UNIVERSIDAD AUTÓNOMA DE MADRID

ESCUELA POLITÉCNICA SUPERIOR

Grado en Ingeniería de Tecnologías y Servicios de Telecomunicación

TRABAJO FIN DE GRADO

LABORATORIO DE CIBERSEGURIDAD EN UN ENTORNO EMPRESARIAL VIRTUALIZADO

Javier Gómez Velázquez
Tutor: Víctor A. Villagrá González
Ponente: Jorge E. López de Vergara Méndez

Julio 2015

LABORATORIO DE CIBERSEGURIDAD EN UN ENTORNO EMPRESARIAL VIRTUALIZADO

AUTOR: Javier Gómez Velázquez
TUTOR: Víctor A. Villagrá González

Dpto. de Tecnología Electrónica y de las Comunicaciones
Escuela Politécnica Superior
Universidad Autónoma de Madrid
Julio 2015

Resumen

En la última década el número de amenazas cibernéticas ha crecido de manera exponencial por lo que garantizar la seguridad en Internet de las empresas y de los propios ciudadanos hace cada vez más imprescindible la formación en ciberseguridad. En este contexto, parece fundamental que los graduados en Ingeniería de Tecnologías y Servicios de telecomunicación, como futuros responsables de ciberseguridad ó especialistas en tecnologías de telecomunicación tengan nociones básicas de seguridad.

El principal objetivo de este Trabajo Fin de Grado es la creación de un laboratorio de ciberseguridad basado en un entorno empresarial virtualizado. El diseño teórico de las prácticas del laboratorio se ha basado en la creación de máquinas virtuales configuradas para reproducir una red empresarial virtualizada. Sobre esta base se han creado cuatro prácticas principales. Algunos de los requisitos funcionales que han guiado el diseño han sido el realismo, la portabilidad, su rendimiento, el uso de software de código libre y el control de la complejidad.

La metodología seguida para el diseño de los guiones de las prácticas ha sido a partir de la selección de algunos de los controles de la ISO/IEC 27002 para la implantación de un sistema de gestión de la seguridad de la información. A partir de ahí se ha creado una narración como contexto docente basado en una empresa ficticia que permite al alumno introducirse en un escenario realista y aumentar su motivación. La narración guía al alumno a través de cuatro escenarios de ciberseguridad: ataques asociados a la ingeniería social, uso de equipos en red en entornos externos a la empresa, el diseño y la configuración adecuada de las redes de la empresa como elemento fundamental para evitar ciberataques y el posible control de acceso externo a través de un protocolo cifrado.

El entorno de laboratorio para el desarrollo de las prácticas, así como sus soluciones, ha sido totalmente implementado y validado técnicamente. Este laboratorio podría servir para aportar un material que ofreciera una formación práctica en materia de ciberseguridad al equipo docente del Grado de Ingeniería de Tecnologías y Servicios de Telecomunicación (GITST) o los másteres que se ofrecen en la Escuela Politécnica Superior de la Universidad Autónoma de Madrid. Obviamente, la puesta en práctica de un laboratorio de estas características dentro del plan de estudios excede los objetivos de este trabajo y estará condicionada por múltiples factores académicos y económicos.

El objetivo último ha sido volcar el conocimiento y la experiencia adquirida durante los últimos años, y principalmente durante la realización del TFG, en un producto tangible que pueda despertar el interés en los estudiantes y contribuir a su formación en un área tan relevante y de creciente importancia futura como la ciberseguridad.

Palabras clave

Ciberseguridad, formación, laboratorio, prácticas, sistemas de gestión de la seguridad de la información, entornos de virtualización, red empresarial.

Abstract

In the last decade the number of cyber threats has grown exponentially. Therefore to ensure the Internet security both for companies and citizens makes the training in cybersecurity a necessity. In this context, it can be essential for graduates in Engineering Technology and Telecommunications Services, as future engineers or specialists in cybersecurity, to be trained on the basics of cybersecurity.

The first aim of this Bachelor Thesis is the creation of a cybersecurity-lab in a virtualization environment based on a real corporate network. The theoretical design has been the creation and configuration of virtual machines to reproduce a virtual corporate network. On this basis, four main practical exercises have been created. Some of the functional requirements that have guided the design have been realism, portability, performance, use of open source software and control complexity.

The methodology for the design of the exercises or wargames is based on the selection of some of the ISO / IEC 27002 controls for the implementation of an information security management system. In addition, t a narrative story based on a fictional company has been written aiming to increase students motivation. The narrative guides the student through four cybersecurity scenarios: attacks associated with social engineering, the risk of using corporate computers in external networks, the secure design of a corporate network as the main element to prevent successful attacks and the use of cryptography to protect the confidentiality, authenticity and integrity of information.

The lab environment and the exercises have been fully implemented and technically validated. Obviously, the implementation of this laboratory in a university curriculum goes beyond the scope of this paper and will be conditioned by multiple academic and economic factors.

The ultimate goal has been to exploit as much as possible the knowledge and experience gained in recent years, and mainly during the implementation of this TFG, in a tangible product that can arouse interest in students and contribute to their education in such an important field as cybersecurity.

Keywords

Cybersecurity, training, laboratory, exercises, wargames, information security management system, virtualization environment, corporate network

Agradecimientos

Es de bien nacido ser agradecido y si he finalizado esta etapa en mi vida es porque tengo mucho que agradecer.

Me gustaría empezar por Víctor, que siendo profesor de otra universidad y experto en ciberseguridad aceptó tutorizar este trabajo de fin de grado sin apenas conocerme. Desde el primer día hasta el último ha confiado en mí. Gracias.

También nombrar a Jorge, uno de los profesores más atentos para con los estudiantes de esta escuela. Desde que acudí a él no ha parado de ofrecerme su ayuda y su experiencia para que este trabajo pudiese llevarse a cabo y finalizarse. Gracias.

Agradecer a todos los profesores de la escuela que aunque no lo sepan me han ayudado y me han obligado a mejorar, Susana Holgado, José Luis Castaño, Jorge A. Ruiz Cruz, Jesús Bescós y Luis Salgado. Gracias profes.

Dicen que los amigos de la universidad son los amigos que quedan para siempre, no sé si es verdad, lo que sí sé es que he tenido muy buenos compañeros y que con muchos estoy en deuda. Por lo que agradecer a todos estos compañeros que de una manera u otra me han ayudado y han conseguido hacer esta etapa más fácil. Gracias chicos y chicas.

Quiero darle las gracias a Miguel Rego, director de Incibe, por haberse preocupado de mí, de mi beca y de que mi primera experiencia profesional haya sido en un instituto de ciberseguridad. Gracias.

Agradecerle muy especialmente todo lo que ha hecho y sigue haciendo por mí, a Raúl, mi mentor en Incibe y fuente inagotable de conocimiento, que día tras día, conversación tras conversación, no ha parado de enseñarme y motivarme por la ciberseguridad. Gracias a él he podido entender el verdadero significado de ser un buen ingeniero en todos los niveles, desde el más teórico hasta el más práctico donde hay que "mancharse las manos". Gracias amigo.

Agradecerle con mucho cariño a Carolina toda su involucración y ayuda. Del mismo modo nombrar a Gabriel Arriero, con quién comparto dos aspectos muy importantes en la vida: su familia, y su pasión y dedicación por la ciberseguridad. Gracias.

De una forma muy especial quiero darles las gracias a mis padres y a mi hermana por estar ahí siempre que lo he necesitado. Gracias por la educación y los valores que me habéis regalado. Destacar toda la ayuda que me ha ofrecido y me seguirá ofreciendo mi padre, un gran "teleco". Mencionar también a mis abuelos, porque siempre han estado apoyando a sus nietos, muy orgullosos de nosotros. Gracias familia.

Por último quiero darle las gracias a Laura, la mujer más bella, valiente y sincera que he conocido. Porque gracias a ella los momentos duros no lo han sido tanto y que si no fuera mi compañera de viaje en esta vida, todo sería un bucle de convoluciones a mano, es decir, un martirio.

INDICE DE CONTENIDOS

INDICE DE FIGURAS

INDICE DE TABLAS

1 Introducción

1.1 Motivación

Desde el origen de los ordenadores personales, las redes de comunicaciones de datos y principalmente con el despliegue masivo de Internet los incidentes de seguridad han estado siempre presentes. El gusano de Morris en 1988 en Berkeley, la competición entre grupos de hackers como MOD y LOD en 1990, o el Blue-Boxing que realizaron en la década de los 70 los dos Steves, Jobs y Wozniak, son algunos ejemplos de las primeras experiencias en este tipo de incidentes. La gran mayoría de estos ataques tenían como motivación la curiosidad por las nuevas tecnologías, la diversión o la demostración de quién poseía los conocimientos necesarios para poder acceder a máquinas y entornos que nadie había logrado jamás.

En la última década se ha producido en el campo de la ciberseguridad una transición en los perfiles de los atacantes, su motivación así como en los objetivos de los ataques informáticos. Los atacantes que actualmente están detrás de la mayoría de los ataques a usuarios de internet son delincuentes y mafias cuya única motivación es económica. Estos delincuentes y mafias han visto en internet un nuevo medio para poder explotar sus negocios y sacar beneficio gracias a la rápida adopción de internet por parte de los ciudadanos, empresas y gobiernos, y la falta de conocimientos en materia de ciberseguridad. Desgraciadamente, no sólo los que están etiquetados en el "bando de los malos" hacen uso de las comunicaciones en su propio beneficio, sino que algunas agencias y gobiernos con su gran capacidad económica y conocimientos técnicos realizan constantes ataques contra empresas y otros gobiernos en un contexto que se ha acuñado con el término de “ciberguerra” o “cibervigilancia”. Claros ejemplos de esta ciberguerra son los eventos producidos por el gusano Stuxnet en 2010 [1], los ataques descubiertos en 2014 a la empresa Gemalto en 2011 [2] ó los más recientes a la OPM (Office of Personnel Management) de Estados Unidos en 2015 [3].
En cuanto a la cibervigilancia los hechos más destacados en los últimos años han sido todas las operaciones que estaba llevando a cabo la NSA (National Security Agency) de los EEUU y que Edward Snowden denunció al filtrar numerosos documentos confidenciales.

Ante este escenario y para poder garantizar la seguridad en internet de las empresas y los propios ciudadanos se hace cada vez más imprescindible la formación en ciberseguridad. En este contexto, los graduados en ingeniería de tecnologías y servicios de telecomunicación, como futuros responsables de la ciberseguridad ó simplemente trabajadores involucrados en cualquier ámbito profesional de carácter tecnológico, deben tener las nociones fundamentales de seguridad para poder defenderse de los ataques que recibirán diariamente.

Habiendo realizado un análisis del plan de estudios de la titulación de Grado en Ingeniería de Tecnologías y Servicios de Telecomunicación y de los posteriores másteres en la Universidad Autónoma de Madrid, se ha identificado la necesidad de potenciar la formación de ciberseguridad. Este Trabajo de Fin de Grado (TFG) intenta contribuir a cubrir con un formato escalable esta necesidad detectada.

Por todo ello, el objetivo principal de este TFG se ha centrado en la creación de un laboratorio de ciberseguridad basado en un entorno empresarial virtualizado. Este entorno,

altamente portable e instalable en equipos de rendimiento medio, permitirá que un alumno pueda desarrollar y practicar sus capacidades técnicas, complementando así los conocimientos teóricos obtenidos previamente en una asignatura teórica, en un área tan relevante y de creciente importancia futura como la ciberseguridad.

1.2 Objetivos

El principal objetivo de este TFG es contribuir a la formación en ciberseguridad de los futuros graduados en Ingeniería de Tecnologías y Servicios de Telecomunicación. Para poder desarrollar las capacidades técnicas en materia de seguridad, los alumnos necesitan un entorno donde puedan aplicar y practicar todo lo que aprenden en la parte de teoría en una asignatura de ciberseguridad.

Un segundo objetivo ha sido que las prácticas deben poder ser realizadas por todos los alumnos, tengan conocimientos previos en materia de ciberseguridad o no, por ello se han planteado sobre algunos de los conceptos fundamentales y de una manera gradual para que su comprensión y la curva de aprendizaje sea lo más lineal posible. Además, y desde mi experiencia como alumno de universidad, se ha intentado dotar a todas las prácticas de una historia ficticia que sirva de contexto aparte del propio guión de la práctica y cuyos objetivos son: 1) situar y motivar al alumno posicionándole en un escenario de un ataque y defensa que facilite que pueda entender mejor qué se persigue con cada práctica, 2) que le genere un cierto interés y le permita introducirse en el mundo de la seguridad y 3) que sirva como hilo conductor de todas las prácticas para crear una cohesión como laboratorio de una asignatura.

Con estos objetivos, se han diseñado un conjunto de prácticas de ciberseguridad en las que el alumno pudiese situarse en las dos perspectivas distintas en un incidente de ciberseguridad: por un lado, la perspectiva del atacante y por otro, la de quien tiene que implementar una política y controles de seguridad para que el ataque no tenga éxito.

El último objetivo de este proyecto y no por ello menos importante ha sido volcar una parte del conocimiento técnico en ciberseguridad adquirido durante estos últimos años, y principalmente en la realización de este TFG, en un producto tangible que pueda despertar la pasión por la ciberseguridad en otros estudiantes.

En resumen de todo lo anterior, los objetivos específicos de este TFG son:

- El estudio y análisis del estado del arte en ciberseguridad
- El análisis de las soluciones posibles para el diseño de un laboratorio de ciberseguridad
- El diseño, implementación y validación de un conjunto de prácticas de laboratorio que permitan al alumno adquirir y practicar conocimientos fundamentales en esta materia
- La elaboración de los guiones de las prácticas y su entorno

1.3 Fases de Realización

Para haber podido completar este TFG con éxito se han realizado las siguientes fases:

1) **Investigación:** teniendo en mente la idea principal y los objetivos del TFG había que realizar una investigación para saber cuál era el estado en el que se encontraba la formación en ciberseguridad en el ámbito académico, cuáles eran los estándares de seguridad más implementados por las empresas hoy en día y qué herramientas de virtualización había en el mercado para construir el laboratorio.

2) **Análisis:** una vez completada la labor de investigación y determinados los límites entre los que nos podíamos mover, se inicia la fase de análisis del problema. En esta fase se realizó un análisis de cómo podía ser el escenario de aprendizaje del alumno, qué requisitos hardware y software demandaba el escenario propuesto y que conocimientos teóricos-técnicos se quería que el alumno obtuviese una vez completado el laboratorio.

3) **Diseño:** en esta fase se realizó el diseño, con el nivel de detalle más alto posible, de las prácticas que el alumno iba a realizar y de los componentes del entorno empresarial virtualizado que se iba a necesitar en cada escenario.

4) **Implementación y validación:** terminadas las fases anteriores que servían de base para ésta, se inició la implementación del entorno y las prácticas del laboratorio diseñado en este TFG. Una vez concluido todo el diseño "en papel" en la fase previa, se pasó a la parte práctica donde se crearon las máquinas y redes virtuales que dan nombre al laboratorio de ciberseguridad en un entorno empresarial virtualizado, así como el conjunto de prácticas que lo componen. Este laboratorio será el que el alumno utilice como base para todos los escenarios propuestos en las prácticas. Una vez desarrolladas todas las pruebas junto con el laboratorio, entramos en la fase de validar todo lo realizado. Para ello, se realizaron y documentaron todas las pruebas del laboratorio en el entorno preparado para comprobar que todos los objetivos se cumplían, una validación que consistió en una primera validación técnica realizada por el autor del TFG y una segunda fase en la que se llevó a cabo una validación preliminar del laboratorio por un alumno de la URJC.

5) **Redacción de la memoria:** la última fase, como en todo proyecto, fue la de documentar todo el trabajo realizado y el conocimiento adquirido durante el desarrollo de este TFG.

1.4 Organización de la memoria

La estructura de este documento está estrechamente relacionada con las fases que se han llevado a cabo a lo largo de este Trabajo de Fin de Grado. La memoria conforma un total de siete capítulos junto con un apartado de referencias bibliográficas, un glosario de acrónimos y dos anexos.

- Capítulo 1: Introducción

  Sección inicial en la que se explican la motivación, los objetivos, las fases del proyecto y la estructura de la memoria.

- Capítulo 2: Estado del Arte

  En este apartado se expone toda la investigación previa que ha sido realizada en este TFG en el ámbito de la ciberseguridad en general, los sistemas de gestión de la seguridad de la información y el estándar 27001, el estado actual de la formación en ciberseguridad en las universidades y los entornos de virtualización de máquinas y redes. Este capítulo conforma por lo tanto, la base teórica sobre la que se ha sustentado el diseño e implementación de este proyecto.

- Capítulo 3: Análisis

  Descripción del escenario real que se pretende emular, los conocimientos teóricos-técnicos que se pretenden conseguir por parte del alumnado, los requisitos funcionales y las limitaciones que vienen impuestas por los requisitos hardware y software del laboratorio.

- Capítulo 4: Diseño

  Explicación de cada prueba diseñada para el laboratorio y el entorno necesario para completar con éxito cada una de ellas.

- Capítulo 5: Implementación y validación

  Este apartado describe en detalle todos los pasos que se han seguido para pasar de un diseño teórico a uno práctico y crear el entorno empresarial virtualizado donde se puedan realizar todas las pruebas. De igual forma se complementa con los guiones y soluciones de las prácticas incluidas en los anexos de la memoria. Se muestran los resultados obtenidos de cada prueba así como se corrobora que todo lo que se ha diseñado e implementado cumplen los objetivos, primero a nivel técnico y segundo mediante pruebas con usuarios.

- Capítulo 6: Conclusiones y trabajo futuro

  Para concluir, en este capítulo se realiza una recapitulación de los resultados obtenidos a lo largo de este proyecto y el planteamiento de posibles trabajos futuros que este trabajo fin de grado permite.

- Referencias bibliográficas:

  Catálogo de publicaciones, libros y documentos web que se han ido referenciando a lo largo de este documento y han servido de soporte de información para algunos contenidos de este proyecto.

- Anexo I: Guiones de prácticas

  Apartado que incluye todos los guiones de prácticas completos, con los enunciados de los ejercicios, que un alumno necesitará para poder realizar el laboratorio de ciberseguridad creado en este TFG.

Con el fin de poder establecer un hilo conductor a lo largo de todo el proyecto, todos los capítulos referentes al desarrollo del proyecto (desde el estado del arte hasta la validación) incluyen una introducción que permite situar al lector en un contexto y anticipar el contenido a desarrollar en el resto del capítulo.

Al final de cada uno de los capítulos de desarrollo se realiza una breve conclusión para resaltar las partes fundamentales.

2 Estado del arte

2.1 Introducción

En este capítulo se va a realizar un estado del arte de la situación actual de la ciberseguridad para poder entender por qué es necesaria la formación en esta materia y por ende soportar la justificación de este TFG.

No se puede hablar de ciberseguridad en un entorno empresarial sin hablar de un sistema de gestión de la seguridad de la información, que como su propio nombre sugiere, es un conjunto de políticas y buenas prácticas para la correcta administración de la información. Este término recogido en el estándar ISO/IEC 27001 pretende asegurar la confidencialidad, integridad y disponibilidad de la información en una empresa, por lo que también estudiaremos en este capítulo el origen de este estándar y qué beneficios aporta su implantación en una empresa.

Con este marco global se va a exponer en qué estado se encuentra la formación en seguridad en el ámbito académico universitario y por qué es muy importante su inclusión en los planes de estudios. Es necesario resaltar que aunque esté habiendo un gran impulso para la formación en ciberseguridad por parte de las empresas privadas, la realidad es que en general, en los grados procedentes de los antiguos ingenieros de telecomunicación y en especial en el grado de Ingeniería de Tecnologías y Sistemas de Telecomunicación de la UAM, puede ser beneficioso introducir asignaturas y laboratorios en el plan de estudios en materia de ciberseguridad. Principalmente porque los futuros trabajadores, responsables y directores de empresas tecnológicas en ciberseguridad pueden ser graduados de esta universidad.

Por último se va a realizar un análisis de cuáles son las herramientas y entornos de virtualización que hay en el mercado actual. También se hará hincapié en los motivos que han llevado a las opciones escogidas para el desarrollo del entorno de este TFG.

2.2 Ciberespacio, ciberguerra y ciberseguridad

2.2.1 Ciberespacio

La primera vez que se utilizó el término *ciberespacio* fue en el relato de ciencia-ficción *Johnny Mnemonic* [4] de William Gibson aunque el término no se popularizó hasta su siguiente novela *Neuromante* [5] a principios de los ochenta.

El ciberespacio se podría definir como “un conjunto de sistemas de información interconectados, dependientes del tiempo, junto con los usuarios que interactúan con estos sistemas” [6].

Sin embargo, el ciberespacio es mucho más que Internet, más que los mismos sistemas y equipos, el hardware y el software e incluso que sus propios usuarios, es un nuevo espacio, con sus propias leyes que, a diferencia de los demás espacios, ha sido creado por el hombre para su servicio. Este espacio ha experimentado un enorme y veloz desarrollo, así como la dependencia que nuestra sociedad tiene de él, lo que contrasta con el menor y lento avance en materias de ciberseguridad. Por este motivo, las empresas, gobiernos, particulares,

etcétera que decidan operar en el ciberespacio sobretodo en el ámbito de la seguridad, deben ser conscientes de lo siguiente:

- El ciberespacio es un «campo de batalla» de grandes dimensiones y donde todavía es posible mantener el anonimato. Los ataques se pueden lanzar desde casi cualquier parte del mundo.
- Los efectos de los ataques son desproporcionados con respecto a su coste. Las operaciones se pueden realizar sin necesidad de efectuar fuertes inversiones en recursos humanos y materiales.
- Cada vez más la naturaleza de los ciberataques fuerza a la mayoría de las víctimas, tanto reales como potenciales, a poseer unos conocimientos técnicos avanzados para poder defenderse.
- El ciberespacio no tiene una franja horaria de uso, debido a su acceso e interconexión a nivel mundial el único requisito para realizar un ataque de punta a punta en el globo es tener acceso al ciberespacio. La conexión al ciberespacio de cualquier sistema lo convierte en un objetivo susceptible de ser atacado.

2.2.2 Ciberguerra

Como en todo espacio que el hombre ha podido dominar (tierra, mar y aire) se han producido conflictos bélicos, el nuevo espacio tampoco iba a ser un lugar donde reinase la paz. *«Cyberwar. The thread from the Internet»* [7], la portada y *«Cyberwar»* el título de la editorial del primer número del mes de julio de 2010 de la prestigiosa revista británica The Economist, quería destacar que era el momento de que los países comenzasen a dialogar sobre el control de las armas cibernéticas en Internet.

El editorial comienza analizando como a través de la historia las nuevas tecnologías han revolucionado la guerra, a veces abruptamente, a veces sólo gradualmente; pensemos en el carro de combate, en la pólvora, el avión, el radar o la fusión nuclear. Las Tecnologías de la Información, las computadoras e Internet han transformado de manera radical el mundo según han evolucionado desde el último cuarto del siglo pasado y han dado grandes ventajas a los ejércitos tales como la capacidad de enviar aviones controlados remotamente para capturar inteligencia o desarmar cabezas nucleares enemigas. Sin embargo, la expansión de la tecnología digital también tiene sus riesgos al exponer a los ejércitos y a la sociedad a ciberataques desde cualquier parte del globo. En este mundo globalizado, los gobiernos de los países deben comenzar a pensar en el modo de reducir las amenazas de la ciberguerra con el objetivo de intentar evitar los ataques antes de que sea demasiado tarde o afrontarlas con éxito si se realizan.

Cada vez más aparecen noticias, reportajes y descubrimientos que demuestran que esta ciberguerra ha comenzado y de una manera sigilosa para el ciudadano, aunque le afecte de una manera directa.

Algunos de los hechos que mayor repercusión han puesto de manifiesto esta afirmación fueron los documentos clasificados como alto secreto que fueron filtrados a los periódicos The Guardian y The Washington Post por Edward Snowden, antiguo empleado de la CIA y NSA, donde se indicaban numerosos programas de la NSA incluyendo los programas de vigilancia PRISM y XKeyscore.

La ciberguerra en consecuencia no sólo afecta a los bandos que la conformen, sino también a las personas civiles de todos los estados en los que la tecnología haya sido implantada.

2.2.1 Ciberseguridad

Desde que Internet se empezó a introducir en la sociedad en los años noventa, nuestra sociedad y nuestro modo de vida han ido evolucionando y se han ido expandiendo y adaptando a este medio hasta tal punto que, si la infraestructura de Internet se derrumbase el mundo entraría en caos.

Internet ha tenido una gran inmersión en la vida de las personas gracias a los dispositivos móviles inteligentes y el nacimiento de aplicaciones informáticas de uso comercial para todo tipo de sectores (banca, transporte, consumo, ocio...), donde los usuarios continuamente facilitan datos económicos y personales.

Este increíble auge de las nuevas tecnologías ha supuesto un cambio en las relaciones e interacciones de la sociedad actual, donde usuarios, legisladores y gobiernos no acaban de vislumbrar la forma de ordenar la convivencia en internet. Los "ciberdelitos" han existido desde la creación de la primera red de ordenadores pero toda esta accesibilidad que ofrece internet ha propiciado que el perfil de los atacantes haya ido variando desde los antiguos hackers adolescentes de los 80 a los delincuentes, mafias y grupos terroristas que se han amoldado rápidamente a este nuevo escenario, aprovechando las deficiencias legislativas y del nuevo espacio jurídico. Su adaptación queda demostrada cuando constantemente desarrollan sus actividades ilegales y salen impunes. Estos ciberdelincuentes simplemente han sabido ver en Internet una vía más para cometer sus actos delictivos y no ser juzgados por ellos.

En los últimos años el número de amenazas cibernéticas se ha multiplicado de manera exponencial [8] produciéndose además un cambio en la naturaleza de las mismas; se ha pasado de amenazas conocidas, puntuales y dispersas, a amenazas de gran sofisticación, persistentes y con objetivos muy concretos.

En la actualidad, los ciberataques, los fallos en los sistemas de infraestructuras críticas y el robo de datos o fraude se encuentran en el Top 10 de riesgos globales según el reciente informe 'Global Risk 2015' que publica cada año el World Economic Forum (WEF) [9], en el que refleja la interconexión actual entre riesgos geopolíticos, ambientales, sociales, económicos y tecnológicos.

Dentro de los riesgos tecnológicos, los relacionados con la ciberseguridad ocupan un lugar preeminente como principal preocupación, ya que poseen un grado de probabilidad de ocurrencia y un impacto económico elevado.

Las inversiones de las empresas en la protección de sus activos físicos (ordenadores, muebles de oficina…) son desproporcionadas si las comparamos con lo que invierten en la seguridad de las informaciones digitales. Sin embargo, estas son las más amenazadas. El mes de noviembre de 2014, el Instituto Ponemon publicó un estudio para HP Enterprise Security en el que muestra que el coste medio anual de los ciberataques es de 4.8 millones de euros por empresa: un coste muy superior al de la protección [10].

Por lo tanto la ciberseguridad más que una disciplina añadida al marco de las nuevas tecnologías es una necesidad. La ciberseguridad implica la protección de la información y de los sistemas en los que confiamos en nuestro día a día, ya sea en nuestro hogar, en el trabajo o en los centros educativos. De la ciberseguridad dependen nuestras vidas, desde

los datos privados que confiamos a las empresas y aplicaciones hasta los complejos que alojan armas nucleares que dependan de sistemas informáticos [11].

Debido a todo esto existe una creciente demanda en formar a futuros ingenieros en esta materia y aplicar en todas las empresas que manejen información un sistema de gestión que garantice los tres principios de la ciberseguridad: confidencialidad, integridad y disponibilidad.

2.3 SGSI y el estándar ISO/IEC 27001

2.3.1 Sistemas de Gestión de la Seguridad de la Información

Los rápidos avances en los sistemas de información y telecomunicación han favorecido que se desarrolle hardware y software más asequible para todo tipo de empresas y el usuario doméstico. Debido a la gran inmersión de Internet y su infraestructura, todos estos equipos se han interconectado a través de todo el mundo.

Este despliegue de medios ha generado multitud de oportunidades para las empresas que han visto en Internet un medio más para ofrecer sus productos y servicios. Nacen así, las páginas de comercio electrónico, los sistemas de procesamiento electrónico de datos y todo tipo de aplicaciones, entre las que podemos destacar la de los bancos y los métodos de pago online.

Esta cantidad de tráfico y almacenamiento de información sensible y privada ha suscitado un gran interés en los ciberdelincuentes. Para evitar los posibles vectores de ataques a estas infraestructuras, algunas organizaciones profesionales y de estandarización han diseñado un conjunto de políticas y buenas prácticas para garantizar la seguridad y la fiabilidad de los sistemas de información. Los principios fundamentales de los sistemas de gestión de seguridad de la información son:

- *Confidencialidad*: hablando de privacidad en la información, este principio se basa en prevenir la divulgación de información o datos a sistemas e individuos no autorizados y asegurar que estos datos e información confidenciales solo llegan a manos que están autorizadas a su acceso. Asegurar la confidencialidad es una obligación considerando que una mala gestión de esta puede resultar en fraude, robo de identidad y pérdida económica. Para una empresa o un gobierno puede ser incluso peor, ya que un robo de contraseñas puede derivar en algún tipo de ataque de acceso a áreas con una gran cantidad de información sensible.

- *Integridad*: se refiere a los métodos y acciones que se llevan a cabo para proteger la información de alteraciones o revisiones no legítimas, tanto si los datos están en tránsito o almacenados. La integridad básicamente mide si los datos que ha enviado un emisor son los mismos que los que recibe el destinatario. Normalmente, la integridad se suele asegurar a través de las funciones hash. Una función hash simplemente es una función matemática o algoritmo de un solo sentido (como por ejemplo MD5 y SHA-1) que genera un número de una longitud determinada que se denomina valor hash. Cuando un usuario o un sistema envía un mensaje, esto genera un valor hash que también se le envía al destinatario, de tal forma, que si un cambio de un solo bit, el valor hash será completamente distinto.

- *Disponibilidad*: es el principio más básico y fácil de entender aunque no por ello es el menos importante. La disponibilidad se refiere a que los sistemas de telecomunicación y de datos estén preparados cuando un usuario legítimo necesite usarlos. Existen diferentes métodos para garantizar la disponibilidad, dependiendo de si nos enfocamos en un sistema de datos, recursos de red o información simplemente. Un claro ejemplo de ataque contra este principio son los ataques de denegación de servicio, comúnmente abreviados DoS (*Denial-of-service*).

Con el fin de poder garantizar estos principios básicos, las instituciones, las empresas privadas y las organizaciones internaciones de estandarización han desarrollado un conjunto de políticas y buenas prácticas para garantizar la seguridad de la información. Todos estos puntos vienen recogidos de manera rigurosa dentro de los estándares. A partir de los cuales se podrán utilizar para realizar auditorías de seguridad y otorgar las certificaciones correspondientes.

Los estándares de seguridad aseguran que los responsables de los sistemas de información sepan gestionar adecuadamente estos sistemas garantizando los principios fundamentales descritos en los puntos anteriores.

2.3.2 Estándar ISO/IEC 27001

El conjunto de estándares ISO/IEC 27000 [12] es un conjunto de estándares desarrollados y en continua revisión por ISO (International Organization for Standardization) e IEC (International Electrotechnical Comission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización tanto pública o privada como grande o pequeña.

El ISO-27000 especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un SGSI según el conocido "Ciclo de Deming": PDCA – acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Tiene su origen en la segunda parte del estándar británico BS7799 (BS7799:2) y está compuesto a grandes rasgos por el ISM (Information Security Management System), valoración de riesgos y los controles específicos.

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares entre los que se destacan los siguientes:

- ISO 27000: contiene los términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión. Esta norma es gratuita a diferencia del resto de la serie.

- ISO 27001: es la norma principal de requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con la cual se certifican los SGSI de las organizaciones a través de auditores externos.

- ISO 27002: proporciona unas recomendaciones de las mejores prácticas en la gestión de seguridad de la información. Incluye catorce dominios principales cada cual contiene una serie de controles junto con sus guías de implementación para ser aplicados por aquellos que tienen la responsabilidad de iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

Los beneficios que una empresa puede observar después de implantar un SGSI a través del estándar ISO/IEC 27001 son:

1. En primer lugar, obtener una reducción de riesgos debido al establecimiento y seguimiento de controles sobre ellos. Con ello se logra reducir las amenazas hasta alcanzar un nivel asumible por la organización. De este modo, si se produce una incidencia, los daños se minimizan y la continuidad del negocio está asegurada.

2. En segundo lugar, se produce un ahorro de costes derivado de una racionalización de los recursos. Se eliminan las inversiones innecesarias e ineficientes como las producidas por desestimar o sobrestimar riesgos.

3. En tercer lugar, la seguridad se considera un sistema y se convierte en una actividad de gestión. La seguridad deja de ser un conjunto de actividades más o menos organizadas y pasa a transformarse en un ciclo de vida metódico y controlado, en el que participa toda la organización.

4. En cuarto lugar, la organización se asegura del cumplimiento de la legislación vigente y se evitan riesgos y costes innecesarios. La entidad se asegura del cumplimiento del marco legal que protege a la empresa de aspectos que probablemente no se habían tenido en cuenta anteriormente.

5. Por último, pero no por ello menos importante, la certificación del Sistema de Gestión de Seguridad de la Información contribuye a mejorar la competitividad en el mercado, diferenciando a las empresas que lo han conseguido y haciéndolas más fiables e incrementando su prestigio.

La implantación y posterior certificación de estos sistemas no es sencilla ya que supone la implicación de toda la empresa, empezando por la dirección sin cuyo compromiso es imposible su puesta en marcha. La dirección de la empresa debe liderar todo el proceso, ya que es la que conoce mejor que nadie los riesgos del negocio y las obligaciones con sus clientes y accionistas. Además, es la única que puede introducir los cambios de mentalidad, de procedimientos y de tareas que requiere el sistema.

Un certificado mejora la imagen y confianza de la empresa entre los clientes, proveedores y socios que, poco a poco, exigen la certificación para abrir y compartir sus sistemas de información con cualquier empresa. La exigencia de este certificado es el modo de garantizar un equilibrio en las medidas de seguridad entre las partes [13].

Algunos de los controles especificados en la ISO 27002 han servido para marcar el conocimiento teórico y práctico que se pretende que el alumno obtenga una vez finalizadas las pruebas del laboratorio creado en este TFG.

2.4 Formación en ciberseguridad

Últimamente, debido a todas las noticias que los medios de comunicación están emitiendo, se está consiguiendo empezar un proceso de cambio en la gestión de la seguridad de la información que nos rodea. Los ciudadanos están empezando a mentalizarse de que una mala gestión de la seguridad y privacidad en el mundo virtual puede tener consecuencias

directas en el mundo real. Por ello el límite entre ambas cada vez es más difuso. Irremediablemente, la ciberseguridad ha pasado a formar una parte fundamental en la sociedad.

A pesar de este inicio de cambio de mentalidad el Global Information Security Survey de 2015 recoge que el 34.55% de los incidentes tienen su origen en empleados actuales y el 30.42% en antiguos empleados. Esto demuestra que la simple existencia de un departamento de informática o de un CERT (Computer Emergency Response Team) en las empresas no resuelve el problema de la ciberseguridad. Esto es válido para acabar con las incidencias de un mínimo riesgo y que se puedan solucionar estando físicamente en la propia empresa. Aun así, un especialista podrá resolver una situación de crisis siempre a posteriori pero no puede anticiparse al error humano de un empleado que por desconocimiento descargue un archivo malicioso o que proteja su cuenta personal con una contraseña muy débil. La ciberseguridad no es solo responsabilidad del departamento de informática o del CERT, sino de toda la jerarquía de la empresa y de todas las empresas, independientemente de la actividad a la que se dediquen.

Ante este problema, la única solución es la formación en ciberseguridad. Las empresas privadas son poco a poco más conscientes de esta realidad y desde hace unos años se está iniciando una carrera para la formación de sus trabajadores y una demanda de puestos de trabajo en el ámbito de la ciberseguridad. Esto se puede comprobar fácilmente con la última encuesta de ISACA (Information Systems Audit and Control Association) en la que afirma que existen un millón de vacantes en el ámbito de la seguridad de la información, dato que se apoya también en los cálculos realizados por la empresa Cisco. Otras empresas están creando sus propios grupos de seguridad por lo que como bien indican las encuestas la demanda de este tipo de perfil profesional se está disparando. Incluso hay compañías que han visto en este vacío de formación una oportunidad para crear negocio ya que, para recibir una formación en ciberseguridad alguien tiene que ofrecerla, por lo que el espectro de oferta laboral también se amplía.

Como las universidades tienen como fin formar lo mejor posible a sus estudiantes para que se puedan desenvolver en el mundo profesional, es evidente que si el mercado laboral demanda con tanta necesidad un tipo de perfil con unas determinadas competencias, la universidad debe en la medida de lo posible incluir la ciberseguridad en sus planes de estudios. De esta forma, harán más llamativa su oferta académica para aquellos estudiantes a los que les apasione la ciberseguridad o que simplemente deseen cursar un graduado les asegure un puesto de trabajo.

Muchas universidades ya han empezado a ofrecer grados y másteres orientados al mundo de la seguridad y sus múltiples disciplinas, tales como: análisis forense, sistemas de gestión de la seguridad de la formación, auditor de sistemas, etcétera. Algunos ejemplos pueden encontrarse en las titulaciones de grado y máster que se ofrecen en universidades como la Universidad Politécnica de Madrid o la Universidad Carlos III de Madrid.

Este laboratorio podría servir para aportar un material que ofreciera una formación práctica en materia de ciberseguridad al equipo docente del Grado de Ingeniería de Tecnologías y Servicios de Telecomunicación (GITST) o los másteres que se ofrecen en la Escuela Politécnica Superior de la Universidad Autónoma de Madrid

2.5 Entornos de virtualización

Hoy en día la virtualización es uno de los puntos calientes del sector informático a nivel mundial. Las cifras demuestran el creciente número de empresas que virtualizan, prácticamente a todos los niveles posibles la infraestructura de sus servicios y servidores, data centers, etc. Los buenos resultados obtenidos tras su implantación en la mayoría han hecho que su implementación haya sido rápidamente acogida por las empresas tecnológicas.

Aunque esta tecnología haya empezado a ser acogida masivamente en la actualidad lo más sorprendente de todo es que se trate de una tecnología disponible desde hace más de cuarenta años, utilizada fundamentalmente en grandes centros de cálculo, tanto bancarios como militares y universitarios. Algunos de los usos pioneros de la virtualización incluyen al IBM 7704 (en el que la máquina física era la M44 que albergaba varias máquinas lógicas 44X para los procesos), el CTSS desarrollado por el MIT en el IBM 7044 y el proyecto *Atlas* de la Manchester University [14].

Se puede definir la virtualización como el efecto de abstraer los recursos de un computador y proporcionar acceso lógico a recursos físicos para crear, a través de software, una versión virtual de algún recurso tecnológico, como puede ser una plataforma de hardware, un sistema operativo, un dispositivo de almacenamiento u otros recursos de red. Dependiendo del recurso que se abstraiga, individual –almacenamiento, red– o plataforma completa –un servidor, máquina–, y de por quién sea usado ese recurso, podemos clasificar distintos modelos de virtualización.

Se pueden distinguir cuatro modelos principales de virtualización: *virtualización de plataforma, virtualización de recursos, virtualización de aplicaciones y virtualización de escritorio*.

Modelo	Submodelo	Recurso abstraído	Ejemplo(s)
Virtualización de Plataforma	Sistemas operativos invitados	Plataforma hardware completa	VMware Workstation, Parallels Desktop, Sun xVM VirtualBox, VMware Player, Microsoft Virtual PC
	Emulación	Plataforma hardware completa	Bochs, MAME, DOSBox, Hercules, MESS, VirtualPC, Qemu
	Virtualización Completa	Plataforma hardware completa	VMware Server, XenServer, z/VM, Oracle VM, Sun xVM Server, Virtual Server, VMware ESX Server, VMware Server, VMware Fusion, Xen, Hyper-V (en algunos casos solo es posible si existe hardware con soporte de virtualización)
	Paravirtualización	Plataforma hardware completa	Xen, Logical Domains, Oracle VM, Sun xVM Server
	Virtualización a nivel del Sistema Operativo	Plataforma hardware completa	OpenVZ, Linux V-Server, Virtuozzo, FreeBSD´s chroot jails, Free VPS, Solaris Zones y Solaris Containers
	Virtualización a nivel del kernel	Plataforma hardware completa	KVM, User-mode Linux
Virtualización de Recursos	Encapsulación	Recurso individual	
	Memoria virtual	Memoria y disco	Espacio Swap, técnicas de

				paginado de memoria
	Virtualización de almacenamiento		Disco, almacenamiento	RAID, LVM, SAN, NAS, NFS, AFS, GFS, iSCSI, AoE
	Virtualización de red		Red	OpenVPN, OpenSwarm, que permiten crear VPNs
	Unión de interfaces de red (Ethernet Bonding)		Enlaces de red	vHBA (Virtual Host Bus Adapter), vNIC (Virtual Network Interfaces Card)
	Virtualización de E/S		Conexiones de entrada/salida y transporte	Xsigo Systems, 3Leaf Systems, en el futuro: Cisco Systems, Brocade
	Virtualización de memoria		Memoria RAM	
Virtualización de aplicaciones	Virtualización de aplicaciones limitada	Aplicaciones Portables	Sistema operativo	
	Virtualización de aplicaciones completa	Portabilidad Multiplataforma (Cross-platform)	CPU y sistema operativo	Java Virtual Machine, Common Language Runtime, Mono, LLVM, Portable .NET, Perl Virtual Machine, Citrix XenApp, Novell ZENworks Application Virtualizacion, VMware ThinApp, Microsoft Application Virtualization
		Simulación	API del Sistema Operativo, Interfaz	Wine, Crossover office, coLinux, Zebra, Quagga
Virtualización de escritorio			Sistema completo - localización física del escritorio, que se encuentra en un servidor remoto-	Wyse Technology, VMware View, Sun VDI, vDesk de Ring Cube, XenDesktop de Citrix, vWorkspace de Quest Software, o ThinLinc de Cendio

Tabla 2.5-1: Modelos de virtualización según el recurso que se abstrae

En este TFG se ha realizado una investigación de varias herramientas de virtualización para conseguir la que más se adecuase a los requisitos que había que cumplir.

Las herramientas que se barajaron fueron VMWare ESXi, Proxmox, VMWare Workstation, VMWare Fusion y Oracle VirtualBox. Como se puede observar en la tabla las dos primeras están dentro del submodelo virtualización completa y las tres últimas del submodelo sistemas operativos invitados, ambos submodelos se encuentran dentro del modelo virtualización de plataforma.

Las dos primeras opciones se diferencian de las siguientes en cuanto que necesitan del concepto denominado *hipervisor*.

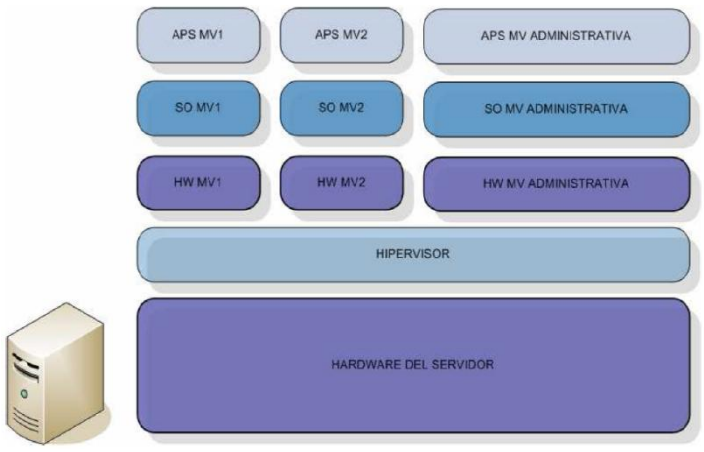


Figura 2.5-1: Capas de virtualización con hipervisor

El *hipervisor* o *hypervisor* es un pequeño monitor de bajo nivel de máquinas virtuales que se inicia durante el arranque, antes que las máquinas virtuales, y que normalmente corre justo sobre el hardware (denominado en algunos textos como native o baremetal) como podemos observar en la figura anterior, aunque también lo puede hacer sobre un sistema operativo (llamado en este caso *hipervisor hosted*).

Esta capa adicional de virtualización proporciona dos funcionalidades básicas:

- Identifica, capta, maneja y responde a operaciones de CPU e instrucciones privilegiadas o protegidas emitidas por las máquinas virtuales.

- Maneja el encolado, envío y devolución de resultados de peticiones de acceso a los recursos hardware instalados en el host anfitrión por parte de las máquinas virtuales.

Por todo esto cualquier modelo basado en *hipervisor* sólo podrá gestionar máquinas virtuales con sistema operativo, librerías y utilidades compiladas para el mismo hardware y juego de instrucciones que el de la máquina física.

Las tres últimas opciones: VMWare Workstation, WMWare Fusion y Oracle Virtualbox pertenecen al submodelo *sistemas operativos invitados.*

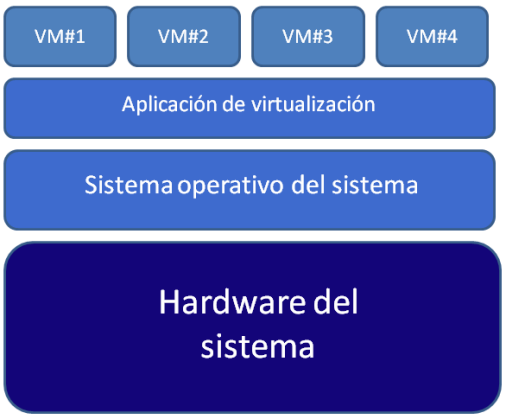


Figura 2.5-2: Modelo de virtualización de aplicación con sistemas operativos invitados.

Esta categoría se basa en una aplicación para la virtualización. Al contrario que las dos primeras ésta no hace uso de hipervisor u otra capa de virtualización. La aplicación que permite virtualizar corre sobre la instancia de un sistema operativo denominado host, que permite la ejecución de servidores virtuales como sistemas operativos independientes. Si la aplicación implementa traducción de juego de instrucciones o emulación, permitirá a la máquina física anfitriona ejecutar máquinas virtuales con un sistema operativo, utilidades y aplicaciones diferentes.

3 Análisis

3.1 Introducción

En este tercer capítulo se presenta un análisis de los conocimientos teóricos y técnicos que se pretende que el alumno obtenga una vez haya finalizado el laboratorio de ciberseguridad, el escenario de aprendizaje y los requisitos técnicos para crear el entorno.

Para poder adquirir los conocimientos deseados, el alumno debe poder practicar en un entorno que intente simular lo más posible un escenario real. La especificación del entorno se realizará considerando los recursos posibles disponibles por parte del alumno y la infraestructura del laboratorio y una vez establecidos los dos puntos anteriores, se ajustará el entorno a las limitaciones que ofrece una máquina de prestaciones medias.

En los siguientes apartados se va a realizar un análisis de todos estos aspectos ya que son la base para realizar el diseño y la implementación posterior del laboratorio.

3.2 Análisis de los conocimientos a obtener por el alumno

Este trabajo fin de grado pretende que los alumnos se inicien en el mundo de la ciberseguridad y aprendan los conocimientos fundamentales. El mundo de la seguridad informática se puede abordar desde muchos puntos de vista aunque suele ser más conocido su aspecto ofensivo. Sin embargo, la ciberseguridad no es una cuestión de hackers que se intentan infiltrar en sistemas ajenos para cumplir sus objetivos, sino que es muchos casos más importante establecer el mayor nivel de seguridad en nuestros sistemas cibernéticos.

Como en todo en lo que existe una dualidad, en ciberseguridad también ocurre que no se puede entender sin haber visto su contraparte. Es decir, no se le puede explicar a un alumno como aplicar unas medidas de protección y seguridad si no sabe qué tipo de ataques puede recibir, ya que de esta manera siempre estará por detrás del atacante.

Los controles de seguridad como se ha dicho antes, se aplican para evitar ataques específicos. Se ha considerado cuales son algunos de los vectores de ataque más comunes que suelen comprometer la seguridad de una empresa. A partir de aquí se han establecido los controles que se querían aplicar en cada práctica según los conocimientos que queríamos abordar.

Uno de los retos más difíciles de afrontar en este TFG ha sido el análisis de los conocimientos a obtener por el alumno así como introducir el estándar ISO-IEC 27001 y los controles de la ISO/IEC 27002 de una manera amena para el alumno y no apagar su interés. Como se decía al principio que la parte más llamativa del mundo de la ciberseguridad es la ofensiva y que se necesita conocer esta parte para poder defenderse, se ha utilizado esta premisa para "enganchar" al alumno en el mundo de la seguridad informática y así darle un sentido a las prácticas introduciendo el estándar. El alumno así podrá realizar ataques en un entorno controlado y asimilar los controles que propone el estándar de una manera mucho más atractiva. Por todo esto las prácticas se componen

de dos partes, una desde el punto de vista del atacante y otra desde el punto de vista del defensor.

En total se han realizado cuatro prácticas en las que se espera que el alumno obtenga conocimientos específicos relativos a los siguientes temas:

3.2.1 Práctica 1

Parte 1:

- Ciclo de vida de un ataque de hacking ético
- Principal distribución de GNU/Linux para la auditoría y seguridad informática
- Hacking con buscadores web
- Elementos básicos en un ataque de ingeniería social
- Herramientas técnicas para un ataque de ingeniería social
- Framework principal para realizar ataques a vulnerabilidades de seguridad

Parte 2:

- Los errores técnicos y humanos producidos en un ataque de ingeniería social
- El impacto de este tipo de ataques en una empresa
- Los controles de la ISO/IEC 27002 para la protección contra la ingeniería social
- La capacidad teórica y técnica para implementar dichos controles

3.2.2 Práctica 2

Parte 1:

- Ciclo de vida de un ataque de hacking ético
- Principal distribución de GNU/Linux para la auditoría y seguridad informática
- Principal herramienta de escaneo de puertos en máquinas
- Escaneo básico de puertos
- Vulnerabilidades en el sistema operativo Windows XP
- Framework principal para realizar ataques a vulnerabilidades de seguridad

Parte 2:

- Los errores técnicos y humanos producidos en un ataque en redes públicas
- El impacto de este tipo de ataques en una empresa
- Los controles de la ISO/IEC 27002 referentes al teletrabajo, acceso a redes externas, gestión de vulnerabilidades técnicas y restricciones de instalación de software
- La capacidad teórica para implementar dichos controles

3.2.3 Práctica 3

Parte 1:

- Ciclo de vida de un ataque de hacking ético

- Principal distribución de GNU/Linux para la auditoría y seguridad informática
- Principal herramienta de escaneo de puertos en máquinas
- Escaneos más avanzados de puertos
- Herramienta de escaneo de vulnerabilidades de seguridad
- Vulnerabilidades en un servidor web
- Framework principal para realizar ataques a vulnerabilidades de seguridad

Parte 2:

- Los errores técnicos y humanos producidos en un servidor web mal configurado
- El impacto de este tipo de ataques en una empresa si no se tiene el servidor web en una zona desmilitarizada
- Los controles de la ISO/IEC 27002 referentes a la segregación de redes y gestión de control de cuentas
- Principios fundamentales de un firewall
- Políticas de un firewall
- Segmentación de una red empresarial

3.2.4 Práctica 4

Parte 1:

- Ciclo de vida de un ataque de hacking ético
- Principal distribución de GNU/Linux para la auditoría y seguridad informática
- Herramienta para analizar protocolos
- Identificación de protocolos en redes de comunicaciones
- Consecuencias del uso de comunicaciones no cifradas

Parte 2:

- Los errores técnicos y humanos producidos
- El impacto para una empresa al usar comunicaciones no cifradas
- Los controles de la ISO/IEC 27002 referentes a teletrabajo y acceso a redes y servicios de red externos
- La capacidad teórica para implementar dichos controles

3.3 Análisis del escenario de aprendizaje

En este apartado se va a exponer el escenario real que se ha simulado virtualmente para el desarrollo de las prácticas.

El contexto elegido es el siguiente: una empresa pequeña o una start-up que tiene una infraestructura de red empresarial sencilla para el desarrollo de sus actividades. Se ha denominado una infraestructura sencilla al conjunto de los siguientes elementos:

- *Cortafuegos*: este dispositivo es uno de los elementos técnicos más importantes respecto a la seguridad en una empresa ya que, aparte de ser la primera capa de seguridad, tiene la principal tarea de permitir o bloquear el tráfico que circula

hacia dentro o hacia fuera en una red empresarial o entre las distintas redes de área local virtuales que pueda haber en ésta.

- *Servidor web*: como su propio nombre indica será el encargado de ofrecer el servicio web para albergar la página web de la empresa.

- *Servidor DNS*: es el responsable de realizar las traducciones de los nombres de dominio a sus respectivas direcciones IP y viceversa para las peticiones dentro de la red corporativa.

- *Servidor FTP*: este servidor almacena los archivos que permiten el intercambio de ficheros con una máquina cliente autorizada.

- *Equipos de trabajo:* conforman las distintas máquinas de trabajo necesarias para el desarrollo de las tareas de los trabajadores en una empresa.

El esquema básico de red empresarial que se considera en el escenario del laboratorio es el siguiente:

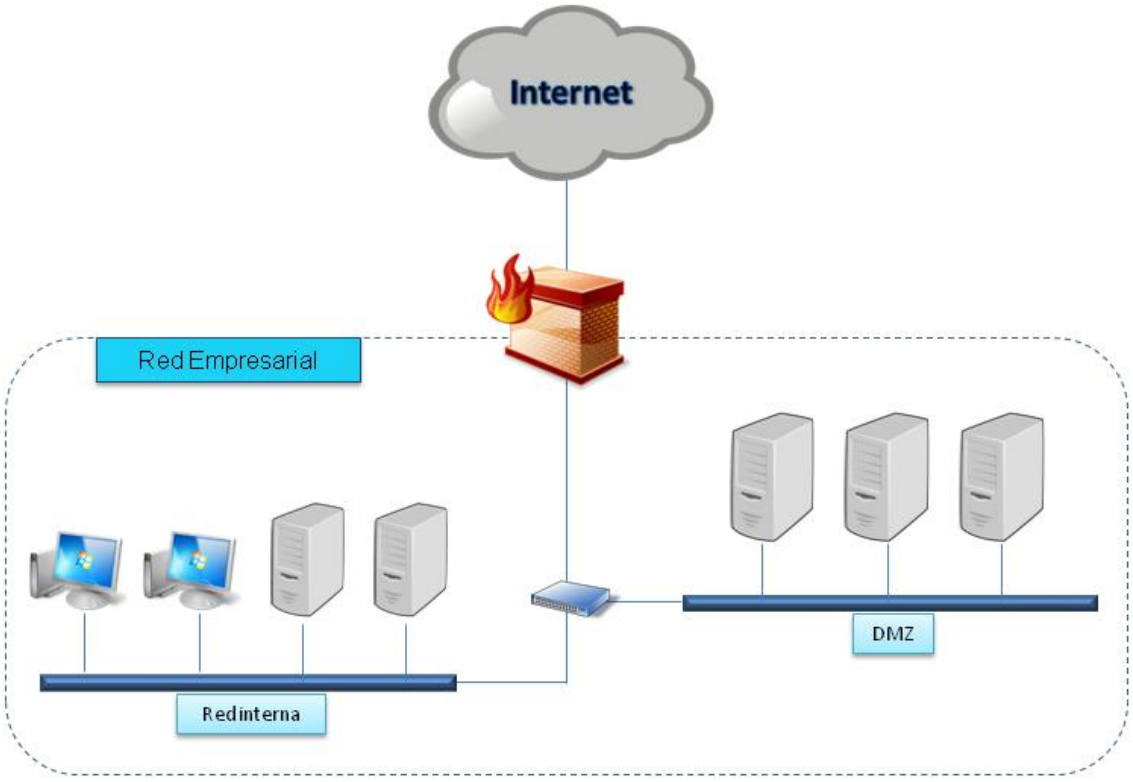


Figura 3.3-1: Red empresarial con segregación.

Esta red empresarial cuenta con dos redes de área local virtuales, una es la zona desmilitarizada y la otra, la red interna de los trabajadores. Con esta configuración, el cortafuegos solo permitiría las conexiones a los puertos que ejecutan un servicio que se quiera exponer a internet en los servidores de la DMZ. Por ejemplo, si la empresa quisiese tener una página web, el cortafuegos debería tener el acceso habilitado al puerto ochenta del servidor web en la zona desmilitarizada. Otro ejemplo podría ser que

la empresa quisiese ofrecer archivos en cuyo caso debería habilitar el puerto 21 para que las conexiones TCP desde el exterior pudiesen establecerse.

En la red interna podrían estarían los servidores de archivos reservados para la empresa, el servidor de correo y los distintos equipos de trabajo personales de los empleados. A esta red nunca le llegarían las peticiones de fuera de la red empresarial asegurando así que no se produjese ningún tipo de ataque externo.

Esta segregación evitaría que si alguno de los servidores que ofrece un servicio a Internet y que simplemente por estar expuesto pueda recibir un ataque, en caso de quedar comprometido, el atacante nunca pudiera pivotar o tener acceso a las máquinas privadas de la empresa. Un modelo imprudente sería el siguiente:

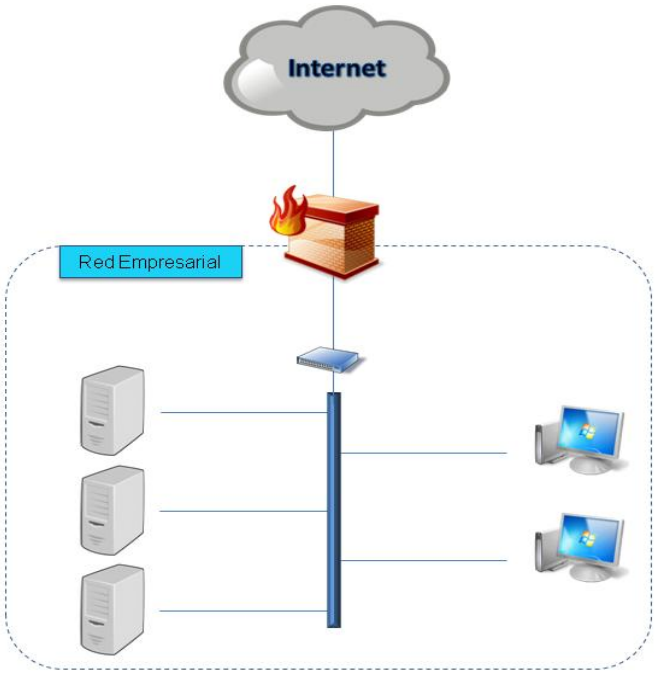


Figura 3.3-2: Red empresarial sin segregación.

En esta configuración un atacante que comprometiese un servidor que ofrece un servicio a Internet podría tener acceso a cualquier máquina del resto de la red.

Es por esta razón que el cortafuegos es un elemento muy crítico en la infraestructura empresarial, ya que una mala configuración de los accesos puede permitir que un atacante consiga conectarse a cualquier equipo privado, con las consecuencias que eso conlleva.

Estos son algunos de los conceptos que se pretende inculcar al alumno, por lo que el entorno que se le entregará al alumno en las prácticas estará mal configurado de tal manera que no exista la segregación de redes. De esta forma, cuando el alumno realice la primera parte de las prácticas desde el punto de vista del atacante podrá aprovecharse de esta mala configuración como lo haría cualquier intruso y estudiar en la segunda parte desde el punto de vista defensor las consecuencias y como evitarlas.

3.4 Análisis del escenario de aprendizaje

En este capítulo se va a realizar un análisis de los requisitos técnicos con los se ha pretendido desarrollar el entorno empresarial virtualizado. Los requisitos funcionales en los que se ha fundamentado el diseño e implantación de este laboratorio de ciberseguridad han sido:

- **Realismo**: el objetivo de este TFG es formar a los alumnos en materia de ciberseguridad en un ambiente profesional por lo que el escenario debe ser lo más real posible.

- **Portabilidad**: el entorno debe ser fácilmente desplegable, trasladable y que pueda ser realizado tanto en las máquinas de los laboratorios como en los equipos portátiles o de escritorio de los alumnos.

- **Rendimiento**: las máquinas virtuales deben poder ser utilizadas sin grandes recursos hardware para ampliar el abanico de posibilidades de los equipos en los que se pudiesen emplear.

- **Software de código libre:** debido a que los fondos para la compra de licencias de la universidad para los laboratorios son limitados y más en tiempos de crisis económica, se plantea la creación del laboratorio a partir de software libre o de licencias de estudiantes y por lo tanto gratuito.

- **Complejidad**: para evitar que los alumnos tengan que necesitar una preparación previa en los entornos de virtualización, se han valorado más los entornos de virtualización que tuviesen un equilibrio entre sencillez y prestaciones.

Como hemos visto en el capítulo anterior el escenario de una empresa real requiere de varios servidores y equipos de trabajo, es por ello que el laboratorio debe tener los servidores y equipos mínimos para crear una infraestructura empresarial realista. Como las máquinas virtuales de los servidores solo se utilizarían para tareas sencillas y no tendrían mucha demanda de recursos, el mínimo de memoria RAM que requerirían serían unos 256Mb o 512Mb por máquina. En el caso de los equipos, con simplemente dos sistemas operativos de Windows obtenidos a partir de las licencias que ofrece la UAM a los estudiantes se podría conseguir un cierto realismo. Con un sistema Windows XP con 256Mb y un sistema Windows 7 con 1Mb de RAM se puede conseguir una funcionalidad satisfactoria para el propósito del laboratorio. Por lo que si sumamos toda la memoria RAM que necesitaría un ordenador personal para utilizar todas estas máquinas virtuales, el resultado de la configuración se asemeja a las prestaciones de un equipo medio a día de hoy.

Tal como se presentó el capítulo 2.5 de este TFG, se realizó una investigación de varias herramientas de virtualización para conseguir la que más se adecuase a los requisitos que había que cumplir. Las herramientas que se barajaron fueron VMWare ESXi, Proxmox, VMWare Workstation, VMWare Player y Oracle VirtualBox. Como se puede observar en la tabla 2.5-1 contenida en el estado del arte de entornos de virtualización, las dos primeras opciones están dentro del submodelo *virtualización completa* y las tres últimas del submodelo *sistemas operativos invitados*, ambos submodelos se encuentran dentro del modelo *virtualización de plataforma*.

Los entornos de virtualización VMWare y Proxmox parecían la mejor elección para crear el laboratorio en un contexto lo más profesional posible. Después de realizar multitud de pruebas analizando estas alternativas durante un periodo de cinco semanas se descartó utilizar estos entornos debido a la necesidad de tener un servidor físico con todo su hardware dedicado a la virtualización, la complejidad en ambas y la falta de documentación en la segunda.

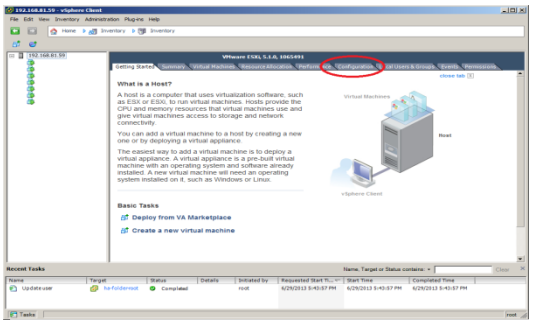


Figura 3.4-1: VMWare ESXi

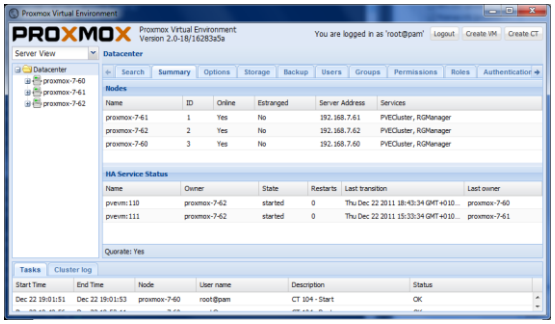


Figura 3.4-2: Proxmox

Por las limitaciones que teníamos y el tipo de entorno que se pretendía crear en este TFG, todas las opciones que se barajaron siempre estuvieron dentro del primer modelo de virtualización, pero finalmente hubo que centrarse en alguna herramienta que estuviese dentro del submodelo *sistemas operativos invitados*.

Por otro lado y al ser un requisito fijado del proyecto el uso de software libre, la opción de VMWare Workstation aunque ofreciese grandes posibilidades, no podía seleccionarse al ser necesario una licencia de pago. La opción gratuita que ofrece VMWare similar a Workstation es VMWare Fusion pero algunos elementos esenciales para la creación de este laboratorio como la clonación de maquinas virtuales no venían incluidos en esta versión libre.

Por todo esto la elección para albergar este entorno virtualizado ha sido finalmente el software de virtualización gratuito desarrollado por Oracle Corporation llamado Oracle Virtualbox. Además esta aplicación ofrece una gran sencillez para los usuarios nuevos en entornos de virtualización que las otras no poseen, por lo que esto beneficiará a los alumnos indudablemente. Aun así, todas las máquinas creadas en este laboratorio pueden ser convertidas y utilizadas en las aplicaciones mencionadas previamente. Es decir, el diseño escalable del laboratorio permite que que si un alumno poseyera una opción de pago de WMWare o la universidad tuviese los fondos para comprar licencias, este laboratorio podría seguir siendo igualmente útil.

Figura 3.4-3: Oracle Virtualbox

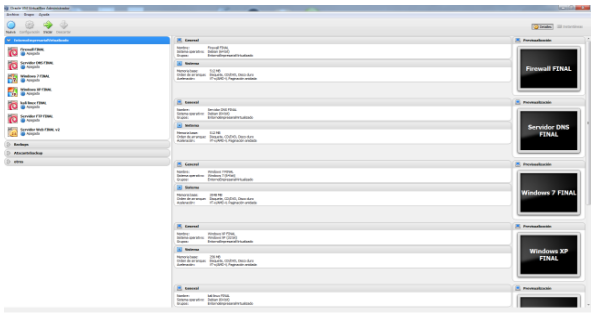


Figura 3.4-4: Máquinas virtuales en Virtualbox

3.5 Conclusiones

En este capítulo se han visto cuáles han sido los conocimientos principales que se espera que obtenga un alumno que realice este laboratorio de ciberseguridad. Se han analizado cuales son las infraestructuras empresariales más básicas que han servido de modelo para la creación de un entorno virtualizado lo más semejante a un entorno real y en donde se desarrollarán las prácticas. Para poder cumplir los requisitos técnicos explicados en el último apartado se ha hecho un estudio de algunos entornos y aplicaciones de virtualización que hay en el mercado actual para llegar a la alternativa sobre la que se han creado todas las máquinas del entorno de laboratorio y las pruebas o prácticas a desarrollar.

4 Diseño

4.1 Introducción

En este capítulo se va a detallar el diseño del laboratorio de ciberseguridad tanto en el entorno como en las prácticas. Los apartados siguientes se van a estructurar de tal forma que se va a ir explicando el diseño de cada práctica dentro de las diversas fases de desarrollo del proyecto.

4.2 Diseño del entorno del laboratorio

En este apartado se va a precisar cómo ha sido el diseño del entorno con un elevado grado de detalle. Como se ha explicado anteriormente en el capítulo de análisis, la red que se pretendía crear debía contener los elementos mínimos con los que se pudiese simular una infraestructura de red empresarial. Todo este entorno debía estar contenido dentro de la aplicación de virtualización Oracle Virtualbox.

La configuración básica la red incluye los siguientes componentes:

- 1 Cortafuegos
- 1 Servidor web
- 1 Servidor DNS
- 1 Servidor de archivos
- 2 Ordenadores personales

Todos estos servidores y ordenadores personales se deben crear como máquinas virtuales en Virtualbox. Para mayor enriquecimiento y aprendizaje del alumno se ha querido dar diversidad a las distribuciones utilizadas quedando de esta manera:

Máquina Virtual	Distribución
Cortafuegos	Debian 7
Servidor web	Metasploitable2
Servidor DNS	Debian 7
Servidor archivos	Ubuntu 14.04 LTS server
Equipo personal #1	Windows XP
Equipo personal #2	Windows 7

Tabla 4.2-1: Distribuciones de SO de las máquinas virtuales

4.2.1 Red

Como se pretendía crear en primera instancia una infraestructura de red insegura para que el alumno pudiese practicar en ella y ver las consecuencias, el modelo que se ha tomado como ejemplo fue el de una red no segregada, es decir, los servidores que tienen servicios expuestos a internet en vez de estar en una zona desmilitarizada estarían dentro de la red interna.

Los servidores que ofreciesen un servicio a Internet debían tener una dirección IP "pública" accesible desde fuera de la red corporativa. Esto serviría para que cuando un cliente realizase una petición TCP a esta IP, el cortafuegos efectuase una traducción de

direcciones IP y enviara la petición a la dirección IP privada de la red local correspondiente.

Al contener estas máquinas una configuración errónea en sus servicios y vulnerabilidades para ser explotadas, no se podían exponer a Internet ni aunque fuese un entorno virtualizado. Por ello, para simular el acceso Internet dentro de la infraestructura virtual se ha diseñado una red interna con un direccionamiento IP privado que obtiene conexión Internet a través de la interfaz NAT de Virtualbox.

Las únicas máquinas que tendrían una interfaz de tipo NAT para tener acceso real a Internet serían la máquina atacante y el cortafuegos. Este último permitiría conexiones desde la red interna a través de sus interfaces hacía la interfaz con conexión a Internet simulado y el Internet real.

La máquina atacante que se ha elegido para este laboratorio ha sido creada a partir de la distribución Kali Linux basada en Debian y diseñada para la auditoría y seguridad informática. Esta distribución fue fundada y es mantenida por Offensive Security Ltd. Mati Aharoni and Devon Kearns. Es bastante conocida en el mundo de la seguridad informática ya que es una evolución de distribución BackTrack.

Puesto que hay dos prácticas que se centran en obtener conocimientos específicos en cómo afecta a la seguridad de la empresa conectarse a redes públicas con ordenadores del trabajo, se ha diseñado también una red "pública" dentro de Virtualbox.

Para entender mejor el entorno se plantea el siguiente diagrama de red:

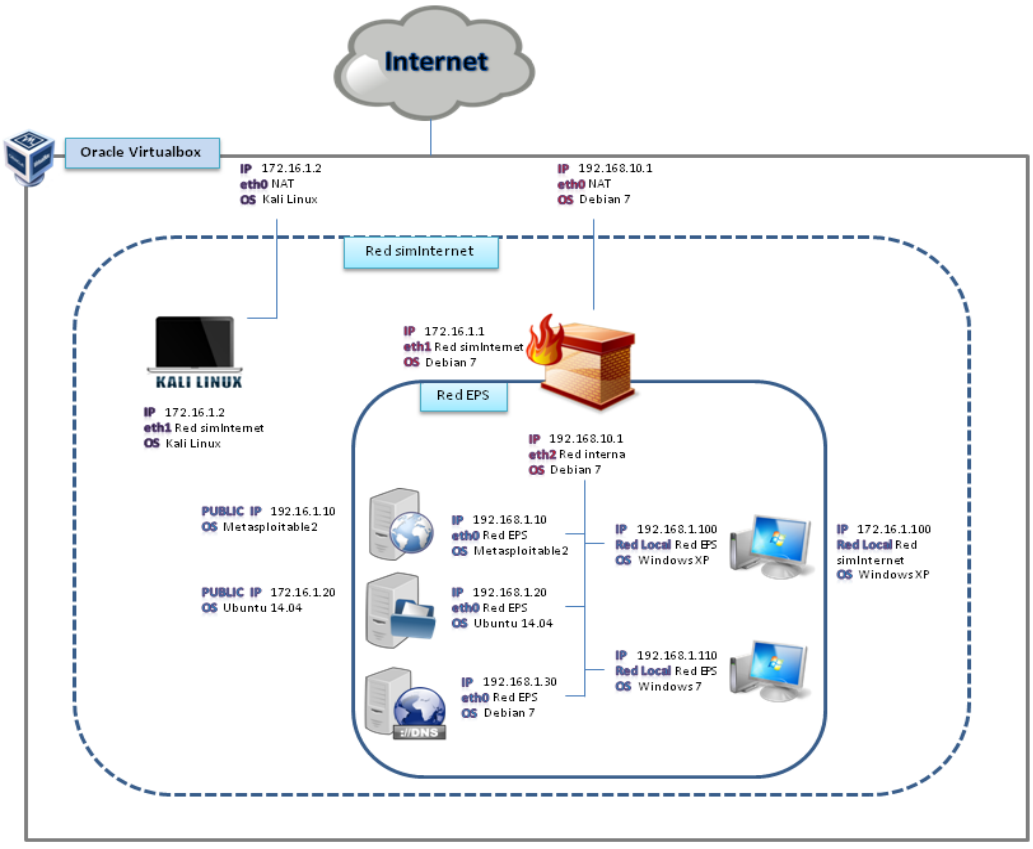


Figura 4.4.1-2: Diagrama de red del escenario de aprendizaje virtualizado

4.2.2 Servicios y configuración

Para que las máquinas funcionen en conjunto como una empresa es necesario instalar los servicios y realizar las configuraciones necesarias en cada uno los servidores.

- *Cortafuegos*: en esta máquina virtual hay que realizar lo siguiente:

    i. Configurar los adaptadores de Virtualbox para que tenga un adaptador por cada red: Internet, Internet simulado y red privada de la empresa.
    ii. Configurar las interfaces de red dentro de la propia máquina en relación con los adaptadores de Virtualbox para que cada una soporte su correspondiente dirección IP estática, máscara de red, dirección IP de broadcast, puerta de enlace predeterminada y dirección IP del servidor de dominios de la empresa.
    iii. Configurar la política del cortafuegos para todo el tráfico de la empresa teniendo en cuenta que está virtualizada.
    iv. Configurar la tabla de enrutamiento y traducción de direcciones del cortafuegos.
    v. Instalar una aplicación de gestión de iptables.
    vi. Crear las cuentas de usuarios correspondientes a los trabajadores de una empresa.

- *Servidor web*: en esta máquina virtual debe realizarse lo siguiente:

    i. Configurar los adaptadores de Virtualbox para que disponer de un adaptador para la red privada de la empresa.
    ii. Configurar las interfaces de red dentro de la propia máquina en relación con los adaptadores de Virtualbox para que cada una soporte su correspondiente dirección IP estática, máscara de red, dirección IP de broadcast, puerta de enlace predeterminada y dirección IP del servidor de dominios de la empresa.
    iii. Modificar la tabla de enrutamiento para que tenga conexión con el cortafuegos.
    iv. Adaptar y modificar todos los archivos necesarios pre-configurados de la máquina Metasploitable2 para que fuesen las del servidor web.
    v. Configurar el servidor apache.
    vi. Realizar una página web sencilla de la empresa ficticia.
    vii. Comprobar todas las vulnerabilidades del servidor y para conseguir accesibilidad desde la red simulada de Internet.
    viii. Crear las cuentas de usuarios correspondientes a los trabajadores de una empresa.
    ix. Introducir las carpetas y datos necesarios para simular archivos de una empresa.

- *Servidor DNS*: en esta máquina virtual debe realizarse lo siguiente:

    i. Configurar los adaptadores de Virtualbox para que realizar un adaptador para la red privada de la empresa.
    ii. Configurar las interfaces de red dentro de la propia máquina en relación con los adaptadores de Virtualbox para que cada una soporte su correspondiente dirección IP estática, máscara de red, dirección IP de

broadcast, puerta de enlace predeterminada y dirección IP del servidor de dominios de la empresa.

iii. Modificar la tabla de enrutamiento para que tenga conexión con el cortafuegos.
iv. Instalar y configurar el servidor de dns bind para que funcione el dominio empresarial ficticio *eps.tfg* en la red empresarial virtualizada.
v. Crear las cuentas de usuarios correspondientes a los trabajadores de una empresa.

- *Servidor de archivos*: en esta máquina virtual debe realizarse lo siguiente:

i. Configurar los adaptadores de Virtualbox para que tenga un adaptador por para la red privada de la empresa.
ii. Configurar las interfaces de red dentro de la propia máquina en relación con los adaptadores de Virtualbox para que cada una soporte su correspondiente dirección IP estática, máscara de red, dirección IP de broadcast, puerta de enlace predeterminada y dirección IP del servidor de dominios de la empresa.
iii. Modificar la tabla de enrutamiento para que tenga conexión con el cortafuegos.
iv. Instalar y configurar el servidor de archivos vsftpd.
v. Configurar con vulnerabilidades los accesos al servicio ftp con los cuentas locales del servidor.
vi. Crear las cuentas de usuarios correspondientes a los trabajadores de una empresa.
vii. Introducir las carpetas y datos necesarios para simular archivos de una empresa.

- *Equipo de trabajo #1 y #2*: en estas máquinas virtuales debe realizarse lo siguiente:

i. Configurar los adaptadores de la máquina #1 en Virtualbox para que tenga un adaptador por cada red: Internet simulado, red "pública" local y red privada de la empresa. En la máquina #2 solo será necesario que esté conectado a la red privada de la empresa.
ii. Configurar las interfaces de red dentro de la propia máquina en relación con los adaptadores de Virtualbox para que cada una soporte su correspondiente dirección IP estática, máscara de red, dirección IP de broadcast, puerta de enlace predeterminada.
iii. Modificar la tabla de enrutamiento para que tenga conexión con el cortafuegos.
iv. Desactivar el cortafuegos de Windows y AV para ser explotable.
v. Crear las cuentas de usuarios correspondientes a los trabajadores de una empresa.
vi. Introducir las carpetas y datos necesarios para simular archivos de una empresa.

4.3 Diseño de las prácticas

Una vez que se ha diseñado el entorno del laboratorio el siguiente paso en el diseño de las prácticas. En cada práctica se han considerado distintas máquinas, herramientas, frameworks, conceptos y escenarios.

Las prácticas que se han diseñado se han dividido en dos grandes bloques, uno desde el punto de vista del atacante y otro desde el punto de vista del defensor, quien tras recibir un ataque decide implantar los controles necesarios de la ISO/IEC 27002 para evitar que sus sistemas vuelvan a ser comprometidos en un futuro.

Para dar un contexto a los ciberataques y que las prácticas no fuesen simples tutoriales sin objetivo claros de formación para el alumno, se han diseñado las prácticas siguiendo una metodología de creación de una historia basada en una empresa ficticia denominada EPS - *Emprendedores Para Siempre*- que permita dar más realidad a las pruebas. Esta empresa ficticia está constituida por varios empleados y departamentos y que son los siguientes: el director gerente, el departamento de recursos humanos, el departamento económico-financiero, el equipo de desarrolladores y un técnico junior para la administración de los sistemas. Para cada una de las anteriores entidades se ha creado una cuenta de acceso en los distintos servidores y equipos de la empresa. Como el objetivo es poder completar con éxito los ataques en un entorno vulnerable, se han configurado incorrectamente estas cuentas y se han dado privilegios más elevados de los necesarios en las distintas máquinas de la empresa.

También, en cada práctica se ha creado una breve historia novelada que sirve para: 1) generar un cierto interés por el mundo de la ciberseguridad, 2) hacer más amena la práctica y 3) situar al alumno en el escenario del ataque y que eso facilite la compresión de las tareas a realizar en el guión de prácticas. A continuación se explicará en qué consiste cada práctica.

4.3.1 Práctica 1: Protección contra malware e ingeniería social

En esta práctica se ha querido mostrar al alumno la eficacia de un ataque de ingeniería social. El ataque que se ha diseñado consiste en la preparación de un correo electrónico malicioso por parte del atacante para el director de la empresa ficticia con la que se pretende obtener el control de la máquina y por lo tanto penetrar en la red corporativa. Para llevar a cabo el ataque con éxito, el atacante ha utilizado la ingeniería social de manera que ha preparado el correo electrónico con información personal a partir de una investigación realizada sobre el objetivo a través de fuentes existentes en Internet.

Las tareas específicas incluidas en esta práctica son:

1. Explicar brevemente la potencia que tiene el hacking con buscadores para recabar información sobre un objetivo
2. Introducir el concepto de ingeniería social
3. Presentar los frameworks BeEF y Metasploit
4. Explicar en detalle cómo cometer un ataque de ingeniería social con los frameworks anteriores
5. Mantener el control de una máquina-víctima después de su explotación
6. Aprender a documentar en una memoria todo un ataque cibernético

7. Analizar los elementos técnicos y humanos que han producido que el ataque haya tenido éxito
8. Analizar el impacto que podría tener este tipo de ataques en una empresa real y como podría repercutir en su economía.
9. Analizar qué medidas implementaría el alumno si fuese el administrador de sistemas de la empresa
10. Identificar los controles de la ISO/IEC 27002 que se deberían implantar en este escenario
11. Implementar teóricamente o técnicamente dos puntos de la guía de implementación de un control que se aplique en este escenario

4.3.2 Práctica 2: Actualización de software y uso de equipos de trabajo fuera de la infraestructura laboral

En el siguiente escenario se ha querido mostrar al alumno posibles situaciones de riesgo asociadas al uso de equipos de trabajo de la empresa en entornos externos. Este tipo de ataques suelen ser muy efectivos debido a que los empleados de una empresa muchas veces asocian la seguridad laboral a un edificio y no a los equipos electrónicos empresariales con información sensible que llevan consigo a todas partes. El ataque de esta práctica consiste en que un atacante realiza un ataque al ordenador de la víctima que está conectada a la red pública de un establecimiento y como al ser una computadora de la empresa, toda la seguridad de ésta queda comprometida en este punto.

Las tareas específicas de esta práctica son:

1. Explicar brevemente la potencia que tiene el hacking con buscadores para geolocalizar objetivos
2. Presentar la herramienta de escaneo de puertos Nmap
3. Realizar un escaneo con opciones específicas a una máquina objetivo
4. Identificar algunas de las vulnerabilidades más conocidas de Windows XP
5. Conocer más en detalle el framework Metasploit
6. Utilizar el intérprete de comandos de Metasploit; meterpreter
7. Mantener el control de una máquina víctima después de su explotación
8. Aprender a documentar en una memoria todo un ataque cibernético
9. Analizar los elementos técnicos y humanos que han producido que el ataque haya tenido éxito
10. Analizar las consecuencias del uso del equipos de trabajo fuera del ambiente laboral y el impacto que podría tener este tipo de ataques en una empresa real y como podría repercutir en su economía.
11. Analizar qué medidas implementaría el alumno si fuese el administrador de sistemas de la empresa
12. Identificar los controles de la ISO/IEC 27002 que se deberían implantar en este escenario
13. Implementar teóricamente el control 6.2.2.

4.3.3 Práctica 3: Segregación de redes y configuración de cuentas

Esta práctica es una de las principales del laboratorio y en la que se quiere mostrar al alumno la importancia estratégica desde el punto de vista de la ciberseguridad de disponer de redes segregadas dentro de una red empresarial. Uno de los conceptos más

fundamentales de este laboratorio que se pretendeenseñar es que el alumno comprenda la importancia de crear una zona desmilitarizada para los servidores que expongan servicios a Internet. En el caso de no existir segregación de redes, si un servidor expuesto a Internet se comprometiese, toda la red empresarial estaría a merced del atacante.

El escenario de la primera parte de esta práctica se basa en que un atacante tras comprometer el servidor web consigue pivotar hacia el servidor de archivos de la empresa privado donde debido a una mala configuración de las cuentas y las contraseñas consigue acceder con las credenciales del usuario root del servidor web.

En la segunda parte de la práctica se enseñarán los conceptos fundamentales de un cortafuegos y se realizará una segmentación de la red con la creación de una zona desmilitarizada.

Las tareas específicas de esta práctica son:

1. Presentar la herramienta de escaneo de puertos Nmap
2. Realizar un escaneo sigiloso con opciones específicas a una máquina objetivo
3. Identificar todas las vulnerabilidades del servidor web en especial la vulnerabilidad de la versión 5.5 de la aplicación Tomcat
4. Introducir diccionario CVE de las vulnerabilidades de seguridad conocidas
5. Conocer más en detalle el framework Metasploit
6. Utilizar el intérprete de comandos de Metasploit; meterpreter
7. Conocer los ataques de fuerza bruta y de diccionario y algunos de los diccionarios más extensos y eficaces de contraseñas
8. Presentar el concepto de 'pivoting'
9. Aprender a documentar en una memoria todo un ataque cibernético
10. Analizar los elementos técnicos y humanos que han producido que el ataque haya tenido éxito
11. Analizar las consecuencias de la falta de segregación de redes en una infraestructura de red de una empresa y el impacto que podría tener este tipo de ataques en una empresa real y como podría repercutir en su economía.
12. Analizar qué medidas implementaría el alumno si fuese el administrador de sistemas de la empresa
13. Identificar los controles de la ISO/IEC 27002 que se deberían implantar en este escenario
14. Estudiar los fundamentos de un cortafuegos
15. Crear una zona desmilitarizada para el servidor web y opcionalmente el servidor de archivos
16. Diseñar una política segura en el cortafuegos tanto para la red interna como para la zona desmilitarizada con sus respectivas traducciones de direcciones y direccionamientos

4.3.4 Práctica 4: Control de acceso externo a través de un protocolo cifrado

En esta práctica se ha querido enseñar al alumno la importancia de usar protocolos con un cifrado seguro en las comunicaciones ya que en caso de no usarlo se estaría exponiendo toda la información que circula por ella, incluyendo obviamente, las credenciales. Por lo que el escenario de esta práctica consiste en que un empleado realiza una conexión no cifrada desde una red externa de la empresa para conectarse a un servidor de la red

empresarial. Al no utilizar un cifrado seguro en las comunicaciones y transmitir toda la información en texto claro, un atacante con un analizador de tráfico podría capturar todas las credenciales del usuario con lo que eso supone para la seguridad de la empresa. En la segunda parte de la práctica se mostrará al alumno la manera de realizar este tipo de conexiones con un cifrado seguro.

1. Explicar brevemente la potencia que tiene el hacking con buscadores para geolocalizar objetivos
2. Presentar la herramienta de escaneo de puertos Nmap
3. Realizar un escaneo con opciones específicas a una máquina objetivo
4. Identificar algunas de las vulnerabilidades más conocidas de Windows XP
5. Conocer más en detalle el framework Metasploit
6. Utilizar el intérprete de comandos de Metasploit; meterpreter
7. Mantener el control de una máquina víctima después de su explotación
8. Aprender a documentar en una memoria todo un ataque cibernético
9. Analizar los elementos técnicos y humanos que han producido que el ataque haya tenido éxito
10. Analizar las consecuencias del uso del equipos de trabajo fuera del ambiente laboral y el impacto que podría tener este tipo de ataques en una empresa real y como podría repercutir en su economía.
11. Analizar qué medidas implementaría el alumno si fuese el administrador de sistemas de la empresa
12. Identificar los controles de la ISO/IEC 27002 que se deberían implantar en este escenario
13. Implementar teóricamente el control 6.2.2.

4.4 Conclusiones

En los apartados anteriores se ha mostrado el diseño teórico de las prácticas del laboratorio para su posterior implementación en el capítulo siguiente. Se ha visto en detalle qué distribuciones se han utilizado para la creación de las máquinas virtuales y cómo deben ser sus configuraciones para implementar la red empresarial virtualizada con el detalle más técnico que lo teórico permite.

Sobre esta base se han creado las cuatro prácticas del laboratorio con tareas específicas para cada una y toda la historia que da soporte al alumno para situarle en un contexto y hacer de este laboratorio un escenario lo más real posible. La metodología seguida para la creación de los guiones de las prácticas ha sido la de crear una historia basada en una empresa ficticia que permite al alumno introducirse en un escenario realista que ayude a conseguir una mayor motivación en su proceso formativo. La narración guía al alumno a través de cuatro escenarios de ciberseguridad: ataques asociados a la ingeniería social, uso de equipos en red en entornos externos a la empresa, el diseño y configuración adecuado de las redes informáticas de la empresa como paso fundamental para evitar ciberataques y el posible control de acceso externo a través de un protocolo cifrado.

5 Implementación y validación

5.1 Introducción

En este capítulo se va explicar cómo ha sido la implementación de todo lo que se ha detallado en la parte de diseño. Por lo tanto en los apartados siguientes se va a desarrollar como ha sido la implementación del entorno del laboratorio, la de las prácticas y cuál ha sido el resultado final.

Los siguientes apartados han sido el punto clave en el desarrollo de este proyecto y la parte más difícil sin duda de este trabajo de fin de grado, ya que se ha pasado del diseño teórico donde todo era posible, al producto final, donde se ha implementado y evaluado todo el contenido del laboratorio para conseguir unas prácticas robustas, flexibles y escalables.

5.2 Implementación del entorno del laboratorio

Este apartado refleja todas las acciones que se han llevado a cabo para implementar el diseño teórico.

Lo primero que hubo que crear fueron las máquinas virtuales en Virtualbox con los requisitos de memoria que se habían calculado y los adaptadores de red necesarios para la instalación. Después se instalaron las distribuciones específicas en cada una de las máquinas, quedando el siguiente resultado final:

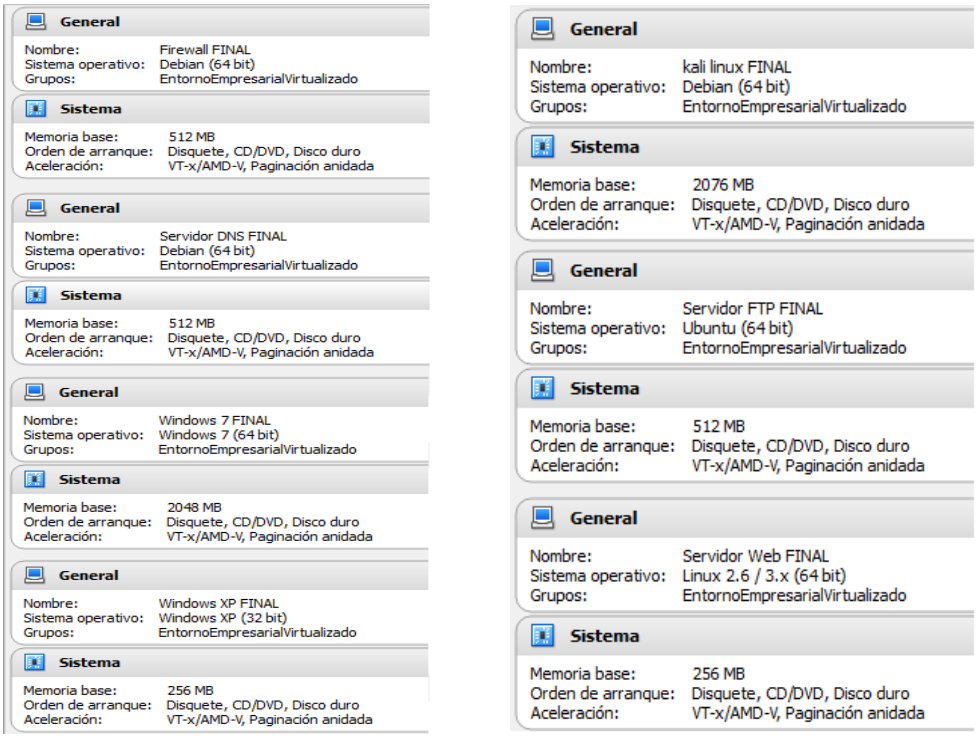


Figura 5.5-1: Máquinas virtuales con sus requisitos técnicos

Una vez se tuvieron todas las máquinas recién instaladas hubo que habilitar los adaptadores de red en Virtualbox dependiendo del número de interfaces de red que necesitaba cada una de las máquinas.

Siguiendo el diseño de red de la figura 4.5.1-2 en el apartado de *Diseño del entorno* en el capítulo *Diseño*, la configuración final es la siguiente:

- Kali linux:
  - lo: esta es la interfaz de local loopback
  - eth0: esta interfaz permite el acceso a Internet a través de la conexión del equipo de anfitrión utilizando un NAT virtual.
  - eth1: esta interfaz permite el acceso a Internet al servidor web a través de la interfaz eth1
  - eth2: esta interfaz está asociada a la red pública de un establecimiento ficticio

.

```
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet dhcp

# The simInternet network interface
auto eth1
iface eth1 inet static
        address 172.16.1.2
        netmask 255.255.255.0
        network 172.16.1.0
        broadcast 172.16.1.255

# The public "Starbucks" network interface
auto eth2
iface eth2 inet static
        address 172.16.10.2
        netmask 255.255.255.0
        network 172.16.10.0
        broadcast 172.16.10.255
```

Figura 5.5-2: Interfaces de red de Kali Linux

- Cortafuegos:
  - lo: esta es la interfaz de local loopback
  - eth1: esta interfaz permite el acceso a Internet a través de la conexión del equipo de anfitrión utilizando un NAT virtual.
  - eth1:0: esta interfaz permite el acceso a Internet al servidor web a través de la interfaz eth1
  - eth1:1: esta interfaz permite el acceso a Internet al servidor de archivos a través de la interfaz eth1.
  - eth2: esta interfaz realiza el papel de conmutador y enrutador de paquetes para la red empresarial EPS.

```
# The loopback network interface
auto lo
iface lo inet loopback

# The simInternet network interface
auto eth1
auto eth1:0
auto eth1:1
iface eth1 inet static
        address 172.16.1.1
        netmask 255.255.255.0
        network 172.16.1.0

iface eth1:0 inet static
        address 172.16.1.10
        netmask 255.255.255.0
        network 172.16.1.0

iface eth1:1 inet static
        address 172.16.1.20
        netmask 255.255.255.0
        network 172.16.1.0

# The EPS network interface
auto eth2
iface eth2 inet static
        address 192.168.1.1
        netmask 255.255.255.0
        gateway 20.20.20.20
        broadcast 192.168.1.255
        network 192.168.1.0
        dns-nameservers 192.168.1.30
```

Figura 5.5-3: Interfaces de red del cortafuegos

- Servidor Web:
  - lo: ésta es la interfaz de local loopback
  - eth0: esta interfaz de red está asociada a la red local de la empresa ficticia EPS

```
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
        address 192.168.1.10
        netmask 255.255.255.0
        network 192.168.1.0
        gateway 192.168.1.1
        broadcast 192.168.1.255
        dns-nameservers 192.168.1.30
```

Figura 5.5-4: Interfaces de red del servidor web

- Servidor FTP:
  - lo: ésta es la interfaz de local loopback
  - eth0: esta interfaz de red está asociada a la red local EPS

```
# The loopback network interface
auto lo
iface lo inet loopback

# The EPS network interface
auto eth0
iface eth0 inet static
        address 192.168.1.20
        netmask 255.255.255.0
        gateway 192.168.1.1
        broadcast 192.168.1.255
        network 192.168.1.0
        dns-nameservers 192.168.1.30
```

Figura 5.5-5: Interfaces de red del servidor ftp

- Servidor DNS:
  - lo: ésta es la interfaz de local loopback
  - eth0: esta interfaz de red está asociada a la red local EPS

```
# The loopback network interface
auto lo
iface lo inet loopback

# The EPS network interface
auto eth0
iface eth0 inet static
        address 192.168.1.30
        netmask 255.255.255.0
        gateway 192.168.1.1
        broadcast 192.168.1.255
        network 192.168.1.0
        dns-nameservers 127.0.0.1
```

Figura 5.5-6: Interfaces de red del servidor dns

- Equipo #1:
  - Conexión de área local 2: interfaz asociada a la red local EPS
  - Conexión de área local 3: interfaz asociada a la primera red pública
  - Conexión de área local 4: interfaz asociada a la segunda red pública

```
Configuración IP de Windows

        Nombre del host . . . . . . . . . . . . : eps-winxp-pc
        Sufijo DNS principal . . . . . . . . . :
        Tipo de nodo . . . . . . . . . . . . . : desconocido
        Enrutamiento habilitado. . . . . . . . : No
        Proxy WINS habilitado. . . . . . . . . : No

Adaptador Ethernet Conexión de área local 4:

        Sufijo de conexión específica DNS :
        Descripción. . . . . . . . . . . . . . : Adaptador Ethernet PCI AMD PCNET Family #4
        Dirección física. . . . . . . . . . . . : 08-00-27-2F-8E-85
        DHCP habilitado. . . . . . . . . . . . : No
        Dirección IP. . . . . . . . . . . . . . : 172.16.1.100
        Máscara de subred . . . . . . . . . . . : 255.255.255.0
        Puerta de enlace predeterminada . . . . :

Adaptador Ethernet Conexión de área local 2:

        Sufijo de conexión específica DNS :
        Descripción. . . . . . . . . . . . . . : Adaptador Ethernet PCI AMD PCNET Family #2
        Dirección física. . . . . . . . . . . . : 08-00-27-E0-31-AA
        DHCP habilitado. . . . . . . . . . . . : No
        Dirección IP. . . . . . . . . . . . . . : 192.168.1.100
        Máscara de subred . . . . . . . . . . . : 255.255.255.0
        Puerta de enlace predeterminada . . . . : 192.168.1.1
        Servidores DNS . . . . . . . . . . . . : 192.168.1.30
                                                 8.8.8.8

Adaptador Ethernet Conexión de área local 3:

        Sufijo de conexión específica DNS :
        Descripción. . . . . . . . . . . . . . : Adaptador Ethernet PCI AMD PCNET Family #3
        Dirección física. . . . . . . . . . . . : 08-00-27-8E-26-D2
        DHCP habilitado. . . . . . . . . . . . : No
        Dirección IP. . . . . . . . . . . . . . : 172.16.10.100
        Máscara de subred . . . . . . . . . . . : 255.255.255.0
        Puerta de enlace predeterminada . . . . :
```

Figura 5.5-7: Adaptadores de red de Windows XP

- Equipo #2:
  - Conexión de área local 2: interfaz asociada en la red local EPS

Figura 5.5-8: Adaptadores de red de Windows 7

Con todas las redes y sus respectivas interfaces configuradas se deben crear las cuentas de acceso y configurar los privilegios según los departamentos de la empresa ficticia en cada una de las máquinas.

Máquina Virtual	Usuarios	Contraseña	Privilegios
Kali Linux	root	toor	Root
Cortafuegos	root	root	Root
	técnico	1234	sudo
Servidor Web	root	root	Root
	técnico	1234	sudo
	desarrolladores	pythonpower	sudo
Servidor FTP	root	root	Root
	técnico	1234	sudo
	director	Realcr7	sudo
	rrhh	loveandpeace	sudo
	desarrolladores	pythonpower	sudo
	eco-finan	wallstreetpros	sudo
Servidor DNS	root	root	Root
	tecnico	1234	sudo
Equipo #1 (Windows XP)	Administrador	root	admin
	técnico	1234	admin
	director	Realcr7	sudo
	rrhh	loveandpeace	sudo
	desarrollad	pythonpower	sudo
	eco-finan	wallstreetpros	sudo
Equipo #2 (Windows 7)	Administrador	admin	admin
	técnico	1234	admin
	director	Realcr7	sudo
	rrhh	loveandpeace	sudo
	desarrolladores	pythonpower	sudo
	eco-finan	wallstreetpros	sudo

Tabla 5.2-4: Cuentas locales de cada máquina virtual

Por último, se tendrán que instalar y configurar todos los servicios que ofrezca cada máquina virtual para lograr así el entorno empresarial virtualizado de una manera totalmente funcional.

Los principales servicios y aplicaciones que se han instalado han sido:

1. *Firewall Builder:* es una aplicación cliente que permite diseñar cómodamente la política de seguridad y luego aplicarla a la máquina cortafuegos de forma directa, mediante una conexión SSH. Dispone de una versión libre y funcional para Linux, así como versiones de pago, aunque con un coste muy bajo, para Windows y Mac OS X. Como nuestro cortafuegos estaba basado en Debian se ha optado por utilizar iptables para definir las reglas.
   En las siguientes imágenes se puede ver como con esta aplicación se ha configurado la política del cortafuegos y la tabla de enrutamiento. Hay que resaltar que se ha configurado erróneamente la política del cortafuegos para que éste sea vulnerable.

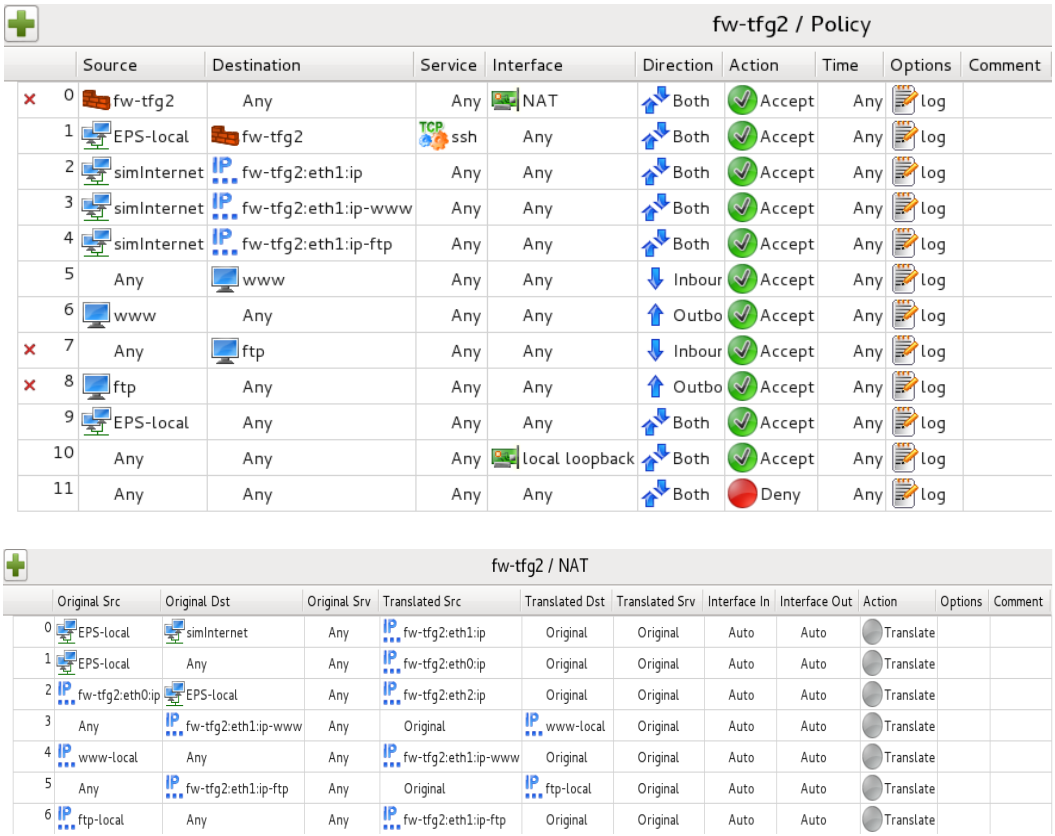


Figura 5.5-9: Política y NAT del cortafuegos en fwbuilder

2. *Servidor Apache*: es un servidor web HTTP de código abierto, para plataformas Unix, Microsoft Windows, Macintosh y otras, que implementa el protocolo HTTP/1.1 y la noción de sitio virtual. Para esta práctica se ha creado una web sencilla de la empresa ficticia simplemente para ilustrar el concepto.

Figura 5.5-10: Página web de la empresa ficticia

3. *Bind*: es el servidor de DNS más común usado en Internet, especialmente en sistemas Unix, en los cuales es un Estándar de facto. Es patrocinado por la Internet Systems Consortium. BIND fue creado originalmente por cuatro estudiantes de grado en la University of California, Berkeley y liberado por primera vez en el 4.3BSD. Paul Vixie ha sido la persona que lo ha mantenido desde 1988.
   Para este laboratorio se ha creado el dominio *eps.tfg*. A continuación se muestran los archivos de configuración de bind donde se han asignado las IPs a los nombres de dominio.

```
root@dns:/home/tecnico# cat /etc/bind/db.eps.local
;
; BIND data file for local loopback interface
;
$TTL            604800
@               IN      SOA     eps.local. root.eps.local. (
                      210620151         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;

eps.local.      IN      NS      ns1.eps.local.

localhost       IN      A       127.0.0.1
eps.local.      IN      A       192.168.1.30

ns1             IN      A       192.168.1.30

www             IN      A       192.168.1.10
ftp             IN      A       192.168.1.20
root@dns:/home/tecnico# cat /etc/bind/db.192.eps.tfg
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@               IN      SOA     eps.tfg. root.eps.tfg. (
                      210620151         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;

1.168.192.in-addr.arpa.         IN      NS      ns1.eps.tfg.

30              IN      PTR     eps.tfg.
10              IN      PTR     www.eps.tfg.
20              IN      PTR     ftp.eps.tfg.
```

Figura 5.5-51: Archivos de configuración de dominio en bind

El funcionamiento de la traducción de dominios se puede comprobar de la siguiente forma:

```
; <<>> DiG 9.4.2 <<>> www.eps.tfg
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15426
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;www.eps.tfg.                   IN      A

;; ANSWER SECTION:
www.eps.tfg.            604800  IN      A       192.168.1.10

;; AUTHORITY SECTION:
eps.tfg.                604800  IN      NS      ns1.eps.tfg.

;; ADDITIONAL SECTION:
ns1.eps.tfg.            604800  IN      A       192.168.1.30

;; Query time: 0 msec
;; SERVER: 192.168.1.30#53(192.168.1.30)
;; WHEN: Mon Jun 29 17:56:20 2015
;; MSG SIZE  rcvd: 79
```

Figura 5.5-62: Comprobación del funcionamiento del dominio con la herramienta dig

4. *Vsftpd*: es un servidor FTP para los sistemas Unix, incluido Linux y tiene una licencia bajo GNU GPL. Vsftpd es el servidor FTP por defecto de las distribuciones Ubuntu, CentOs, Fedora, NimbleX, Slackware y RHEL Linux.

En este laboratorio el servidor FTP se ha realizado una configuración vulnerable de tal manera que se han permitido todas las cuentas locales del servidor de la máquina virtual con las mismas credenciales pero no se han permitido los accesos anónimos.

5. *Correo*: para algunas de las prácticas ha sido necesario crear una cuenta de correo corporativa. Para no complicar a los alumnos con un servicio de correo por línea de comandos se ha creado una cuenta en el servicio de correo electrónico de Gmail con la siguiente dirección: *tfg.eps@gmail.com*.

También para dar más realismo al entorno y como objetivo del atacante en algunas de las prácticas, se han creado carpetas y archivos de la empresa ficticia que se han alojado en algunas máquinas del laboratorio.

5.3 Implementación de las prácticas del laboratorio

En este apartado se han implementado los posibles guiones de las prácticas de un laboratorio de ciberseguridad. Las prácticas completas con los objetivos, las narraciones inventadas y las indicaciones de la memoria se encuentran en el anexo A.

5.4 Validación y resultados

Una vez concluida toda la implementación del entorno del laboratorio y los guiones finales de las pruebas es el momento de evaluar si todo funciona correctamente en la red empresarial virtualizada y cuál es la calidad de las prácticas planteadas.

Para comprobar la validez del entorno virtualizado se han utilizado tres equipos distintos. También las prácticas han sido evaluadas prácticamente por un estudiante de último curso del grado de Ingeniería en Sistemas Audiovisuales y Multimedia de la URJC y teóricamente por el tutor de este TFG profesor de la asignatura Seguridad en Sistemas y Redes de Telecomunicación de la ETSI de la UPM.

Los resultados obtenidos han sido bastante óptimos y muy parecidos a los esperados. Las pruebas han despertado en el alumno el interés por la ciberseguridad y los retos propuestos son adecuados para poder realizarse con un breve conocimiento de seguridad pero manteniendo un nivel de complejidad que resulte gratificante al terminarlo.
Lo único que no se ha podido determinar exactamente es la duración de las mismas, ya que al no poseer el alumno conocimientos previos y no haber visto ninguna asignatura de ciberseguridad durante el grado, su tiempo empleado ha sido más de lo calculado previamente.

Finalmente decir que el uso de los resultados de este TFG para la creación del laboratorio de ciberseguridad dependerá de un análisis previo por parte del equipo docente que desee utilizarlo, por lo que para obtener los resultados de una validación completa habría que esperar a su implantación real dentro del contexto académico adecuado.

6 Conclusiones y trabajo futuro

6.1 Introducción

En el último capítulo de este Trabajo de Fin de Grado se realizará un análisis de todas las fases por las que ha pasado este proyecto hasta llegar a su producto final y se extraerán las conclusiones finales de todo el proceso de desarrollo.

Además, en el apartado de Trabajos Futuros se puntualizará cuáles son los puntos que pueden mejorar este proyecto y principalmente todos los pasos que pueden llevar a hacer realidad la existencia del nuevo laboratorio de ciberseguridad.

6.2 Conclusiones

El objetivo de este TFG ha sido proporcionar un material que pueda servir al equipo docente para complementar la formación práctica en materia de ciberseguridad de los estudiantes en el Grado en Ingeniería en Tecnologías y Servicios de Telecomunicación o en los másteres de ciberseguridad que ofrece la Universidad Autónoma de Madrid. Debido a que la formación en ciberseguridad requiere de una parte práctica muy importante se ha intentado crear un escenario de aprendizaje donde el alumno pueda desarrollar esta actividad situándolo en un escenario lo más fiel a la realidad posible.

Para conseguir este objetivo se han realizado las fases de análisis, diseño e implementación de unas pruebas y de un entorno empresarial virtualizado donde poder realizarlas. Las prácticas conforman un total de cuatro ejercicios, cada una de ellos relacionado con uno o varios puntos del estándar ISO/IEC 27002. Este estándar proporciona las buenas prácticas y guías de implementación de los controles para la implantación de un sistema de gestión de la seguridad de la información recogido en el estándar ISO/IEC 27001. Para dar una mayor visión y motivación al alumno, todas las prácticas cuentan con un contexto didáctico ficticio y dos puntos de vista, desde la postura del atacante y la del defensor.

Además este TFG ha creado un entorno virtual donde se puedan ejecutar todas las prácticas. Este escenario virtualizado basado en un escenario básico de una infraestructura de red empresarial ha conseguido que se pueda utilizar en equipos sin muchos requerimientos de hardware y sin coste económico alguno para la universidad o el estudiante.

Por todo esto se ha conseguido un laboratorio de ciberseguridad flexible, portable, modular y escalable.

Finalmente, el objetivo último ha sido que este trabajo pueda ser de utilidad futura, después de ser analizado por un equipo docente y validado por un mayor número de estudiantes, para el laboratorio de una asignatura de ciberseguridad en la Escuela Politécnica Superior de la Universidad Autónoma de Madrid.

6.3 Trabajo futuro

El primer trabajo futuro sería implementar el laboratorio de ciberseguridad dentro de un plan de estudios de una titulación de Grado en Ingeniería de Tecnologías y Servicios de Telecomunicación. Obviamente, este trabajo futuro está condicionado por muchos factores académicos, económicos y de política universitaria.

Desde un punto de vista técnico y práctico asociado al TFG, algunos de los aspectos a considerar serían:

1) Coordinar los contenidos prácticos del laboratorio con las asignaturas teóricas de la titulación
2) Valorar el interés de los contenidos propuestos en este TFG por los profesores coordinadores responsables del laboratorio
3) Realizar un estudio de viabilidad de análisis de costes y carga docente para la implementación del laboratorio en el centro educativo
4) Dimensionar adecuadamente el esfuerzo del alumno y del profesor para la implementación de las prácticas en función del número de ECTS de las prácticas.
5) Rediseñar las prácticas y esencialmente los guiones para adaptarlas al diseño curricular decidido
6) Finalmente, realizar una evaluación de las prácticas con alumnos voluntarios de la titulación

En segundo lugar y debido a la naturaleza modular y escalable de este TFG, las opciones de mejora y ampliación del laboratorio son ilimitadas. El trabajo futuro más obvio para ampliar este laboratorio es el de crear más prácticas para este entorno virtualizado para cubrir muchísimo mejor todo el espectro de la ciberseguridad. Algunas de las ideas para estas posibles prácticas son las siguientes:

1) Esteganografía: realizar una práctica basado en el intercambio de información a través de mensajes inyectados en imágenes y como detectarlo con estegoanálisis.
2) Ingeniería inversa: a partir de ficheros ofuscados obtener información sensible.
3) Ataques al servidor DNS: aprovechando la infraestructura ya creada se pueden diseñar multitud de ataques como por ejemplo obtener información de la estructura empresarial atacando al servidor de dominio realizando una transferencia de zona.
4) Anonimato: introducir al alumno escaneos de redes y servidores detrás de un proxy o la red Tor.
5) Windows Server: introducir en la infraestructura creada un sistema vulnerable con la autenticación de Active Directory propia de los servidores Windows.
6) Análisis forense: tras recibir un ataque realizar aprender los pasos para realizar un análisis forense con éxito.
7) Implantar más controles de la ISO/IEC 27002 de manera práctica.

Como se puede apreciar, las posibilidades son numerosas y si se desea profundizar en pruebas de este tipo con realizar una investigación en Internet sobre las numerosas competiciones de CTF (Capture The Flag), wargames o hacking-labs, se puede encontrar un abanico de pruebas en todos los niveles de aprendizaje muy interesantes y educativas.

Referencias

[1] Kim Zetter, "Countdown to zero day: Stuxnet and the launch of the world's first digital weapon", Crown, Noviembre 2014, pp. 448

[2] Jeremy Scahill, Josh Begley, "The Great Sim Heist, how spies stole the keys to the encryption castle", The Incercept, Febrero 2015. Disponible en: https://firstlook.org/theintercept/2015/02/19/great-sim-heist/

[3] Kim Zetter, Andy Greenberg, "Why the OPM breach is such a security and privacy debacle", Wired Magazine, Junio 2015. Disponible en: http://www.wired.com/2015/06/opm-breach-security-privacy-debacle/

[4] William Gibson, "Johnny Mnemonic", Omni magazine, Mayo, 1981.

[5] William Gibson, "Neuromancer", Julio, 1984.

[6] *The Economist,* volumen 396 número 8689, Julio 2010.

[7] María José Caro Bejarano, "Alcance y ámbito de la seguridad nacional en el ciberespacio", Febrero 2011.

[8] José Miguel Holguín, Maite Moreno, Borja Merino, "Detección de APTs", Mayo 2013, pp. 195.

[9] World Economic Forum, "Global Risk 2015", décima edición, 2015. Disponible en: http://reports.weforum.org/global-risks-2015/

[10] Ponemon Institute LLC, "2012 Cost of Cyber Crime Study", Octubre 2012.

[11] Luis Joyanes Aguilar, "Introducción. Estado del arte de la ciberseguridad", Febrero 2011.

[12] Organización Internacional para la Estandarización, Comisión Electrotécnica Internacional, "ISO/IEC 27001", Octubre 2015.

[13] www.adminso.es/images/d/dc/PFC_**eugenio**.pdf

[14] Raúl Jusdado, "Implantación de un SGSI en la empresa", Diciembre 2009.

[15] Eugenio Eduardo Villar Fernández, "Virtualización de servidores de telefonía IP en GNU/Linux", PFC, Junio 2010.

Glosario

Backtrack	Distribución GNU/Linux en formato LiveCD pensada y diseñada para la auditoría de seguridad.
BeEF	Herramienta de pentesting de código libre para la explotación de aplicaciones web y de vulnerabilidades en los navegadores web.
CentOS	*Community ENTerprise Operating System* es una bifurcación a nivel binario de la distribución Linux Red Hat Enterprise Linux RHEL, compilado por voluntarios a partir del código fuente publicado por Red Hat
CERT	*Computer Emergency Response Team* es un centro de respuesta a incidentes de seguridad en tecnologías de la información.

CTF	*Capture The Flag* es un tipo de competición dentro del mundo del hacking donde cada equipo tiene una "bandera" en su servidor que debe proteger y conseguir la "bandera" del resto de equipos atacando sus servidores.
CTSS	*Compatible Time-Sharing System* fue uno de los primeros sistemas operativos de tiempo compartido; fue desarrollado en el Centro de Computación del MIT.
Debian	Comunidad conformada por desarrolladores y usuarios, que mantiene un sistema operativo GNU basado en software libre.
DMZ	*Demilitarized Zone* es una zona segura que se ubica entre la red interna de una organización y una red externa, generalmente en Internet.
DNS	*Domain Name System* es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada.
Esteganografía	Del griego *steganos* (cubierto u oculto) y *graphos* (escritura), trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia.
Estegoanálisis	Disciplina dedicada al estudio de la detección de mensajes ocultos usando esteganografía.
eth0	Identificador que se la a las interfaces de red en los sistemas operativos UNIX
Exploit	Fragmento de software, fragmento de datos o secuencia de comandos y/o acciones, utilizado con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.
Fedora	Distribución Linux para propósitos generales basada en RPM, que se caracteriza por ser un sistema estable.
FTP	*File Transfer Protocol* es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor.
Gemalto	Vendedor de tarjetas inteligentes y otros productos de seguridad digital fundada en junio del 2006, mediante la fusión de Axalto y Gemplus International SA.
GNU/Linux	Término empleado para referirse a la combinación del núcleo o *kernel* libre similar a Unix denominado Linux con el sistema GNU.

Hacker ético	Persona experta en ordenadores y redes que realiza un ataque sistemático a una infraestructura de red o de ordenadores con la autorización de sus propietarios con el objetivo de descubrir vulnerabilidades que un hacker malicioso podría explotar.
Hacking ético	Actividad que realiza un hacker ético.
Hipervisor	Plataforma que permite aplicar diversas técnicas de control de virtualización para utilizar, al mismo tiempo, diferentes sistemas operativos en una misma computadora.
IEC	*International Electrotechnical Commission* es una organización de normalización en los campos: eléctrico, electrónico y tecnologías relacionadas.
Ingeniería inversa	Obtener información o un diseño a partir de un producto, con el fin de determinar de qué está hecho, qué lo hace funcionar y cómo fue fabricado.
Ingeniería social	Práctica de obtener información confidencial a través de la manipulación de usuarios legítimos.
IP	*Internet Protocol* es un protocolo de comunicación de datos digitales clasificado funcionalmente en la Capa de Red según el modelo internacional OSI.
ISACA	*Information Systems Audit and Control Association* es una asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades auditoría y control en sistemas de información.
ISO	*International Organization for Standardization* es el organismo encargado de promover el desarrollo de normas internacionales de fabricación (tanto de productos como de servicios), comercio y comunicación para todas las ramas industriales.
Kali Linux	Distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría a partir de la distribución BackTrack.
MD5	*Message-Digest Algorithm 5* es un algoritmo de reducción criptográfico de 128 bits diseñado por el profesor Ronald Rivest del MIT
Metasploit	Proyecto open source de seguridad informática que proporciona información y exploits de vulnerabilidades de seguridad.
Meterpreter	*Metasploit Interpreter* es el intérprete de comandos de Metasploit.

NAT	*Network Address Translation* es un mecanismo utilizado por Routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles.
Nessus	Programa de escaneo de vulnerabilidades en diversos sistemas operativos.
NimbleX	Distribución de Linux basada en Slackware.
Nmap	Programa de código abierto que sirve para efectuar escaneo de puertos escrito originalmente por Gordon Lyon.
Pivoting	Método usado por los hackers éticos que utiliza un sistema comprometido para acceder a otro sistema en la misma red evitando el cortafuegos.
Proxy	Servidor que sirve de intermediario en las peticiones de recursos que realiza un cliente a un servidor.
RAM	*Random Access Memory* es la memoria principal de la computadora, donde residen programas y datos, sobre la que se pueden efectuar operaciones de lectura y escritura.
RHEL Linux	*Red Hat Enterprise Linux* es una distribución comercial de Linux basada en Fedora desarrollada por Red Hat.
Root	Nombre convencional de la cuenta de usuario que posee todos los derechos en todos los modos (mono o multi usuario) en sistemas operativos UNIX.
SHA-1	*Secure Hash Algorithm -1* es un algoritmo de la familia de funciones hash.
Slackware	Distribución Linux más antigua que tiene vigencia.
Stuxnet	Primer gusano conocido que espía y reprograma sistemas industriales, en concreto sistemas SCADA de control y monitorización de procesos, pudiendo afectar a infraestructuras críticas como centrales nucleares.
TCP	*Transmission Control Protocol* (Protocolo de Control de la Transmisión), protocolo de transporte que garantiza que los datos serán entregados
TomCat	Contenedor web de servlets desarrollado bajo el proyecto Jakarta en la Apache Software Foundation.
Tor	*The Onion Router* es un proyecto cuyo objetivo principal es el desarrollo de una red de comunicaciones distribuida de baja latencia y superpuesta sobre internet, en la que el encaminamiento de los

	paquetes intercambiados entre los usuarios no revela su identidad su dirección IP.
Ubuntu	Sistema operativo basado en GNU/Linux y que se distribuye como software libre
VLAN	*Virtual Local Area Network* es un método para crear redes lógicas independientes dentro de una misma red física.

Anexos

A Prácticas del laboratorio de ciberseguridad

LABORATORIO DE CIBERSEGURIDAD

PRÁCTICA 1: PROTECCIÓN CONTRA MALWARE E INGENIERÍA SOCIAL

Objetivos:

- Conocer algunas de las herramientas más populares y conceptos básicos de un ataque hacking en cada una de las fases que establece la certificación CEH (Certified Ethical Hacker) y la metodología OSSTMM (Open Source Security Testing Methodology Manual). El ataque de esta práctica estará basado en técnicas de ingeniería social con contenido malicioso.
- Conocer el estándar ISO-IEC 27001 v2013, especialmente los controles que el estándar ISO-IEC 27002 proporciona como las mejores prácticas de seguridad en la gestión de la seguridad de la información.
- El alumno deberá determinar, relacionar e implantar, si fuese posible, los controles propuestos por la ISO-IEC 27002 en el entorno empresarial virtualizado entregado que aplican en el escenario propuesto.

Instrucciones generales preliminares:

En el paquete *EntornoEmpresarialVirtualizado.rar* entregado al alumno encontrará todas las máquinas virtuales necesarias para el buen desarrollo de la práctica. El paquete incluye las siguientes máquinas virtuales:

- Firewall
- Servidor Web
- Servidor DNS
- Servidor FTP
- Windows 7
- Windows XP
- Kali Linux

Para preparar el entorno virtual realizar los siguientes pasos:

1) Abrir Oracle VirtualBox
2) Descomprimir el paquete *EntornoEmpresarialVirtualizado.rar*
3) Lanzar todas las máquinas virtuales haciendo doble-click en el archivo *NombreMáquina.vbox*

Comprobar las interfaces y las IPs que tiene la máquina atacante Kali Linux
1) Mirar las interfaces de red levantadas (eth0, eth1...ethN, lo) y toda la información relativa a ellas:

- root@kali-tfg:~# ifconfig

El resultado debería ser el siguiente:

La interfaz eth0 será la interfaz de tipo NAT de VirtualBox para tener acceso a internet en el caso de que necesitemos buscar información.
La interfaz eth1 será una interfaz de tipo Red Interna de VirtualBox con nombre <Internet> y que simulará Internet y en la que tendremos asignada una IP "pública".
La interfaz eth2 será una interfaz Red Externa con nombre <Starbucks> y que simulará una red local pública y en la que tendremos asignada una IP local.

Creación de una base de datos en postgresql para metasploit

Iniciar postgresql y crear una nueva base de datos para metasploit para poder almacenar todos los datos y poder guardar todos los exploits en caché para entre otras cosas, agilizar las búsquedas de exploits.

i. Cambiar al usuario postgres
```
root@kali:~# su postgres
```
ii. Crear un usuario msf4_user y poner una contraseña
```
postgres@kali:$ createuser msf4_user -P
Enter password for new role: password
Enter it again: password
Shall the new role be a superuser? (y/n) n
Shall the new role be allowed to create database? (y/n) n
Shall the new role be allowed to create more new roles? (y/n) n
```
iii. Crear una base de datos cuyo propietario sea el usuario msf4_user
```
postgres@kali:$ createdb –owner=msf4_user msf4_database
```
Configurar postgresql para que se ejecute en el inicio de la máquina
```
root@kali:~# update-rc.d postgresql enable
```
iv. Iniciar metasploit y comprobar si está conectado a alguna base de datos
```
root@kali:~# msfconsole
msf > db_status
```
v. Conectar con la base de datos creada anteriormente
```
msf > db_connect msf4_user:password@127.0.0.1:5432/msf4_database
```
vi. Reconstruir la caché de la base de datos de metasploit
```
msf > db_rebuild_cache
```

vii. En otra terminal crear un archivo .yml nuevo a partir del archivo database.yml.example con el siguiente comando:

```
root@kali:$ cp
opt/metasploit/apps/pro/ui/config/database.yml.example
/opt/metasploit/apps/pro/ui/config/database.yml
```

Configurar el archivo database.yml con los datos con los que hemos creado la base de datos de metasploit en postgresql. Tanto development como production tienen que tener los mismos datos. (Nota: hay que borrar &default para que funcione)

PARTE 1: ATAQUE

HISTORIA

A. FASE DE RECONOCIMIENTO

Un amigo que trabaja en una start-up te comenta que sus socios le han engañado y le han echado de la empresa, han cambiado las contraseñas de sus cuentas y se han quedado con todo su trabajo. Ante esta injusticia, decides ponerte tu sombrero negro y con tus conocimientos técnicos investigar un poco gracias a hacking con buscadores. Con la información que te da tu amigo de los posibles nombres que habían pensado para la futura empresa no encuentras mucha información ya que el proyecto acaba de empezar. Encuentras una entrada en un blog de start-ups y proyectos emprendedores, aunque no dice mucho de la empresa, sí dice lo suficiente como para conseguir los nombres de las principales personas que trabajan en ella y la localización de sus oficinas temporales. Es lo que tienen las start-ups; necesitan darse a conocer, necesitan dar demasiada información y si no se tiene control se puede llegar a dar demasiada información interna, privada y sensible.

Decides buscar en las redes sociales a estas personas para ver qué tipo de información puedes sacar de ellas. Las siguientes páginas son un buen comienzo:
Redes Sociales:
https://www.facebook.com/
https://es.linkedin.com/
https://twitter.com/

Registros:
https://whois.net/

Buscadores de personas:
https://pipl.com
https://www.123people.com
www.peekyou.com
www.webmii.com
La investigación te lleva a averiguar que el director gerente de la empresa le encanta salir de fiesta y le encanta colgar fotos, algunas un poco bochornosas, por lo que dices aprovechar su poca discreción para preparar el ataque. Al tener su Facebook abierto para cualquier persona y varios de sus amigos también, eso te permite crear unos buenos

vectores de ataque de ingeniería social sobre todo cuando ya tienes un punto de contacto; el email empresarial.

B. FASE PREPARACIÓN DEL ATAQUE DE INGENIERÍA SOCIAL

Para realizar el ataque de ingeniería social te creas una página web sencillita. Lo ideal sería montarla en un servidor con el que no se te pudiese relacionar ni personalmente ni geográficamente...alguno obtenido en antiguas aventuras. Como no crees que tengan mucho conocimiento técnico las personas de esta empresa decides que no es necesario de momento hacer el ataque por medio de uno de tus servidores. A lo mejor luego cambias de idea.

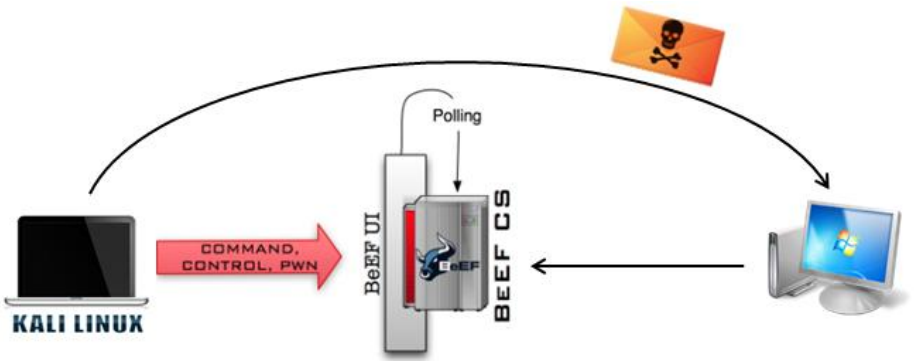
La página web simplemente contendrá una supuesta imagen del director gerente. Si tienes tiempo intentarás copiar alguna de alguna red social y hacerla más realista, pero el tiempo apremia.

C. FASE DE EXPLOTACIÓN

Después de tener preparados todos los anzuelos decides realizar el ataque de ingeniería social.
Preparas un correo que irá dirigido al correo empresarial del director que aparece en la página web en el apartado de contactos, en el que irá incluido un enlace a la página web que hemos creado y si tienes tiempo un archivo comprimido malicioso como adjunto.

Arrancas los frameworks BeEF y Metasploit dejando este último con un exploit cargado a la espera de que la víctima se conecte.

Cuando la persona que reciba el email, pinche en la url maliciosa se conectará a tu página web y realizarás un ataque con el framework de BeEF redirigiendo la página a otra que vulnere su navegador que servirá para conectarse con tu metasploit y así tener el control de la máquina de la víctima.



A partir de este momento, inicias una sesión de meterpreter y consigues las credenciales del director de su cuenta de administrador, que posiblemente al ser descuidado las utilice en cuentas de otros equipos de la empresa. Del escritorio de la máquina vulnerada obtienes información sensible que hará las delicias de tu amigo, al final es verdad que a su antiguo jefe le gustan las fotos comprometedoras.

GUIÓN

A. FASE DE RECONOCIMIENTO

1) Tras haber realizado una investigación con los buscadores web (google hacking, bing hacking...) y las redes sociales de nuestro objetivo obtienes:

Email empresarial:
Aficiones del director: la fiesta, viajes a Costa Rica, Venezuela.. y congresos de Start-ups
Imágenes del director: *directorparty.jpg, Costarica.jpg*
Nombres de amigos y empresas en las que trabajan:

B. FASE PREPARACIÓN DEL ATAQUE DE INGENIERÍA SOCIAL

2.1) Montar una página web sencilla con una imagen o una red social donde se pueda colgar una imagen (cuanto más detallista y creíble sea la página web, más probabilidades de éxito tendrá el ataque de ingeniería social).

i. La creación de la web se puede hacer desde cero, tomar como ejemplo otras webs o copiarlas enteras utilizando la herramienta SET (Social Engineering Toolkit) ó con la herramienta BeEF (que utilizaremos más adelante) y que vienen en la distribución Kali Linux
ii. En la página web habrá que insertar el código HTML que redirija la víctima a la página web de enganche con el que se tomará el control de su navegador web. Por lo que el código deberá contener lo siguiente:
   - <title>directorio_imagen</title>
   - <script src="http://nuestra_IP:3000/hook.js"></script>
     (al iniciar BeEF en Kali, en el terminal de comandos, aparece donde se encuentra el archivo hook.js en caso de que no sea la estructura anterior)
   -

(OPCIONAL) Realizar todo nuestro ataque con un servidor de por medio para dificultar que se relacione directamente nuestra IP y terminal con el ataque. Para ello habría que crear una máquina virtual con un servidor de preferencia del alumno donde se alojará nuestra página web para realizar el ataque de ingeniería social y desde donde se instalará el troyano.

i. A este servidor se accederá remotamente través de ssh
ii. Realizar el punto 2.1) en nuestro servidor en vez de en nuestra máquina

2.2) Preparar el email que se le va a enviar a la víctima. Se va a utilizar la página https://emkei.cz ya que permite falsificar todos los parámetros que se requieren en un email. Para que parezca totalmente real, se utilizarán los datos que se obtuvieron en la fase de reconocimiento; nombres de amigos en Facebook, empresas en las que trabajan de Linkedin...
Dentro del cuerpo del correo se añadirá la URL de la página maliciosa que se ha creado

(Nota: No se puede enviar un correo falso (que no existe o existente) a un buzón del mismo servidor de correo. Gmail, Hotmail, etc. comprueban sus propios remitentes, por lo que se puede inventar uno que visualmente sea parecido como gmai1, que sea corporativo obtenido de una persona conocida de la víctima en la fase de reconocimiento...)

C. FASE DE EXPLOTACIÓN

3.1) Iniciar la herramienta BeEF en Kali y realizar lo siguiente:

i. Acceder vía web al panel de administración con la cuenta usuario=beef y contraseña=beef

ii. Crear el mismo directorio en nuestro servidor ó Kali en /var/www/nombre_directorio_imagen (el nombre_directorio_imagen es el que se ha puesto en title, esto se hará así para confundir a la víctima, y que al ver la URL piense que es solamente una imagen)

3.2) Mandar el email e iniciar Metasploit, cargar el módulo auxiliary/server/browser_autopwn e introducir los parámetros necesarios y dejarlo correr hasta que cargue todos los exploits y podamos coger la URL del exploit que se vaya a utilizar.
Para cargar, ejecutar módulos o exploits en metasploit, introducir parámetros, etc. acudir a la "chuleta" de comandos de metasploit que se encuentra en la parte de documentación.

3.3) En este apartado el alumno asumirá el rol de víctima. Por lo que tendrá que iniciar sesión como director en la máquina virtual de Windows 7, abrir el gestor de correo gmail con la cuenta corporativa vía web y pinchar en la URL del email malicioso. Este enlace le llevará a la página web que se ha creado previamente con la imagen a elección del alumno o la obtenida en la fase de reconocimiento. Una vez hecho ésto su navegador web ya estará enganchado a BeEF.

3.4) Acceder al framework BeEF a través del navegador web en Kali en la dirección *localhost:3000*, introducir las credenciales y seleccionar la IP de la víctima que aparecerá en Online Browsers. Posteriormente en 'Commnds' en el apartado de browser se pasará a realizar un ataque de redireccionamiento del navegador dentro de Hooked Domain. En el cuadro de Redirect URL se pondrá la URL que en metasploit nos ha entregado.

Una vez hecho todo esto, se conseguirá una sesión de meterpreter en el ordenador de la víctima.

3.5) Con el control total de la víctima, a través de meterpreter se podrá realizar cualquier acción, desde cargar un archivo malicioso, descargar archivos, crear un backdoor, una elevación de privilegios, desinstalar el antivirus...
En caso de necesitarse, se puede mirar la "chuleta" de comandos de meterpreter que se encuentra en la parte de documentación.
Acciones a realizar en la víctima desde la sesión de meterpreter:

- Descargarse la carpeta 'Fotitos' de la cuenta del director
- Limpiar los registros de los eventos para borrar las huellas

PARTE 2: CONTROLES

GUIÓN

A. ANÁLISIS DEL ATAQUE

1.1) Analizar cuáles han sido los elementos técnicos y humanos que han producido que el ataque haya tenido éxito.

1.2) Analizar qué impacto podría tener este tipo de ataques en una empresa real y como podría repercutir en su economía.

1.3) Analizar qué medidas implementarías si fueses el administrador de sistemas de la empresa

B. IDENTIFICACIÓN DE LOS CONTROLES

2.1) Abrir el documento *Controles-ISO-IEC-27002:2013.pdf* e identificar en el índice qué control ó controles aplicarían a este escenario. Indicar los controles.

2.2) Especificar cuáles son los apartados en la guía de implementación del documento *Controles-ISO-IEC-27002:2013.pdf* que habría que aplicar para prevenir este tipo de ataques de cada control identificado en el apartado anterior.

C. IMPLEMENTACIÓN DE LOS CONTROLES

3.1) Implementar, teóricamente o técnicamente si es posible, al menos dos apartados de los especificados en el apartado anterior.

MEMORIA

El alumno deberá documentar todo el proceso del ataque a través de capturas de pantalla de lo únicamente pedido e incluyendo las explicaciones necesarias para su comprensión por parte del profesor en la corrección.
Para no extender la memoria hasta límites insospechados, incluir los comandos que tengan una cierta cohesión en una misma captura. (p. ej. ifconfig, cat /etc/network interfaces; set lhost, set rhost, set...)
En la segunda parte se deberá contestar a todas las preguntas realizadas y documentar las implementaciones de los controles tanto prácticas como teóricas.

LABORATORIO DE CIBERSEGURIDAD

PRÁCTICA 2: ACTUALIZACIÓN DE SOFTWARE Y USO DE EQUIPOS DE TRABAJO FUERA DE LA INFRAESTRUCTURA LABORAL

Objetivos:

- Conocer algunas de las herramientas más populares y conceptos básicos de un ataque hacking en cada una de las fases que establece la certificación CEH (Certified Ethical Hacker) y la metodología OSSTMM (Open Source Security Testing Methodology Manual). El ataque de esta práctica estará basado en técnicas escaneo en redes públicas y uso de vulnerabilidades en equipos desactualizados.
- Conocer el estándar ISO-IEC 27001 v2013, especialmente los controles que el estándar ISO-IEC 27002 proporciona como las mejores prácticas de seguridad en la gestión de la seguridad de la información.
- El alumno deberá determinar, relacionar e implantar, si fuese posible, los controles propuestos por la ISO-IEC 27002 en el entorno empresarial virtualizado entregado que aplican en el escenario propuesto.

Instrucciones generales preliminares:

En el paquete *EntornoEmpresarialVirtualizado.rar* entregado al alumno encontrará todas las máquinas virtuales necesarias para el buen desarrollo de la práctica. El paquete incluye las siguientes máquinas virtuales:

- Firewall
- Servidor Web
- Servidor DNS
- Servidor FTP
- Windows XP
- Windows 7
- Kali Linux

Para preparar el entorno virtual realizar los siguientes pasos:

1) Abrir Oracle VirtualBox
2) Descomprimir el paquete *EntornoEmpresarialVirtualizado.rar*
3) Lanzar todas las máquinas virtuales al hacer doble-click en el archivo *NombreMáquina.vbox*

Instrucciones generales específicas:

Para esta práctica el alumno necesitará comprobar las IPs de algunas máquinas virtuales para simular una red pública externa de la empresa. La red de Starbucks.
La máquina virtual Windows XP deberá tener una IP 172.16.10.100 en red local 3
La máquina virtual Kali Linux deberá tener una IP 172.16.10.2 en la interfaz eth2

Para comprobar las direcciones IP en Windows es necesario abrir un terminal de comandos:

1) Presionar las teclas: Win+R, escribir cmd y darle a enter
2) Escribir en el terminal de comandos: ipconfig /all
3) Comprobar que el 'Adaptador Ethernet Conexión de área local 3' contiene la IP 172.16.10.100 en IPv4

En caso de no estar la IP descrita habrá que configurarlo.
Para poner una IP estática en Windows 7 hay que seguir los siguientes pasos:
1) Ir a Inicio > Panel de Control > Redes e Internet > Centro de Redes y Recursos Compartidos
2) En el panel de la izquierda pinchar con el botón izquierdo en 'Cambiar configuración del adaptador'
3) Pinchar con el botón derecho en 'Conexión de área local' y en 'Propiedades'
4) Seleccionar 'Protocolo de Internet versión 4 (TCP/IPv4)' y pinchar en propiedades
5) Seleccionar 'Usar la siguiente dirección IP' e introducir los siguientes valores:
   - Dirección IP: 172.16.10.100
   - Máscara de subred: 255.255.255.0
   - Puerta de enlace predeterminada: 176.16.10.1

PARTE 1: ATAQUE

HISTORIA

A. FASE DE RECONOCIMIENTO

Tras haber accedido a la máquina del jefe y haber obtenido información sensible, en realidad te das cuenta de que no has conseguido lo que tu amigo quería de verdad, es decir, a todo su trabajo que tanto le había costado desarrollar y que su empresa se había negado a darle siguiendo utilizándolo ellos. Por lo que decides realizar un poco de google hacking de otros trabajadores de la empresa de los tres nombres e emails que te pasó tu amigo. El segundo de la lista puede ser interesante, es un chico y en su foto de perfil de Facebook aparece con un ordenador antiguo (un poco estilo vintage) tomando un café en un starbucks. Puede ser interesante averiguar donde vive y ver si hay algún starbucks cerca al que suela ir habitualmente.
A través de Instagram descubres que nuestro objetivo normalmente sube las fotos los lunes y los miércoles a la misma hora por la tarde y todas suelen ser en un starbucks. En

uno de sus múltiples selfies identificas otro establecimiento a través de la ventana del starbucks por lo que rápidamente con una búsqueda en Google Maps averiguas las coordenadas exactas.
Perfecto, mañana es miércoles, allí estarás.

B. FASE DE ESCANEO Y ENUMERACIÓN

Una vez estando en el establecimiento esperas a que llegue la víctima que al poco tiempo llega, se pide un café, se sienta, abre su portátil de por lo menos hace 10 años y empieza a navegar por la red. Rápidamente echando un vistazo a su pantalla te das cuenta del SO qué es y de lo fácil que va a ser esto.
Con tu portátil ya abierto y con un café al lado para pasar desapercibido, abres Nmap y empiezas a escanear esa red. Te das cuenta de que el café de nuestro objetivo está casi acabado por lo que decides tomar la decisión de arriesgarte y realizar un escaneo más agresivo y no tan sigiloso como te gustaría. Porque si pierdes esta oportunidad, mínimo hasta el lunes siguiente no podrías hacer nada, no hay tiempo que perder. Descubres la IP local de la víctima, los servicios que está corriendo su máquina y en qué puertos... Es tan vintage que no tiene siquiera activado el firewall ya que ni un puerto de su máquina está filtrado. Esto cada vez se pone mejor. Pasemos a metasploit.

C. FASE DE EXPLOTACIÓN

Abres tu gran aliado metasploit y cargas uno de los mejores y más eficaces exploits para este escenario. Configuras todos los parámetros del exploit con los datos obtenidos del escaneo de nmap y lo lanzas. ¡BINGO! Entras hasta la cocina. Una sesión de meterpreter con la que puedes hacer todo lo que desees.

GUIÓN

A. FASE DE RECONOCIMIENTO

1) Tras haber realizado una investigación con los buscadores web (google hacking, bing hacking...), las redes sociales de nuestro objetivo y el reconocimiento físico, obtienes:

- Coordenadas del Starbucks de la víctima.
- La distribución que tiene el portátil de nuestra víctima: Windows.

B. FASE DE ESCANEO Y ENUMERACIÓN

2) Conectarse a la misma red pública que la víctima y realizar un escaneo para determinar la IP local que tiene nuestra víctima. Realizar un escaneo con nmap, al tratarse de una red pública de un establecimiento comercial pequeño no tiene por qué ser muy sigiloso (siempre es recomendable mantener un nivel de sigilo y anonimato, pero al no saber cuando la víctima se puede marchar del establecimiento, es necesario agilizar el escaneo aunque con ello se genere más ruido en la red).

Para escoger las mejores opciones para realizar el escaneo es recomendable mirar la "chuleta" de las opciones de nmap que viene en la parte de documentación.

2.1) Determinar qué sistema operativo tiene la víctima y que servicios corre el sistema. Buscar vulnerabilidades de ese SO en la web.

C. FASE DE EXPLOTACIÓN

3) Abrir metasploit:

i. Buscar el exploit por su nombre en metasploit
ii. Cargar el exploit
iii. Configurar los parámetros:
    - RHOST (IP remote host)
    - RPORT(port remote host)
    - LHOST (IP local host)

    En algunos parámetros los valores introducidos no tienen por qué ser los que se necesiten para el ataque que se esté realizando por lo que no habrá que dejar nada preconfigurado sin comprobarlo. Si deseamos obtener información sobre los parámetros que se necesitan rellenar se puede utilizar el comando 'show options' ó para un informe más detallado el comando 'info'.
    Para configurar un valor se realiza de la siguiente manera:
    msf exploit(nombre_del_exploit) > set parámetro valor
iv. Lanzar el exploit
v. Con la sesión de meterpreter abierta:
    - Realizar una elevación de privilegios
    - Listar los procesos de la víctima
    - Migrar a otro proceso más permanente
    - Hacer un captura de su pantalla (abrir imágenes de la terminal de kali: gnome-open)
    - Limpiar los registros de la máquina vulnerada
    - Cargar mimikatz
    - Obtener las contraseñas en texto claro de los usuarios que se hayan autenticado desde el último inicio
    - Obtener los hashes de todas las contraseñas de los usuarios del sistema se hayan autenticado o no y guardarlos en un fichero local para posteriormente realizar un ataque de fuerza bruta o diccionario a las que no se hayan obtenido en texto claro
    - Registrar todas las pulsaciones de teclado de la actividad del proceso explorer.exe
    - Registrar todas las pulsaciones de teclado de la actividad en el proceso explorer.exe y de los inicios de sesión y guardarlo en ficheros diferentes
    - Dejar dos puertas traseras desde meterpreter:
        a. Un usuario nuevo desde el módulo incógnito
        b. Cargar el exploit 'persistence' de windows catalogado como excelente y configurar los siguientes parámetros y posteriormente correr el exploit:
            - Payload: reverse_tcp
            - STARTUP: SYSTEM

- SESSION: id de la sesión de meterpreter que se tenga corriendo en la víctima
- LHOST
- LRPORT: 5554

Cargar el exploit 'multi/handler', configurar los parámetros y correr el exploit en background (run -j, para ver las tareas que estamos realizando en background el comando es 'jobs -j'):

- LHOST
- LPORT: 5554

PARTE 2: CONTROLES

GUIÓN

A. ANÁLISIS DEL ATAQUE

1.1) Analizar cuáles han sido los elementos técnicos y humanos que han producido que el ataque haya tenido éxito.

1.2) Analizar qué impacto podría tener este tipo de ataques en una empresa real y como podría repercutir en su economía.

1.3) Analizar qué medidas implementarías si fueses el administrador de sistemas de la empresa.

B. IDENTIFICACIÓN DE LOS CONTROLES

2.1) Abrir el documento *Controles-ISO-IEC-27002:2013.pdf* e identificar en el índice qué control ó controles aplicarían a este escenario. Indicar los controles.

2.2) Especificar cuáles son los apartados en la guía de implementación del documento *Controles-ISO-IEC-27002:2013.pdf* que habría que aplicar para prevenir este tipo de ataques de cada control identificado en el apartado anterior.

C. IMPLEMENTACIÓN DE LOS CONTROLES

3.1) Implementar teóricamente el control 6.2.2.

MEMORIA

El alumno deberá documentar todo el proceso del ataque a través de capturas de pantalla de lo únicamente pedido e incluyendo las explicaciones necesarias para su comprensión por parte del profesor en la corrección.
Para no extender la memoria, incluir los comandos que tengan una cierta cohesión en una misma captura. (p. ej. ifconfig, cat /etc/network interfaces; set lhost, set rhost, set...)
En la segunda parte se deberá contestar a todas las preguntas realizadas y documentar las implementaciones de los controles tanto prácticas como teóricas.

LABORATORIO DE CIBERSEGURIDAD

PRÁCTICA 3: SEGREGACIÓN DE REDES Y CONFIGURACIÓN DE CUENTAS

Objetivos:

- Conocer algunas de las herramientas más populares y conceptos básicos de un ataque hacking en cada una de las fases que establece la certificación CEH (Certified Ethical Hacker) y la metodología OSSTMM (Open Source Security Testing Methodology Manual). El ejercicio de esta práctica estará basado en ataques a aplicaciones web y en lo que puede desencadenar si el servidor que aloja esas aplicaciones a internet en vez de estar en una DMZ (Zona Desmilitarizada) está en la red interna de la empresa.
- Conocer el estándar ISO-IEC 27001 v2013, especialmente los controles que el estándar ISO-IEC 27002 proporciona como las mejores prácticas de seguridad en la gestión de la seguridad de la información.
- El alumno deberá determinar, relacionar e implantar, si fuese posible, los controles propuestos por la ISO-IEC 27002 en el entorno empresarial virtualizado entregado que aplican en el escenario propuesto.

Instrucciones generales preliminares:

En el paquete *EntornoEmpresarialVirtualizado.rar* entregado al alumno encontrará todas las máquinas virtuales necesarias para el buen desarrollo de la práctica. El paquete incluye las siguientes máquinas virtuales:

- Firewall
- Servidor Web
- Servidor DNS
- Servidor FTP
- Windows XP
- Windows 7
- Kali Linux

Para preparar el entorno virtual realizar los siguientes pasos:

1) Abrir Oracle VirtualBox
2) Descomprimir el paquete *EntornoEmpresarialVirtualizado.rar*
3) Lanzar todas las máquinas virtuales al hacer doble-click en el archivo *NombreMáquina.vbox*

Instrucciones generales específicas:

Para esta práctica el alumno necesitará comprobar el funcionamiento de la red EPS y la de simInternet.
La máquina virtual Kali Linux deberá tener una IP 172.16.1.2 en la interfaz eth1.

Comprobar las interfaces y las IPs que tiene la máquina atacante Kali Linux

1) Mirar las interfaces de red levantadas (eth0, eth1...ethN, lo) y toda la información relativa a ellas:

- root@kali-tfg:~# ifconfig

El resultado debería ser el siguiente:

PARTE 1: ATAQUE

HISTORIA

A. FASE DE RECONOCIMIENTO

Tras el último ataque, aunque fue más productivo que el anterior, todavía no conseguiste lo que andabas buscando así que no te queda más opción que buscar otra alternativa; no parece que los altos cargos de esa empresa sean los que hacen el código de la aplicación. Habrá que realizar un ataque más directo, pero aún no sabes cómo. Abres tu navegador y aunque no esperas encontrar nada nuevo, un nuevo hallazgo te da una sensación de alegría enorme; han creado su página web. La página web es bastante sencilla por lo que en principio no hay mucho que explotar. Pero de cualquier manera el servidor web puede ser una posibilidad para entrar en su red laboral privada. Perfecto.

B. FASE DE ESCANEO Y ENUMERACIÓN

Decides lanzar un escaneo con Nmap a la dirección IP de la página, es posible que el servidor que la aloja tenga algún servicio corriendo que tenga alguna versión vulnerable.

Como este escaneo no tiene límite de tiempo decides hacerlo lo más sigiloso posible no vaya a ser que tengan un IDS (Intrusion Detection System) entre otras cosas y tengamos un problema. Esperemos que la política de empresa sea como la de nuestro último trabajador; sin firewall, o al menos que no lo hayan configurado bien y nos deje pasar todo...

Cuando obtenemos los resultados del escaneo, un servicio concreto nos llama la atención por la versión que corre, parece un poco vieja... Recuerdas que esa versión

sufrió una vulnerabilidad hace unos años en los servidores web con apache que utilizaban esa aplicación. En vez de buscar la vulnerabilidad directamente en internet, decides que a lo mejor tienes más suerte y el servidor puede tener alguna vulnerabilidad más por lo que realizas un escaneo con Nessus. Vaya, esto se pone interesante.

C. FASE DE EXPLOTACIÓN

Abres metasploit, buscas por el identificador CVE (Common Vulnerabilities and Exposures) la vulnerabilidad que te han devuelto Nessus y Google que tiene ese servicio que te había llamado la atención. Metasploit muy obedientemente te da unos cuantos resultados.

Primero abres el exploit clásico 'deploy' y empiezas a introducir los parámetros necesarios para lanzar el exploit. Hay dos parámetros que te faltan el usuario y la contraseña, por lo que buscas en metasploit por el nombre del servicio por si hay algún escáner que pueda ayudarte a encontrar esos parámetros.
La base de datos de metasploit de devuelve varios y utilizas un escáner del módulo auxiliar, que hace referencia al exploit que estás utilizando.
Cargas el escáner y lo lanzas rellenando los parámetros previamente. A los pocos segundos el escaneo te devuelve un username y un password, justo lo que necesitabas.

Terminas de introducir todos los parámetros necesarios en el exploit y lo lanzas. Lanzas un Shell para inspeccionar el servidor tranquilamente y ver que usuario eres. Este servicio no corría con un usuario con privilegios root, por lo que tendrás que realizar una elevación de privilegios. Se te ocurre que tal vez hayan configurado mal las carpetas y haya algunas con información sensible que tenga permisos de lectura para todos.
Te diriges directamente hacia la carpeta de las llaves autorizadas de ssh porque sabes que había una vulnerabilidad en OpenSSL hace unos años que descifraba las llaves cifradas ssh. A lo mejor quien ha instalado este servidor, viendo su fallo anterior, ha podido dejar este también.

Efectivamente ahí están las llaves para todo aquel que quiera verlas sin necesidad de privilegios, vas directo a un terminal nuevo de Kali y buscas con searchsploit 'openssl' para que te refresque como era aquella vulnerabilidad. Lees el archivo de texto con las instrucciones y realizas el ataque. Tras un rato tienes la llave descifrada.

A partir de aquí es coser y cantar, te conectas por ssh con la llave descifrada al servidor con el usuario root. Una vez obtenido el usuario root, vamos a intentar conseguir las contraseñas de todos los usuarios del sistema. Como Linux guarda sus contraseñas en hashes vamos a tener que recurrir a realizar un ataque de diccionario, ya que de fuerza bruta puede llevarte horas, meses, años o incluso morir antes de conseguir descifrarlo, y más aún teniendo en cuenta la capacidad de tu ordenador que es bastante normalita.

En realidad que estén en hashes no te preocupa mucho ya que tienes el gran diccionario de 122 millones de hashes con sus contraseñas en claro que un cracker obtuvo después de dedicarle cinco meses intensivos a un torrent que contenía 145 millones de contraseñas que se filtró por twitter. Descifrar estos hashes con ese diccionario te lleva segundos. Una vez obtenidos las contraseñas en claro tiene pinta de que vas a poder acceder a cualquier máquina de esa red. Por lo que echas un vistazo a ver que hay.

Escaneas la red interna con Nmap y descubres un servidor de archivos, seguramente este ahí lo que verdaderamente busca tu amigo. Acceder vía web al servidor FTP con las cuentas que acabas de obtener es pan comido.

GUIÓN

A. FASE DE RECONOCIMIENTO

1) Tras haber realizado una investigación con los buscadores web (google hacking, bing hacking...) y las redes sociales de nuestro objetivo obtienes:

Página web de la empresa en la IP: 172.16.1.10

B. FASE DE ESCANEO Y ENUMERACIÓN

2) Realizar un escaneo sigiloso con nmap sin demorarse muchísimo, para ello se presentarán las siguientes condiciones:

i. Realizar la mitad de la conexión TCP three-way-handshake, es decir, realizar el escaneo sólo con el primer handshake para evitar que quede registrado en el servidor que se ha abierto/establecido una conexión TCP. Si sospechamos que hay un firewall se podría realizar un escaneo Christmas
ii. Detectar servicios remotos
iii. Detectar sistema operativo
iv. Realizar el escaneo con paquetes fragmentados para dividir la cabecera de TCP para dificultar la detección por un filtro de paquetes, un IDS...
v. Guardar los resultados del escaneo en un archivo .xml para poder cargarlo en la base de datos de metasploit en un futuro

2.2) (OPCIONAL) Utilizar la herramienta Nessus.

i. Descargar e instalar la última versión desde la página oficial
ii. Reiniciar el servicio nessusd
iii. Acceder a https://localhost:8834/
iv. Registrarse en página web para uso personal
v. Realizar un escaneo desde su interfaz web
vi. Observar los resultados vía web
vii. Iniciar Metasploit
viii. Conectar la base de datos al servidor Nessus con tus credenciales
ix. Realizar un nuevo escaneo con Nessus
x. Observar los resultados vía terminal

C. FASE DE EXPLOTACIÓN

3) Encontrar la vulnerabilidad CVE de Tomcat de Apache.

3.1) Arrancar metasploit y buscar por el código CVE cargar el exploit y configurar todos sus parámetros. Explotar el sistema.

i. Buscar el exploit en metasploit por el código CVE.Se utiliza el comando 'search'
ii. Cargar el exploit que esté catalogado como excelente y tenga una descrIPción: "Apache Tomcat Manager Application Deployer Authenticated Code Execution" Los exploits se cargan usando el comando 'use'
iii. Configurar los parámetros:
    - PASSWORD
    - RHOST (IP remote host)
    - RPORT(port remote host)
    - LHOST (IP local host)
    - USERNAME
    - TARGET

    En algunos parámetros los valores introducidos no tienen por qué ser los que se necesiten para el ataque que se esté realizando por lo que no habrá que dejar nada preconfigurado sin comprobarlo. Si deseamos obtener información sobre los parámetros que se necesitan rellenar se se puede utilizar el comando 'show options' ó para un informe más detallado el comando 'info'.
    Para configurar un valor se realiza de la siguiente manera:
    `msf exploit(nombre_del_exploit) > set parámetro valor`
iv. Si faltase información para rellenar algunos parámetros (PASSWORD y USERNAME) se tendrán que usar otros módulos de metasploit como por ejemplo los scanners del módulo auxiliary. Para ello habrá que buscar por tomcat en metasploit y seleccionar el scanner del módulo auxiliar que tiene como descripción: " Tomcat Application Manager Login Utility"
v. Por último faltaría elegir que payload cargaríamos dentro del exploit. Para saber que payloads hay disponibles utilizamos el comando 'show payloads'.
    Habrá que elegir el más adecuado teniendo en cuenta que queremos una sesión de meterpreter y el protocolo necesario. Las conexiones de tipo 'reverse' lo que realizan es que la conexión se establece de la víctima al atacante. Por lo que siempre será preferible ya que las conexiones de origen interno hacia afuera siempre suelen estar menos protegidas por los firewalls y antivirus que las conexiones de origen externo hacia dentro.

3.1) Una vez lanzado el exploit, se tendría el control del usuario del servicio. Por lo que habrá que conseguir tener acceso a root para hacer 'pivoting' y acceder a otros sistemas de la red debido a que no hay segregación de redes. Para poder realizar una elevación de privilegios y poder tener el control total de la máquina o bien tenemos las contraseñas, las llaves públicas o accedemos explotando algún servicio. En este caso existe un ataque que permite realizar un ataque de fuerza bruta a la llave pública debido a una contraseña débil. Debido a una mala configuración de las cuentas y de los privilegios de las carpetas, a través de un usuario no privilegiado se puede acceder a la llave ssh cifrada del usuario root.

i. Lanzar una Shell del sistema desde meterpreter
ii. Averiguar que usuario eres en el sistema
iii. Encontrar la llave de autorización del usuario root para acceder por ssh en el servidor
iv. Hacer uso de la aplicación searchsploit en una terminal nueva para buscar en Kali un exploit de OpenSSL. Buscar entre los resultados entregados uno que sea para realizar un ataque de fuerza bruta RNGA. Seguir las instrucciones del archivo .txt

v. Buscar con un comando de Linux en el directorio ../rsa/2048/ una clave que coincida la que hemos obtenido
vi. Acceder al mismo servidor a través de ssh con el usuario root y la contraseña obtenida

3.2) Una vez obtenido el acceso al servidor web como root intentar obtener los credenciales de la cuenta por si sirven para otros servidores de la misma red. Las contraseñas en los sistemas Unix se encuentran por defecto en hashes. Por lo que si se quiere obtener en texto claro se deberá realizar un ataque de fuerza bruta ó de diccionario por si la contraseña es débil.

i. Encontrar donde se alojan las contraseñas en el servidor
ii. Seleccionar la contraseña root y guardarle en un archivo .txt
iii. Para crackear una contraseña normalmente se utilizan las herramientas John the ripper, Hashcat ó alguna otra que viene en la distribución de Kali Linux. Estas herramientas realizan ataques de fuerza bruta ó de diccionario para romper el hash.

Crear un buen diccionario puede llevar años ó el haber realizado un robo masivo de contraseñas de alguna base de datos importante. Si no tienes tu propio diccionario puedes usar los siguientes:

- m3g9tr0n 122 million passwords
- RockYou: diccionario obtenido en 2009 de un juego de una red social y una página de publicidad.
  (En Kali: /usr/share/wordlists/rockyou.txt.bz2)
  (http://downloads.skullsecurity.org/passwords/rockyou.txt.bz2)
- Un buen listado de diccionarios:
  (https://wiki.skullsecurity.org/Passwords)

El diccionario m3g9tr0n se puede conseguir en varios sitios de internet. Como el archivo es demasiado grande, se ha hecho una fragmentación con algunas contraseñas y sus hashes por lo que no es necesario ni siquiera utilizar una herramienta de fuerza bruta. Encontrar la contraseña en texto claro utilizando el comando `grep` de los sistemas Unix.

3.3) Realizar un escaneo sigiloso con nmap dentro de la red y encontrar el servidor de archivos. Acceder como root y obtener los archivos con información sensible de la carpeta 'Proyecto'.

PARTE 2: CONTROLES

GUIÓN

A. ANÁLISIS DEL ATAQUE

1.1) Analizar cuáles han sido los elementos técnicos y humanos que han producido que el ataque haya tenido éxito.

1.2) Analizar qué impacto podría tener este tipo de ataques en una empresa real y como podría repercutir en su economía.

1.3) Analizar qué medidas implementarías si fueses el administrador de sistemas de la empresa.

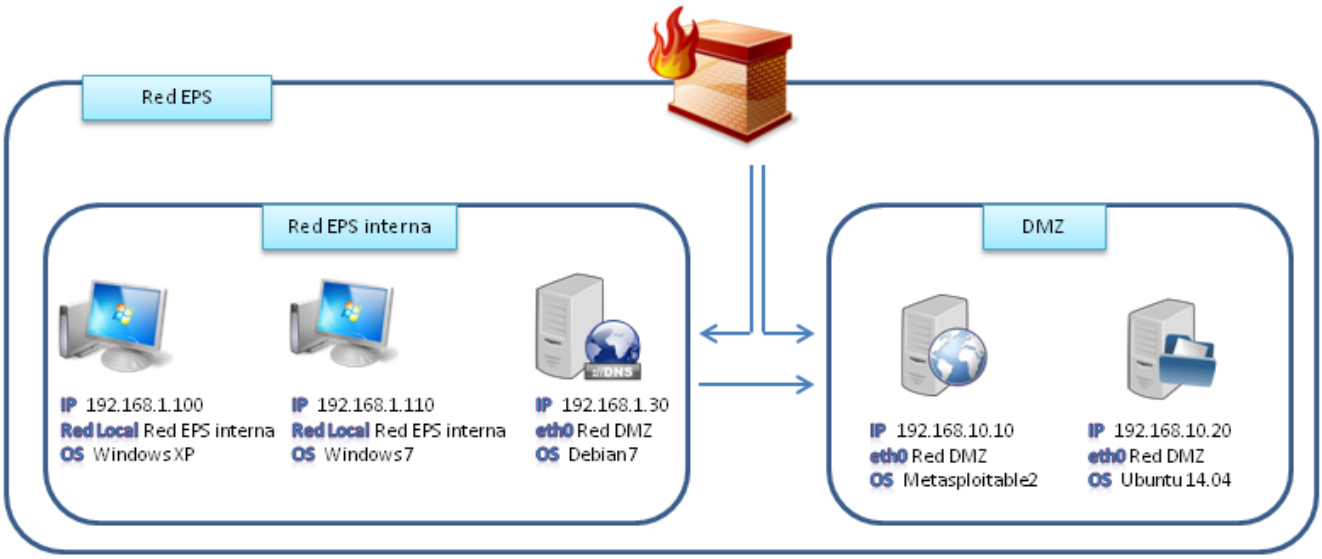
B. IDENTIFICACIÓN DE LOS CONTROLES

2.1) Abrir el documento *Controles-ISO-IEC-27002:2013.pdf* e identificar en el índice qué control ó controles aplicarían a este escenario. Indicar los controles.

2.2) Especificar cuáles son los apartados en la guía de implementación del documento *Controles-ISO-IEC-27002:2013.pdf* que habría que aplicar para prevenir este tipo de ataques de cada control identificado en el apartado anterior.

C. IMPLEMENTACIÓN DE LOS CONTROLES

3.1) Implementar técnicamente el control Segregación en redes. Para poder implementar con éxito este control habrá que configurar las reglas de iptables del firewall para poder redirigir el tráfico hacia la DMZ o la red interna. También habrá que configurar las interfaces de red del firewall para definir distintas vlans. La red debería seguir el siguiente diagrama:



Los cambios a realizar son los siguientes:

i. Abrir Virtualbox y antes de arrancar la máquina virtual firewall ir al apartado de Red.
   El primer adaptador deberá estar en modo NAT (es el que dará internet real a nuestra máquina).
   El segundo adaptador deberá estar en modo Red Interna en la red 'simInternet' (es la red que simulará internet para hacer posible que el atacante tenga conexión con la empresa y todo el tráfico sea en local).
   El tercer adaptador deberá estar en modo Red Interna en la red 'EPS' (es la red interna que simula la red interna de una empresa que utilizarían los trabajadores y el servidor FTP).
   El cuarto adaptador deberá estar en modo Red Interna en la red 'DMZ' (es la zona desmilitarizada donde estarán los servidores Web y DNS)

ii. Acceder como usuario root al firewall. Abrir un terminal y confirmar que tenemos las interfaces configuradas levantadas (ifconfig). En Virtualbox las interfaces ethX se corresponden por orden numérico a los adaptadores, por lo que la interfaz eth0 será el que actúe como NAT, eth1 como simInternet, eth2 como DMZ y eth3 como EPS. En el firewall se han creado interfaces virtuales asociadas a una misma interfaz de la manera eth1:X
En caso de que alguna interfaz no estuviese levantada introducir el siguiente comando:

- root@firewall:~$ ifconfig ethX up

Comprobar que se le ha asignado una IP. En el caso de que no tuviese asignada una IP habrá que configurar el archivo /etc/network/interfaces:

- root@firewall:~$ vi /etc/network/interfaces
  Pulsar la tecla 'i' para habilitar la escritura en vi. La configuración debería quedar así:

```
root@fw:/home/tecnico# cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The simInternet network interface
auto eth1
auto eth1:0
auto eth1:1
iface eth1 inet static
        address 172.16.1.1
        netmask 255.255.255.0
        network 172.16.1.0

iface eth1:0 inet static
        address 172.16.1.10
        netmask 255.255.255.0
        network 172.16.1.0

iface eth1:1 inet static
        address 172.16.1.20
        netmask 255.255.255.0
        network 172.16.1.0



# The EPS network interface
auto eth2
iface eth2 inet static
        address 192.168.1.1
        netmask 255.255.255.0
        gateway 20.20.20.20
        broadcast 192.168.1.255
        network 192.168.1.0
        dns-nameservers 192.168.1.30
```

- root@firewall:~$ service networking restart
- root@firewall:~$ update-rc.d networking enable
- root@firewall:~$ reboot

iii. Con las interfaces bien configuradas, visualizar las reglas configuradas en iptables:

- root@firewall:~$ iptables -L

En iptables las reglas se establecen en cadena, eso significa que primero se aplicará la primera regla, luego la segunda y así hasta completar la cadena.
Para facilitar el proceso de creación de reglas de iptables se va a utilizar una GUI llamada Fwbuilder que permite diseñar la política de seguridad y aplicarla en la máquina que haga de cortafuegos.

Un firewall dependiendo de que esté asegurando puede tener distintas reglas, pero los elementos esenciales suelen ser comunes a todos, entre los que se incluyen:

1) El destino nunca debe ser el firewall
2) Incluir siempre como última regla una regla de denegación por defecto
3) Incluir siempre registro en reglas de denegación
4) Restringir al máximo los elementos que conforman las reglas
5) Restringir al máximo el tráfico saliente. Por ejemplo: sólo permitir el tráfico saliente a puertos 80, 443 y 21.

Acceder a la máquina firewall y abrir fwbuilder. Cargar el archivo fw-tfg-policy2_nat.fwb y comprobar todas las reglas en el apartado Policy. En el apartado NAT, habilitar el enrutamiento para el servidor FTP desde la red Biblioteca.

Guardar la nueva configuración y ejecutar el script fw_last_policy.sh en el directorio /etc/fw/ para cargar las nuevas reglas de iptables.

iv. Con estas buenas prácticas, diseñar teóricamente qué reglas se necesitarían para hacer una segregación de redes.
v. Implementar las reglas en el firewall y realizar los ajustes necesarios en todas las máquinas virtuales para el buen funcionamiento de la red empresarial.

MEMORIA

El alumno deberá documentar todo el proceso del ataque a través de capturas de pantalla de lo únicamente pedido e incluyendo las explicaciones necesarias para su comprensión por parte del profesor en la corrección.
Para no extender la memoria, incluir los comandos que tengan una cierta cohesión en una misma captura. (p. ej. ifconfig, cat /etc/network interfaces; set lhost, set rhost, set...)
En la segunda parte se deberá contestar a todas las preguntas realizadas y documentar las implementaciones de los controles tanto prácticas como teóricas.

LABORATORIO DE CIBERSEGURIDAD

PRÁCTICA 4: CONTROL DE ACCESO EXTERNO A TRAVÉS DE UN PROTOCOLO CIFRADO

Objetivos:

- Conocer algunas de las herramientas más populares y conceptos básicos de un ataque hacking en cada una de las fases que establece la certificación CEH (Certified Ethical Hacker) y la metodología OSSTMM (Open Source Security Testing Methodology Manual). El ataque de esta práctica estará basado en capturar y analizar el tráfico de una red pública donde la víctima usa protocolos sin cifrado.
- Conocer el estándar ISO-IEC 27001 v2013, especialmente los controles que el estándar ISO-IEC 27002 proporciona como las mejores prácticas de seguridad en la gestión de la seguridad de la información.
- El alumno deberá determinar, relacionar e implantar, si fuese posible, los controles propuestos por la ISO-IEC 27002 en el entorno empresarial virtualizado entregado que aplican en el escenario propuesto.

Instrucciones generales preliminares:

En el paquete *EntornoEmpresarialVirtualizado.rar* entregado al alumno encontrará todas las máquinas virtuales necesarias para el buen desarrollo de la práctica. El paquete incluye las siguientes máquinas virtuales:

- Firewall
- Servidor Web
- Servidor DNS
- Servidor FTP
- Windows XP
- Windows 7
- Kali Linux

Para preparar el entorno virtual realizar los siguientes pasos:

1) Abrir Oracle VirtualBox
2) Descomprimir el paquete *EntornoEmpresarialVirtualizado.rar*
3) Lanzar todas las máquinas virtuales al hacer doble-click en el archivo *NombreMáquina.vbox*

Instrucciones generales específicas:

Para esta práctica el alumno necesitará comprobar las IPs de algunas máquinas virtuales para simular una red pública externa de la empresa.
La máquina virtual Windows XP deberá tener una IP 172.16.1.110
La máquina virtual Kali Linux deberá tener una IP 172.16.1.2

Para poner una IP estática en Windows 7 hay que seguir los siguientes pasos:

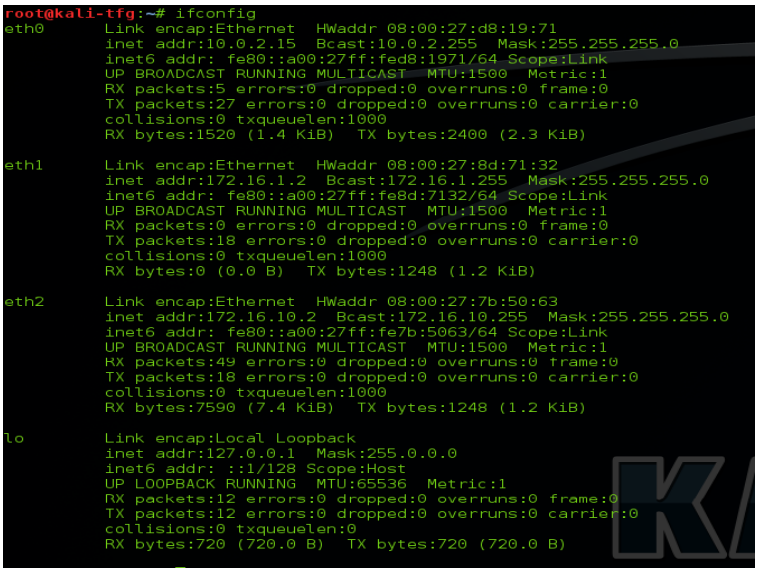
1) Ir a Inicio > Panel de Control > Redes e Internet > Centro de Redes y Recursos Compartidos
2) En el panel de la izquierda pinchar con el botón izquierdo en 'Cambiar configuración del adaptador'
3) Pinchar con el botón derecho en 'Conexión de área local' y en 'Propiedades'
4) Seleccionar 'Protocolo de Internet versión 4 (TCP/IPv4)' y pinchar en propiedes
5) Seleccionar 'Usar la siguiente dirección IP' e introducir los siguientes valores:

- Dirección IP: 172.16.1.100
- Máscara de subred: 255.255.255.0
- Puerta de enlace predeterminada: -

Comprobar las interfaces y las IPs que tiene la máquina atacante Kali Linux
1) Mirar las interfaces de red levantadas (eth0, eth1...ethN, lo) y toda la información relativa a ellas:

- root@kali-tfg:~# ifconfig

El resultado debería ser el siguiente:



La interfaz eth0 será la interfaz de tipo NAT de VirtualBox para tener acceso a internet en el caso de que necesitemos buscar información.
La interfaz eth1 será una interfaz de tipo Red Interna de VirtualBox con nombre simInternet y que simulará Internet y en la que tendremos asignada una IP "pública".
La interfaz eth2 será una interfaz Red Interna con nombre <Starbucks> y que simulará una red local pública y en la que tendremos asignada una IP local.

PARTE 1: ATAQUE

HISTORIA

A. FASE DE RECONOCIMIENTO

A pesar de encontrar la última vez todo lo que tu amigo quería, te pide si puedes conseguir la lista de contactos de una persona del departamento económico financiero para obtenr información que le permita montarse él su propia empresa que les haga la competencia robándoles sus clientes.
La persona de económico financiero en su Facebook no para de poner comentarios de lo que está estudiando para sacarse un máster y que encima tiene que trabajar en la biblioteca para sacar adelante su 'proyecto' start-up. En sus comentarios también añade la localización de la biblioteca a la que suele asistir por lo que decides ir a ver si capturas algo.
Una vez llegas te sientas detrás de ella a ver si averiguas sus credenciales grabando su teclado con tu móvil cuando se conecte a alguna red social. Después de pensarlo bien decides que puede ser arriesgado hacer eso ya que alguien te puede ver y puedes meterte en problemas más graves.
Así que decides esperar, de repente realiza una llamada agobiada en la que oyes partes de la conversación:

-Necesito unos excels muy importantes que hice el otro día y me dejé en el servidor de archivos
-...
-¿Por telnet?¿Qué es eso?
-...
-¿Y ya está? Ok, muchas gracias, te debo una

Al oír telnet, se te abren los ojos como platos y se te ilumina la cara, no estará pensando acceder por telnet a un servidor hoy en día ¿no? ¡Pero si no está cifrado! Rápidamente abres tu portátil y tardas en escribir Wireshark en un terminal lo mismo que en pensarlo. Te preguntas por qué la gente ataja y hace las cosas mal, pero sabes la respuesta. La seguridad es incompatible con la usabilidad y funcionalidad.

B. FASE DE ESCANEO Y ENUMERACIÓN

Como todavía tienes unos minutos hasta que la persona investigada, que como cualquier persona ajena a lo verdaderamente técnico, le llevará unos minutos abrir un terminal en windows y entrar en telnet.

Eso te da el tiempo perfecto para escribir un script en Bash para que te muestre las contraseñas en texto claro a través de tcdump (más clásico que wireshark, mucho más discreto sin colorines y menos conocido por si alguien te ve).

Cuando estás a medias con el script, parece ser que el tiempo se te ha pasado sin darte cuenta ya que la chica tiene todo instalado y acaba de abrir un terminal. Tendrás que usar Wireshark, aunque ya luego termines ese script, por amor al arte.

Empieza a parecer el protocolo telnet en la pantalla, aún así te sigue chocando, es tan de la vieja escuela... Sigues el stream tcp de un paquete telnet y como por arte de magia (es lo que tienen los protocolos sin cifrado) aparecen los caracteres del usuario y de la contraseña.

C. FASE DE EXPLOTACIÓN
Con las contraseñas obtenidas accedes al servidor de archivos y buscando entre los directorios consigues la lista de contactos de los clientes.

GUIÓN

A. FASE DE RECONOCIMIENTO

1) Tras haber realizado una investigación con los buscadores web (google hacking, bing hacking...), las redes sociales de nuestro objetivo y el reconocimiento físico, obtienes:

Localización de la biblioteca.
Protocolo de acceso remoto que va a utilizar: telnet.

B. FASE DE ESCANEO Y ENUMERACIÓN

2.1) Conectarse a la misma red pública que la víctima y realizar un escaneo para determinar la IP local que tiene nuestra víctima. Empezar a capturar todo el tráfico de nuestro objetivo con la herramienta wireshark (tcdump si se prefiere en modo terminal).

2.2) En este apartado el alumno asumirá el rol de la víctima por lo que tendrá que iniciar sesión en el ordenador de Windows XP como rrhh e iniciar una sesión telnet con el servidor de archivos FTP.

2.3) Desde Kali Linux, con wireshark abierto:

i. Identificar la IP objetivo
ii. Establecer los determinados filtros en wireshark para capturar todo el tráfico de esa IP de los siguientes protocolos:
    - TCP
    - HTTP
    - Telnet
iii. Seguir la transmisión TCP de telnet y obtener las credenciales

2.2) (OPCIONAL) Automatizar la obtención de las credenciales a partir de tcdump.
Programar un script en Bash que:

i. Muestre las credenciales en tiempo real por el terminal
ii. Tras haber guardado todo el tráfico telnet en un archivo, extraiga sólo las credenciales

C. FASE DE EXPLOTACIÓN
3) Una vez obtenidas las claves:

i. Acceder con las credenciales al servidor víctima

ii. Crear una puerta trasera para futuras explotaciones del sistema:
   - Crear un nuevo usuario con privilegios root

PARTE 2: CONTROLES

GUIÓN

A. ANÁLISIS DEL ATAQUE

1.1) Analizar cuáles han sido los elementos técnicos y humanos que han producido que el ataque haya tenido éxito.

1.2) Analizar qué impacto podría tener este tipo de ataques en una empresa real y como podría repercutir en su economía.

1.3) Analizar qué medidas implementarías si fueses el administrador de sistemas de la empresa

B. IDENTIFICACIÓN DE LOS CONTROLES

2.1) Abrir el documento *Controles-ISO-IEC-27002:2013.pdf* e identificar en el índice qué control ó controles aplicarían a este escenario. Indicar los controles.

2.2) Especificar cuáles son los apartados en la guía de implementación del documento *Controles-ISO-IEC-27002:2013.pdf* que habría que aplicar para prevenir este tipo de ataques de cada control identificado en el apartado anterior.

C. IMPLEMENTACIÓN DE LOS CONTROLES

3.1) Implementar, teóricamente OpenVPN y prácticamente el cliente SSH en Windows del apartado d) del control Teletrabajo.

i. Los trabajadores deberían poder usar una vpn (OpenVPN) y el técnico de sistemas ssh (OpenSSH).

ii. Instalar un cliente SSH en las máquinas de los trabajadores. Un cliente de SSH en Windows es PuTTy que se puede descargar en el siguiente enlace:

   1) http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe
   2) Instalar PuTTY y ejecutarlo
   3) En el espacio Host Name escribir la IP del servidor Web y el puerto 22
      En Saved Sessions escribir el nombre con el que queremos guardar esta configuración para un futuro y pinchar en Save.
   4) Pinchar en Open y se abrirá una terminal para introducir las credenciales del sistema remoto.

MEMORIA

El alumno deberá documentar todo el proceso del ataque a través de capturas de pantalla de lo únicamente pedido e incluyendo las explicaciones necesarias para su comprensión por parte del profesor en la corrección.
Para no extender la memoria, incluir los comandos que tengan una cierta cohesión en una misma captura. (p. ej. ifconfig, cat /etc/network interfaces; set lhost, set rhost, set...)
En la segunda parte se deberá contestar a todas las preguntas realizadas y documentar las implementaciones de los controles tanto prácticas como teóricas.