# Apuntes SinCara sesión 2

## Modulo 06

- Kerberos:
  - https://www.tarlogic.com/es/blog/como-funciona-kerberos/ - Cómo funciona Kerberos
  - https://www.tarlogic.com/es/blog/como-atacar-kerberos/ - Ataques a Kerberos
  - Kerberos se divide principalmente en 5 pasos:
    - KRB_AS_REQ: El cliente requiere que el AS (Authentication Service) le proporcione un TGT (Ticket Granting Ticket), válido durante unas horas
      - TGT nos permite pedir TGS (Tickets de acceso a servicios)
    - KRB_AS_REP: Respuesta del AS con el TGT
      - KRB_TGS_REQ: El cliente requiere un ticket TGS (Ticket Granting Service)
      - KRB_TGS_REP: Respuesta con el TGS, válido durante unos segundos
        - KRB_AP_REQ: El cliente requiere acceso al servicio que quiere usar, utilizando el ticket TGS
  - Ataques a Kerberos:
    - AS-REP Roasting (Cracking TGT)
      - El ataque ASREPRoast se basa en encontrar usuarios que no requieren pre-autenticación de Kerberos. Lo cual significa que cualquiera puede enviar una petición AS_REQ en nombre de uno de esos usuarios y recibir un mensaje AS_REP correcto.
      - Esta respuesta contiene un pedazo del mensaje cifrado con la clave del usuario, que se obtiene de su contraseña.
      - Por lo tanto, este mensaje se puede tratar de crackear offline para obtener las credenciales de dicho usuario.
    - Kerberoasting (Cracking TGS)
      - Cualquier usuario válido dentro de Kerberos puede lanzar este ataque, consiguiendo una escalada de privilegios.
      - El ataque consiste en conseguir un listado de TGS de un usuario en concreto que tiene acceso a una aplicación en concreto.
      - Estos TGS incluyen un pedazo de datos cifrado con una clave derivada de la contraseña de dicho usuario, que pueden ser crackeada offline a posteriori.
      - https://blog.segu-info.com.ar/2024/12/que-es-un-ataque-de-kerberoasting.html
    - Pass the Ticket Attack
      - Este tipo de ataque es similar al Pass The Key, pero en lugar de utilizar los hashes NTLM para solicitar un ticket, el propio ticket es robado para autenticarse como su propietario. La manera de recolectar estos tickets varía en Windows y Linux.
    - NTLM Relay Attack
      - El atacante lanza un ataque de tipo Man-in-the-middle para interceptar y reutilizar el hash NTLM para autenticarse o crackear el hash para sacar la contraseña
- Contraseñas,emails, autenticación, algoritmos
  - https://password.kaspersky.com/es/ - cuanto se tarda en crackear una password.
  - https://www.hivesystems.com/blog/are-your-passwords-in-the-green - Tiempo en crackear una password
  - Filtraciones
    - https://blog.segu-info.com.ar/2024/07/rockyou2024-10-mil-millones-de.html - RockYou2024, recopilación de 10 mil millones de contraseñas únicas filtradas a lo largo de los últimos años, (45GB comprimido)
    - https://github.com/RickdeJager/stegseek - Crackeador de passwords mediante diccionario muy rápido (para usar con RockYou)
    - https://haveibeenpwned.com/ - Mi contraseña ha sido filtrada?
      - https://blog.elhacker.net/2022/07/falso-sitio-de-have-i-been-pwned-para-robar-credenciales-usuarios-incautos.html - Falso sitio de «Have I Been Pwned» para robar

credenciales de usuarios
        - https://www.malwarebytes.com/digital-footprint - Analizan tu huella digital.
        - https://blog.segu-info.com.ar/2020/12/analisis-estadistico-de-contrasenas.html - Análisis estadístico de contraseñas
- Buffer Overflow
    - https://www.welivesecurity.com/la-es/2014/11/05/como-funcionan-buffer-overflow/ - Buffer Overflow
    - https://hunasec.wordpress.com/2018/08/11/stack-based-buffer-overflow-sbbf-1/ - Explicación más técnica
    - https://revista.seguridad.unam.mx/numero23/uno-de-los-cl-sicos-buffer-overflow - Tipos, pero solo explica el de stack
    - malloc: Asignación dinámica de memoria en el Lenguaje de programación C
    - Stack (Pila) - LiFo (Last-in, First-out)
        - Generalmente utilizada para almacenar variables temporales durante la ejecución de un programa
        - Si una aplicación es vulnerable al desbordamiento del búfer basado en la pila, los atacantes toman el control del registro EIP para sustituir la dirección de retorno de la función por el código malicioso que les permite obtener acceso shell al sistema de destino.
        - Error del tipo Stack: Segmentation fault
    - Heap (Montón) - FiFo (First-in, First-out)
        - La memoria de montón se asigna dinámicamente en tiempo de ejecución durante la ejecución del programa y almacena los datos del programa.
        - El desbordamiento basado en la pila se produce cuando se asigna un bloque de memoria a una pila y se escriben datos sin ninguna comprobación de límites.
        - Esta vulnerabilidad conduce a la sobreescritura de punteros de objetos dinámicos, cabeceras de heap, datos basados en heap, tabla de funciones virtuales, etc.
        - Los atacantes explotan el desbordamiento de búfer basado en la pila para tomar el control de la ejecución del programa. A diferencia de los desbordamientos de pila, los desbordamientos de montón son inconsistentes y tienen diferentes técnicas de explotación
        - Error del tipo Heap: malloc(): corrupted top size
- Escalada de Privilegios
    - https://www.elladodelmal.com/2018/01/named-pipe-impersonation-escalando.html - Named Pipe Impersonation: Escalando privilegios en Windows
    - https://thehackerway.com/2023/12/13/herramientas-para-la-elevacion-de-privilegios/ - Herramientas para la elevación de privilegios
    - CPUs:
        - Spectre y Meltdown
            - https://es.wikipedia.org/wiki/Spectre_(vulnerabilidad%29 - Spectre
            - https://github.com/speed47/spectre-meltdown-checker - Script para saber si tu procesador es vulnerable a spectre y meltdown o derivados
            - https://www.grc.com/inspectre.htm - Aplicación para detectarlo en Windows
        - Intel Management Engine
            - https://www.enlacehw.com/minix-el-sistema-operativo-que-se-oculta-en-tu-procesador-intel/ - MINIX, el sistema operativo que se oculta en tu procesador Intel
            - https://en.wikipedia.org/wiki/Intel_Management_Engine - Intel Management Engine (ME)
            - https://github.com/corna/me_cleaner - Para limpiar o desactivarlo, aunque tiene riesgos
            - https://en.wikipedia.org/wiki/AMD_Platform_Security_Processor - AMD tiene algo parecido
- Spyware:
    - https://jbeex.com/multa-a-avast/ - Multa a AVAST por vender a terceros datos de los usuarios sin su conocimiento
    - https://hackaday.com/2019/02/18/wifi-hides-inside-a-usb-cable/ - Cable de carga keylogger, con

Wifi
        - https://shop.hak5.org/products/omg-cable - Para comprarlo
    - https://www.hackplayers.com/2024/12/malware-graba-video-con-led-apagado.html - Malware capaz de grabar vídeo con el led de la cámara apagado
    - Sonido:
        - https://www.lavanguardia.com/tecnologia/20170504/422279139232/smartphones-seguridad-ultrasonidos-privacidad-uxdt.html - Spyware mediante ultrasonidos
        - https://github.com/ggerganov/kbd-audio - Si tienen acceso al micrófono, pueden sacar los passwords tecleados
        - https://www.amazon.es/Privise%C2%A9-Bloqueador-micr%C3%B3fono-Protecci%C3%B3n-Smartphone/dp/B07L1QYVYF - Bloqueador de micrófono
- NTFS Streams:
    - Listar datastreams mediante linea de comandos: dir /R
    - NTFS Streams funciona en linux, pero hay que activar la opción «streams_interface=windows» al montar el FS
- Esteganálisis:
    - Los componentes son:
        - El mensaje transmitido
        - El algoritmo utilizado para codificar el mensaje
        - El stego-object en el cual está oculto el mensaje
        - La herramienta utilizada para crear el stego-object
        - El medio por el que se transmite el mensaje
    - Técnicas de descifrado:
        - Stego-only: Si solo tenemos el stego-object
        - Known-stego: Si tenemos acceso al stego-object, y conocimiento del algoritmo y del medio
        - Known-message: Conocimiento del mensaje y del stego-object
        - Known-cover: Conocimiento del medio y del stego-object
        - Chosen-message: Este ataque consiste en usar distintas herramientas con el mensaje conocido, para poder generar el stego-object y averiguar el algoritmo utilizado.
        - Chosen-stego: Acceso al stego-object y conocimiento del algoritmo.
        - Chi-square: El atacante utiliza análisis probabilístico para probar si el stego-object y el mensaje original coincide.
        - Distinguishing Statistical: analiza el algoritmo utilizado para detectar cambios estadísticos significativos, junto con la longitud de los datos incrustados
        - Blind Classifier: Conocido el mensaje, a través de un software especial, se analiza desde multitud de puntos de vista, para poder luego analizar mejor el stego-object
- Enlaces variados:
    - https://book.hacktricks.xyz/v/es/windows-hardening/windows-local-privilege-escalation/dpapi-extracting-passwords - DPAPI, Data Protection API
    - https://pberba.github.io/security/2021/11/22/linux-threat-hunting-for-persistence-sysmon-auditd-webshell/ - Hunting for Persistence in Linux
    - https://runcloud.io/blog/flush-dns-cache - How To Flush DNS Cache
        - Para ver el histórico de peticiones DNS en Windows: `ipconfig /displaydns | find «Record Name»`
        - Para borrar el histórico: `ipconfig /flushdns`
    - https://blog.elhacker.net/2022/03/tecnicas-de-intrusion-hacking-con-vectores-iniciales-poco-frecuentes.html - Ejemplos de vectores de ataque peculiares
    - https://github.com/bitsadmin/wesng - WES-NG

# Molulo 07

- Ransomware:
    - https://www.nomoreransom.org/es/index.html - Ayuda para luchar contra ransomwares.
    - https://www.hackplayers.com/2021/08/un-vistazo-al-kung-fu-de-conti.html - Análisis de Conti, una de las bandas RaaS (Ransomware-as-a-Service) más activas en los últimos tiempos, gracias a

datos filtrados por un afiliado descontento.
    - https://blog.segu-info.com.ar/2021/03/analisis-del-ransomware-ryuk.html - Análisis de Ryuk, que afectó al SEPE, por parte del CCN-CERT.
    - https://web.archive.org/web/20200527225511/http://www.zonavirus.com/noticias/2020/maquinas-virtuales-lo-ultimo-del-ransomware-para-esconderse.asp - Ransomware que instala una Máquina virtual para no ser detectado por la máquina física.
- Fileless:
    - https://www.welivesecurity.com/la-es/2019/12/05/fileless-malware-que-es-como-funciona-malware-sin-archivos/ - Qué es y cómo funciona el malware que no utiliza archivos
    - https://www.hackplayers.com/2021/03/entendiendo-los-ataques-con-wmi.html - WMI
    - https://telefonicatech.com/blog/lolbins-living-off-the-land-atacantes-emplean-tus-herramientas-provecho - Listados de binarios legítimos usados por malware de tipo fileless en Windows, Linux y Mac
        - https://lolbas-project.github.io/ - Windows
        - https://gtfobins.github.io/ - Linux
        - https://www.loobins.io/binaries/ - Mac
        - https://lolrmm.io - Remote Monitoring and Management (RMM) tools
        - https://lots-project.com/ - Dominios usados
        - https://filesec.io/ - Extensiones de archivo
        - https://www.loldrivers.io/ - Drivers
        - https://lottunnels.github.io/ - Living Off The Tunnels
        - https://malapi.io/ - APIs
        - https://wadcoms.github.io/ - WADComs is an interactive cheat sheet, containing a curated list of offensive security tools and their respective commands, to be used against Windows/AD environments.
- Sandboxes:
    - https://www.hackplayers.com/2020/04/listado-de-sandboxes-de-analisis-de-malware.html - Listado de sandboxes de análisis de malware gratuitos y online
    - https://github.com/kevoreilly/CAPEv2 - CAPEv2, es un derivado de Cuckoo Sandbox (actualmente abandonado). Es un script que se instala en una MV Ubuntu 20.04 LTS..
    - https://github.com/mandiant/flare-vm - Flare-VM, parecido a lo anterior, pero en Windows
- Análisis de ficheros:
    - https://blog.segu-info.com.ar/2020/01/herramienta-open-source-para-analizar.html - Microsoft ha publicado en GitHub una herramienta de análisis de código creada para ayudarnos a entender lo que hace un software y también lo que es. Su nombre es Microsoft Application Inspector.
    - https://www.virustotal.com/ - VirusTotal
    - http://virustotal.github.io/yara/ - YARA rules para analizar virus, creado por Virus Total
- Windows
    - https://www.elespanol.com/omicrono/software/20170101/ejecutar-programas-viejos-windows/182732154_0.html - Ejecutar un programa en Windows con una versión anterior del mismo
    - https://www.adslzone.net/esenciales/windows-10/ejecutar-programas-antiguos/ - ejecutar programas antiguos
    - https://www.hackplayers.com/2024/08/windows-downdate-downgrade.html - Windows Downdate: desactualiza tu Windows, y reporta que está actualizado.
    - https://es.wikipedia.org/wiki/Portable_Executable - Portable Executable (PE) es un formato de archivo para archivos ejecutables.
    - https://blog.elhacker.net/2022/05/documentos-microsoft-office-word-y-excel-permiten-infectar-malware-sin-macros.html - Documentos Word y Excel permiten ocultar malware sin necesidad de ejecutar macros
- Varios:
    - https://www.avast.com/es-es/c-computer-worm - Qué es un gusano
    - https://unaaldia.hispasec.com/2019/04/analisis-del-codigo-fuente-de-carbanak.html - Análisis del código fuente de un virus.
    - https://indetectables.net/ - foro de mlware.
    - https://dangerzone.rocks/ - Herramienta DangerZone, para manejar documentos sospechosos

    - https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-atp-linux - Microsoft Defender ATP for Linux
    - https://www.youtube.com/watch?v=_q0nt-dQtas - Video de David Sierra, instructor colaborador del PUE, en una charla de 4 horas sobre los tipos de Malware.

# Modulo 08

- https://www.redeszone.net/tutoriales/redes-cable/switch-vs-hub/ - Diferencias entre switch y hub
- https://es.wikipedia.org/wiki/Modo_promiscuo - Artículo acerca del modo promiscuo, y técnicas para detectarlo en la red
- https://medium.com/@marvin.soto/el-protocolo-irdp-posibilidad-de-spoofing-6a966dd5c8fd - El protocolo IRDP, ¿posibilidad de Spoofing?
- https://www.solvetic.com/tutoriales/article/1280-ataque-port-stealing-simple/ - Ataque de tipo port stealing
- ARP
    - https://www.ionos.es/digitalguide/servidores/know-how/arp-resolucion-de-direcciones-en-la-red/ - Cómo funciona ARP
    - https://www.redeszone.net/tutoriales/seguridad/que-es-ataque-arp-poisoning/ - Aprende todo sobre el ataque ARP Poisoning
    - https://capa3.es/dynamic-arp-inspection-prevencion-de-ataques-mitm.html - Dynamic ARP Inspection
    - https://es.wikipedia.org/wiki/Neighbor_Discovery - Neighbor Discovery (ND) protocolo de IPv6, equivalente al protocolo Address Resolution Protocol (ARP) en IPv4. Está integrado en ICMPv6.
- MACs
    - http://standards-oui.ieee.org/oui/oui.txt - Listado de fabricantes y sus MACs asociadas
    - https://www.ionos.es/digitalguide/servidores/know-how/direccion-mac/ - Todo acerca de las MACs
    - https://macaddress.io/ - Info acerca de una MAC
    - https://mac2vendor.com/ - Otro
- https://blog.haschek.at/2019/the-curious-case-of-the-RasPi-in-our-network.html - The curious case of the Raspberry Pi in the network closet.
- https://brsi.blogspot.com/2006/08/ataques-mitm.html - Varios tipos de ataques MITM
- Wireshark:
    - https://www.comparitech.com/net-admin/wireshark-cheat-sheet/ - Cheat Sheet
    - https://www.wireshark.org/docs/man-pages/tshark.html - TShark es la herramienta de Wireshark para línea de comandos. Funciona como tcpdump.
    - https://thehackerway.com/2024/02/26/filtros-utiles-en-wireshark-para-administracion-y-pentesting/ - Filtros útiles en Wireshark para administración y pentesting
- Nuevos proyectos de protocolos para internet:
    - https://www.redeszone.net/tutoriales/internet/que-es-http-3-quic/ - Qué es HTTP/3
    - https://www.tecnonews.info/noticias/huawei_y_el_gobierno_chino_proponen_una_nueva_arquitectura_de_internet - Huawei y el gobierno chino proponen una nueva arquitectura de Internet

## Tools

- Capsa Network Analyzer
- macof
- Wireshark