HERRAMIENTAS AUDITORIA SISTEMAS

Herramientas del Sistema operativo

- Usadas para gestión redes

Ping

- Ping (Packet Internet Groper) Permite comprobar el estado de la comunicación del host local con uno o varios equipos remotos de una red. Por medio del envío de paquetes ndel protocolo ICMP, diagnostica el estado, conectividad, velocidad y calidad de una red determinada.
- Ping es un comando del protocolo de capa 3 del modelo OSI ICMP, que son las siglas de Internet Control Message Protocol, que se encarga de revisar y notificar si hay errores en la comunicación entre dos host y/o redes. Para ello, ICMP envía 3 paquetes al destino, y en base a lo que suceda en el origen obtendrá una respuesta.
- Dentro de la cabecera de ICMP hay una serie de campo sque contienen código y tipo de respuesta, y según el valor que tengan tendremos un diagnostico.
- Para simplificar cuando hacemos un ping a un equipo, enviamos 4 paquetes, y esperamos recibir la confirmación por parte del destino de la recepción de esos cuatro paquetes, con lo que establecemos que tenemos conectividad con el equipo, como ves en el siguiente ejemplo.
- Las respuestas de ICMP pueden indicar otros estados, como por ejemplo host de destino inaccesible, host inalcanzable, etc.

Ping

- Este campo puede tomar los siguientes valores cuyo significado es:
- 0 Rspuesta de eco (Echo Reply).
- 3 Destino inaccesible (Destination Unreachable).
- 4 Disminución del tráfico desde el origen (Source Quench).
- 5 Redireccionar (cambio de ruta) (Redirect).
- 8 Solicitud de eco (Echo).
- 11 Tiempo excedido para un datagrama (Time Exceeded).
- 12 Problema de Parámetros (Parameter Problem).
- 13 Solicitud de marca de tiempo (Timestamp).
- 14 Respuesta de marca de tiempo (Timestamp Reply).
- 15 Solicitud de información (obsoleto) (Information Request).
- 16 Respuesta de información (obsoleto) (Information Reply).
- 17 Solicitud de máscara (Addressmask).
- 18 Respuesta de máscara (Addressmask Reply).

tracert

- Tracert nos permite conocer la ruta que siguen los paquetes hasta llegar a su destino y también es un comando del protocolo ICMP.
- También obtenemos una estadística del RTT, tiempos de ida y vuelta o latencia de red de esos paquetes, que corresponden al envío de 3 paquetes ICMP, ofreciendo una estimación de la distancia en saltos, o routers por los que se pasa, a la que están los extremos de la comunicación.
- Esta utilidad de diagnóstico de red determina la ruta a un destino mediante el envío de paquetes de eco de Protocolo de mensajes de control de Internet (ICMP) al destino.
- En estos paquetes, TRACERT usa valores de período de vida, conocido como TTL por sus siglas en inglés Time to Live. Dado que los enrutadores de la ruta deben disminuir el TTL del paquete como mínimo una unidad antes de reenviar el paquete, el TTL es, en realidad, un contador del número de saltos o routers por los que vamos pasando.
- Cuando el TTL de un paquete alcanza el valor cero, el router devuelve al equipo de origen un mensaje ICMP de “Tiempo agotado para esta solicitud”, ya que el paquete no ha podido llegar a su destino y ha expirado en tránsito.
- TRACERT es útil a la hora de solucionar problemas en redes propias donde tengamos varios routers y se pueden tomar varias rutas para llegar a un destino, de forma que podemos observar dónde podemos tener un problema en la red.

pathping

- Pathping es una mezcla de ping y tracert.

- Es más informativo, ya que nos devuelve también una serie de estadísticas, por lo que tarda más tiempo para ejecutar. Después de enviar los paquetes a un destino determinado, se analiza la ruta tomada y se calcula la pérdida de paquetes, proporcionando detalles entre dos hosts.

- Muestra la ruta a un host TCP/IP y las pérdidas de paquetes en cada enrutador del camino, además de información acerca de la latencia de red y pérdidas en saltos intermedios entre origen y destino.

- Pathping envía varios mensajes de solicitud de eco mediante el protocolo ICMP a cada enrutador entre un origen y destino durante un período de tiempo y, a continuación, calcula los resultados en función de los paquetes devueltos desde cada enrutador.
- El modificador -n Impide la resolución DNS de las direcciones IP, lo que acelera la presentación de los resultados.
- Con -h especificamos el número máximo de saltos para llegar al destino, el valor predeterminado es 30 saltos.

netstat

- Netstat me permite conocer las conexiones establecidas en el momento de su ejecución, indicando protocolo (TCP), direcciones en formato socket de origen y destino y el estado de la conexión.
- Un **socket** es el formato de dirección IP: puerto, es decir que lo que me quiere decir, en el siguiente ejemplo es que la dirección IP 172.26.1.236 se está comunicando a través del puerto 1447, con la dirección IP 151.101.2.109 mediante el puerto 443 que es correspondiente al protocolo https que aquí viene en formato texto en lugar del numérico.
- Visualizar todos los puertos abiertos y las conexiones activas con los puertos en formato numérico y mostrando el PID o ID de proceso, que podríamos usar junto con el administrador de tareas para identificar el proceso que corresponde a ese PID.
- Añadiendo el modificador **-b** podemos ver el ejecutable asociado.
- Existe una aplicación de entorno gráfico que también proporciona la información anteriormente citada y los ejecutables con sus dependencias, que es la aplicación de **Sysinternals (actualmente propiedad de Microsoft) llamada Process Explorer.**

whois

- Whois es un protocolo de comunicación, que almacenan información de registro sobre direcciones ip o dominios. Es un protocolo TCP.
- A través de whois podemos obtener cierta información sobre la organización, aunque a día de hoy poquito debido a la protección de datos, aunque en algunos casos con suerte puedes encontrar información sobre quien ha registrado un dominio, correos, teléfono, etc.
- Podemos hacer whois a una ip o a un dominio, y son cosas totalmente distintas, una es el registro del dominio y otra es el registro de la IP.
- El comando whois ya no funciona en Windows, si en Linux, pero existen multitud de aplicaciones online que nos facilitan esta tarea.

- Aplicaciones web para hacer whois:

- Netcraft: https://www.netcraft.com/
- Domaintools.com: https://whois.domaintools.com/
- ICANN: https://whois.icann.org/es

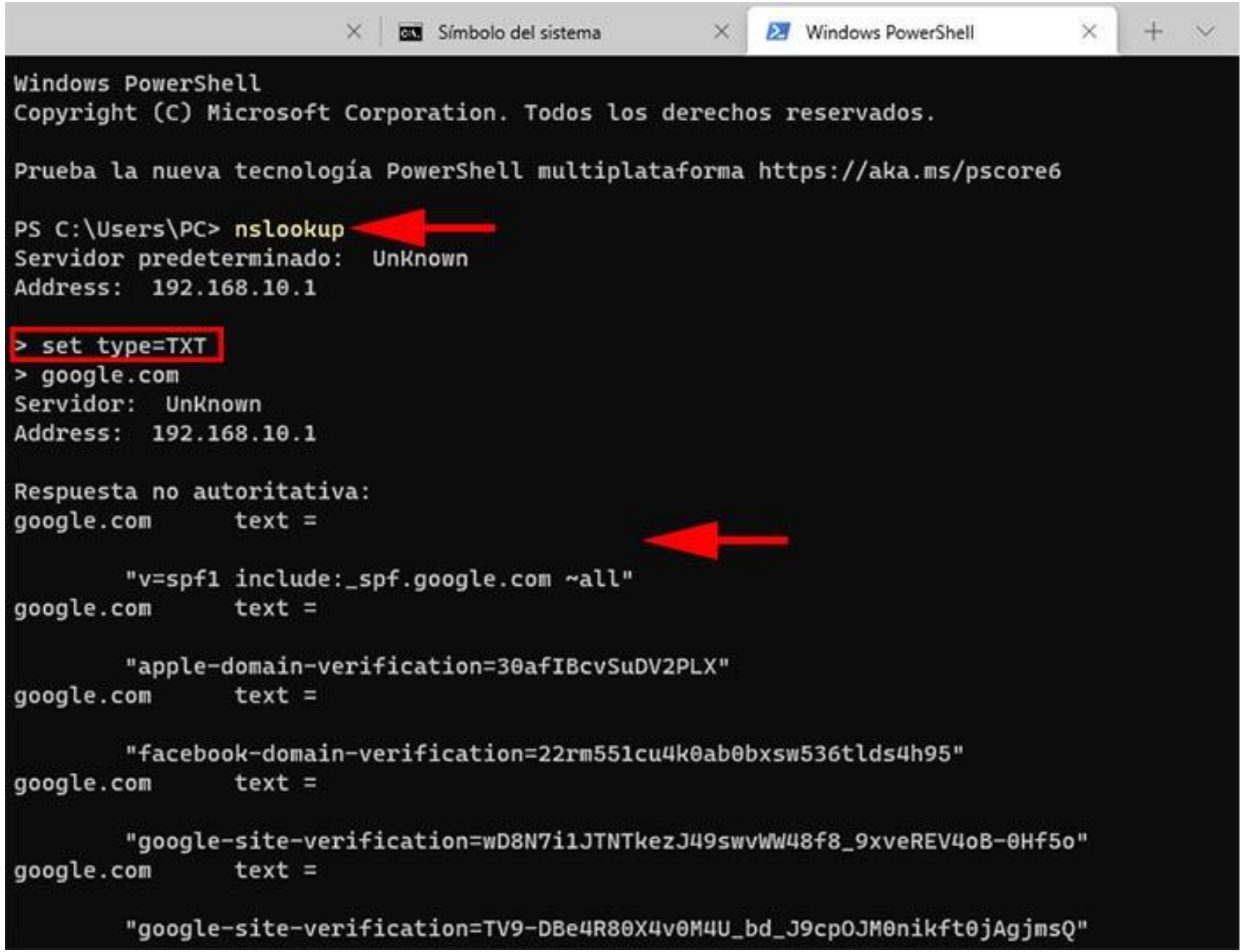
DNS ¿Qué ES?

- El DNS, o sistema de nombres de dominio, traduce los nombres de dominios aptos para lectura humana (por ejemplo, www.amazon.com) a direcciones IP aptas para lectura por parte de máquinas.

Proveedor	DNS Primario	DNS Secundario
Google	8.8.8.8	8.8.4.4
Quad9	9.9.9.9	149.112.112.112
OpenDNS Home	208.67.222.222	208.67.220.220
Cloudflare	1.1.1.1	1.0.0.1

nslookup

- Se emplea para conocer si el DNS está resolviendo correctamente los nombres de dominio y las IPs. También nos permite averiguar la dirección IP detrás de un determinado nombre de dominio.
- En principio, nslookup está pensado para las consultas de direcciones IPv4 e IPv6. Sin embargo, también nos permite conocer información de otros tipos registros DNS, para ello, una vez dentro de la aplicación escribimos set type y el registro que se quiere conocer sobre el nombre de dominio indicado en la segunda línea.
- La sintaxis :
  - set type=TIPODEREGISTRO
  - En la parte “TIPODEREGISTRO” se introduce el tipo de petición que se desea:
- **set type=A**, para buscar registros A que son los relacionados con la dirección IPv4..
- **set type=AAAA**, para buscar registros AAAA que son los relacionados con la dirección IPv6. Si una web utiliza direccionamiento IPv6 y nosotros también, entonces tendremos que indicar este registro DNS.
- **set type=PTR**, para buscar registros reversos.
- **set type=MX**, para buscar los registros Mail Exchange del correo.
- **set type=TXT**, para buscar registros de texto como SPF o DKIM.
- **set type=CNAME**, para buscar alias del dominio, esto también se conoce como subdominios, por ejemplo, el «www» siempre es un subdominio del principal» o el típico «ftp.» que es también un subdominio.
- Disponemos de herramientas nslookup online como ping.eu y centralops.net, además ambas ofrecen herramientas de red adicionales como Traceroute y Whois.


Símbolo del sistema
Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.
Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6
PS C:\Users\PC> nslookup
Servidor predeterminado: UnKnown
Address: 192.168.10.1
> set type=TXT
> google.com
Servidor: UnKnown
Address: 192.168.10.1
Respuesta no autoritativa:
google.com text =
"v=spf1 include:_spf.google.com ~all"
google.com text =
"apple-domain-verification=30afIBcvSuDV2PLX"
google.com text =
"facebook-domain-verification=22rm551cu4k0ab0bxsw536tlds4h95"
google.com text =
"google-site-verification=wD8N7i1JTNTkezJ49swvWW48f8_9xveREV4oB-0Hf5o"
google.com text =
"google-site-verification=TV9-DBe4R80X4v0M4U_bd_J9cpOJM0nikft0jAgjmsQ"

ipconfig

- Con ipconfig podemos realizar varias cosas mediante sus modificadores, pero lo más habitual es usarlo para conocer la configuración TCP/IP de una forma simple solo escribiendo ipconfig, nos devuelve nuestra IP, la máscara de red y puerta de enlace del router, y con ipconfig /all vemos una configuración más completa.
- También nos permite liberar y renovar las direcciones ip que han sido asignadas mediante un servidor dhcp con los modificadores /release, y /renew para todos los adaptadores de red o para uno específico.
- Ejemplos:
- Ipconfig :Muestra información TCP/IP de todos los adaptadores de red.
- ipconfig /all : Muestra información TCP/IP detallada de todos los adaptadores de red.
- ipconfig /renew. :Renueva la IP de todos los adaptadores asignada mediante dhcp.
- ipconfig /renew EL* :Renueva cualquier conexión cuyo nombre comience con EL.
- ipconfig /release *Con* :Libera todas las conexiones coincidentes, por ejemplo: “Conexión cableada Ethernet 1” o “Conexión cableada Ethernet 2”. Solo para direcciones IP asignadas mediante dhcp.
- Utilizar estos comandos es útil cuando a veces el servidor dhcp se queda “pillado” o cuando de pronto perdemos la conexión WIFI, no quiere decir que todas las soluciones sean estas, pero a veces ayuda.

- Windows almacena la cache de resolución DNS, es decir la relación que existe entre las direcciones IP y los sitios visitados con sus nombres de dominio, de forma predeterminada se renueva cada 24 minutos.

- IPCONFIG /displaydns: muestra el contenido de la caché de resolución DNS.
- IPCONFIG /flushdns: vacía la memoria caché de resolución DNS.
- IPCONFIG /registerdns: actualiza todas las concesiones DHCP y vuelve a registrar los nombres DNS.

Getmac

- obtiene la MAC del equipo donde se ejecuta.
- La dirección MAC es un identificador único para cada dispositivo de red de 48 bits conocida también como dirección física y que es única para cada dispositivo. Sus siglas vienen del inglés, y significan Media Access Control.
- Las direcciones MAC están formadas por 48 bits representados generalmente por dígitos hexadecimales, como cada hexadecimal equivale a cuatro binarios (48:4=12), la dirección acaba siendo formada por 12 dígitos agrupados en seis parejas separadas generalmente por dos puntos, aunque también puede haber un guion o nada en absoluto.
- un ejemplo de dirección MAC podría ser 00:1e:c2:9e:28:6b.

Cambiar la dirección MAC

- En linux
- Ifconfig.
- ifconfig nombredelainterfaz down.
- ifconfig nombredelainterfaz hw ether 91:75:1a:ec:9a:c7.
- ifconfig nombredelainterfaz up.
- /etc/init.d/network-manager restart.
- Microsoft Windows
- En Windows, no puede cambiarse la MAC por comandos, pero puede cambiarse en la configuración de la tarjeta de red en el Panel de control, o alterando el valor “NetworkAddress” en la clave HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}.
- En Kali Linux dispones de la herramienta Machanger

Arp : ¿Qué ES ARP?

- Address Resolution Protocol (Protocolo de resolución de direcciones) El primer protocolo a nivel de red es el ARP (Address Resolution Protocol - Protocolo de resolución de direcciones). ARP convierte dinámicamente las direcciones de Internet en las direcciones de hardware exclusivas de las redes de área local.

- A diferencia de la mayoría de protocolos, los paquetes **ARP** no tienen cabeceras de formato fijo. En lugar de ello, el mensaje está diseñado para ser útil con diferentes tecnologías de red.

- El kernel mantiene las tablas de conversión y el **ARP** no está directamente disponible a los usuarios o aplicaciones. Cuando una aplicación envía un paquete de Internet a uno de los controladores de interfaz, el controlador solicita la correlación de direcciones apropiada. Si la correlación no está en la tabla, se envía un paquete de difusión **ARP** a través del controlador de interfaz solicitante a los sistemas principales de la red de área local.
- Las entradas de la tabla de correlación **ARP** se suprimen después de 20 minutos; las entradas incompletas se suprimen después de 3 minutos.
- ARP es imprescindible para la transmisión de datos en redes Ethernet por dos razones: por un lado, las tramas de datos (también tramas Ethernet) de los paquetes IP solo pueden enviarse con ayuda de una dirección de hardware a los hosts de destino, pero el protocolo IP no puede obtener estas direcciones físicas por sí mismo.

Arp -a

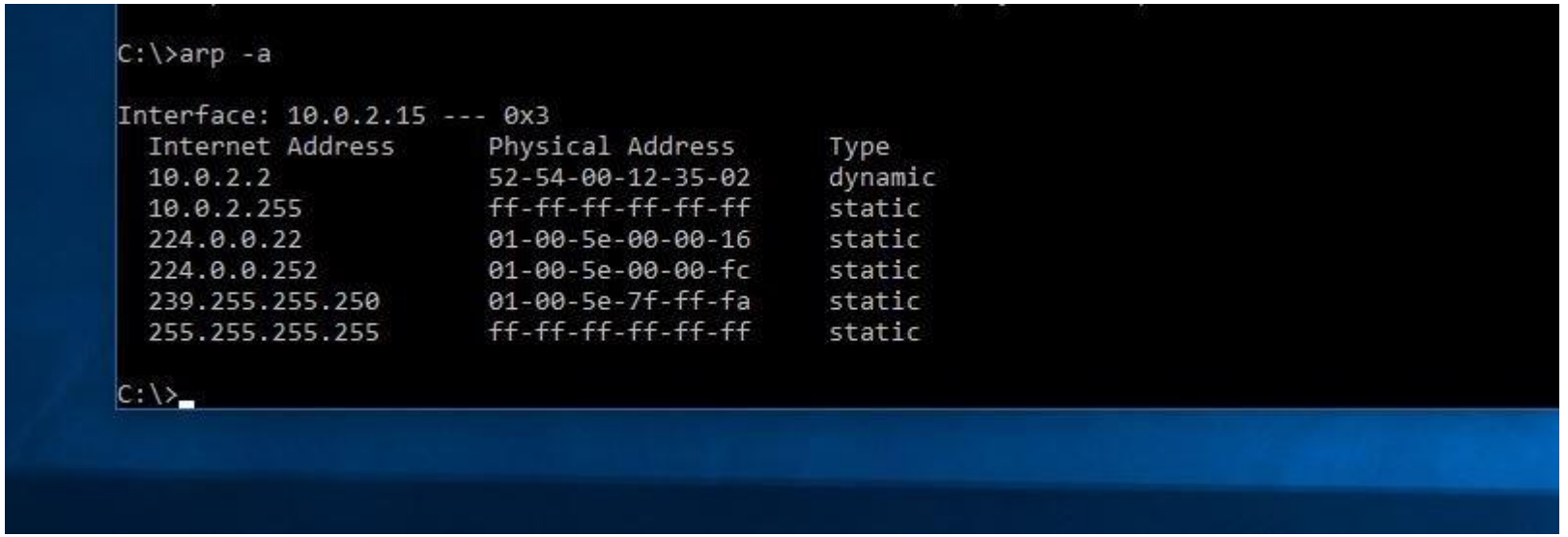
- El comando ARP resulta útil para visualizar la caché de resolución de direcciones, conocida como caché arp, que son básicamente los equipos con los que se ha comunicado mi equipo en la red (LAN).
- Muestra y modifica las tablas de traducción de direcciones IP a direcciones físicas usadas por el protocolo de resolución de direcciones ARP.

- En caso de querer añadir la combinación de direcciones de un host o eliminarla de la usaremos -s y -d. Se puede crear una nueva entrada estática con el siguiente comando:

- arp -s 10.0.2.15 00-aa-00-62-c6-09

- Para crear una entrada permanente en las tablas de correlación ARP, utilice el mandato arp con el parámetro pub:

- arp -s 802.3 host2 0:dd:0:a:8s:0 pub



- En caso de querer añadir la combinación de direcciones de un host o eliminarla de la tabla del protocolo ARP se necesitan los parámetros -s y -d. Si la dirección física 00-aa-00-62-c6-09 está oculta tras, por ejemplo, la dirección IP 157.55.85.212, se puede crear una nueva entrada estática con el siguiente comando:

- arp -a 157.55.85.212 00-aa-00-62-c6-09
- También se puede eliminar esta información de la caché si se recurre al parámetro “Delete” en una de las direcciones archivadas:

- arp -d 157.55.85.212
- En lugar de utilizar una dirección de Internet específica, también se puede optar por el símbolo del asterisco (*) para eliminar toda la información almacenada en la memoria caché.

netsh

- Netsh significa shell de red, permite modificar, administrar y diagnosticar la configuración de una red.

- Tenemos que ejecutarlo con permisos de administrador en la consola de comandos (CMD).

- Una vez hemos ejecutado el comando netsh, podemos ver su ayuda escribiendo help.

- Netsh, es una aplicación muy extensa, que nos permite configurar el firewall, especificar rangos de puertos dinámicos tanto para UDP como para TCP, ver claves WIFI almacenadas, configurar el protocolo TCP/IP, entre otras muchas acciones.

netsh

- **Asignar ip estática a una interfaz de red**
- netsh interface ipv4 set address “Wi-Fi”static 192.168.1.40 255.255.255.0 192.168.1.1
- Donde:
- Interface IPv4 indica el tipo de interfaz a configurar.
- Set address «Wi-Fi»: selecciona la dirección IP de la interfaz llamada en este caso «Wi-Fi».
- Static: indicamos que la dirección IP se asignará de forma fija o estática aportando los valores de IP, máscara y puerta de enlace del router.

- **Configuración de red de la interfaz Wi-Fi dinámica mediante DHCP.**
- netsh interface ipv4 set address “Wi-Fi” dhcp
- netsh interface ipv4 set dnsservers “Wi-Fi” dhcp

- **Mostrar la configuración solo para el interfaz de nombre Wi-Fi:**

- netsh interface ipv4 show address Wi-Fi
- netsh interface ipv4 show dns Wi-Fi

- **Ver perfiles de red Wi-Fi**
- netsh wlan show profiles

- **Desplegar los perfiles de una sola interfaz.**
- netsh wlan show profiles interface=”nombre_interfaz”

- **Conocer la configuración del adaptador Wi-Fi**
- Conocer en detalle la configuración del controlador es importante en tareas de soporte ya que nos permiten saber con el soporte necesario. Podemos ver detalles específicos tales como nombre, dirección MAC, tipo de red, versión Wi-Fi, canal actual, porcentaje de la señal, velocidad de recepción, etc.
- netsh wlan show interfaces

- **Recuperar claves de seguridad de perfiles almacenados**
- En algunas situaciones es posible que hayamos olvidado la clave de seguridad de un perfil WIFI:
- netsh wlan show profile name=”Perfil” key=clear

- **Borrar un perfil de red Wi-Fi**
- Si tenemos almacenados diversos perfiles a los que ya no nos conectamos, una solución es eliminarlos para evitar conexiones fallidas.
- netsh wlan delete profile name=”nombre de perfil”.

hostname

- El comando hostname es muy simple y no tiene modificadores, nos muestra el nombre del host, o lo que es lo mismo el nombre del equipo.

route

- El comando Route permite ver y modificar la tabla de rutas.

- **Route print** muestra todo el contenido de la tabla de enrutamiento IP.

- **Route add** se utiliza para añadir rutas a la tabla,
- **route delete** se utiliza para borrar rutas de la tabla.

nbtstat

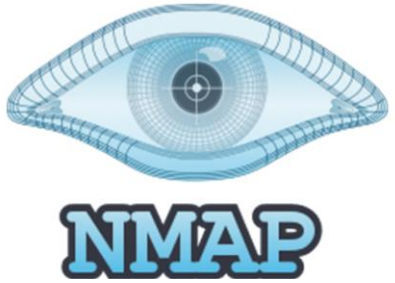
- Muestra estadísticas del protocolo y conexiones TCP/IP actuales utilizando NBT (NetBIOS sobre TCP/IP). NBTStat es una herramienta que resulta de utilidad para solucionar problemas con la resolución de nombres llevada a cabo por NetBIOS. es un servicio de red del nivel de sesión que se encarga de asociar los nombres a direcciones IP

- Nbtstat se puede usar en redes WiFi públicas para recopilar todas las direcciones IP y utilizarlas en la fase de recopilación de información llamada footprinting o en un ataque a cualquier dirección IP pública, se pueden usar para enumerar todas las conexiones TCP/IP en la máquina de Windows y para solucionar problemas con la resolución de nombres.

- -n: muestra nombres locales NetBIOS.

HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS: NMAP

Nmap



- Después de recopilar información sobre un objetivo, se debe pasar a otro paso que es escanear puertos.
- Nmap (la abreviatura de Network mapper) es el escáner de red más potente y utilizado.
- Es gratuito y de código abierto. Nos brinda la capacidad de realizar diferentes tipos de escaneos de red además de otras capacidades gracias a sus scripts nse que además podemos ampliar con los propios nuestros.
- Podemos descargarlo desde aquí: https://nmap.org/download.html
-

- Nmap es una herramienta con la que podemos escanear puertos y redes para comprobar que puertos están abiertos, servicios que corren tras esos puertos, si está el host detrás de un cortafuegos, el Sistema Operativo de los hosts en la red, las versiones de las aplicaciones que están detrás de los puertos, identificar equipos activos en la red, y obtener sus direcciones MAC, entre otras muchas más posibilidades.

- Tenemos una versión gráfica y una de comandos, Zenmap y Nmap, ambas tanto para Windows como para Linux

- Escaneo básico con NMAP

- El escaneo más básico que podemos hacer con Nmap, es poner nmap junto con el nombre de dominio a escanear, dirección ip o rango de direcciones o el nombre de equipo.

- Este escaneo nos devuelve la versión de nmap, fecha y hora del escaneo, internamente realiza una resolución de nombre de dominio, un Ping Arp Scan, para comprobar que el equipo está activo, y el escaneo donde se indica, puerto, estado del puerto (abierto, cerrado o filtrado) y servicio/protocolo que corre tras ese puerto.

- Escanear una IP: nmap 10.0.0.2
- Escanear varias IP no contiguas: nmap 10.0.0.2 10.0.0.10
- Escanear varias IP no contiguas separadas por comas: nmap 10.0.0.2,10,20
- Escanear un rango de direcciones IP: nmap 10.0.0.2-100
- Escanear una red completa con rangos de IP: nmap 192.168.1.1-255
- Escanear una red completa indicando la máscara de red: 192.168.1..0/24
- Escanear red completa:192.168.1.*
- Generalmente la mayoría de los escaneos de nmap se hacen a los 1000 puertos más importantes,

- Escanear un único puerto: Nmap -p 80 google.es
- Escanear varios puertos no contiguos separados por comas: Nmap -p 80,443 google.es
- Escanear un rango de puertos: Nmap -p 80-3000 google.es
- Escanear todos los puertos: nmap -p- Google.es
- Escanear todos los puertos especificando el rango: nmap -p 1-65535 google.es
- Escanear rango completo de puertos: nmap -p- Google.es
- Escanear puertos UDP (implica escaneo UDP): Nmap -sU -p U:53 google.es
- Escanear puertos TCP (implica escaneo TCP): Nmap -sT -p T:80
- Con la opción -vv nos muestra la razón por la que los puertos están abiertos, que es porque ha recibido un SYN-ACK.
- Con nmap - - iflist podemos listar todas las interfaces de red.

- **Existen varias opciones para detectar el sistema operativo del equipo remoto, una de ellas es usando -O.**
- SI a este escaneo anterior le añadimos - -osscan-guess, obtendremos mejores resultados.
- Para detectar las versiones de los servicios que corren tras los puertos, usamos -sV.

- **En el escaneo anterior podemos obtener más información usando - -verion-intensity pero deja más rastro en el sistema y logs de firewalls. Podemos poner valores de 0 a 5 siendo 0 un escaneo más ligero y 5 más ruidoso.**
- Nmap -sV - -version-intensity 5 10.0.2.15
- Se hace interesante volcar los resultados del escaneo en un archivo de texto, : nmap 192.168.1.17> c:\NmapEscaneo.txt,

- **Escaneo de Sistema Operativo y servicios: modo agresivo**

- Este escaneo, además, lanza una serie de scripts, descubre versiones y el sistema operativo.
- nmap -sS 192.168.1.17

- Mostrar los puertos TCP usados más comunes utilizando TCP SYN Scan
- TCP Maimon scan
- nmap -sM 192.168.1.1
- TCP Window scan
- nmap -sW 192.168.1.1
- TCP ACK scan:
- nmap -sA 192.168.1.1
- Stealthy scan:
- nmap -sS 192.168.1.1
- Mostrar los puertos TCP usados más comunes utilizando TCP connect scan
- nmap -sT 192.168.1.1

- Existen multitud de Scripts que puedes ejecutar para diferentes fines, como por ejemplo comprobar alguna vulnerabilidad específica, entre otras cosas, la sintaxis para poner un script es la siguiente:

- Nmap - -script= NOMBRE SCRIPT
- Los scripts los puedes encontrar en la carpeta de scripts de Nmap.

- Escanear haciendo MAC Spoofing

- nmap --spoof-mac [MAC-AQUÍ] 192.168.1.1
- Usar una MAC aleatoria. El 0 indica que nmap escoge la MAC:

- nmap -v -sT -PN --spoof-mac 0 192.168.1.1

- Enlace a vídeos NMAP: https://www.youtube.com/playlist?list=PL_tQGI-arXHp1qGJboawfhmpUCm8IsdfP

Otras herramientas

- **TCP Port Scanner:** que sólo escanea puertos TCP mediante el método SYN.
- **Netcat**: herramienta multipropósito, también llamada la “Navaja suiza” que tiene una función de escaneo de puertos, y que también se puede usar para establecer conexiones inversas o reversas con el equipo remoto.
- **Advanced Port Scanner:** escáner que verifica puertos abiertos con sus servicios.
- **NetScanTools**: una herramienta con múltiples utilidades para diferentes protocolos, ICMP, ARP, SNMP, DNS, entre otros.
- **Angry IP Scanner**: que además de escanear puertos también es capaz de buscar información NetBIOS, direcciones IP, detectar servidores web, etc.

HERRAMIENTAS DE ANÁLISIS DE VULNERABILIDADES.

- Un análisis de vulnerabilidades nos ayuda a:

- Identificar y clasificar fallos del software que comprometen la disponibilidad, integridad y confidencialidad.
- Ayuda a tomar decisiones a la hora de reemplazar, reparar o sustituir el hardware y software de la infraestructura tecnológica.
- Favorece la implementación de correctas configuraciones de software.
- Apoya la mejora continua de los controles de seguridad.
- Permite documentar los niveles de seguridad alcanzados con fines a la auditoría y el cumplimiento de las leyes, reglamentos y políticas que tiene que seguir la empresa.

Nessus

- Nessus es posiblemente una de las aplicaciones para analizar sistemas en busca de vulnerabilidades más conocida. (Es de pago)

- Una gratiuta : Nessus Essentials, Esta versión gratuita te permite analizar hasta 16 equipos y está disponible tanto para Windows como para Linux. (pide registro)

CVSS

- El CVSS es un sistema de puntuaje que Estima el impacto derivado de vulnerabilidades.

- Vulnerabilidad= debilidad explotada por una o más amenazas= riesgo de seguridad.

- Es un estándar FIRST (Forum of Incident Response and Security Teams) y se usa en bases de datos de vulnerabilidades como.

- NVDB (National vulnerability database).
- CVE (Common vulnerabilities and expoxures).
- OSVDB (Open source vulnerability database).

- Actualmente coexisten 2 versiones de CVSS que clasifican la severidad del riesgo de 0 a 10 de la siguiente forma:
- Enlace a Web NVD y métricas CVSS: https://nvd.nist.gov/vuln-metrics/cvss
- Enlace a Web Calculadora CVSS: https://nvd.nist.gov/Vulnerability-Metrics/Calculator-Product-Integration

MBSA

- En ocasiones, en el transcurso del análisis de vulnerabilidades en entornos Windows, puede resultarnos de utilidad conocer el nivel de parcheado del equipo que estamos analizando.
- MBSA (Microsoft Baseline Security Analyzer) permite conocer la falta de parches de seguridad, así como configuraciones de seguridad incorrectas. Su uso es limitado ya que se creó para Windows Server 2008 y no ha evolucionado mucho.

- MBSA puede analizar sirve para:
- Windows 2000, Windows XP, Windows 2003 y Windows 2008.
- Microsoft Internet Information Server (IIS) 5.0, 5.1, 6.0 y 7.0.
- Microsoft Internet Explorer 5.01, 5.5, 6.0 y 7.0.
- MBSA 2.3 no se está completamente actualizado para Windows 10 y Windows Server 2016, no obstante, es una herramienta que aún se usa.

- Descarga MBSA: https://www.microsoft.com/en-us/download/details.aspx?id=19892

OpenVas

- (Open Vulnerability Assessment System), un escáner de vulnerabilidades de uso libre utilizado para la identificación y corrección de fallas de seguridad. En la siguiente imagen puedes ver un reporte con los resultados de un escaneo.

- En el informe puedes ver con mayor detalle la vulnerabilidad identificada y evaluada, así como posibles soluciones.

- Enlace Web Descarga OpenVas y documentación: https://www.openvas.org/

ANALIZADORES DE PROTOCOLOS

Wireshark

- La herramienta más adecuada para monitorizar la red es definitivamente Wireshark. Wireshark es una herramienta gratuita y de código abierto que nos ayudará a analizar protocolos de red con capacidades de deep inspection. Brinda la capacidad de realizar capturas de paquetes online o análisis fuera de línea. Es compatible con muchos sistemas operativos, incluidos Windows, Linux, MacOS, FreeBSD y muchos más.
- Podemos descargarla desde aquí:: https://www.wireshark.org/download.html

Wireshark

- Wireshark se trata de un analizador de protocolos también conocido como sniffer de red de software libre, sucesor de Ethereal, que nos permite capturar y monitorizar los paquetes de red de una gran cantidad de protocolos que pasan por nuestro equipo poniendo la tarjeta de red a escuchar en modo promiscuo, o lo que es lo mismo, diciéndole a nuestra tarjeta que capture todo el tráfico que pase por ella.

- Es una herramienta que sirve muchas cosas, detectar problemas en la red, capturar información sensible de algunos protocolos como aquellos que son inseguros (sin cifrado), conocer sistemas operativos, versiones de aplicaciones, conocer la fecha y hora en la que se solicitó una web, resoluciones DNS, redirecciones, etc. Se trata de un potente sniffer de red de software libre heredero de Ethereal, que nos permite capturar y monitorizar todos los paquetes de red que pasan por nuestro equipo con el solo hecho de poner nuestra tarjeta de red a escuchar en modo promiscuo, es decir, diciéndole a nuestra tarjeta que capture todo el tráfico que pase por ella.

Otras apps

- CAIN Y ABEL

- Cain y Abel es una herramienta, ya discontinuada pero que aún se usa y que puede recuperar muchos tipos de contraseñas utilizando métodos como el sniffing de paquetes de red, también averiguar varios tipos hashes de contraseñas mediante cracking utilizando métodos como ataques de diccionario, fuerza bruta e incluso ataques basados en criptoanálisis.

- TCPDUMP

- TCPdump es un sniffer de red para Linux de línea de comandos, mostrando el tráfico capturado en tiempo real de paquetes transmitidos y recibidos

ANALIZADORES DE PÁGINAS WEB

OWASP ZAP

- OWASP (Open Web Application Security Project) es una metodología de aplicaciones web de las más usadas que busca el desarrollo seguro, la seguridad informática y especialmente la seguridad web. En su web puedes encontrar multitud de documentación para la seguridad web, desarrollo seguro, la propia metodología, etc.
- Dispone de herramientas enfocadas a la seguridad web como es OWASP ZAP, que empezó como un proyecto en el que teníamos un proxy donde podíamos ver las peticiones realizadas, pero esta herramienta ha crecido y permite hacer auditorias de seguridad de aplicaciones web tanto a nivel manual como automático.

- Dispone de una función Spider hace la enumeración completa de todos los enlaces de la web de forma automática, y nos va identificando donde hay formularios, subidas de archivos, etc., que pueden ser a los ojos de un auditor puntos clave para hacer auditorías de seguridad.
- Además, tiene funciones muy útiles como el escáner automático de fallos de seguridad.

- Este programa genera un reporte, en el menú tenemos la opción Reporte que podemos generar en diferentes formatos, XML, HTML, que es el más adecuado. Puedes guardarlo donde tú quieras, y al abrirlo se abre en el navegador.

- En alertas de sumario, aparecen las vulnerabilidades con su nivel de criticidad, alto, medio, bajo o informativo, en la parte de abajo nos describe el problema, las referencias para informarnos mejor y la solución.

- Enlace Web descarga OWASP ZAP: https://owasp.org/www-project-zap/

Acunetix

- Acunetix es un analizador de vulnerabilidades web capaz de detectar más de 7000 vulnerabilidades del tipo SQL Injection, secuencia de comandos entre sitios (XSS), contraseñas débiles, bases de datos expuestas y un largo etc., escaneando páginas web y aplicaciones web con tecnologías como, por ejemplo, Joomla, Wordpress, HTML5 o JavaScript. No dispone de versión gratuita, es de pago, pero podemos usar una prueba gratuita, disponible para Windows, Linux y MacOS.

- Los piratas informáticos concentran cada vez más sus esfuerzos en vulnerar páginas web, por lo tanto, es muy importante conocer sus vulnerabilidades, ya que las vulnerabilidades web permiten a los atacantes realizar actividades delictivas como, por ejemplo, phishing o transferir contenido ilícito.

ATAQUES DE DICCIONARIO Y FUERZA BRUTA TIPO BRUTUS, JOHN THE RIPPER

- Ncrack, Medusa o Hydra, que ya se encuentran en el framework de Kali Linux.
- Jphn the Ripper

Herramientas de uso comun

TheHive

- TheHive es una plataforma de respuesta a incidentes gratuita y de código abierto escalable y 4-en-1 diseñada para facilitar la vida de los SOC, CSIRT, CERT y cualquier profesional de la seguridad de la información que se enfrente a incidentes de seguridad que deban investigarse y actuar rápidamente. Gracias a Cortex, el potente motor de análisis gratuito y de código abierto, puede analizar (y clasificar) observables de forma escalable y utilizando más de 100 analizadores.
- Sitio web oficial: https://thehive-project.org

OSSIM

- OSSIM es un sistema de gestión de eventos e información de seguridad (SIEM) de código abierto. Fue desarrollado en 2003. El proyecto fue adquirido posteriormente por AT&T.
- Puedes descargarlo desde aquí: https://cybersecurity.att.com/products/ossim

The HELK

- Threat hunting, proyecto HELK. HELK fue desarrollado por Roberto Rodríguez (Cyb3rWard0g) bajo licencia GPL v3.
- El proyecto se creó en base a la pila ELK además de otras herramientas útiles como Spark, Kafka, etc.

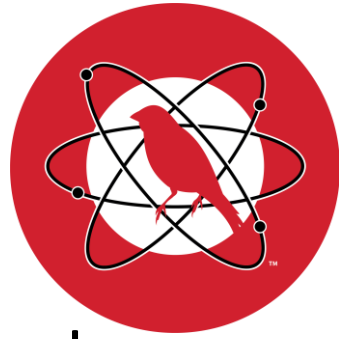
- Su sitio web oficial: Cyb3rWard0g/HELK: The Hunting ELK - GitHub

- El análisis de malware en memoria se usa ampliamente para la investigación digital y el análisis de malware. Se refiere al acto de analizar una imagen de memoria volcada de una máquina objetivo después de ejecutar el malware para obtener múltiples caracterísitcas de los artefactos, incluida información de red, procesos en ejecución, enlaces API, módulos cargados del kernel, historial de Bash, etc. Es un proyecto de código abierto desarrollado por Volatility Foundation. Se puede ejecutar en Windows, Linux y MacOS. Volatility admite diferentes formatos de volcado de memoria, incluidos dd, formato Lime, EWF y muchos otros archivos.
-
- Podemos descargar Volatility desde aquí: https://github.com/volatilityfoundation/volatility

Demisto Community Edition

- Security Orchestration, Automation and Response o simplemente SOAR son plataformas y herramientas muy efectivas para evitar la fatiga de los analistas al automatizar muchas tareas de seguridad repetitivas. Una de las plataformas más conocidas es Demisto. La plataforma también ofrece muchos playbooks gratuitos.
- Podemos descargar la edición comunidad desde aquí: https://www.demisto.com/community/

Atomic Red Team



- Atomic Red Team permite que cada equipo de seguridad pruebe sus controles mediante la ejecución de "pruebas atómicas" sencillas que ejercen las mismas técnicas utilizadas por los adversarios (todas mapeadas al framework ATT&CK de Mitre)
- Su sitio web oficial:https://github.com/redcanaryco/atomic-red-team

Caldera

- Otra herramienta de simulación de amenazas es Caldera. CALDERA es un sistema de emulación de adversarios automatizado que realiza un comportamiento de post-explotación de adversarios dentro de las redes empresariales. Genera planes de operación utilizando un sistema de planificación y un modelo adversario preconfigurado basado en el proyecto *Adversarial Tactics, Techniques & Common Knowledge* (ATT&CK™).
-
- Su sitio web oficial: https://github.com/mitre/caldera

Suricata

- Los sistemas de detección de intrusos son un conjunto de dispositivos o piezas de software que juegan un papel muy importante en las organizaciones modernas para defenderse de intrusiones y actividades maliciosas. La función de los sistemas de detección de intrusos en red es detectar anomalías en la red al monitorizar el tráfico entrante y saliente. Uno de los IDS más utilizados es Suricata. Suricata es un IDS/IPS de código abierto desarrollado por la Open Information Security Foundation (OISF)
- Su sitio web oficial: https://suricata.io
-

Zeek (formalmente Bro IDS)

- Zeek es uno de los NIDS más populares y potentes. Zeek fue conocido antes por Bro. Esta plataforma de análisis de red está respaldada por una gran comunidad de expertos. Por lo tanto, su documentación es muy detallada y buena.
- Su sitio web oficial: https://www.zeek.org

OSSEC

- OSSEC es un potente sistema de detección de intrusos basado en host. Proporciona detección de intrusos basada en registros (LID), detección de rootkits y malware, auditoría de cumplimiento, monitorización de integridad de archivos (FIM) y muchas otras capacidades.
- Su sitio web oficial:https://www.ossec.net

OSQuery

- OSQuery es un framework que es compatible con muchos sistemas operativos para realizar análisis y monitorización del sistema mediante consultas simples. Utiliza consultas SQL.
- Su sitio web oficial:https://www.osquery.io
-

AccessData FTK Imager

- Las imágenes forenses son una tarea muy importante en el análisis forense digital. La generación de imágenes consiste en copiar los datos con cuidado para garantizar su integridad y sin omitir un archivo porque es muy importante proteger la evidencia y asegurarse de que se maneje correctamente. Es por eso que existe una diferencia entre la copia normal de archivos y la creación de imágenes. Las imágenes capturan todo el disco. Al crear una imagen de la unidad, el analista crea una imagen de todo el volumen físico, incluido el registro de arranque maestro. Una de las herramientas utilizadas es "AccessData FTK Imager".
- Su sitio web oficial: https://accessdata.com/product-download/ftk-imager-version-4-2-0

Cuckoo

- El análisis de malware es el arte de determinar la funcionalidad, el origen y el impacto potencial de una muestra de malware determinada, como un virus, un gusano, un troyano, un rootkit o una puerta trasera. Como analista de malware, nuestra función principal es recopilar toda la información sobre el software malicioso y tener una buena comprensión de lo que sucedió con las máquinas infectadas. El sandbox de malware más conocido es cuckoo.
- Su sitio web oficial:https://cuckoo.sh/blog/

CAPE

- CAPE (Configuration And Payload Extraction) Es otra sandbox que se derivó de Cuckoo con el objetivo de agregar el desempaquetado automatizado de malware y la extracción de configuración. El desempaquetado automatizado permite la clasificación basada en las firmas de Yara para complementar las firmas de red (Suricata) y de comportamiento (API). Hay una instancia de comunidad gratuita en línea que cualquiera puede usar: https://capesandbox.com
- Repositorio: https://github.com/kevoreilly/CAPEv2

MISP

- Malware Information Sharing Platform o simplemente MISP es una plataforma de threat sharing de código abierto donde los analistas colaboran y comparten información sobre las últimas amenazas entre ellos. El proyecto fue desarrollado por Christophe Vandeplas y está bajo licencia GPL v3.
- Su sitio web oficial:https://www.misp-project.org

Ghidra

- Otra gran herramienta de ingeniería inversa es Ghidra. Este proyecto es de código abierto y lo mantiene la NSA. Ghidra brinda la capacidad de analizar diferentes formatos de archivo. Es compatible con Windows, Linux y MacOS. Necesitamos instalar Java para poder ejecutarlo. El proyecto viene con mucha documentación y cheatsheets. Además, nos da la posibilidad de desarrollar nuestros propios complementos utilizando Java o Python.
- Su web oficial es: http://ghidra-sre.org

Snort

- Otro potente sistema de detección de intrusos basado en la red es Snort. El proyecto está muy desarrollado, bien documentado y cuenta con el respaldo de Cisco y una gran comunidad de expertos en seguridad de redes.
- Su sitio web oficial: https://www.snort.org
-

Security Onion

- sistema operativo listo para usar que contenga muchas de las herramientas mostradass anteriormente, simplemente puedes descargar Security Onion. IT es una distribución de Linux gratuita y de código abierto para la detección de intrusos, la supervisión de la seguridad empresarial y la gestión de logs.
- Su sitio web oficial: https://github.com/Security-Onion-Solutions/securityonion/