Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE GRADO

Despliegue del gestor de contenidos WISE y análisis de vulnerabilidades

Grado en Ingeniería Mecánica

ALUMNO: Miguel López Garay

DIRECTORES: Belén Barragáns Martínez

Pablo Sendín Raña

CURSO ACADÉMICO: 2015-2016

Universidade Vigo

Centro Universitario de la Defensa
en la Escuela Naval Militar

TRABAJO FIN DE GRADO

Despliegue del gestor de contenidos WISE y análisis de vulnerabilidades

Grado en Ingeniería Mecánica

Intensificación en Tecnología Naval

Cuerpo General

Universidade Vigo

RESUMEN

A diario se producen miles de incursiones en sistemas informáticos y robos de información. Constantemente salen a la luz nuevas formas de ciberdelitos que ponen en peligro a infinidad de equipos y sistemas, en todo el mundo. Esta realidad, unida a la enorme expansión de las aplicaciones web y los gestores de contenidos, pone de manifiesto la necesidad de desarrollar e implantar las medidas oportunas en materia de ciberdefensa.

Los administradores y desarrolladores de aplicaciones deben concienciarse de la importancia que la ciberseguridad representa y emplear todas las herramientas disponibles para localizar posibles errores o fallos en los sistemas ya que las vulnerabilidades constituyen un factor crítico para cualquier organización. De este modo, el presente TFG se ha orientado al análisis de vulnerabilidades del gestor de contenidos WISE (*Web Information Services Environment*). En este documento se recoge una amplia recopilación gráfica de su instalación y configuración *Classic*, generando un entorno en el que se simule el uso académico que tendría en la Escuela Naval Militar.

A continuación, se emplean una serie de herramientas de análisis de vulnerabilidades, todas ellas de *software* libre. Estas herramientas permiten identificar los fallos de seguridad que presenta el sistema. Por último, se realizará un test de intrusión en WISE, analizando los fallos de seguridad presentes. Una vez finalizado este *pentesting* se analizarán los resultados obtenidos y se propondrán posibles soluciones para solventarlos.

ABSTRACT

Thousands of raids on computer systems and information thefts occur every day. Constantly, new forms of cybercrime that threat countless computers and systems worldwide come to light. This fact and the huge expansion of web applications and content management systems highlight the need to develop and to implement appropriate measures for

cyberdefense.

Administrators and application developers should be aware of the importance that cybersecurity represents. They must use all the tools available to locate possible code errors or system failures. Vulnerabilities represent a critical factor for any organization. Thus, this final degree project will analyze the vulnerabilities on the CMS WISE (Web Information Services Environment). This document provides a complete illustrated guide of both installation and WISE Classic configuration. An environment has been developed in order to simulate the academic use that WISE would have at the Naval Academy.

Several free vulnerability scanning tools have been used. These tools help to identify security flaws on the system. Finally, a pentesting into WISE has been run with the purpose of discovering the WISE security flaws. To conclude, the obtained results are analyzed and some possible solutions are proposed.

PALABRAS CLAVE

WISE, Gestor de Contenidos, CMS, Ciberdefensa, Vulnerabilidades, Web.

AGRADECIMIENTOS

Querría expresar mi más profundo agradecimiento a los directores de este proyecto por su consejo, disposición y dedicación durante el desarrollo de este trabajo.

Un ciberataque a gran escala puede hacer un daño sólo comparable con las armas nucleares. (Scott Borg, director de la U.S. Cyber Consequences Unit)

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1 INTRODUCCIÓN Y MOTIVACIÓN

1.1 Presentación

En las últimas décadas se ha producido un enorme proceso de informatización en todos los aspectos. Por ello, herramientas y técnicas que garanticen la ciberseguridad constituyen un factor fundamental para asegurar el éxito en las organizaciones. El gran desconocimiento general de los peligros que entraña la web se traduce, muchas veces, en el empleo incorrecto de las nuevas tecnologías, provocando una exposición innecesaria de los sistemas a posibles ciberataques. La concienciación en materia de seguridad y la adecuada formación, son imprescindibles para reducir el riesgo al que nos vemos expuestos.

Esta introducción resalta la importancia que ha alcanzado la seguridad de las aplicaciones web, realizando a continuación un análisis de los principales riesgos inherentes en el ciberespacio. A su vez, se presentan los objetivos que se persiguen con la realización de este trabajo de fin de grado y se indica la organización del presente documento.

1.2 Importancia de la seguridad informática

El siglo XXI se define por un gran número de autores como la revolución de las TIC (Tecnologías de la Información y Comunicación) [1], pues el número de datos procesados, almacenados y transmitidos es infinitamente mayor que en cualquier época anterior. El concepto de las TIC hace referencia al conjunto de avances tecnológicos que nos proporcionan la informática, las telecomunicaciones y las tecnologías audiovisuales; que hacen que los costes de producción y de comunicación sean cada vez menores.

Estos avances, unidos al rápido desarrollo de Internet y su penetración tanto a nivel personal como empresarial, han afectado directamente a la economía, política, educación y sociedad, convirtiéndolo en una herramienta crítica para las empresas, instituciones e individuos. El propio Bill Gates hacía referencia, en una entrevista personal, a este nuevo ciberespacio como: "Si tu negocio no está en Internet, no existe" [2].

La dependencia que la sociedad actual tiene de la tecnología y los sistemas de comunicación a través de Internet y aplicaciones web, trae como resultado una nueva visión de confort, inconcebible sin estos servicios indispensables para su funcionamiento y futuro. La red se ha convertido en una de las tecnologías más populares de la historia de la humanidad. Cada día aparecen nuevas aplicaciones que ofrecen productos y servicios novedosos, así como herramientas muy poderosas que facilitan una gran diversidad de gestiones personales o hacen posible la realización de compras y adquisiciones desde cualquier lugar del mundo.

Sin embargo, a pesar de las grandes posibilidades que presentan, acarrean un gran número de vulnerabilidades y amenazas a la seguridad. La seguridad de estas nuevas tecnologías pasa a ser un factor fundamental que condiciona su utilidad. El mundo no podría renunciar a los ordenadores, Internet y los teléfonos móviles. El proceso de informatización es irreversible y la única alternativa es crear un ciberentorno más seguro.

A diario se producen miles de incursiones en sistemas informáticos y robos de información. Constantemente se publican noticias en los medios de comunicación [3], sobre nuevas formas de ciberataques a ciudadanos, administraciones públicas, empresas e incluso a las instalaciones críticas de países como pueden ser centrales nucleares, plantas eléctricas o industrias.

Las garantías y la tranquilidad, que antes constituían los espacios, físicamente cerrados o aislados, desaparecen por completo. Los sistemas de información se convierten ahora en vulnerables y los contenidos sensibles o de interés que puedan almacenar se ven comprometidos. El número de posibles atacantes crece rápidamente y los medios empleados para su realización se desarrollan a la misma velocidad que los propios sistemas informáticos. Ambos sucesos, enlazados con la globalización de Internet, nos plantean un nuevo entorno de confrontación donde estas hostilidades pueden provenir de cualquier lugar del planeta. El concepto de privacidad o seguridad de las personas, las organizaciones o los estados, se ha visto modificada por estas nuevas actividades maliciosas.

Todo ello ha contribuido a la evolución del concepto de Seguridad Nacional y el desarrollo de una nueva Política de Seguridad, alterando incluso la estructura de las Fuerzas Armadas, que se topan ahora con la complicada tarea de adaptarse a una nueva modalidad de guerra, muy alejada de la convencional. A los tres ejércitos (Tierra, Armada y Aire) se le suma ahora el Mando Conjunto de Ciberdefensa (MCCD), o como algunos ya lo denominan, el Ciberejército. El MCCD está destinado a localizar vulnerabilidades y defenderse de una forma organizada, dirigida y legítima, de ataques, en muchas ocasiones invisibles, accesibles y con una autoría muy difícil de adjudicar. Se pretende garantizar de esta forma la confidencialidad, integridad y disponibilidad de los sistemas de comunicación del Estado, así como la seguridad en las redes, garantizando el cumplimiento de las misiones o servicios para los que fueron concebidos. Se hace frente de esta forma, a una nueva realidad: el ciberespacio y las amenazas que entraña.

El Mando Conjunto de Ciberdefensa constituye una declaración de intenciones de alto nivel, con el propósito de garantizar la seguridad de los sistemas de información y proporcionar las bases al Gobierno para definir y delimitar las responsabilidades para las diversas actuaciones técnicas y organizativas que requiere la defensa de los intereses individuales y colectivos, de la nación y sus ciudadanos. Para garantizar la seguridad en la red y evitar las agresiones, tanto internas como externas, es primordial el establecimiento de planes de contingencia, comprendidos por el conjunto de procedimientos, prácticas y tecnologías de protección a los servidores, usuarios y organizaciones que integran la web. Su violación repercute en grandes pérdidas económicas o de reputación para las compañías.

Todo ello genera la necesidad de emplear herramientas de seguridad eficaces. Estas herramientas tratan de garantizar la integridad, confidencialidad y disponibilidad de los tres elementos que constituyen cualquier sistema informático: *hardware*, *software* y sus datos.

1.3 Concepto de Ciberseguridad y Ciberdefensa

Desde el principio de los tiempos, el hombre ha combatido sobre el terreno. La historia muestra la evolución desarrollada en las técnicas y procedimientos empleados. Primero se incorporó la caballería, posteriormente las armas de fuego y la artillería, los vehículos blindados; y por último, las armas de destrucción masiva: químicas y nucleares.

El mar fue el segundo dominio de la guerra. Las primeras batallas se realizaban a bordo de pequeños botes a remo, que combatían al abordaje. A continuación se desarrolla la propulsión a vela que, desde la Edad Media, empleaba artillería naval. En el siglo XIX aparece la propulsión a vapor, que supone una enorme revolución. En el siglo XX, el submarino se convierte en un arma decisiva. Como consecuencia de ello, la táctica y la estrategia naval deben evolucionar continuamente para adaptarse a los nuevos retos que entraña la evolución de los medios y materiales empleados: los misiles, la aviación naval, las comunicaciones satélite y las tecnologías *stealth* o de reducción de RCS (*Radar Cross-Section*), entrañan algunos de los últimos progresos.

A principios del siglo XX, el aire pasa a ser objeto del interés militar gracias a la aparición del motor a reacción, los radares, los misiles y, últimamente, las aeronaves no tripuladas. También el espacio se convierte en un medio de estudio, pues las operaciones se sustentan en comunicaciones por satélite para la ejecución del mando y control, el apoyo a las unidades desplegadas y la obtención de inteligencia del adversario.

En el siglo XXI, el ciberespacio. El concepto de ciberespacio ha sufrido una transformación extremadamente rápida. Mientras que en el año 1984 pertenecía a la novela de ciencia ficción *Neuromante* de William Gibson [4]; en 2010 el Departamento de Defensa de los Estados Unidos lo convierte en el quinto dominio de la guerra. Como en los cuatro dominios anteriores, se puede combatir, y los intereses propios deben ser defendidos ante posibles hostilidades del enemigo. Pero, además, presenta unas características especiales. Se trata de un dominio prácticamente infinito, donde se emplean técnicas y armas que difieren a las empleadas en los campos de batalla tradicionales. Infinidad de grupos, organizaciones e incluso individuos aislados, tienen la capacidad causar enormes daños. A ello se suma un entorno legal muy complejo, donde la legislación de nuevas medidas, que castiguen actividades de este tipo, se realiza un paso por detrás de la evolución tecnológica. Este hecho favorece a los atacantes, que muchas veces se ven amparados por un vacío legal.

El detonante de este rápido aumento, tanto en su importancia como en la repercusión que alcanza el control del ciberespacio a la hora de garantizar la Seguridad Nacional, tiene su origen en el ataque sufrido por Estonia en abril del año 2007: el peor ataque cibernético ocurrido hasta el momento [5].

Tras un incidente diplomático, hackers rusos bloquearon los sistemas informáticos de las instituciones públicas. El país permaneció totalmente desconectado. Los bancos, ministerios y medios

de comunicación se vieron paralizados durante varios días. De la preocupación común, que este notable acontecimiento suscitó en las naciones, así como del propósito de prevenir la repetición de un ataque similar, nace el concepto de ciberdefensa.

La ciberdefensa consiste en el conjunto de acciones activas o pasivas, preventivas o de corrección, que garanticen el uso del ciberespacio y traten de negarlo al enemigo para la obtención de inteligencia. El JEMAD define la Ciberdefensa Militar como "el conjunto de recursos, actividades, tácticas, técnicas y procedimientos para preservar la seguridad de los sistemas de mando y control propios y la información que manejan, así como para permitir la explotación y respuesta sobre los sistemas adversarios, para garantizar el libre acceso al ciberespacio de interés militar y permitir el desarrollo eficaz de las operaciones militares y el uso eficiente de los recursos" [6].

Por su parte, la ciberseguridad se centra en las acciones de carácter preventivo que garanticen el uso de las redes propias, evitando la incursión de terceras personas. En general, una nación aislada no tiene la capacidad técnica para enfrentarse a ciberataques a gran escala. La OTAN y la Unión Europea se encuentran en pleno desarrollo de sus capacidades en materia de ciberdefensa. El propósito es la defensa por capas de la Organización y de los países constituyentes.

En enero de 2008 se aprobó la Política de Ciberdefensa de la OTAN [7], impulsando el desarrollo de los conceptos de ciberdefensa, la protección de las redes militares, la integración de ciberarmas para la defensa de sus intereses y la creación del Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN, en Tallin (Estonia).

Durante el año 2011, se hace pública una nueva política y un plan de acción informático; y la Unión Europea aprueba el "concepto de operaciones en red, en operaciones militares lideradas por la Unión Europea" [8]. En febrero de 2013 se redacta la primera Estrategia de Ciberseguridad [9]. Dicho documento representa la visión del conjunto de naciones de la Alianza sobre cómo prevenir y resolver mejor las perturbaciones de la red y los ciberataques. Todos estos sucesos hacen reflejo de las características que conciernen al ciberespacio y las medidas que se requieren para su control. Se comprende ahora su condición como un espacio mundial común. Desde esa perspectiva, surge la conciencia de necesidad de una respuesta internacional que se adapte a sus peculiaridades. Aunque se destinasen todos los recursos económicos, ninguna nación podría enfrentarse por sí sola a esta amenaza. Por esta razón, la cooperación internacional con gobiernos aliados y organizaciones de ámbito supranacional, es esencial.

En lo que respecta a política nacional, la Directiva de Defensa Nacional de 2012 [10] recoge la necesidad de reforzar los sistemas de obtención de información e inteligencia para el apoyo a las operaciones, así como los sistemas de mando y control para reducir el riesgo de ciberataques. Señala, además, la voluntad de impulsar una gestión integral de la ciberseguridad, así como la elaboración de una Estrategia de Seguridad Cibernética que reduzca su riesgo. Así, el 19 de febrero de 2013, el Ministro de Defensa español, Pedro Morenés, promulga la Orden Ministerial 10/2013 por la que se crea el Mando Conjunto de Ciberdefensa.

Ante este nuevo reto prioritario, comienzan a incrementarse los recursos económicos y de personal que se destinan a la causa, no sólo en el ámbito de Defensa, sino también en el mundo académico y civil. Algunas universidades nacionales contribuyen a la formación de nuevos expertos en la materia. Asimismo, múltiples compañías de seguridad informática irrumpen en este panorama ofreciendo sus servicios a las grandes empresas. *Cybersecurity 500* muestra un ranking, que actualiza cada tres meses, donde se reflejan las 500 mejores empresas internacionales dedicadas a esta disciplina. Destacan *Fireeye*, *Landcope*, *AlienVault* o *Norse*.

En España, *S21sec* es una de las compañías más conocidas. Además, destacan: *Ciberseguridad Profesional S.L*, *SCASSI Ciberseguridad SL*, *Eleven Paths* o *Hispasec*. Cabe destacar que, desde 1998 y de manera gratuita, *Hispasec* realiza una enorme labor de distribución de información sobre

seguridad informática, con el propósito de concienciar a la sociedad de los riesgos que se esconden en la web, a través de la iniciativa "una-al-día" [11].

Cada día se descubren en estos centros varias decenas de virus nuevos. En su mayoría son controlados y anulados en cuestión de minutos, dificultando enormemente la expansión de las amenazas. No obstante, mantener un nivel aceptable de seguridad en una empresa es responsabilidad de todos. Por este motivo, desarrollar una cultura de ciberseguridad e impartir cursos de formación para el personal constituye una tarea fundamental.

Igualmente, se debe definir e implantar una normativa que regule su uso, protegiendo así nuestra reputación online. Una buena concienciación y la aplicación de un reglamento, que restrinja y controle el uso de las redes, reducirá el número de accesos no autorizados a nuestra organización.

1.4 Sistemas de gestión de contenidos y seguridad en aplicaciones web

La web fue el motor que realmente impulsó el rápido desarrollo de Internet, así como su popularización en todo el mundo. En pocos años ha evolucionado de páginas sencillas con pocas imágenes y contenidos estáticos, a páginas dinámicas y complejas que emplean contenidos multimedia y permiten el intercambio de información entre un servidor y programas externos. Con el paso del tiempo han ido apareciendo diferentes arquitecturas, motivadas por la necesidad de corregir los problemas localizados, como: el uso ineficiente de recursos o la falta de seguridad en ciertas aplicaciones o ejecutables. Así en 2004 aparece la web 2.0, donde el concepto de la red toma un giro hacia una plataforma de contenidos, en la cual los enlaces se estructuran de forma ordenada en función de su popularidad. Este cambio en la web trae consigo la aparición de los gestores de contenidos, CMS (*Content Management System*).

1.4.1 Sistemas de gestión de contenidos (CMS)

CMS hace referencia a aplicaciones que permiten la creación y la fácil administración de contenidos orientados a páginas web. Los gestores de contenidos son aplicaciones en las que se permite la edición, creación y administración de contenidos que se muestran en un sitio web. La información publicada se almacena en una o varias bases de datos. Permiten realizar una separación entre el diseño propiamente dicho y los contenidos que en ellos se presentan. De esta manera, proporcionan un enorme ahorro en tiempo y esfuerzo a los administradores, en la instalación y el diseño de su propia aplicación, ya sea personal o corporativa.

En esta nueva era digital, los gestores de contenidos se emplean en infinidad de aplicaciones y su uso se ha extendido enormemente. La web ofrece una gran cantidad de recursos en los que se puede compartir cualquier tipo de información. Todo ello ha generado una nueva forma imperativa de dirigir un negocio, anunciarse y compartir la información. Incluso los gobiernos e instituciones incorporan sistemas CMS, como herramienta publicitaria y de difusión de su imagen corporativa, siendo necesario la contratación de expertos o la creación de departamentos o gabinetes de comunicación con dedicación exclusiva a estas herramientas.

Sin embargo, el rápido desarrollo de estos sistemas viene acompañado de nuevas formas de delitos o ataques. Estos ciberdelitos acarrean una relevancia fundamental en este entorno virtual, donde no se tiene certeza del lugar donde se almacenan nuestros datos o la seguridad bajo la que se ven amparados. A comienzos de este siglo, empiezan a aparecer nuevos ataques cuyo impacto ha ido creciendo de una forma sustancial.

1.4.2 Seguridad en aplicaciones web

El incremento exponencial en la actividad maliciosa que prospera en la web hace imprescindible el desarrollo de nuevas herramientas de seguridad, para administradores y usuarios. El primer reflejo de las nuevas amenazas es el *software* malicioso (*malware).* Dentro del término *malware*, se incluyen todos aquellos programas destinados a realizar una función dañina para el usuario y que principalmente suele ser:

- Mal funcionamiento del sistema.
- Robo de información sensible o confidencial.
- Borrado o modificación de datos.

El nacimiento de muchos de estos programas se produce dentro de un entorno universitario, donde algunos estudiantes, con el único afán de notoriedad y sin ánimo de lucro, desarrollaban programas, que podían considerarse "benignos" y que, en un principio, no iban más allá de una broma pesada. No obstante, su filosofía ha derivado hacia otra perspectiva y, actualmente, los ataques se dirigen contra el mundo industrial u objetivos estratégicos.

El número y tipo de virus crece continuamente. Ninguna marca escapa a su amenaza y los teléfonos móviles ya son uno de los mayores objetivos para los ciberdelincuentes [12]. La empresa de seguridad en la web *RiskIQ* afirma que el número de aplicaciones maliciosas se ha incrementado un 400% en *Google Play* [13]. Un estudio de 2014 revela que más de 16 millones de *smartphones* se encuentran infectados y el número de virus destinados a estos dispositivos se equipara al que afecta a los ordenadores [14].

Actualmente, los llamados *bulletproof hosting* ofrecen a sus clientes el *software* y los medios necesarios para efectuar actividades maliciosas. En estas páginas se permite la visualización de casi cualquier contenido y actividades ilegales (como juego o narcotráfico). La mayoría de estos portales se localizan en Rusia, China y países colindantes, aprovechando la ausencia de legislación en materia informática. Ryan Flores, experto en los nuevos métodos de ciberataques, apunta que las amenazas tienden a ser cada vez más locales [15], en muchas ocasiones, debido a la facilidad de obtención de medios necesarios. Se han registrado recientes manifestaciones de esta tendencia en ataques que afectan a objetivos muy particulares como pueden ser: la empresa en la que trabaja el supuesto ciberdelincuente o su banco. Los hackers implicados conocen los mecanismos de seguridad de sus víctimas, principalmente bancos, consiguiendo librar sus mecanismos de seguridad sin gran esfuerzo.

La empresa de seguridad *Trend Micro* [16] ha elaborado una lista en la que se muestran datos sorprendentes sobre los precios que se barajan en el mercado negro, por productos y servicios solicitados por piratas y ladrones de datos, y que les permiten cometer sus fechorías sin grandes conocimientos técnicos. Según la lista publicada, hackear una cuenta de *Facebook* ronda los 90 euros, bloquear un sitio web oscila entre los 15 y 440 euros, y el precio medio solicitado por el robo de los datos de una tarjeta de crédito es de 10 euros. Sin embargo, a pesar de indicar este precio en divisas europeas, el *Bitcoin* es la moneda virtual más utilizada para estas transacciones, por la dificultad que conlleva la identificación de los usuarios que la emplean.

Este mercado, más accesible de lo que podemos imaginar, es una viva imagen de la facilidad para adquirir cualquier tipo de producto destinado a la ciberdelincuencia. Se precisa solo una conexión a Internet y dinero disponible para este fin. El informe sobre amenazas de la empresa *McAfee* [17], publicado en mayo de 2015, ofrece pruebas contrastadas que demuestran este "cibertráfico negro". Lejos de la ficción o de una realidad muy alejada de nuestra rutina, el informe demuestra la evolución de esta nueva "puerta trasera" a la ciberdelincuencia. Como usuarios debemos estar concienciados de esta realidad y poner todos los medios a nuestra disposición, tratando de prevenir la posibilidad de que nuestra vida digital se vea afectada.

En la Figura 1-1 se muestran una tabla con los precios estimados que se solicitan para la sustracción de información bancaria en distintos países:

Número de tarjeta de pago con código CVV2	Estados Unidos	Reino Unido	Canadá	Australia	Unión Europea
Aleatorio	5-8 dólares	20-25 dólares	20-25 dólares	21-25 dólares	25-30 dólares
Con identificador bancario	15 dólares	25 dólares	25 dólares	25 dólares	30 dólares
Con fecha de nacimiento	15 dólares	30 dólares	30 dólares	30 dólares	35 dólares
Con Fullzinfo	30 dólares	35 dólares	40 dólares	40 dólares	45 dólares

Precios estimados por tarjeta, en dólares estadounidenses, por datos de tarjetas de pago robados (Visa, MasterCard, Amex, Discover)

Fuente: McAfee Labs

Figura 1-1 Precio del robo de información bancaria (tomado de [17])

Con el gran crecimiento en el uso de las aplicaciones web, debemos analizar y conocer las principales amenazas a las que nos enfrentamos cada vez que nos conectamos. De esta forma, nosotros mismos contribuiremos a generar un entorno más seguro.

1.5 Objetivos del TFG

El presente trabajo de fin de grado presenta los siguientes objetivos:

1- Realizar un análisis de los principales problemas de seguridad en la web.

Este TFG presenta las amenazas más frecuentes y comunes en la red. Especialmente se estudiarán las vulnerabilidades más extendidas en las aplicaciones CMS (*Content Management Systems*). Para ello, previamente se introduce el panorama actual en torno a los ataques informáticos y se muestra el cambio de rumbo en cuanto a estrategia en materia de ciberdefensa, introduciendo algunas de las organizaciones nacionales encargadas de garantizar la defensa de España en el ciberespacio. Estas instituciones suponen una medida de prevención y protección ante ataques a las libertades de sus ciudadanos y sus infraestructuras críticas.

2- Recoger una serie de herramientas susceptibles de emplear a la hora de analizar si una aplicación web en particular es o no sensible a este tipo de ataques.

Se presentan algunas de las herramientas más conocidas y empleadas por los profesionales en materia de seguridad informática. Estas herramientas, en su mayoría *software* libre, se destinan a la realización de auditorías para localizar y a corregir vulnerabilidades en sistemas y en aplicaciones web. La finalidad es familiarizarnos con dichas herramientas para su empleo sobre WISE.

3- Despliegue del gestor de contenidos WISE (*Web Information Services Enviroment*).

La primera parte del desarrollo del TFG se compondrá de la instalación y configuración del gestor de contenidos empleado en la Armada española: WISE. Se ilustrará el proceso de instalación y configuración *Classi*c llevado a cabo para la simulación del uso que del sistema WISE se haría en la Escuela Naval Militar. De esta forma, se pretende configurar un entorno académico en el que alumnos y profesores tengan acceso a contenidos didácticos y puedan compartir documentación para el estudio.

4- Análisis de seguridad WISE.

Para la identificación de las vulnerabilidades que presenta WISE se desarrolla una auditoría. El objetivo de la auditoría es aplicar alguna de las herramientas de seguridad informática más conocidas y localizar fallos de seguridad o errores en el gestor. Para su desarrollo desde un entorno controlado, se configurará un PC como servidor WISE en la red local del Centro Universitario de la Defensa.

Tras analizar e investigar sus vulnerabilidades, se pretende proponer soluciones de fácil aplicación, que pongan solución a los problemas encontrados. Finalmente, tras los resultados obtenidos, se presentarán posibles líneas de actuación o soluciones a implementar, con el objetivo de que los administradores de estas aplicaciones puedan garantizar la seguridad de la información que sobre el sistema WISE se presenta.

1.6 Organización de la memoria

Los objetivos descritos en el apartado anterior definen las líneas generales de los puntos a abordar en este TFG. A continuación se describe la organización del trabajo y el desglose de sus apartados.

En el primer capítulo se ha realizado una introducción que contextualiza el desarrollo del trabajo en una era de grandes avances tecnológicos y expansión del uso de las aplicaciones web. Se expone la situación actual en materia de ciberdefensa, en un momento de cambio internacional, en el que los estados comienzan a tomar medidas para la defensa ante las amenazas. El capítulo finaliza con una breve introducción a los gestores de contenidos y al incremento de las actividades maliciosas que se desarrollan en la web.

El capítulo 2 contextualiza la situación actual de la seguridad informática, reflejando la evolución y el rápido desarrollo de Internet. Se hace mención a las instituciones nacionales encargadas de la ciberseguridad en las redes y sistemas informáticos en España. Se aborda, de modo muy resumido, el panorama jurídico bajo el que se amparan los ciberdelincuentes. Se presentan los gestores de contenidos más empleados en la actualidad, analizando las propiedades que los caracterizan. Posteriormente se introduce el gestor de contenidos WISE como objeto de estudio para el desarrollo del trabajo. Y finalmente, se exponen los principales riesgos y amenazas que conlleva el uso extendido de las aplicaciones web, presentando algunas de las plataformas disponibles para la realización de análisis de vulnerabilidades y test de penetración o *pentesting*.

En el capítulo 3 se presentan de forma detallada los sucesivos pasos que componen el proceso de instalación y configuración *Classic*, para un completo despliegue del sistema WISE, realizado para el estudio. Asimismo, se presentan las posibilidades que ofrece, describiendo los diferentes objetos susceptibles de compartirse en el sistema. En el despliegue desarrollado se configura un portal web que simula el uso académico que de WISE se haría en la Escuela Naval Militar, seleccionando material didáctico destinado a los alumnos, así como impresos y solicitudes administrativas tanto para oficiales y profesores, como para la dotación de la ENM.

En el capítulo 4, se muestran la auditoría realizada sobre WISE, aplicando algunas de las distintas herramientas de *software* libre presentadas en el segundo capítulo. De esta forma, se detallan los pasos más comunes en la realización de un test de intrusión. En primer lugar, se realiza un escaneo de puertos y análisis de metadatos con el objetivo de obtener toda la información necesaria para realizar el ataque. Posteriormente se emplearán herramienta de análisis de vulnerabilidades. Conocidas los fallos de vulnerabilidad se intenta explotarlos y, tras una serie de ataques, se obtiene las credenciales del usuario administrador y se realiza un ataque DoS, imposibilitando el acceso al servidor a los usuarios legítimos.

En el capítulo 5 se analizan los resultados obtenidos y se exponen las limitaciones que presenta el gestor, haciendo una valoración del uso que en la Armada se le otorga y proponiendo posibles soluciones ante los problemas localizados. Finalmente, en el capítulo 6, tras el desarrollo del estudio, se presentan las conclusiones finales. Además, se definen unas líneas futuras que sirvan de guía para futuros estudios del gestor.

2 ESTADO DEL ARTE

2.1 Presentación

A lo largo del presente capítulo se detalla la historia y evolución de lo que hoy conocemos como Internet y se describen los diferentes organismos y centros nacionales que integran la Defensa Nacional y combaten contra la ciberdelincuencia. A continuación, se analizan los principales CMS y se introduce el gestor de contenidos WISE, empleado en el desarrollo del presente TFG como objeto de estudio para el análisis de vulnerabilidades, por su uso extendido en el ámbito de la Armada.

Posteriormente, se presentan los ataques principales que afectan a las aplicaciones web y, finalmente, se expondrán los diferentes medios existentes para la realización de auditorías en aplicaciones web, mostrando algunas de las plataformas más populares, en su mayoría de *software* libre. Estas plataformas de análisis son empleadas en infinidad de organizaciones, para localizar fallos de diseño o vulnerabilidades en sus portales y garantizar un entorno seguro, evitando en la manera de lo posible, que los ataques recalen en los sistemas.

2.2 Evolución de la red

El inicio de lo que hoy se conoce como Internet se remonta a la década de los 60. Durante el transcurso de la guerra fría, el Departamento de Defensa de los Estados Unidos crea una red de uso exclusivamente militar, que garantizase el acceso a la información y sirviese como sistema de mensajería para coordinación, mando y control de las unidades, en caso de un hipotético ataque por parte de Rusia a los sistemas de telecomunicaciones tradicionales. Esta red se llamó Arpanet (1969) y constituía la primera red de comunicaciones descentralizada, formada por cuatro nodos independientes que enlazaban cuatro universidades: la Universidad de California de Los Angeles (UCLA), la Universidad de California de Santa Bárbara (UCSB), la Universidad de Utah y el *Stanford Research Institute* (SRI).

A pesar de su origen como sistema de comunicaciones militares, su evolución se desarrolló en el mundo académico, donde Arpanet se empleó para conectar a científicos de estas distintas universidades, los cuales compartían opiniones y conocimientos para desarrollarla. En 1971 ya disponía de quince nodos y en el año 1973, Arpanet se internacionalizó con la incorporación de las universidades *College of London* (Gran Bretaña) y *Norsar* (Noruega). En el año 1982 los científicos Vinton G. Cerf y Robert Kahn propusieron el protocolo TCP/IP como el protocolo estándar para el funcionamiento de Internet. La red continuó en expansión y en 1983 el Ministerio de Defensa estadounidense decide desvincularse de Arpanet, creando una red independiente: MILNET [18].

Aparecen también las primeras computadoras personales, destinadas en un primer momento a facilitar cálculos y operaciones en el trabajo, sin conexión a la red. Es a mediados de los ochenta cuando aparecen los primeros sistemas operativos que permitían la interconexión. A pesar de este desarrollo exponencial, hasta la década de los noventa y la incorporación del protocolo HTML (*Hyper Text Markup Language*), lenguaje de programación para la creación de páginas web, Internet no pasó a ser un medio de comunicación popular. Así, en 1994 y tras el levantamiento de la prohibición del comercio en la red, Internet encontró una nueva oportunidad, dejando de ser un medio destinado a la transmisión de información y mensajería electrónica, poco utilizado. Durante este año, sucedieron varios sucesos importantes para la popularización y el desarrollo de la web tal y como la entendemos hoy en día:

- Los estudiantes de la universidad de Stanford, David Filo y Jarry Jang, crean el buscador Yahoo! [19], que en menos de tres años se valoraba en más de tres millones de dólares.

- El restaurante de comida rápida de California Pizza Hut, se convierte en la empresa pionera en la realización de pedidos de comida a domicilio online, dándose a conocer como Pizza Net [20]. La idea causó tal furor y tuvo tal repercusión, que la compañía llegó a ocupar la portada de un periódico nacional. Se abre así una nueva forma de comercio a nivel global, llegando hoy en día, a ser fundamental para el desarrollo de cualquier empresa.

El uso de la red aumentaba a pasos agigantados y comienzan a aparecer numerosas empresas pioneras en el sector que apostaron por esta nueva forma de negocio. El uso del correo electrónico se extiende y la empresa *Amazon* se coloca como referente en un nuevo entorno de ventas. Poco después aparece la empresa *Google*, alzándose como principal buscador de Internet. La novedad que incorporaba *Google* radicaba en el empleo de una nueva tecnología, que clasifica las páginas web en función de su importancia (*PageRank*) [21]. Hoy en día se ha convertido en una de las empresas más grandes del mundo, con unos ingresos de más de 50 billones de dólares anuales [22] y alrededor de 3 billones de búsquedas diarias.

En 2004 aparece *Facebook*, revolucionando el mundo de las redes sociales. Comienzan desde entonces a aparecer un gran número de aplicaciones que llevan a la web a convertirse en el medio de comunicación más usado. En 2005 surge *Youtube*. Lo que comenzó como una sencilla plataforma para la compartición de vídeos, hoy ofrece millones de videos al día, permite el alquiler de películas y

series, y es empleado por muchos artistas para darse a conocer. Continuando con esta rápida evolución, en 2007 sale al mercado el primer *smartphone* de Apple: el Iphone.

Estas nuevas aplicaciones web, y la tecnología que junto a ellas se extiende, tienen un impacto directo sobre la forma de dirigir un negocio, la transmisión de información y la vida de las personas. En resumen, los desarrolladores de aplicaciones web de hoy y el aumento exponencial del uso de los sistemas de gestión de contenidos, está dando forma al futuro digital.

2.3 Ciberdefensa: organismos nacionales

Debemos remarcar que no todo lo que proporcionan las nuevas herramientas web son ventajas. El aumento de los ciberdelitos que acompañan a las aplicaciones y a la extensión del comercio en la red, supone un nuevo reto al que hacer frente. Según un estudio emitido por *Deloitte* [23], durante el año 2015, el aumento de los robos de información se ha incrementado en un 13%. De la misma forma, se muestra un incremento en la preocupación de los usuarios por los temas relacionados con la seguridad web. Existe un cambio general en la actitud de los consumidores, concienciándose en la necesidad de tomar acciones individuales para la protección de sus datos online.

Las amenazas de este entorno afectan también a los estados y sus actividades. Transporte, comunicaciones, industria energética, medios de comunicación social, y hasta el deporte y el ocio, pueden verse afectados. Los planes estratégicos para la ciberdefensa, en los que se establezcan las medidas para la detección y la respuesta ante los ataques, suponen el punto de partida para reducir el impacto y limitar los daños que, sobre una nación, pueden ocasionar.

En la Figura 2-1 se muestra una pirámide de las ciberamenazas más comunes, que afectan a cualquier sistema informático, así como a las aplicaciones web. En el primer escalón se localizan los *Script Kiddies*, que hace alusión a individuos que emplean herramientas básicas y que carecen de conocimientos técnicos necesarios para el desarrollo de sus propios productos [24]. Estos individuos son capaces de realizar acciones simples como el robo o *hackeo* de contraseñas.

Figura 2-1 Pirámide tipos de ataques vs capacidades (tomada de [25])

En el siguiente nivel encontramos los *Black Hat Pro*. Estos ciberdelincuentes disponen de conocimientos suficientes para realizar modificaciones de productos existentes y realizar acciones más complejas como ingeniería social, *phising* o *pharming*, para su beneficio personal. (Ver Anexo II para más información).

Ya alcanzando la parte alta de la pirámide, encontramos a los grupos organizados. Estos colectivos se encuadran dentro del crimen organizado y el hacktivismo [26]. El hacktivismo combina el activismo político con el hacking online. Éste es un nuevo movimiento masivo que, en muchas ocasiones, hace

referencia a ideales de libertades individuales, de expresión e información. Dentro de los ataques que estos individuos realizan destacan: DoS (*Denial of Service*), *hijacking* (robo de información) o *defacement* (deformación o cambio intencionado de una página web). Hoy en día, existen diferentes variantes del hacktivismo:

- **Anonymous:** Es el componente público más popular. Sus miembros defienden la independencia de Internet y se oponen a la censura o las barreras existentes al flujo de información. En algunas ocasiones, realizan acciones de robo y distribución de información personal y/o confidencial, reivindicando el control que los gobiernos ejercen sobre la información. Actualmente han declarado la guerra informática a las plataformas de propaganda yihadista, como respuesta a los últimos atentados en occidente.
- Los verdaderos activistas son los llamados **Ciberocupas**. Estos utilizan las redes sociales para difundir propaganda e información. Cometen actos delictivos para defender sus ideales, reforzar la democracia y luchar contra la corrupción, mediante el robo y la publicación de la información sustraída.
- Por último, los **ciberguerreros**, se autodefinen como patriotas, agrupándose en "ciberejércitos". Normalmente dicen actuar en nombre de sus naciones y prestan su apoyo a movimientos extremistas. Mediante el uso de ataques de DDoS (*Distributed Denial of Service*), se ocupan de silenciar a los opositores.

La Figura 2-2 representa la evolución desarrollada por el hacktivismo en los últimos años:

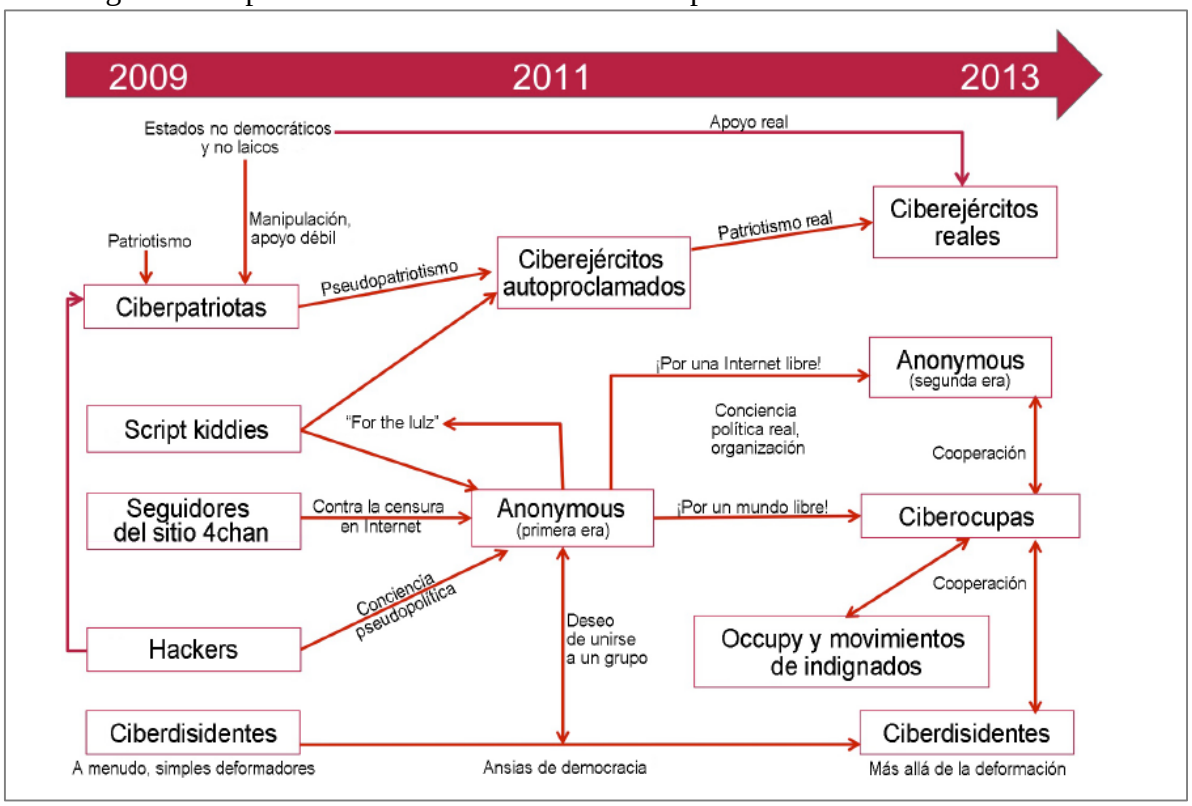

Figura 2-2 Evolución del ciberactivismo (tomada de [27])

La cima de la pirámide, ilustrada en la Figura 2-1, está ocupada por las agencias gubernamentales y las APT´s (*Advanced Persistent Threats*) [28]. Estas agencias cuentan con importantes recursos materiales, humanos y económicos. Son capaces de desarrollar armas informáticas y causar ataques con consecuencias devastadoras, con un alto grado de anonimato.

Para nuestra defensa, la Administración española cuenta con:

- El **Consejo Nacional de Ciberseguridad**. Elabora la Política de ciberseguridad.

- El **Centro Nacional de Excelencia en Ciberseguridad (CNEC)**. Coordina la ciberseguridad Nacional.
- El **Instituto Nacional de Ciberseguridad** (**INCIBE**). Responde ante incidentes de ciberseguridad y realiza labores de investigación, seguimiento y estudio de los riesgos emergentes.
- Las **Fuerzas y Cuerpos de Seguridad de Estado**. Investigan y hacen frente a las nuevas formas de ciberdelincuencia.
- Las Fuerzas Armadas Españolas con el **Mando Conjunto de Ciberdefensa** (**MCCD**). Planea y ejecuta las acciones relativas a la ciberdefensa militar y protege al ciberespacio de amenazas y agresiones que afecten a la Seguridad Nacional.

2.3.1 Consejo Nacional de Ciberseguridad

El Consejo Nacional de Ciberseguridad se crea el 5 de diciembre de 2013 [29], tras el acuerdo del Consejo de Seguridad Nacional. Entre sus funciones se encuentran [30]:

- El análisis, estudio y propuesta de iniciativas relacionadas con el ámbito de la seguridad informática.
- Elaboración de normativas de ciberseguridad.
- Verificar el grado de cumplimiento de la Estrategia de Seguridad Nacional y promover e impulsar sus revisiones.
- Analizar los riesgos y amenazas, así como los posibles escenarios de crisis.
- Mantener, elaborar planes de respuesta y formular las directrices para la realización de ejercicios de gestión de crisis, analizando los resultados obtenidos.
- Contribuir a la disponibilidad de los recursos existentes y al mantenimiento de las Administraciones Públicas.
- Facilitar la coordinación con los órganos y autoridades competentes cuando las situaciones que afecten a la ciberseguridad lo precisen.

Como se muestra en la Figura 2-3, tiene una coordinación directa con Presidencia de Gobierno, el Centro Nacional de Inteligencia y los distintos ministerios:

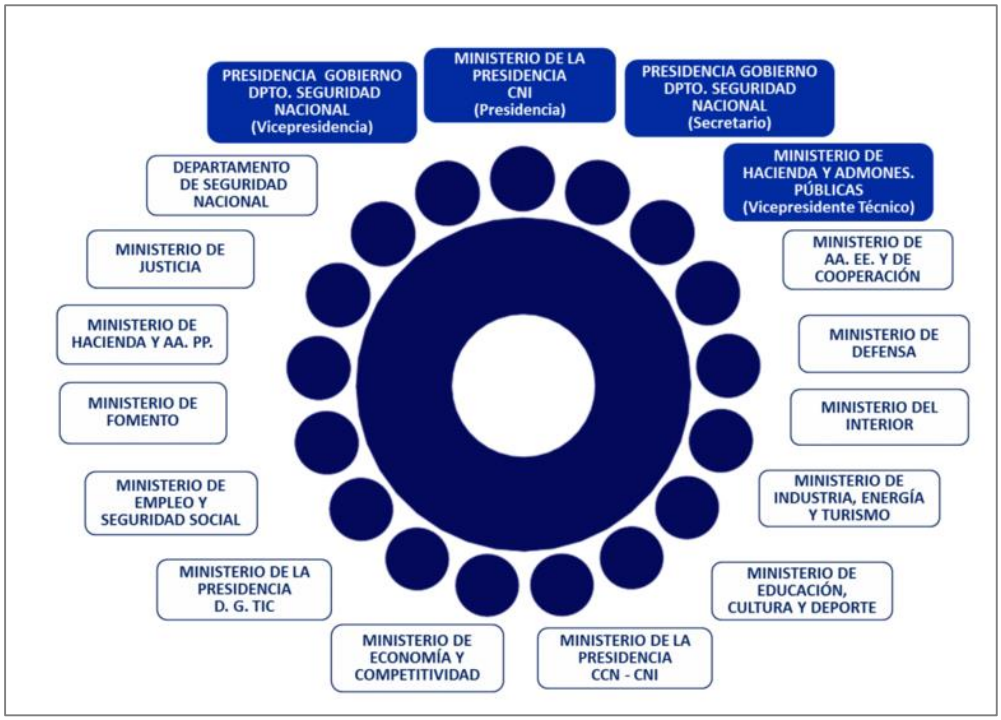

Figura 2-3 Composición del Consejo Nacional de Ciberseguridad

2.3.2 Centro Nacional de Excelencia en Ciberseguridad

El Centro Nacional de Excelencia en Ciberseguridad (CNEC) responde al proyecto europeo para la creación de centros de ciberseguridad nacionales. Colabora estrechamente con los Cuerpos y Fuerzas de Seguridad del Estado, la universidad y el mundo empresarial.

El Centro se encuadra dentro de la estructura del Instituto de Ciencias Forenses y de Seguridad y focaliza sus esfuerzos a la formación, entrenamientos, investigación y desarrollo tecnológico en materia de ciberseguridad. Su objetivo principal es el desarrollo de los medios eficientes para combatir el cibercrimen. En la actualidad destina parte de sus recursos a la localización de nuevos talentos que deseen formarse en esta doctrina.

2.3.3 Instituto Nacional de Ciberseguridad (INCIBE)

El Instituto Nacional de Tecnologías de la Comunicación pasa a llamarse Instituto Nacional de Ciberseguridad de España (INCIBE), el 27 de octubre de 2014 [31].

INCIBE colabora en la construcción de la ciberseguridad nacional. Su actividad se centra en garantizar el uso seguro de las tecnologías de la información. A su vez, realiza labores de formación, concienciación en seguridad en la red y análisis de herramientas de seguridad. Además, organiza y participa en iniciativas para mejorar el escenario de la ciberseguridad, con el fin de enriquecer el marco de colaboración de todos los agentes implicados en esta materia.

2.3.4 Mando Conjunto de Ciberdefensa (MCCD)

Mientras que en los otros dominios de la guerra la mayor parte del armamento está en posesión de los ejércitos, para combatir en el ciberespacio, no hay ninguna herramienta técnica específica del ámbito militar, sino que se encuentran accesibles a múltiples actores, con un enorme abanico de motivaciones e intereses, todos ellos, capaces de producir daños.

Con el fin de ejercer la acción militar en el ciberespacio, se creó el Mando Conjunto de Ciberdefensa (MCCD) que desde 2013, opera en este ámbito tan complicado. Su ámbito primario de actuación son las redes de mando y control para las operaciones. No obstante, puede actuar en la defensa de otras redes o sistemas que se le encomienden. En determinadas circunstancias está autorizado a responder ante ciertos tipos de ataques que afectan a la Seguridad Nacional.

Las medidas de protección de los sistemas que están bajo su seguridad se estructuran en capas. En un primer lugar, se encuadran las medidas preventivas. Éstas incluyen control de acceso, control de información, análisis de vulnerabilidades, redacción de nuevas normativas y procedimientos, así como el desarrollo de actividades de concienciación y adiestramiento del personal. Ya enfocadas a detectar las amenazas y su corrección de manera temprana, se encuentran las medidas proactivas. Para ello, el centro dispone de equipos para la monitorización de eventos, equipos de inspección y auditorías que realizan tests de penetración. En el tercer escalón se encuentran las medidas reactivas, dirigidas a minimizar los efectos de los ataques que a diario sufre España, así como a investigar las causas que los motivan. Para ello disponen de equipos de análisis forense, restauración de sistemas y el conjunto de acciones legales, en caso de ser necesarias.

En sus centros de formación asociados, se realizan cursos de seguridad en: *malware*, redes inalámbricas, hacking ético, ingeniería social, criptografía, ciberderecho, bases de datos seguras, APT´s, diseño de ciberarmas, arquitecturas seguras, *big data*, *honeynets*, etc. Además, el MCCD participa en ejercicios de carácter internacional.

De la misma forma, todas las naciones de nuestro entorno se han concienciado y están desarrollando iniciativas y planes, tratando de hacer frente a estas amenazas emergentes. Gran parte de

ellas se basan en fortalecer la capacidad técnica y coordinarla, interviniendo en forma de respuesta y sólo en caso de que la amenaza ya se haya materializado.

Pero, la seguridad no es gratuita y es vital también el presupuesto que se le dedique. En un mundo con un carácter evolutivo tan volátil, las naciones deben actualizarse de manera continua si se pretende alcanzar una capacidad técnica competente, capaz de hacer frente a las amenazas emergentes y más exigentes.

Actualmente, el MCCD cuenta con unas 70 personas, civiles y militares, y se ubica en Pozuelo de Alarcón (Madrid). Sus cometidos actuales son [32]:

- El desarrollo de los medios y procedimientos necesarios que garanticen el acceso libre a la red.
- Garantizar la disponibilidad, integridad y confidencialidad de la información.
- Garantizar el funcionamiento de los servicios críticos.
- Analizar y obtener información sobre ciberataques e incidentes en la web.
- Ejecutar una respuesta legítima, oportuna y proporcionada ante cualquier agresión que afecte a la Seguridad Nacional.
- Dirigir y coordinar la actividad de los centros de respuesta a incidentes de seguridad de la información de los Ejércitos y Armada, y el de operaciones de seguridad de la información del Ministerio de Defensa.
- Cooperar, en materia de ciberdefensa, con los centros nacionales de respuesta, ante incidentes de seguridad de la información.
- Definir, dirigir y coordinar la concienciación, la formación y el adiestramiento especializado en materia de ciberdefensa.

2.4 Nueva normativa en seguridad de la información

Los nuevos ciberdelitos evidencian la necesidad de una nueva legislación. Su rápido desarrollo dificulta la aplicación de un código penal acorde con esta realidad. Todavía, en muchas ocasiones, las sanciones impuestas quedan solo a criterio del juez designado para el caso. Esto, sin duda, favorece a los ciberdelincuentes que, aprovechando estos vacíos legales, no ven consecuencias tras sus actos. En el Anexo I del presente documento se recogen los artículos del Código Penal, que regulan actualmente en España los sistemas informáticos y su uso.

No obstante, el 1 de julio de 2015 entró en vigor la Ley Orgánica 1/2015. Esta ley supone una reforma en el Código Penal, que intenta ofrecer una respuesta más adecuada a las nuevas formas de ciberdelincuencia.

Con el mismo objeto, el Parlamento Europeo, tras largas negociaciones y el análisis de distintas propuestas, alcanzó un acuerdo a finales de 2015 con dos propuestas legislativas. Previsiblemente entrarán en vigor durante el presente año y serán de obligada aplicación por todos los estados de la Unión a partir de 2018 [33].

La primera propuesta consiste en la elaboración de un reglamento relativo a la protección de los datos personales y a su circulación en la red. El Reglamento General de Protección de Datos regulará el tratamiento de los datos personales con el objetivo de defender a las personas físicas. Se recogerá una lista de infracciones penales e imposición de sanciones con carácter correctivas. Además, el tratamiento de los datos personales se verá regido por una normativa común, en la Unión Europea.

Además, las empresas con sede en territorio europeo o cualquier compañía que ofrezca sus servicios a sus ciudadanos, deberán adaptarse al nuevo reglamento. Algunos de los puntos que se verán regulados son:

- **Seguridad de los datos:** Se establece como obligatoria la aplicación de medidas para la defensa de los riesgos que afectan a la información que se encuentra disponible en Internet.

- **Brechas de seguridad:** En un máximo de 72 horas desde su conocimiento, se deberá comunicar a la autoridad correspondiente la violación de cualquier dato de carácter personal. El comunicado hará mención a la naturaleza y número de los datos afectados, a la identidad de los afectados, y las medidas propuestas o en marcha para su solución.
- **Evaluación de la privacidad:** Se deberá detallar el tratamiento previsto de la información privada, evaluar las operaciones en las que dicha información se emplee y se evidenciarán las garantías que la protejan.

En referencia a las sanciones previstas en lo expuesto anteriormente, la potestad sancionadora residirá sobre los estados y, en caso de transposición de delitos entre autoridades, se deberá llevar a cabo en un período inferior a dos años.

En materia de ciberdefensa, la nueva política aclara que, ante un ataque digital contra un estado miembro, se puede efectuar una respuesta, respaldada en el artículo 5 del Tratado Atlántico, la cláusula para la defensa colectiva. En el caso de este supuesto ataque, se consideraría la apertura de hostilidades contra el conjunto de la OTAN y se podría actuar de manera legítima, empleando las medidas necesarias que garanticen la seguridad, incluyendo el uso de las FAS. Estas medidas finalizarían una vez que se haya restablecido la paz y el control del ciberentorno afectado.

Estos acontecimientos son un pequeño intento por paliar la problemática legal de esta realidad virtual. Las leyes y su legislación deberán alcanzar en los próximos años el dinamismo suficiente, para igualar a la constante evolución tecnológica y ejercer una clara clasificación de los actos que en la red se desarrollan. A su vez, las nuevas medidas se deben encaminar hacia el robustecimiento de los controles informáticos en materia de seguridad, de manera que se prevengan los delitos.

2.5 Revisión de los gestores de contenidos. Introducción a WISE

Los gestores de contenidos se utilizan en multitud de aplicaciones en la web y abarcan un amplio conjunto de entornos, con diferentes usos y objetivos. Facilitan la creación y la administración de infinidad de sitios en la red y hacen posible que, cualquier persona, sin la necesidad de tener conocimientos en programación, pueda desarrollar un sitio web. Debido a la facilidad que presentan, se suelen emplear en aquellos portales que necesitan una constante actualización. Estos pueden ser periódicos, tiendas virtuales o portales de noticias. Los más utilizados actualmente suponen una base importante para la realización de estrategias de *marketing* de muchas empresas. La característica que ha hecho tan populares a los CMS (*Content Management System*) es la facilidad que presentan para su manejo, actualización y mantenimiento. De todas formas, cada gestor de contenidos presenta una serie de peculiaridades que lo diferencia de los demás.

Los CMS se dividen de dos partes. La primera de ellas en la parte pública, es decir, la web tal y como se encuentra accesible a cualquier usuario que acceda a la URL o la dirección del gestor. La segunda parte se conoce como la parte privada y es aquella a la que solamente pueden acceder las personas registradas, mediante su usuario y contraseña. En esta parte se realiza la edición y administración del sistema. Para ello, los distintos tipos de gestores disponen un panel de herramientas que permiten la modificación y personalización del entorno, permitiendo realizar los cambios deseados de manera sencilla y clara (véase Figura 2-4).

Figura 2-4 Funcionamiento de un gestor de contenidos (tomada de [34])

Debido al número y a los distintos grupos de usuarios que acceden a estos gestores, normalmente, se otorgan distintos roles a cada uno de ellos. Dentro de estos roles se encuentran los permisos de administración, modificación, edición o simplemente, lectura y visualización de contenidos.

A nivel de arquitectura, los gestores de contenidos se estructuran en tres capas, tal y como se ilustra en la Figura 2-5:

- **Capa de datos:** La capa o base de datos es el repositorio en el que se almacena la información publicada en el CMS. Además de almacenar la información, la capa de datos permite el acceso a los recursos.
- **Capa de aplicación:** En esta capa intermedia se procesan las peticiones del usuario y se envían las respuestas tras el proceso. Se denomina capa lógica y supone el canal de comunicación entre el usuario y la base de datos en la que se almacena la información.
- **Capa de presentación:** Esta capa es la que ve el usuario que accede al sistema. Es conocida como la interfaz gráfica y suele ser amigable. En ella se muestra la información estructurada.

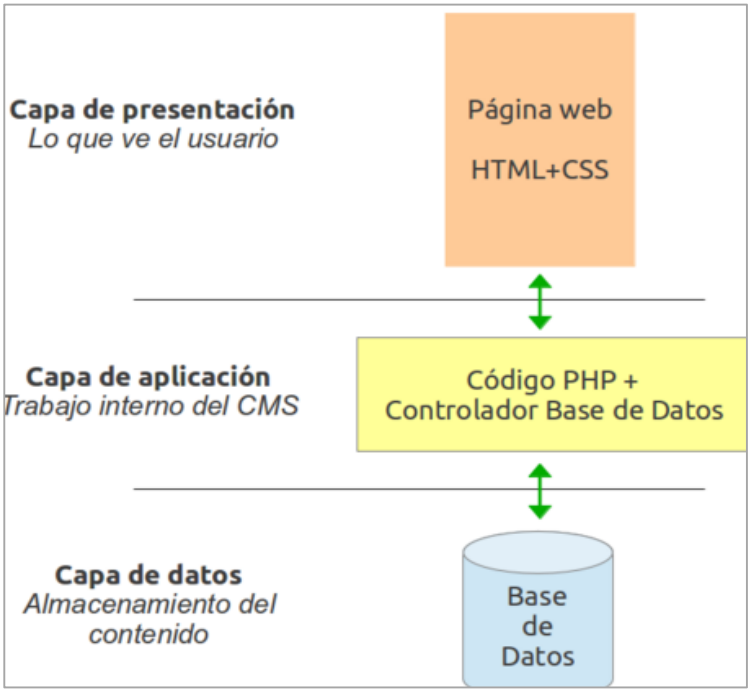

Figura 2-5 Arquitectura de un CMS (tomada de [35])

2.5.1 *WordPress*

WordPress [36] es sin duda el gestor de contenidos más empleado (al final de esta sección se representan los datos de uso). Este CMS permite la creación de una gran variedad de entornos y su enorme popularidad se debe, principalmente, a su facilidad de administración, sus funciones y actualizaciones. Ha sido desarrollado en lenguaje PHP para entornos que trabajen sobre bases de datos *MySQL* y el servidor web Apache. Permite múltiples funciones y destaca por su facilidad de empleo, actualización y personalización. Existen diversas empresas dedicadas a su programación y desarrollo. Estas empresas desarrollan constantemente *plugins* que mejoran sus funciones o plantillas para facilitar su manipulación.

Se calcula que alrededor del 70% de los sitios web basados en gestores de contenidos emplean *WordPress* [37]. El conocido servicio público de prensa BBC emplea este CMS para la distribución de contenidos multimedia en Estados Unidos (Figura 2-6).

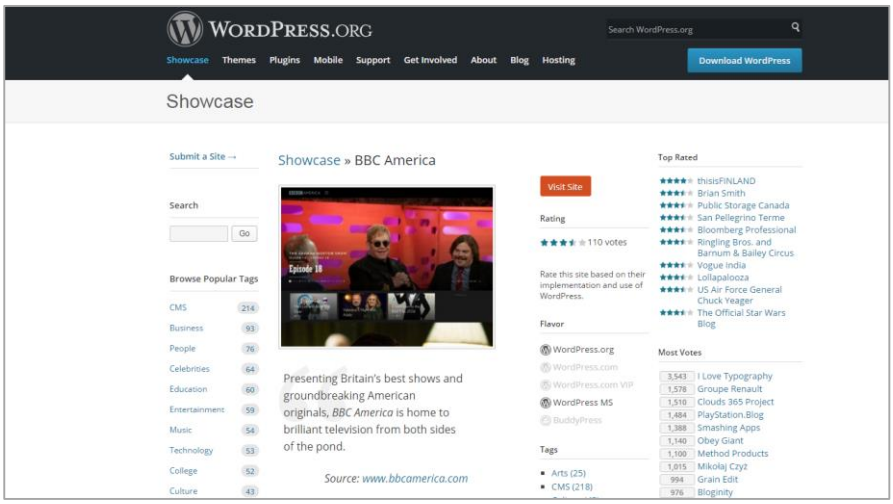

Figura 2-6 Portal web de la BBC America, desarrollado en *WordPress* (tomada de [38])

Entre sus características destacan:

- Lenguaje: **PHP**.
- Flexibilidad para implementar funcionalidades personalizadas: **Alta.**
- Dificultad de administración: **Baja.**
- Dificultad y problemática de actualización: **Baja.**
- Documentación de apoyo: **Excelente.**

2.5.2 Joomla!

Joomla! [39] es el segundo gestor más empleado. Este gestor de contenidos se caracteriza, principalmente, por presentar una versión optimizada para dispositivos móviles, permitir la gestión de *Banners* para la publicación de anuncios sobre el gestor o la avanzada gestión de permisos y roles. A pesar de ser un sistema sencillo, su aprendizaje requiere más tiempo que en *WordPress.* Como características, destacamos:

- Lenguaje: **PHP**.
- Flexibilidad para implementar funcionalidades personalizadas: **Baja.**
- Dificultad de administración: **Media.**
- Dificultad y problemática de actualización: **Alta.**
- Documentación de apoyo: **Buena.**

Figura 2-7 Portal web de la Torre Eiffel, desarrollado en *Joomla!* (tomada de [40])

En la Figura 2-7 se ilustra la página de la Torre Eiffel, que emplea este gestor de contenidos para publicar información turística como horarios, precios, mapas, itinerarios, etc.

2.5.3 Drupal

En tercer lugar en cuanto a su uso, se encuentra el gestor de contenidos *Drupal* [41]. Este CMS se basa en un sistema modular con una arquitectura muy consistente. Permite implementar una gran variedad de sitios web como son: blogs personales o profesionales, un portal corporativo, tiendas online, redes sociales, foros, etc.

Este CMS presenta una mayor dificultad para nuevos administradores. Sin embargo, tras la familiarización con el sistema, presenta una enorme ventaja sobre los sistemas anteriormente expuestos. Esto se debe a que *Drupal* soporta una mayor cantidad de visitas, permite una alta personalización, posee una gran comunidad de desarrolladores y un buen nivel de seguridad. No obstante, esta seguridad depende del administrador, que deberá configurar adecuadamente el sistema.

- Lenguaje: **PHP**.
- Flexibilidad para implementar funcionalidades personalizadas: **Muy Alta.**
- Dificultad de administración: **Alta.**
- Dificultad y problemática de actualización: **Alta.**
- Documentación de apoyo: **Bastante.**

En la Figura 2-8 se representa el gestor de contenidos *Drupal*, que emplea de la Casa Blanca [42].

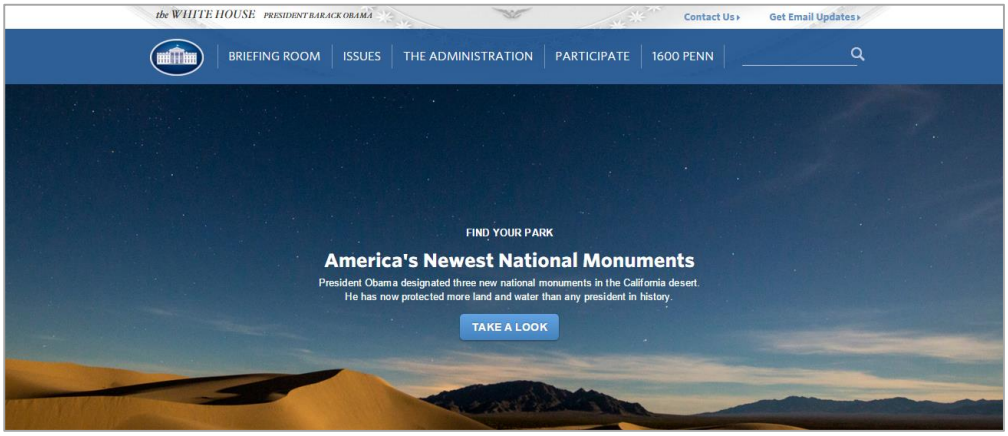

Figura 2-8 Portal web de la Casa Blanca, desarrollado con *Drupal*

2.5.4 Moodle

Moodle [43] es otro ejemplo de CMS. Este gestor de contenidos se emplea principalmente en el ámbito de la enseñanza, como medio para la distribución de material educativo.

Este sistema permite establecer conversaciones privadas entre estudiantes así como foros de debate en el que los profesores plantean una serie de preguntas con el objetivo de que los estudiantes las respondan. De esta forma, permite crear un *feedback* entre alumnos y profesores, de manera que se fomente el aprendizaje de manera amena e iterativa.

La aplicación permite crear distintos usuarios con diferentes roles de configuración o visualización de contenidos. Entre sus características, destacamos:

- Lenguaje: **PHP**.
- Flexibilidad para implementar funcionalidades personalizadas: **Media.**
- Dificultad de administración: **Baja.**
- Dificultad y problemática de actualización: **Media.**
- Documentación de apoyo: **Bastante.**

2.5.5 Magento

Magento [44] constituye una variante más de estos sistemas. Se destina principalmente a páginas web orientadas a la venta online.

Su uso se basa en las características básicas de todo CMS: la facilidad de configuración y personalización. Entre sus propiedades destacan: permite la creación de inventarios y controles de *stock*, permite múltiples formas de pago y envío, pone a uso de los administradores herramientas de *marketing* (productos sugeridos, ventas cruzadas, cupones de descuento), etc.

Trabaja sobre *Zend Framework* para asegurar que el código base sea escalable y seguro. Como características, presenta:

- Lenguaje: **PHP**.
- Flexibilidad para implementar funcionalidades personalizadas: **Alta.**
- Dificultad de administración: **Media.**
- Dificultad y problemática de actualización: **Baja.**
- Documentación de apoyo: **Bastante.**

2.5.6 PrestaShop

PrestaShop [45] constituye otro ejemplo más de sistema CMS dedicado al comercio electrónico. Basado en el lenguaje de programación PHP, supone una variante ante *Magento.* Incluye más de 300 funciones integradas para la gestión y comercio online. Se puede configurar en más de 60 idiomas y actualmente se encuentra en expansión.

Entre sus capacidades permite compartir vídeos, enlaces, actualizaciones de *Twitter*, etc. Destacamos las siguientes propiedades:

- Lenguaje: **PHP**.
- Flexibilidad para implementar funcionalidades personalizadas: **Alta.**
- Dificultad de administración: **Media.**
- Dificultad y problemática de actualización: **Baja.**
- Documentación de apoyo: **Bastante.**

Una de las características que adquiere una mayor importancia a la hora de seleccionar un gestor u otro, es la curva de aprendizaje. Esta curva ilustra las posibilidades que presenta el gestor, analizando el tiempo y conocimiento que, para su configuración, se requiere. En la Figura 2-9 se ilustra la curva de aprendizaje de algunos de los gestores de contenidos más empleados, donde se señala al gestor *Drupal* como el que mayor esfuerzo requiere. Sin embargo, una vez se obtienen las habilidades necesarias, *Drupal* permite desarrollar portales web más complejos.

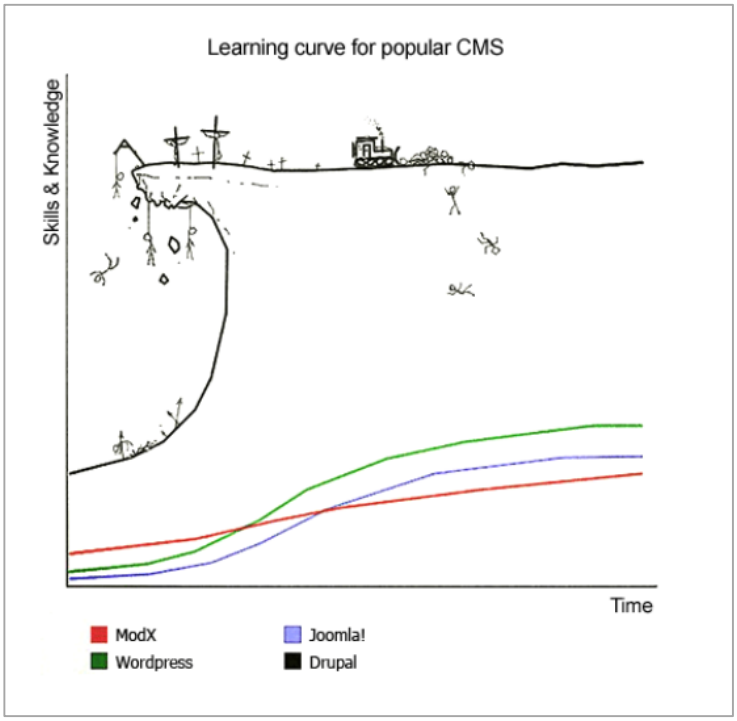

Figura 2-9 Curva de aprendizaje CMS (tomada de [46])

La gran diversidad de gestores presentes en la web se pueden clasificar, principalmente en:

- **Blogs:** Se emplean para la difusión de noticias o artículos en orden cronológico y poseen un espacio para comentarios y discusión. *WordPress* destaca en este grupo. Se trata de un gestor de contenidos que, a pesar de permitir la creación de múltiples entornos, se ha popularizado en su uso como blog.
- **Galerías:** Permiten compartir contenido audiovisual, imágenes, o vídeos. *Youtube* constituye el mejor de sus ejemplos.
- **Wikis:** En ellas cualquier usuario puede aportar información y redactar artículos sobre cualquier tema. Normalmente permiten comentarios o realizar correcciones sobre la información que proyectan. Actualmente *Wikipedia* es una de las aplicaciones más usadas para la búsqueda de información.
- **Gestores de contenidos personales:** Sirven de lugar de almacenamiento online de nuestros archivos. Se emplean frecuentemente en *smartphones* o *tablets*, ya que estos dispositivos se encuentran, en muchas ocasiones, limitados en memoria. Además permiten compartir la información para ser leída o modificada por usuarios autorizados.
- **Redes sociales:** *Facebook* se ha convertido en la reina de las redes sociales y en el medio de comunicación más usado, donde los usuarios comparten fotos y noticias todos los días. Otro ejemplo de esta variante es *Twitter*. Esta aplicación nace en 2006 como un servicio para la publicación de mensajes cortos (140 caracteres), que ha servido como la plataforma fundamental para la difusión de noticas, cambios sociales y expansión de tendencias en todo el mundo.

Tal y como se ha expuesto anteriormente, existe una gran variedad de gestores de contenidos. La Figura 2-10 representa el porcentaje de los CMS más usados en el año 2014.

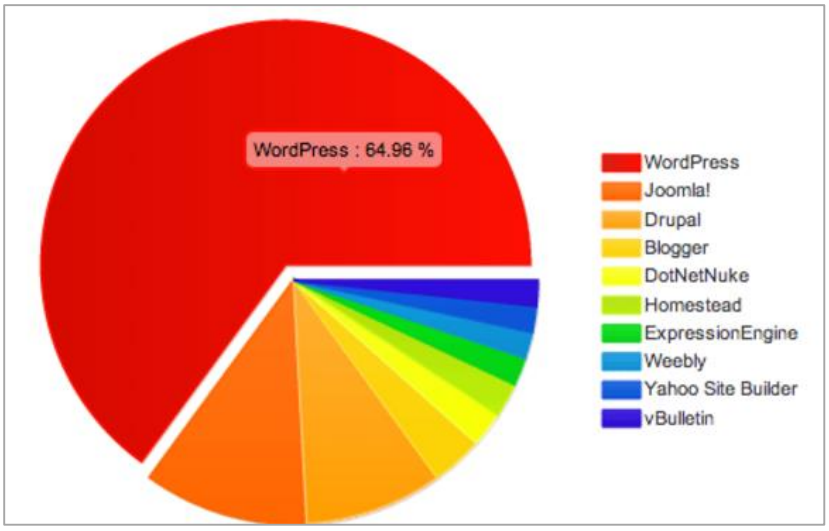

Figura 2-10 Uso de los principales CMS (tomada de [47])

2.5.7 WISE

WISE (*Web Information Service Environment*) [48] es un sistema gestor de contenidos altamente configurable y muy amigable. Inicialmente fue desarrollado como parte del *Maritime Command and Control Information System* (MCCIS) [49] para posibilitar a los usuarios diseñar, desarrollar y manejar sus propios sitios web, aplicaciones y contenidos en tiempo real. Posteriormente se extendió su uso al resto de usuarios OTAN, en posesión de ordenadores con sistema operativo Windows, como herramienta para compartir información de interés. Actualmente esta aplicación es utilizada tanto por organismos OTAN y nacionales (secciones del Estado Mayor de la Armada), como medio para la difusión de información entre los diferentes usuarios de la red.

El gestor dispone de una serie de herramientas y acciones predefinidas, que permiten la creación de un entorno jerarquizado. La información publicada se puede estructurar en distintas subpáginas, de forma que se dividan los contenidos a sus usuarios legítimos. El uso de este entorno se restringe actualmente a la Intranet de la Armada, trabajando en servidores independientes conectados a la red de propósito general, o a su uso local, a bordo de unidades navales. De esta forma, WISE se emplea en buques, Estados y Planas Mayores Operativos, así como en el CEVACO (Centro de Evaluación para el Combate). El resto de las unidades navales publican todos sus contenidos en sus páginas correspondientes de Intranet.

El gestor de contenidos WISE trabaja sobre ZOPE (Z *Object Publishing Environment*) [50]. ZOPE es un servidor de aplicaciones de código abierto, escrito en lenguaje Python, especializado en la gestión de contenidos, portales y aplicaciones web personalizadas. ZOPE le proporciona las funciones básicas a WISE como son los servicios de red, la aplicación de herramientas de seguridad y la integración de aplicaciones. Las páginas web que trabajan sobre ZOPE se construyen mediante la adición y modificación de objetos. Como se mostrará en el capítulo 3, existe una gran variedad de tipos de objetos incluidos en el *software*.

ZOPE proporciona los protocolos de red estándar tales como: el protocolo de transferencia de hipertexto (HTTP), el protocolo de transferencia de archivos (FTP), *Web Distributed Authoring* (*Webdav*) y el protocolo simple de acceso a objetos (SOAP). No obstante, para el funcionamiento correcto de la versión 1.2 de WISE, sólo se requiere el uso del protocolo HTTP [51]. Asimismo, ZOPE

proporciona servicios de seguridad para la identificación y autenticación de los usuarios, controles de acceso y auditoría. WISE incorpora estas características para su aplicación y cumplimiento de las políticas de seguridad.

ZOPE utiliza CGI (*Common Gateway Interface*). CGI permite a un cliente (conectado desde un navegador web), comunicarse con el servidor. Cualquier entrada introducida en WISE es procesada en el servidor por un *script* CGI. El diagrama ilustrado en la Figura 2-11 representa una petición web genérica, procesada por CGI.

1- Alguien realiza una petición de acceso a un documento en el servidor
2- El servidor web determina si la petición solicitada se corresponde con algún archivo y si es así se transfiere.
3- El servidor CGI procesa la petición de entrada y realiza una búsqueda en la base de datos.
4- El servidor devuelve los resultados al navegador, presentando la información al usuario. La respuesta se entrega en forma de documento HTML al navegador web.

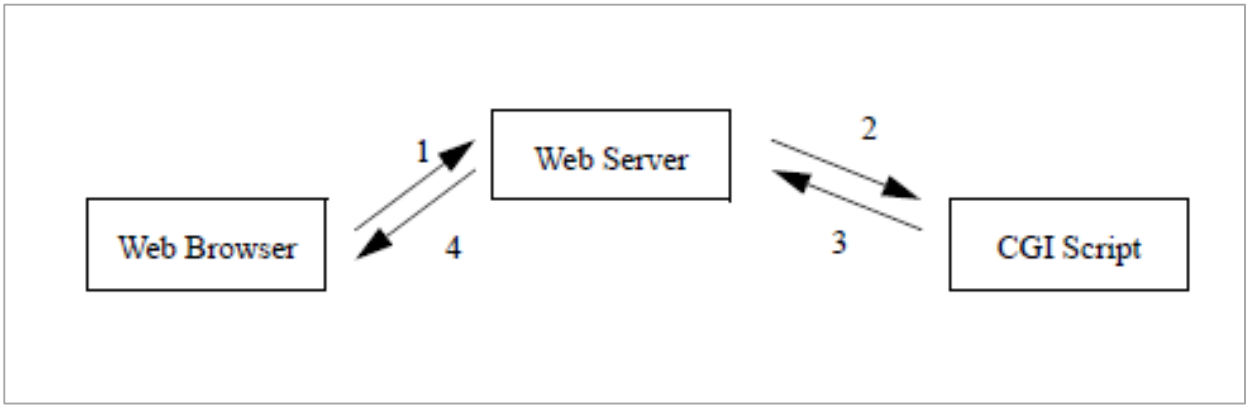

Figura 2-11 Funcionamiento de CGI (tomada de [52])

Cuando un gestor de contenidos WISE trabaja con ZOPE, el sitio web se compone de objetos almacenados en la base de datos, donde los objetos se almacenan asociados a direcciones URL. De esta forma, se genera un árbol de contenidos, que se almacenará en el directorio WISE, preestablecido en la instalación. Esta base de datos constituye una manera simple y familiar de administración de los objetos publicados. Se permite, no obstante, emplear otro tipo de base de datos, pues ZOPE presenta adaptadores que le permiten trabajar con bases de datos relacionales como, por ejemplo, *Oracle*, *PostgreSQL*, *Sybase* o *MySQL*.

2.6 Explotación de vulnerabilidades: Ataques sobre entornos web

Antes de abordar el análisis de seguridad del gestor de contenidos WISE, debemos conocer las amenazas y peligros que afectan a las aplicaciones web. Las aplicaciones en general suelen presentar errores y fallos que, en la mayoría de los casos, son debidos a errores en su diseño o en su implementación. La explotación de vulnerabilidades aprovecha los "puntos débiles" para realizar acciones no permitidas en el sistema. La explotación suele tener como objetivos:

- Obtener acceso al sistema y a su base de datos.
- Robo de información confidencial.
- Causar daños en el sistema.
- Suplantación de identidad.
- Modificar o cambiar información.
- Dañar la imagen corporativa.

Aunque las vulnerabilidades se pueden explotar de forma manual, normalmente se emplean los *exploits* para este fin. Un *exploit* es un programa o un conjunto de comandos utilizado para explotar una vulnerabilidad conocida. Actualmente circulan por la red los conocidos *frameworks de exploit* que constituyen paquetes de software para la creación de nuevos *exploits*. Para su uso se debe configurar el *payload*, un fragmento de código asociado al *exploit* y que realiza la función buscada dentro del sistema. Por ejemplo, la creación de un usuario con derechos de administrador.

Esto se conoce como el proceso de explotación. Llegado a este punto, si el atacante consigue acceder al sistema, podrá realizar uno o varios de los ataques mencionados o, incluso, usarlo para acceder a otro sistema de igual nivel o superior en la jerarquía. Esta técnica se conoce como *pivoting.* En la Figura 2-12 se reflejan los ataques en tiempo real que se lanzan contra infraestructuras críticas, empresas o cajeros automáticos en todo el mundo.

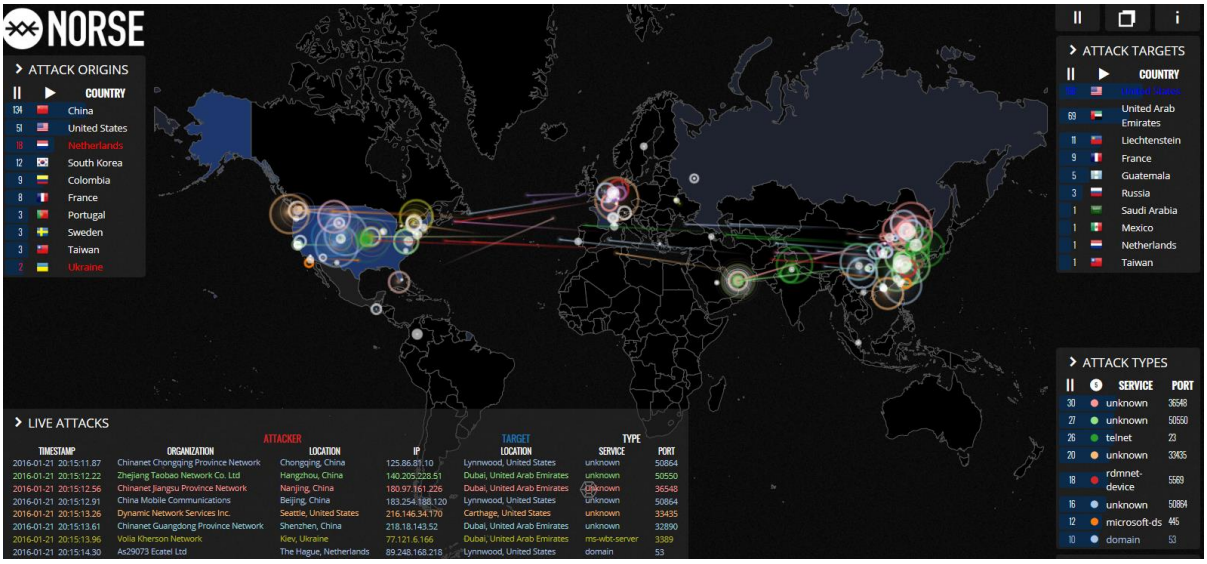

Figura 2-12 Captura de los ataques informáticos en tiempo real (tomada de [53])

A continuación, analizaremos los principales tipos de vulnerabilidades que afectan a las aplicaciones web.

2.6.1 Inyecciones SQL

Actualmente existen muchos y distintos tipos de aplicaciones web como, por ejemplo, los gestores de contenidos o los servicios de correo electrónico. Cada grupo engloba sus características y particularidades que los hacen exclusivos. Sin embargo, la inmensa mayoría precisa de un sistema gestor de bases de datos con soporte para el lenguaje SQL (*Structured Query Language)* [54].

SQL es el lenguaje estándar para la comunicación con bases de datos relacionales. Es dentro de las bases de datos donde se almacena y gestiona la información. En función de su valor o de la clasificación de seguridad, suele protegerse por una serie de técnicas y mecanismos que le proporcionen el nivel de seguridad necesario. Pero, en ocasiones, las medidas adoptadas no son suficientes para subsanar sus vulnerabilidades que, muchas veces, pueden esquivarse por los atacantes.

Como se mostrará posteriormente en la sección 2.7.1, el ataque web más frecuente es la Inyección SQL y consiste en alterar un mensaje SQL, provocando la mala validación en la entrada de un elemento almacenado y la obtención de información. Además se puede realizar este ataque para sobreescribir datos, cambiar información, modificar transacciones económicas o ejecutar comandos que causen alguna acción no deseada en el sistema. Se considera como un ataque de alto impacto.

2.6.2 Pérdida de autenticación y gestión de sesiones

Este ataque permite al usuario suplantar identidades dentro del sistema, no solo provocando un acceso no deseado, sino que, un fallo en la gestión de sesiones. Se puede incluso suplantar la identidad del administrador, dejando el control de la web en manos del atacante.

Existen diferentes formas de realizar el robo de contraseñas o la suplantación de identidad. Algunas de ellas radican en un escaso control de los cambios de contraseña, en los recordatorio de las mismas, en los métodos de recuperación o simplemente en no realizar un adecuado cierre de sesión. Además, como ya se ha mencionado, existen *exploits* capaces de crear un usuario con derechos de administración.

2.6.3 Cross-Site Scripting (XSS)

Cross-site Scripting (XSS) es otra vulnerabilidad común en aplicaciones web que se aprovecha de la falta de mecanismos de filtrado o de validación de comandos de entrada. De esta forma, se permite enviar al sistema *scripts* completos. Normalmente este ataque se es utilizado en aplicaciones web Javascript. Se denomina ataque del lado del cliente. Esto es debido a que el servidor no analiza el código HTML, si no que éste se descifra directamente en el navegador o en una aplicación local. El código malicioso se suele incrustar en programas, archivos PDF, enlaces o vídeos. De forma que, para su detonación, requieren la acción del usuario. Tras el ataque, la página web mostrará el código HTML o los comandos que ha introducidos el usuario. En la Figura 2-13 se refleja este ataque.

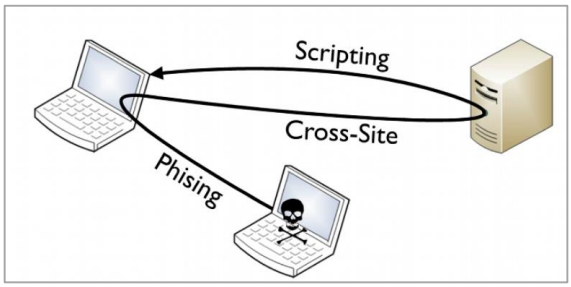

Figura 2-13 Ataque *Cross-Site Scripting* (tomada de [55])

2.6.4 Cross-Site Request Forgery (XSRF)

El XSRF no está destinado al robo de datos, sino a modificar el funcionamiento de la aplicación en favor del atacante. Se basa en que el hacker emplea al usuario para que sea el mismo el que realice el daño mientras se encuentra conectado, aprovechando la mala costumbre del usuario de navegar por la red, permaneciendo conectado a páginas de interés como puede ser un banco. Mediante este ataque, un ciberdelincuente puede impulsar un enlace con una orden al sitio en el que se encuentra conectado. Un ejemplo de esta orden puede ser la realización de una transferencia bancaria al atacante. Este ataque se refleja en la Figura 2-14. Para paliar estos ataques, las aplicaciones bancarias aplican un tiempo máximo en el que el usuario puede permanecer sin actividad, bloqueando la sesión transcurrido dicho periodo.

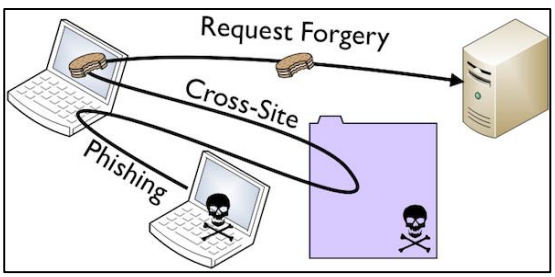

Figura 2-14 Ataque *Cross Site Forgery* (tomada de [56])

2.6.5 Denegación de servicio

La denegación de servicio (DoS) es un ataque normalmente dirigido a un servidor, con el objetivo de imposibilitar el acceso a sus recursos o de impedir el desarrollo normal de su actividad. Normalmente es empleado contra organizaciones o empresas con el objetivo de afectar a su reputación o como arma para imposibilitar sus actividades financieras. Existen, principalmente, tres formas de realizar este tipo de ataque:

- La primera de ellas consiste en saturar el buffer del servidor mediante la transmisión de un mayor número de paquetes de los que puede procesar (***buffer overflow***). Como resultado las peticiones reales no pueden ser atendidas.
- El ***Syn Flood*** es otra variante de DoS. Aprovecha el protocolo para el establecimiento de la conexión en TCP, *Three Way Handshake* [57], de forma que se envían miles de mensajes de sincronización SYN sin finalizar la conexión. Se consigue de esta forma que el sistema reciba un gran número de peticiones para el establecimiento de la conexión, agotando sus recursos. Las peticiones legítimas son rechazadas por saturación.
- Por último, **el ataque de inundación ICMP**, consiste en enviar un enorme número de peticiones ICMP (*echo request,* ping). El sistema responde a estas peticiones mediante un ICMP (*echo reply*, pong), llevando el sistema a su límite de carga e impidiendo la atención a otras peticiones.

2.6.6 Spoofing

Spoofing es un tipo de ataque que afecta a la autenticidad. Para ello, el ciberdelincuente falsea sus datos, simulando ser un *host* o página de confianza. De esta forma, el usuario accede a estas páginas, pensando que se trata de un sitio web autorizado y puede verse afectado por una gran diversidad de ataques.

El *spoofing* se puede realizar sobre diferentes componentes que integran la web, sus protocolos y equipos que a ella se conectan: *IP Spoofing*, *ARP Spoofing*, *DNS Spoofing*, *Web Spoofing*, *E-mail Spoofing* o *GPS Spoofing* son sus principales manifestaciones.

Además de los ataques sobre entornos web, existen infinidad de programas o código malicioso conocido como *malware*, que afectan a los sistemas informáticos. En el Anexo II del presente documento se presentan las principales variantes englobadas dentro del término *malware*.

2.7 Herramientas de análisis de seguridad web

Un análisis de vulnerabilidad consiste en la detección de servicios, protocolos o *software* vulnerable. El término vulnerable indica que posee fallos de seguridad o su información privada se encuentra fácilmente accesible. Las vulnerabilidades pueden ser conocidas o desconocidas. Estas últimas se conocen como *0-day* [58] y constituyen un problema cuya solución no se conoce hasta el momento.

Las herramientas de análisis web o auditorías se destinan a analizar los datos y el tráfico de un sitio web. Su objetivo es mejorar su funcionamiento y detectar comportamientos anómalos o conexiones sospechosas. Por un lado, existen herramientas destinadas a la monitorización. Estas herramientas nos presentan datos que reflejan el número de usuarios que nos visitan, las actividades que realizan en nuestra web y los aspectos a mejorar o corregir para enriquecerla. En definitiva, reflejan los contenidos más populares, las horas de mayor densidad de tráfico y las acciones a

implementar para que funcione mejor y sea más segura. En segundo lugar, se encuentran aquellas destinadas a la ciberseguridad. Su objetivo principal se centra en la detección de servicios, protocolos o *software* vulnerables. También podemos encontrar un amplio abanico de plataformas para la realización de *pentesting* (test de penetración). Estas herramientas llevan a la práctica diversos ataques para descubrir las vulnerabilidades o errores de código. Son totalmente legales siempre que se realicen sobre nuestros equipos o el de los usuarios de una organización, siempre que lo autoricen previamente. Estos sondeos se realizan sobre páginas web, equipos y sobre el factor humano, aplicando técnicas propias de la ingeniería social. Posteriormente se redacta la documentación correspondiente a los fallos deducidos por la auditoría para tomar las acciones oportunas que las solventen.

2.7.1 Realización de un análisis de seguridad

Una auditoría de seguridad web comienza con la recopilación de toda la información disponible sobre el sitio web a analizar. Para ello se emplean buscadores, envío de peticiones HTTP o establecimientos de conexión. De esta forma se buscan errores de código documentados, puertos abiertos y tecnologías usadas. Por tanto, el primer paso será realizar un análisis de puertos. El objetivo de un análisis de puertos es determinar los puntos de entrada que tiene abiertos un equipo, detectar la existencia de *firewalls* o comprobar el funcionamiento de los equipos y los servicios que se están ejecutando. Esta técnica la realizan tanto administradores, como hackers. A cada puerto se le asigna un servicio concreto. Un puerto puede encontrarse cerrado, filtrado por un cortafuegos, o abierto.

Existen distintas formas de realizar un escaneo de puertos. Uno de ellos es el protocolo de establecimiento de la conexión en TCP, *Three Way Handshake*. Pero además existen otros métodos como, por ejemplo, escaneo de *firewalls* o UDP.

- ***Three Way Handshake**:* El método de establecimiento de la conexión en TCP se utiliza para escanear los puertos abiertos. Para ello se envía un paquete SYN (, que puede ser respondido de dos maneras: si recibimos otro paquete SYN/ACK, el puerto estará abierto. Si obtenemos a cambio un paquete RST (*reset*), el puerto estará cerrado.

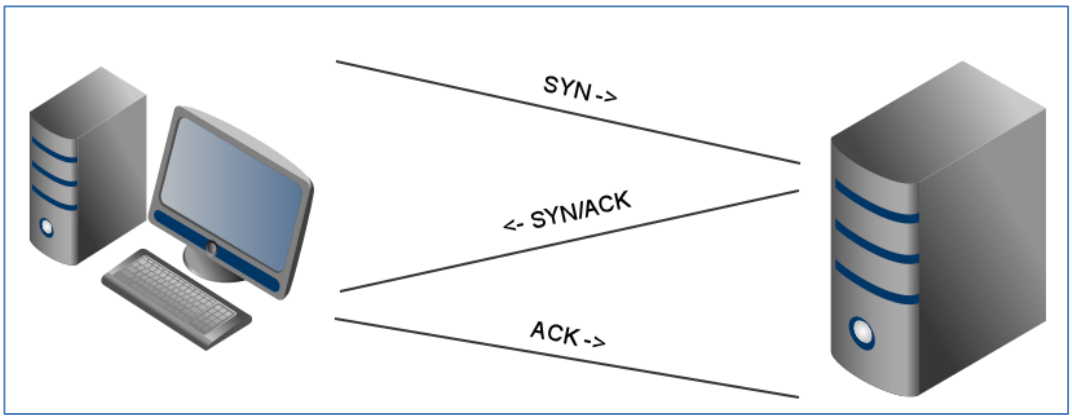

Figura 2-15 Funcionamiento del protocolo *Three Way Handshake* (tomado de [59])

- **ACK Scan:** es un método utilizado para detectar *firewalls.* Si enviamos un paquete ACK (*acknowledgement*) y obtenemos un RST (*reset*), no habrá cortafuegos. Sin embargo, si al enviar un paquete ACK, no obtenemos respuesta, es que hay un *firewall* que deshecha nuestras peticiones.

- ***UDP Scan:*** UDP (*User Datagram Protocol*) es un protocolo de la capa de transporte no orientado a establecimiento de la conexión. Si enviamos un mensaje UDP y no obtenemos

respuesta, el puerto estará abierto. Si por el contrario, recibimos un mensaje ICMP (*Internet Control Message Protocol*), el puerto estará cerrado.

Una vez tenemos el listado de puertos en uso, se debe realizar un *Banner Grabbing*, que consiste en ver las versiones de las aplicaciones que se ejecutan en cada puerto abierto. Tras obtener dichas versiones empleadas, se procede a compararlas con una base de datos de vulnerabilidades. En el caso de obtener alguna coincidencia con alguna vulnerabilidad conocida, el sistema analizado sería vulnerable y se podrían aplicar técnicas para acceder al sistema. Existen técnicas que realizan este proceso de análisis de forma automática. *Openvas* [60] es un escáner de vulnerabilidades de *software* libre. Su objetivo es facilitar el análisis de vulnerabilidades, así como proporcionar herramientas para auditorías, formación en seguridad y prevención de fallos de seguridad. Para facilitar la ayuda e identificación de las posibles amenazas, el proyecto de código libre de seguridad en la web *Owasp* [61] muestra periódicamente el *top ten* de amenazas web. En la Figura 2-16 se representan, ordenadas en función de su importancia, las mayores amenazas a la web en el año 2013.

OWASP Top 10 – 2013 (New)
A1 – Injection
A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References
A5 – Security Misconfiguration
A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control
A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards
Merged with 2010-A7 into new 2013-A6

Figura 2-16 Clasificación de las 10 principales amenazas web (tomada de [62])

2.7.2 Plataformas para análisis de seguridad web

Como administradores de un sistema de información, se debe tener una preocupación constante por su seguridad y protección. Hoy en día se encuentran disponibles un gran número de herramientas para la realización de auditorías. Se describen a continuación algunas de las plataformas más destacadas.

2.7.2.1 ZAP (ZED ATTACK PROXY)

ZAP [63] es una herramienta de código libre desarrollada por la empresa *Owasp*, destinada a la realización de tests de penetración en aplicaciones web.

Dispone de numerosas herramientas para realizar análisis de forma automática, así como un conjunto de programas y aplicaciones que le permiten realizar el análisis de forma manual. Es una de las herramientas más empleadas para la detección de errores y vulnerabilidades de *software* en las primeras fases de un test de penetración.

2.7.2.2 BACKTRACK

Backtrack [64] es una distribución Linux desarrollada por *Offensive Security*, para la realización de auditorías y seguridad informática. Se trata de una aplicación gratuita y de código abierto, variante del sistema operativo Ubuntu. *Backtrack* ofrece al usuario una gran lista de herramientas que pueden usarse desde un CD o memoria USB. Entre ellas se encuentran algunas muy populares como *Wireshark, Medusa o Nmap.* Entre las acciones que puede realizar se encuentran: la recopilación de información, el mapeo de puertos, análisis de vulnerabilidades, tests de penetración o técnicas para la realización de ingeniería inversa.

Sin embargo, su última versión fue lanzada en 2012. Actualmente ha sido sustituida por *Kali Linux*, que presenta nuevas mejoras y mayor robustez.

Figura 2-17 Logo de la herramienta de análisis de seguridad *BackTrack*

2.7.2.3 KALI LINUX

Kali Linux [65] es un proyecto de seguridad basado en su predecesor. Al igual que *Backtrack*, es completamente gratuito. Esta nueva actualización trabaja sobre el sistema operativo Debian, considerado más seguro, actualizado y eficiente. Trae preinstaladas numerosas aplicaciones, más de 600 programas y cuenta con una enorme lista de herramientas para la realización de test de penetración. Además en su menú incluye una lista con las diez herramientas más usadas en seguridad informática, información sobre *gathering*, análisis de seguridad, tutoriales para insertar código SQL, herramientas para realización de ingeniería social, DoS, etc.

Figura 2-18 Logo de la herramienta de análisis de seguridad *Kali Linux*

A continuación se presentan las herramientas de la distribución *Kali Linux* que serán empleadas en el capítulo 4 del presente documento:

1- ***Whatweb*** [66]: Es una herramienta que permite identificar las tecnologías de un servidor web, incluyendo los CMS. Dispone de más de 900 *plugins* orientados a este propósito. Además de las tecnologías, *Whatweb* identifica las versiones de las aplicaciones, sistemas operativos que se ejecutan sobre el servidor o direcciones IP. Ofrece la posibilidad de realizar escáneres pasivos o tests de vulnerabilidades agresivos.
Por todo ello, podría ser empleada en un *pentesting* tanto para la recogida de información como en el escáner de vulnerabilidades.

2- ***Zenmap*** [67]: Constituye el interfaz gráfico de *Nmap*, herramienta de código abierto empleada para la exploración de redes y la auditoría de seguridad. A partir de paquetes IP, determina qué equipos se encuentran conectados, así como los puertos abiertos y servicios que sobre ellos se ejecutan.
Además de su empleo en auditorías de seguridad, *Zenmap* puede emplearse para la monitorización de equipos propios.

3- ***BlindElephant*** [68]: La herramienta *BlindElephant* cuenta con 15 *plugins* de aplicaciones web conocidas. Tras un rápido escáner, la herramienta identifica las versiones de las aplicaciones que sobre un servidor se ejecutan, comparándola con dichos *plugins*. Tras obtener la versión de una aplicación específica, se podría realizar un ataque dirigido a explotar las vulnerabilidades que presenta dicha versión.

4- ***ZAP (Zed Attack Proxy):*** ZAP, comentado en la sección 2.7.2.1, es una herramienta escrita en Java destinada a servir como escáner de vulnerabilidades y a realizar tests de penetración sobre aplicaciones web. Dispone de escáneres automáticos, no obstante, también permite realizar el escaneo de forma manual. Durante estos escáneres ZAP lanza distintos ataques. Entre otros se encuentran: XSRF, XSS o Inyección SQL.

5- ***VEGA:*** VEGA [69] es otra de las herramientas que presenta *Kali Linux* para analizar la seguridad de aplicaciones web. Tras el análisis, la herramienta genera un informe en el que clasifica las vulnerabilidades por niveles de riesgo.

6- ***Armitage:*** *Armitage* [70] es el interfaz gráfico de ciberataques de *Metasploit*. La propia herramienta recomienda qué tipo de *exploit* emplear para vulnerar un sitio web concreto. Se emplea para el descubrimiento y explotación de vulnerabilidades.

7- ***Wireshark:*** *Wireshark* [71]es un analizador de protocolos de red de libre distribución. Su objetivo principal es el análisis y la captura de tráfico. Se emplea por los administradores de red para detectar, analizar o localizar anomalías en la red. De esta forma se puede mejorar su rendimiento. Además, a través de las técnicas *sniffing*, se pueden obtener contraseñas de usuarios que se envían por la red sin cifrar. Contraseñas, correos electrónicos o procesos que un equipo determinado está ejecutando, son algunos de los datos que se puede obtener.

8- ***GoldenEye:*** *GoldenEye* [72] es una de las herramientas que presenta *Kali Linux* para la realización de ataques de denegación de servicio. Con su empleo se pueden localizar las vulnerabilidades que presenta un sistema o aplicación web ante este tipo de ataques.

2.7.2.4 SAMURAI WEB TESTING

Samurai Web Testing [73] se define como una plataforma Linux desarrollada para funcionar como un entorno web de *pentesting.* Comparte también una gran cantidad de herramientas de análisis de

vulnerabilidades. Además, la distribución incorpora una guía detallada para la realización de auditorías y test de penetración para usuarios no experimentados.

2.7.2.5 ACUNETIX WEB VULNERABILITY SCANNER

Acunetix WVS [74] es otro ejemplo de herramienta de seguridad informática desarrollada para la realización de auditorías sobre aplicaciones web. Comprueba las vulnerabilidades como inyección SQL o *Cross-Site scripting*, entre muchas otras. Como parte de la auditoría, *Acunetix* analiza las vulnerabilidades del servidor web y, mediante un escaneo y análisis de puertos, identifica los servicios en funcionamiento. Además realiza un test de verificación de contraseñas y muestra los fallos de programación, generando finalmente un informe de seguridad. La distribución es de pago, no obstante, permite una prueba gratuita de 14 días para conocer su funcionamiento.

Figura 2-19 Logo de la herramienta de análisis de seguridad *Acunetix*

2.7.2.6 FOCA (FINGERPRINTING ORGANIZATIONS WITH COLLECTED ARCHIVES)

FOCA [75] es un *software* para *pentesting*, desarrollado por la empresa española de seguridad informática *Eleven Paths* y que se basa en el análisis de metadatos. No obstante, también permite la realización de escaneo de puertos, búsqueda de servidores de dominio, así como el descubrimiento de equipos conectados. De los metadatos, podemos obtener todas las modificaciones que se han realizado sobre un documento, la versión sobre la que se ha creado o incluso extraer contraseñas y direcciones. En el caso de fotografías, se podría obtener la ubicación GPS donde fue tomada, la fecha y hora exacta en la que se realizó. Esto puede suponer un riesgo para personas públicas como políticos o famosos, que suben constantemente imágenes a las redes sociales, pudiendo estar revelando su ubicación.

El proceso que realiza este software comienza por la descarga de todos los documentos de una página web (PDF, DOC, JPEG), para descubrir información que pueda interesar en un test de penetración. Esta puede ser: usuarios, en qué dispositivo trabaja cada usuario, la versión del sistema operativo, correos electrónicos, etc. Esta práctica no es ilegal, pues los documentos han sido colgados en la red y, por tanto, son públicos. El objetivo final de *FOCA* es reforzar la privacidad y evitar la mala imagen de la organización y, además, localizar vulnerabilidades y eliminar toda la información privada que haya podido ser publicada inconscientemente.

Figura 2-20 Logo de la herramienta de análisis de metadatos *FOCA*

3 DESPLIEGUE DEL CMS WISE

3.1 Presentación

A lo largo de la siguiente sección se explican detalladamente los procesos de instalación y configuración *Classic* del gestor de contenidos WISE, utilizado en el ámbito de la OTAN. Para este despliegue, se ha empleado la **versión 1.2 R1** de WISE. Proporcionada por el Arsenal de Ferrol, para el desarrollo del TFG, esta es la versión más moderna que se ha podido conseguir.

La descripción del despliegue se acompaña de una amplia recopilación gráfica del proceso realizado. Además, se analizan las diferentes posibilidades que ofrece WISE en cuanto diseño y publicación de contenidos. Las opciones seleccionadas en la instalación y configuración, así como la temática general del gestor y los archivos que se muestran en el portal, simulan el uso que se le daría a WISE en la Escuela Naval Militar, como centro militar de formación para los futuros oficiales.

3.2 Instalación de WISE

La instalación que se describe a continuación se ha desarrollado siguiendo los pasos descritos en la guía que proporciona la aplicación [76]. WISE se ha instalado en un equipo Toshiba Satélite C660, que hará de servidor de nuestro gestor de contenidos. El equipo presenta las siguientes características:

- **Sistema Operativo**: Windows 7 Profesional. 64 bits
- **Procesador**: Intel® Core™ i5-3230M CPU @ 2.60GHz.
- **Memoria instalada (RAM):** 4,00GB (3,89GB utilizable).

Para proceder a la instalación de la aplicación, entraremos en el CD y seleccionaremos la aplicación **wise_1.2R1,** como se muestra en la Figura 3-1.

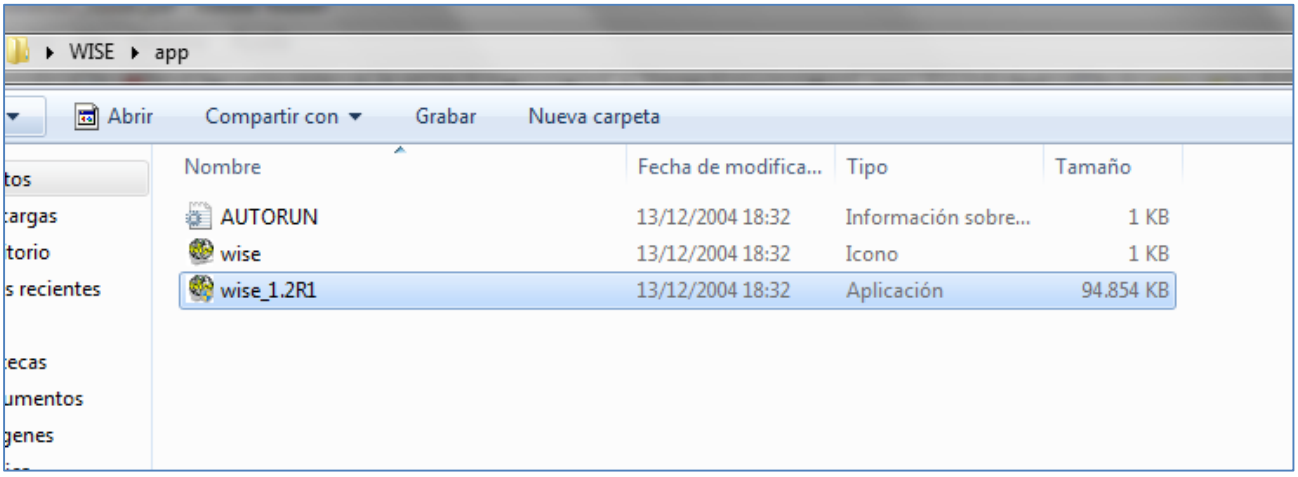

Figura 3-1 Captura: CD gestor de contenidos WISE 1.2R1

El primer paso será seleccionar el directorio donde deseamos guardar el sistema de archivos del CMS. En nuestro caso, hemos seleccionado. **C\Archivos de Programa(x86)\WISE.** Pulsaremos en *next* para continuar.

La siguiente ventana será *Development Tools* (Herramientas de desarrollo). Esta ventana proporciona la opción de seleccionar herramientas de desarrollo, que contienen documentación para el desarrollo de aplicaciones y la creación de nuevos objetos WISE. Esta opción sólo se debe seleccionar si se prevé el desarrollo de software en el servidor de WISE. Además, al marcar la casilla, permite al usuario acceder a la siguiente documentación: guía del desarrollador, *Python* y documentación ZOPE. En estos documentos se muestra toda la información necesaria sobre ZOPE y el sistema, para futuros administradores.

Para nuestra aplicación, cuyo uso se asemeja al realizado en las unidades de la Armada, dejaremos la casilla sin marcar, como se refleja en la Figura 3-2. Este hecho se justifica en que en las unidades navales, WISE se emplea como un gestor de contenidos sencillo para compartir información de interés como: orden diaria, documentos administrativos, imágenes o enlaces a sitios web de interés. El desarrollo de aplicaciones o nuevos objetos WISE no se realiza en este ámbito.

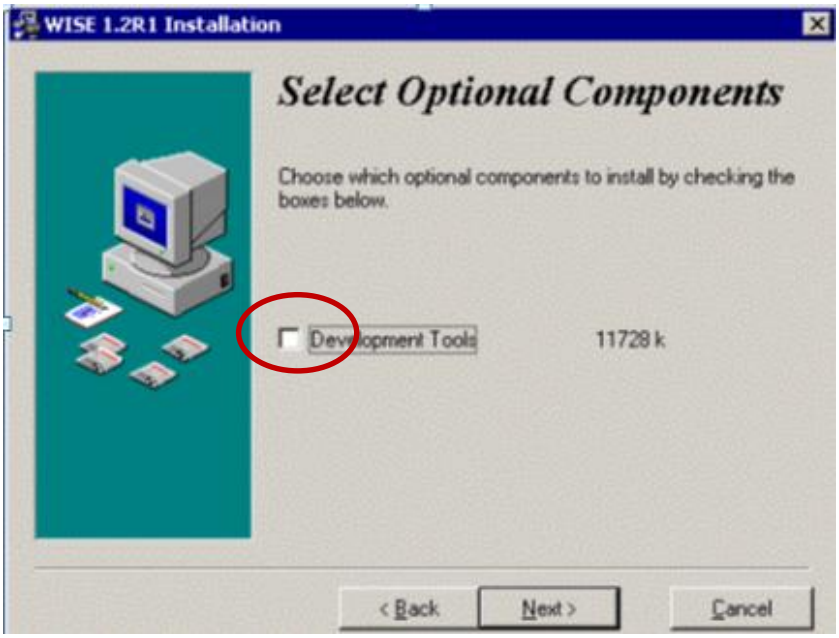

Figura 3-2 Captura: Ventana de selección de *Development Tools*

A continuación deberemos seleccionar una de las dos posibles configuraciones disponibles:

- La primera es la versión *Classic*, que es una instalación típica de WISE que permite al usuario diseñar, desarrollar y administrar sus propios sitios web.

- La segunda es la opción *Enterprise*, que añade una capa adicional a la versión *Classic*. Un segundo servidor HTTP (en forma de Apache) se instala para manejar las solicitudes GET, sirviendo de apoyo a WISE para la gestión de otras solicitudes de servicio web. Aunque esto hace la instalación más compleja de gestionar, aumenta la capacidad de respuesta y el rendimiento de WISE.

En nuestra aplicación, seleccionamos la **configuración Clásica** o estándar (Figura 3-3). Hemos optado por esta opción en la que la configuración del portal ya que es la que se suele emplear en los buques de la Armada. Además, es ideal para entornos pequeños, en los que el número de usuarios y el volumen de información son reducidos.

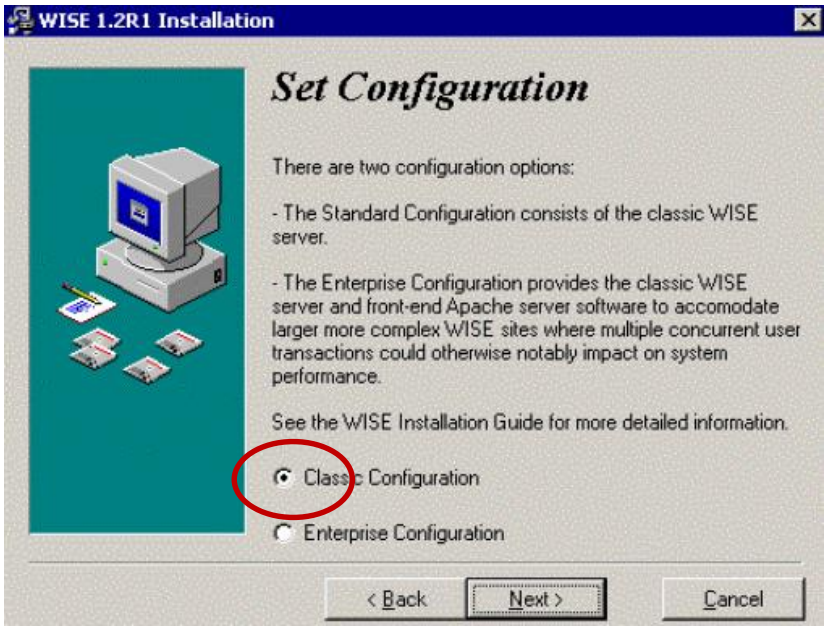

Figura 3-3 Captura: Selección del tipo de instalación (*Classic* o *Enterprise*)

A continuación, tendremos que seleccionar el puerto de escucha del servidor web (Figura 3-4). Por defecto, la aplicación preselecciona el puerto 80. No obstante, en caso de tener ocupado dicho puerto por otra aplicación, se propone el 8080 como alternativo.

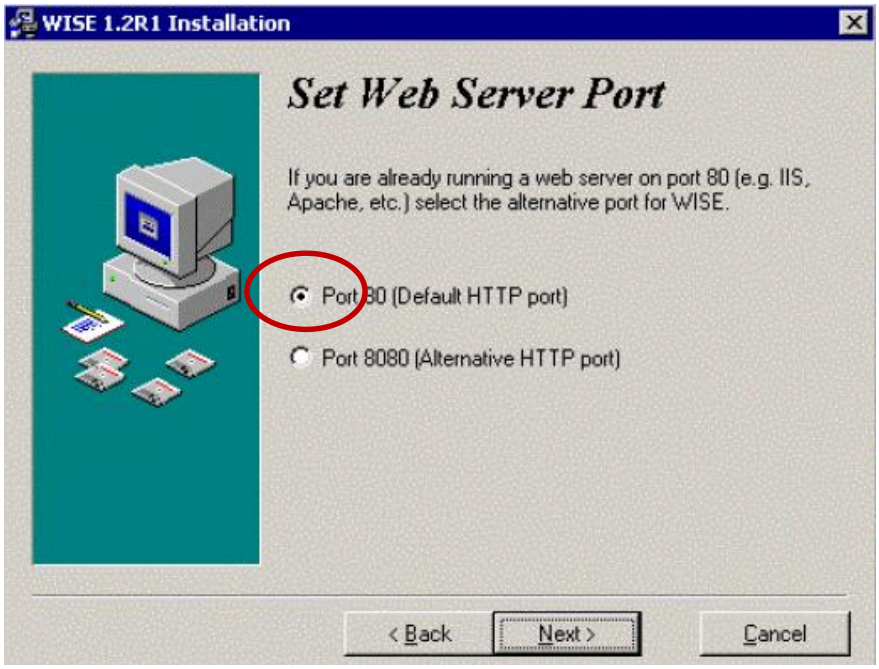

Figura 3-4 Captura: Selección del puerto para el servicio web

En el siguiente paso, debemos introducir los datos del usuario de emergencia (ver Figura 3-5). Éste usuario se empleará para restablecer las contraseñas en caso de pérdida u olvido. Por lo tanto, la contraseña seleccionada deberá conocerla el administrador de WISE y almacenarla en un lugar seguro. El nombre de este usuario (*emergency*, por defecto), se puede modificar.

Para nuestro usuario *emergency* hemos seleccionado una clave de acceso segura, contando con 8 caracteres en los que se incluyen números y letras, símbolos y mayúsculas.

Figura 3-5 Captura: Establecimientos de los datos de usuario de emergencia

Justo después del usuario de emergencia, definiremos la cuenta de administrador WISE. Este administrador es el responsable de la creación del gestor y del control de su base de datos. En nuestro caso, tal y como se refleja en la Figura 3-6, hemos mantenido este nombre y hemos seleccionado una contraseña segura.

Figura 3-6 Captura: Establecimiento de la cuenta del administrador de WISE

En este paso, se crea el sitio web para nuestra WISE. Tanto el título como la ubicación pueden seleccionarse en los recuadros que aparecen en la Figura 3-7. En nuestro caso, hemos mantenido la dirección y sitio por defecto durante la instalación. No obstante, la dirección se puede modificar, cambiando el nombre del sitio en la configuración, tal y como se explicará posteriormente. De esta manera nuestra URL incluirá **WISE: WISE** y se especificará en el título.

Si la opción *Allow Self Registration* se marca, los usuarios tendrían la capacidad de registro en el sistema WISE. Esta casilla se ha dejado sin marcar (véase Figura 3-7), de forma que será el administrador quien tendrá que registrar a todos los nuevos usuarios. Como veremos más adelante, esta opción también podrá ser modificada posteriormente en la configuración.

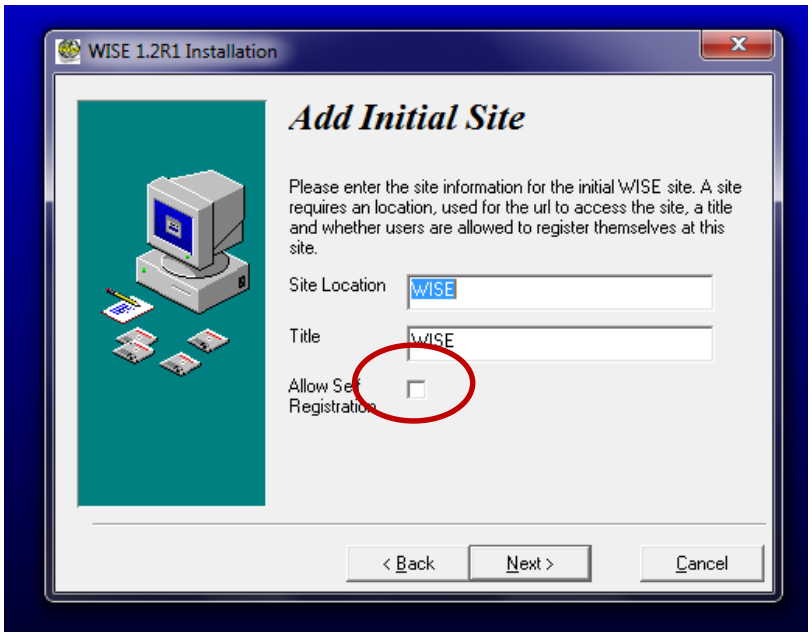

Figura 3-7 Captura: Establecimiento de la información del sitio WISE

El administrador del sitio o *site administrator* gestionará el sistema WISE. Este usuario controlará el acceso y será el encargado de subir y gestionar los contenidos que se publican en la web, así como registrar los nuevos usuarios (Figura 3-8).

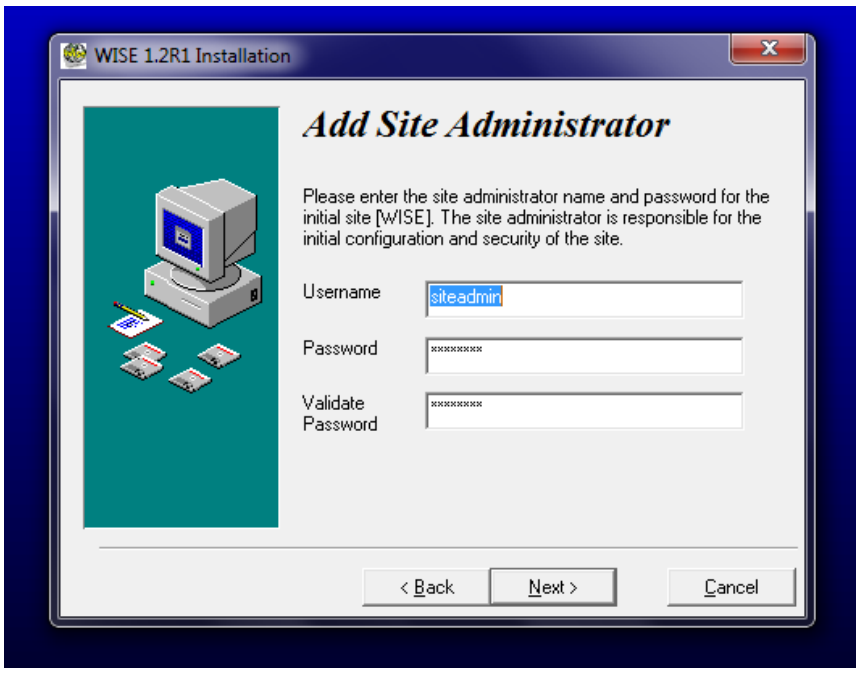

Figura 3-8 Captura: Establecimiento de la cuenta de administrador del sitio WISE

La ventana de *Simple Mail Transfer Protocol* (SMTP) solicita el nombre o la dirección IP del servidor de correo electrónico para WISE. Este servidor se empleará cada vez que se quiera mandar un e-mail a un usuario registrado. Además, algunos de los objetos WISE se apoyan en este servidor para su presentación web. En nuestro caso hemos seleccionado el servidor público de gmail: **smtp.gmail.com.**

El número de puerto predeterminado es 25; éste es el número de puerto estándar para SMTP y, como se refleja en la Figura 3-9, el que seleccionaremos.

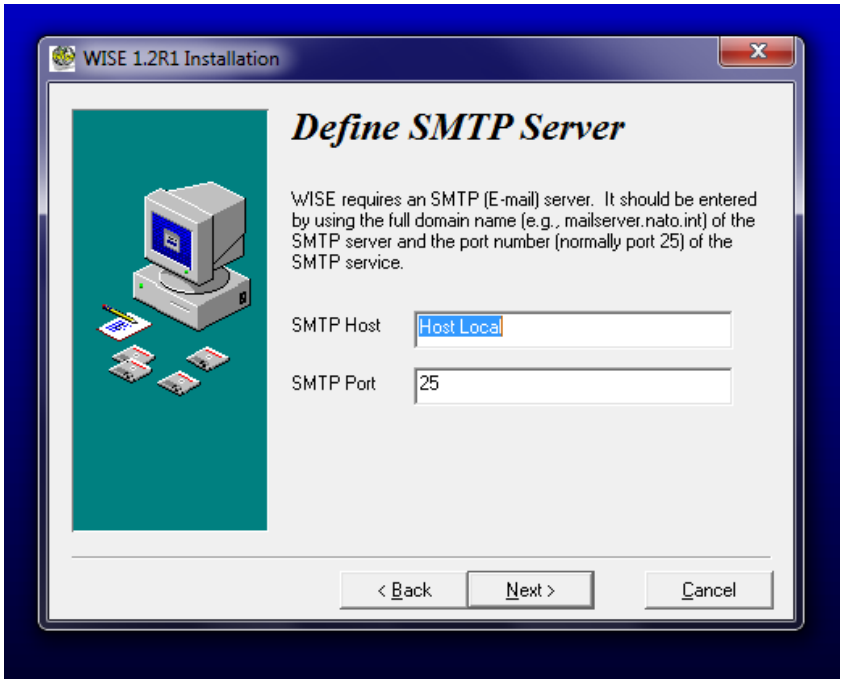

Figura 3-9 Captura: *Define SMTP Server*

Tras el establecimiento de todos los parámetros previos, nuestra aplicación ya está disponible para su instalación (ver Figura 3-10). En caso de necesitar modificar algún dato introducido, se permite la opción de volver hacia atrás.

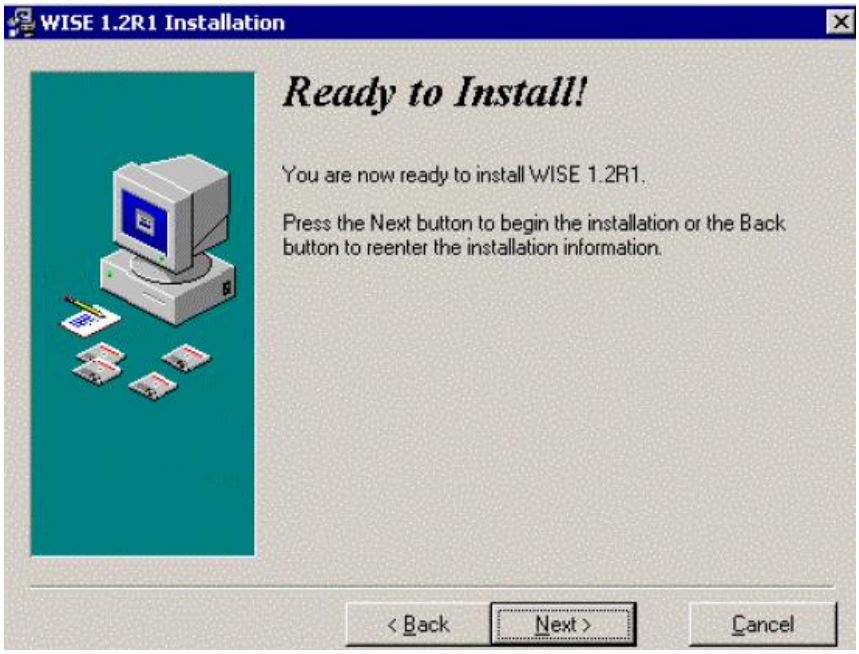

Figura 3-10 Captura: Mensaje de inicio de instalación de WISE

Una vez completada la instalación (ver Figura 3-11), accedemos a WISE con la URL: http://cud-tosh./ Posteriormente, se le ha asignado al equipo la IP fija **192.168.1.79** para su acceso en red local. No obstante, siempre se puede acceder con el título configurado en la instalación (ver Figura 3-7).

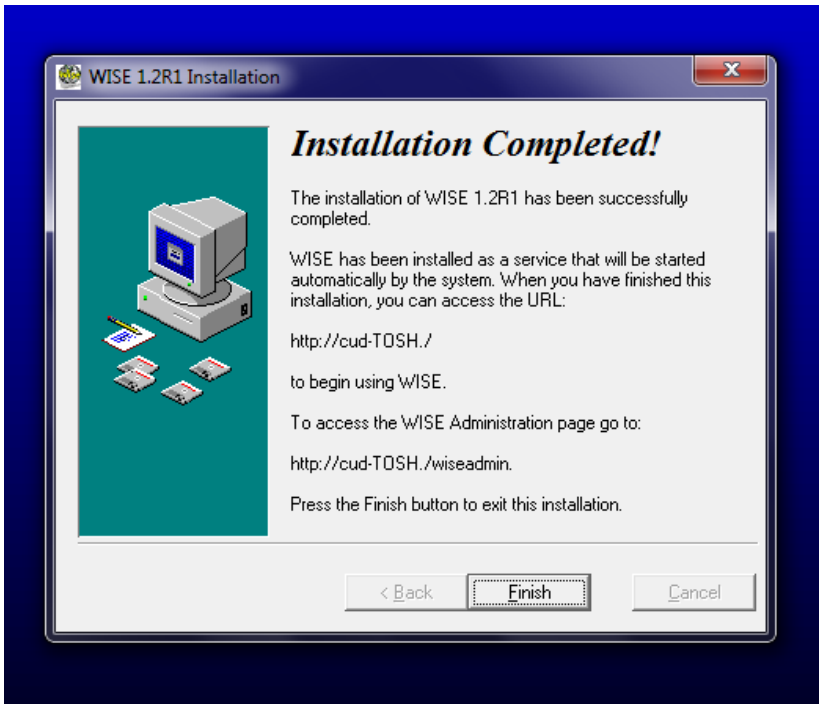

Figura 3-11 Captura: Mensaje mostrado tras la instalación con éxito de WISE

3.3 Configuración de WISE

Una vez realizada la instalación, accederemos a nuestra página introduciendo en el navegador la URL indicada en el apartado anterior o simplemente **WISE: WISE**. Como estamos accediendo localmente, no precisamos conexión a Internet o red LAN para ello.

Una vez en nuestro portal WISE, nos autenticaremos como ***siteadmin*** para proceder a su diseño (ver Figura 3-12).

Figura 3-12 Captura: Pantalla de autentificación de WISE

Una vez autenticados como administrador, procederemos a la generación de nuestro entorno, diseñando los contenidos que deseamos mostrar. Para ello, pinchamos sobre el icono que nos aparece a la derecha de la pantalla, y que representa un ordenador detrás de una llave (ver Figura 3-13).

Figura 3-13 Acceso a la configuración WISE

Accederemos de este modo a la ventana menú (ver Figura 3-14). En ella podremos ir introduciendo los diferentes contenidos que deseemos colgar en el portal:

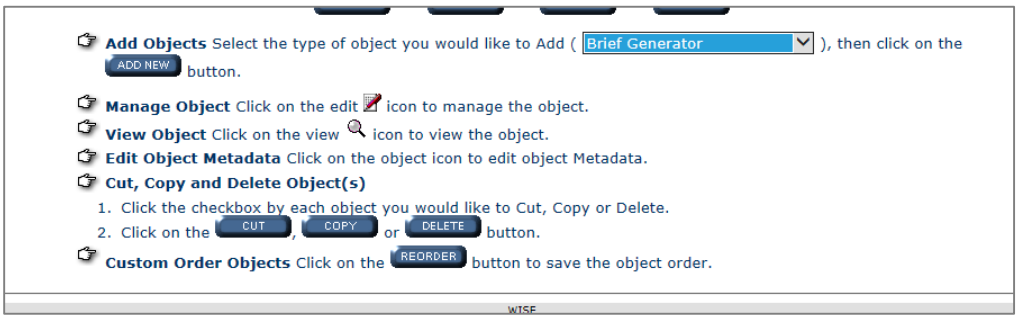

Figura 3-14 Ventana de generación de objetos WISE

Desplegando la ventana de ***Add Objects***, se nos muestra el listado de los distintos tipos de documentos que podemos colgar (ver Figura 3-15). A continuación, realizaremos una breve explicación de cada tipo de objeto disponible.

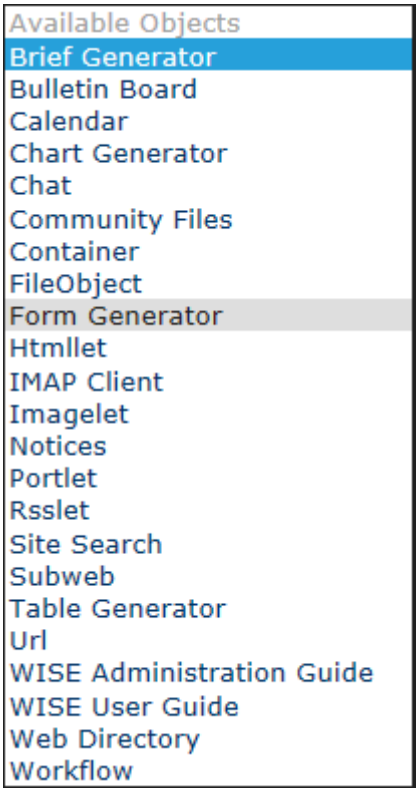

Figura 3-15 Lista de objetos WISE

- ***Brief Generator***

Permite a uno o más usuarios la creación de una presentación o un sitio web dinámico. Después de crear cada presentación individual, se puede cargar y posteriormente se compila en una única, para su revisión antes de su aprobación final.

Una vez que se concede la aprobación final, la presentación se puede visualizar en cualquier ordenador conectado a WISE.

- ***Bulletin Board***

Estos tablones de anuncios pueden emplearse por destinos o grupos para diferentes propósitos.

Son el equivalente electrónico de los antiguos tablones de anuncios, donde cualquier persona puede publicar folletos sobre cualquier tema de interés, tales como artículos para la venta de objetos, eventos y anuncios.

El objeto *Bulletin Board* permite a los visitantes invitados (sin registro de usuario necesario) publicar artículos, adjuntar archivos y mantener conversaciones sobre temas relevantes. Los usuarios pueden responder y asociar sus comentarios con un mensaje específico ya publicado. Este hecho podría suponer una vulnerabilidad puesto que cualquier visitando podría publicar archivos infectados.

- ***Calendar***

El calendario permite publicar de manera fácil los eventos o actividades previstas. La aplicación ofrece una variedad de opciones de visualización, capacidad para marcar los eventos con un código de colores de fácil interpretación y agregar enlaces URL a los eventos.

Sólo los usuarios con privilegios de administrador del sitio pueden añadir o editar eventos.

- ***Chart Generator***

El objeto *Chart Generator* es una herramienta rápida y fácil para la construcción de gráficos en línea que muestren información estadística.

- ***Chat***

El *Chat* de WISE ofrece un primer nivel informal para discutir temas y cuestiones pertinentes al destino o departamento, o de hacer preguntas a otros usuarios.

Se trata de una aplicación abierta que permite interactuar a todos los usuarios, incluyendo los clientes no registrados. El *chat* dispone de un registro, de forma que los usuarios que trabajan en turnos diferentes pueden leerlos más tarde.

- ***Community Files***

El objeto de los *Community Files* es permitir al usuario ver el contenido de los directorios ubicados en el servidor o acceder a las carpetas compartidas adicionales.

Normalmente, el servidor WISE tiene restringido el acceso de los usuarios. Por ello el administrador tendrá que colocar los archivos en el directorio por defecto o compartir el directorio para los usuarios.

- ***Container***

El *Container* es uno de los objetos más utilizados disponibles en WISE. Se trata básicamente de un archivador que permite almacenar cualquier tipo de archivo (por ejemplo, archivos de Word, PowerPoint, Excel, archivos de imágenes, aplicaciones de bases de datos, etc.)

Los contenedores son análogos a las carpetas o directorios que usamos en cualquier ordenador. Pueden contener otros contenedores para proporcionar una estructura de archivos jerárquica. Se deben elegir títulos lógicos para hacer el acceso a la información los más intuitiva posible. No obstante, pueden modificarse posteriormente. En la Figura 3-16 se muestra uno de los *containers* empleados.

Figura 3-16 Captura: Ejemplo de *Container*, Asignaturas CUD

- ***FileObject***

Los *FileObject* permiten al administrador colgar cualquier archivo, con gran facilidad. La única limitación en el tipo de archivo que se utiliza es que el usuario debe tener instalada en su equipo la aplicación necesaria para abrir el archivo.

- ***Htmllet***

La herramienta *Htmllet* está diseñada principalmente para los usuarios familiarizados con *Hypertext Markup Language* (HTML). Puede contener HTML, XML, texto plano y texto estructurado. Por ejemplo, un *Imagelet* (descrito más adelante) sólo permitirá la publicación de una sola imagen en su página y no permite cambiar el tamaño de esa imagen, mientras que una *Htmllet* facilita la publicación múltiples imágenes y el cambio de tamaño. En el despliegue del sistema WISE para la creación del portal de la ENM, se ha empleado este objeto para la difusión de avisos, a partir de texto en movimiento.

Figura 3-17 Captura: Ejemplo de *Htmllet* en la página principal del portal WISE

- ***IMAP Client***

El protocolo de acceso a mensajes de Internet *(IMAP)* es un método de acceso a mensajes de correo electrónico que se almacenan en un servidor.

El cliente IMAP permite al usuario ver sus carpetas y mensajes de correo electrónico, integrado en el portal WISE.

- ***Imagelet***

Imagelet permite agregar una imagen o un gráfico a su página. La imagen utilizada debe estar disponible en una unidad local y estar en un formato compatible con el navegador, por ejemplo GIF o JPEG, de modo que pueda ser correctamente visualizada en la web. Además no se puede modificar su tamaño, por lo que debe ser comprobada antes de subirla.

Imagelet permite la introducción de texto que acompañe a la imagen, aunque se debe señalar que el objeto no dispone de los comandos para la edición de texto. Para la redacción de cualquier texto con título, párrafos o cursiva, se deberán introducir comandos HTML.

Figura 3-18 Captura: Ejemplo *Imagelet* con texto editado en HTML

- ***Notices***

Notices proporciona un tablón de noticias en el que el administrador puede colgar información. Al contrario que *Bulletin Board*, no es interactivo y no permite los comentarios.

Se emplea como medio de difusión de información importante para la organización.

- ***Portlet***

Portlet es una aplicación que permite la utilización de WISE como un puerto o una ventana para mostrar otro sitio web.

El resultado es una página web a la que se puede acceder directamente desde su propio sitio WISE.

- ***Rsslet***

Este objeto utiliza RSS (*Rich Site Support)* publicados en otras webs. *Rsslet* permite que otras webs compartan un resumen de información de interés. Este resumen se muestra en una tabla de contenidos, que se actualizan cada vez que actualizamos las tablas. Algunos de los objetos que permiten el uso de *Rsslet* son: el tablón de anuncios, calendario o *containers*. Al contrario que las URL, en las ventanas *Rsslet* se muestran una serie de enlaces a los archivos de interés externos a nuestra página.

Ésta es una aplicación muy utilizada en los sitios web que publican los últimos titulares de noticias generados por una agencia exterior.

- ***Site Search***

Site Search proporciona un buscador local. Introduciendo una palabra muestra todas las entradas que contengan esa búsqueda (ver Figura 3-19).

Figura 3-19 Captura: Buscador local para el portal WISE

- ***Subweb***

WISE permite generar un entorno estructurado jerárquicamente mediante subwebs.

Las *subwebs* deben usarse para crear una secuencia lógica en su página, ordenando la información específica por destinos o departamentos, facilitando la navegación y estructurando los contenidos.

- ***Table Generator***

Table Generator es una aplicación que permite al administrador construir y mantener las tablas. Ofrece una variedad de opciones para mostrar los contenidos. Sólo los usuarios con los permisos adecuados pueden añadir o modificar los datos de la tabla, pero cualquier visitante invitado puede ver los datos.

Un uso típico podría ser una lista de contactos, como se ilustra en la Figura 3-20.

Figura 3-20 Captura: Ejemplo de tabla en WISE

- ***URL***

El objeto *URL* permite formar enlaces a recursos externos. Es una dirección web o ruta de acceso a otras páginas que permite dirigir a los usuarios de WISE a sitios en los que se muestren contenidos de interés. En la Figura 3-21 se muestran algunos de los enlaces que se muestran en el portal WISE, diseñado para la ENM.

Figura 3-21 Captura: Ejemplo de uso del objeto URL

- ***WISE Administration Guide***

La Guía de Administración detalla los procedimientos para la gestión y mantenimiento de sitios web de WISE, incluyendo temas como la seguridad y facilidad de acceso.

También detalla los procedimientos y las posibles opciones al instalar WISE en el servidor.

- ***WISE User Guide***

Este documento proporciona orientación sobre el uso genérico de WISE, es decir, la estructura, los procesos y procedimientos. Además muestra cómo desarrollar subwebs y añadir objetos; explica roles y permisos de seguridad que afectan a los usuarios; y utiliza algunos objetos disponibles dentro de WISE para construir ejemplos de sitios web.

- ***Web Directory***

El objeto permite mostrar el directorio web de nuestro sitio WISE.

Este recurso se utiliza ampliamente en Internet y contiene enlaces de diferentes categorías con el fin de dirigir al usuario a sitios específicos. En la Figura 3-22 se muestra, a modo de ejemplo, el directorio de Google.

Figura 3-22 Directorio de Google

- ***Workflow***

Workflow se utiliza para definir las tareas previstas, los pasos a realizar para alguna actividad o la organización y personas involucradas en un evento. En general se centran en procesos y no documentos.

En términos más simples, podemos definir *Workflow* como el conjunto de tareas, en serie o en paralelo, llevadas a cabo por dos o más miembros de un grupo de trabajo, que buscan un objetivo común. En muchas ocasiones se emplean las redes de Petri para organizar estas tareas.

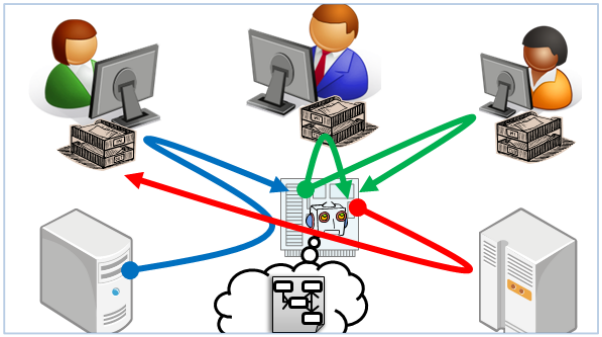

Figura 3-23 *Workflow*

3.4 Creación del portal WISE para la ENM

Los objetos expuestos en el apartado anterior han sido utilizados sobre la página principal (*Home*), creando los contenidos que queremos mostrar a cualquier invitado que acceda a nuestro sitio WISE. Como se indica en las normas de uso de WISE aplicadas en el ámbito de la Armada, la información, dada la clasificación de seguridad de la red física de Intranet, deberá ser SIN CLASIFICAR: ningún documento con una clasificación de seguridad superior a *SINCLAS* ha sido empleado.

En la Figura 3-24 se muestra el diseño desarrollado para el estudio. Para lograrlo se han empleado los objetos WISE enunciados en el capítulo anterior (principalmente *Containers*, *FileObjects*, *Imagelets*, *Htmllet*, *Calendars*, *Site search* y *URLs)*, creando distintas carpetas, seleccionando la información que en ellas se presenta y que quedarán accesibles a cualquier individuo que acceda a nuestro portal.

Figura 3-24 Captura: Página principal WISE Escuela Naval Militar

Una vez diseñada la parte pública, crearemos tres Subwebs: Alumnos, Dotación y Oficiales y Profesores. Éstas contendrán información destinada a cada uno de los grupos mencionados y su acceso quedará limitado a los usuarios legítimos a los que se dirige. Por ello deberán autenticarse como usuarios del sistema.

En la Figura 3-25 se muestra la página destinada a Oficiales y Profesores. En ella los contenidos que se publican se destinan a este grupo específico. De esta forma, podemos observar carpetas empleadas por los distintos profesores que imparten asignaturas en la Escuela Naval o manuales de educación.

Figura 3-25 Captura: Subwise de Oficiales y Profesores

La Figura 3-26 es una captura de pantalla de la subweb destinada a los alumnos del centro. En ella la información publicada se centra en apuntes de las diferentes asignaturas cursadas, publicaciones de interés, horarios de clases o presentaciones de ayuda para la gestión del primer destino en las unidades.

Figura 3-26 Captura: Subwise de Alumnos

Por último, la Figura 3-27 muestra la subwise creada para la dotación. Los documentos que sobre ella se publican, se dirigen al personal destinado en la Escuela Naval, los cuales realizan funciones

ajenas a la enseñanza. Entre los documentos que en ella se pueden encontrar, destacamos: impresos para tramitaciones administrativas, previsión de guardias, publicaciones de maniobra, etc.

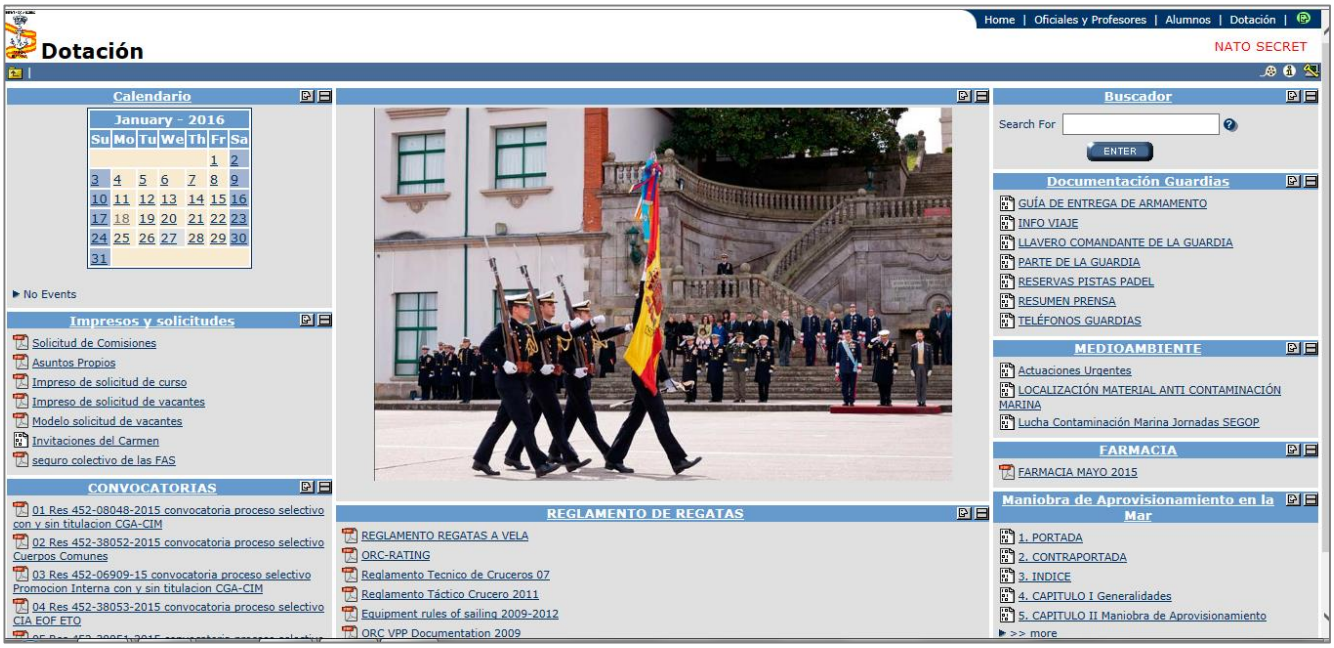

Figura 3-27 Captura: Subwise Dotación

El control de acceso a WISE se realiza por roles. Como se expuso durante el proceso de instalación, al no seleccionar la opción *Allow Self Registration*, el administrador del sitio es el único que puede registrar a los usuarios. Una vez registrados asignará a cada uno el rol que le corresponda en cada subweb. En función de este rol, el usuario ostentará permisos de acceso y, en ciertos casos, administración. Existen dos clases de roles, aplicadas a cada usuario en cualquiera de las subwise:

- ***Site Administrator:*** este rol otorga el control de subir información, así como de modificar los contenidos.
- ***User:*** simplemente tiene acceso a los contenidos, sin poder alterarlos.

Los usuarios se crean desde la página principal y, por defecto, aparecen como usuarios de esta misma, es decir, tienen acceso únicamente a la *Homepage*, la cual no requiere autenticación. Para proporcionarle acceso a alguna subwise específica, tras la creación de un nuevo usuario, se debe acceder a su configuración en la ventana *Access*. En ella, se nos presentará una lista con todos los usuarios. Para otorgar los roles al nuevo usuario, debemos buscar su nombre en esta lista y marcar la casilla con los roles que correspondan. Este proceso podría resultar laborioso o, incluso, dar lugar a errores, en el caso de disponer de una larga lista de usuarios.

Los usuarios creados para nuestro portal se muestran en la Figura 3-28. Ésta es una captura de los usuarios con acceso a la página principal, donde sólo el administrador (*siteadmin*) puede configurarla. Si accedemos al menú *Access* dentro de cada subwise, se observan los distintos roles o privilegios asignados, a cada uno de los distintos usuarios.

User				Roles	
			ID ↓↑	Email ↓↑	Site Administrator	User
			Carlosgval	[redacted]v@gmail.com	☐	☑
			Cristiansil	[redacted]@gmail.com	☐	☑
			Gestoso93	[redacted]@gmail.com	☐	☑
			Guest		☐	☑
			Guillerggam	[redacted]0@gmail.com	☐	☑
			Lantto	[redacted]@gmail.com	☐	☑
			Nercarey	[redacted]@gmail.com	☐	☑
			Pdodero	[redacted]@gmail.com	☐	☑
			alumno	[redacted]@gmail.com	☐	☑
			andrescampg	[redacted]@gmail.com	☐	☑
			careper	[redacted]1@gmail.com	☐	☑
			dotacion	[redacted]@gmail.com	☐	☑
			emergency		☐	☑
			profesor	[redacted]@gmail.com	☐	☑
			siteadmin	[redacted]@gmail.com	☑	☑

Figura 3-28 Captura: Usuarios asociados a la página principal del portal WISE

3.4.1 Configuración de Subweb WISE

Dentro de la configuración de cada subweb, disponemos de distintas opciones que se analizarán a continuación.

- ***Content***

Muestra todos los archivos subidos y objetos creados en el portal. Estos pueden modificarse, o incluso eliminarse. En la Figura 3-29 se muestran los contenidos de la página principal (constituye la primera subwise).

Import/Export | Page Layout | Content Layout | Site Map | Undo | Access

Contents

Type ↓↑	Title ↓↑	Size (KB) ↓↑	Date Created ↓↑	Date Modified ↓↑	Classification ↓↑	Responsible Person ↓↑
	Calendario	0	300203Z DEC 2015	052031Z JAN 2016	NATO SECRET	webmaster
	Enlaces de interés	0	300109Z DEC 2015	141820Z JAN 2016	NATO SECRET	webmaster
	Buscador	0	300147Z DEC 2015	130658Z JAN 2016	NATO SECRET	webmaster
	Info METEO	0	121822Z JAN 2016	122229Z JAN 2016	NATO SECRET	webmaster
	Acceso a la Escala de Oficiales	0	122243Z JAN 2016	122244Z JAN 2016	NATO SECRET	webmaster
	Aviso Terroristas	0	122309Z JAN 2016	141814Z JAN 2016	NATO SECRET	webmaster
	WELCOME	492	122330Z JAN 2016	122330Z JAN 2016	NATO SECRET	webmaster
	Deportes	0	130647Z JAN 2016	130649Z JAN 2016	NATO SECRET	webmaster
	Orden Diaria	0	130652Z JAN 2016	130657Z JAN 2016	NATO SECRET	webmaster
	Oficiales y Profesores	0	140643Z JAN 2016	180629Z JAN 2016	NATO SECRET	webmaster
	Alumnos	0	140658Z JAN 2016	141823Z JAN 2016	NATO SECRET	webmaster
	Dotación	0	140701Z JAN 2016	180629Z JAN 2016	NATO SECRET	webmaster
	Concienciación en CIBERSEGURIDAD	0	141432Z JAN 2016	141436Z JAN 2016	NATO SECRET	webmaster

CUT COPY REORDER DELETE

Add Objects Select the type of object you would like to Add (Brief Generator), then click on the ADD NEW button.

Figura 3-29 Captura de los contenidos publicados en el portal WISE

- ***Properties***

Las propiedades permiten modificar el título y las características del sitio. Además, empleando la opción *Application Icon*, se permite subir un archivo para logo del sistema WISE. En la Figura 3-30 se refleja la modificación del nombre de nuestro sitio (**Escuela Naval Militar).**

Figura 3-30 Captura de las propiedades de nuestro sitio WISE

- ***Page Layout***

Ofrece distintas posibilidades de diseño y colocación de los objetos. La aplicación presenta seis diseños. Hemos elegido la tercera opción (*Layout #3*), para situar una foto ilustrativa de la ENM en el centro de la página, en un tamaño mayor a los objetos que la rodean (Figura 3-31).

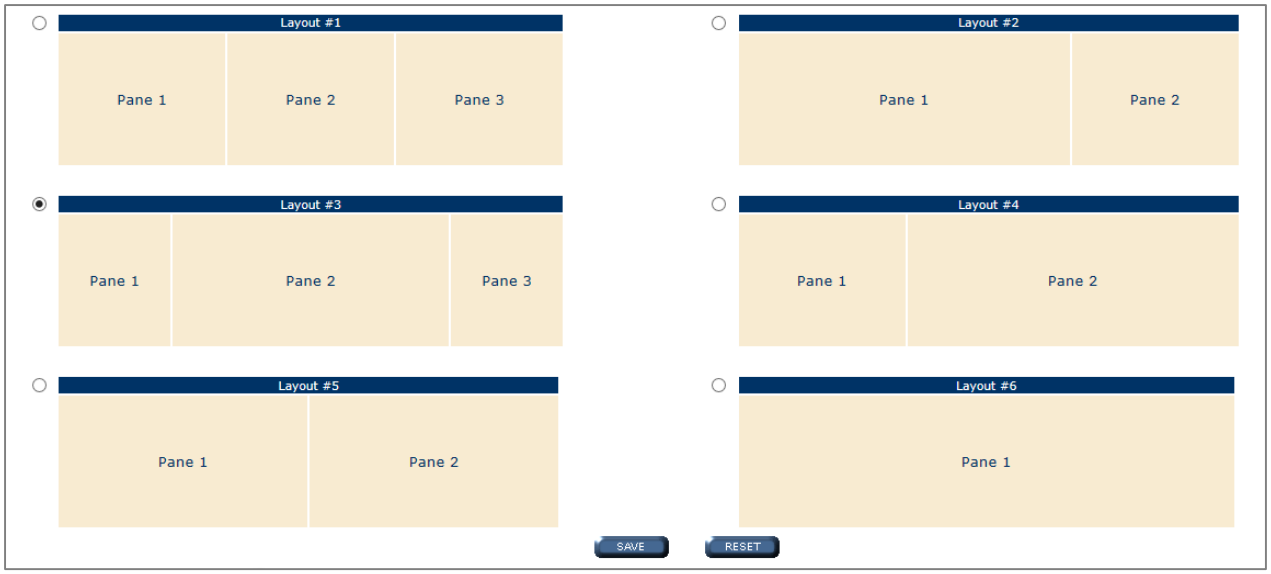

Figura 3-31 Captura: *Page Layout*

- ***Content Layout***

Muestra una tabla que se emplea para ordenar los objetos como se desee. Además, contiene una columna *Hidden*. Los objetos situados en ella permanecerán ocultos. El administrador suele emplear

esta columna en la etapa de diseño o para guardar alguna carpeta que pueda ser de interés el futuro (Figura 3-32).

Figura 3-32 Captura: Ejemplo de *Content Layout* para nuestro sitio WISE

- ***Site map***

La Figura 3-33 muestra una lista compuesta por todos los archivos subidos a la subwise *Homepage*. Esta lista permite desplegar los contenidos de las carpetas para una visualización más amplia.

Figura 3-33 Captura: Ejemplo de *Site map* para nuestro sitio WISE

- ***Access***

En *Access* podemos modificar los roles de cada usuario y las autorizaciones que tiene en cada subwise. En Figura 3-28 se muestra una captura de los roles de los distintos usuarios en la página principal. Como se puede observar, el usuario *siteadmin* ostenta los derechos de administración. El resto de usuarios sólo tienen derechos de invitado (*guest*). Una vez creados los nuevos usuarios, desde el menú *Access* de cada subwise, se le otorgarán los roles correspondientes. De esta forma, se puede otorgar los derechos de administración de cualquier subwise a cualquier usuario.

Este proceso resulta un poco rudimentario ya que el administrador debe otorgar individualmente los privilegios a cada uno de los usuarios. En el caso de existir un enorme número de usuarios esto sería una tarea muy laboriosa.

- ***UNDO***

La ventana *UNDO* da acceso a las últimas modificaciones realizadas. Para deshacer cualquier cambio, se debe seleccionar la acción en la lista y seleccionando *UNDO* (ver Figura 3-34).

Este comando permite deshacer la última acción realizada sobre un objeto. El administrador del sitio podría emplear este comando para eliminar una modificación no autorizada que haya realizado alguno de los usuarios. Cabe destacar que solamente se puede deshacer la última acción realizada sobre un objeto.

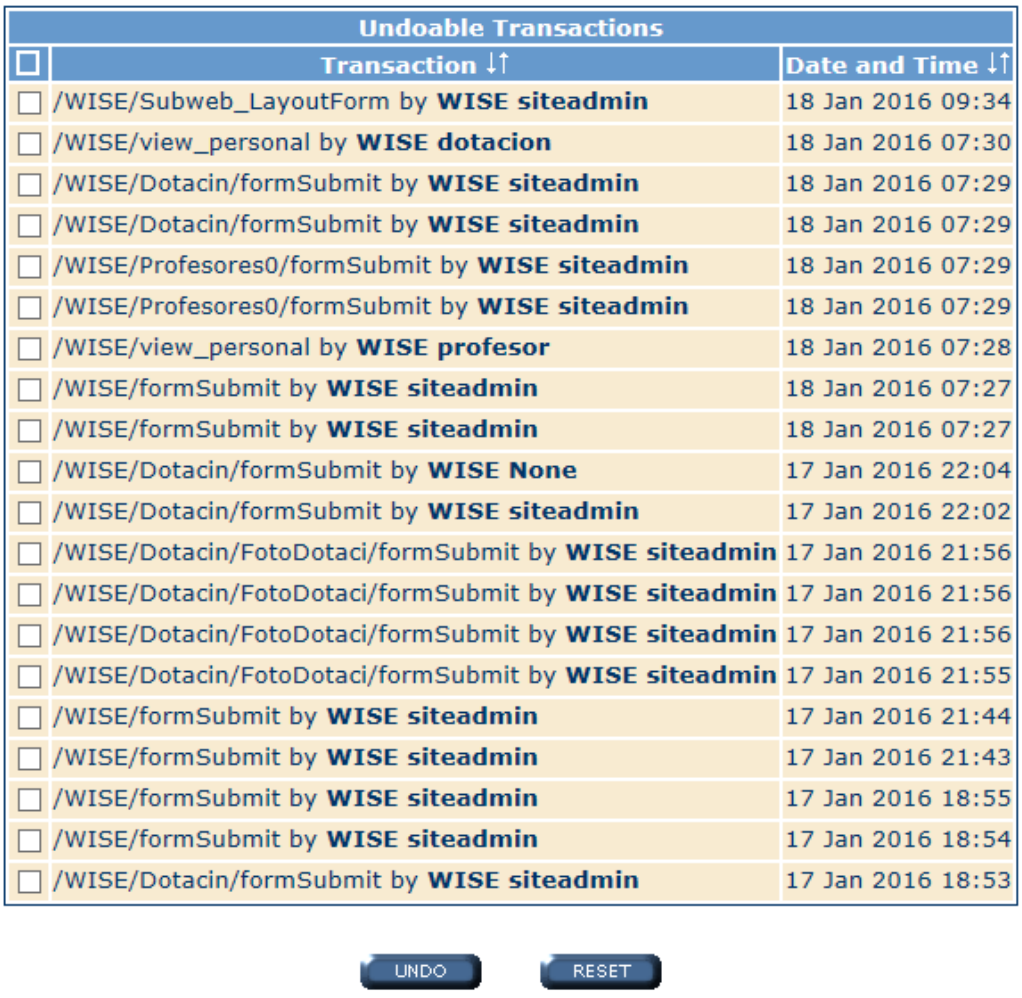

Figura 3-34 Captura: *Undo*

Para más información sobre el uso de WISE, en el Anexo III del presente documento se incluye una guía visual práctica para nuevos administradores, así como la configuración del equipo como servidor.

4 ANÁLISIS DE VULNERABILIDADES WISE

4.1 Presentación

Este capítulo detalla el análisis de seguridad realizado sobre el servidor WISE, instalado en la red local de laboratorios del Centro Universitario de la Defensa en la Escuela Naval Militar. En dicha red se sitúan diferentes equipos empleados por los alumnos del centro.

La explotación de vulnerabilidades es el objetivo de todo atacante. Para efectuar un ataque sofisticado, se debe dedicar el tiempo necesario a investigar el sistema en profundidad. El proceso de recogida de información o *gathering* ha sido realizado desde dos perspectivas:

1. La primera de ella es el análisis a nivel interno, desde la figura del administrador. Para ello se presentará la arquitectura del sistema y los fallos de seguridad o vulnerabilidades encontradas. Este análisis se denomina *Internal Footprinting.*
2. Posteriormente, se realizará un análisis de vulnerabilidades a nivel externo (*External Footprinting).* Para ello se emplearán algunas de las herramientas que incorpora la plataforma *Kali Linux*, así como la herramienta de análisis de metadatos *FOCA*, ambas presentadas en el segundo capítulo.

Para concluir este apartado, se describe el test de intrusión llevado a cabo en el servidor.

4.2 Análisis de vulnerabilidades a nivel interno *(Internal Footprinting)*

Para estudiar el grado de vulnerabilidad del sistema WISE y descubrir sus posibles fallos, los administradores deben conocer su funcionamiento y la estructuración de su base de datos. Además, conviene realizar análisis de manera continua, que permitan detectar errores o funcionamientos anómalos en el sistema, asociados a errores de programación o, en el peor de los casos, a ciberataques. A continuación procederemos a realizar un análisis desde el punto de vista del administrador del sistema.

El administrador de un portal web debe realizar un análisis y monitorización del sistema, con el objetivo de garantizar el nivel de seguridad correspondiente a sus contenidos y localizar posibles amenazas o ataques en curso sobre el sistema. Analizaremos la base de datos WISE, los puertos que el sistema tiene abiertos y, a continuación, se extraerán los metadatos contenidos en los archivos que en WISE se comparten.

4.2.1 Base de datos WISE

En primer lugar, analizaremos la base de datos del sistema y su protección. Esta base de datos se encuentra en el directorio generado durante la instalación: **C:Archivos de Programa(x86)\WISE.** Este directorio se estructura en distintas subcarpetas con los *plugins* de instalación y la información subida al gestor (Figura 4-1).

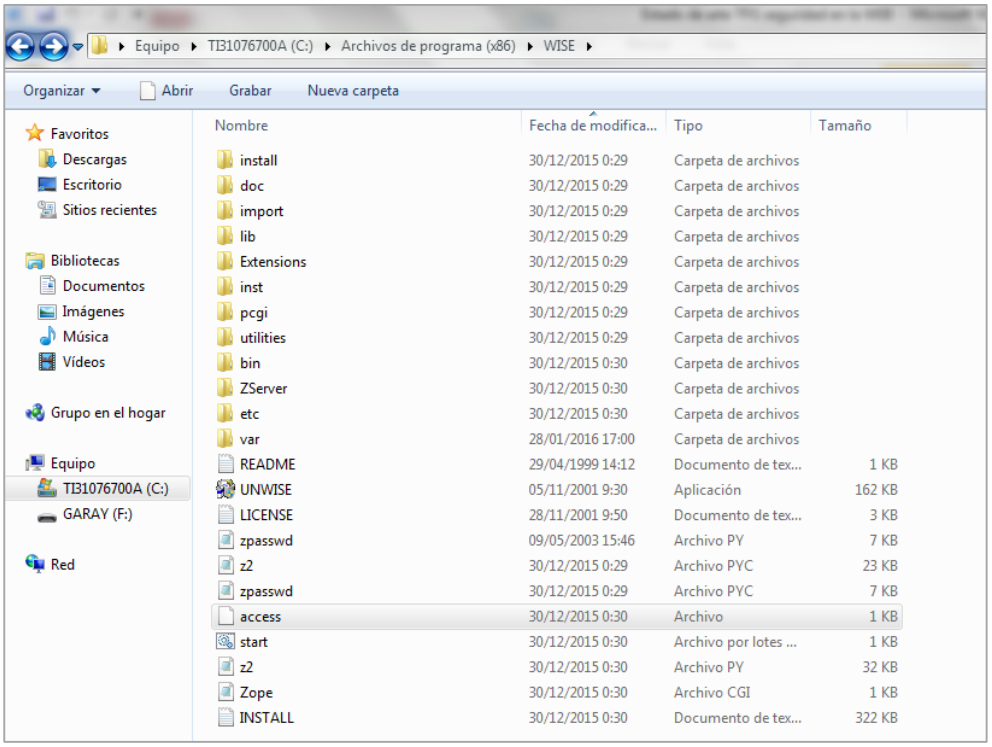

Figura 4-1 Captura: Base de datos WISE

En este directorio encontramos varios archivos de interés. El primero de ellos es *access*, donde se almacenan las credenciales del usuario *emergency*, creadas durante la instalación. Este usuario tiene acceso a WISE y su función es la de modificar las contraseñas en caso de pérdida u olvido. Si accedemos a este documento, podemos obtener su contraseña, cifrada con SHA (*Secure Hash Algorithm*).

Entrando en la carpeta **C:Archivos de Programa(x86)\WISE\var\FileobjectStore\WISE**, encontramos todos los archivos subidos a WISE, y además la información se estructura en carpetas para las diferentes subwises. Esta información se muestra sin cifrar, por lo que los documentos se

encuentran accesibles. Sin embargo, si algún documento se modifica desde el sistema de ficheros, WISE no permitirá acceder a él de nuevo (Figura 4-2). Esto supone una de las pocas medidas de seguridad que implementa el sistema.

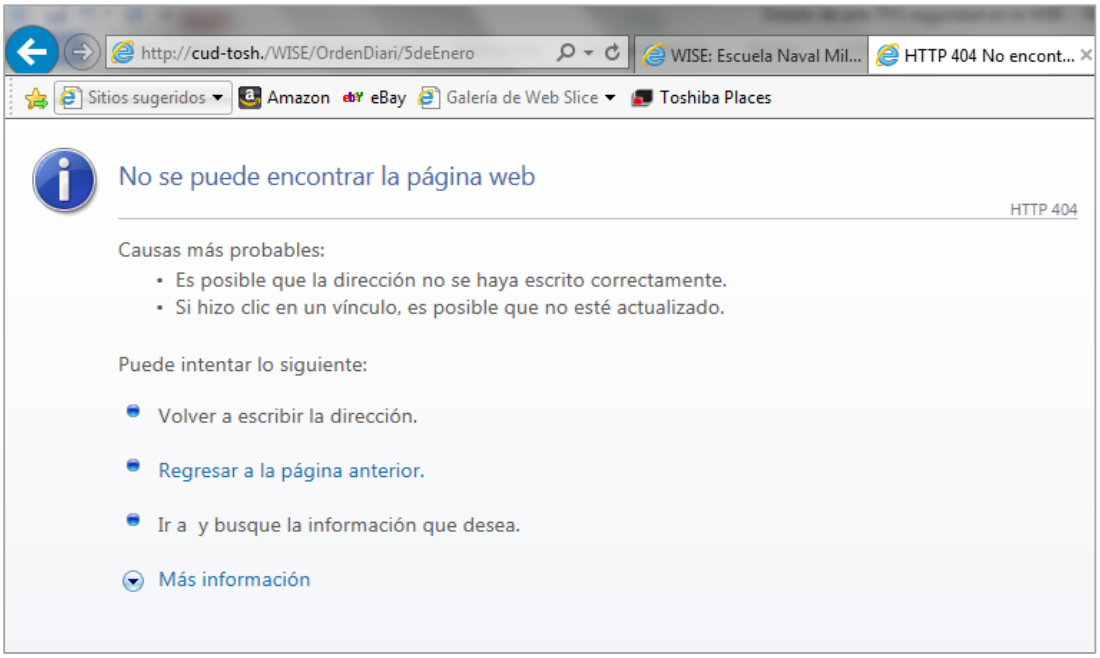

Figura 4-2 Captura: Error de acceso tras modificar un archivo del sitio WISE

Pero, sin duda, el fichero más interesante es *Data.fs* (almacenado en **C:Archivos de Programa(x86)\WISE\var*Data.fs***). Este archivo es el registro de todas las entradas y cambios realizados en el sistema. Además, en este documento, aparecen sin cifrar las contraseñas de los distintos usuarios WISE. En la Figura 4-3 se muestran las credenciales del usuario *Carlosgval*. En esta carpeta también encontramos la contraseña de los usuarios de instalación *siteadmin* y *emergency*, también sin cifrar.

Figura 4-3 Captura del archivo *Data.fs*: Credenciales de usuario

Este supone el punto crítico del sistema: en la propia guía de administración se señala como una de las mejoras previstas para las futuras actualizaciones del gestor. Además, si el archivo excede los 2GB de tamaño, el sistema WISE deja de funcionar. Para evitar esto, se propone a los administradores empaquetar este documento cada quince días.

4.2.2 Herramientas del sistema operativo para monitorización del sistema

La monitorización del sistema supone una buena práctica para la detección de intrusiones, observar las conexiones de red, los usuarios o dispositivos conectados. El sistema operativo Windows, sobre el que trabaja WISE, dispone de varias herramientas para ello, algunas de las cuales se presentan a continuación.

4.2.2.1 Conexiones

Las conexiones son un elemento muy importante a analizar. Como se muestra en la Tabla 4-1, existen herramientas del sistema Windows que permiten realizar un análisis de estas conexiones, ver los recursos compartidos, así como la configuración de la red.

Herramienta	Utilidad
Netstat	Puertos y conexiones abiertas
Net	Recursos compartidos
Route	Configuración de la red
Ipconfig	Interfaces de red

Tabla 4-1 Herramientas de análisis de datos y función

Para analizar las conexiones, abriremos el terminal CMD y ejecutaremos el comando *netstat –a*, que muestra los puertos y conexiones abiertas. En la Figura 4-4 se muestra un escaneo de puertos. Esta captura muestra el estado de los puertos (en escucha o espera) y las conexiones del equipo 192.168.1.138, conectado al puerto 80 de nuestro servidor. Estas conexiones corresponden a un ordenador del laboratorio (en la red LAN), realizando consultas al sitio WISE.

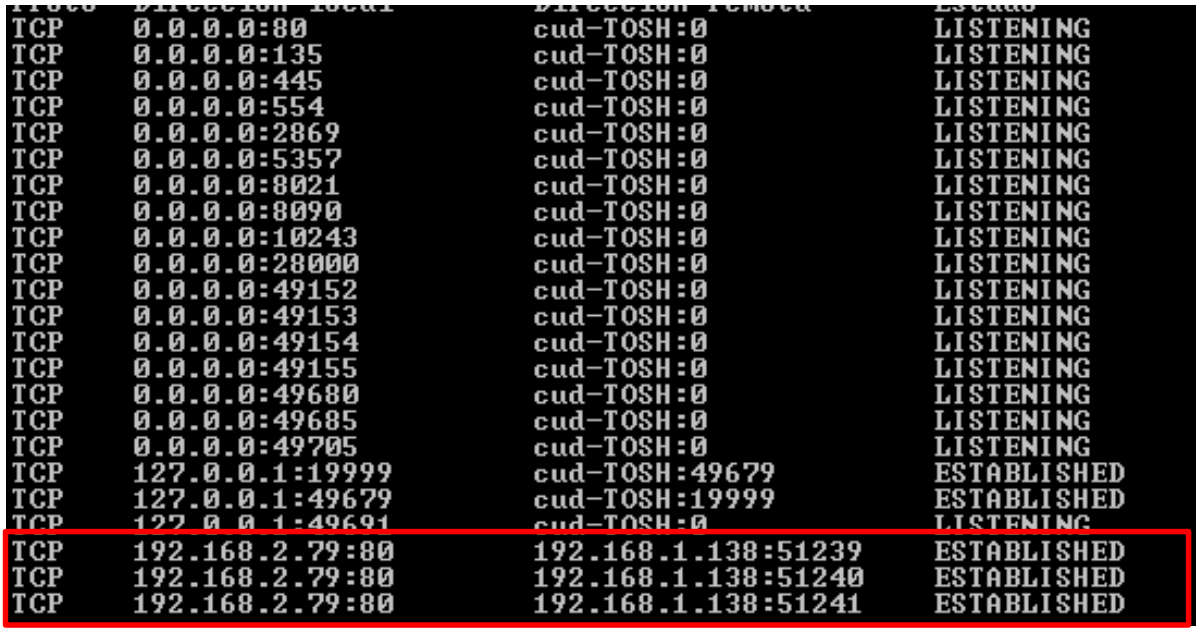

Figura 4-4 Puertos y conexiones abiertas capturados por *netstat –a*

Ahora cambiaremos el parámetro e introduciremos *netstat –es.* Este comando muestra las estadísticas de las conexiones. De esta manera, en la Figura 4-5 podemos ver los paquetes recibidos o descargados, los errores de dirección recibidos, etc. Un intento de ataque al servidor puede verse reflejado en estas estadísticas, en forma de errores, paquetes descartados o errores de dirección o encabezado recibidos.

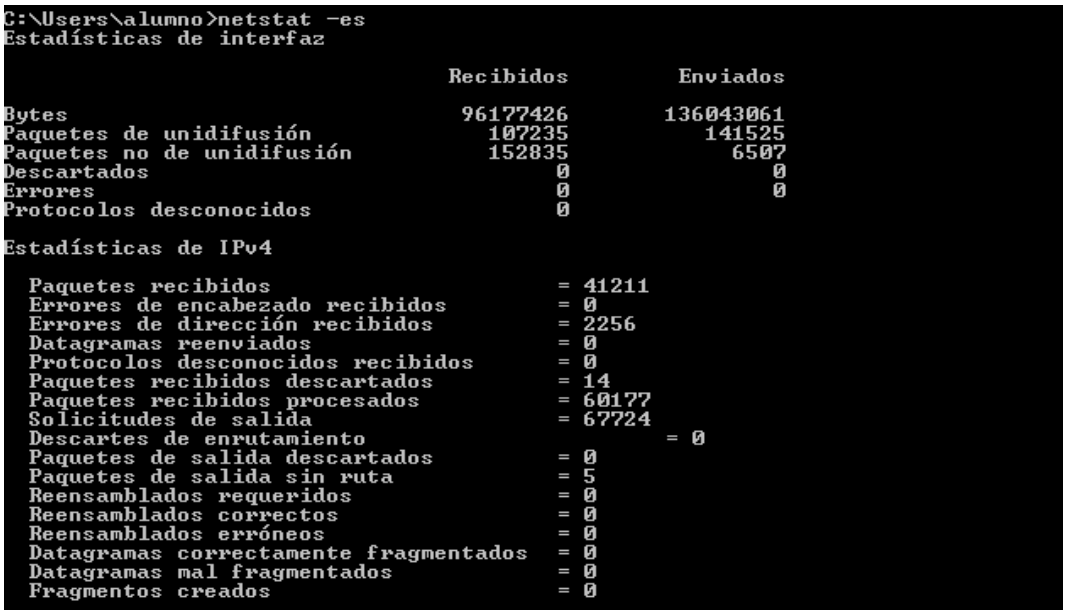

Figura 4-5 Estadísticas recopiladas con *netstat –es*

Y, por último, el comando *net share* (Figura 4-6), nos mostrará los recursos compartidos que tiene nuestro equipo.

Figura 4-6 Vista de los recursos compartidos con *net share*

4.2.1.2 Usuarios

El segundo punto importante a analizar son los usuarios del sistema. Para ello emplearemos el comando de Windows *nbtstat –n.* Este comando muestra los usuarios de NetBIOS. En este caso, el usuario es el ordenador que estamos analizando (Figura 4-7).

Figura 4-7 Listado de nombres de NETBIOS en el equipo local (*nbtstat –n*)

El comando *net users* permite ver los usuarios que tienen acceso al equipo. Sin embargo, no muestra si estos se encuentran activos o no. Como observamos en la Figura 4-8, el equipo posee cuentas de usuarios Administrador, alumno, cud, Invitado y Profesor. El acceso al servidor supone el punto más vulnerable del sistema, por lo que se deberá restringir al mínimo y necesario este acceso.

Figura 4-8 Captura: *net users* (Usuarios del sistema)

4.3 Análisis de vulnerabilidad a nivel externo *(External Footprinting)*

Durante el presente apartado se procederá a analizar las vulnerabilidades WISE desde un equipo externo. Este análisis se ha llevado a cabo mediante el empleo de una serie de herramientas que ofrece la distribución *Kali Linux*. En la Figura 4-9 se muestra el menú de herramientas que ofrece el sistema. Estas herramientas se ordenan según su función. Asimismo, se analizarán los metadatos de nuestro sitio WISE con *FOCA*.

La primera fase del análisis se centrará en la recogida de información WISE. Mediante el empleo de diversas herramientas se puede obtener la información necesaria para concretar las vulnerabilidades presentes en el sistema. Éstas, una vez hayan sido localizadas, pueden ser explotadas para realizar un ataque específico al gestor. Entre los datos recogidos, los más interesantes son: nombres de dominio, sistemas operativos, la versión del CMS empleada o los metadatos contenidos en los documentos publicados.

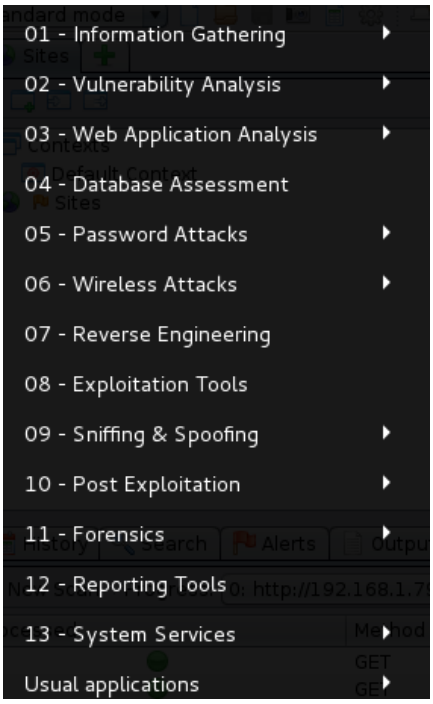

Figura 4-9 Categorías de las herramientas *Kali Linux*

4.3.1 Gathering con Kali Linux

Definido WISE como el objetivo de análisis, en la etapa de recogida de información, el ciberdelincuente emplea todas las herramientas disponibles para conseguir la información sobre las direcciones IPs de una compañía, el listado de usuarios, cuentas de correo electrónico, metadatos y rutas de acceso a documentos internos, entre otros. A continuación, emplearemos algunas de las herramientas proporcionadas por *Kali Linux* para este fin.

- ***Whatweb***

Esta herramienta nos permite identificar el tipo de sistema de gestión de contenidos que se ejecuta sobre el servidor, sirviendo como primer paso del análisis web, previo al ataque. De *Whatweb* extraemos la siguiente información:

El gestor de contenidos WISE trabaja en Windows (32 bits). Además, observamos que trabaja sobre ZOPE (el servidor de aplicaciones Python para el desarrollo de aplicaciones web) en su versión 2.6.4 de 32 bits:

- Version: Zope 2.6.4 (binary release, python 2.1, win32-x86)
- Module: python 2.1
- String: win32-x86

En la Figura 4-10 se muestra la información extraída por la herramienta.

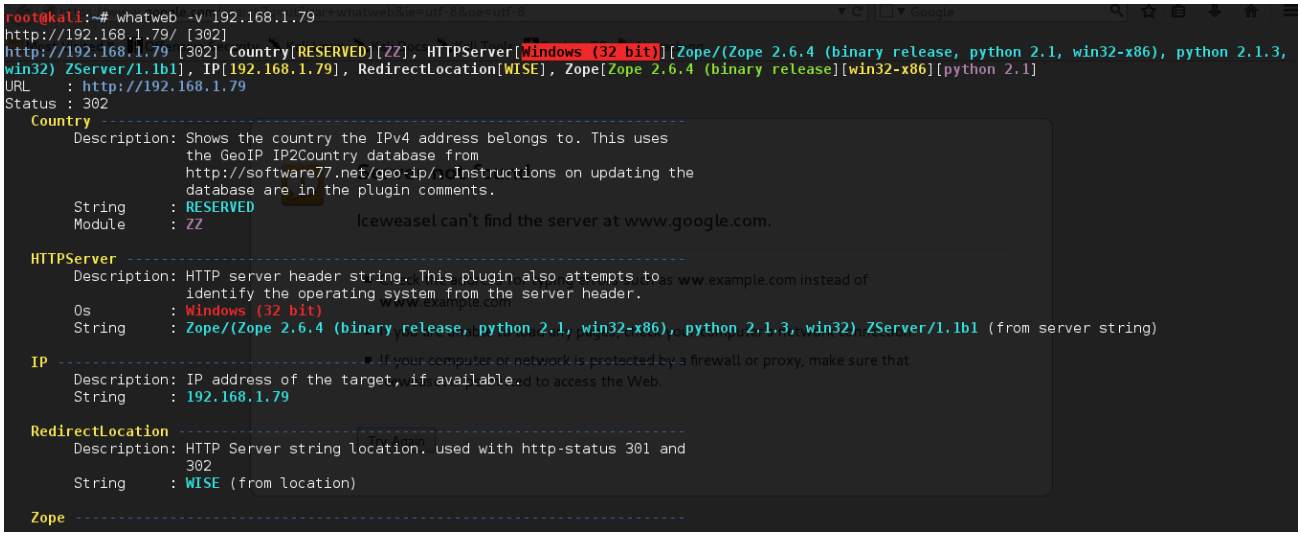

Figura 4-10 Escaneo de WISE con *Whatweb*

Conocida la versión en la que trabaja la aplicación web, realizaremos una búsqueda sobre las vulnerabilidades conocidas en dicha versión. Con una rápida búsqueda online encontramos la siguiente información sobre las CVE (*Common Vulnerabilities and Exposures*) que ZOPE 2.6.4 presenta [77]:

- Permite a atacantes obtener contraseñas debido a errores en la validación de contraseñas.
- Permite a usuarios remotos acceder a contenidos restringidos mediante a través de vectores no especificados.
- Permite la inyección de cabeceras HTTP mediante el comando de salto de línea (LF).
- Usuarios remotos no autenticados podrían realizar un ataque DoS.
- Presenta debilidades en la gestión de recursos del sistema.
- Presenta debilidades en la gestión de permisos y privilegios en el sistema.

- ***Zenmap***

Zenmap es el interfaz gráfico de la herramienta de código abierto *Nmap*, uno de los programas más empleados para el escaneo de puertos. En la Figura 4-11, se reflejan los puertos abiertos y, principalmente, los programas que se ejecutan sobre el puerto 80. El color rojo, en el que se muestran los puertos abiertos, indica que el sistema presenta más de 6 puertos abiertos.

Se puede observar que ZOPE se encuentra en servicio en el puerto 80. Por tanto, WISE se encuentra preconfigurada en dicho puerto.

Ports (15) | Extraports (985) | Special fields

Port	Protocol	State	Service	Method
80	tcp	open	http	probed
80	state	reason_ip		
80	state	state	open	
80	state	reason		
80	state	reason_ttl		
80	service	product	Zope httpd	
80	service	name	http	
80	service	extrainfo	python 2.1, win32-x86; python 2.1.3, win32) ZServer/1.1b1	
80	service	version	2.6.4 (binary release	
80	service	conf	10	
80	service	method	probed	
135	tcp	open	msrpc	probed
139	tcp	open	netbios-ssn	probed
445	tcp	open	microsoft-ds	probed
554	tcp	open	rtsp	table
2869	tcp	open	http	probed
5357	tcp	open	http	probed

Figura 4-11 Captura: Escaneo de puertos con *Zenmap*

4.3.2 Análisis de metadatos

Una vez conocidos los puertos y servicios activos en el servidor, procedemos a realizar un análisis de metadatos mediante el empleo de la herramienta *FOCA*. Esta herramienta también resulta de mucha utilidad para la recogida de toda la información. De los metadatos se puede extraer toda la información necesaria para realizar un *pentesting*. Para extraer los metadatos de los documentos colgados en el portal, una vez descargados, los arrastraremos directamente al programa *FOCA*. Una vez cargados, extraeremos los metadatos de cada archivo. Se debe señalar que, aunque esta herramienta puede obtener información muy valiosa en el caso de un test de intrusión en un entorno web real, en el portal WISE configurado para este TFG, los documentos subidos han sido seleccionados al azar y, por tanto, los resultados no son completamente verídicos. En el caso de un gestor de contenidos real, con el uso de la herramienta, se alcanzarían unos resultados más aproximados.

Como se muestra en la Figura 4-12, tras analizar más de 400 archivos descargados de WISE, obtenemos información muy interesante. Entre los datos extraídos se encuentran 20 usuarios, 23 tipos de *software* empleado, 4 carpetas de contenido y el sistema operativo sobre el que se encuentra instalado WISE.

Entrando en la ventana de usuarios, nos encontramos con los creadores de los documentos subidos en el gestor y la ruta donde se encuentran almacenados dichos documentos.

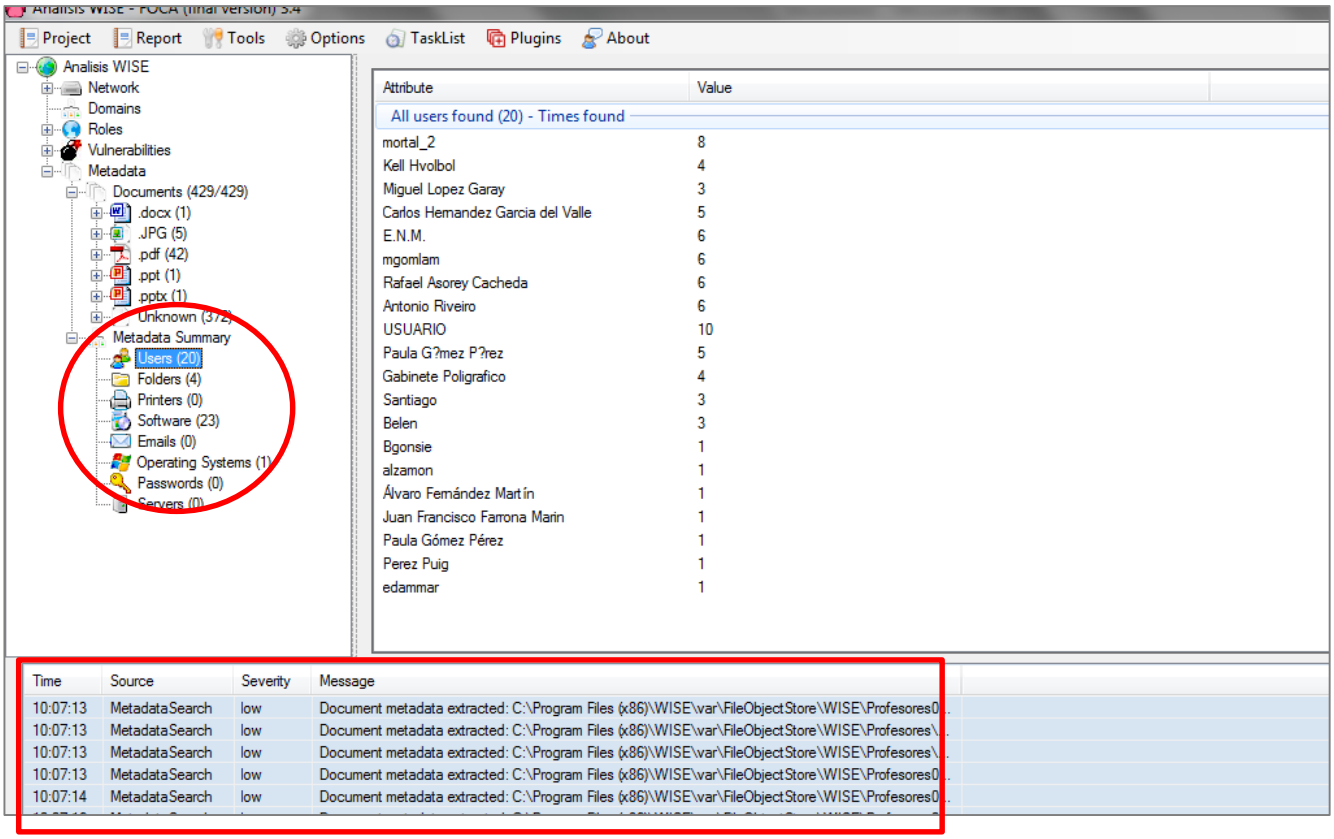

Figura 4-12 Análisis metadatos del sitio WISE con *FOCA*

Otro dato importante que nos muestra la aplicación es el *software* empleado. En los archivos analizados encontramos 23 tipos de *software* diferentes. Este *software* se corresponde con los programas empleados en el desarrollo de los documentos analizados. Tal y como se muestra en la Figura 4-13, se encuentran documentos realizados con distintos programas y con distintos sistemas operativos (Mac OS X y Windows).

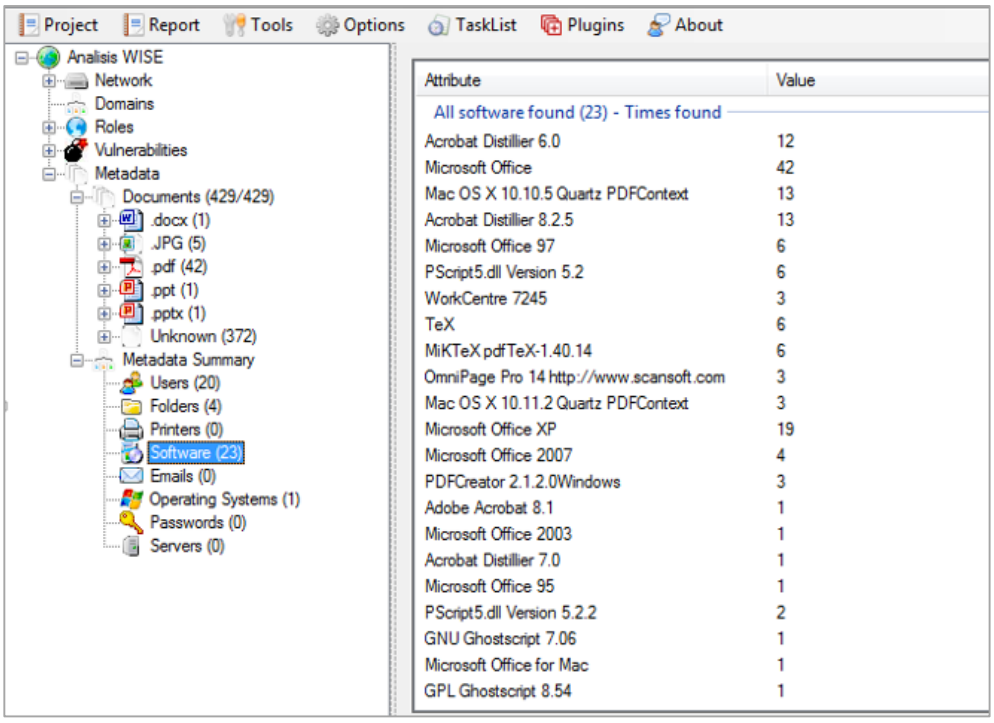

Figura 4-13 Extracción de información de software con *FOCA*

Analizando las imágenes (Figura 4-14), se puede extraer el modelo de *smartphone* utilizado (IPhone 5s), la fecha asociada e incluso información de localización si el dispositivo cuenta con GPS activado.

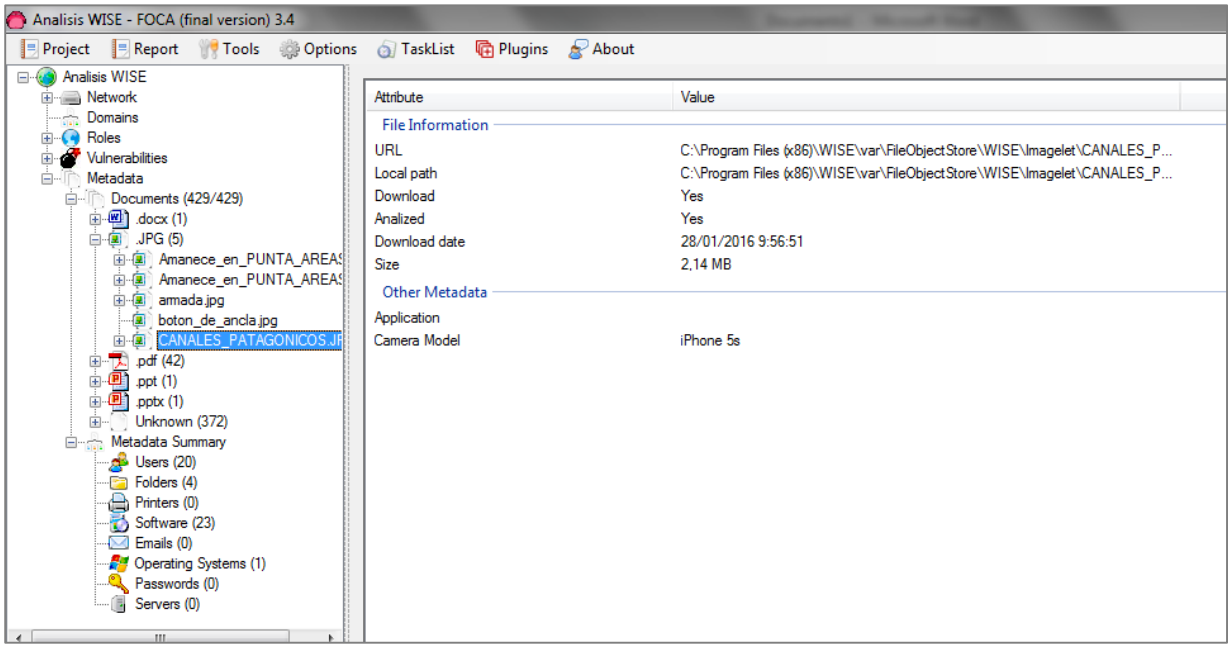

Figura 4-14 Análisis de los metadatos contenidos en imágenes publicadas en el portal WISE

En este caso, no se han obtenido impresoras relacionadas con los equipos, ni cuentas de correo electrónico o contraseñas. Sin embargo, los datos extraídos ya suponen información valiosa para un proceso de *pentesting*. Conocemos un importante número de personas relacionadas con la organización, qué usuario trabaja en cada equipo, etc. Esta información se podría utilizar para realizar un mapa de red y realizar un ataque dirigido.

4.3.3 Evaluación de vulnerabilidades

Tras la recogida de información, el segundo paso de la auditoría será la evaluación de las vulnerabilidades que presenta el sistema. Para ello se emplearán algunas de las herramientas de escaneo disponibles en *Kali Linux*. Estas herramientas simplifican mucho la búsqueda de vulnerabilidades en un servidor web específico. A continuación, se exponen las herramientas empleadas.

Antes de efectuar los ataques se ha desactivado el *firewall* de Windows y el antivirus del servidor. Aunque ningún servidor se encuentra en este estado de desprotección, estas medidas se han adoptado con el fin de identificar las vulnerabilidades de WISE.

4.3.3.1 BlindElephant

BlindElephant es una herramienta Python que se emplea para identificar la versión de aplicaciones web. Para ello el gestor de contenidos WISE, con *plugins* correspondientes a diferentes versiones de aplicaciones conocidas.

Al analizar WISE, como aplicación exclusiva del entorno militar, no encontramos coincidencia con los *plugins* de aplicaciones conocidas. Por tanto, el programa no encuentra vulnerabilidades correspondientes a la versión de nuestro gestor de contenidos (ver Figura 4-15).

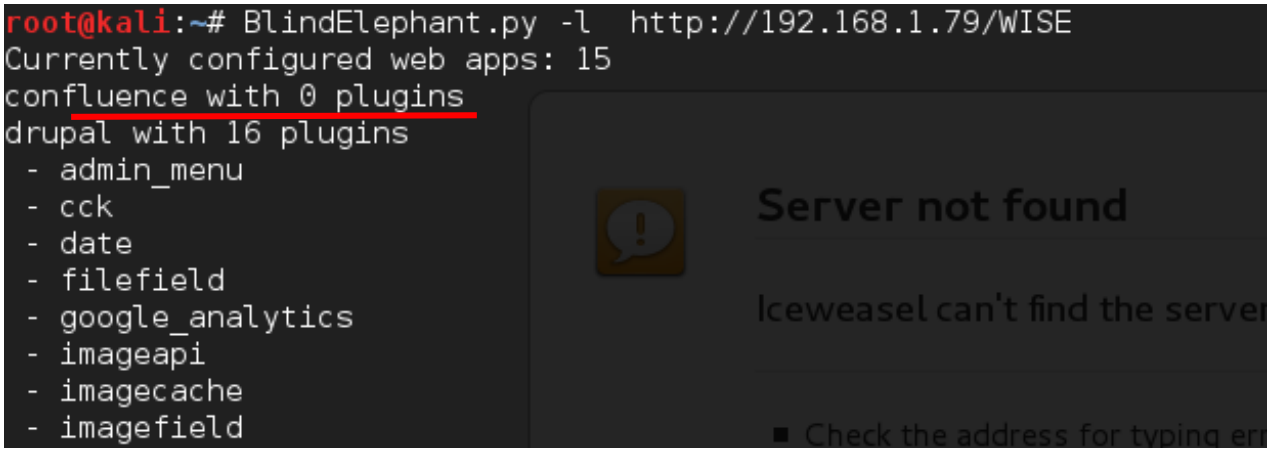

Figura 4-15 Análisis de WISE con la herramienta *BlindElephant*

4.3.3.2 Zed Attack Proxy (ZAP)

La herramienta ZAP efectúa una serie de pruebas y ataques sobre el sistema, descubriendo sus vulnerabilidades. Para comenzar el escaneo introduciremos la URL del portal WISE (ver Figura 4-16).

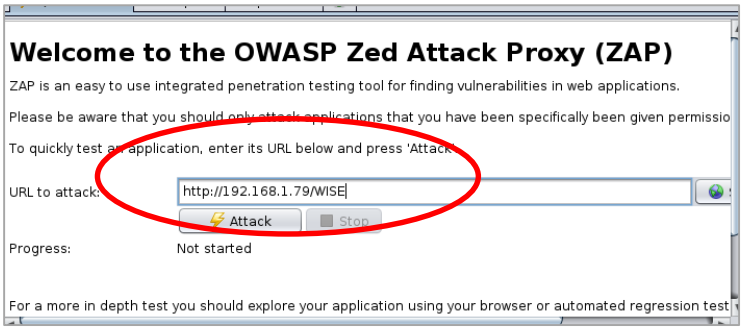

Figura 4-16 Captura: URL a analiza por ZAP

A partir de este momento, ZAP comienza un análisis automático, recorriendo todos los archivos y enlaces que se presentan en la web. Una vez analizadas todas las URL, muestra un enorme número de vulnerabilidades presentes en el sistema ordenadas por materia en siete carpetas (Figura 4-17). Además de definir estas brechas de seguridad, ZAP proporciona posibles soluciones para solventar el problema.

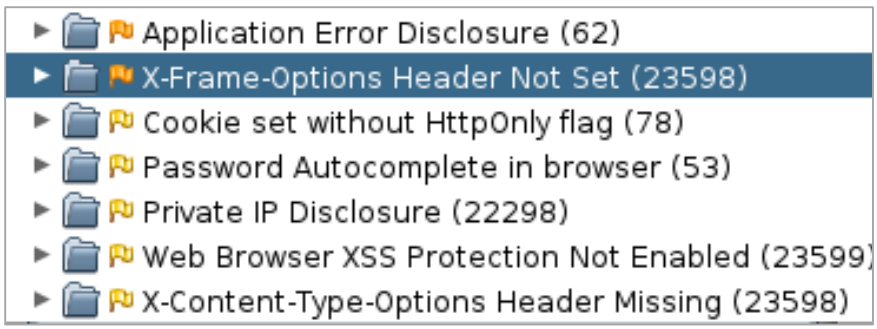

Figura 4-17 Listado de vulnerabilidades de nuestro portal WISE, localizadas con ZAP

Asimismo ZAP otorga una clasificación a las alertas de vulnerabilidades. En los resultados del análisis, mostrado en la Figura 4-18, podemos observar que las dos primeras alertas (*Application Error Disclosure* y *X-Frame-Options Header Not Set*) se clasifican con prioridad media (código de colores en las banderas), mientras que las cinco siguiente se clasifican con una prioridad baja. Esta prioridad

está directamente relacionada con el riesgo que supone la vulnerabilidad hallada. A continuación, se indicarán las vulnerabilidades más importantes.

***Application Error Disclosure*:** WISE contiene mensajes de error en los que puede revelarse información sensible como la ubicación del archivo en el que se encontró el problema. Esta información puede ser utilizada para lanzar nuevos ataques contra la aplicación web. La alerta podría ser un falso positivo si el mensaje de error fue encontrado al abrir algún documento. No obstante, en la URL de acceso a cada archivo se muestra la ubicación de cada documento. En la Figura 4-18 se muestra el error de acceso a un archivo. En la URL se puede ver la ubicación del documento.

Figura 4-18 Captura: Ubicación del PDF Orden Diaria_1 de Enero

***X-Frame-Options Header Not Set*:** No se incluyen cabeceras X-Frame en la respuesta HTTP. Esta cabecera sirve como protección a las páginas web contra ataques *ClickJacking*. El objetivo de este tipo es engañar al usuario mediante la introducción de una capa transparente colocada delante de un enlace o cuadro de diálogo, provocando que el usuario realice una opción sin conocimiento, o creyendo que está realizando otro fin. Para ilustrar este tipo de ataque, a modo de ejemplo, se podría aplicar este ataque para modificar los comandos realizados, camuflando la capa transparente en una votación online, la venta de seguir a alguien en *Facebook*, darle a *Me Gusta*, etc [78].

***Cookie set without HttpOnly Flag*:** Si la cabecera HTTPOnly se incluye en la respuesta, no se podrá acceder a las *cookies* desde un *script* enviado por un atacante. Además en caso de existir un ataque *Cross-Site Scripting* en el que un usuario acceda accidentalmente al enlace, el navegador no revelará la *cookie* al atacante.

Como se muestra en la Figura 4-19, en el caso de WISE, la *cookie* es accesible. En el caso de tratarse de obtener mediante *sniffing* la *cookie* de sesión, se podrían obtener las credenciales del usuario.

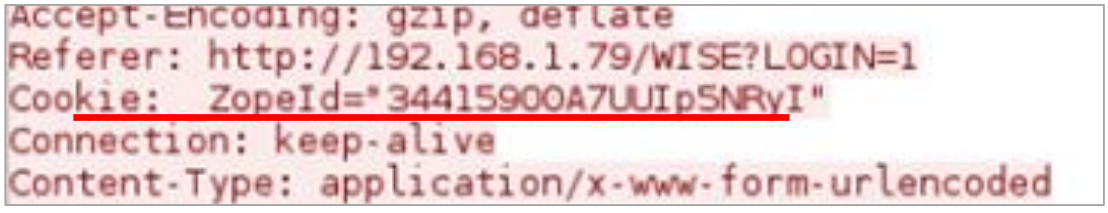

Figura 4-19 Captura: Obtención de *Cookie* con la herramienta *Wireshark*

Password Autocomplete in browser: Esta alerta nos indica que las contraseñas se pueden almacenar automáticamente en el navegador. Esto no supone un problema sino que se trata de una de las herramientas que proporcionan los navegadores actuales. Simplemente, el usuario debe evitar dejar sus credenciales en equipos ajenos.

Private IP Disclosure: En las respuestas HTTP se devuelve la IP privada del equipo. Esta alerta no debería extrañarnos ya que WISE se encuentra configurada en el PC indicado en el capítulo 3. La cabecera HTTP XSS permite al servidor web activar o desactivar el mecanismo de protección XSS del navegador. Sin embargo, esta alerta solamente supone un riesgo si las respuestas HTTP del servidor contienen información útil para XSS, como puede ser un contenido de texto. En el caso de WISE las peticiones HTTP tan sólo contienen acceso a recursos.

4.3.3.3 VEGA

Otra herramienta que nos ofrece *Kali Linux* para localizar las vulnerabilidades en el sistema es VEGA. Esta herramienta realiza un examen controlado sobre la estructura del sitio y proporciona información sobre el árbol de directorios y archivos. Como se muestra en la Figura 4-20 VEGA clasifica las vulnerabilidades obtenidas en tres niveles: *High*, *Medium* e *Info*. En este último escalón (*Info*) simplemente se informa sobre problemas encontrados, que podrían derivar en algún tipo de vulnerabilidad.

Utilizando esta herramienta se detectan nuevas vulnerabilidades. Entre ellas destacamos las siguientes:

Shell Injection: Los comandos de inyección se pueden explotar para obtener privilegios de usuarios en el sistema. Las inyecciones *Shell* más comunes ejecutan de forma remota procesos en el sistema, modifican contenidos o envían información de interés al atacante. Para explotarlas, existen distintos tipos de *exploits* en función del sistema operativo y su versión.

URL Injection: Que un sitio se encuentre comprometido por inyección URL significa que algún hacker podría crear enlaces a nuevas páginas en las que se presente contenido fraudulento o incluso manipular la base de datos usando direcciones URL.

Esta vulnerabilidad podría basarse en la posibilidad de introducir enlaces en WISE, no llegando a suponer un peligro para el sistema con una correcta gestión en los roles se otorgan a cada usuario.

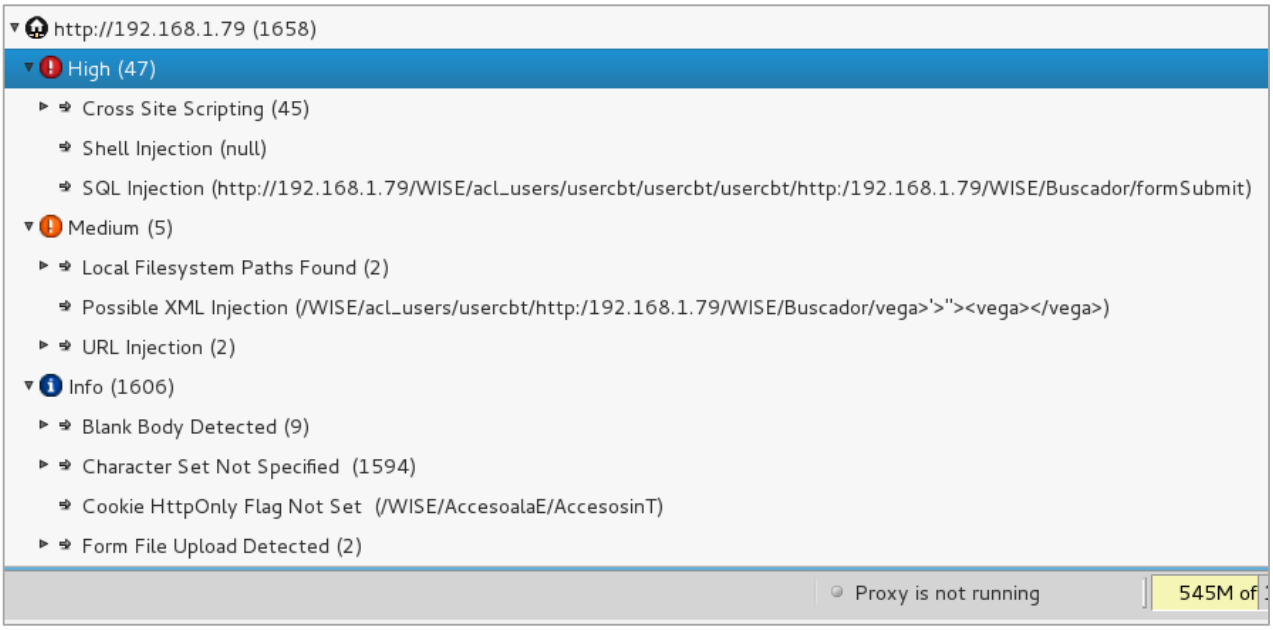

Figura 4-20 Captura: Herramienta VEGA

4.3.4 Pentesting

Una vez conocidas algunas de las vulnerabilidades que presenta WISE, procedemos a realizar un test de intrusión. El objetivo del *pentesting* es sortear las barreras y seguridades que implementa el gestor, para evitar accesos no deseados. Para ello, se ejecutarán una serie de *exploits* y se aplicarán técnicas de *sniffing*.

En primer lugar, se analizará la inyección SQL. Para ello, probaremos a introducir una comilla simple después de la URL de nuestro gestor (http://192.168.1.79/WISE'). Ésta es una de las inyecciones más básicas que nos sirve para probar si un sistema es vulnerable a este tipo de inyección. Como muestra la Figura 4-21, no se encuentra respuesta ante la URL introducida. Además, debemos destacar esta vulnerabilidad puesto que en la versión configurada para el portal WISE analizado, no se emplea una base de datos relacional, por lo que aunque el sistema presente alertas ante la posibilidad de este tipo de inyecciones, no suponen un riesgo.

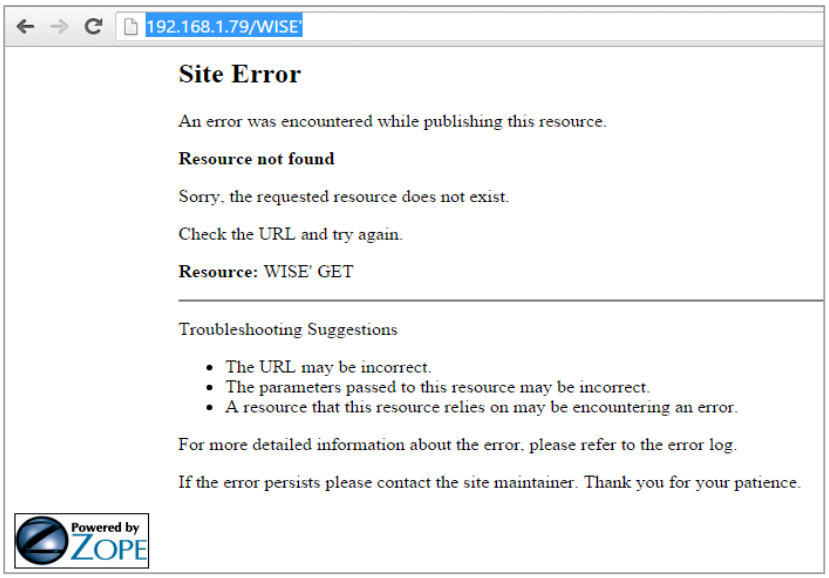

Figura 4-21 Captura: Error tras inyección SQL

De forma automatizada, utilizando la herramienta *sqlmap* que proporciona *Kali Linux*, obtenemos como respuesta, tras la comprobación de todos los parámetros, que WISE no es inyectable. Este dato ya era conocido puesto que WISE no emplea una base de datos relacional. Por tanto, al no emplear SQL, esta vulnerabilidad puede descartarse en la versión actual. Además, *Sqlmap* resalta que debe de existir algún tipo de protección en el sistema (ver Figura 4-22).

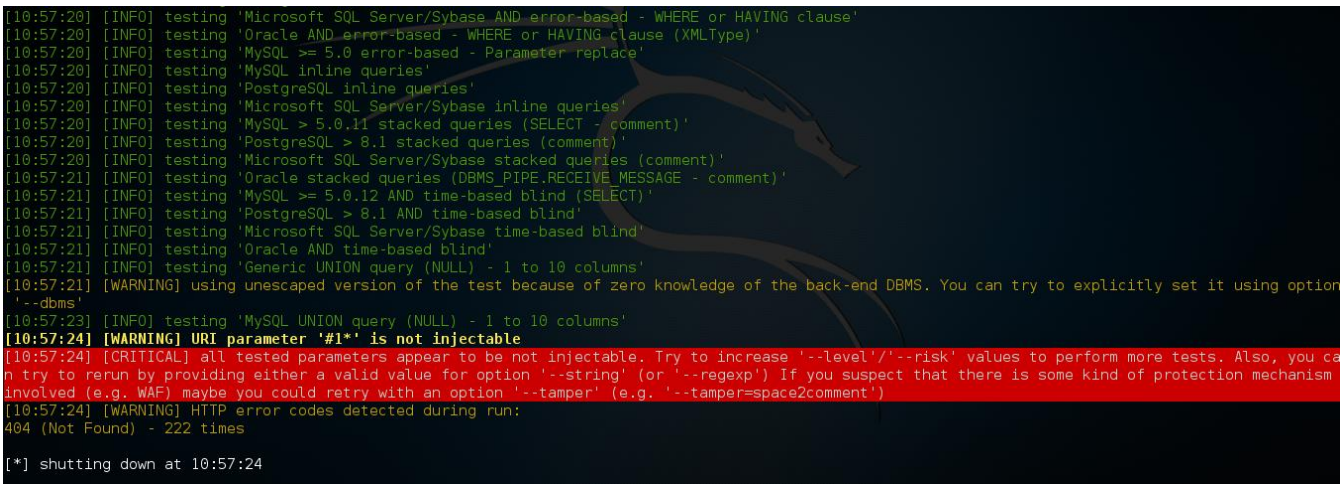

Figura 4-22 Resultado del empleo de la herramienta *Sqlmap* contra el portal WISE

4.3.4.1 Armitage

A continuación, emplearemos la herramienta *Armitage*, el interfaz gráfico de *Metasploit Framework*. Como se muestra en la Figura 4-23, el proceso de *hacking* con *Armitage* comienza como el proceso de *gathering*. En primer lugar, en el menú *Hosts* seleccionaremos *Nmap Scan* en el menú y realizaremos un *Quick Scan (OS detect)*. De esta forma identificaremos los hosts activos y sus sistemas operativos. A continuación, añadiremos la IP del servidor WISE.

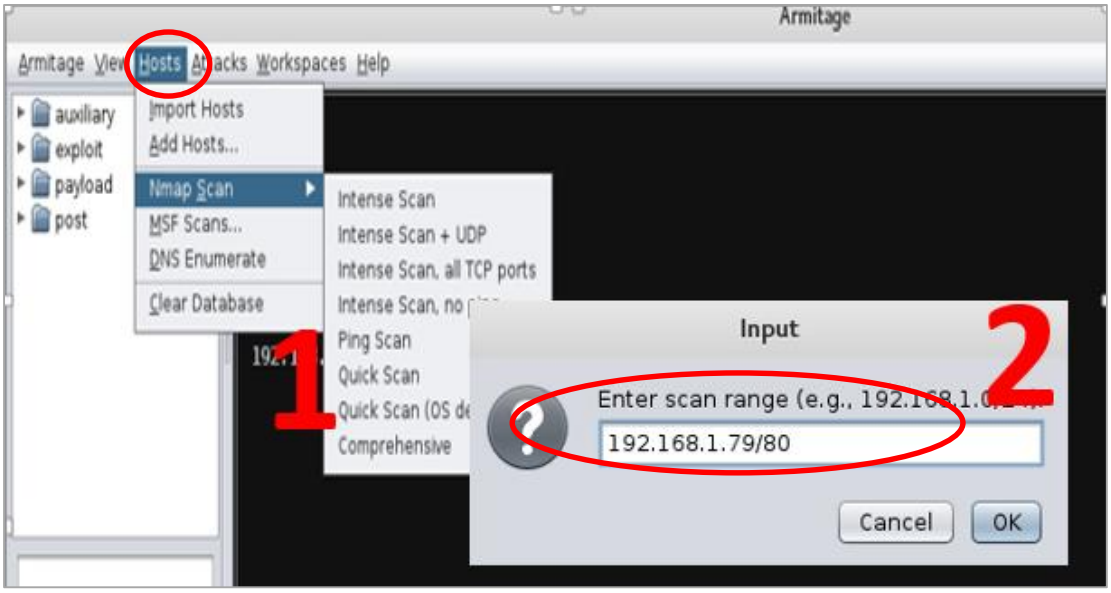

Figura 4-23 Definición del host a atacar con *Armitage*

Tras el escaneo, se presenta la ubicación del servidor y el puerto en el que se encuentra WISE. El sistema ya tiene localizado al servidor y, como se ilustra en la Figura 4-24, lo muestra con el icono de un PC Windows sobre su IP. Si sobre el icono pulsamos con el botón derecho y seleccionamos *Services*, nos mostrará un listado de los mismos en la ventana inferior.

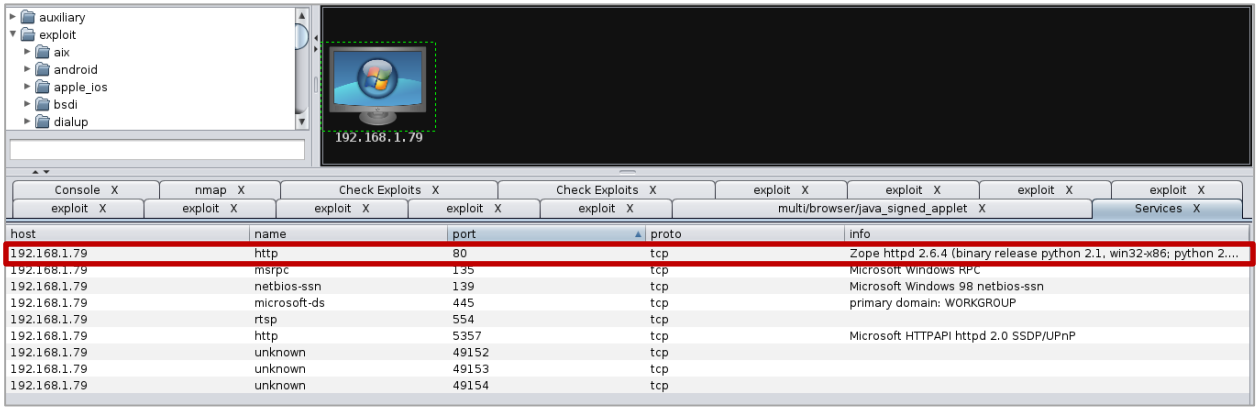

Figura 4-24 Captura: Host 192.168.1.79 con *Armitage*

Una vez identificado WISE en el puerto 80 y el servicio HTTP, el siguiente paso será atacar al sistema empleando los *exploits* HTTP que proporciona *Armitage*. Para ello, pulsando con el botón derecho sobre el equipo y seleccionando *Attack*, se nos presenta una gran lista de *exploits*, ordenados por categorías. Si se conoce con certeza algún *exploit* que vulnere las seguridades de WISE, se puede emplear directamente. Sin embargo, *Armitage* permite ejecutar una prueba con un gran número de ataques a la vez y descubrir así los *exploits* a los que WISE es vulnerable *(Attack\Http\check exploits)*. Una vez seleccionada esta opción, la herramienta nos presenta, en la ventana de diálogo, el resultado de la prueba de cada uno de los *exploits*. En la Figura 4-25, se refleja este proceso, donde Armitage

muestra los *exploits* inválidos, aquellos que no han podido ser comprobados o los candidatos a vulnerar el sistema.

Una vez realizada esta primera aproximación y descartada una gran parte de los exploits, procedemos a comprobar manualmente todos aquellos que, o bien no han podido comprobarse, o han sido señalados como explotables. Como se muestra en la Figura 4-25, la herramienta dispone de un buscador que facilita la localización de cada uno de los *exploits*, una vez conocido su referencia.

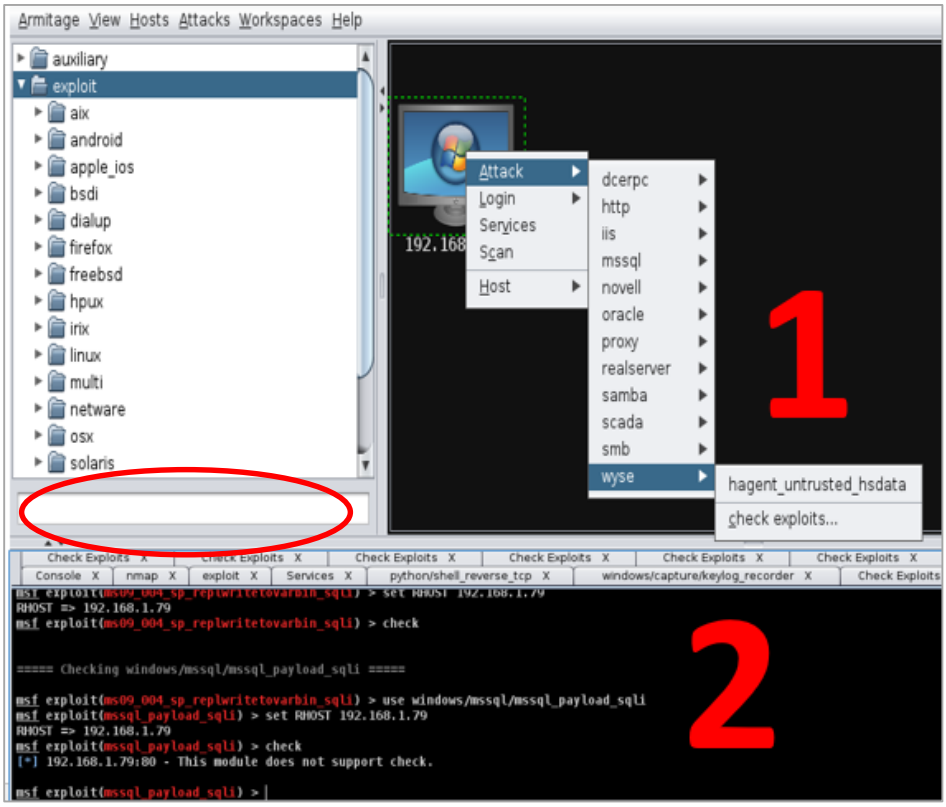

Figura 4-25 Captura: Comprobación de *exploits* con *Armitage*

Empleando el buscador, comprobaremos cada uno de los *exploits*. En la Figura 4-26 se refleja el ataque ejecutado por *processmaker_exec*. Este *exploit* intenta acceder a WISE creando un usuario con el rol de administrador, para posteriormente autenticarse como *admin*. Sin embargo, el *exploit* falla.

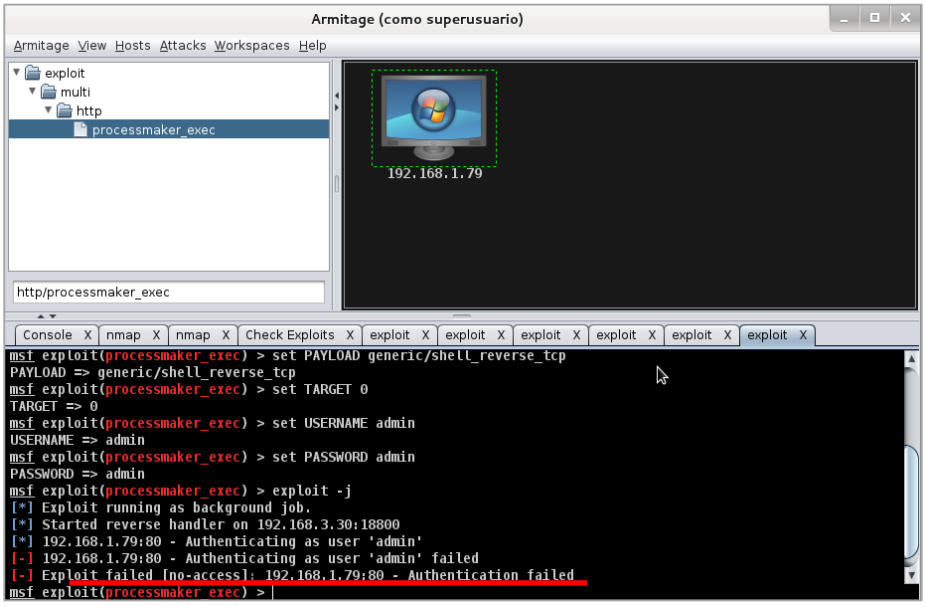

Figura 4-26 Ataque utilizando el *exploit http/processmaker_exec*

Tras comprobar los posibles *exploits* indicados por *Armitage*, no se consigue vulnerar el equipo. Varios de los *exploits* son desechados por el servidor (Figura 4-27), otros por el sistema operativo (Figura 4-28) y por último se presentan varios que, sin una razón conocida, fracasan en el intento de vulnerar el servidor (Figura 4-29).

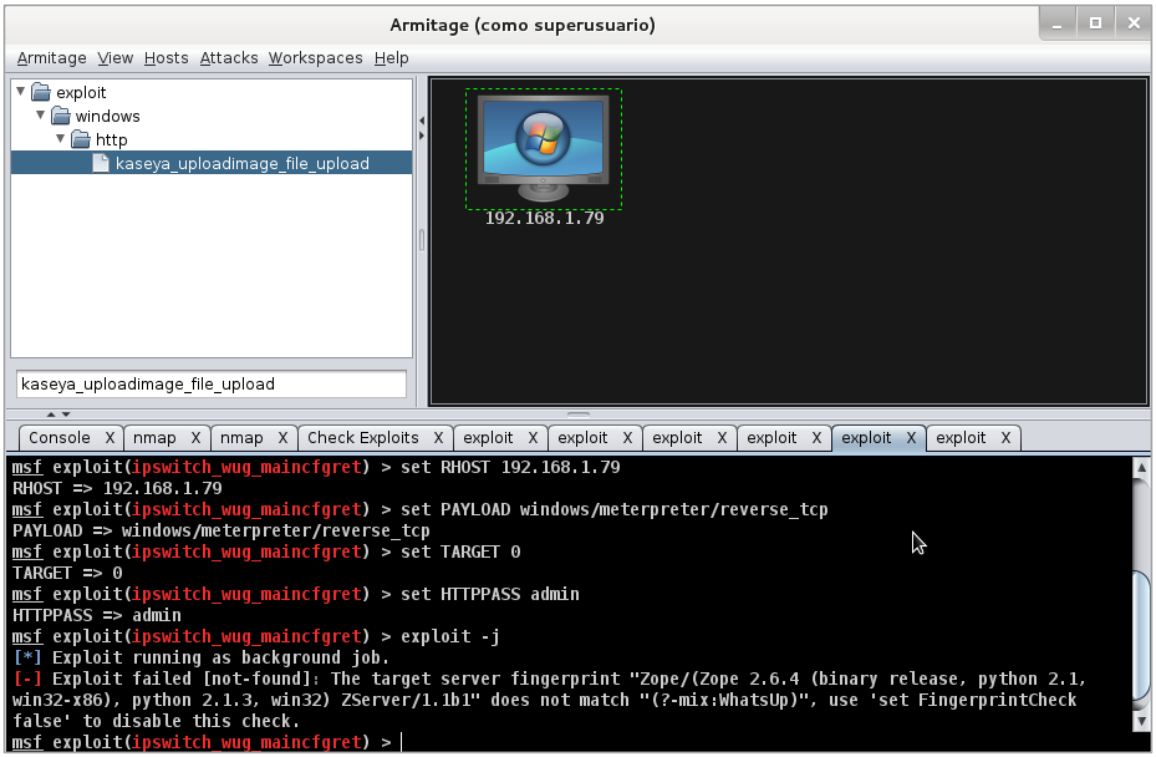

Figura 4-27 Ataque al portal WISE con el *exploit kaseya_iploadimage_file_upload*

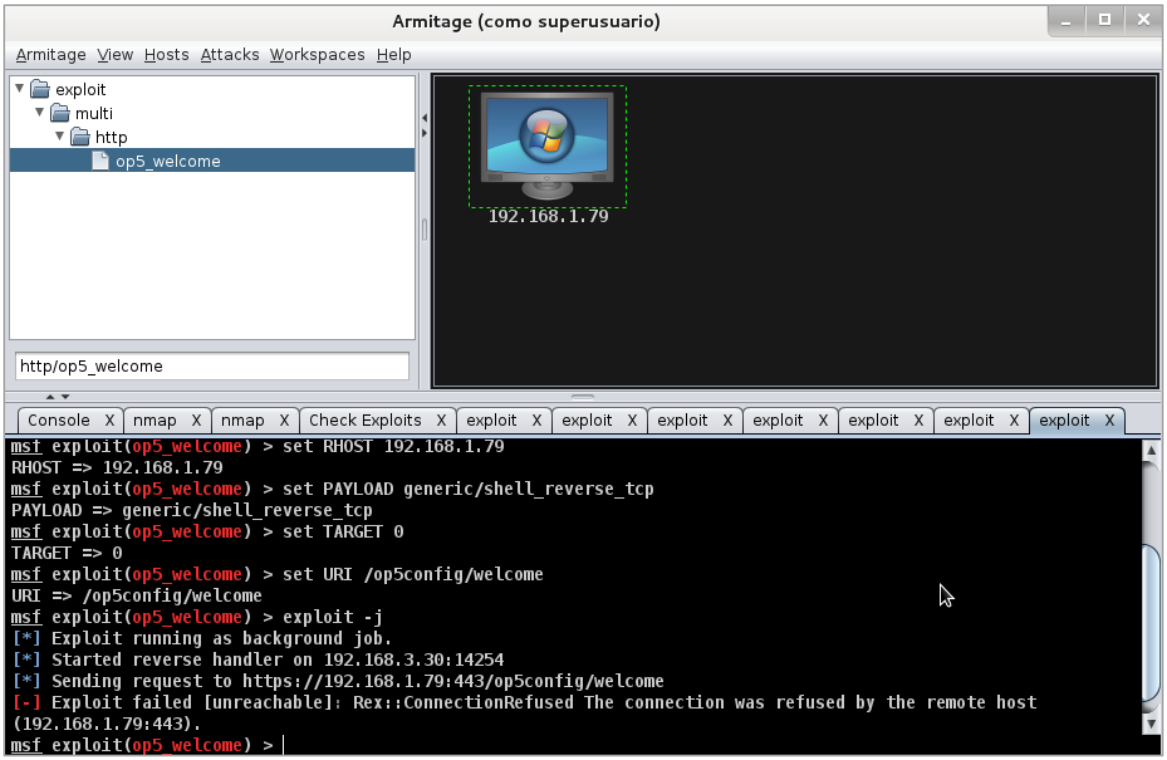

Figura 4-28 Mensaje obtenido al atacar el sitio WISE con el *exploit http/op5_welcome*

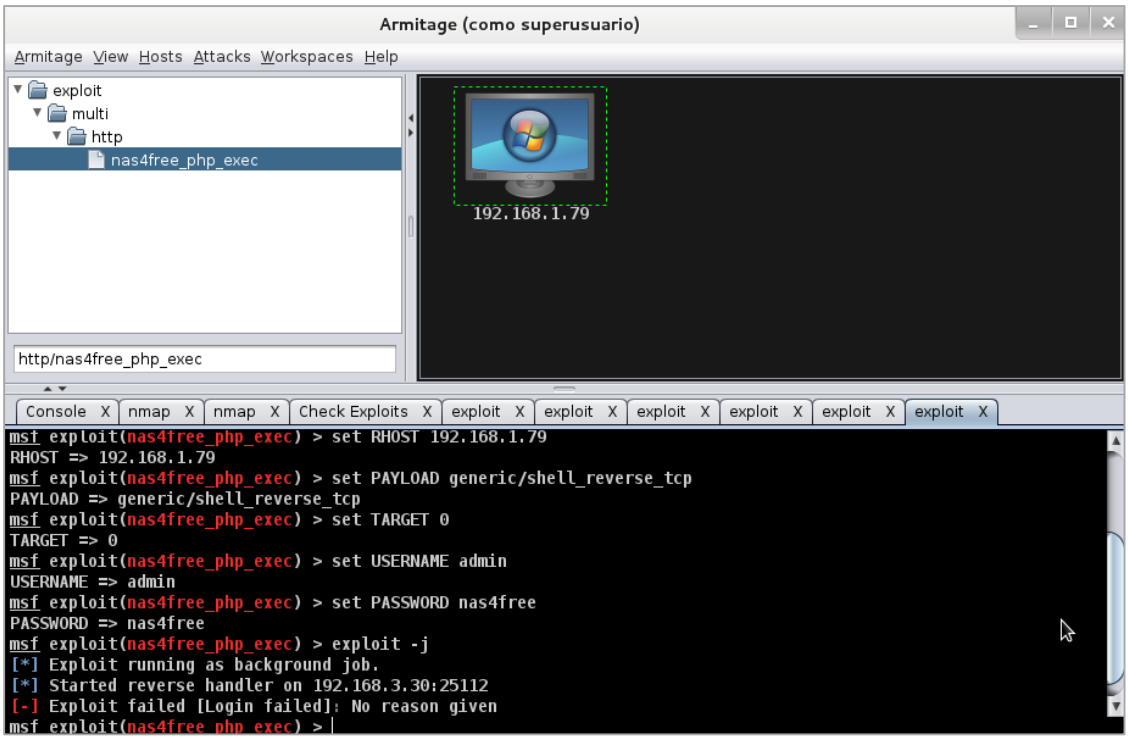

Figura 4-29 *Exploit Failed (No reason given)* tras el ataque con *http/nas4free_php_exec*

Tras analizar los distintos *exploits* que presenta la herramienta *Armitage*, descartamos esta vía de acceso al sistema. A pesar de las vulnerabilidades obtenidas tras los escáneres, al ser un gestor de contenidos no mantenido desde el año 2001 y, además, desarrollado en el ámbito de la OTAN y empleado en el ámbito militar, resulta complicado encontrar *exploits* que permitan el acceso al sistema, puesto que estos no son publicados.

4.3.4.2 Wireshark

Para interceptar el tráfico que avala entre el servidor y un equipo específico, se empleará la técnica *Man in the middle*. Por ejemplo, un cliente conectado a una red WIFI, podría ser objeto de este ataque de forma muy sencilla.

Para comenzar a interceptar el tráfico, abrimos *Wireshark* y seleccionamos el interfaz *eth0* para comenzar la captura en la red local. A continuación, se debe seleccionar el modo promiscuo. De esta forma, el equipo analizará todos los paquetes que circulan por la red sin importar el destino. Una vez comienza a capturar el tráfico, filtrando por la dirección IP del servidor (192.168.1.79), recibiremos los mensajes dirigidos al portal WISE (ver Figura 4-30).

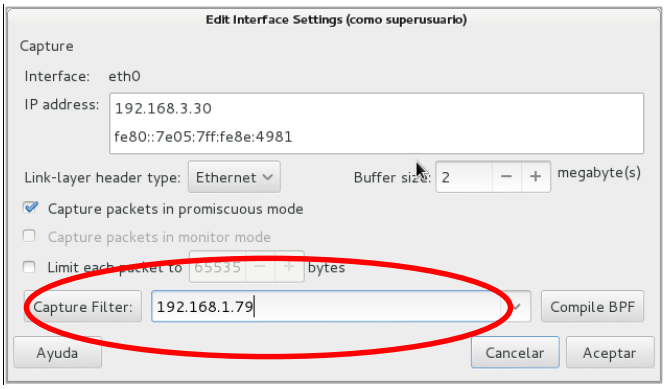

Figura 4-30 Captura: Filtrado de IP del portal WISE

Ya seleccionado el modo de análisis, *Wireshark* comienza a capturar todos los paquetes que se dirigen a la IP especificada (Figura 4-31). Cada una de estas líneas se corresponde con un paquete capturado. De cada uno de ellos, *Wireshark* muestra su tiempo de captura, destino, protocolo, longitud, etc.

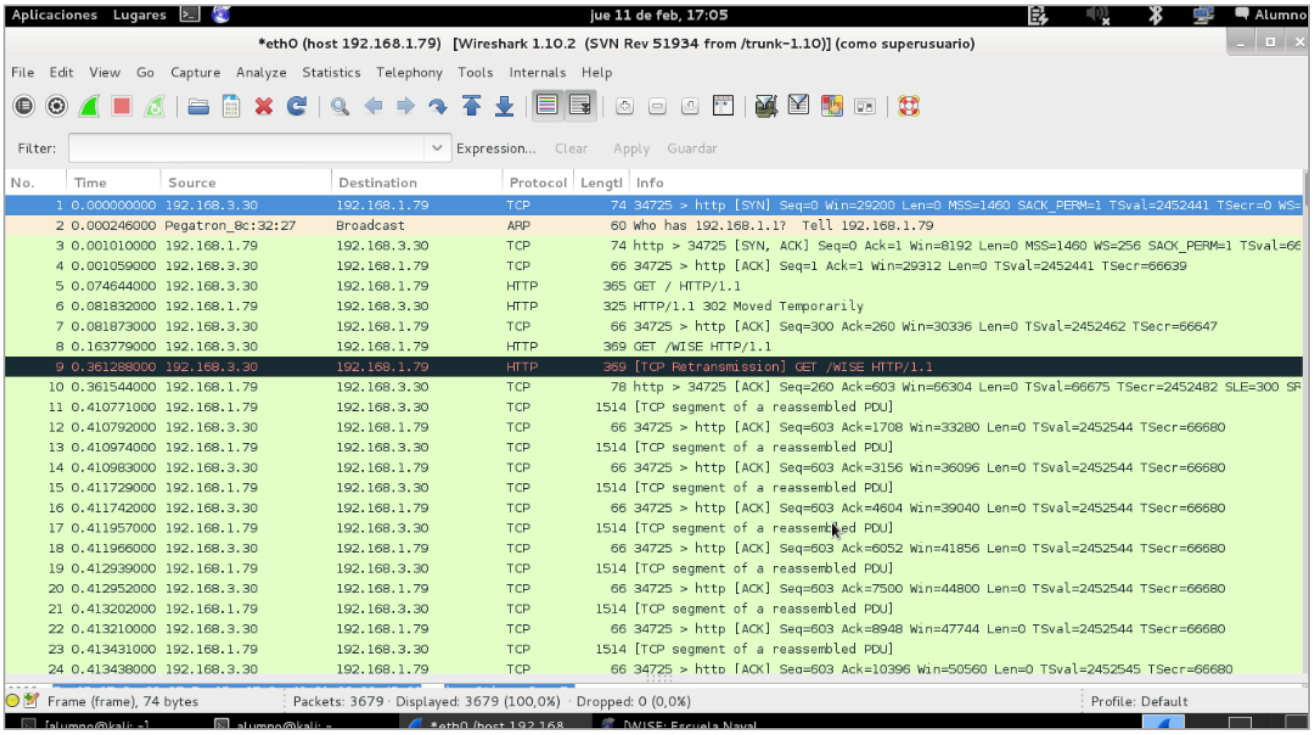

Figura 4-31 Captura: Tráfico capturado por *Wireshark*

Seleccionando alguno de los paquetes y haciendo clic en *Follow TCP Stream*, se nos presenta detalladamente el contenido completo de la captura. En cada uno de estos paquetes se muestra el usuario y la contraseña de la persona que realiza la acción. De esta forma, como se refleja en la Figura 4-32, en apenas unos segundos se obtiene la clave del administrador WISE.

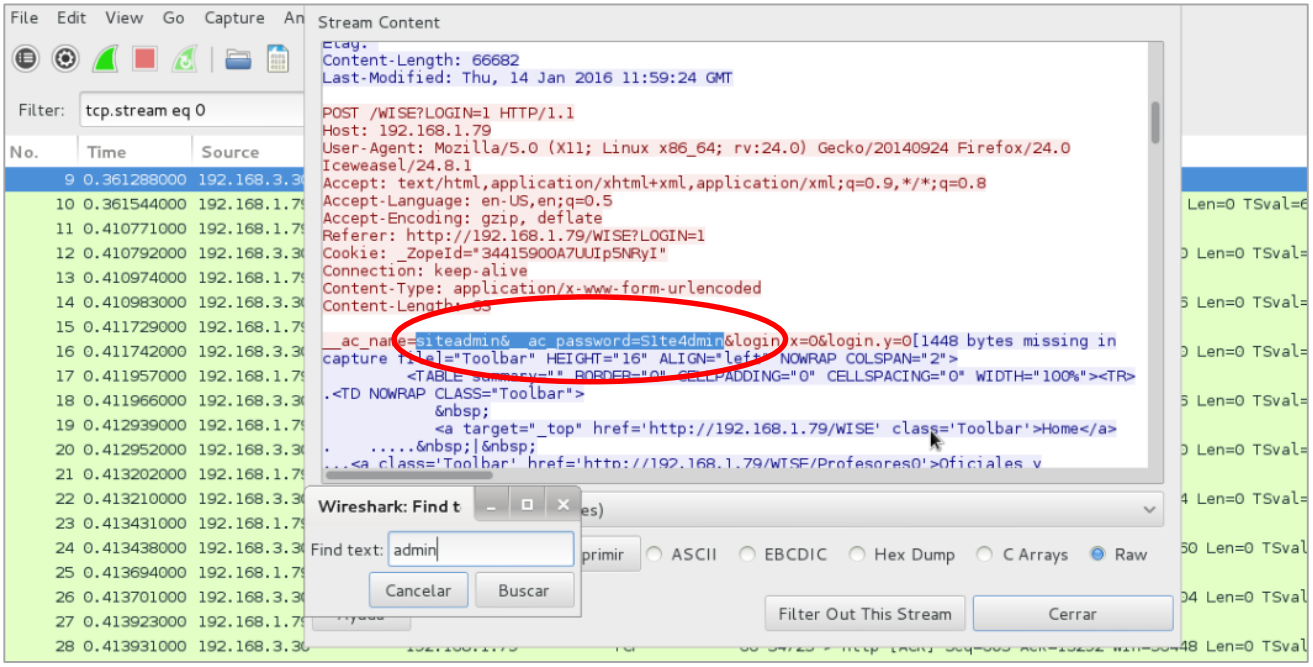

Figura 4-32 Captura: Obteniendo la contraseña del administrador con *Wireshark*

Mediante *sniffing* obtenemos las credenciales *siteadmin* que otorgan derecho de acceso y configuración del portal. Estas credenciales pueden emplearse para infinidad de acciones. De la misma forma, todos los paquetes se transmiten sin cifrar. En la Figura 4-33 se muestran los datos de un usuario creado por el administrador.

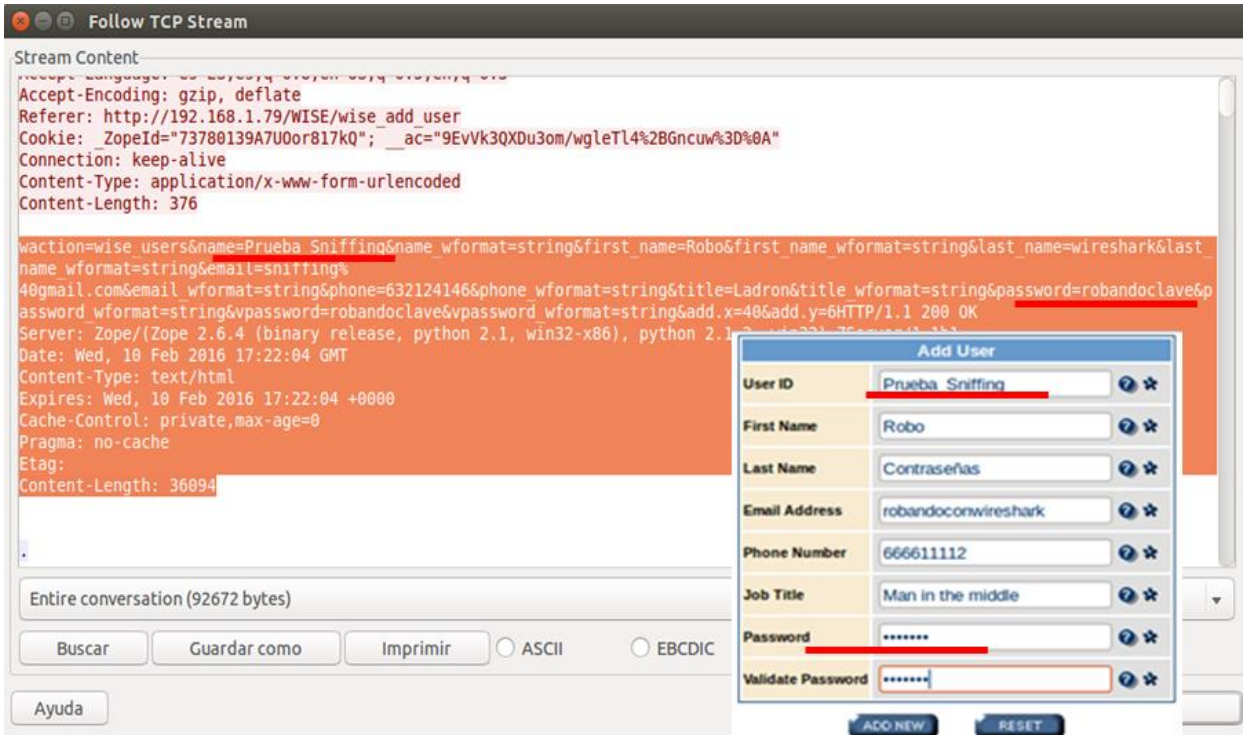

Figura 4-33 Captura: Obteniendo los datos de un nuevo usuario con *Wireshark*

Asimismo, todos los procesos realizados sobre el gestor quedan reflejados. En la Figura 4-34 se observa la modificación del mensaje de bienvenida que muestra WISE en su página principal.

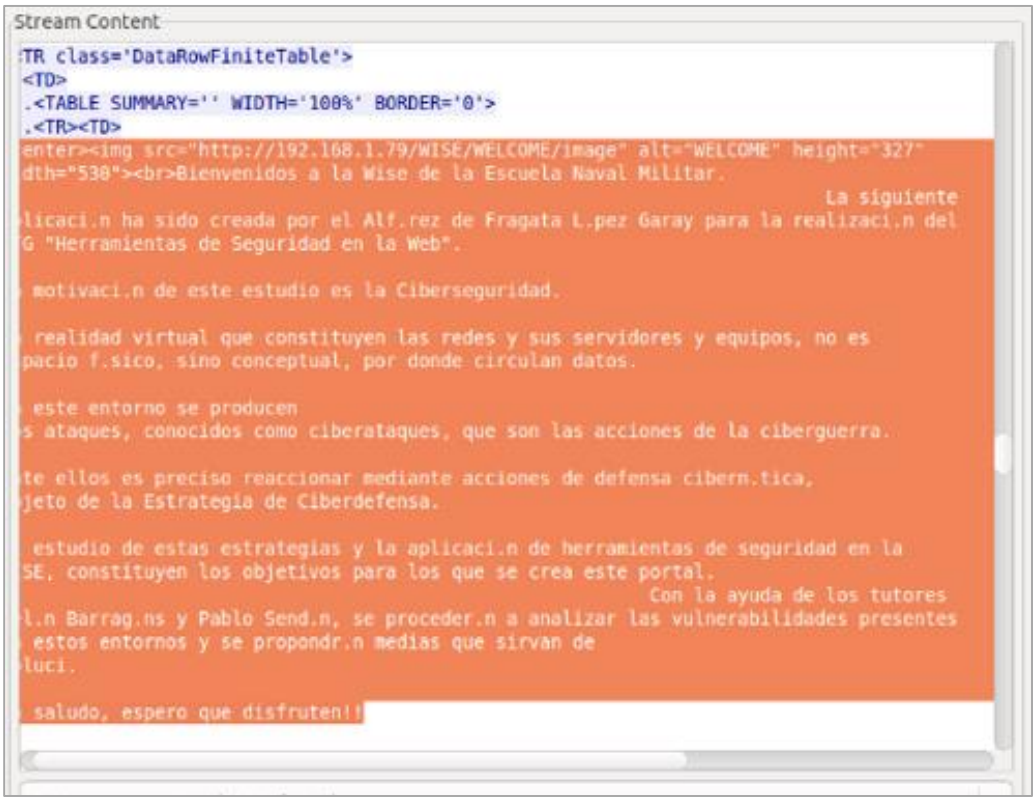

Figura 4-34 Captura: Texto editado en WISE

De esta forma, con el empleo de la herramienta, se pueden interceptar todos los procesos que se realizan sobre el sistema y lo peor de todo, se pueden obtener las credenciales de los usuarios conectados. Esto supone una de las mayores vulnerabilidades del gestor de contenidos. Para solventarla, se recomendaría utilizar el protocolo HTTPS donde la comunicación va cifrada de extremo a extremo y, por tanto, no sería posible la captura de credenciales.

4.3.1 Ataque DoS

Como última etapa en el análisis de las vulnerabilidades que presenta WISE, procederemos a realizar un ataque de denegación de servicio. El objetivo de esta prueba es comprobar el número máximo de conexiones que permite el sistema. En un entorno con un volumen considerable de usuarios, el número máximo de peticiones que es capaz de procesar el sistema es un punto importante. Para ello emplearemos la herramienta *GoldenEye*.

GoldenEye es una herramienta de ataques de denegación de servicio. Utiliza peticiones *KeepAlive* combinados con *Cache–Control*. A partir de estas peticiones se consigue saturar el servidor evitando que las conexiones legítimas puedan establecerse.

Por defecto, al iniciar un ataque sobre una página web, la herramienta simula a 10 usuarios realizando 500 peticiones simultáneas cada uno. No obstante, como se muestra en la Figura 4-35, estos parámetros pueden modificarse.

Figura 4-35 Captura: Opciones *GoldenEye*

Tras variar los parámetros del ataque DoS, comprobamos que el sistema colapsa cuando un único usuario realiza 100 conexiones simultáneas (Figura 4-36).

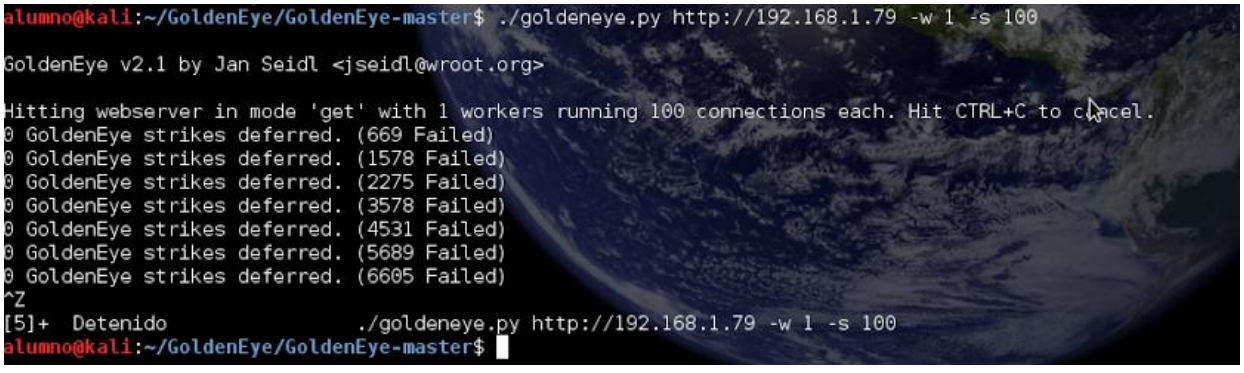

Figura 4-36 Captura: Ataque con un trabajador realizando 100 conexiones

Una vez lanzado el ataque, el sistema rechazará nuevas conexiones. En la Figura 4-37 se refleja la respuesta proporcionada por el navegador al intentar realizar una nueva conexión mientras se atacaba al sistema.

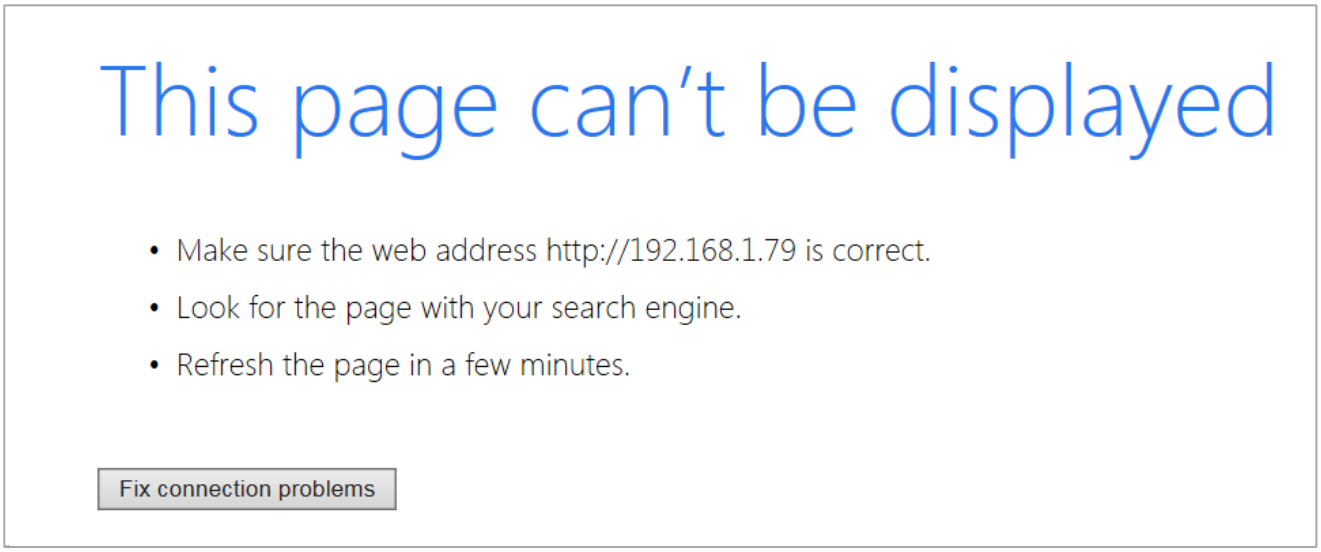

Figura 4-37 Captura: WISE no puede ser mostrada tras ataque DoS

Del uso de *GoldenEye* podemos concluir que WISE es un sistema bastante limitado. Con tan sólo 100 peticiones simultáneas se ha conseguido saturar el sistema imposibilitando las conexiones verdaderas. Este hecho pone de manifiesto la escasa capacidad que presenta WISE para su uso en organizaciones en las que un gran número de usuarios necesiten acceder al sistema de manera frecuente.

5 EVALUACIÓN DE LOS RESULTADOS

5.1 Análisis del gestor de contenidos WISE

5.1.1 Instalación y configuración

Durante el capítulo 3 se ha llevado a cabo la instalación y configuración *Classic* del gestor de contenidos WISE. Se ha seleccionado la versión *Classic* por ser la configuración empleada en las unidades de la Armada. El desarrollo de este capítulo ha servido para familiarizarnos con el gestor a nivel administrador. A pesar de ser un sistema manejable y sencillo, se trata de un CMS obsoleto cuya última versión fue desarrollada en el año 2002. Este hecho, unido a su uso extendido en las unidades navales, contrasta con las políticas del Ministerio de Defensa, que abogan por la renovación, desarrollo e innovación de los sistemas y las tecnologías, de forma que se garantice la seguridad de la información en el ámbito de Defensa.

Analizando WISE dentro de la curva de aprendizaje, se puede afirmar que se trata de un gestor de contenidos muy sencillo. En pocas horas, el nuevo administrador conoce las posibilidades que presenta y es capaz de explotarlas. Sin embargo, tanto las posibilidades como los procesos, son limitados, convirtiendo a WISE en un CMS poco desarrollado. Como apoyo durante el desarrollo del TFG, se ha empleado la documentación que proporciona el gestor. En este proceso se ha desarrollado una página web que ilustra con detalle el uso que de WISE se realizaría en la Escuela Naval Militar. Durante la

configuración del portal han ido apareciendo numerosas carencias o limitaciones que presenta el sistema.

- El primer punto a destacar es que, tanto en la configuración *Classic* como *Enterprise*, WISE almacena las entradas y modificaciones del sistema en el fichero *Data.fs*. En un entorno con múltiples usuarios en el que el portal se actualice frecuentemente, este fichero crecería rápidamente. Asociado a su tamaño encontramos uno de los mayores defectos del sistema. Si el archivo supera los 2GB, el sistema se bloquea. Como solución, en la misma guía de administración, se recomienda realizar un empaquetado del archivo *Data.fs* cada quince días.
- En segundo lugar, en cuanto a las limitaciones en las posibilidades que presenta WISE, se han localizado ciertas carencias debidas a la falta de actualizaciones del sistema. Un ejemplo de ello es la inexistencia de un editor de texto (WYSIWYG), debiéndose realizar la edición mediante el empleo de comandos HTML. Aunque se trata de un hecho de importancia menor, recalca la antigüedad del gestor.
- En tercer lugar, se deben señalar las limitaciones en cuanto a la gestión de los usuarios. WISE no permite otorgar roles comunes a un grupo específico de usuarios, como podrían ser los roles comunes para cada una de las subwise Profesor, Alumno o Dotación. Actualmente, la gestión de roles se realiza de forma individual. A cada nuevo usuario se le conceden unos permisos particulares, dentro de la configuración de cada subpágina. Esta tarea, en principio sencilla, puede ser tediosa a medida que aumente el número de usuarios. Este hecho se refleja en los buques, donde más de 200 personas tienen acceso a WISE. Para simplificar la creación de usuarios, se suelen crear usuarios genéricos, en los que se agrupa un gran colectivo (por ejemplo, el usuario *Guardiamarina* para todos los alumnos embarcados en el Juan Sebastián Elcano). Este hecho supone una pérdida de control sobre las acciones que realiza cada usuario. Al conceder usuarios genéricos, un empleado descontento podría realizar un ataque desde el anonimato que proporciona el usuario compartido. Una tabla en la que se pudiesen conceder roles genéricos a una serie de usuarios, facilitaría mucho la tarea de gestión de sesiones y el control de la información.
- Estos entornos WISE, en su conjunto, tienen como puntos negativos la exigencia de un esfuerzo de actualización a las unidades que lo utilizan y, además, el hecho de que el gestor haya quedado obsoleto, dejando de actualizarse, puede suponer un problema en algunas ocasiones. Por otra parte, presenta puntos positivos, para las unidades operativas que hacen uso de él, como son la facilidad para compartir documentos y establecer calendarios y, especialmente, por el hecho de trabajar sobre servidores propios, se realiza un mejor aprovechamiento del ancho de banda. Esto supone un punto destacable en condiciones de conexión restrictivas, como son, las de los buques en la mar.
- En cuanto a los roles, el sistema proporciona únicamente dos posibilidades: *Site Administrator* y *User*. Este hecho constituye otra de las limitaciones del gestor. Mientras que el rol *User* solamente proporciona acceso, el rol *Site Administrator* otorga el privilegio de la configuración completa de la subwise. El sistema carece de roles intermedios que establezcan una diferencia entre el administrador y los usuarios destinados a descargar o actualizar la documentación. Además, estos roles se aplican a toda la subwise, no pudiendo establecerse restricciones a áreas o *containers* específicos.
- Otro de los puntos a destacar en WISE es que, en la configuración estándar para la versión *Classic*, no se emplea una base de datos relacional, si no que se genera un directorio WISE en el que se almacenan los archivos y usuarios. La mayoría de sistemas CMS actuales trabajan sobre una base de datos relacional. Entre las múltiples ventajas que presenta, se encuentran la velocidad para realizar operaciones y la compatibilidad con diferentes sistemas operativos. No obstante, la instalación en la versión *Enterprise* permite incorporar una base de datos relacional como repositorio para el portal.
- Por último, WISE es una aplicación diseñada para ser empleada exclusivamente sobre el sistema operativo Windows. Esto supone una limitación en cuanto las plataformas sobre las que se puede desplegar.

5.1.2 Auditoría

Tras la instalación y configuración, se ha llevado a cabo una auditoría sobre el gestor. El primer punto a analizar han sido las vulnerabilidades a nivel interno, también conocidas como *Internal Footprinting*. En esta primera fase, desde el punto de vista del administrador, se ha analizado el directorio en el que se almacenan todos los documentos que se vuelcan sobre WISE, así como los *plugins* de instalación. En este directorio se encuentra el documento *Data.fs*. Además de los problemas que su tamaño puede ocasionar, en este fichero quedan registradas las transacciones realizadas, así como las entradas de los usuarios y sus contraseñas, todas ellas sin cifrar. Simplemente accediendo al directorio WISE, se podrían obtener todas las credenciales de los usuarios, con los problemas que ello supondría.

Posteriormente se presentaron algunas de las herramientas de monitorización del sistema que presenta el sistema operativo. Si bien existen herramientas más sofisticadas para la monitorización del servidor, a modo de ejemplo se ilustraron algunos comandos que permiten analizar las conexiones y usuarios del servidor. Estos comandos podrían reflejar intentos de acceso al sistema o ataques en curso.

A continuación se ha analizado el gestor de contenidos desde un nivel externo (*External Footprinting*). Como primer paso se ha realizado una recogida de información sobre las versiones de programas ejecutados, sistema operativo y puertos en funcionamiento. Para ello se han empleado distintas herramientas que proporciona *Kali Linux* como son: *Whatweb, Zenmap* o *Nmap.* Tras su empleo se han obtenido los siguientes datos:

- La versión de ZOPE empleada (*Zope 2.6.4 (binary release, python 2.1, win32-x86)*).
- El puerto sobre el que se ejecuta WISE (Puerto 80).
- El sistema operativo Windows 7, 64 bits.

Tras la obtención de estos datos, se puede concretar el tipo de ataque a realizar, obteniendo las vulnerabilidades conocidas que las versiones empleadas presentan.

Con el mismo propósito y a modo de ejemplo, se ha realizado un análisis de metadatos con la herramienta *FOCA*. De los metadatos se puede obtener información muy valiosa como nombres de usuarios, cuentas de correo electrónico, *software* y programas utilizados para su creación, entre otros. Se debe señalar que los datos obtenidos proceden de los documentos publicados en WISE. Al tratarse de una página desarrollada para el estudio de sus vulnerabilidades, los datos obtenidos no tienen relevancia y desde luego, el resultado sería totalmente diferente si variásemos el contenido. No obstante, el empleo de *FOCA* ha servido para ilustrar la cantidad de información que, de manera desconocida, se puede llegar a publicar en la red. Gracias al empleo de *FOCA* se ha obtenido el nombre completo de los creadores de los documentos que en WISE se publican, el *software* o programas empleados en el desarrollo de estos documentos, así como la versión de dispositivos electrónicos. En el caso de un ataque real sobre un sitio web, de la información extraída se podrían obtener los usuarios que componen la organización, así como los sistemas y versiones que emplean. Una vez conocidos los usuarios, el siguiente paso sería localizar sus direcciones de correo electrónico para interactuar con ellos. En este caso, la ingeniería social podría ser un método para la obtención de contraseñas que proporcionasen el acceso al sistema.

El siguiente paso ha sido analizar las vulnerabilidades. Para ello, en primer lugar se ha empleado la herramienta *BlindElephant*. Sin embargo, al escanear WISE no se han encontrado coincidencias con ninguna versión de aplicación o CMS conocido. Esto se debe a que, tanto el uso como el desarrollo de WISE, se restringen al ámbito de Defensa.

A continuación, se han empleado los escáneres ZAP y VEGA. Estas herramientas lanzan una serie de ataques que destapan las vulnerabilidades o fallos de seguridad. De los fallos obtenidos se deben descartar todos aquellos que aluden a la inyección SQL, puesto que en la configuración seleccionada no se emplea una base de datos relacional.

Las vulnerabilidades localizadas tras la realización de la auditoría son las siguientes:

- Se accede a las credenciales del administrador mediante la captura de tráfico.
- Al acceder a un documento publicado en WISE, se muestran los directorios de los contenidos en el servidor.
- Usuarios remotos no autenticados podrían realizar un ataque DoS.
- Debilidades en la gestión de permisos y privilegios en el sistema.
- Debilidades en la gestión de recursos en el sistema.

Por otro lado, a pesar de las vulnerabilidades localizadas mediante las herramientas, se extraen las siguientes conclusiones:

- Al no trabajar sobre base de datos relacional, no se puede explotar esta vulnerabilidad.
- ZOPE bloquea los *exploits* lanzados contra el sistema.
- A pesar de detectarse vulnerabilidades XSS, no se consigue introducir URL en el gestor sin autenticarnos. No obstante, una vez se obtienen las credenciales de usuario, podría ejecutarse mediante la introducción de enlaces URL que permite generar WISE.

En último lugar se empleó la herramienta *GoldenEye*. Mediante esta herramienta, se consiguió realizar un ataque de denegación de servicio, demostrando la facilidad que presenta el sistema para ser vulnerado por un ataque de estas características. Este problema puede deberse a la instalación de WISE sobre un servidor no optimizado para procesar un gran número de peticiones simultáneas. De todas formas, el resultado obtenido resalta la limitación que el sistema WISE podría tener en una organización en la que un gran número de usuarios hagan uso del gestor de forma simultánea. No obstante, en el caso de la Armada, la posibilidad de que 100 usuarios accedan de forma simultánea al servidor, resulta una opción casi imposible.

5.1.3 Posibles soluciones

Los sistemas deben evolucionar constantemente para corregir los errores de seguridad que los comprometan. De la misma forma, los usuarios deben instalar las actualizar de las aplicaciones, evitando así que vulnerabilidades corregidas puedan ser explotadas. Además, los administradores de los sistemas WISE deben conocer las vulnerabilidades que el gestor presenta.

El servidor WISE debe encontrarse protegido. Para ello se deben emplear contraseñas seguras, así como un antivirus y *firewall* actualizados. Además, se debe restringir el acceso físico al equipo pues, una vez se tiene acceso al servidor, es fácilmente vulnerable. Como solución a las vulnerabilidades detectadas se propone:

- Aplicar el protocolo SSL/HTTPS en el servidor WISE. De esta forma, las peticiones que se realicen hacia el servidor irán cifradas. Este protocolo evitaría que las credenciales de los usuarios sean capturadas mediante el análisis del tráfico.
- Modificar la gestión que actualmente se realiza de los usuarios. Cada usuario debe poseer sus credenciales personales, de forma que se pueda realizar un control y seguimiento de las acciones que cada usuario lleva a cabo.
- Como defensa ante la posibilidad de un ataque DoS, se podría bloquear la IP de origen del equipo que esté realizando un comportamiento anómalo. Los servidores Windows permiten el bloqueo selectivo de las peticiones de este tipo. Además, resulta conveniente la instalación de WISE en un servidor, no en un equipo de sobremesa. En los buques, la instalación de WISE se realiza sobre servidores independientes que trabajan sobre el sistema operativo Windows 2008, por lo que los resultados obtenidos cambiarían sustancialmente.

- Finalmente, la gestión de los usuarios y los activos es uno de los aspectos más complicados y a la vez más interesantes. Además del personal, son muchos los activos que se gestionan en la Armada, desde ordenadores corporativos hasta dispositivos personales, pasando por servidores, memorias portátiles, *tablets* y teléfonos móviles. Por ello es necesario disponer de un inventario de los activos para gestionarlos de una manera correcta. Limitar el número de dispositivos con acceso a información clasificada, es una de las primeras medidas a establecer para la creación de un entorno seguro.

6 CONCLUSIONES Y LÍNEAS FUTURAS

6.1 Conclusiones

Finalizado el trabajo, es hora de analizar si se han conseguido cumplir con éxito los objetivos generales y específicos que se marcaron al inicio.

Tras la investigación y estudio desarrollado, se ha adquirido una visión clara y actual de los principales problemas que afectan a la seguridad en aplicaciones web. El rápido desarrollo y expansión de las aplicaciones y los gestores de contenidos viene acompañado de un crecimiento exponencial de los ciberdelitos. En este contexto, los estados y organizaciones se ven obligados a desarrollar nuevas políticas y estrategias en materia de ciberdefensa, de forma que se interpongan barreras para la defensa ante estas amenazas.

Del mismo modo, se han analizado las diversas formas de ataques sobre entornos web y variantes del *malware* (Anexo II). El incremento de estos ataques y la falta de concienciación de los usuarios suponen uno de los mayores riesgos para las organizaciones. Para la defensa contra estas amenazas y la generación de un entorno más seguro, se han recogido una serie de plataformas y herramientas para el análisis de vulnerabilidades web. Estas herramientas permiten auditar las aplicaciones y localizar fallos de seguridad.

Como objeto de estudio, se ha instalado y configurado el gestor de contenidos WISE. De esta forma, se han adquirido los conocimientos necesarios para la administración del sistema. Se conoce ahora el funcionamiento de este CMS empleado en la Armada.

Por último, se ha realizado un análisis de vulnerabilidades del gestor, aplicando distintas herramientas con las que nunca antes se había trabajado. Analizado el gestor, se han descubierto ciertas vulnerabilidades, llegando a la conclusión de que el sistema tiene un nivel de seguridad bajo.

Debido al tiempo limitado, no se han explotado de manera extensiva todas las posibilidades en las que se podría vulnerar el sistema. Tampoco se han podido aplicar medidas que generen una plataforma más segura, parte que se plantea como líneas futuras.

6.2 Líneas futuras

A continuación, se presentan como líneas futuras una serie de tareas que profundicen en las vulnerabilidades del sistema WISE.

Para comenzar, sería recomendable repetir el estudio sobre la configuración *Enterprise*, empleando una base de datos relacional. De esta forma se podrían analizar las ventajas y desventajas que, desde el punto de vista de la seguridad en la web, se proporciona la versión *Enterprise* frente a la *Classic*. Durante el análisis, se han descubierto algunas vulnerabilidades no explotadas. En caso de realizarse la configuración indicada, se recomienda analizar:

- Inyección SQL.
- Realización de un ataque XSS.
- Realización de un ataque XSRF.
- Inyección URL.

Después, se podría avanzar en la adopción de protocolos de seguridad y cifrado de información. Esto corregiría la mayor parte de las vulnerabilidades localizadas: la obtención de las credenciales mediante *sniffing*. Para ello, se podría utilizar el protocolo HTTPS. De la misma forma, se debería analizar si estas medidas son de utilidad o, por el contrario, sería oportuno sustituir WISE por un gestor de contenidos más actual y potente. En esta línea, se propone analizar los distintos CMS existentes, estudiando la posibilidad de sustituir WISE por un sistema actualizado que presente las capacidades que se requieren en las unidades navales, y garantice el nivel de seguridad adecuado a los contenidos que en WISE se comparten. Para ello, se debería proceder a la instalación y configuración de distintos gestores de contenidos, evaluando la facilidad de configuración, administración y empleo. De realizarse este estudio, se deberían comparar los beneficios que la sustitución de WISE tendría, considerando el esfuerzo de implantación y aprendizaje que ello supondría.

Finalmente, se deberían analizar el grado de seguridad que cada uno de estos sistemas presenta, realizando una valoración que identifique al mejor candidato para una posible sustitución de WISE.

6.3 Valoración personal

En un entorno donde los sistemas informáticos se encuentran en continua expansión, se deben revisar todos los procesos de seguridad para asumir este desarrollo. La formación en ciberseguridad es necesaria para que los empleados puedan desempeñar sus funciones de forma segura y adecuada. En línea con las nuevas políticas en materia de ciberdefensa, las unidades navales deben velar por la implementación de buenas prácticas, evitando la exposición de información sensible. En los buques existen zonas e información consideradas como críticas a las que no debe tener acceso cualquier persona. En ellas se almacena información confidencial y por eso, se establecen permisos de acceso al personal estrictamente necesario. En cuanto al empleo del gestor de contenidos WISE, se deben establecer las medidas necesarias para seguir haciendo uso de las nuevas tecnologías, de manera segura.

7 BIBLIOGRAFÍA

En esta sección figuran todas las referencias empleadas para la realización del presente TFG.

[1] «Revolución de las TIC» [En línea]. Available: http://www.ite.educacion.es/formacion/materiales/112/cd/m7/la_revolucin_informtica.html. [Último acceso: 30 Noviembre 2015].

[2] «*Syonetwork*_Entrevista a Bill Gates sobre Internet» [En línea]. Available: http://syonetwork.com/bill-gates-miente-luego-existe/. [Último acceso: 18 Enero 2016].

[3] Á. Espinosa, «Irán sufre un ataque informático contra sus instalaciones nucleares» El País, 28 Septiembre 2010.

[4] W. Gibson, Neuromante, 1984.

[5] J. Á. Martos, «¡Esto es la ciberguerra!» Muy Interesante.

[6] C. F. Z. Pasquín, «Las Fuerzas Armadas se preparan para afrontar con éxito los nuevos retos del siglo XXI en materia de ciberseguridad» Marzo 2013. [En línea]. Available: http://www.defensa.gob.es/Galerias/documentacion/revistas/2013/red-293-ciberdefensa.pdf. [Último acceso: 29 Diciembre 2015].

[7] «Nuevas amenazas: el ciberespacio (NATO)» [En línea]. Available: http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/ES/index.htm. [Último acceso: 11 Enero 2016].

[8] C. d. Defensa, «Guerra_cibernética_aspectos organizativos» [En línea]. Available: http://docplayer.es/2279115-Guerra-cibernetica-aspectos-organizativos.html. [Último acceso: 15 Enero 2016].

[9] P. d. Gobierno, «Estrategia de Ciberseguridad Nacional» 2013.

[10] «Ministerio de Defensa_Directiva de Defensa Nacional» [En línea]. Available: http://www.defensa.gob.es/defensa/politicadefensa/directivadefensa/. [Último acceso: 15 Enero 2016].

[11] S. d. l. Santos, Una al día, http://unaaldia.hispasec.com/2011/09/libro-seguridad-en-windows-secretos.html, 2009.

[12] D. Verdú, «Los móviles, objetivo de los virus» El País, 21 Septiembre 2015.

[13] «Actividad maliciosa en *Google Play*» [En línea]. Available: http://www.zdnet.com/article/riskiq-claims-malicious-android-apps-up-by-almost-400-percent-on-google-play/. [Último acceso: 21 Diciembre 2015].

[14] «Los móviles, objetivo de los virus» El país, 21 Septiembre 2015. [En línea]. Available: http://tecnologia.elpais.com/tecnologia/2015/09/15/actualidad/1442327365_650658.html. [Último acceso: 11 Enero 2016].

[15] J. M. A. Liñán, «Cada vez resulta más fácil hacerse hacker» El País, 23 Julio 2015.

[16] «Anticiparse a los riesgos: las vulnerabilidades actuales son la antesala de ataques inminentes» 2015. [En línea]. Available: http://www.trendmicro.es/informacion-seguridad/investigacion/trendlabs-q3-2015-security-roundup/index.html. [Último acceso: 17 Enero 2016].

[17] V. W. V. p. d. M. Labs, «Estudio de las amenazas web en el año 2015» Agosto 2015. [En línea]. Available: http://www.mcafee.com/es/resources/reports/rp-quarterly-threats-aug-2015.pdf. [Último acceso: 17 Enero 2016].

[18] «La historia del lenguaje de Internet» Eveliux, [En línea]. Available: http://www.eveliux.com/mx/La-historia-del-lenguaje-de-Internet-TCP/IP.html. [Último acceso: 21 Diciembre 2015].

[19] J. Comin, «Dos estudiantes de la Universidad de Stanford crean el buscador *Yahoo!*» 2001 Diciembre 2011. [En línea]. Available: http://www.maestrosdelweb.com/yahoohis/. [Último acceso: 11 Enero 2016].

[20] «*Pizza Net* realiza su primer pedido online en 1994» [En línea]. Available: https://www.qsrmagazine.com/news/pizza-hut-celebrates-20th-anniversary-online-ordering. [Último acceso: 20 Enero 2016].

[21] «*Page Rank*» [En línea]. Available: http://www.admarketing.com.ar/faqs/28-ique-es-el-page-rank.html. [Último acceso: 21 Diciembre 2015].

[22] «*How Much Google Makes Per Second Globally - Web Profits*» [En línea]. Available: https://www.webprofits.com.au/blog/how-much-google-makes-per-second-globally/. [Último acceso: 15 Febrero 2016].

[23] «Los ataques con malware a consumidores aumentaron un 13% en 2015» [En línea]. Available: http://www2.deloitte.com/es/es/pages/governance-risk-and-compliance/articles/los-ataques-con-malware-a-consumidores-aumentaron-en-2015.html. [Último acceso: 17 Enero 2016].

[24] G. Cristalino, «Seguridad Informática_ataques *script kiddies*» 7 Abril 2013. [En línea]. Available: http://seguridadinformatica4b.blogspot.com.es/2013/04/script-kiddie.html. [Último acceso: 16 Enero 2016].

[25] M. R. y. D. d. Revenga, Inteligencia en el Ciberespacio, 2015.

[26] F. Paget, «*Hacktivism*» [En línea]. Available: http://www.mcafee.com/es/resources/white-papers/wp-hacktivism.pdf. [Último acceso: 16 Enero 2016].

[27] CNN-CERT, «Resumen de ciberamenzas» [En línea]. Available: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/795-ccn-cert-resumen-ia-09-15-ciberamenazas-2014-tendencias-2015/file.html. [Último acceso: 11 Febrero 2016].

[28] «*Advanced Persistent Threats*» [En línea]. Available: http://www.gitsinformatica.com/glosad.html. [Último acceso: 16 Enero 2016].

[29] «Consejo Nacional de Ciberseguridad» [En línea]. Available: http://www.dsn.gob.es/es/sistema-seguridad-nacional/comit%C3%A9s-especializados/consejo-nacional-ciberseguridad. [Último acceso: 18 Enero 2016].

[30] «DSN GOB_Sistema de Seguridad Nacional» [En línea]. Available: http://www.dsn.gob.es/es/sistema-seguridad-nacional/comit%C3%A9s-especializados/consejo-nacional-ciberseguridad#collapseSix. [Último acceso: 17 Enero 2016].

[31] «INCIBE» [En línea]. Available: https://www.incibe.es/que_es_incibe/. [Último acceso: 26 Enero 2016].

[32] «Mando Conjunto de Ciberdefensa - EMAD» [En línea]. Available: http://www.emad.mde.es/CIBERDEFENSA/cometidos/. [Último acceso: 16 Enero 2016].

[33] P. Hernández, «Real Instituto Elcano_Nueva legislación en materia informática» [En línea]. Available: http://www.realinstitutoelcano.org/wps/portal/web/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=%2Felcano%2Felcano_es%2Fzonas_es%2Fciber-elcano-10-enero-2016%2F#.VpU5vuDpXA0.linkedin. [Último acceso: 16 Enero 2016].

[34] «¿Cómo funciona un CMS o Gestor de contenidos (II)?» 29 Abril 2014. [En línea]. Available: http://www.neosoft.es/blog/como-funciona-un-cms-o-gestor-de-contenidos/. [Último acceso: 20 Enero 2016].

[35] «Arquitectura de un CMS» [En línea]. Available: http://ecommerceupv.com/2013/07/el-rincon-del-principiante-en-comercio-electronico-que-es-un-cms-y-como-funciona/. [Último acceso: 15 Febrero 2016].

[36] «CMS *Wordpress*» [En línea]. Available: https://es.wordpress.com/. [Último acceso: 18 Febrero 2016].

[37] «Gestores de contenidos más utilizados» [En línea]. Available: http://marketingwebconsulting.uma.es/gestores-de-contenidos-mas-utilizados-actualmente/. [Último acceso: 10 Febrero 2016].

[38] «Portal web de la Casa Blanca, desarrollado en *WordPress*» [En línea]. Available: https://wordpress.org/showcase/bbc-america/. [Último acceso: Febrero 10 2016].

[39] «CMS *Joomla!*» [En línea]. Available: https://www.joomla.org/. [Último acceso: 18 Febrero 2016].

[40] «Portal web de Torre Eiffel, desarrollado en *Joomla!*» [En línea]. Available: http://www.toureiffel.paris/. [Último acceso: 14 Febrero 2016].

[41] «CMS *Drupal*» [En línea]. Available: https://www.drupal.org/. [Último acceso: 18 Febrero 2016].

[42] «Portal web de la Casa Blanca EEUU, desarrollado en *Drupal*» [En línea]. Available: https://www.whitehouse.gov/. [Último acceso: 14 Febrero 2016].

[43] «CMS *Moodle*» [En línea]. Available: https://moodle.com/. [Último acceso: 18 Febrero 2016].

[44] «*Magento*» [En línea]. Available: https://magento.com/. [Último acceso: 18 Febrero 2016].

[45] «CMS *PrestaShop*» [En línea]. Available: https://www.prestashop.com/es/.

[46] «Curva de aprendizaje según el CMS» [En línea]. Available: http://wpdirecto.com/la-curva-de-aprendizaje-segun-el-cms-999/.

[47] «Porcentaje de uso de los sistemas CMS» [En línea]. Available: http://mongemalo.es/wordpress-joomla-drupal-mejor-gestor-contenidos-cms/. [Último acceso: 14 Febrero 2016].

[48] P. S. &. E. Group, «NATO WISE HSI Success Story» 2001.

[49] A. C. Transformation, «WISE 1.2 Administration Guide» 2001.

[50] «ZOPE Documentation» 2001.

[51] A. C. Transformation, «Instalation Guide» 2001.

[52] C. V. D. H. S., «Protocolo CGI (*Common Gateway Interface*)» 2001. [En línea]. Available: http://www.maestrosdelweb.com/cgiintro/. [Último acceso: 9 Febrero 2016].

[53] «*Real time attacks* (*Nose Attack Map*)» [En línea]. Available: http://map.norsecorp.com/. [Último acceso: Enero 20 2016].

[54] «SQL *Inyection Attack* (OWASP)» 14 Agosto 2014. [En línea]. Available: https://www.owasp.org/index.php/SQL_Injection.

[55] «Ataque *Cross-Site Scripting* (OWASP)» [En línea]. Available: http://eoftedal.github.io/presentations/owasp-top-10-js-and-rest/OWASP%20Top%2010%20for%20JS/index.html#1. [Último acceso: 29 Enero 2016].

[56] Josep, «Ataque *Cross Site Request Forgery*» [En línea]. Available: http://blog.evidaliahost.com/2015/09/16/cross-site-request-forgery-csrf/. [Último acceso: 15 Febrero 2016].

[57] «Protocolo *Three Way Handshake*» [En línea]. Available: http://neo.lcc.uma.es/evirtual/cdd/tutorial/transporte/twhandshake.html. [Último acceso: Enero 20 2016].

[58] Q. e. u. 0-day, «*Vulnerabilidades 0-day*» [En línea]. Available: http://www.welivesecurity.com/la-es/2015/02/25/que-es-un-0-day/. [Último acceso: Enero 20 2016].

[59] «Conceptos básicos de una conexión TCP» [En línea]. Available: http://www.kontrol0.com/2013/04/conceptos-basico-de-una-conexion-tcp.html. [Último acceso: 14 Febrero 2016].

[60] «Openvas» [En línea]. Available: http://www.openvas.org/. [Último acceso: 20 Enero 2016].

[61] «OWASP» [En línea]. Available: https://www.owasp.org/index.php/Main_Page. [Último acceso: 23 Enero 2016].

[62] OWASP, «Owasp *top ten* 2013» 2013. [En línea]. Available: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=OWASP_Top_10_for_2013. [Último acceso: 25 Enero 2016].

[63] «*Zed Attack* Proxy_OWASP» [En línea]. Available: https://www.owasp.org/index.php/Top_10_2013-Top_10. [Último acceso: Enero 20 2016].

[64] «*Backtrack Linux*» [En línea]. Available: http://www.backtrack-linux.org/. [Último acceso: 25 Enero 2016].

[65] «*Kali Linux*» [En línea]. Available: https://www.kali.org/. [Último acceso: 26 Enero 2016].

[66] «*Whatweb*» [En línea]. Available: http://whatweb.net/. [Último acceso: 12 Febrero 2016].

[67] «*Zenmap*» [En línea]. Available: https://nmap.org/zenmap/. [Último acceso: 12 Febrero 2016].

[68] «*BlindElephant*» [En línea]. Available: http://blindelephant.sourceforge.net/. [Último acceso: 12 Febrero 2016].

[69] «VEGA *vulnerability scanner*» [En línea]. Available: https://subgraph.com/vega/.

[70] «*Armitage - Metasploit Unleashed*» [En línea]. Available: https://www.offensive-security.com/metasploit-unleashed/armitage/. [Último acceso: 12 Febrero 2016].

[71] «*Wireshark*» [En línea]. Available: https://www.wireshark.org/. [Último acceso: 12 Febrero 2016].

[72] «*GoldenEye*» [En línea]. Available: http://wroot.org/projects/goldeneye/. [Último acceso: 2016 Febrero 2016].

[73] «*Samurai Web Testing*» [En línea]. Available: http://www.samurai-wtf.org/. [Último acceso: 20 Enero 2016].

[74] «*Web application security with Acunetix*» [En línea]. Available: http://www.acunetix.com/. [Último acceso: 29 Enero 2016].

[75] «*FOCA - Eleven Paths*» [En línea]. Available: https://www.elevenpaths.com/es/labstools/foca-2/index.html.

[76] A. C. Transformation, «AG01_Installation_Guide» 2001.

[77] «*Security-database* (ZOPE *vulnerabilities*)» [En línea]. Available: http://www.security-database.com/cpe.php?detail=cpe:/a:zope:zope:2.6.4. [Último acceso: 20 Febrero 2016].

[78] «Blog *Elevn Paths* (*ClickJacking*)» 29 Octubre 2013. [En línea]. Available: http://blog.elevenpaths.com/2013/10/algunos-ejemplos-y-defensas-contra-el.html. [Último acceso: 3 Febrero 2016].

[79] «Zona Virus_*Backdoors*» 16 Diciembre 2008. [En línea]. Available: http://www.zonavirus.com/articulos/puertas-traseras-o-backdoors.asp. [Último acceso: 18 Enero 2016].

[80] «George Bush autoriza el espionaje masivo» Actualidad.rt, Diciembre 2013.

[81] «Puerta trasera *Duuzer*» [En línea]. Available: http://www.redeszone.net/2015/10/28/duuzer-una-nueva-puerta-trasera-descubierta-por-symantec/. [Último acceso: 21 Diciembre 2015].

[82] «*Trojan Cryptolocker*» [En línea]. Available: https://www.symantec.com/security_response/writeup.jsp?docid=2015-030201-5710-99&tabid=2. [Último acceso: 25 Febrero 2016].

[83] «Delitos informáticos_Bombas lógicas» [En línea]. Available: http://www.delitosinformaticos.com/10/2013//danos-informaticos/ataque-informatico-mediante-bomba-logica-o-bomba-de-tiempo. [Último acceso: 21 Diciembre 2015].

[84] «El *Spam* supone el 60% del tráfico» [En línea]. Available: http://www.seguridadpc.net/spam.htm. [Último acceso: 11 Enero 2016].

[85] «Ataques informáticos de ingenería social» [En línea]. Available: http://hackstory.net/Ingenier%C3%ADa_social. [Último acceso: 20 Enero 2016].

[86] «Convenio sobre Ciberdelincuencia de Budapest» 2001. [En línea]. Available: http://web.archive.org/web/20120107073324/http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_spanish.PDF. [Último acceso: 11 Enero 2016].

[87] F. Serrato, «Publicados los datos de 39 millones de infieles registrados en *Ashley Madison*» El país, 20 Agosto 2015.

ANEXO I: LEGISLACIÓN SOBRE DELITOS INFORMÁTICOS EN ESPAÑA

Artículos del Código Penal Español referentes a Delitos Informáticos (Ley-Orgánica 10/1995, de 23 de noviembre BOE número 281, de 24 de noviembre de 1995)

• *Artículo 197*

1.- El que para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.
2.- Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.
3.- Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.
4.- Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.
5.- Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.
6.- Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años.

• *Artículo 198*

La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.

• *Artículo 199*

1.- El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.

2.- El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años.

• *Artículo 200*

Lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este código.

• *Artículo 201*

1.- Para proceder por los delitos previstos en este capítulo será necesaria denuncia de la persona agraviada o de su representante legal. Cuando aquélla sea menor de edad, incapaz o una persona desvalida, también podrá denunciar el Ministerio Fiscal.
2.- No será precisa la denuncia exigida en el apartado anterior para proceder por los hechos descritos en el artículo 198 de este Código, ni cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas.
3.- El perdón del ofendido o de su representante legal, en su caso, extingue la acción penal o la pena impuesta, sin perjuicio de lo dispuesto en el segundo párrafo del número 4º del artículo 130.

• *Artículo 211*

La calumnia y la injuria se reputarán hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante.

• *Artículo 212*

En los casos a los que se refiere el artículo anterior, será responsable civil solidaria la persona física o jurídica propietaria del medio informativo a través del cual se haya propagado la calumnia o injuria.

• *Artículo 238*

Son reos del delito de robo con fuerza en las cosas los que ejecuten el hecho cuando concurra alguna de las circunstancias siguientes:
1º.- Escalamiento.
2º.- Rompimiento de pared, techo o suelo, o fractura de puerta o ventana.
3º.- Fractura de armarios, arcas u otra clase de muebles u objetos cerrados o sellados, o forzamiento de sus cerraduras o descubrimiento de sus claves para sustraer su contenido, sea en el lugar del robo o fuera del mismo.
4º.- Uso de llaves falsas.
5º.- Inutilización de sistemas específicos de alarma o guarda.

• *Artículo 239*

Se considerarán llaves falsas:
1º.- Las ganzúas u otros instrumentos análogos.
2º.- Las llaves legítimas perdidas por el propietario u obtenidas por un medio que constituya infracción penal.
3º.- Cualesquiera otras que no sean las destinadas por el propietario para abrir la cerradura violentada por el reo.

A los efectos del presente artículo, se consideran llaves las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia.

• *Artículo 248*

1.- Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.
2.- También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.

• *Artículo 255*

Será castigado con la pena de multa de tres a doce meses el que cometiere defraudación por valor superior a cincuenta mil pesetas, utilizando energía eléctrica, gas, agua, telecomunicaciones u otro elemento, energía o fluido ajenos, por alguno de los medios siguientes:
1º.- Valiéndose de mecanismos instalados para realizar la defraudación.
2º.- Alterando maliciosamente las indicaciones o aparatos contadores.
3º.- Empleando cualesquiera otros medios clandestinos.

• *Artículo 256*

El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a cincuenta mil pesetas, será castigado con la pena de multa de tres a doce meses.

• *Artículo 263*

El que causare daños en propiedad ajena no comprendidos en otros Títulos de este Código, será castigado con la pena de multa de seis a veinticuatro meses, atendidas la condición económica de la víctima y la cuantía del daño, si éste excediera de cincuenta mil pesetas.

• *Artículo 264*

1.- Será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses el que causare daños expresados en el artículo anterior, si concurriera alguno de los supuestos siguientes:
1º.- Que se realicen para impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones, bien se cometiere el delito contra funcionarios públicos, bien contra particulares que, como testigos o de cualquier otra manera, hayan contribuido o pueden contribuir a la ejecución o aplicación de las Leyes o disposiciones generales.
2º.- Que se cause por cualquier medio infección o contagio de ganado.
3º.- Que se empleen sustancias venenosas o corrosivas.
4º.- Que afecten a bienes de dominio o uso público o comunal.
5º.- Que arruinen al perjudicado o se le coloque en grave situación económica.
2.- La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

• *Artículo 270*

Será castigado con la pena de prisión de seis meses a dos años o de multa de seis a veinticuatro meses quien, con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.
La misma pena se impondrá a quien intencionadamente importe, exporte o almacene ejemplares de dichas obras o producciones o ejecuciones sin la referida autorización. Será castigada también con la misma pena la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinada a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador.

• *Artículo 278*

1.- El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.
2.- Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.
3.- Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos.

• *Artículo 400*

La fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador o aparatos, específicamente destinados a la comisión de los delitos descritos en los capítulos anteriores, se castigarán con la pena señalada en cada caso para los autores.

• *Artículo 536*

La autoridad, funcionario público o agente de éstos que, mediando causa por delito, interceptare las telecomunicaciones o utilizare artificios técnicos de escuchas, transmisión, grabación o reproducción del sonido, de la imagen o de cualquier otra señal de comunicación, con violación de las garantías constitucionales o legales, incurrirá en la pena de inhabilitación especial para empleo o cargo público de dos a seis años.
Si divulgare o revelare la información obtenida, se impondrán las penas de inhabilitación especial, en su mitad superior y, además, la de multa de seis a dieciocho meses.

ANEXO II: AMENAZAS A LOS SISTEMAS INFORMÁTICOS

A medida que los sistemas de información son más complejos y almacenan un mayor número de datos, se ponen de manifiesto nuevas amenazas y puntos vulnerables. Queda clara la necesidad de aplicar herramientas para la protección de la información, pero no es sencillo concretar qué se debe proteger. Todos los elementos que constituyen los sistemas informáticos, las personas que hacen uso de ellos e incluso, su privacidad, son vulnerables.

Anexo II.I *Malware*

Normalmente, el *malware* se clasifica dentro de dos grandes grupos, tal y como se muestra en la Tabla A2-1. Por un lado, aquellos programas o códigos que necesitan ser infiltrados en otro programa que realice una función útil para el usuario; o programas con la capacidad de viajar a través de la red, infectando a equipos, sin la necesidad de un programa que los sustente.

Incrustados en programa	Independientes
Puerta Trasera	Gusanos
Caballo de Troya	Bacterias
Bombas lógicas	
Virus	

Tabla A2-1 Clasificación de los distintos tipos de *malware*

- **Puerta Trasera**

Las puertas traseras (*Backdoors*) son programas informáticos que permiten acceder al sistema sin tener que pasar por los procedimientos ordinarios de autenticación. En algunas ocasiones, los propios programadores crean estas puertas, que sirven de pasarela rápida, para la corrección de errores, sobre todo en las fases de diseño. No obstante, éste no es el caso por el que se clasifican como *malware*, sino que generalmente son empleadas por piratas informáticos para acceder al sistema. De esta forma, en muchas ocasiones, y sin que el usuario se percate, permiten acceder a todo el proceso del equipo, infectándolo con la instalación de virus, para proceder al robo de información, la ejecución de programas o incluso el empleo del ordenador, para que realice ataques de denegación de servicio [79].

Durante varios años, se sospechó sobre la involucración de la NSA en el uso de este tipo de *malware* como herramienta de inteligencia para obtener información e interceptar el tráfico en Internet. Pues bien, en 2013 fueron revelados a la opinión pública una serie de documentos en los que se reconocía la labor de recopilación de inteligencia mediante el uso de puertas traseras y virus. Esta actividad llevaba siendo realizada por la agencia desde octubre de 2001, poco después de los atentados del 11S, y estaba autorizada por el mismísimo George Bush, presidente por aquel entonces de los EE.UU. Según fuentes oficiales, el objetivo principal de esta decisión era el de detectar y prevenir ataques terroristas [80].

Este mismo año, la compañía de seguridad *Symantec* descubrió una nueva puerta trasera conocida como *Duuzer* [81]. Esta *backdoor* ha infectado a un gran número de empresas, siendo distribuida a través de campañas *spam* de correo electrónico, dejando a los equipos en manos de ciberdelincuentes.

- **Caballo de Troya**

Un caballo de Troya o troyano es un programa caracterizado por engañar al usuario, "escondiéndose" dentro de otro programa que realice una función útil o benigna. El objetivo principal de este *malware* suele ser la creación de una puerta trasera, generando un acceso remoto a la administración de los equipos. Existen múltiples tipos de troyanos en función de su complejidad y el fin para el que se emplea.

Trojan Cryptolocker [82] está considerado como uno de los más peligrosos. Este troyano encripta el disco duro de los equipos infectados y activa un cronómetro que amenaza con borrar todos los archivos cuando el contador llega a cero. Esta práctica se conoce como *Ransomware* y constituye un secuestro cibernético. Para poder recuperar los datos, el usuario se ve obligado a realizar un pago económico, generalmente mediante *bitcoins* u otras formas de dinero virtual, que dificultan la localización del delincuente. Hoy en día no existen herramientas contra este *software*, el único remedio que podemos emplear, es la realización de copias de seguridad de los archivos de interés.

En la Figura A2-1 se muestra el porcentaje del empleo de las distintas variantes de *malware*. Podemos apreciar que más de dos tercios del *malware* que circula por la red se manifiesta en forma de troyano.

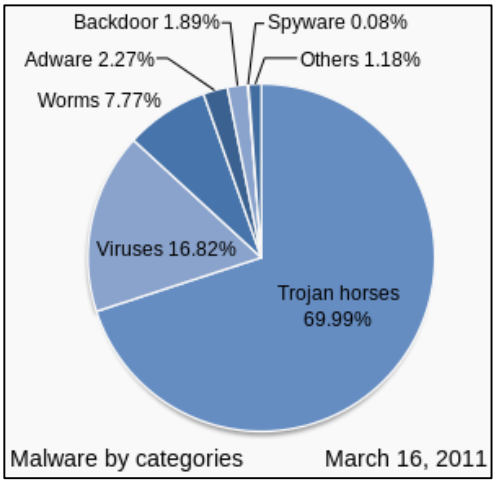

Figura A2-1 Gráfico de empleo de *malware*

- **Bombas lógicas**

Estos programas se caracterizan por permanecer inactivos hasta una determinada fecha, o hasta el momento en que se introduzca un determinado código de activación, dificultando enormemente su detección. Este tipo de *malware* de actuación retardada suele ser empleado por personal interno de la organización, que se encuentre descontento. Su objetivo principal suele ser: destrucción de ficheros, robo de información o posibles ataques de denegación de servicio.

En diciembre de 2002, un empleado descontento de la empresa *UBS PaineWebbe*, en Silicon Valley (California), llegó a infectar cerca de mil ordenadores de la sucursal donde trabajaba, con el objetivo de simular una gran caída en las acciones de la empresa y aprovecharse económicamente [83].

- **Virus**

Estos programas malignos tienen como objetivo alterar el funcionamiento del equipo al que infectan. Sus características similares a los virus que infectan a los seres humanos, dan nombre a esta variante. Presentan capacidad de reproducirse, se transportan desde terminales infectados a otros terminales "sanos", creando una copia del virus y además se encapsulan dentro de paquetes o programas ejecutables, pasando inadvertidos hasta que son activados y ya han infectado al sistema.

Disponen de distintas formas de transmisión: a través de memorias externas, como USBs; con la simple visita de páginas web; descargando *software* pirata de Internet, mediante correo electrónico, entre otras.

Los virus pueden afectar tanto al *software* como al *hardware*. La eliminación o modificación de programas, el robo de información o el mal funcionamiento del sistema, se corresponden con ataques al *software*. Por otra parte, existen virus cuya misión consiste en causar daños en el disco duro, modificar la memoria BIOS, o incluso quemar el microprocesador de la computadora afectada.

Dentro de los virus se puede distinguir:

- **Virus de archivo:** se activan al ejecutar un archivo. Normalmente suelen ir introducidos en archivos con la extensión .EXE.
- **Virus de sector de arranque (*boot*):** Se instalan en el sistema cuando se inicia desde una memoria externa (por ejemplo, un USB), infectando a todas las memorias.
- **Virus Polimórficos:** bajo esta denominación se conoce a los virus que cambian su arquitectura cada vez que realizan una copia de su código. De esta forma dificultan enormemente su detección por los antivirus.
- **Retrovirus:** normalmente no son dañinos por sí mismos. Su función consiste en distraer al antivirus, camuflando la entrada de virus destructivos.
- **Macro Virus:** estos virus se instalan en los macros de documentos de Microsoft como Word o Excel. Son los primeros virus multiplataforma que afectan tanto a PCs como a sistemas Macintosh.

- **Gusanos**

El gusano informático (*worm*) es considerado una subclase dentro del virus, con la diferencia de que son capaces de viajar a través de la red, infectando a un gran número de equipos. Para ello se suelen apoyar en algún archivo como medio de transporte. Su principal característica es que son capaces de reproducirse, normalmente enviando una copia del gusano a cada uno de nuestros contactos de e-mail. Este método de propagación es automático y no necesita de la acción del usuario.

El problema que suele acarrear es el excesivo consumo de recursos en los ordenadores, o de ancho de banda en servidores, pudiendo causar incluso el colapso del equipo o la red.

Uno de los gusanos más famosos y dañinos es el anagrama de *Facebook*: *W32.Koobface*. Este *worm* se reproduce a través de perfiles en redes sociales y enlaces a sitios web infectados. Se origina desde equipos afectados por el gusano, creando una red de zombis o *botnets*. Además, el programa accede datos sensibles y ejecuta *adware* (del inglés, *advertisement*), que consiste en la muestra de publicidad durante la instalación de cualquier programa de forma que se generan ingresos en los anunciados. Además el *Koobface* intenta acceder a los nombres de usuario y contraseñas.

Normalmente se transmite a través de *Facebook*, llegando a tener consecuencias devastadoras si logra infectar una red corporativa, siendo capaz de borrar datos o instalar *software* de forma remota.

- **Bacterias**

Las bacterias no dañan directamente al sistema. Su único objetivo es reproducirse en el equipo infectado llegando a agotar los recursos de memoria y capacidad de procesador, hasta el punto de detener el sistema.

Spyware: Keylogger

Un *keylogger* es un dispositivo que registra toda la información que el usuario teclea. Posteriormente envía esta información al atacante. Supone el ejemplo más conocido de *spyware* y se encuentra disponible en distintas versiones. La primera de ellas constituye literalmente otra variante

del *malware*, que se distribuye a través de virus o gusanos que instalan o ejecutan este programa en el terminal afectado. Asimismo, se pueden adquirir fácil y económicamente *keylogge*r físicos en la web. Estos se conectan al terminal directamente desde la clavija USB, por lo que el usuario los puede emplear con gran facilidad.

Anexo II.II *Spam*

El *spam,* también conocido como "correo basura", se basa en la recepción de correos que el usuario no solicita y que contienen publicidad engañosa, en la que se promueven distintos productos de calidad sospechosa.

Suponen un enorme porcentaje del tráfico que circula por la red, amenazando a la disponibilidad de la capacidad de los servidores (actualmente se calcula que entre el 60 y el 80% de los mails son *spam*) [84]. Normalmente estos mensajes tienen como remitente una dirección falsa. De esta forma, resulta muy difícil localizar al verdadero emisor.

El problema que además engloban estos correos no deseados es que, en muchas ocasiones, albergan virus o *malware*, o contienen enlaces a sitios maliciosos. Con sólo la apertura de estos correos o entrando en los enlaces en que se direcciona para la compra de dichos artículos, el usuario puede ver comprometida la seguridad de su equipo.

Se conocen como *spammers* a las empresas dedicadas al reenvío de estos correos. Aprovechando las cadenas de correos, los envían a infinitas cuentas de correo, extraídas de las redes sociales o mediante el análisis del tráfico en Internet. Los grandes servidores de mensajería electrónica llevan años combatiendo este problema mediante el uso de filtros.

Anexo II.III Ingeniería social

Todas las manifestaciones de *malware* o técnicas delictivas, anteriormente expuestas, tienen en común que precisan de conocimientos informáticos, principalmente en programación. Pero paulatinamente, los ataques han evolucionado, de manera que el conocimiento que necesita el atacante es cada vez inferior al que poseían aquellos primeros hackers en la década de los 90. En este momento se está desarrollando una industria del cibercrimen donde se pueden comprar programas por Internet, o donde aparecen mecanismos que amenazan a la confidencialidad de la información del usuario y demandan un conocimiento nulo (un ejemplo de ello es el *keylogger*). Surge de esta manera una nueva rama del hacking denominada: Ingeniería social.

La ingeniería social es una nueva forma de obtener credenciales y cometer delitos cibernéticos que contrasta con lo expuesto hasta ahora, ya que no se precisan grandes conocimientos científicos. Como es bien sabido, un sistema es tan robusto y estable como lo es su eslabón más débil y está más que demostrado que, en cualquier sistema de información, este eslabón es el usuario. En grandes organizaciones o instituciones, esto supone un problema ya que un enorme número de usuarios se encuentran conectados permanentemente a los sistemas, a través de cualquier dispositivo y cualquier ubicación.

El usuario pasa a ser el objetivo de estas prácticas, que normalmente se realizan a través de un correo electrónico o una llamada telefónica. En ellas el malhechor se hace pasar por el banco o algún organismo y solicita información al cliente para subsanar algún tipo de problema inexistente. En la mayoría de los casos, el usuario cae en la trampa, entregando sin remordimiento información confidencial al atacante.

Este ataque que, parece extremadamente sencillo a primera vista, tiene una enorme efectividad y miles de clientes en todo el mundo se han visto afectados por él. Dentro de la ingeniería social

destacan el *phising* y la estafa nigeriana. En ambas modalidades se busca la obtención de información de forma fraudulenta, con la diferencia de que, en la estafa nigeriana (recibe el nombre porque la mayoría de estos delitos se realizaron en este país), se le ofrece a la víctima un fortuna inexistente, por la cual y en forma de señal para recibirla, se solicita cierta cantidad económica como señal para poder acceder a ella.

Se suele realizar una clasificación de las diversas técnicas que se engloban dentro de la ingeniería social [85]:

- **Técnicas pasivas:** Éstas pueden ser la observación, directa o mediante el uso de cámaras, de lo que el usuario teclea en un dispositivo. Sin que la persona se percate, puede estar mostrando sus contraseñas a un tercero.
- **Técnicas no presenciales**: Las técnicas no presenciales suelen ser llamadas telefónicas en las que el hacker se hace pasar por nuestro banco y nos solicita nuestros datos para subsanar algún problema inexistente. También se pueden realizar mediante carta, fax o correo electrónico.
- **Técnicas presenciales no agresivas:** Buscar en la basura correspondencia con datos personales, la sustracción de agendas y teléfonos móviles o el seguimiento de personas y vehículos, son otras maneras de obtener información.
- **Métodos agresivos:** El robo de información muchas veces se consigue mediante chantaje, extorsión o presión psicológica. Normalmente se busca obtener información sensible para suplantar la personalidad del individuo en la red u obtener sus tarjetas de crédito.

Los países miembros de la UE han plantado cara a esta forma de fraude estableciendo medidas legislativas sancionadoras, que castiguen estas estafas. Así en 2001, los países de la Unión firmaron el Convenio sobre ciberdelincuencia de Budapest [86]. Sin embargo, constantemente hay incidentes de seguridad. Bases de datos completas con millones de usuarios y contraseñas quedan expuestas. Se debe señalar que, cuando alguien efectúa un robo de usuarios y contraseñas de un sitio web determinado, en realidad pone en riesgo a un enorme número de compañías. La reutilización de cuentas de correo y contraseñas, que la mayoría de usuarios realizamos, tiene la culpa de ello. Si alguno de los usuarios robados ha empleado el correo de su empresa y la misma contraseña, para inscribirse en dicha web atacada, su empresa puede verse comprometida.

En julio de 2015, el sitio web *Ashley Madison*, destinado a facilitar la infidelidad de las parejas, fue atacado. Los asaltantes amenazaron a *Ashley Madison* con la revelación completa de los datos a menos que el servicio fuese cerrado. Un mes después, se publicaron más de 39 millones de cuentas. Entre los datos comprometidos se encontraban: fechas de nacimiento, direcciones de correo electrónico, etnias, géneros, domicilios, nombres, contraseñas, historiales de pago, números de teléfono, preguntas y respuestas de seguridad, las preferencias sexuales, nombres de usuario, actividad [87].

ANEXO III: GUÍA DE USO PARA NUEVOS ADMINISTRADORES

En el presente Anexo se ilustrará el uso del sistema WISE, a modo de familiarización gráfica con el entorno, para aquellos nuevos administradores.

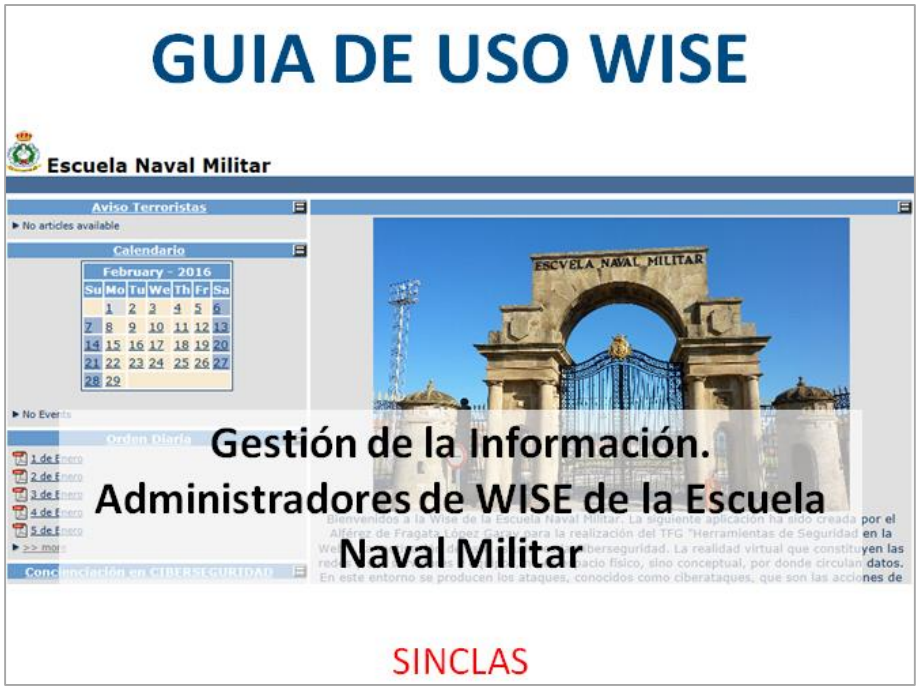

Figura A3-1 Presentación de la guía para uso del gestor WISE

En la Figura A3-2, se muestra el proceso de autenticación.

Figura A3-2 Autenticación

Una vez identificados, en la esquina superior derecha nos aparecerá el icono verde que se muestra en la Figura A3-3 (*Login Ok*). Tras la acreditación como usuarios, en la esquina superior derecha se habilita el acceso a la administración del portal (Figura A3-4).

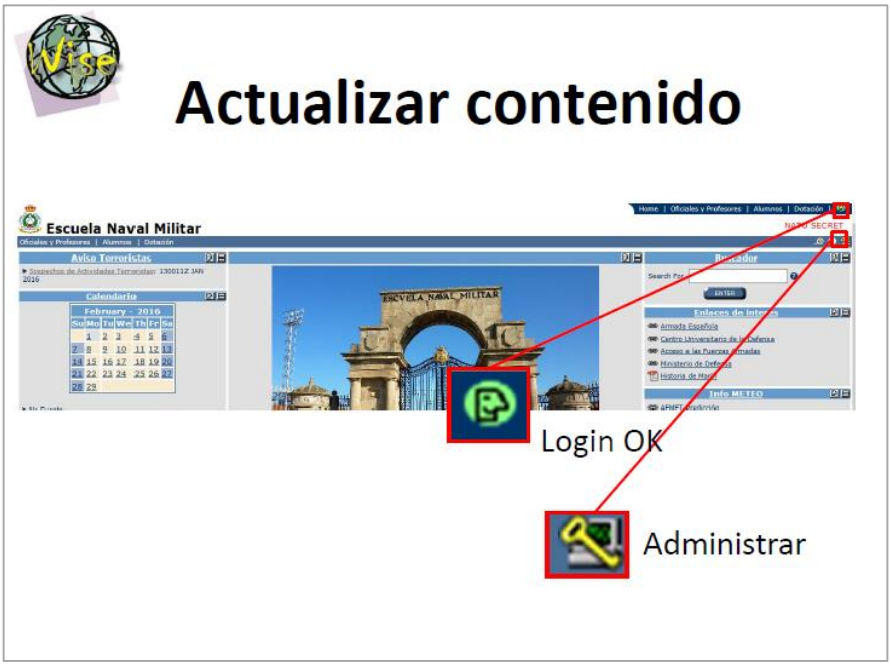

Figura A3-3 Administración del portal

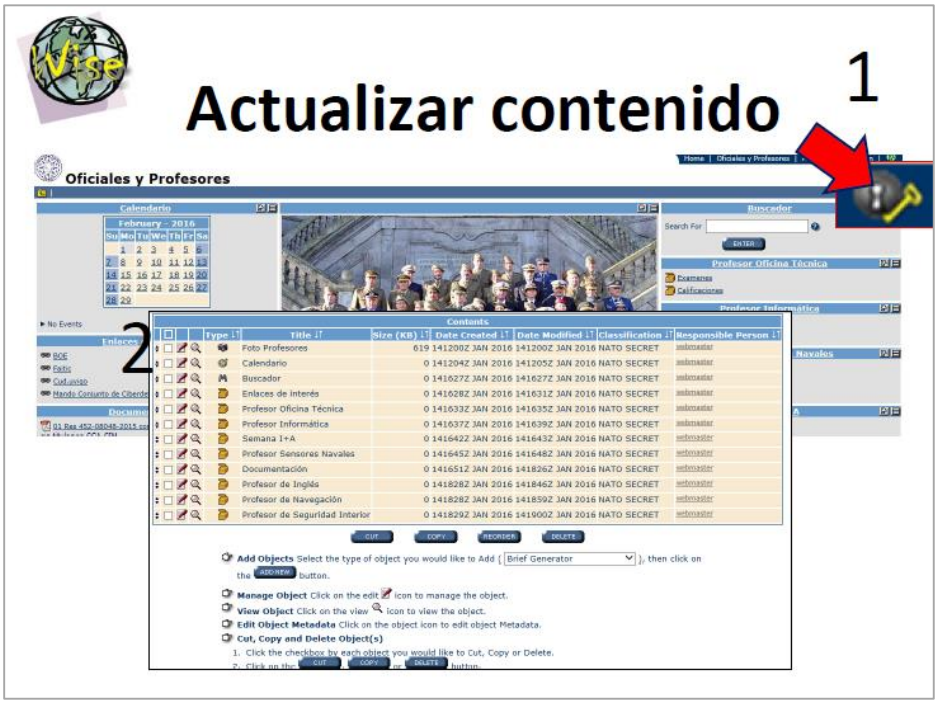

Figura A3-4 Actualizar contenido WISE

En la Figura A3-5 se muestra la disposición de contenidos de la subweb profesor. Esta disposición se relaciona con los objetos WISE empleados.

Figura A3-5 Disposición de contenidos en subweb Oficiales y profesores

Para cada subweb se puede seleccionar la presentación más adecuada (Figura A3-6), de forma que las imágenes y las carpetas se sitúen de una forma ordenada e intuitiva, haciendo de nuestro portal un sitio ameno y ordenado. Igualmente, en la Figura A3-7 se muestra la disposición de archivos. Estos deberán situarse de forma que el contenido global de la página quede compensado y encuadrado en la pantalla, dando un aspecto de seriedad.

Figura A3-6 Presentación empleada

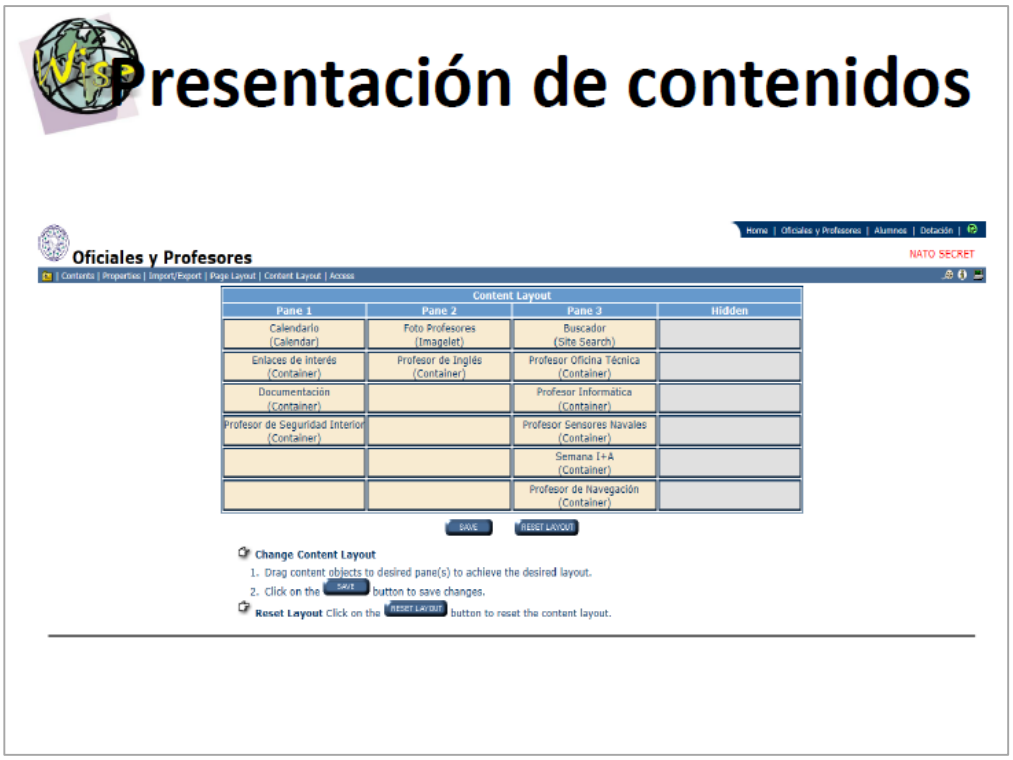

Figura A3-7 Presentación empleada

El control de acceso (Figura A3-8) se deberá configurar dentro de cada subweb. Un punto negativo que presenta el gestor de contenidos es que no se pueden encuadrar los usuarios dentro de un tipo de usuario predefinido, sino que, a cada uno, individualmente, se le deberán otorgar los roles en cada subweb.

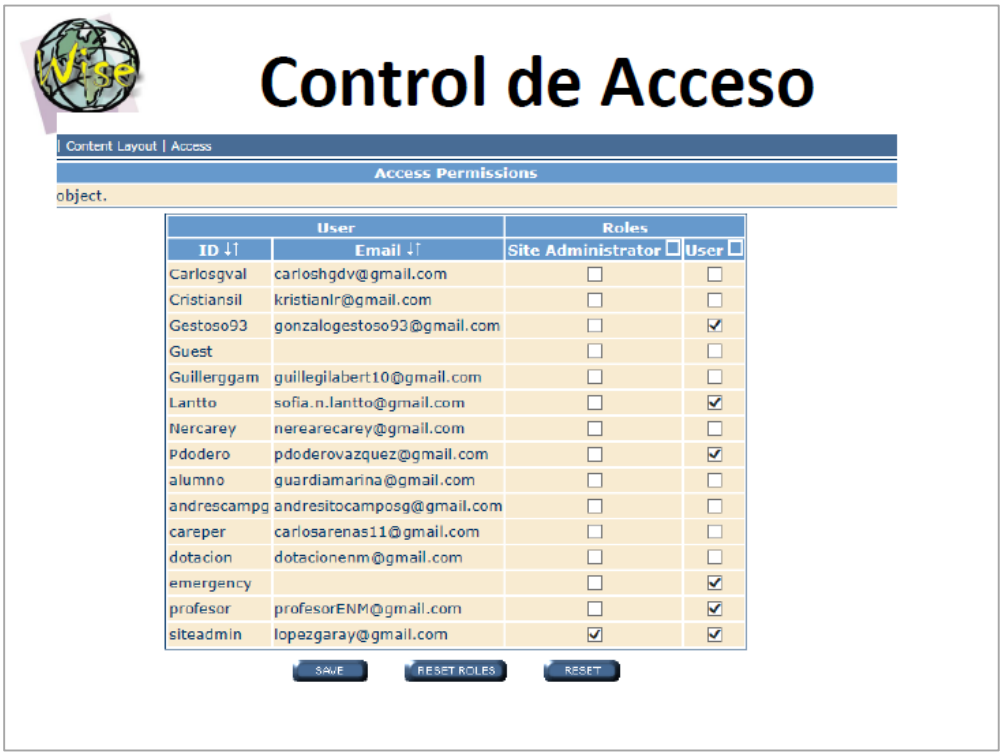

Figura A3-8 Control de Acceso

Como se muestra en la Figura A3-9, para añadir nuevos usuarios, se deberá acceder a la configuración del sitio. Una vez en el menú de configuración, se accederá a *Access* (Figura A3-10) y en la pestaña *Add new*, se desplegará el formulario para generar un nuevo usuario (Figura A3-11)

Figura A3-9 Crear nuevos usuarios (I)

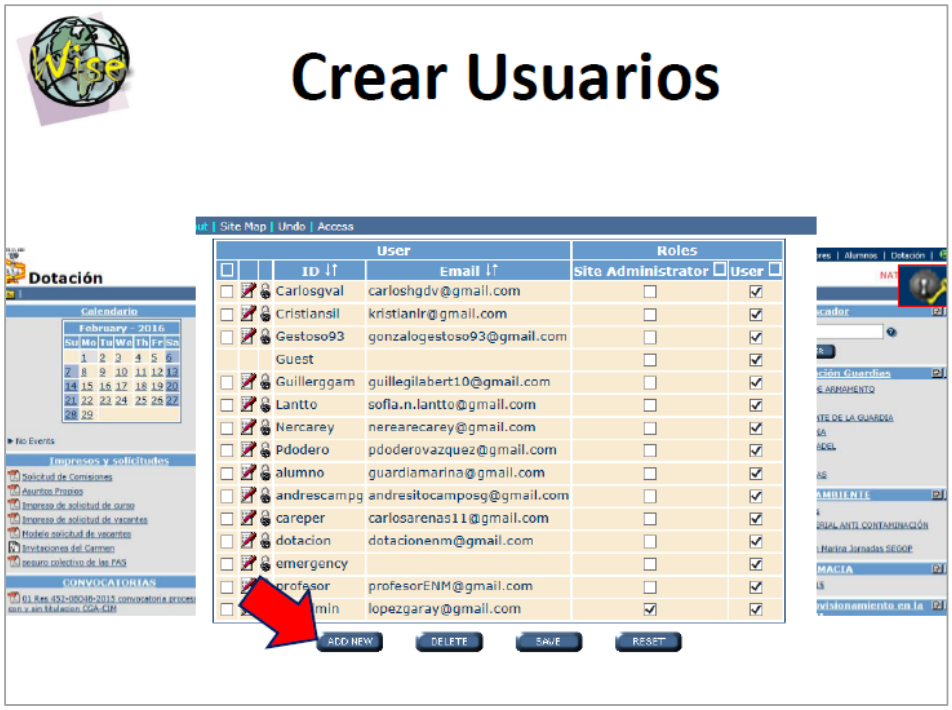

Figura A3-10 Crear nuevos usuarios (II)

Figura A3-11 Formulario para nuevo usuario

En la Figura A3-12, se muestra la organización desarrollada en la subwise Alumnos. Esta disposición de contenidos sigue la estética general que se suele aplicar en estos gestores donde una imagen corporativa ocupa la parte central y la información se localiza a ambas bandas de dicha imagen.

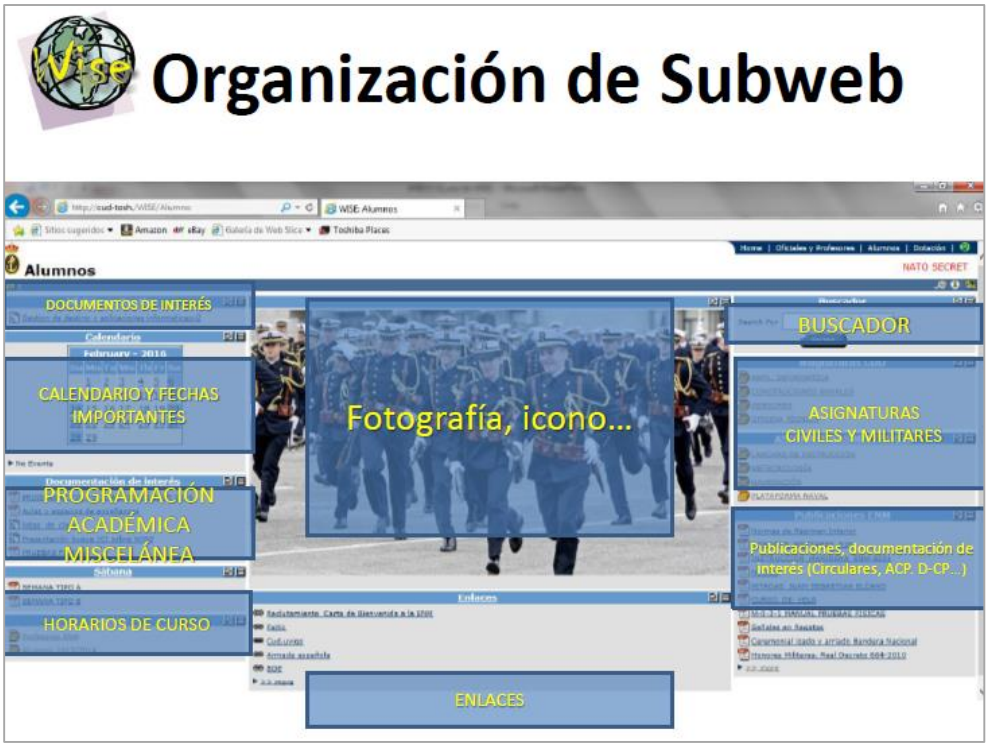

Figura A3-12 Organización WISE

AnexoIII.I Configuración del PC como servidor

El último paso para el despliegue de nuestro gestor de contenidos es la configuración del PC como servidor. Este despliegue ha sido desarrollado en una red local, en el entorno educativo del Centro Universitario de la Defensa en la Escuela Naval Militar. A continuación se describirán los pasos desarrollados para su configuración.

En primer lugar, debemos configurar la dirección IP del equipo como fija. Para ello se accede al Centro de Redes y recursos compartidos. Para ello entraremos en: **Inicio\Panel de Control\Centro de Redes y recursos compartidos**. A continuación, como se refleja en la Figura A3-13 accederemos a Conexión de área local.

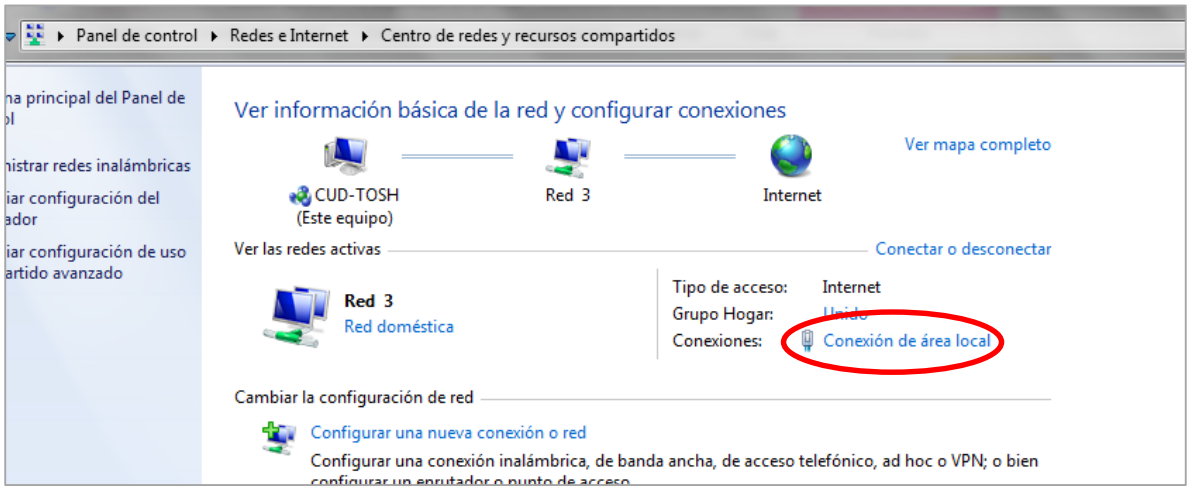

Figura A3-13 Captura: Centro de redes y recursos compartidos

Dentro de conexión de área local, accederemos al menú propiedades (Figura A3-14).

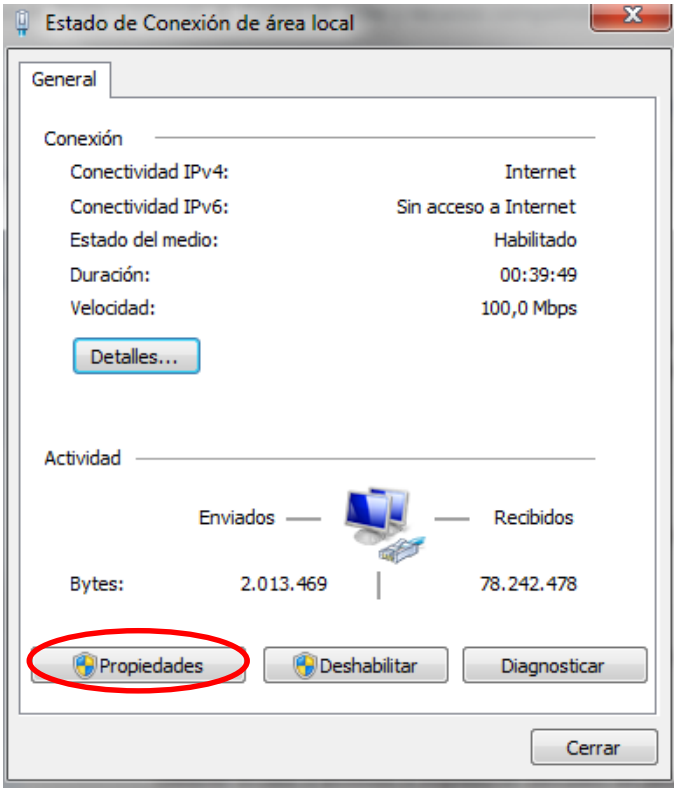

Figura A3-14 Captura: Conexión de área local_Propiedades

A continuación pulsaremos dos veces sobre Protocolo de Internet versión 4 (TCP/IPv4), para acceder a su configuración (Figura A3-15). El menú al que se obtiene acceso permite fijar la dirección IP. Por lo tanto, antes de configurarla, debemos conocer la dirección IP del equipo. Para ello, entraremos en Símbolo del Sistema y teclearemos *ipconfig*. Como muestra la Figura A3-16, el sistema nos devuelve la IP del ordenador, la de la puerta de enlace y la de la máscara de subred.

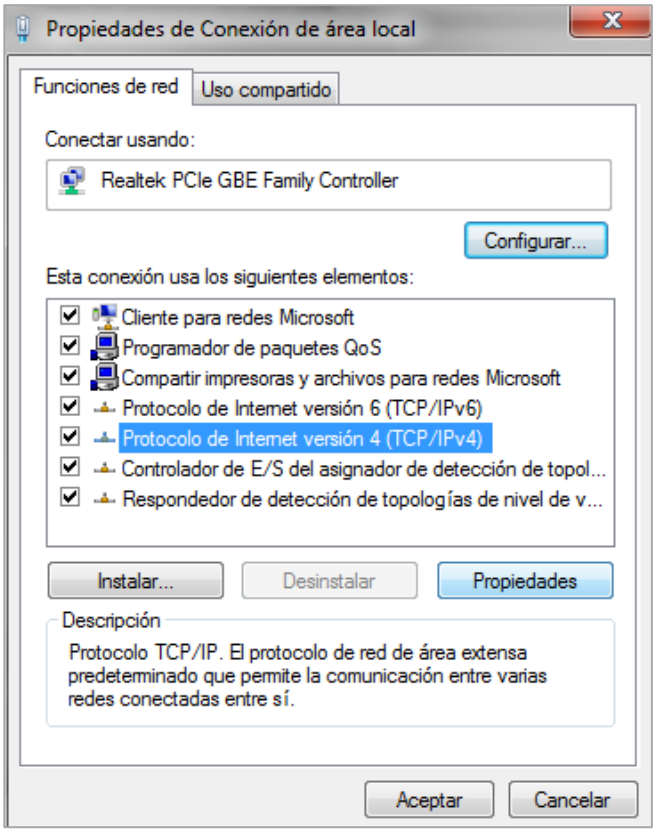

Figura A3-15 Captura: Propiedades de Conexión de área local_ IPv4

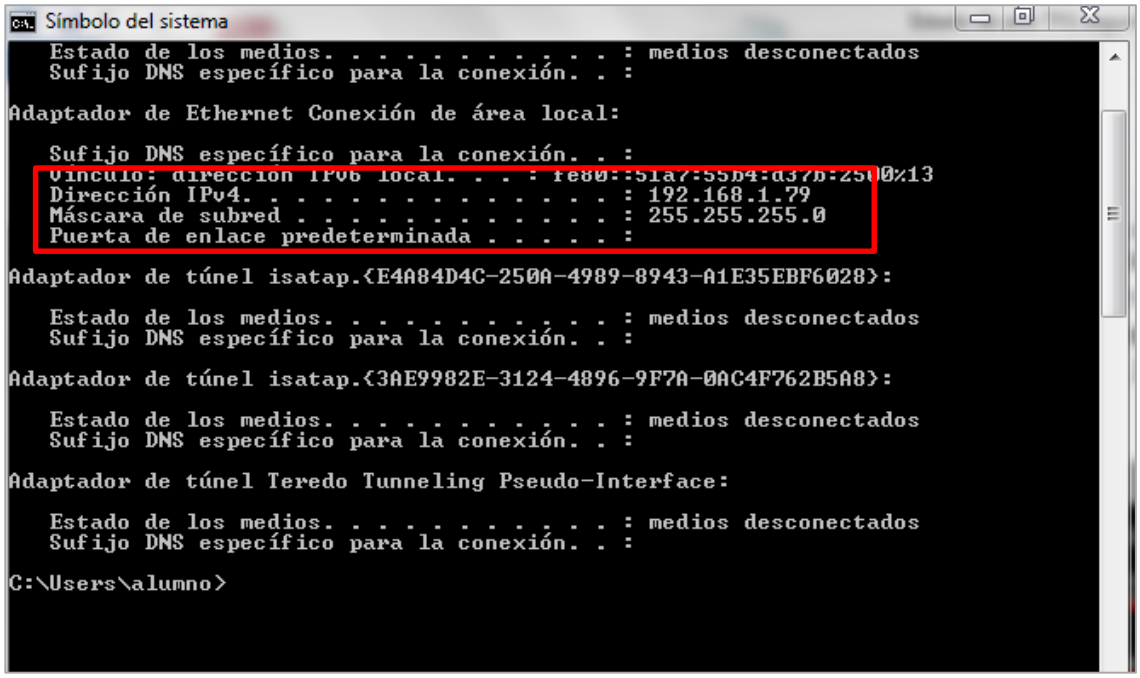

Figura A3-16 Captura: Símbolo del sistema_*ipconfig*

Conocidas estas direcciones, procedemos a fijar la dirección del servidor (Figura A3-17). Como DNS hemos establecido los servidores de dominio de la Universidad de Vigo.

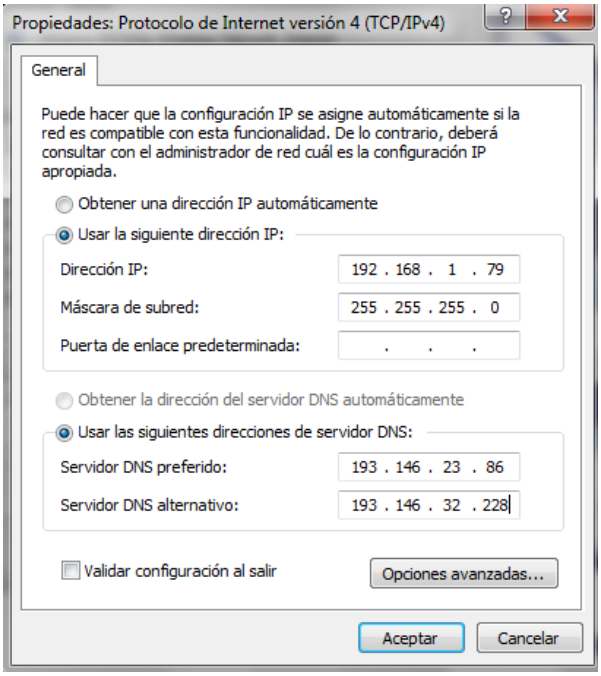

Figura A3-17 Captura: Propiedades_fijar IPv4

El último paso necesario para que el resto de equipos en red puedan acceder al sistema WISE, será desactivar el *firewall* de Windows. Para ello accederemos a: **Panel de control: Sistema y seguridad: Firewall de Windows**. Allí seleccionaremos activar o desactivar Firewall de Windows (Figura A3-18).

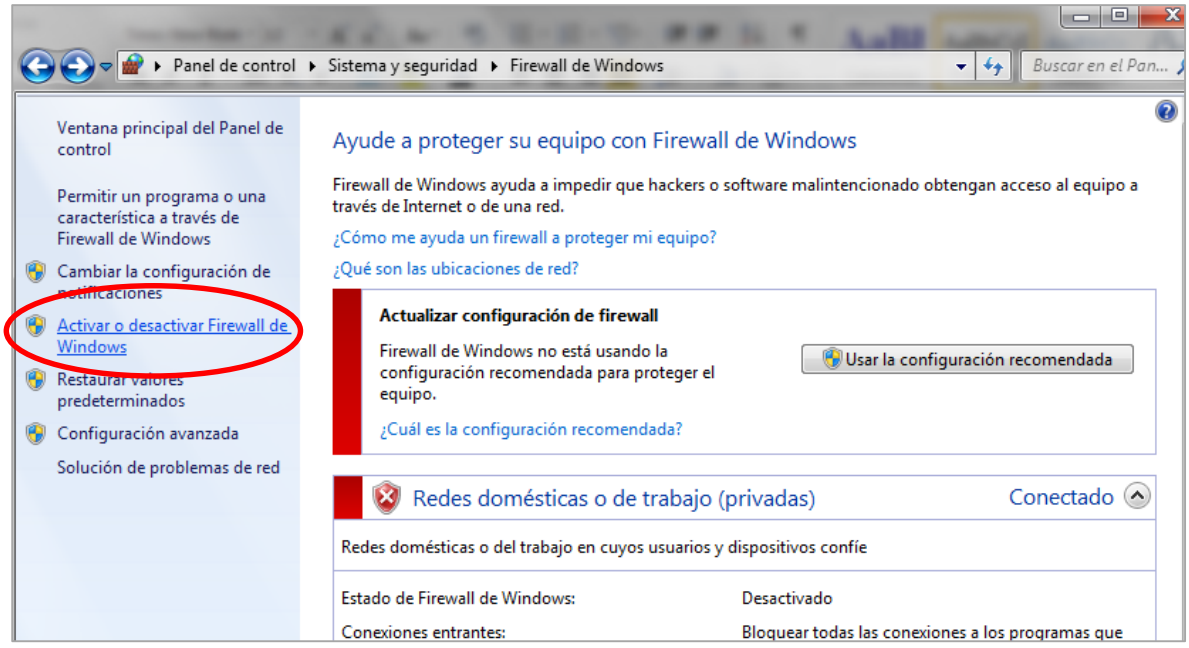

Figura A3-18 Captura: Panel de control_Sistema y seguridad_Firewall de Windows

Y por último, desactivaremos el *firewall* de red doméstica o de trabajo (Figura A3-19). De esta forma, los equipos conectados en la red doméstica podrán acceder a nuestro servidor WISE.

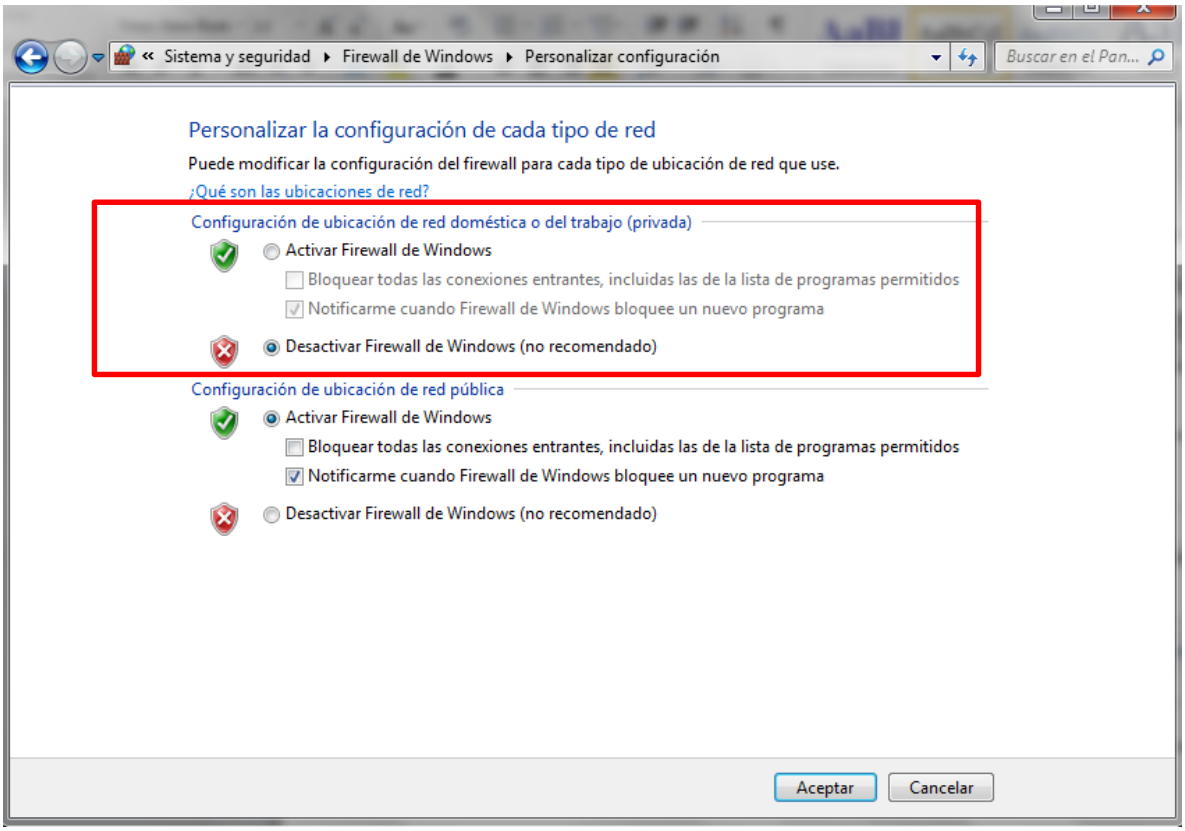

Figura A3-19 Captura: Sistema y seguridad_Firewall de Windows_Personalizar configuración

Llegados a este punto ya tenemos configurado nuestro servidor en el laboratorio. Los equipos conectados en esta red local podrán acceder a él a través del navegador introduciendo la IP 192.168.1.79 o con la URL http://cud-tosh./

Se podrá acceder al sistema desde los siguientes navegadores:

- Internet Explorer.
- Google Chrome.
- Netscape Navigator.
- Netscape Communicator.
- Mozilla.
- Konqueror.

Asimismo, se acceder desde los sistemas operativos: Windows, Linux y MAC.