1. Datos Generales de la asignatura

Nombre de la asignatura:	**HARDENING DE SERVIDORES (ENDURECIMIENTO DE SERVIDORES)**
Clave de la asignatura:	SDI-2203
SATCA[1]:	2 - 3 – 5
Carrera:	Ingeniería en Sistemas Computacionales.

2. Presentación

Caracterización de la asignatura
El Sistema Operativo (SO) es uno de los softwares más vulnerados. La instalación, configuración y puesta a punto de un sistema seguro, es una de las tareas más importantes en la seguridad informática. Se revisan conceptos fundamentales del endurecimiento de un SO (hardening), que requiere de actividades como; actualizaciones, implementación de un firewall, configuración segura de puertos de comunicación (servicios), garantizar el acceso seguro, protocolos seguros para compartir recursos, uso de contenedores de virtualización, métodos de generación de passwords seguros, técnicas de respaldo de datos, uso de la criptografía, perfiles de usuarios, configuración de permisos y monitoreo de logs.
Intención didáctica
El alumno conocerá las actividades más importantes para garantizar el uso de un sistema operativo seguro, se revisará la seguridad en sistemas Unix y Windows y las mejores prácticas utilizadas por estándares de la industria.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Instituto Tecnológico de Morelia, 30 de agosto de 2022.	Dr. Heberto Ferreira Medina Dr. Anastacio Antolino Hernández Dr. Juan Carlos Olivares Rojas MSC. Juan Jesús Ruiz Lagunas ISC. Rubén Lara Bárcenas	Diseño curricular basado en competencias del módulo de “Seguridad en infraestructura y servicios”.

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
El alumno conocerá las actividades más importantes para el endurecimiento en sistemas operativos, además deberá aplicarlas a sistemas Unix y Windows, realizará actualizaciones, implementación de un firewall, configuración segura de puertos de comunicación (servicios),

[1] Sistema de Asignación y Transferencia de Créditos Académicos

garantizar el acceso seguro, protocolos seguros para compartir recursos, uso de contenedores de virtualización, métodos de generación de passwords seguros, técnicas de respaldo de datos, uso de la criptografía, perfiles de usuarios, configuración de permisos y monitoreo de logs.

5. Competencias previas

- Seleccionar, clasificar y analizar información.
- Conocimientos de SO Unix y Windows
- Conocimientos de redes y servicios
- Conocimientos de la infraestructura de llave pública (PKI)
- Conocimiento de certificados digitales SSL
- Capacidad de desarrollar un proyecto para el endurecimiento de SO aplicados a necesidades de la industria

6. Temario

No.	Temas	Subtemas
1	**Introducción**	1. Definición de SO seguros 2. Arquitectura y tipos de seguridad en SO 3. Definición y concepto de vulnerabilidades 4. Estándares de hardening de servidores 5. Hardening en redes de computadoras, aplicaciones y bases de datos 6. Sistemas de virtualización, contenedores y técnicas de protección con firewalls
2	**Seguridad en Unix**	1. Arquitectura de un SO Unix seguro 2. Actualizaciones y parches del SO 3. Eliminación de archivos, bibliotecas, drivers, y funcionalidades innecesarias 4. Actividad en logs; errores y warnings 5. Limites en espacios y permisos del sistema 6. Análisis del SO MacOS X 7. Resiliencia y auditoría
3	**Seguridad en Windows Server**	1. Arquitectura de un SO Windows seguro 2. Actualizaciones y parches del SO 3. Eliminación de aplicaciones, bibliotecas y drivers innecesarios 4. Actividad en logs; errores y warnings 5. Límites de en espacios y permisos del sistema 6. Servidores de dominios (active directory) 7. Resiliencia y auditoría
4	**Seguridad en la conectividad**	1. Estándares y buenas prácticas 2. Seguridad en redes de computadoras

		3. Seguridad de dispositivos móviles e Internet de las cosas (IoT) 4. Monitoreo de procesos, tráfico de red y auditoría

7. Actividades de aprendizaje de los temas

Tema 1: Introducción	
Competencias	Actividades de aprendizaje
Específica(s): - Conocerá los conceptos de un SO seguro y objetivos de la seguridad. - Investigará los tipos de SO y los estándares de seguridad. - Definirá los elementos de un SO seguro. - Conocerá el concepto de vulnerabilidades. - Investigará el hardening en redes de computadoras, aplicaciones y bases de datos. Genéricas: - Conocerá los conceptos de seguridad aplicados a SO. - Conocerá las técnicas de protección.	1. Documentarse en todos los conceptos de seguridad informática para el hardening de SO. 2. Investigar sobre herramientas de auditoría para servidores. 3. Investigar sobre la virtualización y el uso de contenedores en SO para la resiliencia.
Tema 2: Seguridad en Unix	
Competencias	Actividades de aprendizaje
Específica(s): - Conocerá la arquitectura de un SO Unix seguro. - Conocerá los sistemas de protección y autorización en Unix. - Realizará la eliminación de archivos, bibliotecas, drivers, y funcionalidades innecesarias. - Revisará las posibles vulnerabilidades y amenazas de un SO Unix. - Implementará límites de espacios y permisos en el sistema. Genéricas: - Implementará el endurecimiento de SO Unix. - Conocerá los métodos para resiliencia y auditoría de un SO Unix.	1. Implementar el endurecimiento en un SO Unix. 2. Establecer los pasos para el análisis de la seguridad en sistemas Unix. 3. Verificará las posibles vulnerabilidades y amenazas de un SO Unix.
Tema 3: Seguridad en Windows Server	
Competencias	Actividades de aprendizaje

Específica(s): - Conocerá la arquitectura de un SO Windows Server seguro. - Conocerá los sistemas de protección y autorización en Windows Server. - Realizará las actualizaciones, parches, eliminación de aplicaciones, bibliotecas y drivers innecesarios. - Conocerá y auditará los logs del SO; errores y warnings. - Implementará límites de espacios y permisos en el sistema. - Implementará un servidor de dominio (active directory). Genéricas: - Implementará el endurecimiento de SO Windows Server. - Conocerá los métodos de auditoría para Windows Server.	1. Implementar el endurecimiento en sistemas Windows Sever. 2. Establecer los pasos para el análisis de la seguridad en sistemas Windows. 3. Verificará las posibles vulnerabilidades y amenazas en Windows Server.
Tema 4: Seguridad en la conectividad	
Competencias	Actividades de aprendizaje
Específica(s): - Conocerá estándares y buenas prácticas para la seguridad en redes de computadoras. - Conocerá las buenas prácticas de seguridad de dispositivos móviles e internet de las cosas (IoT). Genéricas: - Aplicará el monitoreo de procesos y tráfico de red para la auditoría.	1. Implementar protocolos de comunicación seguros en SO. 2. Realizar el análisis de la seguridad en protocolos de comunicación. 3. Verificará las posibles vulnerabilidades y amenazas en Windows Server.

8. Práctica(s)

- Investigar sobre estándares de hardening en servidores Unix y Windows
- Revisar métodos de detección de vulnerabilidades y amenazas Linux y Windows
- Aplicar actualizaciones y parches para un SO seguro Linux
- Implementar métodos de protección y autorización en Linux
- Realizar un monitoreo y análisis de la seguridad en Linux, auditoría.
- Actualizaciones y parches para un Windows seguro
- Métodos de protección y autorización en Windows
- Monitoreo y análisis de la seguridad servidores Windows
- Implementar un Active Directory y un dominio en Windows Server
- Revisar el estado del endurecimiento en Windows Server, auditoría

9. Proyecto de asignatura

- Llevar a cabo el endurecimiento en Sistemas Operativos Linux y Windows Server.

- Realizará un proyecto del análisis y detección de vulnerabilidades en servidores implementados en la industria
- Implementará esquemas de seguridad que permitan disminuir las amanezcas y vulnerabilidades detectadas en SO

10. Evaluación por competencias

- Elaboración de prácticas y su evaluación.
- Elaborar un proyecto de endurecimiento de un servidor.
- Realizar un análisis de vulnerabilidades y amenazas.
- Aplicar esquemas de seguridad en SO para disminuir las amenazas.

11. Fuentes de información

[1] EC-COUNCIL. “Network Defense Essentials”, EC-COUNCIL OFFICIAL CURRICULA. 2022. https://www.eccouncil.org/official/ (accedido agosto 2022).

[2] Nemeth Evi, Snyder Garth. Unix and Linux system administration. Kindle Edition, 2017.

[3] Tevault Donald. Mastering Linux Security and Hardening: Secure your Linux server and protect it from intruders, malware attacks, and other external threats. Kindle Edition, 2018.

[4] Sivarajan Santhosh. Getting Started with Windows Server Security. Kindle Edition, 2015.

[5] Miroshnikov Andrei. Windows Security Monitoring: Scenarios and Patterns. Ed. Wiley. 2018.

[6] Krause Jordan. Windows Server 2016 Security, Certificates, and Remote Access Cookbook: Recipe-based guide for security, networking and PKI in Windows Server 2016. Kindle Edition, 2018.

[7]. CIS, Center for Internet Security, Estándares y métodos de seguridad en SO. 2022. https://www.cisecurity.org/ (accedido agosto 2022).

[8]. NIST, National Institute of Standards and Technology, NIST SP 800-123, Guide to General Server Security. 2022. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-123.pdf (accedido agosto 2022).

[9]. SANS, SysAdmin Audit, Networking and Security Institute. Políticas de seguridad para servidores. 2022. https://www.sans.org/information-security-policy/ (accedido agosto 2022).