UTN.BA
UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES

TEMARIO

- **Introducción**
  - Las evaluaciones de seguridad
  - El hacker ético
  - Metodología de ataque
  - Entregables
  - Bibliografía

- **Fundamentos de seguridad de la información**
  - Conceptos y definiciones
  - Fuga de información
  - Vulnerability research
  - Ingeniería social
  - Control de accesos

- **Recopilación de información**
  - Método de recopilación
  - Footprinting
  - Sistema DNS
  - Consultas de whois
  - Traceroute
  - Herramientas y sitios

- **Escaneo y enumeración**
  - Tipos de escaneo
  - Método de escaneo
  - Escaneo de puertos
  - OS Fingerprinting
  - Banner Grabbing
  - Tipos de Enumeración
  - Escaneo de vulnerabilidades
  - Explotación de vulnerabilidades
  - Herramientas y sitios

- **Búsquedas online**
  - Funcionamiento de los buscadores
  - Uso avanzado de Google y Bing
  - Metabuscadores
  - Buscadores específicos

- **Malware y Botnets**

  - Conceptos y categorías
  - Métodos de propagación
  - Formato de un ataque con malware
  - Método de ataque de Phishing
  - Cibercrimen
  - Botnets
  - Herramientas y sitios

- **Criptografía**
  - Conceptos y elementos
  - Usos de la criptografía
  - Tipos de algoritmos
  - Protocolos de cifrado
  - Protección de datos locales y en tránsito
  - Esteganografía y esteganálisis

- **Seguridad en redes**
  - Tecnología, Internet y las empresas
  - Firewalls
  - Sistemas de detecciónde intrusos (IDS)
  - Honeypots
  - Conexiones a escritorios remotos
  - Redes virtuales (VPN y VLAN)

- **Redes inalámbricas**
  - Tecnología inalámbrica
  - Componentes
  - Autenticación
  - Protocolos de cifrado
  - Requerimientos de seguridad
  - Técnicas de ataque

- **Técnicas de ataque y análisis de tráfico**
  - Sniffing
  - Spoofing
  - Hijacking
  - Packet Crafting
  - Poisoning
  - Herramientas
- Password Cracking
  - Conceptos
  - Métodos de ataque

  - Técnicas de ataque
  - Herramientas
  - Contramedidas
  - Pruebas de fortaleza

- **Seguridad y correo electrónico**
  - Conceptos
  - Análisis de encabezados
  - Anonimización
  - Cuentas temporales
  - E-mail tracking
  - SPAM y filtrado
  - Herramientas y sitios

- **Anonimidad web**
  - Conceptos
  - Proxies anónimos
  - HTTP Tunneling
  - Sistema TOR
  - Servicios privados
  - Recursos web

- **Vulnerabilidades web**
  - A1: Inyección de código
  - A2: Secuencia de Comandos en Sitios Cruzados (XSS)
  - A3: Perdida de Autenticación y Gestión de Sesiones
  - A4: Referencia Directa Insegura a Objetos
  - A5: Falsificación de Petición en Sitios Cruzados (CSRF)
  - A6: Configuración Defectuosa de Seguridad
  - A7: Almacenamiento Criptográfico Inseguro
  - A8: Falla de restricción de acceso a URL
  - A9: Protección Insuficiente en la Capa de Transporte
  - A10: Redirecciones y Destinos No Validados

- **Ingeniería Social**
  - Conceptos y comportamientos vulnerables
  - Fases de un ataque
  - Ingeniería social inversa
  - Tipos de ataque
  - Dumpster diving
  - Herramientas y sitios

- **Seguridad física**
  - Tipos de amenazas
  - Componentes de seguridad física
  - Sistemas de suministro
  - Perímetro e interiores
  - Controles de acceso físico
  - Protecciones en datacenters
  - Detección y supresión de incendios

- **Ingeniería inversa y seguridad en el software**
  - Conceptos fundamentales
  - Desensambladores
  - Debuggers
  - Editores de encabezados
  - Patchers y loaders
  - Otras heramientas
  - Buffer overflow

- **Metodologías de Penetration Testing**
  - Conceptos principales
  - Etapas de un Penetration Test
  - Herramientas automatizadas
  - Uso de Maltego
  - Marco legal de un test
  - Informes y Entregables
  - Metodologías más utilizadas

TEST DE EVALUCIÓN

Examen dividido en teoría y práctica.

CRONOGRAMA DE CLASES

Clase 1

- Introducción
  - Las evaluaciones de seguridad.
  - El hacker ético.
  - Metodología de ataque.
  - Entregables.
  - Bibliografía.

UTN.BA
UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES

Clase 2

- Fundamentos de seguridad de la información.
  - Conceptos y definiciones.
  - Fuga de información.
  - Vulnerability research.
  - Ingeniería social.
  - Control de accesos.

Clase 3

- Recopilación de información.
  - Método de recopilación.
  - Footprinting.
  - Sistema DNS.
  - Consultas de whois.
  - Traceroute.
  - Herramientas y sitios.

Clase 4

- Escaneo y enumeración.
  - Tipos de escaneo.
  - Método de escaneo.
  - Escaneo de puertos.
  - OS Fingerprinting.
  - Banner Grabbing.
  - Tipos de Enumeración.
  - Escaneo de vulnerabilidades.
  - Explotación de vulnerabilidades.
  - Herramientas y sitios.

- Búsquedas online
  - Funcionamiento de los buscadores.
  - Uso avanzado de Google y Bing.
  - Metabuscadores.
  - Buscadores específicos.

Clase 5

- Malware y Botnets
  - Conceptos y categorías.
  - Métodos de propagación.
  - Formato de un ataque con malware.
  - Método de ataque de Phishing.
  - Cibercrimen.

- Botnets.
- Herramientas y sitios.

Clase 6

- Criptografía
  - Conceptos y elementos.
  - Usos de la criptografía.
  - Tipos de algoritmos.
  - Protocolos de cifrado.
  - Protección de datos locales y en tránsito.
  - Esteganografía y esteganálisis.

Clase 7

- Seguridad en redes
  - Tecnología, Internet y las empresas.
  - Firewalls.
  - Sistemas de detecciónde intrusos (IDS).
  - Honeypots.
  - Conexiones a escritorios remotos.
  - Redes virtuales (VPN y VLAN).

- Redes inalámbricas
  - Tecnología inalámbrica.
  - Componentes.
  - Autenticación.
  - Protocolos de cifrado.
  - Requerimientos de seguridad.
  - Técnicas de ataque.

Clase 8

- Técnicas de ataque y análisis de tráfico
  - Sniffing.
  - Spoofing.
  - Hijacking.
  - Packet Crafting.
  - Poisoning.
  - Herramientas.

- Password Cracking
  - Conceptos.
  - Métodos de ataque.
  - Técnicas de ataque.

- Herramientas.
- Contramedidas.
- Pruebas de fortaleza.

Clase 9

- Seguridad y correo electrónico
  - Conceptos.
  - Análisis de encabezados.
  - Anonimización.
  - Cuentas temporales.
  - E-mail tracking.
  - SPAM y filtrado.
  - Herramientas y sitios.

- Anonimidad web
  - Conceptos.
  - Proxies anónimos.
  - HTTP Tunneling.
  - Sistema TOR.
  - Servicios privados.
  - Recursos web.

Clase 10

- Vulnerabilidades web
  - A1: Inyección de código.
  - A2: Secuencia de Comandos en Sitios Cruzados (XSS).
  - A3: Perdida de Autenticación y Gestión de Sesiones.
  - A4: Referencia Directa Insegura a Objetos.
  - A5: Falsificación de Petición en Sitios Cruzados (CSRF).
  - A6: Configuración Defectuosa de Seguridad.
  - A7: Almacenamiento Criptográfico Inseguro.
  - A8: Falla de restricción de acceso a URL.
  - A9: Protección Insuficiente en la Capa de Transporte.
  - A10: Redirecciones y Destinos No Validados.

Clase 11

- Práctica demostrativa de ataques.

Clase 12

- Ingeniería Social
  - Conceptos y comportamientos vulnerables.
  - Fases de un ataque.

  - Ingeniería social inversa.
  - Tipos de ataque.
  - Dumpster diving.
  - Herramientas y sitios.

- Seguridad física
  - Tipos de amenazas.
  - Componentes de seguridad física.
  - Sistemas de suministro.
  - Perímetro e interiores.
  - Controles de acceso físico.
  - Protecciones en datacenters.
  - Detección y supresión de incendios.

Clase 13

- Ingeniería inversa y seguridad en el software
  - Conceptos fundamentales.
  - Desensambladores.
  - Debuggers.
  - Editores de encabezados.
  - Patchers y loaders.
  - Otras herramientas.
  - Buffer overflow.

Clase 14

- Metodologías de Penetration Testing
  - Conceptos principales.
  - Etapas de un Penetration Test.
  - Herramientas automatizadas.
  - Uso de Maltego.
  - Marco legal de un test.
  - Informes y Entregables.
  - Metodologías más utilizadas.

Clase 15

- Laboratorio: Simulación de un Penetration Test.

Clase 16

- Evaluación final.
- Debate y devolución de resultados.