Módulo: Seguridad Informática

2021 – 1

Docente: Ricardo Pérez – Rodrigo Paredes
Horas de Consultas: Lunes 15:30-17:30

Calendario de Evaluaciones Principales

Evaluación	**Fecha**
Proyecto Unidad 1	**24 Mayo**
Proyecto Unidad 2	**5 de Julio**
Prueba Final	**12 de Julio**
Prueba Recuperativa	**14 de Julio**

Plan de clases

Semana - Fecha	Actividad	/Saber/Tema
1 – 15 Marzo	***Cátedra: Comparar y contrastar los diferentes tipos de amenazas, ataques y vulnerabilidades de un sistema computacional. (2 horas)***	*Conceptos de Amenazas Vulnerabilidades, Riesgos y Ataques en un Sistema Computacional.*
1 – 15 Marzo	***Laboratorio: Introducción a Kali-Linux. Búsqueda y obtención de información. (1 hora)***	*Búsqueda y obtención de Información pasiva, footprinting.* *Utilizar herramientas como IP, MAC y Whois para la obtención de Información.* *Whatweb escaneo silencioso* *Google Hacking.* *Email harvesting y hunter.io* *Encontrando nombres de usuario con Sherlock.* *Shodan.* *DNS zone transfer with dig.*
2 – 22 Marzo	***Cátedra: Principios básicos para el manejo de riesgos y sus estrategias de mitigación. (2 horas)***	*Mitigación de riesgos.*
2 – 22 Marzo	***Laboratorio: Análisis de riesgo de acuerdo con la situación de seguridad. (1 hora)***	*Segunda parte del Laboratorio 1 (Búsqueda y obtención de información).* *Wireshark*
3 – 29 Marzo Suspensión de Actividades miércoles, Jueves, Viernes receso	***Cátedra: Conceptos fundamentales sobre el Hacking Ético. Escaneo de vulnerabilidades (2 horas)***	*Estrategias de escaneo utilizadas por los atacantes.* *Mecanismos de defensa.*
3 – 29 Marzo Suspensión de Actividades miércoles, Jueves, Viernes receso	***Laboratorio: Búsqueda de vulnerabilidades (scanning) y pruebas de penetración. Búsqueda de información y footprinting activo y pasivo. (1 hora)***	*Instalando metasploitable* *Nmap* *Zenmap* *Escaneo TCP* *Bypassing the firewall with nmap* *Usando los scripts de nmap*
4 – 5 Abril	***Cátedra: Tecnologías y herramientas disponibles para mejorar la seguridad. (2 horas)***	*Firewall, ACL, Denegación Implícita, Administración basada en reglas, ACL en routers y switches, proxys, APs.* *Analizadores de protocolos, Scanners de redes, passwords crackers, analizadores de vulnerabilidades, frameworks de explotación, herramientas de sanitización, herramientas de generación de salvas, herramientas desde la terminal, HIDS/HIPS, antivirus*

4 – 5 Abril	***Laboratorio: Desarrollo e instalación de herramientas para disminuir los riesgos. (1 hora)***	*Firewall, ACL, Denegación Implícita, Administración basada en reglas, ACL en routers y switches, proxys, APs.* *Analizadores de protocolos, Scanners de redes, passwords crackers, analizadores de vulnerabilidades, frameworks de explotación, herramientas de sanitización, herramientas de generación de salvas, herramientas desde la terminal, HIDS/HIPS, antivirus*
5 – 12 Abril	***Cátedra: Seguridad en aplicaciones Webs. (2 horas)***	*Seguridad en Aplicaciones Webs.*
5 – 12 Abril	***Laboratorio: Introducción a la seguridad en aplicaciones Webs. (1 hora)***	*Pruebas de penetración de aplicaciones web* *Solicitudes y respuestas HTTP* *Fundamentos de burpsuite* *Ataques de fuerza bruta*
6 – 19 Abril	***Cátedra: Seguridad en aplicaciones Webs. (2 horas)***	*Inyección de comandos* *Inyección SQL* *Secuencias de comandos entre sitios cruzados (XSS)*
6 – 19 Abril	***Laboratorio: Seguridad en aplicaciones Webs (Inyecciones de código y SQL, XSS). (1 hora)***	*Inyección de comandos* *Inyección SQL* *Secuencias de comandos entre sitios cruzados (XSS)*
7 – 26 Abril	***Cátedra: Procedimiento seguido por el atacante para la explotación de vulnerabilidades y la obtención de accesos. (2 horas)***	*¿Qué es la explotación?* *Reverse shells y Bind shells* *Metasploit* *Comandos básicos de Msfconsole* *Nuestro primer exploit: vsftp 2.3.4 Explotación* *Divulgación de información - Exploit Telnet* *Credenciales predeterminadas del enrutador*
	Laboratorio: Pentesting en entornos Windows (1 hora)	*Consola de Metasploit y sus módulos* *Ataque de fuerza bruta con Metasploit* *Explotación de Apache Tomcat con Metasploit* *Obtener sesión de meterpreter con inyección de comandos* *Inyección de código PHP* *Explotando Metasploitable2* *Instalación de wine* *Hexeditor, encoders y antivirus* *Hacking with Ngrok* *Creando payloads para Android con Msfvenom*
8 – 3 Mayo	***Cátedra: Procedimiento seguido por el atacante para la explotación de vulnerabilidades y la obtención de accesos. (2 horas)***	*Exploit de Windows* *Routersploit* *Generando carga útil de Powershell usando Veil* *Creación de carga útil de TheFatRat* *Hexeditor y antivirus* *Hacer que nuestra carga útil abra una imagen*
	Laboratorio: Herramientas de explotación en Windows y Linux. Explotación en el directorio de archivos compartidos de Samba. (1 hora)	*Eternal Blue Attack - Explotación de Windows 7* *DoublePulsar Attack - Exploit de Windows* *Vulnerabilidad de BlueKeep -* *Configuración de Windows 10 vulnerable* *Bloquear la máquina con Windows 10 de forma remota* *Escalando privilegios en Windows10* *Previniendo la escalada de privilegios en Windows10* *Exploit de Windows* *Routersploit* *Generando carga útil de Powershell usando Veil* *Creación de carga útil de TheFatRat*

		Hacer que nuestra carga útil abra una imagen *Explotación remota de la máquina con Windows 10* *Generación de carga útil básica con Msfvenom* *Uso avanzado de Msfvenom* *Vulnerabilidad del software: explotación de Samba*
9 – 10 Mayo	***Cátedra: Post explotación y escalado de privilegios. (2 horas)***	*Teoría posterior a la explotación*
9 – 10 Mayo	***Laboratorio: Post explotación y escalado de privilegios. (1 hora)***	*Comandos básicos en Meterpreter* *Elevación de privilegios con diferentes módulos* *Creando persistencia en el sistema de destino* *Módulos posteriores a la explotación* *Proyecto de codificación Python: puerta trasera*
10 – 17 Mayo Viernes Receso	***Cátedra: Pruebas de penetración inalámbrica. (2 horas)***	*Prueba de penetración inalámbrica* *Capturar handshakes con Airodump-ng* *Descifrando contraseñas con Aircrack-ng* *Generando listas de palabras con crunch* *Rainbowtables*
11 – 24 Mayo	***Defensa Proyecto Unidad 1***	
12 – 31 Mayo	***Cátedra: Python como herramienta principal de hacking ético. (2 horas)***	*Aplicar algoritmos simples para la explotación de información redundante con el objeto de corregir datos. [SF-9.4:U]* *Articular la distinción entre detectar, manejar y recuperar fallos, y los métodos para sus implementaciones. [SF-9.2:C]* *Resumir los principios de a prueba de fallos y denegación por default. [IAS-2.2:C]* *Describir ara cada etapa en el ciclo de vida de un producto qué consideraciones de seguridad deben ser evaluadas (IAS-2.6: C)*
13 – 7 Junio	***Laboratorio: Aplicaciones de Python para hacking ético. (1 hora)***	*Identificar y analizar algunos de los riesgos para un sistema completo, que surgen producto de aspectos distintos al software. [SE-2.25:U]* *Manejar errores desde Python* *Implementando Backdoors y Keylogger con Python*
14 – 14 Junio	***Cátedra: Ingeniería social y Ataque MITM. (2 horas)***	*Conceptos fundamentales de los Ataques de Ingeniería Social y los ataques MITM.*
14 – 14 Junio	***Laboratorio: Ataque MITM. (1 hora)***	*Instalar MITMf* *ARP y DNS Spoofing* *Ataques MITM utilizando Ettercap*
15 – 21 Junio	***Cátedra: Criptografía e infraestructura de llave pública. (2 horas)***	*Describir los aspectos de seguridad que surgen en las fronteras entre múltiples componentes. [IAS-2.12:C]* *Discutir la importancia de los números primos en criptografía y explica su uso en los algoritmos criptográficos. [IAS-6.3:C]*
15 – 21 Junio	***Laboratorio: Principios básicos del cifrado. (1 hora)***	*Describir los aspectos de seguridad que surgen en las fronteras entre múltiples componentes. [IAS-2.12:C]* *Discutir la importancia de los números primos en criptografía y explica su uso en los algoritmos criptográficos. [IAS-6.3:C]*
16 – 28 Junio	***Cátedra: Criptografía e infraestructura de llave pública. (2 horas)***	*Explicar cómo la infraestructura de clave publica soporta el firmado digital y la encriptación y discute sus limitaciones/ vulnerabilidades. [IAS-6.4:C]* *Describir el rol de los códigos correctores de errores para proveer chequeo de errores y*

		técnicas de correlación en memorias, almacenamiento y redes. [SF-9.3:C]
16 – 28 Junio	***Laboratorio: Algoritmo RSA. (1 hora)***	*Implementando el cifrado a través del algoritmo RSA.*
17 – 5 Julio	***Defensa Proyecto Unidad 2***	
18 – 12 Julio	***Prueba Final / Recuperativa***	