Apuntes SinCara Extras

Titulares/Resumen del curso

- Logística del curso
  - Este curso trata de tener una visión 360º de la ciberseguridad. Si quereis profundizar en algún tema, lo leeis con más calma, una vez sacada la certificación
  - Una vez terminado el curso: tests, tests y tests. Eso os permite ver vuestras deficiencias, estudiarlas, y presentaros al examen lo antes posible. Según pasa el tiempo, decrecen las posibilidades. No dejar pasar más de un mes.
- El activo más importante, y más protegido por ley, son los datos.
  - En ciberseguridad industrial, por contra, es la seguridad física.
  - Hay que estar muy actualizado con las novedades tecnológicas que van surgiendo.
- El factor más débil de la ciberseguridad, es el factor humano.
  - El mayor problema de ciberseguridad, son los insiders.
  - El mayor agujero de las contraseñas es la pregunta de seguridad.
  - Enviar fotocopias o escaneos de DNI es super mega peligroso.
  - El perfil más atacado es el del CFO, la directora de finanzas.
- Las redes no son confiables, ninguna. Hay que utilizar siempre cifrado.
  - El Wifi y la telefonía móvil se puede manipular, hay que usar VPN siempre.
  - El SMS es el 2FA más débil, se recomienda usar cualquier otro tipo de 2FA.
- El acelerómetro de los dispositivos es un espía.
- El mayor peligro de cualquier software son los componentes de terceros.

Culturilla Hacker

- https://tebs-game-of-life.com/ - El juego de la vida de John Conway. El deslizador se ha convertido en el emblema de los hackers.
  - https://ih1.redbubble.net/image.356679573.4598/flat,128x128,075,t.u1.jpg
- https://1337.me/ - Leet (1337), el idioma de los hackers.
  - https://es.wikipedia.org/wiki/Leet_speak - Artículo en la wikipedia.
- Fun
  - https://geekprank.com/hacker/ - Emulación de «consola de hacker».
  - http://geektyper.com/ - Emulación de «consola de hacker».
  - http://hackertyper.com/ - para «programar» como un hacker.
  - https://www.microsiervos.com/archivo/juegos-y-diversion/skynet-simulator.html - Un jueguecillo con ambientación hacker
  - en Linux hay un comando llamado «hollywood» que también hace una simulación de una Shell de hacker
- Historia
  - https://es.wikipedia.org/wiki/George_Hotz - La historia de GeoHotz, jailbrake de iPhone y el que «crackeo» el código para liberar y acceder a la parte Linux de PS3
  - https://hackstory.net/Main_Page - Historia de los Hackers
  - https://cuadernosdeseguridad.com/2020/12/historia-del-hacking-en-espana-hackers/ - Libro con la historia de los Hackers en España
  - https://www.amazon.es/Historia-del-hacking-en-espa%C3%B1a/dp/8499649866 - en Amazon
  - https://hackstory.net/Isla_Tortuga - La historia de Isla Tortuga

Distros y Máquinas Virtuales

- https://gbhackers.com/top-10-penetration-testing-ethical-hacking-linux-distributions/amp/ - Top 10 Best Operating System for Ethical Hacking & Penetration Testing – 2019

- http://blog.segu-info.com.ar/2021/12/bugbuntu-distro-con-herramientas-para.html - BugBuntu: distro con herramientas para Bug Bounty
- Páginas en la que podemos acceder a Máquinas virtuales online de distintos sistemas operativos, para probarlos:
    - https://www.onworks.net/ Algunas versiones de Linux y Windows, con conexión a red.
    - https://distrotest.net/ Cientos de versiones de Linux, incluyendo Kali, pero sin conexión a red.
- NETinVM - una MV (3,4GB) de VMware que a su vez contiene una veintena de MVs con sus redes.
    - https://informatica.uv.es/~carlos/docencia/netinvm/ - Página inicial (inglés).
    - https://informatica.uv.es/~carlos/docencia/netinvm/netinvm.html - Documentación en inglés.
    - https://cperez.blogs.uv.es/ - miniblog de uno de los creadores.
    - https://informatica.uv.es/~carlos/docencia/netinvm/es/netinvm-intro/netinvm-intro.html - Introducción y ejercicios en español.
- Windows
    - https://pentestbox.org/es/ - Conjunto de herramientas para instalar en Windows y convertirlo en un sistema para pentesting
    - https://github.com/mandiant/commando-vm - Commando VM, una distro de pentesting basada en Windows
    - https://developer.microsoft.com/es-es/windows/downloads/virtual-machines - Máquinas virtuales de Windows, proporcionadas por Microsoft. Suelen tener un tiempo de vida muy corto, al cabo del cual, te la vuelves a bajar.
    - https://www.microsoft.com/es-es/software-download/windows10ISO - ISO para instalar Windows 10.
        - https://www.hrkgame.com/es/games/product/windows-10-home-standard - Licencia para Windows 10 Home Standard por 3.51€ (OEM).
        - https://www.hrkgame.com/es/games/product/windows-10-professional-standard - Licencia Windows 10 Professional por 1.95€ (OEM)
    - https://www.dprojects.org/minios - Windows MiniOS, Windows modificados y aligerados por un particular. Usar bajo tu propia responsabilidad.

Libros y recopilaciones de recursos

- https://www.redeszone.net/tutoriales/seguridad/paginas-aprender-hacking-etico-internet/ - Páginas con las que puedes aprender hacking ético
- https://github.com/yeahhub/Hacking-Security-Ebooks - Top 100 Hacking & Security E-Books (Free Download).
- https://github.com/Hack-with-Github/Awesome-Hacking - Listado de recopilaciones «awesome» de recursos hacker
- https://github.com/trimstray/the-book-of-secret-knowledge - A collection of inspiring lists, manuals, cheatsheets, blogs, hacks, one-liners, cli/web tools, and more
- https://www.sans.org/blog/the-ultimate-list-of-sans-cheat-sheets/ - The Ultimate List of SANS Cheat Sheets
- https://learning.oreilly.com/ -
    - https://www.oreilly.com/library/view/ceh-certified-ethical/9781264269952/ - CEH Certified Ethical Hacker Practice Exams, 5th Edition (McGraw-Hill)
- https://github.com/Ignitetechnologies/Mindmap - Compendio de Mindmaps
- https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master - Payloads All The Things
- https://github.com/enaqx/awesome-pentest - Awesome Penetration Testing
- https://github.com/mantvydasb/RedTeaming-Tactics-and-Techniques/tree/master - Red teaming notes
- https://start.me/p/dlxe7M/esferared - Esferared

Medios, Blogs, Telegrams, Foros, para estar al día

- Telegram
  - https://t.me/Fwhibbit - Follow the White Rabbit: Comunidad en español bastante activa. Blog de la comunidad:
    - https://fwhibbit.es Unos 3.000 seguidores.
  - https://t.me/sombreroblanco - Sombrero Blanco, otra comunidad bastante activa. En este caso viene de una empresa de origen Chileno, su blog también es interesante:
    - https://www.sombrero-blanco.com/blog/ Unos 2.200 seguidores
  - https://t.me/seguridadinformatic4 - Seguridad Informática, unos 13.700 seguidores.
  - https://t.me/ThreatIntelligence - Canal de Noticias (no se puede escribir en él, solo leer), de la comunidad Ginseg:
    - https://ginseg.com/ 1.000 subscriptores.
    - https://t.me/ginseg - GINSEG - Comunidad de Ciberinteligencia Colectiva
  - https://t.me/HackingCiberseguridad - Hacking y Ciberseguridad, son un poco grises
  - https://t.me/burpsuitegroup - Canal de Burp Suite
  - https://www.hackplayers.com/2018/02/grupos-de-telegram-sobre-hacking-y.html - Enorme listado de grupos de Telegram en español.
  - https://t.me/todosloscanalestelegram - Canal de Telegram con miles de canales de todo tipo indexados.
  - https://t.me/iso27001hispano - Canal de Telegram con las ISO 27k
- Telegram - «Material Sensible»
  - https://t.me/freedomf0x - Freedom F0x
  - https://t.me/geeekgirls - Geek girls
  - https://t.me/Linux_and_hacking_material - Linux, Material de hacking y noticias
  - https://t.me/HackingCiberseguridad - Hacking y Ciberseguridad
  - https://t.me/joinchat/AAAAAEbWpV2DTbtdr5ZLXg - Ebooks Informática
- Noticias y Blogs
  - https://www.redeszone.net/ - Tienen una subsección especializada en seguridad. Muy activo.
  - https://blog.segu-info.com.ar/ - Argentino, muy activo.
  - https://thehackerway.com/ - Español, premiado como mejor blog técnico europeo en 2021 en la categoría de ciberseguridad.
  - https://derechodelared.com/ - Ciberseguridad, Privacidad, Derecho de las TIC
- Video
  - https://www.youtube.com/watch?v=Tlc2T3FjyPY - Ethical Hacker Fundamentals - Certificación Ethical Hacking Associate E|HA - PUE
  - https://downloads.pue.es/CEH-2020-05-27/20-CEH-WEBINAR-20200526T174544Z-001.zip - Los labs del video (59MB)
  - http://downloads.pue.es/CEH-2020-05-27/ClimbingOS.ova - La MV del video
- Foros
  - https://foro.elhacker.net/ -
  - https://discord.gg/u3dsh9M - Invitación al discord de Hacking Ético Hack4u, de s4vitar, válido solo para hoy.
  - https://discord.gg/hKyjmQ9Abm - Brigada OSINT, muy activo

EXAMEN

- Voucher del examen
  - El voucher del examen se consigue en el momento en que hacemos la encuesta del curso en el portal de Aspen de EC Council, os llega inmediatamente por email.
  - Ese voucher es para hacer el examen online, con una caducidad de un año.
  - Ampliar la duración del Voucher
    - Ampliar la duración del voucher activo durante 3 meses tiene un coste de 49$
    - Ampliar la duración del voucher activo o caducado durante 1 año tiene un coste de 99$
  - Cambio de fecha de un examen online desde casa
    - Si el primer cambio es con más de una semana de antelación, es gratuito
    - Si el primer cambio es con menos de una semana de antelación, tiene un coste de $49, a

pagar en el momento del cambio. Este coste no es reembolsable en ningún caso.
        - Si hay un segundo cambio de fecha, el coste es de $99
        - En caso de un tercer cambio o más, el coste es de $149
- Examen en si
    - Son 125 preguntas, a realizar en 4 horas.
    - El examen es en inglés.
    - No resta las preguntas mal contestadas, no dejéis ninguna sin responder.
    - Sólo hay una respuesta correcta.
    - Para aprobar, hay que sacar entre un 60% y 85% de respuestas correctas, depende del set de preguntas que te toquen.
    - Cuando se hace el examen, al responder, se marca como segura o dudosa la respuesta, y luego se pueden repasar por si quieres cambiar alguna respuesta.
        - https://cehtest.org - Ejemplo de Interfaz del examen
    - Es interesante también repasar siempre las 10 primeras.
    - No entregar nunca el examen antes de la primera hora.
        - Un alumno sacó casi un 100%, entregó en 1h y 15 min, y aún así le pidieron el CV y su perfil de Linkedin.
        - Lo que se comenta por los foros es que si tienes más de un 90% en un examen que piden un 70%, tienes casi todas las papeletas para que te auditen.
    - Cuando terminas el examen, te dice si has aprobado o no, a menos que detecten algo raro, y entonces un par de días laborables después, se ponen en contacto con vosotros.
    - Si te dicen que has aprobado, dos días laborables después, os mandan el certificado.
    - https://cert.eccouncil.org/wp-content/uploads/2024/04/CEH-Exam-Blueprint-v5.pdf - Preguntas por tema en el examen
        - Cada tema son 6 ó 7 preguntas.
        - https://cert.eccouncil.org/certified-ethical-hacker.html - Más info
- Recomendaciones
    - Haced el examen cuanto antes. Si pasa un mes desde la formación, se empiezan a olvidar cosas
    - El camino ideal hasta el examen es:
        - Haced test (Viktor de Udemy). Esto os mostrará como son las preguntas, y que carencias teneis.
        - Estudiar las carencias que tengais
        - Repetid los dos pasos anteriores hasta que os sintais cómodos, sin pasar de un mes desde la formación
        - Hacer el examen
- Test viktor de udemy
    - https://www.udemy.com/course/ec-council-ceh/ - El Practice Exam de Viktor Afimov en Udemy es muy recomendable. Cada poco tiempo hay ofertazas en Udemy, hasta gratuito, asi que si veis que cuesta 79€, esperad unos días a alguna oferta.
- Estudiar algún resumen de los temas de los que hay disponibles en GitHub
    - Ver megaresumen del Discord «OSCP y CEH». Está en la carpeta compartida.
        - https://discord.gg/aBYCGYyzn7 - Discord de estudio de las certificaciones OSCP y CEH
    - https://www.reddit.com/r/CEH/comments/nalyqi/here_are_my_comprehensive_study_notes_in_bullet/ - Chuletario de un forero que pasó el examen
        - https://github.com/undergroundwires/CEH-in-bullet-points - Enlace directo
        - https://github.com/Captain-Fancypants/CEH-in-bullet-points - El mismo chuletario en formato PDF
    - https://www.reddit.com/r/CEH/ - Reddit del CEH
- Tests de ejemplo
    - Gratis
        - Examen Online con 274 preguntas: https://www.onlineexambuilder.com/en/cehv11jan2021/exam-243845
        - https://www.examtopics.com/exams/eccouncil/312-50v11/view/ - 300 preguntas
    - de pago

        - https://www.passcollection.com/312-50v11_real-exams.html - Este volcado de preguntas del Examen (Dump), lo ponen muy bien en otros canales de exalumnos. Pero hay un batiburrillo de preguntas de versiones anteriores.
    - Apps para móvil o tablet, recomendadas por ex-alumnos
        - https://play.google.com/store/apps/details?id=com.abc.ceh - Android
        - https://play.google.com/store/apps/details?id=com.upnexo.certifiedethicalhacker - Android
        - https://apps.apple.com/es/app/ceh-v11-2021/id1583976039 - iOS
    - Material del curso:
        - https://www.ebook-converter.com/vitalsource-downloader.htm - Esta herramienta se supone que te permite bajar el contenido del curso desde la página de Vitalsource. Me la comentó uin alumno, pero no la he probado. Otro alumno lo ha probado y nos cuenta que básicamente es un plugin de Chrome, que una vez instalado, entras en la página de Vitalsource y te va pasando páginas y capturándolas. Eso si, el sistema le baneó durante unas horas, asi que lo detectan de alguna forma.
- https://www.eccouncil.org/wp-content/uploads/2022/09/Cyber-Handbook-Enterprise.pdf - Resumen de todos los cursos y tracks de EC Council
- Para hacer el examen desde casa, es recomendable utilizar un sistema recién instalado. Se puede utilizar un USB externo como por ejemplo:
    - https://www.amazon.es/gp/product/B07TSBR114?psc=1 - Carcasa USB-C 3.1 Gen 2 para NVMe
    - https://www.amazon.es/BENFEI-Carcasa-Unidad-Estado-Compatible/dp/B0C572RFLQ - La mia actual
    - Discos para la carcasa:
        - https://www.amazon.es/gp/product/B07VYG5HQD?psc=1
        - https://www.amazon.es/gp/product/B07JW49VZD?psc=1
        - https://www.amazon.es/Crucial-P1-CT500P1SSD8-s%C3%B3lido-Interno/dp/B07J2WBKXF
    - https://www.microsoft.com/es-es/software-download/windows10ISO - ISO para instalar Windows 10.
    - https://www.genbeta.com/herramientas/con-esta-herramienta-puedes-bajar-todos-los-isos-oficiales-de-windows-y-office-desde-los-servidores-de-microsoft - Programa para bajarte cualquier ISO de Microsoft
        - https://www.hrkgame.com/es/games/product/windows-10-home-standard - Licencia para Windows 10 Home Standard por 3.41€ (OEM). Es opcional, no hace falta la licencia.
        - https://www.hrkgame.com/es/games/product/windows-10-professional-standard - Licencia Windows 10 Professional por 1.95€ (OEM)
- Examen en un centro oficial Pearson VUE
    - https://www.pearsonvue.com/us/en/eccouncil.html - Examenes de EC Council
    - https://wsr.pearsonvue.com/testtaker/registration/SelectTestCenterProximity/ECCOUNCIL?conversationId=605857 - Localizaciones en Galicia
- Examen CEH Practical
    - Es un examen práctico con 20 problemas
    - Dura 6 horas
    - 550$
    - Los Labs te da todo lo que entra en el examen
    - Recursos
        - https://medium.com/@ome.murillo/examen-ceh-practical-2022-a82ae0fb48c0 - info
        - https://github.com/CyberSecurityUP/Guide-CEH-Practical-Master - Guía de preparación
        - https://github.com/Creanyx0/CEHv12-practical-Notes/blob/main/Elisa-Alises-NotesCEHv12.md - Notas de preparación del examen práctico
        - https://www.reddit.com/r/CEH/comments/kud9km/passed_cehpractical_today_2020/- Consejos
    - Yo compré los iLabs y con eso es suficiente . Hazlos todos comprendiéndolos . Luego en examen puedes consultar apuntes por lo que es conveniente mientras estudias, hacerte apuntes de cada herramienta y cuando la utilizarías . Hay preguntas en el examen que para poder hacerlas tienes que haber resuelto otras previamente .

Programa ECE

- Suscripción de renovación automática:
  - Los miembros certificados tendrán la opción de inscribirse en planes de renovación automática para sus cuotas anuales de CE, con opciones de suscripciones de 1 año, 2 años o 3 años.
- Validez de la certificación:
  - Los certificados serán válidos durante un año a partir de la fecha de certificación.
  - La fecha de caducidad de la certificación se prorrogará anualmente, hasta un máximo de 3, si se abonan las tasas CE (80$ anuales actualmente)
    - En caso de impago, la fecha de caducidad de la certificación no se modificará.
  - La fecha de caducidad se prorrogará anualmente previo pago de las tasas CE.
  - La renovación está sujeta a la realización de 120 créditos ECE durante tres años y al pago de las cuotas de CE durante los tres años. En este caso, empieza un nuevo ciclo de 3 años, con renovación anual.
- Créditos ECE
  - Los Créditos ECE se consiguen por realizar actividades relacionadas con la ciberseguridad, y reportándolas en el portal de ASPEN. Incluso la simple asistencia a un evento relacionado, una vez acreditado, te da créditos.
  - https://aspen.eccouncil.org/ECE/ViewECECategories - Créditos ECE que otorgan distintas actividades
  - Los créditos se suman a todas las certificaciones que tengas activas.
- Impago de las cuotas ECE (Nuevo):
  - Los miembros que no paguen sus cuotas de CE no podrán añadir/actualizar sus créditos ECE ni compartir insignias en las plataformas sociales.
  - Dichos miembros serán clasificados como «Inactivos»
- Transición para los miembros actuales:
  - Los miembros actuales seguirán con el sistema actual, pero pasarán a la nueva categoría de miembros una vez que completen su proceso de recertificación después del 1 de octubre de 2024.
  - Hasta entonces, el proceso actual de renovación y certificación permanecerá sin cambios.
- https://cert.eccouncil.org/continuing-education-fees.html - Información sobre el programa ECE

Otros formación, certificados

- https://infayer.com/archivos/583 - eJPT: eLearnSecurity Junior Penetration Tester por eLearnSecurity
  - https://my.ine.com/path/a223968e-3a74-45ed-884d-2d16760b8bbd - Penetration Testing Student
- https://en.m.wikipedia.org/wiki/List_of_computer_security_certifications - Listado de certificaciones
- https://start.me/p/Nx2YwX/formacion_ciberseguridad - Formación en ciberseguridad
- https://roadmap.sh/cyber-security - Roadmap ciberseguridad
- https://pauljerimy.com/it-career-roadmap/ - Carreras cyber, sueldos, siglas...