Apuntes SinCara sesión 5

Modulo 18 - IoT Hacking

- https://zumpad.zum.de/p/SinCara-ICS - ICS
- https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10 - OWASP Top 10 IoT 2024
- https://www.fcc.gov/oet/ea/fccid - FCC ID
- https://www.redeszone.net/noticias/redes/web-of-things-wot-que-es-funcionamiento/ - Web of Things (WoT): una capa que unifica y simplifica la comunicación entre dispositivos, usando tecnologías web como HTTP, REST y JSON.
- https://computerhoy.com/amazon/amazon-sidewalk-conecta-gratis-dispositivos-sin-internet-1222624 - Amazon Sidewalk ya cubre el 90%de la población de EEUU
- https://es.wikipedia.org/wiki/Azure_Sphere - Sistema operativo de Microsoft para IoT con kernel linux
- Herramientas
  - https://gurudelainformatica.es/un-nuevo-entorno-virtual-de-pentesting-para-dispositivos-iot - IoT-PT, máquina virtual para test de intrusión
    - https://github.com/IoT-PTv/IoT-PT - Página del proyecto IoT-PT
  - https://github.com/liuhuimin/awesome-iot-1 - Recopilación de recursos
- Noticias
  - https://www.incibe-cert.es/blog/vulnerabilidad-aurora-origen-explicacion-y-soluciones - Vulnerabilidad IoT, que 13 años después sigue sin parchearse.
  - https://www.xataka.com/internet-of-things/peores-ideas-meter-tecnologia-cosa-que-no-necesita-1 - Las 41 peores ideas de meter tecnología en una cosa que no lo necesita
  - https://www.youtube.com/watch?v=bR8RrmEizVg - Robo de coche usando unas llaves radiofrecuencia
  - https://www.bbc.com/mundo/noticias-49442319 - El origen de RFID en la Guerra Fría
  - https://www.elespanol.com/omicrono/hardware/20201121/robot-aspirador-convertirse-consiguen-hackearlos-grabar-distancia/537446597_0.html - Escucha remota a través de un Roomba, a pesar que no tiene micrófono
  - https://www.elmundo.es/tecnologia/2018/04/17/5ad4a14c46163f1f658b4630.html - Un hacker roba en un casino colándose a través de una pecera
  - https://www.theguardian.com/technology/2016/aug/10/vibrator-phone-app-we-vibe-4-plus-bluetooth-hack - vibrador «smart» que enviaba datos de uso al fabricante

Cacharricos

- Hardware
  - https://greatscottgadgets.com/ - HackRF
  - https://itsfoss.com/raspberry-pi-alternatives/ - MiniPCs (PIs)
  - https://beebom.com/best-raspberry-pi-zero-projects/ - 20 proyectos para Raspberry Pi Zero
    - https://hackaday.io/project/17598-diy-usb-rubber-ducky - Uno de ellos es hacerte un Rubber duck
  - Multiwireless portátil
    - https://pwnagotchi.ai/ - Pwnagotchi: Deep Reinforcement Learning for WiFi pwning!
      - https://dev.to/00xciara/how-i-built-my-pwnagotchi-48lj - Como construirte tu propio Pwnagotchi
    - https://www.kickstarter.com/projects/flipper-devices/flipper-zero-tamagochi-for-hackers?lang=es - Flipper Zero
    - https://github.com/CapibaraZero/fw - Capibara Zero
    - https://hak5.org/ - Tienda con cacharros de todo tipo
  - https://github.com/yadox666/The-Hackers-Hardware-Toolkit/blob/master/TheHackersHardwareTool

kit.pdf - The Hacker's Hardware Toolkit.
    - Mini ordenadores para IDS:
        - https://qotom.es.aliexpress.com/store/108231 Fabricante chino QOTOM de miniordenadores con modelos con múltiples RS232 y tarjetas de red.
        - http://qotom.net/product/ Página principal de Qotom
        - https://kansungmicropc.es.aliexpress.com/store/2131173 Fabricante chino KANSUNG de miniordenadores con modelos con múltiples RS232 y tarjetas de red.
        - http://www.kansung.com/ Página principal de Kansung
    - https://shop.netgate.com/products/2100-base-pfsense - Netgate SG-2100 Security Gateway with pfSense Software. 349€ + IVA

Modulo 19 - Cloud Computing

- Cloud
    - Netflix
        - https://en.wikipedia.org/wiki/Chaos_engineering - Chaos Monkey
            - https://harness.io/blog/chaos-engineering-tools/ - 5 Best Chaos Engineering Tools
        - https://spinnaker.io/ - El metagestor de clouds
    - Plataformas
        - AWS
            - https://www.linkedin.com/pulse/listado-de-todos-los-servicios-amazon-web-services-daniel-pe%C3%B1a-silva/ - Resumen de todos los servicios de AWS (se actualiza constantemente).
            - https://github.com/ine-labs/AWSGoat - AWSGoat
        - Azure
            - https://docs.microsoft.com/es-mx/learn/modules/intro-to-azure-fundamentals/tour-of-azure-services - Resumen de los servicios de Azure
            - https://github.com/ine-labs/AzureGoat - AzureGoat
        - GCP
            - https://medium.com/perezak/descripci%C3%B3n-general-de-servicios-ofrecidos-en-google-cloud-platform-6b88b4a8e217 - Resumen de los principales servicios de Google Cloud Platform
            - https://github.com/ine-labs/GCPGoat - GCPGoat
        - GAIA-X
            - https://es.wikipedia.org/wiki/GAIA-X - La nube europea
            - https://iotahispano.com/iota-en-gaia-x-4-la-movilidad-del-futuro/ - Descripción de GAIA-X
    - https://blog.segu-info.com.ar/2020/10/como-prevenir-las-11-amenazas-en-cloud.html - Cómo prevenir las 11 amenazas en Cloud Computing
    - Herramientas:
        - https://attack.mitre.org/matrices/enterprise/cloud/ - Matriz de MITRE ATT&CK para el Cloud
        - https://github.com/tanprathan/OWASP-Testing-Checklist - Adaptación a Cloud de la OWASP Web Security Testing Guide (WSTG)
        - https://cloudsecurityalliance.org/artifacts/security-guidance-v4-spanish-translation/ - Guía de seguridad para la nube
            - El PDF está descargado en el repositorio
        - https://grayhatwarfare.com/ - Buscador de Buckets en distintas nubes
    - https://hackingthe.cloud/ - enciclopedia de TTPs orientadas a las nubes públicas.
    - Noticias
        - https://www.genbeta.com/actualidad/empresa-espanola-ha-expuesto-24gb-datos-personales-millones-clientes-booking-expedia-otros-portales-reservas - Una empresa española ha expuesto 24GB de datos personales de millones de clientes de Booking, Expedia y otros portales de reservas.

- Contenedores
  - https://opensource.com/article/21/8/container-linux-technology - Las 4 tecnologías básicas para que funcionen los contenedores
  - https://dockerlabs.collabnix.com/docker/cheatsheet/ - The Ultimate Docker Cheat Sheet
  - https://devhints.io/docker - Docker CLI resumido
  - https://linuxcontainers.org/incus/ - Incus, fork de LXC
  - https://github.com/anchore/grype - Grype: A vulnerability scanner for container images and filesystems
- Serverless
  - https://impulsate.between.tech/serverless-que-es-ventajas - qué es y qué ventajas tiene
  - https://blog.mdcloud.es/arquitectura-serverless/ - Arquitectura serverless: qué es y qué no es
- Zero Trust
  - https://blog.segu-info.com.ar/2019/09/arquitectura-zero-trust-no-confiar-en.html - Arquitectura Zero Trust: no confiar en nadie en la red.
  - https://www.sealpath.com/es/modelo-zero-trust-ciberseguridad/ - Muy buen artículo acerca de Zero Trust
  - https://blog.segu-info.com.ar/2021/07/principios-de-disenos-de-arquitecturas.html - Principios de diseños de Arquitecturas Zero Trust
  - https://www.redeszone.net/noticias/seguridad/por-que-redes-zero-trust-proteger-mas-vpn/ - Por qué las redes de confianza cero pueden protegerte más que una VPN
- https://www.cloudflare.com/es-es/learning/access-management/what-is-a-casb/ - Qué es un CASB
- https://www.manageiq.org/ - ManageIQ, la base de Red Hat CloudForms (discontinuado), para gestionar entornos heterogéneos: Cloud, MV, contenedores, redes, almacenamiento, etc...

Modulo 20 - Cryptography

- Algoritmos
  - https://rakhesh.com/infrastructure/notes-on-cryptography-ciphers-rsa-dsa-aes-rc4-ecc-ecdsa-sha-and-so-on/ - Descripción de muchos algoritmos de cifrado.
  - https://www.redeszone.net/tutoriales/seguridad/criptografia-algoritmos-clave-simetrica-asimetrica/ - Varios algoritmos.
  - https://en.wikipedia.org/wiki/Secure_Hash_Algorithms - Seguridad de los algoritmos de Hash para cifrado de contraseñas
  - https://es.wikipedia.org/wiki/Advanced_Encryption_Standard - AES (También conocido como Rijndael).
  - https://en.wikipedia.org/wiki/PKCS - PKCS (Public-Key Cryptography Standards) se refiere a un grupo de estándares de criptografía de clave pública con cebidos y publicados por los laboratorios de RSA.
  - http://www.criptored.upm.es/ - Red Temática Iberoamericana de Criptografía y Seguridad de la Información, para la enseñanza de criptografía, y compartición de recursos a nivel Iberoamericano.
  - https://es.wikipedia.org/wiki/ROT13 - Una técnica de cifrado muy simple para foros y blogs
  - https://gchq.github.io/CyberChef/ - Web para codificar y decodificar toda clase de algoritmos
  - Noticias
    - https://blog.segu-info.com.ar/2024/08/nist-lanza-las-primeras-herramientas-de.html - NIST lanza las primeras herramientas de cifrado para resistir la computación cuántica
    - https://blog.segu-info.com.ar/2021/06/google-publica-bibliotecas-de-codigo.html - Google publica bibliotecas de código abierto para realizar cifrado homomórfico
    - https://academy.bit2me.com/que-es-blake3-algoritmo-hash/ - Blake3. El kernel de Linux y WireGuard usan Blake2
    - https://academy.bit2me.com/como-afecta-la-computacion-cuantica-en-bitcoin/ - ¿Cómo afecta la computación cuántica en Bitcoin?
- PKI: Public Key Infrastructure.
  - RA: Registration Authority.
    - Gestiona, Registra y verifica los nuevos Certificados.
    - La petición original la puede generar el propio usuario, o puede delegar en la RA que lo

haga.
        - Se encarga de verificar la identidad de quien registra un nuevo certificado.
    - CA: Certificated Authority.
        - Crea los Certificados, firmando la petición.
        - Teniendo el certificado de la autoridad CA, puedes verificar en local un certificado, pero no ver si está en vigor. OJO: En el curso, cuando dice que el CA valida los certificados, se refiere a este caso de uso, en local.
        - Para ver si está en vigor o revocado, tienes que tirar del VA, que es al que se conecta y mira si está en vigor.
    - VA: Validation Authority.
        - Valida la vigencia actual de los certificados.
    - TSA: TimeStamp Authority.
        - Autoridad de sellado de tiempo
        - Es la encargada de firmar documentos con la finalidad de probar que existían antes de un determinado instante de tiempo.
    - https://es.wikipedia.org/wiki/Infraestructura_de_clave_p%C3%BAblica - Infraestructura de clave pública
- TLS v1.3 pasa de 37 a 5 algoritmos válidos, se limpian todos los inseguros y obsoletos de v1.2 y anteriores.

```
Protocolo    Tiempo de vida
SSL 1.0        Sin publicar
SSL 2.0        1995 - 2011
SSL 3.0        1996 - 2015
TLS 1.0        1999 - 2020
TLS 1.1         2006 - 2020
TLS 1.2        2008 -
TLS 1.3        2018 -
```

    - https://superadmin.es/blog/que-es/tls1.3/ - TLS v1.3
    - https://www.ssllabs.com/ssltest/ - SSL/TLS Online Test
    - https://tls13.ulfheim.net/ - TLS Ilustrado (v1.3)
    - https://www.certificadosdigitales.net/diferencias-entre-ssl-dv-ov-ev/ - Diferencia entre los Certificados TLS DV, OV y EV
    - https://www.linuxito.com/seguridad/1087-analizar-la-seguridad-de-ssl-tls-con-testssl-sh - Recursos varios
    - https://github.com/drwetter/testssl.sh/releases - La última versión del script
    - https://www.eduardocollado.com/2020/12/13/encrypted-clienthello-ech/ - Encrypted ClientHello (ECH), El problema de TLS es que hay partes de la negociación que se realizan en claro, sin encriptar. Ello motiva que se puedan bloquear esas conexiones al saber a dónde te quieres conectar. ECH soluciona esto.
- SSH
    - https://github.com/jtesta/ssh-audit - Script para auditar los algoritmos que usa SSH, y la seguridad que da cada uno de ellos, con el objetivo de deshabilitar los más inseguros.
- Side Channel Attacks:
    - https://es.cointelegraph.com/news/research-team-demonstrates-hard-wallets-vulnerabilities-trezor-promises-firmware-update - Hardware wallets
    - https://retina.elpais.com/retina/2019/04/04/tendencias/1554377884_344087.html - Averiguar tu contraseña oyendo el sonido de las 'teclas'
    - https://www.microsiervos.com/archivo/seguridad/adivina-la-contrasena.html - Adivina la contraseña
    - https://xkcd.com/538/ - Ataque rubberhose (mediante coacción), también conocido como el ataque de los 5$
- Certificados Digitales

- https://www.xataka.com/basics/dni-electronico-vs-certificado-digital-cuales-diferencias - Diferencias entre el DNI-e y los certificados digitales
- https://play.google.com/store/apps/details?id=com.dnie_sign.certificado_digital&hl=es&gl=US - App de Android para crear tus propios certificados digitales
- https://cqesolutions.wixsite.com/tramite - App para gestiones con certificados digitales en España, tanto para Android como para iOS.
- https://es.wikipedia.org/wiki/Fiesta_de_firmado_de_claves - Key Signing Party, fiesta de firmado de claves
- https://keybase.io/ - Almacén público de claves públicas
- https://www.rediris.es/keyserver/index.html.es - Servidor de Red Iris para publicar claves públicas.