ASIGNATURA DE MÁSTER:

# SEGURIDAD DE REDES: AUDITORÍA Y HERRAMIENTAS DE SEGUIMIENTO

Curso 2013/2014

(Código:31102045)

## 1.PRESENTACIÓN

En esta asignatura se pretende que el alumno sea capaz de discernir diferentes modelos de securización de las redes de información corporativa y emplear diferentes herramientas en la detección y prevención de posibles ataques al modelo de seguridad. Para ello se mostrarán las diferentes alternativas al uso de datos de sesión para el análisis en detección y se presentarán los métodos preventivos basados en cortafuegos. La última capacidad básica que debe presentar un modelo NSM es la toma de decisiones en base al tráfico de información de la red, por lo que se definen y muestran los sistemas de detección de intrusión como herramienta básica de toma de decisiones.

## 2.CONTEXTUALIZACIÓN

La llegada de Internet y de los entornos corporativos de red (intranet, DMZ, red local, etc.) ha supuesto un cambio radical en la forma de compartir información y de asegurar que el acceso a ésta se haga de manera efectiva y segura. Esta misma disponibilidad de la información ha hecho que los sistemas de red se hayan convertido en objetivos concretos para el acceso ilegal a dicha información (obtención de acceso privilegiado no autorizado como contraseñas de root de los sistemas), además de sufrir efectos secundarios como son la caída de los sistemas o sus componentes (ataques de denegación de servicio) con el grave perjuicio económico que eso conlleva.

De esta forma es necesario desarrollador un modelo de seguridad global a la organización (NSM, Network Security Model) que permita:

- Analizar el tráfico de red y el uso que se hace de la misma, de forma que se tomen decisiones acerca de la fragmentación del servicio y/o incluso su denegación.
- Detectar accesos no privilegiados a los sistemas.
- Definir las pautas de comportamiento y tipos de acceso a los usuarios.
- Implementar sistemas de detección de intrusos y definir reglas de comportamiento automático de la red en caso de cumplirse los criterios de acceso no autorizado.

Para la implantación de un NSM es necesario contar con todos los elementos relacionados en su definición: personal de las distintas áreas, recursos hardware y software y gestión de la política de seguridad de la institución. Esto implica que un gestor de la seguridad de red debe realizar un plan para el NSM en colaboración con diferentes roles, lo que le obliga a trabajar de manera conjunta con las diferentes áreas de infraestructura informática de la institución.

Esta asignatura pretende centrarse en los conocimientos y mecanismos necesarios para abordar una aproximación profesional a los NSM, presentando las bases y conceptos necesarios para usar la terminología adecuada en un modelo de seguridad de redes. También se realiza una presentación detallada de las diferentes herramientas disponibles en los diferentes objetivos de un NSM (prevención, análisis y detección) y, más en concreto, las herramientas open source disponibles. Complementa de manera efectiva el perfil profesional del resto de asignaturas sobre redes del módulo V (Tecnologías y seguridad de redes) ya que en el resto de asignaturas se cubre la implementación concreta de los

mecanismos de integridad y seguridad a nivel del tratamiento de la información (Criptología aplicada) y la definición de redes móviles e inalámbricas (junto a los mecanismos de seguridad a dichas redes). En este caso la asignatura se centra en los mecanismos globales de securización de la información sin entrar en la información concreta o el tipo de red.

La distribución temporal de la asignatura se ha adecuado a un equilibrio de teoría y práctica mediante la realización de varias actividades prácticas que complementan de manera concreta diferentes áreas del temario de la asignatura. En concreto para cada módulo de la asignatura se desarrollará un conjunto de preguntas de autoevaluación que se elaborarán en la propia plataforma de formación y que permitirá comprobar la efectividad del aprendizaje. Junto a los cuestionarios se fomentará el uso de los foros de discusión sobre los contenidos teóricos que promueva de forma colaborativa la generación de preguntas frecuentas y debates interesantes sobre diferentes aspectos teóricos. Adicionalmente se han programado tres prácticas que pretenden reforzar el aprendizaje de los elementos de análisis de datos (uso de herramientas como Ethereal o TCPDump), prevención (cortafuegos) y detección (IDS como Snort o Nessus) de un NSM. Para finalizar el curso se deberá realizar un NSM global de forma grupal que refleje lo aprendido en un caso prático.

De manera general de las competencias definidas para el módulo V del posgrado, la asignatura cubre las siguientes:

- Comprender el entorno operativo de NSM (Network Security Model) y ser capaz de aplicarlo en un escenario de respuestas e incidentes.
- Conocer y ser capaz de utilizar herramientas para hacer prospecciones en el tráfico de red y para generar paquetes arbitrarios, explorar defectos, manipular el tráfico y efectuar reconocimientos.
- Ser capaz de desarrollar y aplicar conocimientos relativos a armas, tácticas, telecomunicaciones, administradores de sistemas, guiones y programación de un NSM.

De forma particular, se pueden formular las siguientes competencias profesionales particulares que se asumen en esta asignatura y que el alumno deberá tener:

- Adquirir conocimientos generales sobre la seguridad de redes: confidencialidad, integridad, disponibilidad y negación de servicio.
- Distinguir los posibles riesgos en forma de amenazas y/o vulnerabilidades de los componentes hardware o software de la infraestructura corporativa.
- Reconocer los requisitos generales de formación y adecuación del personal involucrado en la definición e implantación del NSM de la institución.
- Ser capaz usar y trabajar de manera efectiva con las diferentes herramientas de análisis de tráfico de red, y detectar anomalías funcionales de uso de la misma.
- Discernir las diferentes situaciones de riesgo de la red mediante las herramientas de detección correspondientes.
- Ser capaz de analizar los datos de red y concluir la utilización correcta o incorrecta del tráfico de red, poniendo los mecanismos necesarios para impedir la utilización incorrecta de la red.
- Situar elementos preventivos (cortafuegos) que definan las reglas de juego de la red, es decir, dando servicios a los componentes del NSM que dispongan del permiso necesario en la política de seguridad de red.
- Organizar y definir la implantación de sistemas de detección de intrusos que permitan obtener información sobre las amenazas reales que sufre la red corporativa.
- Ser capaz de definir reglas de detección no convencionales, adaptadas de manera creativa a la gestión interna de la red de datos de la institución.
- Diseñar y gestionar el proyecto de NSM que implementa la política de seguridad corporativa.

## 3.REQUISITOS PREVIOS RECOMENDABLES

Conocimientos sobre:

- Redes de ordenadores (TCP/IP, Protocolos de aplicación, etc.)
- Arquitectura de ordenadores
- Sistemas operativos

Se considera imprescindible para la realización y seguimiento del curso, que el alumno posea unos sólidos fundamentos en tres áreas fundamentales de la computación moderna:

- Redes de computadores. Todo lo relativo a la seguridad de redes se centra en el conocimiento profundo de los diferentes protocolos de comunicación y los sistemas físicos de interconexión entre dichas redes. Es prioritario el

conocimiento de la pila de protocolos de TCP/IP así como de los protocolos a nivel de capa de enlace (en particular Ethernet).

- Arquitectura de ordenadores. Las amenazas y ataques que se desarrollan a través de las red en muchas casos tienes como objetivos concretos recursos específicos asociados al propio ordenador (servidor) por lo que es frecuente que los componentes de un ordenador se vean afectados por dichos ataques. Es necesario que el alumno conozca dichos componentes y las implicaciones que tiene un fallo o bajada de rendimiento en dichos componentes para realizar valoraciones objetivas de los efectos de un ataque informático.
- Sistemas operativos. Las herramientas de detección y prevención de ataques informáticos se instalan en ordenadores específicos con sistemas operativos enfocados a la compartición de recursos (o componentes) en red. Además la propia programación de los sistemas operativos adolece de fallos que provocan la aparición de vulnerabilidades que pueden ser explotadas a través de ataques de red. Es importante recalcar que la mayor parte de las herramientas que se muestran en el curso han sido desarrolladas mediante la filosofía de software libre y además la mayoría solo están disponibles para el sistema operativo Linux, por lo que es *muy recomendable* un conocimiento alto de este sistema operativo.

Adicionalmente, se recomienda el conocimiento de lenguajes de programación como Java o C que permiten el desarrollo de aplicaciones que permiten la detección y prevención e ataques, además de aplicaciones que simulan, o realizan de forma real, ataques a sistemas informáticos.

## 4.RESULTADOS DE APRENDIZAJE

El objetivo principal de la asignatura consiste en desarrollar y aplicar rápidamente las capacidades necesarias para detectar, prevenir y responder a amenazas nuevas y emergentes en Redes de comunicaciones.

Para lograr el objetivo principal de la asignatura el alumno debe ser capaz de:

- Comprender el entorno operativo de NSM (Network Security Model) y las consideraciones relativas a su implementación
- Utilizar toda una gama de herramientas de software libre, entre las cuales se cuentan Sguil, Argus, y Ethereal, para hacer prospecciones en el tráfico de red en busca de datos de contenido completo, de sesión, estadístico y de alerta.
- Proporcionar un conjunto de prácticas recomendables para la realización de NSM de urgencia en un escenario de respuestas e incidentes, y evaluar a fabricantes de productos de monitorización y despliegue de una arquitectura de NSM.
- Desarrollar y aplicar conocimientos relativos a armas, tácticas, telecomunicaciones, administradores de sistemas, guiones y programación de un NSM.
- Conocer las mejores herramientas para generar paquetes arbitrarios, explorar defectos, manipular el tráfico y efectuar reconocimientos.

## 5.CONTENIDOS DE LA ASIGNATURA

La asignatura está dividida en ocho módulos que abarcan diferentes aspectos del NSM: políticas organizativas en torno a la seguridad, formación del personal cualificado, definición y procesos de la monitorización de la seguridad, casos prácticos de modelos de securización y herramientas de monitorización (Ethereal, Snort), protección (Cortafuegos) y prevención (IDS). El índice detallado para cada uno de los módulos se detalla a continuación:

*Módulo 1. Política de seguridad dentro de una organización*

*1.1. Aspectos físicos*

*1.2. Aspectos lógicos*

*1.3. Aspectos humanos*

*1.4. Aspectos legales*

*1.5. Implantación de políticas de seguridad*

La Política de seguridad es la herramienta básica organizativa que da vida al proceso de seguridad informática. Mediante ella se decide qué se asegura en la organización, cómo se asegura (tanto a nivel técnico como de organización de recursos humanos), qué se monitoriza y cuándo. Es por tanto fundamental tener una idea clara de cómo crearla y mantenerla.

*Módulo 2. Introducción a la monitorización de seguridad en redes*

*2.1. El proceso de securizar*

*2.2. Definición de la monitorización de la seguridad de una red*

*2.3. Consideraciones de implementación*

Mediante la monitorización de la seguridad en redes se llevan a cabo varias fases importantes del proceso de seguridad. Una de ellas es la comprobación permanente de que las políticas de seguridad establecidas están cumpliéndose tal y cómo se ha previsto. Otra fundamental es la vigilancia sobre distintos tipos de problemas no tenidos en cuenta en la política de seguridad y que pueden aparecer en cualquier momento, siendo importante su detección temprana.

*Módulo 3. Principios de la monitorización de la seguridad*

*3.1. El modelo de referencia de intrusiones*

*3.2. Herramientas para el análisis de datos de contenido*

*3.3. Herramientas adicionales*

*3.4. Formato de los datos de sesión*

*3.5. Consideraciones sobre datos estadísticos*

*3.6. Estudio de los datos de alerta*

Se analizan en este modulo los principios más significativos de monitorización siguiendo la idea del “modelo de referencia de intrusiones” y haciendo una exposición de los distintos tipos de herramientas, tanto para análisis de datos como para obtención de estadísticas, finalizando con una aproximación a los modelos de estudio de los datos de alertas.

*Módulo 4. El proceso de monitorización de la seguridad*

*4.1. Prácticas recomendadas*

*4.2. Casos de estudio para administradores*

Se exponen en este módulo una serie de prácticas recomendables sobre cómo gestionar tanto los patrones de búsqueda de problemas en red mediante sistemas de detección de intrusiones como los datos estadísticos de problemas reales encontrados, atendiendo especialmente a la gravedad de la alerta como criterio principal. Se exponen en el módulo también distintos casos de estudio ilustrativos de las ideas precedentes.

*Módulo 5. Características del personal asociado a la monitorización de la seguridad*

*5.1. Definición de un programa de formación*

*5.2. Análisis del tráfico DNS*

*5.3. Análisis de los datos de sesión*

*5.4. Análisis de los datos de los paquetes TCP*

Parece obvio que no cualquier persona podrá hacerse cargo del trabajo de gestión, mantenimiento, configuración y análisis

de resultados de la monitorización. Por esta razón se hace necesario ser especialmente cuidadoso en la definición, estructura y contenidos de un plan de formación adecuado para estas personas, que incluya, entre otros puntos clave, la capacidad de análisis del tráfico DNS, de los datos de sesión y del tráfico de aplicaciones que utilicen transporte TCP

*Módulo 6. Implementación del proceso de monitorización de seguridad*

*6.1. Herramientas para atacar la monitorización de seguridad en redes.*

*6.2. Tácticas para atacar la monitorización de seguridad en redes.*

Como en cualquier disciplina que tenga que ver con la seguridad en cualquiera de sus formas, se ha de conocer las técnicas más habituales para subvertir el proceso de monitorización de seguridad en redes, conociendo las tácticas usadas y, especialmente, las herramientas de las que un posible atacante podría valerse para destruir nuestro sistema de monitorización.

*Módulo 7. Protección de la red: Cortafuegos*

*7.1. Conceptos teóricos*

*7.2. Características de diseño*

*7.3. Componentes de un cortafuego*

*7.4. Arquitecturas de cortafuegos*

*7.5. Casos de estudio*

Una de las herramientas más habituales usada como defensa de una red frente a posibles ataques externos es el cortafuegos. En este módulo se analizan tanto conceptos teóricos como las diferentes características de diseño de los diferentes tipos de cortafuegos. Es especialmente importante conocer los componentes de un cortafuego y su implementación en las diferentes arquitecturas tecnológicas. Igualmente se expone distintos ejemplos ilustrativos.

*Módulo 8. Sistemas de detección de intrusos*

*8.1. Clasificación de los IDS*

*8.2. Requisitos de un IDS*

*8.3. IDS basados en máquina*

*8.4. IDS basados en red*

*8.5. Detección de anomalías*

*8.6. Detección de usos indebidos*

*8.7. Implementación real de un IDS*

La otra herramienta fundamental en cualquier implementación de una buena política de seguridad en redes es el sistema de detección de intrusiones (o “Intrusión Detection System”) que permite implementar prácticamente todas las funciones de monitorización citadas. Es por lo tanto fundamental conocer qué son, qué requisitos deben cumplir, así como la diferencia entre los que se basan en una máquina y los que están basados en red. Igualmente importante es conocer las diferencias tecnológicas entre los que basan su trabajo en detección de anomalías, de usos indebidos o de firmas de ataque.

## 6.EQUIPO DOCENTE

- GABRIEL DIAZ ORUETA
- MANUEL ALONSO CASTRO GIL

- RAFAEL PASTOR VARGAS
- ANTONIO ROBLES GOMEZ

## 7.METODOLOGÍA

De forma resumida la metodología docente se concreta en:

- Adaptada a las directrices del EEES.
- La asignatura no tiene clases presenciales. Los contenidos teóricos se impartirán a distancia, de acuerdo con las normas y estructuras de soporte telemático de la enseñanza en la UNED. Esta asignatura se impartirá a distancia, utilizando una plataforma de educación a través de Internet. Se organizarán foros de discusión para dudas y debates.
- El material docente incluye cuestionarios de autoevaluación sobre los contenidos de cada tema y distintos tipos de actividades relacionadas con la asignatura: consulta bibliográfica, consulta de información en Internet, trabajos de análisis y resumen, y uso avanzado de herramientas software.
- Tratándose de un master orientado de forma profesional, las actividades de aprendizaje se estructuran en torno al estado del arte en cada una de las materias del curso y a los problemas en los que se va a focalizar en el trabajo final, sobre el que se realizará la evaluación.

La metodología docente se desarrolla de acuerdo con los siguientes principios:

- Además de adoptar la metodología docente general del programa de postgrado, y en coherencia con el propósito de utilizar los sistemas interactivos de educación con fines pedagógicos y/o formativos, la asignatura diseñada se apoya en gran medida en los recursos educativos de este medio.
- La metodología del trabajo de la asignatura se basa en una planificación temporal de las actividades. Existirán diferentes módulos o unidades didácticas. Cada uno de éstos tendrá asociado unas unidades de aprendizaje y un material asignado (capítulos del libro base, artículos relacionados, direcciones adicionales de Internet, o cualquier otro material que se proporcione). Se asignará un período para cada módulo, en el que deberán realizar las actividades relacionadas con el mismo.

## 8.BIBLIOGRAFÍA BÁSICA

ISBN(13): 9788420546001
Título: EL TAO DE LA MONITORIZACIÓN DE SEGURIDAD EN REDES (2005)
Autor/es: R. Bejtlich ;
Editorial: PEARSON EDUCACIÓN

Buscarlo en libreria virtual UNED

Buscarlo en bibliotecas UNED

Buscarlo en la Biblioteca de Educación

Buscarlo en Catálogo del Patrimonio Bibliográfico

Comentarios y anexos:

En esta asignatura se han elegido dos textos básicos recomendados:

- El Tao de la monitorización de Seguridad en redes, Richard Bejtlich. Editorial Pearson Educación, 2005
- Seguridad en Unix y Redes, Antonio Villalón Huerta. Disponible de forma gratuita en:

http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec.pdf

El segundo texto se distribuye de forma gratuita por lo que no redunda en ningún tipo de perjuicio económico extra para el alumno. El primer libro se adapta al contenido de los temas 2 a 6 mientras que la publicación electrónica se emplea para el estudio de los temas 1, 7 y 8. Adicionalmente, mediante la utilización de los medios telemáticos necesarios (web, email, etc.) se le proporcionará al alumno realimentación sobre información relevante de la asignatura que, dada la naturaleza de la misma, complementará la formación del alumno.

El libro base, *El Tao de la monitorización de Seguridad en redes*, de la asignatura aborda de una manera profunda los conceptos básicos sobre el modelo de seguridad de redes en todas sus fases: definición, diseño, implantación y evaluación. Se hace especial hincapié en las herramientas de monitorización de redes, en concreto las disponibles como Open Source, como piezas clave para la obtención de información sobre posibles ataques que permita detectar problemas en el modelo de seguridad. Se presentan casos prácticos desde el punto de vista de los administradores de la seguridad de red y sistemas para poder evaluar la seguridad desde el punto de vista de un atacante externo.

Por otra parte la publicación electrónica, Seguridad en Unix y Redes, aborda de manera global el tema de seguridad, no solo a nivel de las redes de comunicaciones, en entornos Linux/Unix. Abarca desde la securización de componentes hardware hasta el conchero de auditoria (y sus herramientas Unix/Linux asociadas). Se presentan diferentes sistemas operativos basados en Linux junto a sus premisas de seguridad. Dispone de una parte dedicada totalmente a las herramientas de seguridad de redes en entornos Unix, con especial detalle en los sistemas de prevención (cortafuegos) y detección (IDS). Es una obra muy completa que cubre muchos conceptos globales de seguridad como la propia criptografía, asignatura de este postrado, entre otras.

## 9.BIBLIOGRAFÍA COMPLEMENTARIA

### Comentarios y anexos:

El alumno puede consultar la siguiente bibliografía con el fin de aclarar o extender los conocimientos que debe adquirir a lo largo del curso, y más en concreto en lo concerniente a las herramientas de software libre disponibles para la realización de las actividades prácticas:

- Seguridad en las comunicaciones e información, Gabriel Díaz y otros, Ed. UNED, 2004.

En este libro se trata de dar una descripción extensiva de conceptos, terminología, modos de administración y configuración de los dispositivos, programas y aplicaciones dirigidas a conseguir la mejor disponibilidad, fiabilidad y privacidad de los sistemas y redes una organización. Todo ello dentro del marco de una política de seguridad, verdadero “cerebro” organizativo de toda la estructura de seguridad de una organización. Igualmente se presentan los conceptos y algoritmos cuyo conocimiento resulta necesario para entender las técnicas criptográficas usadas para redes privadas virtuales y sistemas de comercio electrónico, otra parte esencial de los sistemas de seguridad de la información en cualquier organización.

- Software libre: Herramientas de seguridad, Tony Howlett, Ed. Anaya Multimedia, 2005.

El software de libre distribución es una parte tan integral de Internet que posiblemente la Red no existiría tal y como la conocemos actualmente, ni hubiera crecido de modo tan rápido y dinámico, sin este tipo de software. En el terreno de la seguridad, existen infinidad de programas dirigidos a todas las áreas de la seguridad IT: cortafuegos de libre distribución, sistemas de detección de intrusión, escáneres de vulnerabilidad, herramientas forenses y aplicaciones para las áreas más actuales como las comunicaciones inalámbricas. El libro muestra las mejores aplicaciones en cada área de seguridad de la información, presentándolas de manera detallada, para descubrir no sólo las claves de su funcionamiento, sino también cómo optimizar su uso en el trabajo diario para tener una red más segura.

- Network Intrusion Detection, Stephen Northcutt & Judy Novak, Sams Press, 2002.

La detección de intrusos es una de las áreas de crecimiento más importante en la seguridad de redes. A medida que el número de redes corporativas, del gobierno y educacionales crecen y se interconectan a través de Internet, se aumenta de manera correlativa la propensión a recibir tipos y números diferentes de ataques. El libro constituye una ayuda práctica y de referencia para el análisis de la detección de intrusiones. Se hace una introducción sobre las conceptos básicos de la detección y se muestran ejemplos de experiencias reales y de patrones actuales de tráfico de red factibles de ser ataques.

- Seguridad de redes, Chris McNab, Ed. Anaya Multimedia, 2004.

Para conocer y subsanar las vulnerabilidades de un sistema es necesario profundizar en las características de los ataques a los que puede ser sometido. No obstante, muchos administradores únicamente logran alcanzar los límites de sus sistemas de forma casual. En este libro, se muestran las estrategias que siguen los expertos en seguridad de redes empresariales para identificar y determinar los riesgos existentes en las redes informáticas, logrando de esta manera una reducción significativa de riesgos. El libro comienza presentando las herramientas y rápidamente le conduce a través de los medios de los que dispone un atacante para aprender sobre las máquinas que forman su red. De esta manera, se progresará tanto en el conocimiento de los componentes de su red, como en los diferentes servicios en ejecución y cómo pueden ser atacados, de modo que descubra progresivamente y de una manera efectiva las técnicas a seguir para combatir los temidos ataques.

- Nessus, Snort, & Ethereal Power Tools: Customizing Open Source Security Applications, Brian Caswell, Gilbert Ramirez, Jay Beale, Noam Rathaus, Syngress, 2005.

El libro cubre la personalización de Snort para la tarea de la detección de intrusos y la prevención. Además se muestra como Nessus se emplea para analizar la capa de red en busca de vulnerabilidades y Ethereal para la obtención del tráfico de red en busca de tráfico no usual o malicioso. En el apéndice del libro se puede encontrar de manera detallada las mejores herramientas Open Source de la seguridad de redes. En el libro se describe los conceptos más importantes de la codificación y personalización de las tres herramientas, además de proporcionar scripts que pueden ser usados en situaciones reales.

- Firewalls, Bill McCarty, Ed. Anaya Multimedia, 2003.

Red Hat Linux es un sistema operativo relativamente seguro. Si se instala y configura correctamente, puede ser muy resistente a los ataques. Sin embargo, el nivel de las amenazas que surgen de Internet es considerable. El libro comienza por presentar unos cimientos sólidos sobre la tecnología y filosofía de seguridad. Examina la importancia de la seguridad perimetral y el papel fundamental que juegan los cortafuegos de filtrado de paquetes, muestra los patrones de tráfico de red asociados con los servicios comunes de Internet y explora métodos para desarrollar directivas de cortafuegos que permiten, prohiben o restringen el uso. Con este libro, se muestra cómo diseñar, implementar, probar y operar cortafuegos de filtrado de paquetes construidos con Red Hat Linux. También encontrará valiosa información acerca de temas relacionados, como implementar hosts bastiones y detectar intrusiones en la red.

- Security Through Penetration Testing, T. J. Klevinsky, Scott Laliberte, Ajay Gupta, Addison-Wesley Professional, 2002.

El libro hace una introducción a las pruebas de penetración y su importancia vital en el plan de seguridad global de la red. Muestra los roles y responsabilidades asociadas a un plan de pruebas de penetración profesional, la motivación y estrategias de la comunidad de piratas informáticos (hackers), además de las potenciales vulnerabilidades de los sistemas junto a los correspondientes ataques disponibles. El libro incluye un conjunto de scripts (framework) para la realización de los tests y ofrece descripciones pasos a paso de cada etapa del proceso.

- Snort 2.1 Intrusion Detection, Jay Beale & Caswell, Syngress, 2004.

El libro cubre de una manera muy amplia la instalación y configuración de Snort, además de hacer una inmersión en el propio código de Snort. Snort tiene tres usos principales: como analizador de paquetes de red, como grabador de paquetes de red o como sistema de detección de intrusiones. En el libro se muestra como Snort usa un lenguaje flexible para la definición de reglas que describe el tráfico que debería grabar o dejar pasar, además de la arquitectura modular de componentes (plugins) y el sistema de alerta en tiempo real

- Ethereal Packet Sniffing, Angela D. Orebaugh & Gilbert Ramirez, Syngress, 2004.

Este libro proporciona a los administradores de sistemas toda la información necesaria sobre Ethereal además del software específico para ejecutar el analizador de protocolo de Ethereal en sus propias redes. Cubre la instalación y configuración de Ethereal y tópicos avanzados como la optimización del rendimiento de Ethereal y el análisis de los datos obtenidos por la herramienta.

## 10.RECURSOS DE APOYO AL ESTUDIO

Recursos de apoyo

Curso virtual

Para alcanzar todos los objetivos propuestos, el curso se va a articular, como ya se ha comentado, a través de una plataforma especialmente diseñada para facilitar el trabajo colaborativo en Internet (basada en comunidades virtuales), desarrollada por la Sección de Innovación del Centro de Innovación y Desarrollo Tecnológico de la UNED: aLF, ubicada en http://www.innova.uned.es.

La plataforma de e-Learning aLF, proporcionará el soporte requerido para gestionar los procesos de enseñanza y aprendizaje, compartir documentos y enlaces de interés, crear y participar en comunidades temáticas y grupos de trabajo específicos, realizar proyectos de diversa naturaleza, organizar el trabajo mediante agendas compartidas e individuales, acceder y publicar noticias de interés, etc.

La plataforma de aprendizaje en Internet permitirá realizar el seguimiento de las actividades del curso, así como estar al tanto de cualquier información o documentación de interés relacionada con el mismo. Para poder utilizar esta plataforma y para mantener un contacto personal con el alumnado se necesitará una dirección de correo electrónico suministrada por el Centro de Servicios Informáticos de la Uned. La filosofía de uso es bien sencilla. Todas las interacciones se hacen a través de enlaces. Por lo tanto, con sólo seguir dichos enlaces se podrá acceder a foros de discusión, documentos de compañeros, etc.

Una vez familiarizados con su uso, es importante tener en cuenta que todas las novedades, instrucciones, actividades se van a publicar utilizando este medio, por tanto, el alumno debe entrar en el grupo frecuentemente para ver si hay alguna novedad en el curso. Si, además, tiene activados ciertos avisos, podrá recibir notificaciones en el correo electrónico utilizado para acceder a la plataforma de los mensajes republicados en los foros, los documentos subidos, las citas puestas en el calendario, por lo que tendrá una información instantánea de todo lo que acontece en la plataforma.

Para comenzar las actividades planificadas es necesario registrase en la plataforma de aprendizaje y colaboración aLF. Por otro lado, para poder organizar adecuadamente el grupo de trabajo, es necesario conocer cuáles son los conocimientos de partida de los alumnos, preferencias y temas de interés. Por eso, al inicio del curso pondremos disponibles unos cuestionarios y les pediremos que los rellenen.

Se ofrecerán las herramientas necesarias para que, tanto el equipo docente como el alumnado, puedan compaginar el trabajo individual y el aprendizaje colaborativo.

Software para prácticas.

Se ubicará en la propia plataforma, en el área correspondiente, o bien se darán los enlaces correspondientes de las ubicaciones originales donde descargar tanto el software como los correspondientes manuales

## 11.TUTORIZACIÓN Y SEGUIMIENTO

La tutorización de los estudiantes tendrá lugar esencialmente a través de los foros de la plataforma, aunque también podrán utilizarse ocasionalmente otros medios, tales como chats interactivos, servicios de mensajería instantánea y el correo electrónico. Adicionalmente, está también previsto, para temas personales que no afecten al resto de los estudiantes, atender consultas en persona o por teléfono.

El seguimiento del aprendizaje se realizará revisando la participación de los alumnos en los distintos foros de debate y las aportaciones de material nuevo además de la entrega en fecha de los diferentes trabajos prácticos que se han planificado durante la evolución del curso.

## 12.EVALUACIÓN DE LOS APRENDIZAJES

La evaluación es un aspecto esencial del propio proceso de aprendizaje y como tal se hará uso de la misma. Esto implica que a lo largo del curso, y de acuerdo con la planificación de actividades previstas, el alumno podrá acceder tanto a los resultados de los ejercicios de auto-evaluación propuestos como a las calificaciones y valoraciones de los trabajos

presentados en cada tarea y práctica.

La evaluación estará fundamentalmente centrada en la reorientación y motivación del aprendizaje, así como en facilitar la capacidad de auto-comprensión del los conocimientos y las destrezas adquiridas.

Por otro lado, la evaluación es una herramienta esencial para el control de la tarea docente y, en este sentido, se pedirán valoraciones de las tareas propuestas y del propio planteamiento de la docencia de la asignatura. Se prevée al menos una evaluación de este tipo a lo largo del curso.

En cuanto a los ejercicios que requieran trabajo colaborativo, por la propia naturaleza de la asignatura, se aprovecharán especialmente las ventajas que aporta la plataforma de colaboración de la UNED, aLF.

Los criterios de evaluación que se seguirán en las tareas de tipo colaborativo serán los siguientes:

- Garantizar la interdependencia positiva: se valorará tanto la realización de las tareas individuales como las de grupo de forma que el estudiante se sienta motivado para ayudar al resto para alcanzar los objetivos del grupo.
- Capacidad de interacción: se evaluará el grado de interacción y participación en las actividades propuestas.
- Responsabilidad individual y de grupo: se valorará la consecución de los objetivos del grupo y de las tareas individuales en las que ha participado cada miembro del mismo.
- Desarrollo de capacidades de colaboración: se evaluará de forma independiente el aprendizaje de las destrezas asociadas a la resolución de la tarea objeto de las capacidades propias de colaboración.
- Análisis del trabajo de grupo: se evaluará la propia evaluación que los alumnos hagan de la productividad del grupo, distinguiendo el valor relativo de las distintas tareas individuales y de su gestión a lo largo del tiempo, de forma que puedan tomarse medidas de corrección que ayuden a alcanzar los objetivos de tarea y de colaboración previstos.

El alumno deberá entregar una memoria en la que se concreten sus aportaciones en la realización de todas las actividades propuestas.

La evaluación global se calculará de acuerdo al siguiente polinomio:

Nota (final) = [Nota (ejercicios-prácticos) x 0.7] + [Nota (trabajo final) x 0.3]

## 13.COLABORADORES DOCENTES

Véase equipo docente.