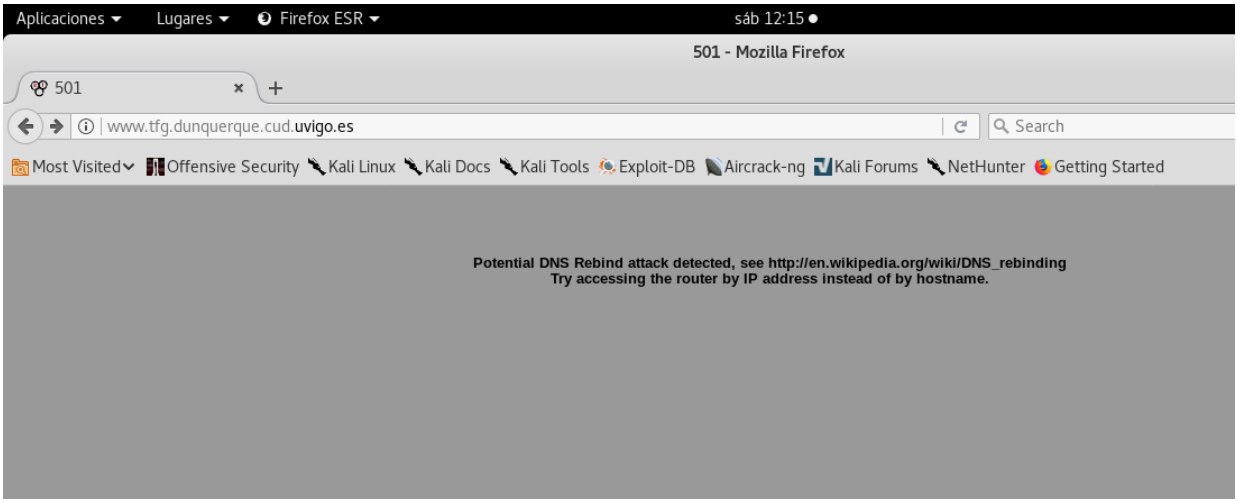


Figura 4-31 Detección del redireccionamiento

La propia imagen ya nos da la solución: debemos conectarnos sin utilizar el servidor DNS y utilizando directamente la IP. Es importante, para evitar interferencias, borrar el historial y las cookies de Firefox antes de conectarnos, pues muchas veces se guardan registros que nos llevarían a utilizar el servidor DNS automáticamente en lugar de utilizar la IP. En la Figura 4-32 podemos ver el acceso al firewall.

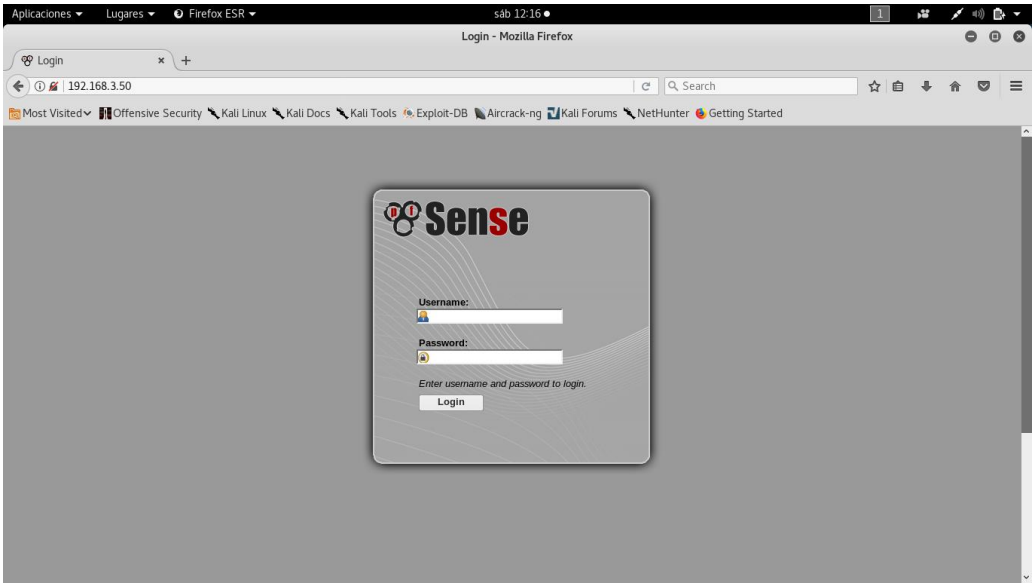


Figura 4-32 Acceso al firewall

Recordemos que el administrador no ha modificado el login y contraseña por defecto del pfsense (claro error de seguridad), por lo que las credenciales pueden encontrarse fácilmente en Internet. Una vez logueados, en la Figura 4-33 podemos observar los diferentes segmentos de red e identificar el segmento de la red LAN.

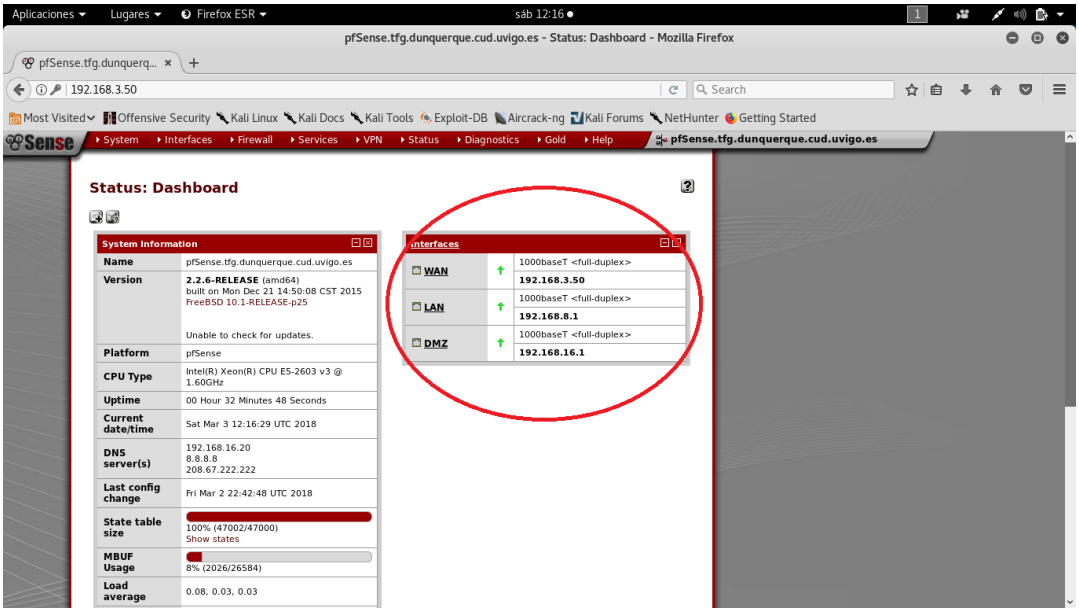


Figura 4-33 Segmentos de red

Nos dirigimos a las reglas que definen el acceso de la DMZ a la red LAN y, como vemos en la Figura 4-34, deshabilitamos la regla de restricción que impide el acceso a la LAN desde la DMZ.

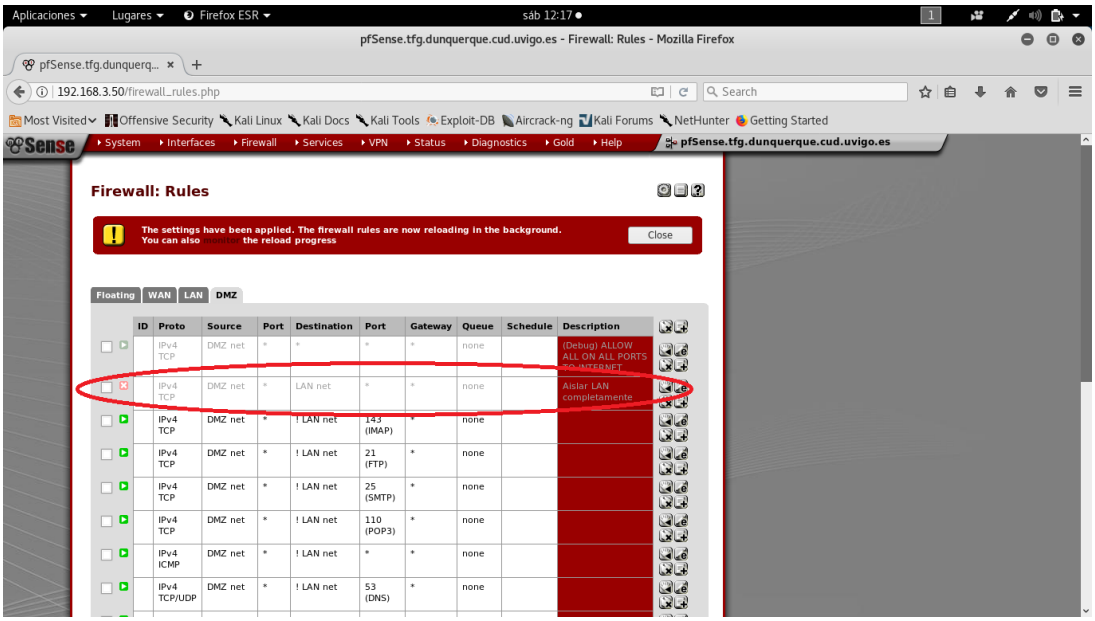


Figura 4-34 Activar acceso a LAN desde DMZ

Una vez modificado el firewall, si no queremos ser detectados es importante que eliminemos las iptables que hemos creado en el servidor y que desactivemos la función de redireccionamiento, aunque después debamos activarlo de nuevo para volver a modificar el firewall y volver a establecer la restricción que hemos desactivado.

- *$ sudo sysctl –w net.ipv4.ip_forward=0*
- *$ sudo sysctl –p*
- *$ sudo iptables –t nat –D PREROUTING –p tcp –s 'IP del alumno' –dport 80 –j DNAT –to-destination 192.168.16.1:80*
- *$ sudo iptables –t nat –D POSTROUTING –j MASQUERADE*

Si ahora escaneamos la red LAN con el segmento 192.168.8.1/21 podemos localizar dos equipos activos.

$ sudo nmap –PS20 –O 192.168.8.1/21

- Equipo 1 (Figura 4-35).
- Equipo 2 (Figura 4-36).

```
Qutaybah@server:~$ sudo nmap -PS20 -O 192.168.8.1/21

Starting Nmap 6.40 ( http://nmap.org ) at 2018-03-03 17:50 CET
Nmap scan report for 192.168.8.14
Host is up (0.0013s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=6.40%E=4%D=3/3%OT=22%CT=1%CU=30013%PV=Y%DS=2%DC=I%G=Y%TM=5A9AD308
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=103%TI=RD%II=RI%TS=8)SEQ(SP=
OS:105%GCD=1%ISR=103%TI=RD%TS=8)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NN
OS:T11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=7120%W2=7120%W3=
OS:7120%W4=7120%W5=7120%W6=7120)ECN(R=Y%DF=N%T=40%W=7210%O=M5B4NNSNW7%CC=Y%
OS:Q=)T1(R=Y%DF=N%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF
OS:=N%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=
OS:164%UN=0%RIPL=G%RID=5434%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
```

Figura 4-35 Descubrimiento del equipo 1

```
Nmap scan report for 192.168.9.1
Host is up (0.0011s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1028/tcp open  unknown
1029/tcp open  ms-lsa
1030/tcp open  iad1
1031/tcp open  iad2
No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=6.40%E=4%D=3/3%OT=135%CT=1%CU=38689%PV=Y%DS=2%DC=I%G=Y%TM=5A9AD30
OS:8%P=x86_64-pc-linux-gnu)SEQ(SP=F5%GCD=1%ISR=10D%TI=RD%TS=7)SEQ(SP=F5%GCD
OS:=2%ISR=10D%TI=RD%II=RI%TS=7)OPS(O1=M5B4NW8ST11%O2=M5B4NW8ST11%O3=M5B4NW8
OS:NNT11%O4=M5B4NW8ST11%O5=M5B4NW8ST11%O6=M5B4ST11)WIN(W1=2000%W2=2000%W3=2
OS:000%W4=2000%W5=2000%W6=2000)ECN(R=Y%DF=N%T=80%W=2000%O=M5B4NW8NNS%CC=N%Q
OS:=)T1(R=Y%DF=N%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=
OS:N%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=80%IPL=1
OS:64%UN=0%RIPL=G%RID=EE25%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 2 hops

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 2048 IP addresses (2 hosts up) scanned in 160.73 seconds
```

Figura 4-36 Descubrimiento del equipo 2

Si estudiamos dichos equipos, veremos que, al igual que el servidor web de la DMZ, uno de ellos tiene abierto el puerto 22. Ya solo debemos acceder a él con las credenciales que obtuvimos en la zona privada de la página web de la ferretería online. En la Figura 4-37 confirmamos el acceso a uno de los equipos de la red LAN desde el servidor web de la DMZ.

```
Aplicaciones ▾   Lugares ▾   Terminal ▾                    sáb 17:56 ●

Archivo  Editar  Ver  Buscar  Terminal  Ayuda
Qutaybah@server:~$ ssh khalid@192.168.8.14
khalid@192.168.8.14's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.10.0-28-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

Pueden actualizarse 371 paquetes.
220 actualizaciones son de seguridad.

Last login: Sat Mar  3 17:33:07 2018 from 192.168.16.10
khalid@khalid:~$
```

Figura 4-37 Acceso a la red LAN

4.5.2.3 Explotación del equipo LAN

Una vez hemos accedido al equipo de la red LAN, nos dirigimos a la carpeta de *Documentos* en la que encontraremos el documento de la factura de la ferretería. Lo primero que deberemos hacer para investigarlo es copiarlo y transferirlo a nuestro equipo personal. Para ello, deberemos hacerlo en dos pasos:

- Transferir el fichero desde el equipo de la red LAN al servidor de la DMZ
- Transferir el fichero desde la DMZ a nuestro equipo personal.

Como muestra la Figura 4-38, transferiremos el documento *.docx* al servidor de la DMZ en la ruta */home/server/*. Una vez copiado el fichero, cerraremos la sesión del equipo LAN.

$ sudo scp Factura.docx Qutaybah@192.168.3.50:/home/server/

```
khalid@khalid-VirtualBox: ~/Documentos
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
khalid@khalid-VirtualBox:~$ ls
Descargas   Escritorio        Imágenes  Plantillas  Vídeos
Documentos  examples.desktop  Música    Público
khalid@khalid-VirtualBox:~$ cd Documentos
khalid@khalid-VirtualBox:~/Documentos$ ls
Factura.docx
khalid@khalid-VirtualBox:~/Documentos$ sudo scp Factura.docx Qutaybah@192.168.3.
50:/home/server/
The authenticity of host '192.168.3.50 (192.168.3.50)' can't be established.
ECDSA key fingerprint is SHA256:8OaSnl7nu7jCU11BN9Svc8x3iPc521L1GNMw8ZSrTRs.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.3.50' (ECDSA) to the list of known hosts.
Qutaybah@192.168.3.50's password:
Factura.docx                                  100% 1126KB   1.1MB/s   00:00
khalid@khalid-VirtualBox:~/Documentos$ exit
```

Figura 4-38 Transferencia del archivo *.docx* al servidor de la DMZ

Puesto que cuando configuramos las reglas permitimos únicamente la conexión por SSH desde el exterior a la DMZ, no podremos copiar el archivo desde la DMZ, de modo que deberemos copiarlo abriendo la conexión por SSH desde nuestro propio equipo. No debemos olvidar eliminar el archivo de a DMZ una vez lo hayamos transferido a nuestro equipo personal. En la Figura 4-39 podemos ver el procedimiento.

$ sudo scp Qutaybah@192.168.3.50:/home/server/Factura.docx /home/rootsudo/Documentos

```
rootsudo@kalicud: /home
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
rootsudo@kalicud:/home$ sudo scp Qutaybah@192.168.3.50:/home/server/Factura.docx /home/rootsudo/Documentos
Qutaybah@192.168.3.50's password:
Factura.docx                                  100% 1126KB   9.9MB/s   00:00
rootsudo@kalicud:/home$
```

Figura 4-39 Transferencia del archivo *.docx* al equipo personal

Convertimos el archivo *.docx* en un archivo *.zip* y nos dirigimos a la ruta */Factura.zip/word/media/*. Como muestra la Figura 4-40, hemos obtenido la información del plan terrorista que buscábamos.

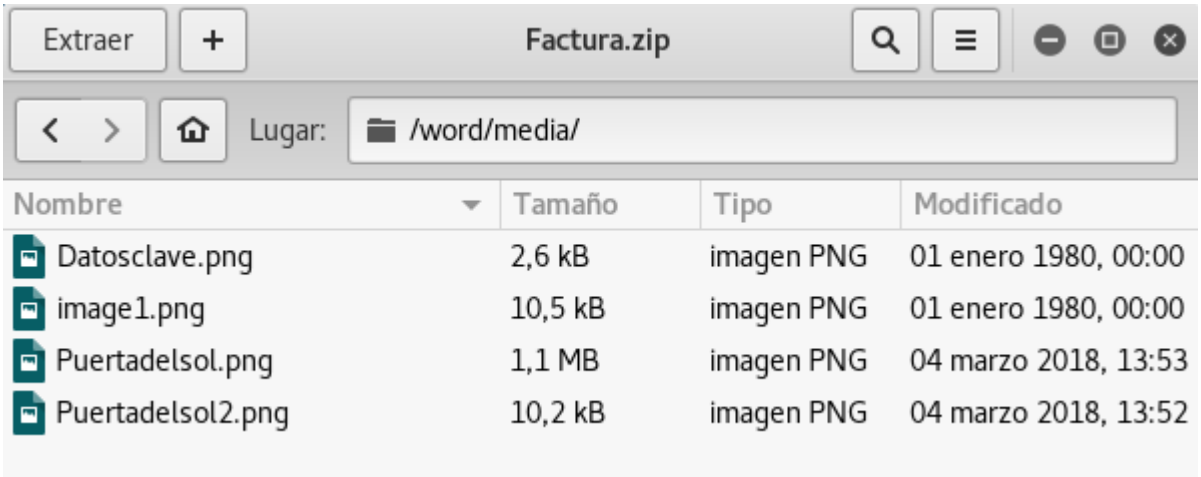


Figura 4-40 Plan terrorista

En la Figura 4-41 podemos ver las imágenes ocultas en el archivo *.docx*.

Figura 4-41 Puerta del Sol

Como ya se indicó al comienzo de este capítulo, el enunciado que se le ha de entregar al alumno que intente resolver este ciberejercicio se presenta en el Anexo I: Enunciado del ciberejercicio, así como las pistas para cada apartado.

5 CONCLUSIONES Y LÍNEAS FUTURAS

Tras la finalización del presente trabajo, analizaremos los diferentes objetivos que nos propusimos al inicio para, posteriormente, proponer algunas líneas futuras que permitan desarrollar la explotación de la maqueta de máquinas virtuales en red que hemos utilizado, y favorecer también el crecimiento de la concienciación de la ciberseguridad en el personal que así lo requiera.

5.1 Conclusiones

En primer lugar, analizando los objetivos propuestos en el apartado 1.3, se ha concluido con éxito el objetivo principal: la finalización del diseño de un ciberejercicio de ataque y su posterior implementación en la maqueta de máquinas virtuales en red. Desde el punto de vista del marco contextual en el que se desarrolla el ciberejercicio, a pesar del nivel de dificultad establecido, se ha conseguido dar el realismo que se pretendía con éxito: la intrusión en una red privada desde Internet a través de la obtención de información y herramientas de pentesting. A pesar de que la ciberseguridad sigue creciendo dentro de los sistemas TIC, el factor humano continúa siendo el eslabón más débil. Es por ello que, en la actualidad, tiende a ser la primera puerta que un ciberatacante ha de explotar para realizar un ciberataque con éxito. Gran parte de las veces, partiendo de un sistema tecnológico con un alto nivel de ciberseguridad, somos nosotras, las personas, las que creamos nuestros propios agujeros de seguridad.

A continuación, iremos analizando los diferentes objetivos secundarios que nos propusimos:

- Debido al nivel medio/bajo que hemos establecido, lo que puede no suponer un adiestramiento completo a personal especializado en el campo TIC, si supone una iniciación a todas aquellas personas interesadas en el ámbito de la seguridad informática. Hemos cumplido los diferentes requisitos que se pretendieron a la hora de diseñar el ciberejercicio para, de cierto modo, familiarizar a un usuario no especializado en la materia con algunos de los diferentes campos de la ciberseguridad.
- Respecto a la validación de la maqueta, podemos confirmar el alto grado de seguridad establecido en el TFG del Tte. Romero Fernández. El acceso restringido a la LAN desde la DMZ, a causa de la configuración del firewall, supuso la necesidad de modificarlo, así como la necesidad de crear nuevas reglas que permitiesen la conexión a la DMZ desde Internet. Una vez más, las vulnerabilidades encontradas más destacadas fueron a causa del factor humano: las credenciales de acceso por defecto al firewall de Pfsense y el nombre de los sistemas operativos como parte del nombre de cada servidor.
- Otro objetivo que consideramos cumplido es la concienciación del personal en torno a la ciberseguridad. Muchas veces el nivel de seguridad de una red depende de las personas: servicios que dejamos activos, usuarios y contraseñas fáciles de romper, datos públicos con

información relevante, etc. Damos por hecho que el alumno que realice el ciberejercicio tomará conciencia de cómo puede llegar a afectar a nuestro entorno el que nuestro ciberespacio sea violado y qué medidas se pueden tomar contra ello.

En lo que respecta a la parte personal, este trabajo me ha supuesto tomar conciencia de lo que pueden suponer vulnerabilidades de seguridad y la importancia de este campo en la actualidad. Conocer el funcionamiento de una red y su arquitectura me ha ayudado a comprender cómo funcionan algunos de los diferentes ciberataques. Por otro lado, saber que el factor humano influye en el diseño, implementación y configuración de una red, me proporciona cierta inseguridad, fomentando en mí la necesidad de saber que toda precaución es poca cuando se habla de proteger datos informáticos. Lo que antes veía como algo lejano, fuera de lo normal, ahora lo veo como una preocupación: una preocupación por saber que, en gran medida, las vulnerabilidades dependen de nosotros mismos. Añadir también que el diseño y la implementación del ciberejercicio también me ha servido para familiarizarme con algunos de los campos de pentesting a la hora de estudiar una red.

Cambiando la dinámica de las conclusiones, tras la finalización de este trabajo puedo decir que la desenvoltura y la capacidad para trabajar desde una terminal a través del uso de comandos también han sido incrementadas. Del mismo modo, también han sido ampliados los conocimientos en el campo de la virtualización y del trabajo de manera remota.

5.2 Líneas futuras

Una vez finalizado el diseño y la implementación del ciberataque, se proponen una serie de líneas a seguir para explotar los beneficios de trabajar con un entorno controlado como el que presenta la maqueta de máquinas virtuales en red.

Las ideas propuestas son las siguientes:

- El diseño y la implementación de otro tipo de ciberataques sobre la maqueta virtual, de modo que el alumno se formase en otros campos de la ciberseguridad.
- Subir el nivel de dificultad del ciberejercicio del presente trabajo, de modo que, una vez el alumno ha consolidado una base de conocimientos sobre ciberseguridad, pueda ir ampliándolos.
- Diseñar e implementar un ciberejercicio de defensa para estudiar y desarrollar el otro punto de vista de la ciberseguridad. Si bien en este ciberejercicio el alumno ha vulnerado la seguridad de una red, se trataría ahora de realizar un análisis forense tras detectar una intrusión.
- Continuando con algunas de las líneas futuras ya propuestas en el TFG del Tte Romero Fernández, se anima también a diseñar un entorno gráfico que facilite la configuración y el uso de la maqueta de red virtual, así como un software que permita visualizar en tiempo real la ejecución de un ciberejercicio de ataque/defensa que se ejecute en la maqueta.

6 BIBLIOGRAFÍA

[1] «Amazon,» [En línea]. Available: www.amazon.com. [Último acceso: 6 enero 2018].

[2] «El director del FBI asegura que la privacidad absoluta en internet "no existe",» Minuto Uno, [En línea]. Available: https://www.minutouno.com/notas/1540617-el-director-del-fbi-asegura-que-la-privacidad-absoluta-internet-no-existe. [Último acceso: 2018 enero 7].

[3] «Invertir en el sector de ciberseguridad,» Estrategias de inversión, [En línea]. Available: https://estrategafinanciero.com/seguridad-informatica-ciberseguridad/. [Último acceso: 10 enero 2018].

[4] «España, tercer país del mundo con más ciberataques,» El Mundo, [En línea]. Available: http://www.elmundo.es/espana/2017/05/15/5918ae9222601d51718b46d7.html. [Último acceso: 7 enero 2018].

[5] «Seguridad al día,» CCN-CERT, [En línea]. Available: https://www.ccn-cert.cni.es/seguridad-al-dia/noticias-seguridad.html?start=10. [Último acceso: 7 enero 2018].

[6] «Inditex sube las ventas en sus tiendas ‘online’ europeas el 35%,» El País, [En línea]. Available: https://elpais.com/economia/2017/10/18/actualidad/1508353708_596240.html. [Último acceso: 10 enero 2018].

[7] «La expansión,» [En línea]. Available: http://www.expansion.com/economia-digital/companias/2017/12/08/5a27d24e268e3ed9598b45f7.html. [Último acceso: 10 enero 2018].

[8] «CCN-CERT,» [En línea]. Available: https://www.ccn-cert.cni.es/. [Último acceso: 7 enero 2018].

[9] «MCCD,» Mando Conjunto de Ciberdefensa, [En línea]. Available: http://www.emad.mde.es/CIBERDEFENSA/. [Último acceso: 10 enero 2018].

[10] «El 90% de los ciberataques más graves en España procede de otros Gobiernos,» [En línea]. Available: https://politica.elpais.com/politica/2016/11/22/actualidad/1479843658_666221.html. [Último acceso: 6 enero 2018].

[11] «Plataforma Atenea,» CCN-CERT, [En línea]. Available: https://atenea.ccn-cert.cni.es/. [Último acceso: 9 enero 2018].

[12] «Diseño e implementación de una maqueta de máquinas virtuales en red para la simulación de ejercicios de ciberdefensa,» Víctor Romero Fernández, 2016. [En línea]. Available: http://calderon.cud.uvigo.es/handle/11621/80. [Último acceso: 23 enero 2018].

[13] «Introducción a los ataques,» [En línea]. Available: http://es.ccm.net/contents/17-introduccion-a-los-ataques. [Último acceso: 12 enero 2018].

[14] «Vulnerabilidad de HTTPS,» We Live Security, [En línea]. Available: https://www.welivesecurity.com/la-es/2015/03/04/freak-attack-vulnerabilidad-rompe-la-proteccion-https/. [Último acceso: 12 febrero 2018].

[15] «Zombie (Informática),» Wikipedia, [En línea]. Available: https://es.wikipedia.org/wiki/Zombi_(informática). [Último acceso: 15 enero 2018].

[16] «Gusano Morris,» Wikipedia, [En línea]. Available: https://es.wikipedia.org/wiki/Gusano_Morris. [Último acceso: 12 enero 2018].

[17] «Ciberamenazas y tendencias 16/17,» CCN-CERT, [En línea]. Available: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos.html. [Último acceso: 13 enero 2018].

[18] «*Internet Organised Crime Threat Assessment* (IOCTA),» Europol, 2017. [En línea]. Available: https://www.europol.europa.eu/iocta/2017/index.html. [Último acceso: 13 enero 2018].

[19] «El cibercrimen preocupa más que la delincuencia física, según una encuesta,» La vanguardia, [En línea]. Available: http://www.lavanguardia.com/vida/20170116/413414349138/el-cibercrimen-preocupa-mas-que-la-delincuencia-fisica-segun-una-encuesta.html. [Último acceso: 13 enero 2018].

[20] «El *ransomware* cerró 2016 con 638 millones de infecciones según SonicWall,» Genbeta, [En línea]. Available: https://www.genbeta.com/seguridad/el-ransomware-cerro-2016-con-638-millones-de-infecciones-segun-sonicwall. [Último acceso: 14 enero 2018].

[21] «*Deep Web*,» Xataka, [En línea]. Available: https://www.xataka.com/analisis/una-semana-en-la-deep-web-esto-es-lo-que-me-he-encontrado. [Último acceso: 13 enero 2018].

[22] «Filozufandus,» Filozufandus, [En línea]. Available: http://filozufandus.blogspot.com.es/2015/06/mais-de-200-sites-da-deep-web-para-voce.html. [Último acceso: 13 enero 2018].

[23] «El Centro Criptológico Nacional prevé que 2017 acabe con más de 26.500 ciberincidentes en el sector público,» Europapress, [En línea]. Available: http://www.europapress.es/portaltic/ciberseguridad/noticia-centro-criptologico-nacional-preve-2017-acabe-mas-26500-ciberincidentes-sector-publico-20171121161915.html. [Último acceso: 14 enero 2018].

[24] «Centro Criptológico Nacional- Seguridad en Tecnologías de la Información y Comunicación,» CCN-CERT, [En línea]. Available: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos.html. [Último acceso: 14 enero 2018].

[25] «Gestión de ciberincidentes,» CCN-CERT, [En línea]. Available: https://www.ccn-cert.cni.es/series-ccn...ccn...gestion-de-ciberincidentes/file.html. [Último acceso: 13 enero 2018].

[26] «Informe anual de seguridad nacional,» Departamento de Seguridad Nacional, 2016. [En línea]. Available: http://www.dsn.gob.es/es/documento/informe-anual-seguridad-nacional-2016. [Último acceso: 12 enero 2018].

[27] «Presentación del CCN-CERT,» CCN-CERT, [En línea]. Available: https://www.ccn-cert.cni.es/sobre-nosotros/video.html. [Último acceso: 15 enero 2018].

[28] «Objetivos del CCN-CERT,» CCN-CERT, [En línea]. Available: https://www.ccn-cert.cni.es/sobre-nosotros/mision-y-objetivos.html. [Último acceso: 15 enero 2018].

[29] «Estrategia de Ciberseguridad Nacional,» 2013. [En línea]. Available: https://www.ccn-cert.cni.es/sobre-nosotros/estrategia-ciberseguridad-nacional-2013.html. [Último acceso: 14 enero 2018].

[30] «Departamento de Seguridad Nacional,» Departamento de Seguridad Nacional, [En línea]. Available: http://www.dsn.gob.es/. [Último acceso: 17 enero 2018].

[31] «Informes de actualidad,» CCN-CERT, [En línea]. Available: https://www.ccn-cert.cni.es/seguridad-al-dia/noticias-seguridad.html. [Último acceso: 14 enero 2018].

[32] «Avisos y alertas del CCN-CERT,» CCN-CERT, [En línea]. Available: https://www.ccn-cert.cni.es/seguridad-al-dia/avisos-ccn-cert.html. [Último acceso: 16 enero 2018].

[33] «Instituto Nacional de Ciberseguridad,» INCIBE, [En línea]. Available: https://www.incibe.es/. [Último acceso: 15 enero 2018].

[34] «Objetivos,» INCIBE, [En línea]. Available: https://www.incibe.es/protege-tu-empresa/blog/que-objetivos-perseguimos-este-blog. [Último acceso: 15 enero 2018].

[35] «Organigrama INCIBE,» INCIBE, [En línea]. Available: https://www.incibe.es/que-es-incibe/organigrama. [Último acceso: 15 enero 2018].

[36] «¿Qué es INCIBE?,» INCIBE, [En línea]. Available: https://www.incibe.es/que-es-incibe. [Último acceso: 14 enero 2018].

[37] «Origen del MCCD,» MCCD, [En línea]. Available: http://www.emad.mde.es/CIBERDEFENSA/historia/. [Último acceso: 15 enero 2018].

[38] «Cometidos del MCCD,» MCCD, [En línea]. Available: http://www.emad.mde.es/CIBERDEFENSA/cometidos/. [Último acceso: 15 enero 2018].

[39] «España fichará a 2.000 hackers y expertos civiles contra las ciberamenazas,» ABC, [En línea]. Available: http://www.abc.es/espana/abci-espana-fichara-2000-hackers-y-expertos-civiles-contra-ciberamenazas-201801140302_noticia.html. [Último acceso: 14 enero 2018].

[40] «iPhalanx,» Indra, [En línea]. Available: https://www.indracompany.com/sites/default/files/indra_iphalanx_cyber_range_solution_es.pdf. [Último acceso: 14 enero 2018].

[41] «Atenea, nueva plataforma de retos en ciberseguridad,» Ciberseguridad, [En línea]. Available: https://cyberseguridad.net/index.php/570-atenea-nueva-plataforma-de-retos-en-ciberseguridad. [Último acceso: 14 enero 2018].

[42] «CTF365,» CTF365, [En línea]. Available: https://ctf365.com/dashboard. [Último acceso: 16 enero 2018].

[43] «Planes de contratación,» CTF365, [En línea]. Available: https://ctf365.com/plans#. [Último acceso: 16 enero 2018].

[44] «OverTheWire,» OverTheWire, [En línea]. Available: http://overthewire.org/wargames/. [Último acceso: 21 enero 2018].

[45] «Donaciones OverTheWire,» OverTheWire, [En línea]. Available: http://overthewire.org/about/. [Último acceso: 19 enero 2018].

[46] «Hacking-Lab,» Hacking-Lab, [En línea]. Available: https://www.hacking-lab.com/index.html. [Último acceso: 17 enero 2018].

[47] «LiveCD,» Hacking-Lab, [En línea]. Available: https://www.hacking-lab.com/download/. [Último acceso: 20 enero 2018].

[48] «Información,» Hacking-Lab, [En línea]. Available: https://www.hacking-lab.com/about/. [Último acceso: 20 enero 2018].

[49] «PWNABLE.KR,» PWNABLE.KR, [En línea]. Available: http://pwnable.kr/. [Último acceso: 20 enero 2018].

[50] «PWN,» Pcmag, [En línea]. Available: https://www.pcmag.com/encyclopedia/term/56903/pwn. [Último acceso: 21 enero 2018].

[51] «netgarage.org,» netgarage.org, [En línea]. Available: http://netgarage.org/. [Último acceso: 20 enero 2018].

[52] «SmashTheStack,» SmashTheStack, [En línea]. Available: http://smashthestack.org/faq.html#a1. [Último acceso: 21 enero 2018].

[53] «Netgarage,» Netgarage, [En línea]. Available: http://netgarage.org/. [Último acceso: 20 enero 2018].

[54] «Microcorruption Login,» Microcorruption, [En línea]. Available: https://microcorruption.com/login. [Último acceso: 21 enero 2018].

[55] «Microcorruption,» Microcorruption, [En línea]. Available: https://microcorruption.com/about. [Último acceso: 19 enero 2018].

[56] «Reversing.kr,» Reversing.kr, [En línea]. Available: http://reversing.kr/index.php. [Último acceso: 21 enero 2018].

[57] «Desafíos,» Reversing.kr, [En línea]. Available: http://reversing.kr/challenge.php. [Último acceso: 21 enero 2018].

[58] «HackThisSite,» HackThisSite, [En línea]. Available: https://www.hackthissite.org/info/about/#chal. [Último acceso: 20 enero 2018].

[59] «HackThisSite,» Wikipedia, [En línea]. Available: https://es.wikipedia.org/wiki/Jeremy_Hammond. [Último acceso: 20 enero 2018].

[60] «W3Challs,» W3Challs, [En línea]. Available: https://w3challs.com/. [Último acceso: 21 enero 2018].

[61] «*How the DMZ works*,» Techrepublic, [En línea]. Available: https://www.techrepublic.com/article/solutionbase-strengthen-network-defenses-by-using-a-dmz/. [Último acceso: 22 febrero 2018].

[62] «Zona DMZ,» Wikipedia, [En línea]. Available: https://es.wikipedia.org/wiki/Zona_desmilitarizada_(informática). [Último acceso: 22 enero 2018].

[63] «Virtualización,» Cursohacker, [En línea]. Available: http://cursohacker.es/que-es-la-virtualizacion-ventajas. [Último acceso: 22 enero 2018].

[64] «VirtualBox,» VirtualBox, [En línea]. Available: https://www.virtualbox.org/. [Último acceso: 23 enero 2018].

[65] «Lenovo,» Tienda Manchanet, [En línea]. Available: https://tienda.manchanet.es/ordenadores/portatiles/portatiles/marca-Lenovo/lenovo-80ew018usp-portatil-lenovo-b50-80ew-5500u-en-paratupc-pid1177292.html. [Último acceso: 1 febrero 2018].

[66] «GNS3,» GNS3, [En línea]. Available: https://www.gns3.com/software/download. [Último acceso: 17 febrero 2018].

[67] «KRDC,» KDE, [En línea]. Available: https://www.kde.org/applications/internet/krdc/. [Último acceso: 29 enero 2018].

[68] «Filezilla,» Filezilla, [En línea]. Available: https://filezilla-project.org/. [Último acceso: 1 febrero 2018].

[69] «SSH,» SSH, [En línea]. Available: https://www.ssh.com/ssh/. [Último acceso: 22 febrero 2018].

[70] «Nmap,» Nmap, [En línea]. Available: https://nmap.org. [Último acceso: 14 febrero 2018].

[71] «Hydra,» Hacking- ético, [En línea]. Available: https://hacking-etico.com/2014/02/05/ataque-de-fuerza-bruta-ssh-con-hydra/. [Último acceso: 19 febrero 2018].

[72] «Wireshark,» Wireshark, [En línea]. Available: https://www.wireshark.org/. [Último acceso: 28 febrero 2018].

[73] «Wpscan,» Wpscan, [En línea]. Available: https://wpscan.org/. [Último acceso: 28 febrero 2018].

[74] «Websploit,» Kali Linux, [En línea]. Available: https://kali-linux.net/article/websploit/. [Último acceso: 28 febrero 2018].

[75] «Descarga de Ubuntu Server 14.04.05,» Linux, [En línea]. Available: http://releases.ubuntu.com/14.04/ubuntu-14.04.5-server-amd64.iso. [Último acceso: 20 enero 2018].

[76] «Módulos del kernel,» [En línea]. Available: https://wiki.archlinux.org/index.php/Kernel_modules_(Espa%C3%B1ol). [Último acceso: 22 febrero 2018].

[77] «Wordpress,» Wordpress, [En línea]. Available: https://es.wordpress.org. [Último acceso: 1 febrero 2018].

[78] «Apache,» Apache, [En línea]. Available: https://www.apache.org/. [Último acceso: 5 febrero 2018].

[79] «Instalar LAMP,» Blog de César Ramírez, [En línea]. Available: https://platzi.com/wordpress/tutoriales/instalar-lamp-stack-en-linux-ubuntu-1404/. [Último acceso: 5 febrero 2018].

[80] «MySQL,» MySQL, [En línea]. Available: https://www.mysql.com/. [Último acceso: 6 febrero 2018].

[81] «Phpmyadmin,» Phpmyadmin, [En línea]. Available: https://www.phpmyadmin.net/. [Último acceso: 6 febrero 2018].

[82] «Traductor de idiomas,» Google, [En línea]. Available: https://translate.google.es/#es/ar/Necesito%20planes%20de%20ataque%0AEstoy%20en%20contacto. [Último acceso: 6 febrero 2018].

[83] «Steghide,» Steghide, [En línea]. Available: http://steghide.sourceforge.net/. [Último acceso: 16 febrero 2018].

[84] «GIMP,» GIMP, [En línea]. Available: http://www.gimp.org.es/. [Último acceso: 23 febrero 2018].

[85] «Descargar GIMP,» GIMP, [En línea]. Available: https://www.mirrorservice.org/sites/ftp.gimp.org/pub/gimp/v2.8/windows/gimp-2.8.22-setup.exe. [Último acceso: 23 febrero 2018].

[86] «Entrevista a Antonio Salas,» Onemagazine, [En línea]. Available: http://www.onemagazine.es/one-hacker-consejos-entrevista-antonio-salas. [Último acceso: 23 febrero 2018].

[87] «Los funcionarios que emiten las alertas de misiles en Hawái posaron para una entrevista con su contraseña en un post-it,» Guizmodo, [En línea]. Available: https://es.gizmodo.com/funcionarios-que-emitieron-la-alerta-de-misil-en-hawai-1822125463?utm_medium=sharefromsite&utm_source=Gizmodo_en_Espanol_twitter. [Último acceso: 24 febrero 2018].

[88] «DHCP,» Redes, [En línea]. Available: https.// camber1redes.wordpress.com/dhcp/. [Último acceso: 2 marzo 2018].

[89] «Documento .docx,» PcWorld, [En línea]. Available: http://pcworld.pe/guias-tips/microsoft-office-2010/cuales-son-las-ventajas-de-docx-vs-doc-y-de-los-demas-formatos-de-microsoft-office/. [Último acceso: 15 febrero 2018].

[90] «Iptables,» Universidad Austral de Chile, [En línea]. Available: https://es.slideshare.net/afiebig/iptables-que-es-y-como-funciona. [Último acceso: 3 marzo 2018].

ANEXO I: ENUNCIADO DEL CIBEREJERCICIO

El siguiente ciberejercicio está destinado al alumno que quiera iniciarse en técnicas básicas de pentesting. Su nivel de dificultad se ha establecido entre un nivel medio/bajo. Se recuerda que se valorará también el sigilo y el rastro que deje el alumno dentro de la red a infiltrarse. Por último, destacar que no existe un único método de resolución. Todos los métodos que cumplan los diferentes objetivos serán evaluados y aceptados. Si en algún momento el alumno se bloquea, podrá acceder a una pista por enunciado del ciberejercicio. ¡Suerte!

- Se ha detectado a un usuario con antecedentes penales visitando algunas páginas de actividad ilegal dentro de la *Deep Web*. Tras varias semanas llevando a cabo una investigación en secreto sobre este usuario, podemos confirmar que visita diariamente la web *www.tfg.dunquerque.cud.uvigo.es*. Al parecer, no es más que una ferretería online. ¿Podrías investigar esta página y confirmar alguna actividad maliciosa?

  - Pista: Investigar imágenes

- Muchas gracias por la información aportada. La confirmación de posibles actividades terroristas ha dado lugar a la autorización de un equipo del CNI a investigar en profundidad a nuestro sospechoso. Por lo que parece, han conseguido capturar una traza de tráfico de su equipo personal. ¿Podrías obtener algún resultado analizando la traza?

  - Pista: Credenciales de autenticación, usuarios, imágenes…

- Parece ser que las sospechas se confirman y se trata de una célula yihadista que se encuentra activa. La información que nos has ofrecido es muy valiosa, sin embargo parece que hemos levantado sospechas en el grupo terrorista y nos hemos visto obligados a detener nuestras acciones. ¿Podrías usar esta información para tener acceso a la red privada?

  - Pista: Accede y toma el control del servidor de la DMZ

- Nos han informado de que tienes acceso a uno de los servidores de la DMZ. ¡Fantástico! Sin embargo, no es suficiente. ¿Podrías acceder a la red LAN y obtener información crítica?

  - Pista: ¿Por qué no pruebas a acceder al firewall de la red?