Seguridad de Sistemas en Redes

UC	HT	HP	HL	Modalidad	Código	Requisitos	Ult. Actualización
5	4	2		Optativa Electiva	6022	Redes de Computadoras	Marzo de 2019

Fundamentación

En nuestra interconectada sociedad, donde altos volumenes de datos e información son transmitidos a lo largo y ancho del mundo a través de Internet, el tópico de la seguridad de redes y sistemas de computadoras cobra especial relevancia. Dada la prevalencia de ataques a sistemas de red por criminales e incluso actores guvernamentales, es de suma importancia que el profesional de las Ciencias de la Computación esté debidamente preparado para encarar el reto que representa el mantenimiento de la seguridad de los sistemas informáticos.

En este curso se plantea el estudio de técnicas y herramientas de seguridad de redes, las cuales permiten adoptar enfoques defensivos como por ejemplo la criptografía y el uso de *firewalls* y sistemas de detección de intrusos, o enfoques proactivos mediante la verificación de software aplicando técnicas de pruebas de penetración o *pentesting*.

Competencias a Desarrollar

Durante el transcurso del curso el estudiante desarrollará las siguientes competencias:

Saber conocer: Las competencias "saber conocer" representan conocimientos teóricos.

- Identifica la problemática del mantenimiento de la seguridad de un sistema informático cumpliendo los requisitos de confidencialidad, integridad, no repudio, control de acceso y disponibilidad.
- Describe los conceptos de criptografía, criptoanálisis, esteganografía y estegoanálisis y sus distintas vertientes.
- Clasifica distintos tipos de amenazas a la seguridad informática, tanto activas como pasivas, y que herramientas existen para defenderse de ellas.
- Describe el funcionamiento de la Infraestructura de Clave Pública (PKI) como mecanismo de autenticación.
- Reconoce los problemas de seguridad en redes TCP/IP cableadas e inalámbricas.

Saber hacer: Las competencias "saber hacer" representan conocimientos prácticos.

- Utiliza herramientas de criptografía simétrica y asimétricas, por ejemplo `gpg`, para cifrar documentos y mensajes.
- Configura *firewalls* `iptables` y `pf` en sistemas Linux y BSD respectivamente.
- Configura redes virtuales privadas (VPN) utilizando túneles IPSec.
- Configura mecanismos de autenticación en servidores HTTP mediante certificados digitales x.509 para el servidor y el cliente.
- Aplica técnicas de pruebas de penetración con Kali Linux y Metasploit para evaluar la seguridad de programas.

Saber ser: Las competencias "saber ser" representan conocimientos actitudinales.

- Identifica la responsabilidad de los profesionales de las Ciencias de la Computación en lo referente a la seguridad de los sistemas informáticos de una organización.
- Reflexiona sobre las implicaciones éticas del uso de aplicaciones de ataque a sistemas como herramientas de prueba de software.
- Describe las diferencias entre los conceptos de *cracking*, *ethical hacking* y *white*, *grey* y *black-hat hacking*.

Contenido temático

1. *Fundamentos Básicos de la Seguridad de Redes.*
   Introducción a la Seguridad: seguridad de la información, mecanismos de seguridad, servicios de seguridad y ataques o amenazas a la seguridad. Características de la Seguridad: confidencialidad, autenticación, integridad, no repudio, control de acceso y disponibilidad. Arquitectura de Seguridad en el Modelo OSI y Modelo Básico de Seguridad en Redes.

2. *Amenazas y Ataques.*
   Ataques a la Seguridad: definición. Categorías de Ataques: interrupción, intercepción, modificación y fabricación del mensaje. Ataques Pasivos: definición, tipos, ataques basados en el contenido y análisis de tráfico. Ataques Activos: definición, tipos, impersonalización, retransmisión, modificación del mensaje, negación de servicio. Intrusos: definición, clases de intrusos. Técnicas de Intrusón. Defensa Contra la Intrusión, Técnicas de Detección de Intrusos: auditoría de registros, estadísticas, basadas en reglas, minería de datos. *Malware*: definición, taxonomía. Virus: estructura y funcionamiento de un virus, tipos de virus, software antivirus. Gusanos: definición, propagación. Contramedidas. Sistemas Confiables: concepto, control de acceso a los datos, reglas y propiedades de un sistema confiable. Seguridad multinivel. Pruebas de Penetración.

3. *Criptografía Convencional o Simétrica.*
   Criptografía: definición, historia, sistemas criptográficos, criptoanálisis. Modelos de Encriptación Convencional o Simétrico. Técnicas Clásicas de Encriptación: técnicas de sustitución, transposición y rotación. Criptoanálisis: criptoanálisis diferencial, criptoanálisis lineal. Distribución de Claves. Generación de Números Aleatorios. Casos de Estudio en Cifrado Simétrico. Esteganografía: definición, historia, estegoanálisis.

4. *Criptología de Clave Pública o Asimétrica.*
   Modelos de Criptosistemas de Cláves Públicas. Requerimientos de los Criptosistemas de Clave Públicas y Aplicaciones. Criptoanálisis en Sistemas de Claves Públicas. Distribución de las Claves Públicas. Red de Confianza. Casos de Estudio de Crifrado Asimétrico.

5. *Integridad, Autenticación y Firmas Digitales.*
   Requerimientos de la Autenticación. Funciones de la Autenticación: encriptación del mensaje, código de autenticación o verificación (MAC) y funciones *hash*. Encriptación basada en esquemas simétricos y esquemas asimétricos para la autenticación. Requerimientos del Código de Autenticación de Mensajes y Casos de Estudio. Funciones *hash*: definición, requerimientos, casos de estudio. Técnicas de Encadenamiento de Bloques. Firmas Digitales: definición, requerimientos, firma digital directa, firma digital arbitrada. Protocolos de Autenticación: autenticación mutua, autenticación en una sola dirección. Certificados Digitales e Infraestructura de Clave Pública (PKI): definición, obtención/revocación del certificado, procedimiento de autenticación con certificados digitales.

6. *Seguridad en Redes Inalámbricas y Redes TCP/IP.*
   Redes Inalámbricas: definición, 802.11x, detección del espectro de frecuencias. Seguridad en Redes 802.11x: protocolos WEP, WPA2 y RADIUS. Vulnerabilidades y Ataques en Redes 802.11x. Seguridad en Redes Bluetooth: bluejacking, bluesnarfing y Blueborne. Seguridad en IP: introducción, arquitectura de la seguridad en el protocolo IP, túneles IPSec. Seguridad en TCP: SSL/TSL, ataques al protocolo TCP. SCTP.

Bibliografía Recomendada

- Stallings, W., *"Fundamentos de Seguridad en Redes: Aplicaciones y Estándares"*. 2^a edición, Prentice-Hall, 2008.
- Mitani, M. et al., *"The Manga Guide to Criptography"*. 1^a edición, No Starch Press, 2018.
- OccupyTheWeb, *"Linux Basics for Hackers"*. 1^a edición, No Starch Press, 2018.
- Tanenbaum, A. *"Redes de Computadoras"*. 4^a edición, Pearson, 2004.
- Yurichev, D., *"Reverse Engineering for Beginners"*. Web `https://beginners.re/`, Consultado el 07-03-2019.
- Lucas, M., *"PGP & GPG"*. 1^a edición, No Starch Press, 2006.
- Rash, M., *"Linux Firewalls"*. 1^a edición, No Starch Press, 2007.
- Free Software Foundation, *"The GNU Privacy Handbook"*. Web `https://www.gnupg.org/gph/en/manual.html`, Consultado el 20-05-2019.
- OpenBSD, *"OpenBSD PF - User's Guide"*. Web `https://www.openbsd.org/faq/pf/`, Consultado el 20-05-2019.
- The netfilter.org project, *"iptables - administration tool for IPv4 packet filtering and NAT"*, Web `https://linux.die.net/man/8/iptables`, Consultado el 20-05-2019.

Evaluación

Evaluación	**Tipo**	**Porcentaje**
Teoría		
	Exposición	15 %
	Quices	10 %
	Portafolio	10 %
	Capture the Flag	15 %
Práctica		
	Laboratorios	20 %
	Proyecto 1	15 %
	Proyecto 2	15 %

Grupo Docente

Cargo	**Nombre**	**Correo-e**	**Sección**	**Horarios**	**Aulas**
Profesor (C)	Miguel Astor	miguel.astor@ciens.ucv.ve	C1	Miércoles y Viernes 1 a 3 PM	Por definir