Ethical Hacker : sesión 1

- Ethical Hacker : 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: https://u.pcloud.link/publink/show?code=kZejslkZw6XkrBbTzRR5dQf1LGglGb2T3jGk
- aspen eccouncil: https://aspen.eccouncil.org/MyCourses

clase

- ASPEN: Modulo 0, Modulo 1, Modulo 2, Modulo 3, Modulo 4, Modulo 5
- ASPEN: Lab 0, Lab 2
- Pendiente:
    - ASPEN: Lab 3, Lab 4, Lab 5

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 and Reconnaissance

- 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 : Scanning Networks

- Escaneo de redes
- Ya es necesario el permiso expreso para realizar cualquier cosa
- nmap, hping3,netspolit, netscantools
- TCP
    - secuencia de paquetes (si pierdo uno, repido desde ahí)
    - tamaño de la ventana: a que velocidad nos comunicamos
    - FLAG:
        - SYN + ACK : sincronización y conformidad (3 hand shaking)
        - FIN + ACK : finalización de conexión y conformidad (4 hand shaking)
        - RST : dejar con la palabra en la boca al otro (reset conn)
        - URG: deshuso - urgente
        - PSH: envia
    - Técnicas de descubirmiento de hosts
        - ICMP Ping
        - ...
    - Técnicas de descubrimiento de puertos
        - EXAM: `nmap` ← parámetros
            - https://wallpapercave.com/wp/wp10179392.jpg
            - https://stationx-public-download.s3.us-west-2.amazonaws.com/nmap_cheet_sheet_v7.pdf
            - scripts: https://nmap.org/nsedoc/scripts/
            - más scripts: https://thehackerway.es/2024/02/12/15-scripts-nse-disponibles-en-nmap/
            - https://thehackerway.es
        - SCTP ← intermedio entre TCP+UDP (https://www.ionos.es/digitalguide/servidores/know-how/sctp/)
    - Técnicas descubrimiento servicios
    - Técnicas descubrimiento OS
        - Banner Grabbing
    - Escan detrás de firewall / IDS / IPS
        - firewall: solo cabecera paquete
        - IDS / IPS: cabecera + contenido. Por detrás del firewall
    - Decoy (señuelo)
        - `nmap -D RND:10 [target]`
        - `nmap -D Decoy1,Decoy2,Decoy3 [target]`
    - Spoofing
        - falsificar origen
    - ping sweep (escaneo a rango)
    - Proxy Servers
    - Contramedidas
        - restringir ICMP
        - IP Spoofing:
            - mirar TTL (saltos)
            - mirar numero de paquete
            - cambio tamaño de ventana
    - Metasploit

Modulo 04 : Enumeration

- Enumeración
- NetBios
    - no funciona IPv6
- SNMP
    - v1: texto plano

    - v2: opcional
    - v3: todo cifrado
- LDAP
- NTP
    - Muchos problemas por mala sincronización horaria
    - Servidor NTP interno (bien protegido)
    - `rdate hora.roa.es rdate hora.roa.es; LANG=C; date`
    - PTP = Precision Time Protocol
    - NTS = NTP secured
    - Delorean - servidor NTP para configurar fechas falsas
- NFS
    - cliente nativo
    - `showmount -e X.X.X.X`
    - desechar v3 o anteriores
- SMTP
    - verificar usuarios por servidores no seguros (:25)
- DNS
    - transmitir datos de zona simulando ser DNS secundario
    - DNSSEC
- IPSec
    - fallo de diseño
    - si monitorizas el tráfico, puedes deducir el algoritmo
- VoIP
- RPC
- SMB

Modulo 05 : Vulnerability Analysis

- Analisis de vulnerabilidades
- NIST - NICE - ENISA
    - https://nvd.nist.gov/
    - CVE - vector, puntuación en función matrix
    - Solo los CNA pueden emitir CVE
- CWE - listado vulnerabilidades programando
    - https://cwe.mitre.org/top25/archive/2024/2024_cwe_top25.html
- SCAP
    - aplicar, verificar y auditar para ver si cumple con los protocolos de seguridad
- Mitre Att&ck
    - organismo publico financiado por el NIST
    - categoriza ataques
    - información de grupos
    - herramientas
- Mitre d3fend
- CTF

From:
https://matebcn.eu/ - **miguel angel torres egea**

Permanent link:
https://matebcn.eu/info:cursos:pue:ethical-hacker:sesion1

Last update: **21/02/2025 08:47**