

# Ethical Hacker : sesión 3

- [Ethical Hacker : sesión 3](#)

## clase

- Modulo 09 - Ingeniería social
- Modulo 10 - Denegación de servicio
- Modulo 11 - Session Hijacking
- Modulo 12 - Evadiendo IDS, cortafuegos y honeypots
- Modulo 13 - Ataques a servidores web

## Modulo 09 - Ingeniería social

- el ser humano es el eslabón más débil de la ciberseguridad

### sección 2

- suplantación: hacerse pasar por alguien
  - <https://github.com/g0njxa/cazandophishing>
- vishing: suplantación por voz
- Eavesdropping: escuchar conversaciones no autorizadas
- Shoulder surfing: mirar por encima del hombro
- Dumpster Diving: bucear en la basura
- Reverse Social Engineering
- Piggybacking: llorar a alguien de dentro para que te abra
- Tailgating: colarme en un turno pasando junto a otro
- Diversion Theft: robo por descuido
- Honey Trap: persona atractiva
- Baiting: cebo con malware (USB)
- Quid Pro Quo: hacerse pasar por empleado de la empresa
- Elicitation: sacar información a través de una conversación

### sección 3

- Phishing
  - spear: dirigido a persona o personas
  - whaling: a más gente que el anterior
  - pharming: cosechar, manipular web o crear una falsa
  - spimming: mensajería instantanea
- tools:
- Otras técnicas..
- Deepfake
- Ocultar / falsear URLs
  - [https://es.wikipedia.org/wiki/Nombre\\_de\\_dominio\\_internacionalizado](https://es.wikipedia.org/wiki/Nombre_de_dominio_internacionalizado)
  - No usar Let's Encrypt
  - Punycode
  - caracter unicode para cambiar sentido escritura
    - \u202E

- <https://unicode-table.com/es/202E/> - Caracter Unicode que invierte el sentido de escritura de lo que venga a continuación
- <https://blog.segu-info.com.ar/2020/08/el-phishing-utiliza-texto-invisible-y.html> - Poner texto al revés, y con el carácter Unicode anterior, mostrarlo bien. Pero los analizadores de texto, ven el texto al revés.
- <https://symbl.cc/es/unicode/blocks/general-punctuation/#subblock-202A> - Otros caracteres que hacen algo parecido. Para poner caracteres unicode en Linux, en la línea de comandos, es con Shift+Ctrl+U y luego el código: u2764 → ♥
- <https://browserling.com> - navegar simulando ser un OS
- <https://www.getlinkinfo.com> - desacortador URLs
- <https://www.thispersondoesnotexist.com/>
- QRJacking

## sección 5

- AntiPhising Toolbar
  - netcraft
- Phishtank
- OhPhish - simular campaña phishing

## Modulo 10 - Denegación de servicio

- DoS / DDoS
  - vender como estrés y resiliencia
- muchas peticiones, es igual el dispositivo
- buscar vulnerabilidades conocidas → SHODAN
- Vectores de ataque DoS/DDoS
  - volumen
    - UDP Flood Attack
    - ICMP Flood
    - Ping of Death → paquete medida superior al standard RFC 791 IP
    - Smurf (pitufo), usar sitios legítimos falseando la IP
    - NTP Amplification Attack
  - protocolo
    - SYN Flood
      - enviar SYN y no responder con el ACK
      - enviar SYN a saco
    - Fragmentation
      - usar recursos de destino volviendo a juntar el paquete fragmentado
    - Spoofed Session Flood Attack
      - establecer sesión SYN-ACK y no hacer nada más
      - consumir recursos
  - Aplicación
    - GET/POST
    - Multi Vector
    - Pear-to-pear
    - Permanent DoS
      - phlashing
  - ENEMA

## sección 3 técnicas de detección

- Profiling

- Oleadas de ataques
- contramedidas
  - recursos y planificación
  - identificar servicios críticos
  - apagar servicios
- deflectar ataques... no (son terceras máquinas)
- mitigar ataques
- Post-ataque forense

## sección 4 protección

- CDNs (apuntes)
  - diseño arquitectura distribuido
  - [https://es.wikipedia.org/wiki/Red\\_de\\_distribuci%C3%B3n\\_de\\_contenidos](https://es.wikipedia.org/wiki/Red_de_distribuci%C3%B3n_de_contenidos) - Qué es una CDN
  - <https://blog.templatetoaster.com/difference-between-cloudflare-and-akamai/> - Comparativa entre las dos soluciones más potentes del mercado: Akamai y Cloudflare. Spoiler: Cloudflare tiene productos gratuitos muy interesantes, cosa que no tiene Akamai.
  - <https://about.netflix.com/es/news/how-netflix-works-with-isps-around-the-globe-to-deliver-a-great-viewing-experience> - Cómo funciona la CDN de Netflix
  - <https://www.xataka.com/streaming/la-compleja-infraestructura-detras-de-netflix-que-pasa-cuando-l-e-das-al-play> -Artículo brutal sobre el funcionamiento de Netflix en 2018
  - <https://ipinfo.io/AS6752> - Sistema autónomo de Andorra
- cloudflare
  - versión gratuita - <https://www.cloudflare.com/es-es/>

## extra

- Protocolo Diffie-Hellman: <https://youtu.be/vZToAM4kwjM?si=ic-75SMu28MVG6ZN>

## Modulo 11 - Session Hijacking

## Modulo 12 - Evadiendo IDS, cortafuegos y honeypots

- IDS - detección intrusos
- IPS - detección y prevención intrusos
- de Host o de red (HIPS, NIDS...)
  - HIDS → <https://wazuh.com/>
  - sshguard → <https://www.sshguard.net/>
  - fail2ban
- tipos de alerta en IDS (EXAMEN)
- arquitecturas de cortafuegos (EXAMEN)
- tipos de firewall
  - dispositivo / host-based
  - capa 3 (por definición)
  - capa 5 (circuit level gateway firewall)
  - capa 7 (Application level gateway firewall - WAF) - contenido paquetes
  - Stateful multilayer inspection firewall
  - Application proxy
  - VPN firewall
- Tools
  - snort (intrusion detection tools) - IDS, IPS
    - reglas (EXAMEN)

- añadido a pfsense
  - suricata IDS/IPS
- técnicas evasión
  - firewalking: averiguar con tracereoute y paquetes sospechosos para que el firewall actue
  - identificación
  - sitios navegación anónimo (no suelen funcionar)
  - tunelización SSH (poor man)
    - herramientas Linux/Windows GUI
  - tunelización DNS
  - ...
- NAC (Network Access Control) / Endpoint (nueva v13 temario)

## sección 5: Honeypot

## sección 6: defensa contra evasión IDS

- normalizador de tráfico

# Modulo 13 - Ataques a servidores web

- <https://zumpad.zum.de/p/SinCara-XSS>

## sección 1

- XSS

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

Permanent link:  
<https://matebcn.eu/info:cursos:pue:ethical-hacker:sesion3>

Last update: **21/02/2025 09:04**

