UNIVERSIDAD DEL NORTE | EDUCACIÓN CONTINUADA

Vigilada Mineducación

Diplomado en Ciberseguridad

JUSTIFICACIÓN

Con el paso de los años, hemos sido testigos de miles de vulnerabilidades e incidentes espectaculares en lo que respecta a la seguridad de los sistemas de cómputos, tales como robos y fugas de información. Estos incidentes muestran que nuestra sociedad depende de sistemas computacionales seguros y confiables. Por tanto, es muy importante formar a los interesados en temas relacionados con la ciberseguridad, en particular, las existentes soluciones y retos para asegurar los datos en los sistemas computacionales.

RESULTADOS DE APRENDIZAJE

- Proponer, definir y establecer políticas para garantizar confidencialidad,
- integridad y disponibilidad de recursos informáticos en la organización.
- Proponer y definir mecanismos y herramientas para implementar políticas de seguridad en la organización
- Identificar, evaluar y proponer controles para los riesgos asociados a un sistema de información
- Realizar análisis de vulnerabilidades y pruebas de penetración a sistemas de información de una organización.
- Diseñar y evaluar sistemas informáticos teniendo en cuenta objetivos de seguridad bien definidos.

METODOLOGÍA

El enfoque será netamente teórico-práctico. Se privilegiará las estrategias de aprendizaje activo y las estrategias usadas estarán enmarcadas en la metodología del aprendizaje en línea (Aprendizaje Colaborativo, Aprendizaje basado en retos y en casos). Ahora bien, desde la interacción entre alumnos y docente se fortalecerá la colaboración, modelado y apropiación de las TIC, donde es importante el acompañamiento no solo sincrónico, sino también garantizando estrategias para la autorregulación del trabajo asincrónico, logrando consigo el andamiaje de consejos, conceptos, estrategias y aplicabilidad de las prácticas eficaces de Ciberseguridad.

Cabe mencionar que, desde esta perspectiva, el estudiante tendrá un rol que cumplir: Antes, durante y después de la sesión sincrónica.

CONTENIDO

MÓDULO 1 INGENIERÍA DE SEGURIDAD

1. Conceptos y definiciones relativos

a. Conciencia de inseguridad
b.Ciberamenazas, Ciber conflictos, Cibercrimen, Ciberterrorismo y Ciberguerra
c. Procesos de ingeniería que utilizan principios de diseño seguro
d. Conceptos fundamentales de los modelos de seguridad
e. Modelos de evaluación de seguridad

2. Amenazas y Vulnerabilidades

a. Definiciones
b. Tipos de programas maligno y otras amenazas cibernéticas
c. Vulnerabilidades de los sistemas basados en la web
d. Vulnerabilidades de los sistemas móviles
e. Amenazas emergentes

3. Criptografía

a. Criptografía simétrica
i. Cifrado simétrico por bloques (e.g. AES)
ii. Cifrado Simétrico de flujo (e.g. Salsa y Chacha)
b. Criptografía asimétrica
i. Criptosistemas basados en factorización.
ii. Criptosistemas basados en el logaritmo discreto.
c. Técnicas para proteger la integridad de los datos
i. Funciones hash criptográficas,
ii. Códigos de autenticación de mensajes.
iii. Firmas Digitales.
d. Técnicas para proveer cifrado autenticado.
e. Protocolos de intercambio de llaves autenticado.

4. Seguridad física

a. Dispositivos integrados y vulnerabilidades de los sistemas ciber físicos
b. Ataques del canal lateral
c. Dispositivos resistentes a manipulación

MÓDULO 2. SEGURIDAD EN LAS REDES Y COMUNICACIONES

1. Ataques en redes de comunicaciones

a. Ataques en protocolos de capa aplicación
i. DNS Spoofing, DNS Poisoning, DNS tunneling
ii. Active Directory Exploitation
iii. Ataques a Remote Desktop Protocol (RDP)
b. Ataques en protocolos de capa sesión
i. Ejemplos de ataques contra el protocolo TLS
ii. Secuestro SSH (SSH Hijacking)
c. Ataques en protocolos de capa transporte
i. Ataque de inundación Syn
ii. Secuestro TCP (TCP Hijacking)
iii. Ataques de inundación UDP
d. Ataques en protocolos de red
i. Falsificación de IPs (IP Spoofing)
ii. Ataques de fragmentación de IP (IP fragmentation attacks)
e. Ataques en redes LAN alámbricas e inalámbricas:
i. DHCP Rogue, DHCP Starvation attacks, ARP spoofing, Mac
Flooding.
ii. Password cracking WPA/WPA2

2. Protocolos de comunicación seguros

a. IPsec,SSH,VPNs,SSL/TLS,Tor
b. Autoridades certificadoras e infraestructura de llave pública.

3. Componentes de red seguros

a. Proxies
b. Firewalls: Primera, segunda y tercera generación
c. Intrusion Detection Systems (IDS) e Intrusion Prevention Systems
(IPS)
d. Host-Based IPS
e. Honeypots
f. Firewall UTM.
g. Next-Generation Firewalls.

4. Diseño de arquitectura de red segura

a. Segmentación de redes.
b. Redes privadas
c. Topologías seguras de red
d. Modelo de confianza-zero usando seguridad perimetral basada en software
e. Seguridad en sistemas windows y linux

5. Seguridad en ambientes nube

a. Fundamentos de computación en la nube
b. Seguridad en Amazon Cloud
c. Seguridad en Microsoft Azure
d. Seguridad en Google Cloud
e. Recomendaciones y buenas prácticas para asegurar ambientes nube.

MÓDULO 3. SEGURIDAD EN EL DESARROLLO DE SOFTWARE

1. Seguridad de software bajo nivel

a. Vulnerabilidades bajo nivel
i. Organización de la memoria
ii. Inyección de código
iii. Vulnerabilidades de formatos de cadenas
b. Defensas contra vulnerabilidades de bajo nivel
i. Aseguramiento de la memoria
ii. Seguridad de tipo
c. Otras técnicas de ataques
i. Programación orientada a retornos (ROP)

2. Seguridad de aplicaciones web

a. Análisis de las 10 vulnerabilidades más populares según OWASP.
i. Controles accesos rotos (Broken Access Control).
ii. Fallos criptográficos (Cryptographic Failures).
iii. Inyección (Injection)
iv. Diseño inseguro (Insecure Design).
v. Configuración inadecuada de la seguridad (Security Misconfiguration).
vi. Componentes desactualizados y vulnerables (Vulnerable and Outdated Components).
vii. Fallos en el proceso de identificación y autenticación (Identification and Authentication Failures).

ix. Fallos de monitoreo y en el registro de eventos (Security
Logging and Monitoring Failures).
x. Peticiones falsas del lado del servidor (Server-Side Request
Forgery)

3. Ciclo de vida de vulnerabilidades

a. Identificación de vulnerabilidades
i. Investigación de vulnerabilidades
ii. Revelación de vulnerabilidades
iii. Mercado de vulnerabilidades
b. Bases de datos y sistemas de puntajes de vulnerabilidades
c. Evaluación de vulnerabilidades
i. Tipos de vulnerabilidades
ii. Clasificación de vulnerabilidades
d. Evaluación de Riesgos
e. Remediación de vulnerabilidades
f. Verificación de remediaciones
g. Monitoreo de vulnerabilidades

4. Desarrollo Seguro de Software

a. Modelamiento de amenazas
b. Requerimientos de seguridad
c. Metodologías para diseño de software Seguro
d. Principios para el desarrollo seguro de software.
i. Favorecer simplicidad
ii. Confiar con renuencia
iii. Defensa en profundidad, monitoreo y rastreabilidad.

5. Técnicas de Análisis de Software

a. Revisión de código
b. Análisis estático
c. Análisis dinámico
d. Ingeniería inversa.

MÓDULO 4: PRUEBAS DE PENETRACIÓN

1. Pruebas de seguridad

a. Pruebas de penetración
b. Tipos de pruebas de penetración
c. Metodologías para pruebas de penetración
d. Diseño de una prueba de penetración

2. Recolección de información y Enumeración de servicios. (KALI)

a. Recolección de información pasiva: Google Hacking, Shodan, Maltego.
b. Recolección de información activa: Enumeración DNS, SMTP, SNMP
c. Escaneo vulnerabilidades

3. Penetración

a. Fuzzing
b. Buffer Overflows e inyección de código.
c. Ataques del lado del cliente: Usando aplicaciones HTML y Microsoft
Office
d. Exploits públicos.
e. Metasploit Framework

4. Escalamiento de privilegios

a. Ejemplos de escalamiento de privilegios en Windows
b. Ataques de diccionarios

5. Mantenimiento del acceso

a. Port forwarding
b. Entunelamiento DNS, HTTP y SSH (DNS, HTTP y SSH tunneling).
c. Movimiento lateral con RDP
d. Movimiento lateral con SSH

DURACIÓN DEL PROGRAMA

120 HORAS

MODALIDAD

REMOTO

EXPERTO FACILITADOR

JOSÉ MÁRQUEZ DÍAZ

Ingeniero de Sistemas de la Universidad del Norte, Magister en Ciencias Computacionales de ITESM (Instituto Tecnológico y de Estudios Superiores de Monterrey) en asocio con la UNAB y PhD en Ingeniería de Sistemas y Computación de Universidad del Norte. Profesor Tiempo Completo del Departamento de Ingeniería de Sistemas en pregrado y postgrado