Apuntes SinCara sesion 3

Modulo 09

- El ser humano es el eslabón más débil de la cadena de la ciberseguridad
  - https://www.xataka.com/robotica-e-ia/ai-pin-ha-llegado-a-sus-primeros-usuarios-conclusiones-horripilantes - AI Pin
  - https://www.incibe.es/protege-tu-empresa/blog/luchando-ingenieria-social-el-firewall-humano - El Firewall Humano - La cadena de la ciberseguridad será tan fuerte como su eslabón más débil.
- La importancia de tus datos personales:
  - https://blog.segu-info.com.ar/2021/05/entrega-tus-datos-personales-y.html - Ofrecen dinero si entregas tus datos personales y credenciales por $500 + $25 al mes mientras sean válidos.
  - Suplantación de identidad a través de fotocopia o foto del DNI
    - https://www.xataka.com/seguridad/enviar-tu-dni-tal-cual-peligrosisimo-estos-tres-consejos-minimizan-riesgos-para-hacer-compras-reservas - Enviar tu DNI tal cual es peligrosísimo: estos tres consejos minimizan los riesgos para hacer compras o reservas
    - https://www.genbeta.com/actualidad/dar-tu-dni-wallapop-internet-te-puede-costar-meses-de-nuncias-juicios - Dar tu DNI en Wallapop e internet te puede costar un infierno de juicios y denuncias
    - https://www.cuatro.com/codigo-10/20230613/codigo-10-investigacion-dni-compraventa_18_09784716.html - Investigación compra venta de DNIs
    - https://saferlayer.com/ - Protege tus documentos con marcas de agua inteligentes y evita estafas
- Phishing
  - https://www.redeszone.net/tutoriales/seguridad/phishtank-comprobar-enlaces-phishing/ - PhishTank: descubre si un enlace es Phishing
  - https://getgophish.com/ - Para crear campañas de phishing
  - https://github.com/pentestgeek/phishing-frenzy - Otra herramienta para crear campañas de phishing
  - https://github.com/g0njxa/cazandophishing - Suplantaciones a bancos en España
- Ocultar URLs
  - https://www.hackplayers.com/2014/01/ataques-homografos-usando-dominios-internacionalizados.html - Ataque Homográfico.
    - https://www.apple.com/ - La página que NO es de Apple.
    - https://www.apple.com/ - La página que SI es de Apple.
    - https://es.wikipedia.org/wiki/Nombre_de_dominio_internacionalizado - Nombres de dominios internacionalizados. Sólo funciona en los hostnames, no en los emails.
    - http://www.irongeek.com/homoglyph-attack-generator.php - Generador de homoglifos.
  - Punycode:
    - https://www.wandera.com/punycode-attacks/ - Qué es el Punycode, y ejemplos de atques (en inglés).
    - https://unaaldia.hispasec.com/2021/10/punycode-es-utilizado-en-ataques-a-traves-de-google-ads-para-distribuir-malware.html - Como utilizan Punycode en ataques
    - Para configurar Firefox que nos muestre el Punycode, y evitar este tipo de ataques, hay que configurar:
      - network.IDN_show_punycode = true
      - network.idn.punycode_cyrillic_confusables = true
  - 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://www.genbeta.com/a-fondo/phishing-a-traves-tu-qr-qrishing-asi-funciona-esta-estafa-que-alerta-policia-espana - Phishing a través de tu QR o Qrishing
- Typosquatting y otras herramientas:
    - https://github.com/elceef/dnstwist - Para detectar dominios registrados que se parezcan al tuyo, para ver posibles ataques de impersonalización de tu web.
    - https://github.com/atenreiro/opensquat - Otra solución parecida a la anterior
    - https://www.hackplayers.com/2021/02/ditto-generar-dominios-homografos.html - Ditto: herramienta para generar variantes homógrafas de un dominio y comprobar cuales están disponibles.
- Chequear URLs no seguras:
    - https://www.virustotal.com/gui/home/url - Virus Total
    - http://www.getlinkinfo.com/ - Des-acortador de URLs
    - https://www.browserling.com/ - Navegador virtual, pones una url y acceden a ella. Para navegar de forma segura en un entorno controlado. Para comprobar URLs dudosas.
- Estafas:
    - https://blog.segu-info.com.ar/2020/10/audio-deepfake-suplantan-voz-de-ceo.html - Audio Deep Fake. Suplantan voz de CEO para realizar estafa
    - https://www.niusdiario.es/sociedad/sucesos/farmaceutica-zendal-victima-estafa-9-millones-euros_18_3052620088.html - Estafan 9 millones de € en una suplantación por email.
    - https://elpais.com/politica/2019/09/27/actualidad/1569591711_014709.html - Estafa del CEO en Valencia
    - https://www.youtube.com/watch?v=F78UdORll-Q - minuto 1:25 ejemplo de Vishing en un evento
    - https://blog.segu-info.com.ar/2024/02/roban-us-20-millones-traves-de-un.html - Roban U$S 20 millones a través de un engaño por DeepFake
    - https://blog.segu-info.com.ar/2024/06/estafa-de-la-videollamada-por-whatsapp.html - Estafa de la videollamada por Whatssap
- Creación de Perfiles Falsos:
    - https://www.fakenamegenerator.com/ - Creación de perfiles
    - Imágenes de perfil:
        - https://www.thispersondoesnotexist.com/ - Imágenes creadas por ordenador
            - https://thisxdoesnotexist.com/ - Recopilación de recursos varios que no existen
        - https://www.genbeta.com/imagen-digital/estos-modelos-no-existen-descarga-gratis-25-000-fotos-stock-generadas-ia - 25.000 fotos de personas, generadas por IA
    - https://amp.20minutos.es/noticia/4480381/0/corea-del-sur-presenta-a-la-primera-presentadora-de-informativos-creada-por-inteligencia-artificial/ - Corea del Sur presenta a su nueva y realista presentadora de informativos creada por inteligencia artificial
- Fun
    - https://www.youtube.com/watch?v=Kv7KWOjN8tw - ¿Cuál es tu password?

Modulo 10

- https://www.technologyreview.es/s/11102/tras-20-anos-del-primer-ddos-seguimos-desprotegidos-contra-ellos - Tras 20 años del primer DDoS seguimos desprotegidos contra ellos.
- https://www.redeszone.net/tutoriales/seguridad/que-es-ping-de-la-muerte/ - Ping de la muerte
- Ataques DDoS históricos
    - https://www.genbeta.com/actualidad/github-acaba-de-sobrevivir-el-ataque-ddos-mas-grande-de-la-historia - Ataque DDOS realizado a GITHUB.
    - https://blog.cloudflare.com/26m-rps-ddos/ - Ataque en junio de 2022 a CloudFlare de 26 millones de solicitudes HTTPS por segundo
    - https://blog.elhacker.net/2022/08/cliente-de-google-cloud-recibe-ataque-ddos.html - Ataque en

junio de 2022 a cliente de Google Cloud que recibió 46 millones de peticiones HTTPS por segundo
    - https://blog.segu-info.com.ar/2024/10/ataque-ddos-mas-grande-de-la-historia.html?m=0 - Ataque DDoS más grande de la historia abusa de Linux CUPS, routers Asus, MikroTik y DVRs. 3,8Tb por segundo
    - https://blog.cloudflare.com/es-es/ddos-threat-report-for-2024-q4/ - Informe de DDoS del 2024 de Cloudflare, e información del mayor ataque conocido hasta la fecha de 5,6Tb por segundo
- Mapas de ciberataques:
    - https://norse-corp.com/map/ - Recopilatorio de mapas de ciberataques en tiempo real
    - https://www.deteque.com/live-threat-map/ - Ataques de Botnets en tiempo real
    - https://threatmap.checkpoint.com/ - Ciberataques en tiempo real por Checkpoint
- Detección de Botnets:
    - https://www.incibe.es/ciudadania/herramientas/servicio-antibotnet - Servicio AntiBotnet
    - https://www.onyphe.io/ - Muestra si en una IP hay alguna BotNET funcionando (1 petición al mes en el plan gratis :/).
    - https://fwhibbit.es/descubrimiento-y-recopilacion-de-activos-con-onyphe-io
    - https://www.abuseipdb.com/ - Otro servicio parecido interesante
    - https://www.ipvoid.com/ - Otro más :)
- Noticias:
    - https://www.qore.com/articulos/6560/Stuxnet-y-el-nacimiento-de-la-ciberguerra - Historia del sabotaje del programa nuclear iraní
    - https://derechodelared.com/botnet-mariposa/ - Botnet Mariposa, muy interesante
    - https://www.wired.com/story/lockbit-ransomware-takedown-website-nca-fbi/ - Desmantelado el grupo criminal de Lockbit, revelando ganancias de más de 120 millones de $ en 2023. Mientras que en 2023 hubo unas ganancias globales de más de 1000 millones.
- Otras Variantes de ataques DoS:
    - https://www.redeszone.net/tutoriales/seguridad/que-son-ataques-rdos/ - Ataques Ransomware DoS (RDoS), exigencia de un rescate para no hacer DDoS a una empresa.
    - https://www.redeszone.net/tutoriales/seguridad/que-son-ataques-pdos-tdos/ - PDoS y TDoS
- CDNs
    - 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-le-das-al-play -Artículo brutal sobre el funcionamiento de Netflix en 2018
    - https://ipinfo.io/AS6752 - Sistema autónomo de Andorra
    - https://computerhoy.20minutos.es/redes/isp-throttling-como-saber-operadora-limitando-velocidad-conexion-sepas-1401929 - ISP Throttling

Modulo 11

- Ataques:
    - https://es.wikipedia.org/wiki/CRIME - CRIME Attack
    - https://www.hackplayers.com/2012/09/CRIME-ataque-SSL-TLS-sucesor-BEAST.html - BEAST, sucesor de CRIME
    - https://blog.ehcgroup.io/2021/07/26/10/55/56/11496/el-nuevo-ataque-de-retransmision-petitpotam-ntlm-permite-que-los-piratas-informaticos-se-apoderen-de-los-dominios-de-windows/herramientas-de-seguridad/windows/ehacking/ - PetitPotam
- https://connect2id.com/learn/token-binding - Token Binding: técnica que consiste en firmar digitalmente el token, mándarlo al al servidor, y verificar que la firma coincide. Es una evolución de TLS-OBC
- Para prevenir el secuestro de sesiones:
    - HTTP Strict Transport Security (HSTS)
        - https://es.wikipedia.org/wiki/HTTP_Strict_Transport_Security - HSTS obliga a usar HTTPS.

        - https://www.redeszone.net/tutoriales/seguridad/que-son-ataques-ssl-stripping-evitarlos/ - Ataque SSL Stripping y cómo evitarlo con HSTS
        - https://blog.desdelinux.net/httpa-un-protocolo-para-servicios-web-en-entornos-de-confianza/ - HTTPA, la evolución de HTTPS
    - HTTP Public Key Pinn (HPKP)
        - https://www.ionos.es/digitalguide/servidores/seguridad/hpkp-seguridad-para-el-certificado-ssltls/ - HPKP en desuso, substuido por:
        - https://es.wikipedia.org/wiki/Certificate_Transparency - Certificate Transparency (CT)
    - https://owasp.org/www-project-webgoat/ - Aplicación insegura para formación.
    - https://zumpad.zum.de/p/SinCara-IPsec - IPsec

Modulo 12

- Server Security Segment = DMZ
- https://community.broadcom.com/symantecenterprise/viewdocument/evading-nids-revisited - Resumen de varias técnicas de evasión de IDS
- NAC y Endpoint Security
    - VLAN Hopping: La suplantación de mensajes DTP (Dynamic Trunking Protocol (auto trunking)) del host atacante hace que el switch entre en modo trunking. Desde aquí, el atacante puede enviar tráfico etiquetado con la VLAN del objetivo, y el switch luego entrega los paquetes al destino.
        - En el tema 8 vimos:
            - Introduciendo un switch engañoso/rogue y habilitando enlaces troncales. El atacante puede acceder todas las VLANs del switch victima desde el switch rogue.
            - Otro tipo de ataque de salto a VLAN es el ataque doble etiqueta o doble encapsulado. Este ataque toma ventaja de la forma en la que opera el hardware en la mayoría de los switches.
    - Using Pre-authenticated Device: Los atacantes usan un dispositivo previamente autenticado, para saltarse el NAC. Un atacante puede usar un dispositivo, por ejemplo una RaspPi, para enrutar el tráfico a través del dispositivo comprometido.
    - Ghostwriting: Técnica que implica el deconstruir el binario del malware, para reconstruirlo de una forma distinta posteriormente, sin que afecte a su funcionalidad. Esto es para dificultar su detección, especialmente mediante la técnica de detección de firmas.
    - Using Application Whitelisting: Application Whitelisting es una funcionalidad de Windows para defenderse de la ejecución de aplicaciones maliciosas. Es una lista blanca de aplicaciones firmadas, que tiene permitido la ejecución en el sistema. Los atacantes usan técnicas como DLL Hijacking para invocar a las DLLs maliciosas desde aplicaciones autorizadas y saltarse esta defensa.
    - XLM Weaponization: Los atacantes usan hojas de cálculo Excel, con macros embebidas (XML - Excel Macro Language), para saltarse las protecciones. XML es un tipo de macro para Excel que permite automatizar tareas cuando el archivo es accedido.
    - Dechaining Macros: La técnica de «Dechaining» consiste en repartir la actividad entre distintas técnicas, distintos procesos, distintos periodos de tiempo, distintos usuarios, etc... para dificultar las posibilidades de ser detectado. Hay una gran cantidad de posibilidades cuando se aplica este concepto a las macros, ya que VBScript le permite cambiar archivos, memoria y el registro, proporcionando muchas formas de evitar el análisis estático y dinámico.
    - Clearing Memory Hooks: El enganche (Hook) es una técnica utilizada para modificar el comportamiento de un sistema operativo o una aplicación interceptando llamadas a funciones o mensajes pasados entre componentes de software. Básicamente es interceptar ciertas llamadas al sistema, para monitorizarlas o modificarlas. Los EDR, implementan Memory Hooks para recolectar información y hacer análisis basados heurísticos en el comportamiento. El atacante inutiliza esta técnica eliminado estos Memory Hooks.
    - Using Metasploit Templates: Los atacantes usan msfvenom para crear payloads maliciosos y analizarlos con VirusTotal para ver si lo identifica como malware. En base al resultado, modifica el

payload para reducir el ratio de detección.
    - Bypassing Symantec Endpoint Protection: El atacante usa herramientas específicas para evitar la detección de Symantec Endpoint Protection (SEP).
- VPN
    - https://www.vpnratings.com/ - Mejores VPNs
    - https://www.softether.org/ - VPN sobre HTTPS, o DNS, o ICMP, etc...
- Anonimizadores:
    - https://hide.me/en/proxy
    - https://www.redeszone.net/tutoriales/internet/listas-servidores-proxy-navegar-anonimamente/ - Proxys anónimos
- Como montarte tu propio IDS / Firewall en casa
    - https://www.redeszone.net/2016/03/26/security-onion-una-distribucion-linux-auditar-la-seguridad-una-red/ - Security Onion, una distribución Linux para auditar la seguridad de una red
        - https://securityonionsolutions.com/ - Security Onion
    - https://bitnami.com/stack/elk/virtual-machine - Máquina virtual con ELK ya instalado
    - https://github.com/dtag-dev-sec/tpotce - Parecido, pero con contenedores

Modulo 13

- https://zumpad.zum.de/p/SinCara-XSS - XSS, CSRF y SSRF
- https://www.redeszone.net/tutoriales/redes-cable/web-crawler-rastreadores-internet/ - Qué es web Crawler o rastreador y cómo funciona
- https://e00-elmundo.uecdn.es/elmundo/imagenes/2013/02/28/espana/1362057405_2.jpg - Imagen del robots.txt de la Casa Real de cuando lo de Urdangarín.
- Plugins para Navegadores:
    - https://thehackerway.com/2021/06/03/pentesting-en-tu-navegador-web-con-hacktools/ - HackTools, un conjunto de herramientas de pentesting para el navegador
        - https://github.com/LasCC/Hack-Tools - Página de HackTools
    - Chrome
        - https://chrome.google.com/webstore/detail/behave/mppjbkhgconmemoeagfbgilblohhcica - Información sobre la página, incluso te hace un escaneo de puertos
        - https://chrome.google.com/webstore/detail/wappalyzer/gppongmhjkpfnbhagpmjfkannfbllamg?hl=es - Wappalyzer para Chrome, browser extension that uncovers the technologies used on websites.
    - Firefox
        - https://addons.mozilla.org/es/firefox/addon/flagfox/ - FlagFox: Muestra la bandera del pais de la web, y más info
        - https://addons.mozilla.org/es/firefox/addon/wappalyzer/ - Wappalyzer para Firefox