Ethical Hacker : sesión 1

- shellgpt
- Ethical Hacker : sesión 1

formador

- Fernando Ruiz-Tapiador fernando@ruiz-tapiador.com malote@gmail.com
- Formador Red Hat

Código proyecto: SinCara

- etherpad
- Telegram
- pCloud
- aspen eccouncil: https://aspen.eccouncil.org/MyCourses

clase

- Modulo 0, Modulo 1, Modulo 2
- Lab 0, Lab 2

Introduction to Ethical Hacking

- importancia de los datos: confidencialidad, integridad, disponibilidiad, autenticidad, no-repudio
- EXAM:

```
Attacks = Motive (Goal) + Method (TTP) + Vulnerability
```

    - TTP: Tácticas, técnicas y procedimientos
        - cada grupo tiene su compendio de TTP
- Ataques
    - pasivos
    - activos
    - close-in (cercanos)
    - internos (50%)
    - distribuidos
- Guerras entre estados
- lackrack
- atención legislaciones: México, modificación o reparación dispositivos.
- White Hat Hackers: Siempre por permiso del propietario y por escrito
- IA, herramienta de ayuda
    - ChatGPT + API = shellgpt (Lab 0)
        - API de pago, por petición
- EXAM: CyberKill Chain Methodology
    - travas en toda la cadena para defgenrer
    - https://ichi.pro/es/modelo-de-diamante-de-analisis-de-intrusion-233418583446217 - Modelo Diamante de análisis de intrusión
    - https://blog.segu-info.com.ar/2023/11/el-modelo-diamante-vs-mitre-att.html - El modelo diamante vs MITRE ATT&CK

- Asegurar los datos
- Estrategia continua/adaptativa de seguridad
- Defensa en profundidad
- Riesgo
    - medir el riesgo (matrix)
    - elimiar algunos riesgos, mitigar otros (no se pueden eliminar)
    - gestión del riesgo
- Ciber seguridad en la empresa
    - estratégica
    - tácticas
    - técnica
    - operacional
- Estandard ISO

Modulo 02

- Footprinting: reconocimiento, captura de información
- pasivo (sin contacto directo) / activo (ingenieria social)
    - atacar por la tarde, con los filtros bajados, cansancio
- Información de la organización
- Información de la red
- Información OS
    - perfil más atacado: CFO - finanzas (pasta, bajo perfil informático) y familia
    - también CEO
- Operadores en Google - Google Dorks
    - https://www.exploit-db.com/google-hacking-database
- SHODAN
    - https://www.shodan.io
- EXAM: preguntas de herramientas
    - casos de uso de las herramientas
- https://archive.org
    - juegos spectrum jugables
    - https://github.com/s0md3v/Photon
- Averiguar información de la competencia (legal)
- https://geospy.ai/
    - búsqueda con IA para averiguar ubicación a través de una foto
- https://ciberpatrulla.com/links/
    - https://onbranding.start.me/p/q6jDm2/ciberpatrulla-tools
    - https://github.com/Ph055a/OSINT_Collection
- Sherlock: búsqueda por nick en redes sociales (500)
- whois DB:
- ip2location
- DNS: `dig`
- `traceroute`, `tracepath`, `mtr [-z]`
- maltego, recon-ng
- foca (metadatos archivos) - elevenpaths, subfinder
- contramedidas
    - publicar poco en internet
- www.insecam.org - cámaras abiertas
- privnote.com

Modulo 03

lab 0

Instalación API key para instalar shell GPT

```
export OPENAI_API_KEY='<KEY>'
```

lab 2

- Google Dorks
- netcraft → resources → research tool → site report → domain
- dnsdumpster.com