MÁSTER DE CIBERSEGURIDAD

TEMARIO

MÓDULO I – CONCEPTOS BÁSICOS DE CIBERSEGURIDAD

- Nuestra privacidad: Consecuencias.
- Ciberacoso, Vulnerabilidades & Malware + Ciberseguridad.
- Ingeniería Social.
- Redes y protocolos: aprendiendo a manejar las redes
- ¿Somos objetivos?
- Hackers
  - Tipos de hackers.

MÓDULO II – DECÁLOGO DEL BUEN PROGRAMADOR

- Accesos sin cuenta de administrador.
- Actualización de sistemas y medidas básicas de protección.
- Gestión de usuarios, contraseñas.
- Principales problemas con las BBDD.

MÓDULO III – FINGERPRINT & FOOTPRINTING

- Información en la red: modo público.
- Controlando la información expuesta.
- Problemas de publicación excesiva.
- Anonimato en la RED:
  - DARKNET
  - TOR
  - PROXY vs o VPN
  - MACCHANGER

MÓDULO IV – ANALISIS DE VULNERABILIDADES

- Ataques dirigidos VS Ataques aleatorios.
- Enumeración, búsqueda y obtención de información.
- E-mail: la gran vía de entrada.
- Suplantación de identidad mediante email.

MÓDULO V – ATAQUE MÁS COMUNES METASPLOIT

- Explotación de vulnerabilidades.
- Creación de troyanos y malware.
- Artimage.

MÓDULO VI – ATAQUE MÁS COMUNES HACKING WEB

- Hacking Web.
- Acceso al panel de administración y suplantación de identidad.
- Pasarelas de pago no seguras.
- Inyección de código en formularios.
- DoS a páginas y servicios web.
- Phising: clonación de páginas web.
- SQLi: Ataques a Bases de Datos.
- XSS: Cross-Site Scripting.

MÓDULO VII – PROYECTO FIN DE MÁSTER