MAESTRIA EN INGENIERIA ELECTRONICA Y TELECOMUNICACIONES

SÍLABO

I. DATOS GENERALES

1	Asignatura	Instrumentación de Sistemas Electrónicos
2	Código	PET 204
3	Semestre	2024-II
4	Ciclo	I
5	Carácter	Obligatorio
6	Área	Ciberseguridad
7	Créditos	4
8	Pre requisito	No aplica
9	Duración	16 semanas
10	Horas Totales	64 horas
11	Docente(s)	M.Sc. Oscar Llerena

II. SUMILLA

Este curso ofrece una formación integral en ciberseguridad, abarcando desde los conceptos fundamentales hasta las técnicas avanzadas utilizadas en la industria. Los estudiantes explorarán una amplia gama de temas, incluyendo la identificación y mitigación de amenazas cibernéticas, la seguridad de redes, y la criptografía. Además, se cubrirán áreas clave como la protección de sistemas operativos, la seguridad en entornos de nube y la gestión de identidades y accesos.

El curso también se enfoca en desarrollar habilidades prácticas en pruebas de penetración y hacking ético, proporcionando herramientas y técnicas para realizar evaluaciones de seguridad exhaustivas. Se incluirá un análisis detallado de malware, donde los estudiantes aprenderán a identificar y neutralizar amenazas. Asimismo, se estudiarán las vulnerabilidades en aplicaciones web, aplicando metodologías para garantizar su seguridad.Esta formación integral preparará a los alumnos para afrontar los desafíos actuales y futuros en el campo de la ciberseguridad, equipándolos con las competencias necesarias para proteger y defender infraestructuras críticas.

III. OBJETIVOS

- Comprender los fundamentos de la ciberseguridad
- Estudiar amenazas cibernéticas y vectores de ataque
- Adquirir conocimientos en seguridad de redes, criptografía, seguridad en sistemas operativos, seguridad en la nube, gestión de identidades y accesos (IAM) y Seguridad tipo Endpoint, etc.
- Desarrollar habilidades en Pentesting y Ethical Hacking y análisis de malware
- Evaluar vulnerabilidades en aplicaciones web

IV. COMPETENCIA Y CAPACIDADES DE LA ASIGNATURA

COMPETENCIA	CAPACIDADES
Evaluar amenazas y vulnerabilidades en sistemas informáticos y redes, implementando medidas de protección adecuadas mediante técnicas avanzadas de ciberseguridad. Diseñar e implementar soluciones de seguridad en redes, criptografía y gestión de identidades y accesos. Aplicar técnicas de pentesting y hacking ético, realizar análisis de malware y vulnerabilidades en aplicaciones web, y gestionar operaciones en un Centro de Operaciones de Seguridad (SOC) para responder eficazmente a incidentes y amenazas en tiempo real, con un enfoque en tecnologías emergentes.	*Desarrollar la habilidad para comprender y analizar los principios fundamentales de la ciberseguridad, así como la evolución de amenazas y vectores de ataque, y la implementación de medidas de protección en redes.*
	Adquirir competencias avanzadas en la aplicación de técnicas criptográficas, la protección de aplicaciones web y puntos finales, y el uso de herramientas para garantizar la integridad y seguridad de los sistemas.
	Desarrollar la capacidad para gestionar operaciones de seguridad y respuesta a incidentes, incluyendo la implementación de un ciclo de vida de respuesta, el uso de inteligencia de amenazas, y la configuración segura de sistemas operativos.
	Adquirir habilidades para evaluar y proteger tecnologías emergentes, gestionar identidades y accesos, y aplicar conocimientos avanzados en proyectos de ciberseguridad, incluyendo la seguridad en entornos de nube y redes inalámbricas.

V. PROGRAMACIÓN DE CONTENIDOS EN UNIDADES DE APRENDIZAJE

Unidad	Temas a abordar
U1.-Introducción al curso	Historia de la Ciberseguridad. Instalación del setup de Laboratorio y el Web Server Jekyll – Chirpy para documentación de trabajos. Etapas del Kill Chain (MITRE ATT&CK)
U2.-Pentesting	Pentesting en un Entorno Controlado usando Kali Linux y Metasploitable 3 Buffer Overflows
U3.- Endpoint security	Elasticsearch Framework

	Caldera & Atomic Red Frameworks
U4.-Tecnologías Emergentes y Aplicaciones Avanzadas en Ciberseguridad	ML-based Cybersecurity Trabajo de investigación

Capacidad U1:			
Conocer los más importantes eventos y repercusiones en la historia de la Ciberseguridad. Implemetación de los setup de laboratorio y documentación de pruebas.			
Sem	Contenido conceptual	Contenido procedimental	Contenido actitudinal
1	Historia de la Ciberseguridad	Recuento histórico de los eventos más importantes en la ciberseguridad	Investigar los eventos más relevantes en la historia de la ciberseguridad (primer ataques, Kevin Mitnick, Cyberwarfare: Stuxnet, etc.)
2	Setup de Laboratorio	Implementación del entorno de laboratorio para pruebas de pentesting. Instalación de la máquina virtual Kali Linux Instalación de la máquina virtual Metasploitable.	Proficiencia en el uso de herramientas para la implementación de un entorno basado en máquinas virtuales atacante y target. Proficiencia en el uso de Windows y Linux. Proficiencia en el uso de powershell (Windows) y bash command terminal (Linux).
3	Implementación del framework para documentación de laboratorios.	Creación de cuenta en Github. Instalación del framework Jekyll. Instalación local del Visual Studio Code con el Theme Chirpy. Implementación del blog personal con Github Actions.	Proficiencia en el uso de herramientas para la implementación de una página web para la documentación de los trabajos de laboratorio.
4	Etapas del Kill Chain	Reconocimiento. Explotación de vulnerabilidad.	Proficiencia en el uso de la secuencia de pasos para realizar un pentesting a un

		Elevación de privilegios. Ganar acceso al sistema target. Exfiltración de data.	sistema o red.
EVIDENCIA DE LA CAPACIDAD 1: Cuestionario de preguntas sobre la historia de la ciberseguridad. Verificación del setup de laboratorio y página online propia de cada alumno para documentación de pruebas.			

Capacidad U2 :			
Adquirir competencias avanzadas en la aplicación de técnicas de pentesting y comprensión de uno de los vectores de ataque más utilizados en Ethical Hacking (Buffer Overflows).			
Sem.	Contenido conceptual	Contenido procedimental	Contenido actitudinal
1	Pentesting en un Entorno Controlado usando Kali Linux y Metasploitable 3 (Parte 1)	Reconocimiento y escaneo de red. Enumeración de servicios y puertos funcionales en el sistema target. Selección de vulnerabilidad a ser explotada en el sistema target.	Proficiencia en el uso de nmap y scripts de descubrimiento de vulnerabilidades. Entendimiento de la vulnerabilidad y su contexto.
2	Pentesting en un Entorno Controlado usando Kali Linux y Metasploitable 3 (Parte 2)	Explotación de vulnerabilidad usando el framework Metasploit. Exfiltración de data del sistema target. Crackeo de passwords del sistema target.	Proficiencia en el uso de módulos de Metasploit para explotación de vulnerabilidades y obtención de acceso al sistema target. Proficiencia en copia de volúmenes de almacenamiento del sistema target. Proficiencia en la extracción de data del sistema target. Proficiencia en el uso de diccionarios y herramientas de crackeo de contraseñas.
3	Buffer Overflows	Entendimiento de la memoria asignada a la ejecución de un	Proficiencia en el entendimiento de los

	(Parte 1)	programa o aplicación. Entendimiento de los registros del segmento de memoria Stack. Instalación y uso de herramientas VulServer e Immunity Debugger	registros clave para la manipulación de Buffer Overflows.
4	Buffer Overflows (Parte 2)	Entendimiento del procedimiento general para encontrar buffer overflows: - Spiking - Fuzzing - EIP overwriting - Explotación vía shellcode	Proficiencia en el uso de scripts y herramientas para encontrar direcciones de registro de memoria vulnerables a Buffer Overflows. Proficiencia en la creación de scripts con shellcode malicioso para obtener acceso remoto al sistema target mediante la explotación de Buffer Overflow.
EVIDENCIA DE LA CAPACIDAD 2: Reporte de laboratorio de Pentesting. Reporte de laboratorio de Buffer Overflows.			

Capacidad U3 :			
Desarrollar la capacidad para gestionar operaciones de seguridad y respuesta a incidentes, incluyendo la implementación de un ciclo de vida de respuesta, el uso de inteligencia de amenazas, y la configuración segura de sistemas operativos.			
Sem.	Contenido conceptual	Contenido procedimental	Contenido actitudinal
1	Framework Elasticsearch para recolección de data de sistemas (Parte 1)	Entendiemiento de herramientas SIEM. Implementación y configuración del framework Elasticsearch.	Proficiencia en el entendiemiento de las soluciones SIEM. Proficiencia en la instalación de un servidor Elasticsearch.
2	Framework Elasticsearch para recolección de data de sistemas (Parte 2)	Recolección y análsisi de eventos de sistema y red. Análisis de eventos maliciosos.	Proficiencia en la recolección de eventos a nivel de métricas de performance, cambios en archivos de sistema, flujos de paquetes

			de red, logs de autenticación.
3	Framework Caldera & Atomic Red Team (Parte 1)	Ejecución de acciones maliciosas usando las etapas del Kill Chain.	Proficiencia en el uso del Framework Caldera & Atomic Red Team.
4	Framework Caldera & Atomic Red Team (Parte 2)	Análisis en Elasticsearch de eventos maliciosos generados en Caldera & Atomic Red Team.	Proficiencia en el tracking de eventos maliciosos.
EVIDENCIA DE LA CAPACIDAD 3: Reporte de laboratorio de generación y análisis de eventos en Elasticsearch. Reporte de de laboratorio de ataques y análsis de eventos maliciosos.			

Capacidad U4 :			
Adquirir habilidades para evaluar y proteger tecnologías emergentes, gestionar identidades y accesos, y aplicar conocimientos avanzados en proyectos de ciberseguridad, incluyendo la seguridad en entornos de nube y redes inalámbricas.			
Sem.	Contenido conceptual	Contenido procedimental	Contenido actitudinal
1	ML-based Cybersecurity (Parte 1)	Comprensión del uso de técnicas de Machine Learning para detección de Intrusiones. Revisión de papers académicos que muestran el uso típico de ML en aplicaciones de Ciberseguridad.	Proficiencia en el uso de determinadas técnicas de ML con datasets relacionados a aplicaciones de ciberseguridad.
2	ML-based Cybersecurity (Parte 2)	Implementación de laboratorio de uso de ML con datasets de aplicaciones de ciberseguridad.	Proficiencia en el uso de determinadas técnicas de ML con datasets relacionados a aplicaciones de ciberseguridad.
3	Trabajo de investigación (Parte 1)	Investigación y exposición de temas relevantes y actuales en ciberseguridad.	Mostrar habilidades de investigación, lectura y comprensión de artículos académicos relacionados al uso de tecnologías emergentos en ciberseguridad.
4	Trabajo de investigación (Parte 2)	Investigación y exposición de temas relevantes y actuales en ciberseguridad.	Mostrar habilidades de investigación, lectura y comprensión de artículos

			académicos relacionados al uso de tecnologías emergentes en ciberseguridad.
EVIDENCIA DE LA CAPACIDAD 4: Reporte de laboratorio de uso de técnicas de Machine Learning en Ciberseguridad. Exposición de trabajos de investigación.			

VI. METODOLOGÍA DEL PROCESO DE ENSEÑANZA-APRENDIZAJE

1. Presentaciones Orales (Lectures)

Sem.	Temas	Evaluación
1	Historia de la Ciberseguridad	T01
2	Instalación del setup de Laboratorio y el Web Server Jekyll – Chirpy para documentación de trabajos.	
3	Etapas del Kill Chain (MITRE ATT&CK)	
4	Pentesting en un Entorno Controlado (Parte 1)	
5	Pentesting en un Entorno Controlado (Parte 2)	T02
6	Buffer Overflows (Parte 1)	
7	Buffer Overflows (Parte 2)	T03
8	-	EP
9	Framework Elasticsearch para recolección de data (Parte 1)	
10	Framework Elasticsearch para recolección de data (Parte 2)	T04
11	Framework Caldera & Atomic Red Team (Parte 1)	
12	Framework Caldera & Atomic Red Team (Parte 2) - PC 02	T05
13	ML-based Cybersecurity (Parte 1)	
14	ML-based Cybersecurity (Parte 2)	T06
15	Trabajo de investigación	EXP
16	-	EF

2. Proyectos integradores

1.- Implementación de un minilaboratorio en base a máquinas virtuales.

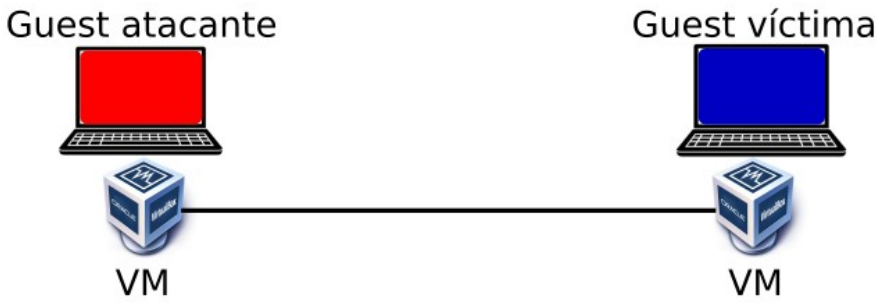

Figura 1. Laboratorio virtual que comprende 02 máquinas virtuales.

2.- Análisis en explotación en sistemas vulnerables.

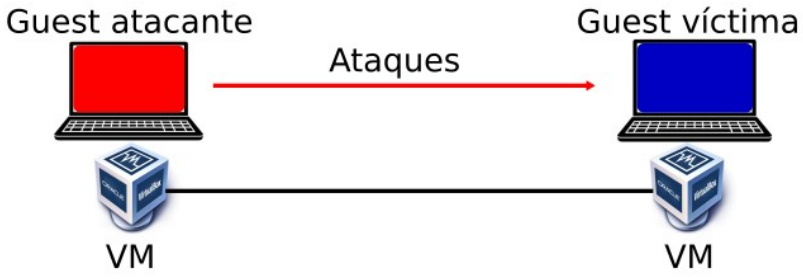

Figura 2. Circuito de instrumentación de electroculografía

3.- Implementación de procedimientos de pentesting.

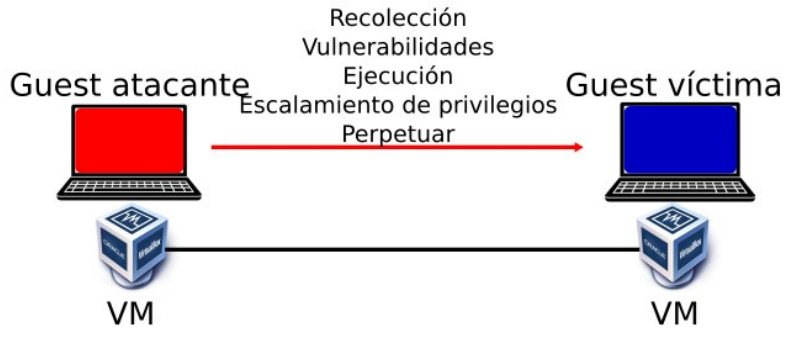

Figura 2. Pasos genéricos de un procedimiento de pentesting

4.- Implementación de una solución SIEM.

Figura 2. Implementación de ElasticSearch SIEM como solución de ciberseguridad.

VII. SISTEMA DE EVALUACIÓN

EVALUACIÓN	CÓD	DETALLE	PESO
Evaluación continua	EC	Promedio de tareas (reportes de laboratorio)	20%
Trabajo de exposición	EXP	Trabajo de investigación y presentación	30%
Evaluación Parcial	EP	Examen Parcial	20%
Evaluación Final	EF	Examen final	40%

Promedio final

$$\textbf{PF} = \frac{(20)EP + (30)EF + 20(EC) + 30(EXP)}{100}$$

EC= (T01 + T02 + T03 + T04 + T05 + T06)/6

VIII. FUENTES DE INFORMACIÓN

IX. LABORATORIOS

Para el desarrollo de las horas de práctica que figuran en los sílabos, la escuela cuenta con los siguientes laboratorios donde los alumnos realizan actividades experimentales y demostrativas, que complementan las horas de teoría y consolidan la adquisición de capacidades y competencias.

Los laboratorios con los que cuenta la escuela de posgrado para la maestría son:

1. Laboratorio de Telecomunicaciones
2. Laboratorio de Control Y Automatización
3. Laboratorio de Investigación Multifuncional I - Área de Prototipado en General
4. Laboratorio de Investigación Multifuncional II - Área de Prototipado Electrónico
5. Laboratorio de Investigación Multifuncional III - Área de Electrofisiología Cognitiva

6. Laboratorio del grupo de Circuitos y Sistemas Electrónicos de Alta Frecuencia
7. Laboratorio de Electrónica Analógica Y Digital

X. RECURSOS NECESARIOS

XI. BIBLIOGRAFIA

[1]. MITRE Corporation, "MITRE ATT&CK Framework," en línea. Disponible: https://attack.mitre.org/. [Accedido: 3 de agosto de 2024].
[2]. D. Stuttard y M. Pinto, The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2ª ed. Indianapolis, IN: Wiley, 2011.
[3]. W. Stallings, Cryptografía y Seguridad de Redes: Principios y Práctica, 7ª ed. Upper Saddle River, NJ: Pearson, 2016.
[4]. A. Pease, Threat Intelligence Handbook: A Practical Guide for Security Teams, 2ª ed. San Francisco, CA: CyberEdge Group, 2020.
[5]. OWASP Foundation, "OWASP Top 10: The Ten Most Critical Web Application Security Risks," en línea. Disponible: https://owasp.org/www-project-top-ten/. [Accedido: 3 de agosto de 2024].
[6]. W. Stallings, Seguridad de Redes: Fundamentos y Aplicaciones, 6ª ed. Upper Saddle River, NJ: Pearson, 2016.

Oscar Enrique Llerena Castro
Docente