THE BRIDGE

CYBER SECURITY

Ataques a Infraestructuras y redes

Conceptos de redes

- **Puerto:**
  - Interfaz lógica que permite proporcionar un servicio.
  - Es un número que se utiliza para identificar de forma exclusiva una transacción a través de una red, especificando tanto el host como el servicio. Son necesarios para diferenciar entre muchos servicios IP diferentes, como el servicio web (HTTP), el servicio de correo (SMTP) y la transferencia de archivos (FTP).
  - Cualquier aplicación o servicio que usemos, desde videojuegos, gestores de correo electrónico, mensajería instantánea o incluso el propio sistema operativo, siempre tienen una serie de puertos abiertos transmitiendo o escuchando lo que sucede a su alrededor
- **Servicio**
  - Funcionalidad que proporciona un sistema.
- **Servidor**
  - Es un sistema que proporciona recursos, datos, servicios o programas a otros ordenadores, conocidos como clientes, a través de una red.
  - En teoría, se consideran servidores aquellos ordenadores que comparten recursos con máquinas cliente.

Conceptos de redes

- **Tipos de puertos:**
  - **Puertos conocidos:** De 0 al 1023, están reservados por la IANA para determinado tipo de aplicaciones (servidor HTTP, FTP, etc.) y se requiere de privilegios de administrador en una máquina para activar una aplicación en uno de estos puertos. Un ejemplo es el puerto 80(HTTP).
  - **Puertos registrados**: de 1024 a 49151, reservados para aplicaciones concretas. Un ejemplo es el 3306(MySQL).
  - **Puertos privados/dinámicos**: de 49152 a 65535, estos no están reservados para ninguna aplicación concreta.

- **Estados de los puertos a nivel simplificado**:
  - **Puerto filtrado**: Un firewall (cortafuegos) bloquea el acceso al puerto.
  - **Puerto cerrado**: El puerto no está bloqueado, pero no hay ninguna aplicación escuchando en él.
  - **Puerto abierto**: El puerto no está bloqueado y hay una aplicación escuchando en él.

Puertos bien conocidos de TCP/UDP

Puerto preasignado	Protocolo	Aplicación
80	TCP	HTTP
21	TCP/UDP	FTP
23	TCP/UDP	Telnet
25	TCP/UDP	SMTP
110	TCP/UDP	POP3
119	TCP/UDP	NNTP
137	TCP/UDP	serv. de nombres NetBIOS
161	TCP/UDP	SNMP
194	TCP/UDP	IRC
389	TCP/UDP	LDAP
396	TCP/UDP	NetWare sobre IP
458	TCP/UDP	Apple QuickTime
500	TCP/UDP	ISAKMP

https://ayudas-it.blogspot.com/2009/10/puertos-mas-conocidos-de-tcpudp.html

SSH

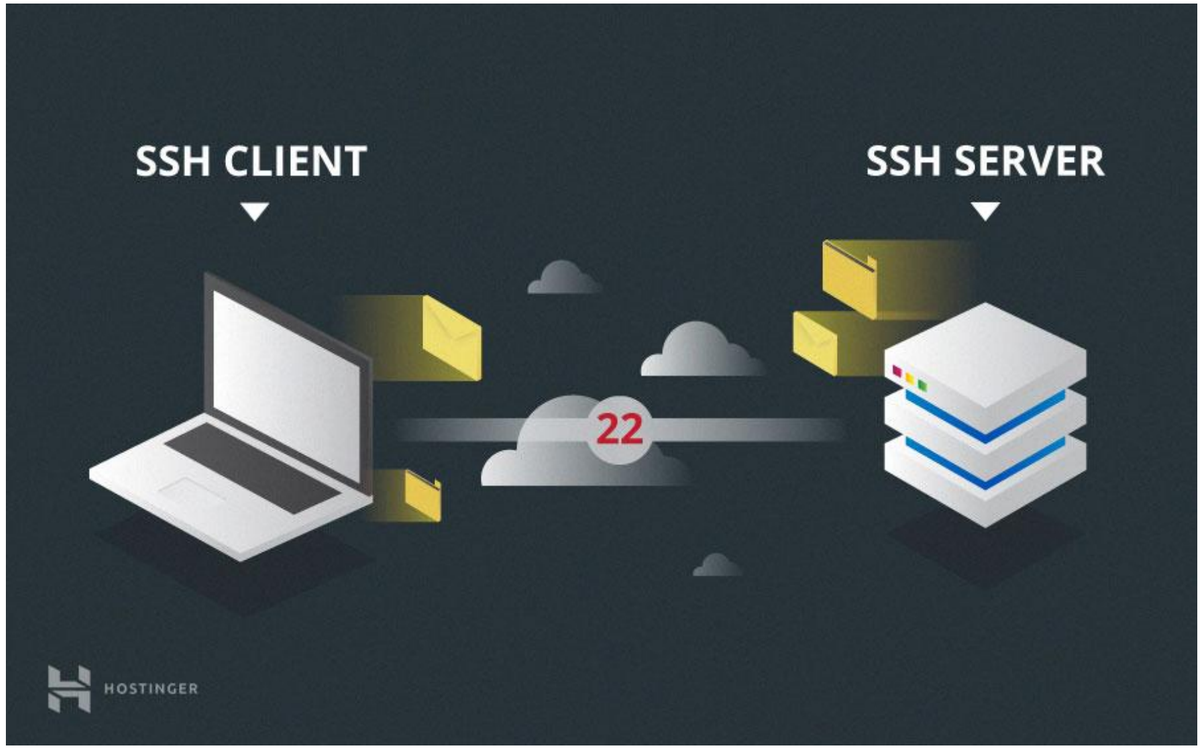
- **Secure Shell**, es un protocolo de administración remota que permite a los usuarios controlar y modificar sus servidores, routers, switches y un largo etcétera de equipos remotos de manera segura a través de Internet.

- Sus claves SSH pueden ayudar a automatizar estos accesos, que en muchas ocasiones utilizan scripts, diferentes sistemas de backup y otras herramientas de gestión para la configuración.

    - Todo el tráfico generado al utilizar este protocolo está encriptado.

    - Las claves SSH hacen que el inicio de sesión sea único, por lo cual los usuarios pueden cambiar entre diferentes cuentas sin necesidad de introducir contraseñas para cada uno

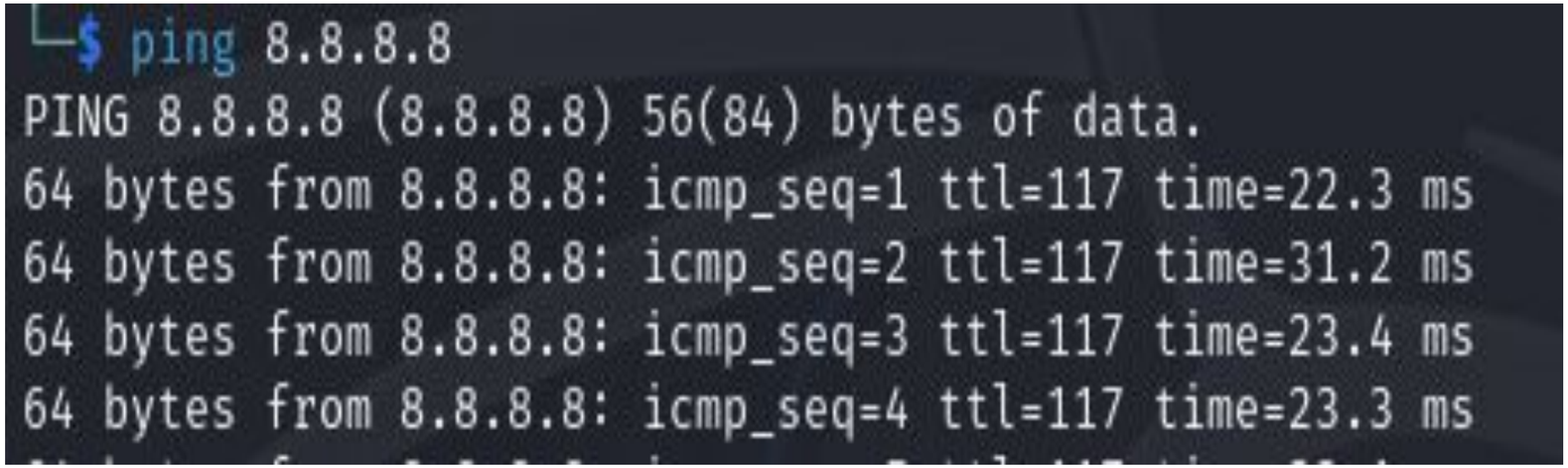
    - Este es muy utilizado para ejecutar scripts y otros softwares que permiten a los programas y sistemas acceder a los datos que establezcamos y a los recursos de forma remota, sin perder seguridad.



https://www.hostinger.es/tutoriales/que-es-ssh

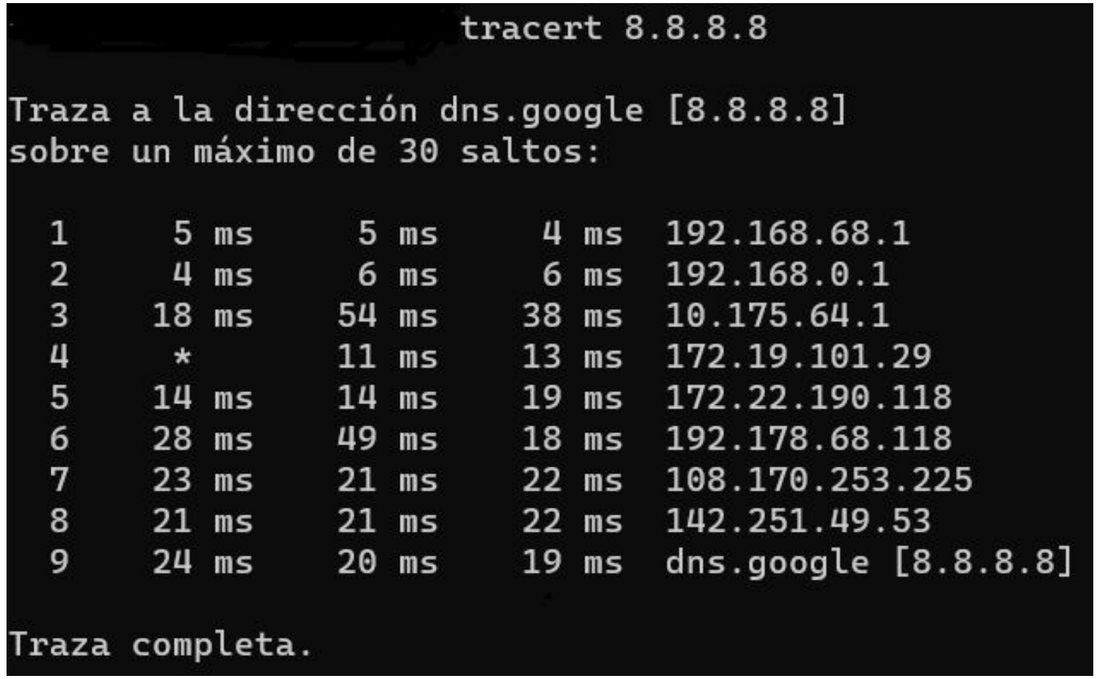
Conectividad entre máquinas

- **Ping**
  - Utilidad de diagnóstico en redes de computadoras que comprueba el estado de la comunicación del anfitrión local con uno o varios equipos remotos de una red que ejecuten IP.
  - Se vale del envío de paquetes ICMP de solicitud (ICMP Echo Request) y de respuesta (ICMP Echo Reply).
  - Mediante esta utilidad puede diagnosticarse el estado, velocidad y calidad de una red determinada
  - TTL: El tiempo de vida (en inglés, time to live, abreviado TTL) es un concepto usado en redes de computadores para indicar por cuántos nodos puede pasar un paquete antes de ser descartado por la red o devuelto a su origen.



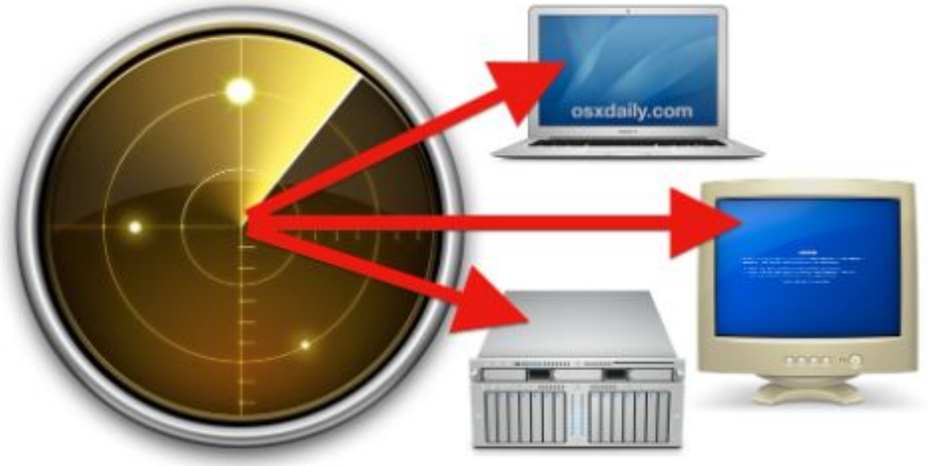
Conectividad entre máquinas

- **Trace Router**
  - Es una herramienta que permite rastrear la ruta que los paquetes siguen desde una dirección IP de red en su camino a un host determinado.
  - Utiliza el **TTL** del protocolo **IP**.
  - Intenta generar una respuesta **ICMP TIME_EXCEEDED** desde cada pasarela en la ruta hacia el host objetivo
  - **Tracert** en Windows, se ejecuta directamente en cualquiera consola del sistema (CMD o PowerShell).
  - También se le conoce como **Traceroute** porque este es el nombre que recibe esta función en GNU/Linux, UNIX y Mac
  - Si no hay respuesta en 5.0 segundos (por defecto), un "*" asterisco será impreso.



Escaner de red

- Se emplea para designar la acción de **analizar** por medio de un programa el estado de los puertos de una máquina conectada a una red de comunicaciones.
- Detecta el estado del puerto.
- Se detectar los servicios que está ofreciendo la máquina
- Posibles vulnerabilidades de seguridad según los puertos abiertos.
- Puede detectar el sistema operativo que está ejecutando la máquina.
- Es usado por administradores de sistemas para analizar posibles problemas de seguridad, pero también es utilizado por usuarios malintencionados que intentan comprometer la seguridad de la máquina o la red
- Una vez detectados los servicios con un escáner de red se puede hacer una comprobación manual de servicios.



https://conpilar.kryptonsolid.com/como-utilizar-el-escaner-de-puertos-en-la-utilidad-de-red-de-mac-os-x/

Vulnerabilidad

- Podemos definir una **vulnerabilidad** de forma genérica como un fallo en un sistema que puede ser explotada por un atacante generando un riesgo para la organización o para el mismo sistema

- Pueden ser **físicas** (que afectan a la infraestructura de la organización de manera física)

    - Como el control de acceso a las instalaciones

- Pueden ser **lógicas** como, por ejemplo:

    - **Desbordamiento de buffer**: un programador no controla el espacio de memoria del programa y un agente malicioso introduce código en dicho espacio de memoria.

    - **Errores de configuración**: contraseñas débiles, usuarios con demasiados privilegios, etc.

    - **Errores web**: errores de validación de entrada, scripts inseguros o errores de configuración de aplicaciones web. Los hackers utilizan métodos como Cross Site Scripting, inyecciones SQL para vulnerar el sitio web.

    - **Errores de protocolo**: vulnerabilidades en el propio protocolo que usa la aplicación o servicio.

CVSS

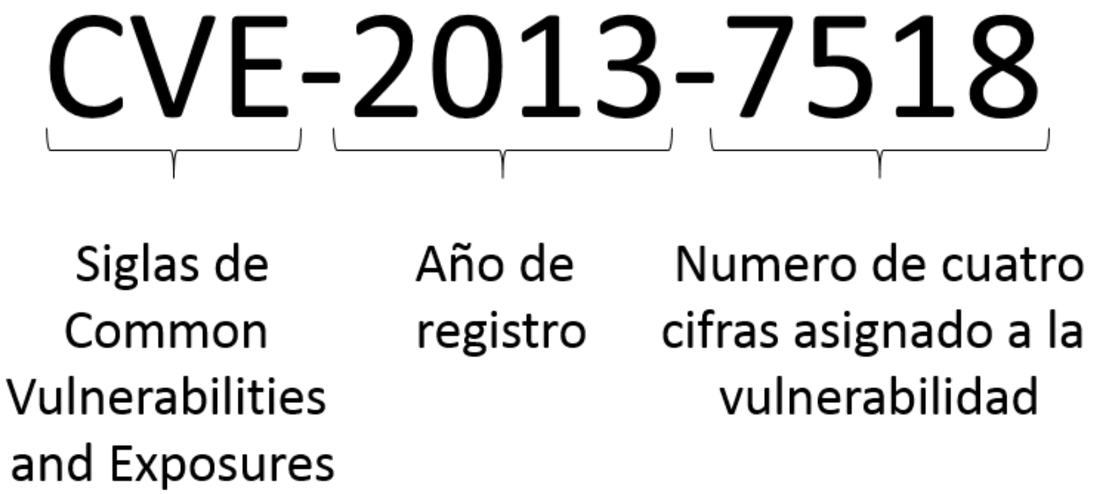
- El **Sistema Común de Puntuación de Vulnerabilidades** o **Common Vulnerability Scoring System** es un método utilizado para proporcionar una medida cualitativa de la gravedad de las vulnerabilidades
- No es una medida de riesgo, sino una forma de evaluar el impacto de las vulnerabilidades identificadas en sistemas cibernéticos.
- El sistema **CVSS** se divide en tres grupos de métricas: **Base**, **Temporal** y **Ambiental**.
- Se basa en dar una puntuación que va de 0 a 10.
- Se usan para calcular la gravedad de las vulnerabilidades descubiertas en los sistemas y priorizar las actividades de remediación de vulnerabilidades.

CVSS v2.0 Ratings		CVSS v3.0 Ratings	
Severity	**Severity Score Range**	**Severity**	**Severity Score Range**
		None*	0.0
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
		Critical	9.0-10.0

https://nvd.nist.gov/vuln-metrics/cvss

CVE

- CVE (**Common Vulnerabilities and Exposures**), es un sistema de catalogación pública que identifica y enumera las vulnerabilidades de seguridad conocidas en productos software y hardware.
- Es una lista de información registrada sobre vulnerabilidades de seguridad conocidas y cada una tiene:
  - Con un número de identificación (CVE-ID).
  - Descripción de la vulnerabilidad.
  - Versiones del software afectadas.
  - Posibles soluciones al fallo (si existen) o mitigación de la vulnerabilidad.
  - Cálculo de la severidad del CVSS
  - Referencias a otras publicaciones.
- https://www.cve.org/



https://securizando.com/cve/

Métodos de escaneo de vulnerabilidades

- **Caja blanca (White Box)**
  - Se tiene toda la información del **Hardware**, **Redes** y **Software**.
  - Se tiene acceso como usuario normal o como súper usuario.
  - El auditor dispone de credenciales, código fuente, mapas de infraestructura
  - Se verifica que se puede hacer con los privilegios concedidos.
  - A través del test se intenta identificar los agujeros de seguridad que pueden llegar a comprometer los sistemas.

- **Caja negra (Black Box)**
  - Solo se tiene la información de acceso a red o al sistema, por ejemplo, una sola dirección IP, algún nombre de alguna empresa, etc.
  - Hay que buscar de toda la información posible por cualquier método.
  - Se simulan los métodos de ataque de un ciberdelincuente con sus mismos recursos.
  - A través del test se intenta identificar los agujeros de seguridad que pueden llegar a comprometer los sistemas.

- **Caja Gris (Grey Box)**
  - Se combinan los métodos anteriores.
  - La información disponible dependerá del acuerdo:
    - Un usuario con acceso limitado al equipo
    - Conocimientos básicos del sistema
    - Existencia de alguna aplicación
    - Cierta información de la red

https://auditech.es/blog/pentesting-que-es-y-para-que-sirve/

Gestión de Vulnerabilidades

- **El análisis de vulnerabilidades** es el proceso de identificar los sistemas en la red que tiene vulnerabilidades conocidas o identificadas.

- Uno de los procesos principales en la ciberseguridad es la de **Gestionar las vulnerabilidades** de los activos cibernéticos, ya que es un vector de entrada o puerta de acceso a un ciberataque. Las Fases de esta gestión son:

- **Identificación de Activos**
  - Tener un inventario y la clasificación de activos. Esto nos servirá para mantener una lista de direcciones IP que tienen los dispositivos o bien para descubrir qué equipos se han conectado a la red sin ser detectados.

- **Planificar análisis**
  - Determinar los activos que van a ser escaneados
  - Seleccionar el método del escaneo a utilizar.

- **Ejecutar Análisis**
  - Escanear los sistemas para detectar fallos.
  - Se revisará el software, las configuraciones o dispositivos que tenga cada dirección IP y determinará si existe alguna vulnerabilidad reportada sobre dicho servicio o software.
  - El escáner revisará también el registro de la máquina para detectar las configuraciones que son inseguras.

https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/guia-para-gestion-vulnerabilidades/guia-para-gestion-vulnerabilidades-2

Gestión de Vulnerabilidades

- **Clasificar Vulnerabilidades**
  - Verificar las vulnerabilidades dentro del inventario de los activos de la empresa.
  - Se identifican que las vulnerabilidades que son detectadas por el escáner sean relevantes.
  - Los escáneres pueden generar tener falsos positivos.
  - Es necesario clasificar y sobre todo priorizar el riesgo que está supondría para la empresa.

- **Priorizar Vulnerabilidades**
  - Normalmente se tiene poco tiempo, poco personal y sobre todo poco dinero.
  - Se debe diseñar un esquema de prioridad que combine el nivel de gravedad de una vulnerabilidad con la importancia que tiene para la empresa.

https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/guia-para-gestion-vulnerabilidades/guia-para-gestion-vulnerabilidades-2

Gestión de Vulnerabilidades

- **Remediar**
  - Probar los parches y cambios de configuración principalmente en unas pocas máquinas.
  - Descargar los parches de sitios oficiales del fabricante y sobre todo no usar parches de sitios de terceros.
  - Luego se proceder a implementarlos en todas las demás máquinas en la red.
  - Hay soluciones de implementación de manera automáticas de parches.

- **Validar**
  - Se realiza un nuevo escaneo de vulnerabilidad
  - Verificación de que las vulnerabilidades que se remediaron **no** aparecen en este escaneo.
  - Documentación e informes. Estos deben incluir:
    - Lista de vulnerabilidades detectadas
    - Lista de dispositivos y servicios vulnerables
    - El nivel de riesgo derivado de cada vulnerabilidad encontrada en cada servicio y dispositivo.

https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/guia-para-gestion-vulnerabilidades/guia-para-gestion-vulnerabilidades-2


THE
BRIDGE