Security Training
Guido Murillo Suárez
CEH, ECSA, CCSK, SEC+, CHFI, CISM, CISSP, CSSLP
www.cybersec506.com


C|EH
Certified Ethical Hacker
CCSK
Certificate of
Cloud Security Knowledge
E|CSA
EC-Council Certified Security Analyst
CompTIA
Security+
C|HFI
Computer Hacking Forensic INVESTIGATOR
CISM
CISSP
CSSLP

CURSO BÁSICO SEGURIDAD

El temario para el curso de ciber seguridad informática básico está diseñado para dar las bases de ciber seguridad y los principios más importantes. El temario se ha diseñado basándose en los dominios de estudio de las certificaciones Ethical Hacker y Security+.

El mismo incluye ejercicios prácticos para reforzar términos y utilizar herramientas reales diseñadas para PenTest.

El temario para el cúrso básico de seguridad va incluir los siguientes temas:

- Confidentiality
- - o Types of attacks
    - ✦ SQL Injection
    - ✦ Session Hijack
    - ✦ Hashing
    - ✦ Encryption
- Integrity
  - o Types of attacks
    - ▪ Wrappers
    - ✦ Rotkits
    - ✦ Hashing
- Availability
  - o Types of attacks
    - ✦ DOS
    - ✦ DDOS
  - o Measures to protect it.
    - ✦ Redundancy
    - ✦ Backups
    - ✦ Load balancing
    - ✦ UPS
- Defense in depth
- Risk Concepts
  - o Risk
  - o Vulnerability
  - o Threat
  - o Qualitative vs quantitative
- Control types
  - o Technical
    - ▪ Encryption
    - ✦ Antivirus

        - HIDS
        - Firewall • ACLs
        - Least privilege o Management
        - Risk assessment
        - Vuln assessment
        - Pen test o Operational
        - Awareness Control
        - Configuration change management
        - Contigency plan
- Social engineering
    - o Shoulder surfing
    - o Impersonating
    - o Tailgating
    - o Dumpster diving
    - o Phising
        - Whaling
        - Spear Phishing
        - Vishing

Los estudiantes van a realizar varios laboratorios a lo largo del curso, entre 2 y 5 laboratorios por clase lo cual lo hace un curso muy dinámico y práctico. Algunos de los laboratorios a realizar son:

- Clonar un sitio web.
- Obtener información sobre algún objetivo.
- Banner grabbing.
- Proxy chain (hacer que un ataque salga por otras IPS u otros países)
- Crear diccionario para crackear password.
- Sniffear un password de una aplicación web.
- Estaganografía (esconder mensajes en archivos imágenes).
- Esconder un .exe en un pdf (troyano).
- MiTM (interceptar una comunicación para ver que URLs visita la víctima y las imágenes que está viendo http).
- Sniffear direcciones MAC en wireless y clonarlas.
- Clonar sitio web, mostrarlo en una red y robar claves.
- Denegación de servicios a una red wireless.
- Cross Site Scripting en sitio web.
- Inyección de SQL y extraer datos.
- Hackear una red wireless.
- Crear red inalámbrica falsa.

El instructor **Guido Murillo** cuenta con más de 12 años de experiencia en seguridad informática y cuenta con las certificaciones en seguridad más reconocidas a nivel mundial como **CISSP, CSSLP, CISM, CEH, ECSA, SEC+, CCSK y CHFI,** además ha estado en cursos y conferencias más grandes en seguridad como DEFCON y Blackhat.

Cualquier duda o consulta se pueden comunicar al 8706-9124 o al correo info@cybersec506.com.