17-18

MÁSTER UNIVERSITARIO EN COMUNICACIÓN, REDES Y GESTIÓN DE CONTENIDOS

GUÍA DE ESTUDIO PÚBLICA

SEGURIDAD DE REDES: AUDITORÍA Y HERRAMIENTAS DE SEGUIMIENTO

CÓDIGO 31102045

UNED

17-18

SEGURIDAD DE REDES: AUDITORÍA Y HERRAMIENTAS DE SEGUIMIENTO

CÓDIGO 31102045

ÍNDICE

Nombre de la asignatura	SEGURIDAD DE REDES: AUDITORÍA Y HERRAMIENTAS DE SEGUIMIENTO
Código	31102045
Curso académico	2017/2018
Títulos en que se imparte	MÁSTER UNIVERSITARIO EN COMUNICACIÓN, REDES Y GESTIÓN DE CONTENIDOS
Tipo	CONTENIDOS
Nº ETCS	10
Horas	250.0
Periodo	SEMESTRE 2
Idiomas en que se imparte	CASTELLANO

PRESENTACIÓN Y CONTEXTUALIZACIÓN

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.

REQUISITOS Y/O RECOMENDACIONES PARA CURSAR ESTA ASIGNATURA

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.

EQUIPO DOCENTE

Nombre y Apellidos	GABRIEL DIAZ ORUETA
Correo Electrónico	gdiaz@ieec.uned.es
Teléfono	91398-7795
Facultad	ESCUELA TÉCN.SUP INGENIEROS INDUSTRIALES
Departamento	ING.ELÉCT., ELECTRÓN., CONTROL, TELEMÁT.

Nombre y Apellidos	MANUEL ALONSO CASTRO GIL
Correo Electrónico	mcastro@ieec.uned.es
Teléfono	91398-6476
Facultad	ESCUELA TÉCN.SUP INGENIEROS INDUSTRIALES
Departamento	ING.ELÉCT., ELECTRÓN., CONTROL, TELEMÁT.

Nombre y Apellidos	RAFAEL PASTOR VARGAS
Correo Electrónico	rpastor@dia.uned.es
Teléfono	91398-8383
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	SISTEMAS DE COMUNICACIÓN Y CONTROL

Nombre y Apellidos	RAFAEL PASTOR VARGAS
Correo Electrónico	rpastor@scc.uned.es
Teléfono	91398-8383
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	SISTEMAS DE COMUNICACIÓN Y CONTROL

Nombre y Apellidos	ANTONIO ROBLES GOMEZ
Correo Electrónico	arobles@scc.uned.es
Teléfono	91398-8480
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	SISTEMAS DE COMUNICACIÓN Y CONTROL

HORARIO DE ATENCIÓN AL ESTUDIANTE

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.

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE

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.

CONTENIDOS

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.

SISTEMA DE EVALUACIÓN

BIBLIOGRAFÍA BÁSICA

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

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.

BIBLIOGRAFÍA COMPLEMENTARIA

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 empreses 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.

RECURSOS DE APOYO Y WEBGRAFÍA

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

---

IGUALDAD DE GÉNERO

En coherencia con el valor asumido de la igualdad de género, todas las denominaciones que en esta Guía hacen referencia a órganos de gobierno unipersonales, de representación, o miembros de la comunidad universitaria y se efectúan en género masculino, cuando no hayan sido sustituido por términos genéricos, se entenderán hechas indistintamente en género femenino o masculino, según el sexo del titular que los desempeñe.