Apuntes SinCara sesión 1

Modulo 01

- El CIO (Director de Información), es el gerente de sistemas o director de tecnologías de la información (responsable de TI). Reporta directamente al CEO, y se encarga directamente de las estrategias de la organización que están alineadas con la tecnología de la información para lograr los objetivos planificados.
    - El CSO (Chief Security Officer) es el responsable de la seguridad de la organización. Al CSO a veces se le denomina responsable de seguridad corporativa.
    - El CISO (Director de Seguridad de la Información) es el director de seguridad de la información. Básicamente es un rol desempeñado a nivel ejecutivo y su función principal es la alineación de la seguridad de la información con los objetivos del negocio. De esta forma se garantiza en todo momento que la información de la empresa está protegida con seguridad.
    - https://www.incibe.es/protege-tu-empresa/blog/ceo-ciso-cio-roles-ciberseguridad
    - https://rafeeqrehman.com/2024/03/31/ciso-mindmap-2024-what-do-infosec-professionals-really-do/ - CISO Mindmap 2024. ¿Qué hacen realmente los profesionales InfoSec?
        - https://rafeeqrehman.com/wp-content/uploads/2024/03/CISO_MindMap_2024-2.png - El Mindmap a máxima resolución
- https://www.hornetsecurity.com/es/knowledge-base/cyber-kill-chain/ - Cyber Kill Chain
- TTP: Las técnicas son las herramientas utilizadas, la táctica es la forma de combinar esas herramientas para hacer un determinado trabajo y el procedimiento es la guía a seguir para hacer el trabajo.
- IoC:
    - Es la descripción de un incidente de ciberseguridad, actividad y/o artefacto malicioso mediante patrones para ser identificado en una red o endpoint pudiendo mejorar así las capacidades ante la gestión de incidentes.
    - https://es.wikipedia.org/wiki/Indicador_de_compromiso - IoCs
- Attacks = Motive (Goal) + Method (TTP) + Vulnerability
- 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
- Information Assurance (IA):
    - Es la práctica de asegurar la información y gestionar los riesgos relacionados con el uso, el procesamiento, el almacenamiento y la transmisión de la información.
    - La garantía de la información incluye la protección de la integridad, la disponibilidad, la autenticidad, el no repudio y la confidencialidad de los datos de los usuarios.
    - La IA abarca no sólo las protecciones digitales sino también las técnicas físicas. Estas protecciones se aplican a los datos en tránsito, tanto en forma física como electrónica, así como a los datos en reposo.
- Cyber Threat Intelligence (CTI):
    - Cyber Threat Intelligence es el arte de convertir los datos en inteligencia sobre amenazas informáticas para prevenir ataques
    - https://www.welivesecurity.com/la-es/2021/11/08/que-es-cyber-threat-intelligence/
- Threat Modeling (Modelado de Amenazas):
    - La elaboración de modelos de amenazas es un proceso mediante el cual se pueden identificar y enumerar las posibles amenazas, como las vulnerabilidades estructurales o la ausencia de protecciones apropiadas, y se puede dar prioridad a su mitigación.
    - El propósito de la modelización de amenazas es proporcionar a los defensores un análisis sistemático de los controles o defensas que deben incluirse, dada la naturaleza del sistema, el perfil del atacante probable, los vectores de ataque más probables y los bienes más deseados por un atacante.
    - https://www.flu-project.com/2014/06/el-modelado-de-amenazas-parte-i.html

    - https://www.flu-project.com/2014/06/el-modelado-de-amenazas-parte-ii.html
    - https://www.flu-project.com/2014/06/el-modelado-de-amenazas-parte-iii.html
    - https://blog.segu-info.com.ar/2023/01/desarrollo-seguro-mediante-el-modelado.html
- Legislación:
    - https://blog.segu-info.com.ar/2020/08/apis-con-certificacion-pci-dss-rgpd-y.html - PCI DSS
        - https://www.pcihispano.com/ - PCI DSS Hispano
        - https://blog.segu-info.com.ar/2022/04/pci-dss-v40-y-la-proteccion-de-scripts.html - PCI DSS v4.0
        - https://blog.segu-info.com.ar/2022/06/analisis-de-pci-dss-v40.html - Análisis de PCI DSS v4.0
        - https://www.incibe.es/protege-tu-empresa/blog/pagos-linea-mas-seguros-pci-dss-version-40 - v4.0
    - https://es.wikipedia.org/wiki/ISO/IEC_27000-series - La serie ISO/IEC 27000 de normas son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).
    - https://www.uprm.edu/p/cpshi/ley_hippa - HIPAA
    - https://www.ineaf.es/tribuna/que-es-la-ley-sox-y-para-que-sirve/ - SOX
        - Aunque la Ley SOX es una normativa estadounidense, afecta a empresas españolas que operan en los mercados financieros de Estados Unidos, y también a proveedores de empresas reguladas por SOX.
        - https://es.wikipedia.org/wiki/Digital_Millennium_Copyright_Act - DMCA
    - FISMA:
        - La certificación FISMA es un requisito para muchos contratos con el gobierno de Estados Unidos, siendo un marco diseñado para proteger al gobierno de los Estados Unidos contra los ataques a la ciberseguridad y los desastres naturales que pongan en riesgo los datos confidenciales, las operaciones y los activos.
        - Obliga a implementar y soportar controles de seguridad de TI uniformes, definidos por el Instituto Nacional de Normas y Tecnología (NIST), permitiendo entre otras cosas, que los contratistas trasladen, de manera segura y confidencial, sus aplicaciones indispensables a la nube, ambientes de hospedaje administrados y que contraten a proveedores de SaaS que cumplan con las disposiciones de la ley FISMA.
- Normas ISO serie 27k:
    - http://iso27000.es/ - El portal de ISO 27001 en Español
    - http://iso27000.es/iso27000.html - Normas ISO 27k
    - https://normaiso27001.es/ - Otro portal que habla de las ISO 27k
    - https://t.me/iso27001hispano - Canal de Telegram con las ISO 27k
    - https://www.enac.es/ - ENAC certifica en España. Entidad Nacional de Acreditación en España.
- https://blog.segu-info.com.ar/2019/11/penetration-testing-vs-red-teaming-cual.html - Pentesting vs Red Teaming
- https://hackernoon.com/introducing-the-infosec-colour-wheel-blending-developers-with-red-and-blue-security-teams-6437c1a07700 - Los colores de la ciberseguridad: Blue, Red, Purple, Orange...
- https://eu.desmoinesregister.com/story/news/crime-and-courts/2019/09/11/men-arrested-burglary-dallas-county-iowa-courthouse-hired-judicial-branch-test-security-ia-crime/2292295001/ - El Incidente de Iowa
- https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ - Historial de hackeos
    - https://blog.elhacker.net/2022/07/la-cadena-de-hoteles-marriott-es-hackeada-por-sexta-vez.html - La cadena de hoteles Marriott es hackeada por sexta vez
- https://www.bbc.com/mundo/noticias-internacional-53102950 - Ciberguerra entre estados
    - https://blog.segu-info.com.ar/2020/09/atacantes-norcoreanos-roban-millones-en.html - Atacantes norcoreanos roban millones en criptomonedas
- https://www.eluniversal.com.mx/techbit/diputados-aprueban-ley-iras-la-carcel-si-reparas-o-modificas-tus-dispositivos-electronicos - Ley mexicana que impide que puedas manipular tus propios dispositivos.
- https://www.youtube.com/results?search_query=atm+robbery - Robo de cajero
    - https://www.elmundo.es/espana/2022/12/28/63ac5f33fc6c8309128b4591.html - Y en Badajoz, con el mismo método
- IKEA hacking
    - https://wiki.eth0.nl/index.php/LackRack - mesita rack

    - https://www.impresoras3d.com/mesa-basica-de-ikea-para-crear-camara-cerrada-de-impresora-3d/
    - https://ikeahackers.net/

Modulo 02

- Google Hacking
    - Google Dorks - «trucos» de Google para búsquedas concisas
    - https://www.redeszone.net/tutoriales/seguridad/google-hacking-que-es-privacidad-usuarios/ - Google Hacking: qué es y cómo afecta a la privacidad de los usuarios
    - https://www.exploit-db.com/google-hacking-database - Google Hacking Data Base
- Internet oculto:
    - Surface Web: La parte conocida de la Web por la que navegamos.
    - Deep Web: Todo el Internet oculto. Es todo el contenido que no está indexado en los motores de búsqueda.
        - Darknet: Redes específicas que se mantienen ocultas, como Tor, I2P, FreeNet.
        - Dark Web: Son los propios sitios que forman parte de la red, de la Darknet
    - https://www.redeszone.net/noticias/redes/motores-busqueda-acceder-deep-web-gratis/ - Motores de búsqueda para acceder a la Deep Web
- SHODAN - https://www.shodan.io
    - El día 17 de julio de cada año suelen sacar una oferta de 5$ de pago único de acceso de por vida a la licencia freelance
    - https://maps.shodan.io/ - También tiene un mapa para buscar
        - https://maps.shodan.io/#27.953164890693838/-15.44059753417969/11/satellite/port:22 - Servidores con el puerto 22 abierto, en Gran Canaria
    - https://github.com/jakejarvis/awesome-shodan-queries/ - Algunas búsquedas curiosas
    - https://awesomeopensource.com/projects/shodan - Recopilación de recursos para Shodan
    - http://www.reydes.com/d/?q=Interfaz_en_Linea_de_Comando_de_Shodan - Para hacer búsquedas en SHODAN desde línea de comando (importando la API)
        - https://cli.shodan.io/
- Otros Buscadores:
    - https://www.redeszone.net/tutoriales/seguridad/buscadores-internet-hackers/ - Los mejores buscadores de Internet que usan los hackers
    - https://www.idcrawl.com/ - Para buscar información de cualquier usuario en redes.
    - http://www.insecam.org - Cámaras IP de acceso libre
    - https://tineye.com - Buscador inverso de imágenes
    - https://yandex.com/ - Yandex, buscador ruso
    - https://geospy.ai/ - Geolocaliza una imagen con IA
- Dominios:
    - https://commons.wikimedia.org/wiki/File:Regional_Internet_Registries_world_map.svg - Mapa RIR
    - https://dnsdumpster.com/ - Información muy completa
    - http://ipv4info.com/ - A través de VT, censys, theharvester, recon-ng e incluso a través de shodan a veces, puedes ir complementando subdominios. Una forma muy pasiva es descargarte los ficheros de scans.io y consultar en estos directamente sin dejar rastros de tus búsquedas en las webs o tools
    - `whois -h whois.radb.net — '-i origin AS20' | grep -Eo «([0-9.]+){4}/[0-9]+»` ⇒ Saca las ips publicas de un sistema autonomo de una empresa, ej AS20
    - https://ftp.ripe.net/ripe/dbase/ - Base de Datos de dominios de RIPE (Europa)
        - `egrep -i -B4 «(Bank)» ripe.db | grep ^inetnum | cut -c17- | tr -d « » | xargs -I {} ipcalc {} | grep -v ^dea` → Saca las ip de bancos registradas en ripe.db
        - https://whoisrequest.com/history/ - Histórico de un dominio, la versión gratis solo permite 5 peticiones al día
        - https://dnslytics.com/reverse-ip - Buscador inverso de dominios, pones un dominio y te dice los que comparten IP con él, vecinos de IP.

- Fuentes de Inteligencia:
  - https://www.intelpage.info/fuentes-de-inteligencia.html - Distintas fuentes de Inteligencia
  - OSINT:
    - https://intelx.io/ - Buscador OSINT
    - https://osintframework.com/ - OSINT Framework
    - https://ciberpatrulla.com/ - CiberPatrulla, Curso y herramientas OSINT
      - https://onbranding.start.me/p/q6jDm2/ciberpatrulla-tools - Las mismas herramientas, pero en otro portal
    - https://github.com/jivoi/awesome-osint - Awesome OSINT
    - https://www.faganfinder.com/ - Recopilatorio
    - https://start.me/p/DPYPMz/the-ultimate-osint-collection - The Ultimate OSINT collection
    - https://papelesdeinteligencia.com/que-son-fuentes-de-informacion-osint/ - Otras fuentes
    - https://github.com/s0md3v/Photon - Photon, es un crawler que recopila información de páginas webs, se descarga ficheros, e incluso tira de archive.org
  - https://wwwhatsnew.com/2020/09/18/alianza-entre-cloudflare-e-internet-archive-permitira-revivir-sitios-caidos-temporalmente/ - Alianza entre Cloudflare e Internet Archive permitirá revivir sitios caídos temporalmente
  - https://www.yougetsignal.com - Recopilatorio de herramientas online

Modulo 03

- nmap
  - https://wallpapercave.com/wp/wp10179392.jpg - Chuleta básica de nmap
  - https://nmap.org/nsedoc/scripts/ - Listado de NSE Scriptsç
    - https://thehackerway.com/2024/02/12/15-scripts-nse-disponibles-en-nmap/ - 15 scripts NSE disponibles en Nmap
  - http://scanme.org/ - Página propiedad de nmap, preparada para que la gente la pueda escanear y jugar con ella.
  - https://openwebinars.net/blog/nmap-uso-basico-para-rastreo-de-puertos/ - Tutorial bastante extenso
  - https://stationx-public-download.s3.us-west-2.amazonaws.com/nmap_cheet_sheet_v7.pdf - Chuleta brutal, en inglés. Sacada de https://www.stationx.net/nmap-cheat-sheet/
  - https://elblogdebart.com/tecnicas-de-escaneo-de-puertos-nmap-parte1/ - Tipos de escaneos. Parte 1
    - https://elblogdebart.com/escaneando-con-nmap-nmap-parte2/ - Parte 2
  - https://tools.kali.org/information-gathering/masscan - Masscan, un port scanner muy rápido.
  - https://blog.haschek.at/2019/i-scanned-austria.html - I scanned the whole country of Austria and this is what I've found.
  - mtr:
    - `mtr –aslookup` # Para que me muestre los Sistemas Autónomos por los que pasa (-z en formato corto)
    - https://winmtr.uptodown.com/windows - WinMTR, MTR para windows (Para windows está también pathping)
- TCP:
  - https://www.ionos.es/digitalguide/servidores/know-how/sctp/ - Protocolo SCTP
  - https://stackoverflow.com/questions/9153566/difference-between-push-and-urgent-flags-in-tcp?noredirect=1&lq=1 - Diferencias entre PSH y URG
  - https://subinsb.com/default-device-ttl-values/ - Default TTL (Time To Live) Values of Different OS
  - https://www.eduardocollado.com/2020/03/13/flags-de-tcp/ - Los Flags de TCP

Modulo 04

- NTP

    - https://www.ionos.es/digitalguide/servidores/know-how/simple-network-time-protocol-sntp/ - SNTP (simple network time protocol), versión simplificada de NTP, desarrollada a principios de los 90, por la escasa potencia de los ordenadores de aquella época.
    - https://www.incibe-cert.es/blog/ntp-sntp-y-ptp-sincronizacion-tiempo-necesito - Comparativa entre SNTP, NTP y PTP.
    - https://fedoramagazine.org/secure-ntp-with-nts/ - NTS, un NTP más seguro
    - https://github.com/PentesterES/Delorean - Delorean - Servidor NTP que podemos configurar para dar respuestas falsas
    - https://www.pool.ntp.org - Servidores NTP accesibles en el mundo

Modulo 05

- https://security.snyk.io/ - Snyk Vulnerability Database
- https://github.blog/2020-09-30-code-scanning-is-now-available/ - Github tiene ya su propio scanner de vulnerabilidades, que se puede utilizar en cualquier proyecto.

Organizaciones y estándares relevantes en la ciberseguridad

- NIST:
    - https://www.nist.gov/ - NIST - Instituto Nacional de Estándares y Tecnología - National Institute of Standards and Technology
    - Es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. La misión de este instituto es promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica y la calidad de vida.
    - https://es.wikipedia.org/wiki/Instituto_Nacional_de_Est%C3%A1ndares_y_Tecnolog%C3%ADa
    - https://csrc.nist.gov/publications - Publicaciones de seguridad informática del NIST
    - https://www.nist.gov/itl/applied-cybersecurity/nice - NICE: National Initiative for Cybersecurity Education. CEH cumple al 100% el programa de NICE.
    - https://www.enisa.europa.eu/ - ENISA - Equivalente europeo del NIST
- NVD:
    - https://nvd.nist.gov/ - NVD - National Vulnerability Database, lanzada por el NIST en 2005. Gestiona los CVEs. Es el repositorio del gobierno de los EEUU de estándares, vulnerabilidades y protocolos. Uno de dichos protocolos es Security Content Automation Protocol (SCAP).
- CVE:
    - Es definido y es mantenido por The MITRE Corporation (por eso a veces a la lista se la conoce por el nombre MITRE CVE List) con fondos de la National Cyber Security Division del gobierno de los Estados Unidos de América. Forma parte del llamado Security Content Automation Protocol (SCAP).
    - https://es.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures - Qué es CVE
    - https://empresas.blogthinkbig.com/ocho-siglas-relacionadas-con-las-6/ - Magnifico artículo explicando CVE
    - https://www.cvedetails.com/vulnerability-list/ - CVEs organizados por fabricante
    - https://cve.mitre.org - info variada,
    - CVSS:
        - https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator - Calculadora CVSS
        - https://unaaldia.hispasec.com/2023/11/cvss-4-0-nueva-version-de-evaluacion-de-vulnerabilidades.html - CVSS 4.0: Nueva versión de evaluación de vulnerabilidades
        - https://www.incibe.es/incibe-cert/blog/cvss-v40-avanzando-en-la-evaluacion-de-vulnerabilidades - CVSS 4.0: avanzando en la evaluación de vulnerabilidades
    - CNA:
        - https://www.cve.org/ProgramOrganization/CNAs - CNAs (CVE Numbering Authorities), entidades que pueden emitir CVEs.
        - https://www.cve.org/PartnerInformation/ListofPartners - Listado
        - https://www.incibe.es/sala-prensa/notas-prensa/incibe-sera-el-unico-organismo-espanol-com

petente-designacion-y-divulgacion - INCIBE será el único organismo español competente en la designación y divulgación de vulnerabilidades a nivel internacional.

- VDP:
  - Vulnerability Disclosure Policy: Un VDP les dice a quienes encuentran fallas en la infraestructura digital de una agencia dónde enviar un informe, qué tipos de pruebas están autorizadas, para qué sistemas y qué comunicación esperar en respuesta.
  - https://blog.segu-info.com.ar/2020/12/divulgacion-de-vulnerabilidades.html - Divulgación de vulnerabilidades responsable en el ámbito público
  - https://blog.segu-info.com.ar/2022/04/securitytxt-es-oficialmente-el-rfc-9116.html - Aprobado el estandard de VDP. Para usarlo se crea el fichero security.txt en la raíz del sitio web
- CWE:
  - https://empresas.blogthinkbig.com/ocho-siglas-relacionadas-con-las_31/ - CWE: es una lista de tipos de debilidades de software dirigida a desarrolladores y profesionales de la seguridad. Fue creada al igual que CVE para unificar la descripción de las debilidades de seguridad de software en cuanto a arquitectura, diseño y código se refiere. Se puede ver como un catálogo de debilidades documentadas que se suelen cometer programando, y que podría derivar en vulnerabilidades.
  - https://cwe.mitre.org/top25/archive/2024/2024_cwe_top25.html - Los 25 errores de software más peligrosos (CWE Top 25) es una lista demostrativa de las debilidades más extendidas y críticas que pueden conducir a vulnerabilidades graves en el software.
- CIS:
  - Desarrollados por el Center for Internet Security, los Controles de Seguridad Crítica de CIS son un conjunto prescriptivo y prioritario de mejores prácticas en seguridad cibernética y acciones defensivas que pueden ayudar a prevenir los ataques más peligrosos y de mayor alcance, y apoyar el cumplimiento en una era de múltiples marcos de seguridad y regulaciones (NIST Cybersecurity Framework, NIST 800-53, NIST 800-171, serie ISO27k, PCI DSS, HIPAA, NERC CIP, y FISMA).
  - https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html - ¿Qué son y cómo implementar los Controles de Seguridad Crítica CIS?
  - https://blog.segu-info.com.ar/2023/04/controles-cis-esenciales-de.html - Controles CIS esenciales de Ciberseguridad
- SCAP:
  - https://es.wikipedia.org/wiki/Security_Content_Automation_Protocol - SCAP
  - https://www.open-scap.org/ - OpenSCAP - Versión open source de SCAP
- STIG:
  - https://public.cyber.mil/stigs/scap/ - Guías STIG (Security Technical Implementation Guides)
  - https://nvd.nist.gov/ncp/repository - Repositorio de Guías del NCP (National Checklist Program), definido por el NIST en el SP 800-70.
  - https://www.cyber.gov.au/publications - Guías de seguridad Australianas, van mucho a lo práctico. Si necesitáis traducirlas al español, se puede hacer en: https://www.onlinedoctranslator.com/es/translationform (no subir nada confidencial)
  - https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-esquema-nacional-de-seguridad.html - Guías 800 (STIG) del CCN-CERT
- MITRE ATT&CK
  - https://attack.mitre.org/ - ATT&CK
    - https://d3fend.mitre.org/ - D3FEND
  - https://blog.segu-info.com.ar/2019/08/la-filosofia-de-att-explicada.html - Artículo pequeño
  - https://blog.segu-info.com.ar/2019/06/matrices-y-herramientas-de-mitre-att.html - Estupendo artículo (largo)
  - https://blog.segu-info.com.ar/2019/10/comenzar-usar-att-y-la-apt38.html - Serie de varios artículos de como usarlo.
  - Threat Hunting:
    - https://blog.segu-info.com.ar/2019/11/threat-hunting-la-piramide-del-dolor-i.html
    - https://blog.segu-info.com.ar/2019/11/threat-hunting-ciclos-de-caceria-ii.html
    - https://blog.segu-info.com.ar/2019/12/threat-hunting-descubrimiento-de-ttp-iii.html

        - https://www.hackplayers.com/2019/12/detectando-tecnicas-y-tacticas-att-en-linux.html - Detectando técnicas y tácticas ATT&CK en Linux
        - https://www.mbsecure.nl/blog/2019/5/dettact-mapping-your-blue-team-to-mitre-attack - Cómo defenderse de cada uno de los ataques
        - https://github.com/rabobank-cdc/DeTTECT/wiki - Script automatizado para MITRE ATT&CK
        - https://blog.segu-info.com.ar/2020/08/mitre-lanza-shield-una-matriz-para-blue.html - Shield
        - https://derechodelared.com/cisa-decider-mitre-attck/ - La Agencia de Seguridad de Ciberseguridad e Infraestructura de los Estados Unidos (CISA) ha lanzado 'Decider', una herramienta de código abierto que ayuda a los defensores y analistas de seguridad a generar rápidamente informes de mapeo MITRE ATT&CK.
    - APT:
        - https://attack.mitre.org/groups/ - APTs
        - https://github.com/StrangerealIntel/EternalLiberty/blob/main/EternalLiberty.csv - Listado de APTs
        - https://blog.segu-info.com.ar/2021/03/conexion-entre-grupos-de-cibercrimen.html - Conexión entre grupos de cibercrimen: servicios, distribución y monetización

Entornos Vulnerables para Testing

- Webs:
    - https://www.flu-project.com/2019/11/7-recursos-para-iniciarse-en-CTFs.html - Para iniciarse con los CTFs
    - https://www.hackingarticles.in/ - Artículos y resolución de CTFs y vulnerabilidades, ideal para empezar en el mundo de los CTFs
    - https://ctftime.org/ - Listado de CTF actuales
    - Nivel inicial:
        - https://www.vulnhub.com/ - Materiales vulnerables para practicar
        - http://www.dvwa.co.uk/ - Damn Vulnerable Web Application (DVWA).
        - https://www.blog.binaria.uno/2019/04/02/que-es-dvwa-y-por-que-los-hackers-eticos-la-aman/ - ¿Qué es DVWA y por qué los hackers éticos la aman?
        - https://pentesterlab.com/
    - Nivel intermedio:
        - https://www.tryhackme.com/ - Orienta un poco por donde tirar
            - https://blog.segu-info.com.ar/2023/02/tryhackme-paso-paso.html - TryHackMe paso a paso…
        - https://hack.me/s/ - Más retos.
        - https://google-gruyere.appspot.com/ - Página web para intentar hackear.
        - https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project - Para descargar y usar en local.
        - https://www.root-me.org/?lang=es - Enorme colección de retos.
        - https://atenea.ccn-cert.cni.es/home - Atenea, plataforma de desafíos de seguridad del CCN-CERT
        - https://www.hackthissite.org/ - Comunidad con muchos retos.
        - https://overthewire.org/wargames/ - Tracks de retos.
        - https://hackingdojo.com/ - Pentesting labs.
        - https://tryhack.me/s/ - Más retos.
        - https://ctf.hacker101.com/ - Más retos y además te invitan a programas de bug bounty
- Nivel Avanzado:
    - https://www.hackthebox.eu/ - Pentesting Labs.
- Cryptografía
    - https://github.com/DamnVulnerableCryptoApp/DamnVulnerableCryptoApp/ - Aplicación con criptografía insegura
- Juegos
    - https://store.steampowered.com/app/365450/Hacknet/ - Juego de Windows y Mac, usado en algunas organizaciones para entrenar.

        - http://hacknet-os.com/
- Máquinas Virtuales
    - https://blog.segu-info.com.ar/2021/04/vvmlist-maquinas-virtuales-vulnerables.html - VVMlist: máquinas virtuales vulnerables
    - https://github.com/rapid7/metasploitable3 -VM Metasploitable3. → http://downloads.metasploit.com/data/metasploitable/metasploitable-linux-2.0.0.zip
        - The default login and password is msfadmin:msfadmin.
    - https://www.vulnhub.com/entry/exploit-exercises-nebula-v5,31/ - Nebula.
        - http://www.cyberry.co.uk/vulnhub/exploit-exercises-nebula-v5/ - Ejercicios de Nebula
- Otros
    - https://blog.segu-info.com.ar/2021/07/aplicacion-damn-vulnerable-bank-para.html - Aplicación «Damn Vulnerable Bank» para Android, para aprender hacking mobile
    - https://github.com/vavkamil/awesome-vulnerable-apps - Awesome Vulnerable Applications
- Cursos
    - https://www.pentesterlab.com/exercises/web_for_pentester/course - Web for Pentester.
    - https://www.hackplayers.com/2017/02/pentesterlab-web-for-pentester-1-xss.html - Instrucciones en Español.

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

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

Last update: **26/02/2025 08:40**