TEMA 5
SEGURIDAD PERIMETRAL Y DE RED

Defendiendo y atacando el entorno de red

José Manuel Redondo López Proyecto *"S-81 Isaac Peral"* v4.0

Fuente: Bing Chat AI

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

Logo: @creative_vanesa (*Instagram*)

OBJETIVOS DEL TEMA

- **Conocer más conceptos sobre terminología y tecnologías de red**
  - Complementando el tema 1
- **Comprender cómo diseñar una infraestructura de red segura**
- **Conocer los conceptos básicos de pentesting de red e identificación (fingerprinting) de máquinas / servicios**
  - Segunda fase típica de una operación de pentesting / CTF (nuestra "kill chain")
- **Conocer software que pueda mitigar ataques de red comunes**
- **No cubriremos detalles sobre cómo configurar redes en Linux/Windows más allá de los elementos estrictamente necesarios**
  - Incluyendo herramientas comunes (`netstat` / `nslookup`)
  - Eso se hace en ASR

ÍNDICE

< Ir al Índice

Fuente: Bing Chat AI

Firewalls >

Conceptos de red adicionales

Complementando el primer tema de teoría con nuevas definiciones

*Iconos por Bing Chat AI

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?

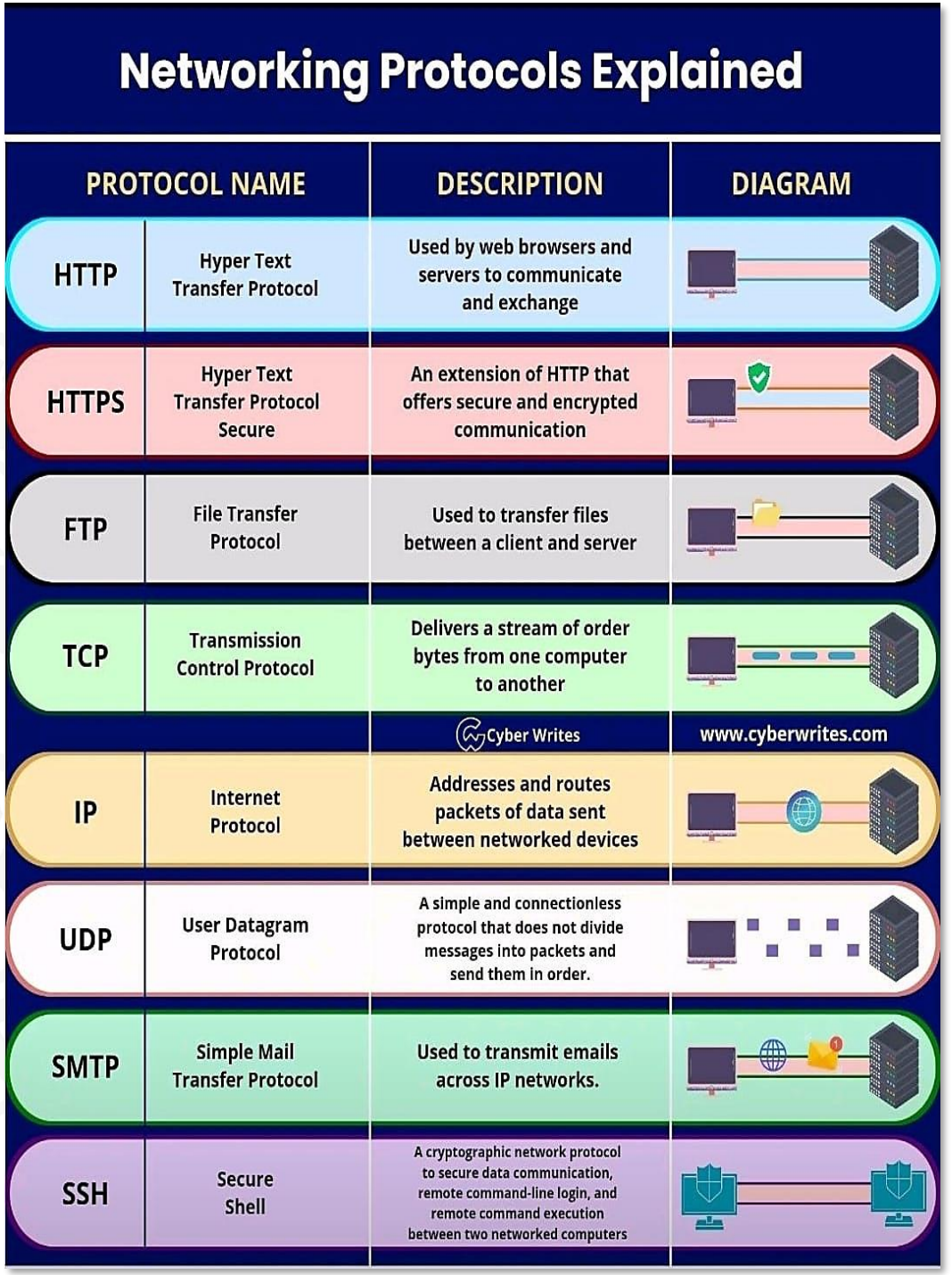
En este bloque aprenderás

- Que hay **muchos protocolos de red** distintos, todos con distintas funciones
- Los **distintos tipos de firewalls** que existen y cómo son sus reglas
- Qué es una **DMZ**
- El uso especial que le podemos dar al **fichero host**

PROTOCOLOS DE RED

Seguridad de Sistemas Informáticos

- **Como dijimos en el tema 1, definen las reglas de comunicación entre dos servicios (software)**
  - Las reglas se definen normalmente en documentos RFC (Request For Comments)
- **Hay muchos protocolos de red: TCP, IP, UDP, FTP, HTTP, SMTP...**
  - Cada uno tiene su propio conjunto de reglas que definen como se hace la comunicación usándolos
- **En internet, los más importantes son**
  - IP (Internet Protocol)
    - Usa las direcciones IP como esquema de direccionamiento de máquinas (**Tema 1**): ¡la base de Internet!
    - Se ven más detalles sobre este protocolo en ASR
  - TCP (Transmission Control Protocol)
- **Los protocolos de red pueden bloquearse configurando el firewall (ASR)**



Recuerda: Firewalls

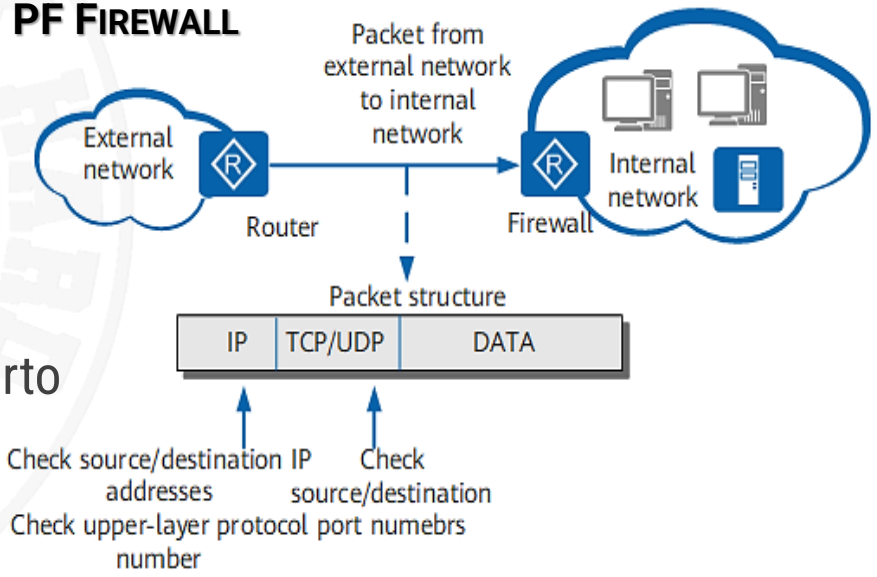
- **Diseñados para bloquear acceso no autorizado (IPs, redes enteras, protocolos...)**
  - Pero normalmente **permitiendo el tráfico saliente**
  - Parte de un sistema informático (software)
  - O una red completa (hardware especializado)
  - También proporciona funciones de log de conexión y auditoría
- **Los firewalls pueden ser de software, hardware o híbridos**
  - Los **firewalls hardware** son máquinas **cuyo hardware está especialmente diseñado** para maximizar el rendimiento de la red y la potencia de procesamiento de paquetes
    - La opción más cara pero más potente
    - Permiten un procesamiento más rápido y una personalización de las reglas más avanzada
  - Los **firewalls híbridos** son software firewall avanzado (Ej.: SSOO), **ejecutado en hardware estándar**
    - Un compromiso entre potencia de procesamiento y coste
    - También implementan funciones de personalización de reglas avanzadas
  - Los **firewalls de software** son un programa que hace funciones de firewall en un PC
    - Solución barata (¡o gratuita!), pero con menos potencia de procesamiento
    - Normalmente, implementan menos características de personalización de reglas

Firewalls: Packet-filtering (PF)

- **Examina estos datos de cada paquete de red recibido**
  - Dirección de origen y destino
  - Protocolo
  - Número de puerto de destino
- **Los datos se procesan así**
  - Los paquetes se examinan uno por uno, y se descartan si no cumplen con sus **reglas**
    - No se utiliza usa contexto de los paquetes (servicio, conexión...) para decidir si descartan o aceptan
  - Ej.: Se define una regla para bloquear el acceso a `telnet`
    - Un firewall PF descartará **cualquier** paquete TCP destinado al puerto 23, sin mirar nada más
  - Linux tiene un firewall PF integrado con múltiples frontends
    - Ufw
    - IPSet (https://wiki.archlinux.org/title/Ipset)
    - Firewalld

Fuente:
https://support.huawei.com/enterprise/es/doc/EDOC1000154776/88191a64/packet-filtering-firewall

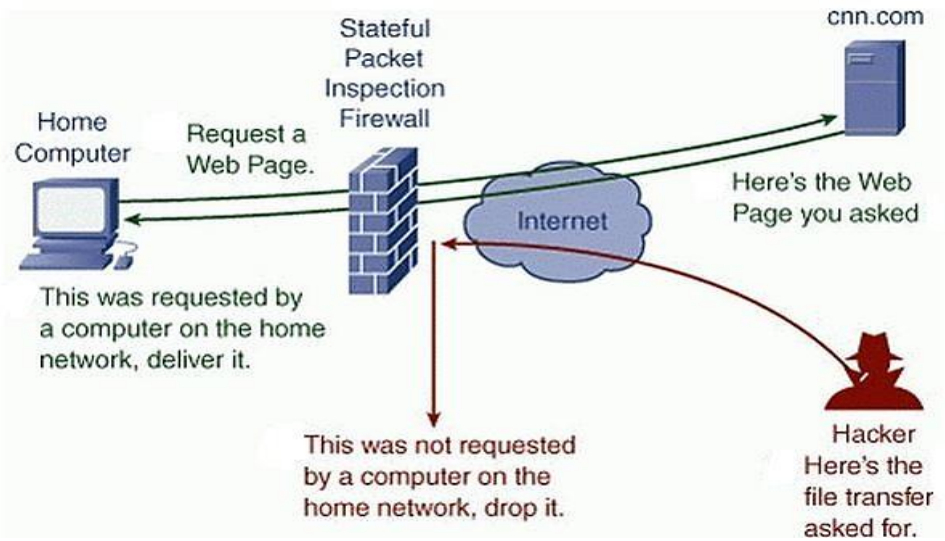
PF Firewall



Firewalls: Stateful Packet Inspection (SPI)

- **Firewalls con filtrado dinámico de paquetes con una tabla que rastrea todas las conexiones abiertas**
  - Cuando llegan nuevos paquetes, el firewall compara la información de la cabecera de cada paquete con esa tabla de estados
  - Y determina **si es parte de una conexión ya establecida** o no
    - Si lo es, entonces el paquete se acepta **sin más análisis**
    - De lo contrario, se evalúa de acuerdo **con un conjunto de reglas para nuevas conexiones**
  - Los firewalls SPI avanzados permiten reglas potentes
    - Basadas en tiempo, geolocalización...
    - Incluyen también **detección de intrusos** (IDS)
    - Y otras características...
  - ConfigServer es un producto de firewall SPI gratuito
    - https://www.configserver.com/cp/csf.html
  - Algunas distribuciones de Linux son solo firewalls SPI
    - IPFire (https://www.ipfire.org/)
    - pfSense (https://www.pfsense.org/)

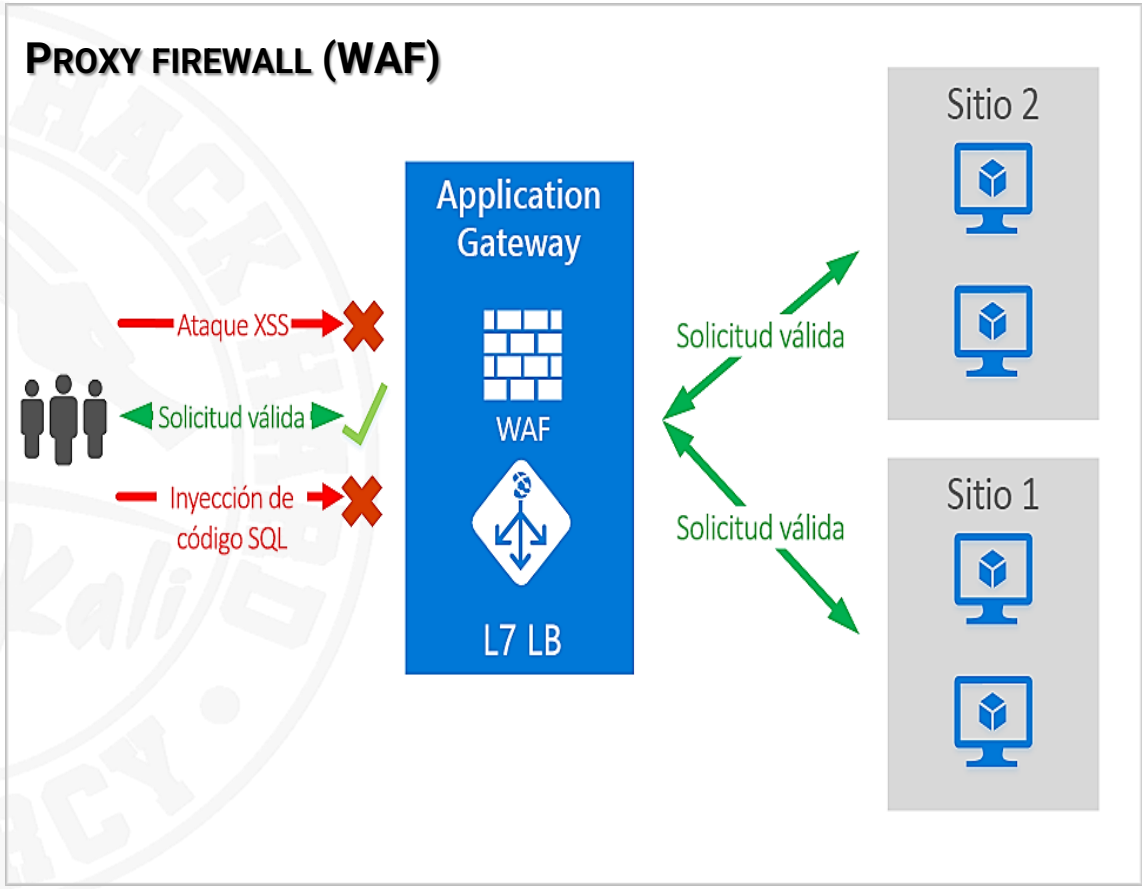
SPI Firewall



Fuente: https://flylib.com/books/en/2.282.1.10/1/

Firewalls: Proxy firewall

- **Proporciona filtrado en la capa de aplicación**
  - Examina el **contenido** del paquete
    - Diferenciando solicitudes válidas, datos...
    - ¡Y **código malicioso** "escondido" en ellos!
  - También conocidos como
    - Application firewalls o gateway firewalls
    - Web Application Firewall (WAF) para la protección de aplicaciones web específicamente
  - Ej.: Podrían permitir/denegar comandos `ssh` específicos de usuarios particulares
    - Un firewall PF solo puede controlar las solicitudes entre hosts que le llegan
    - ¡**No entiende de usuarios**! (no utiliza el contenido de los paquetes para tomar decisiones): **un proxy firewall sí lo hace**
  - `mod_security` es un WAF muy popular
    - Lo describiremos más adelante

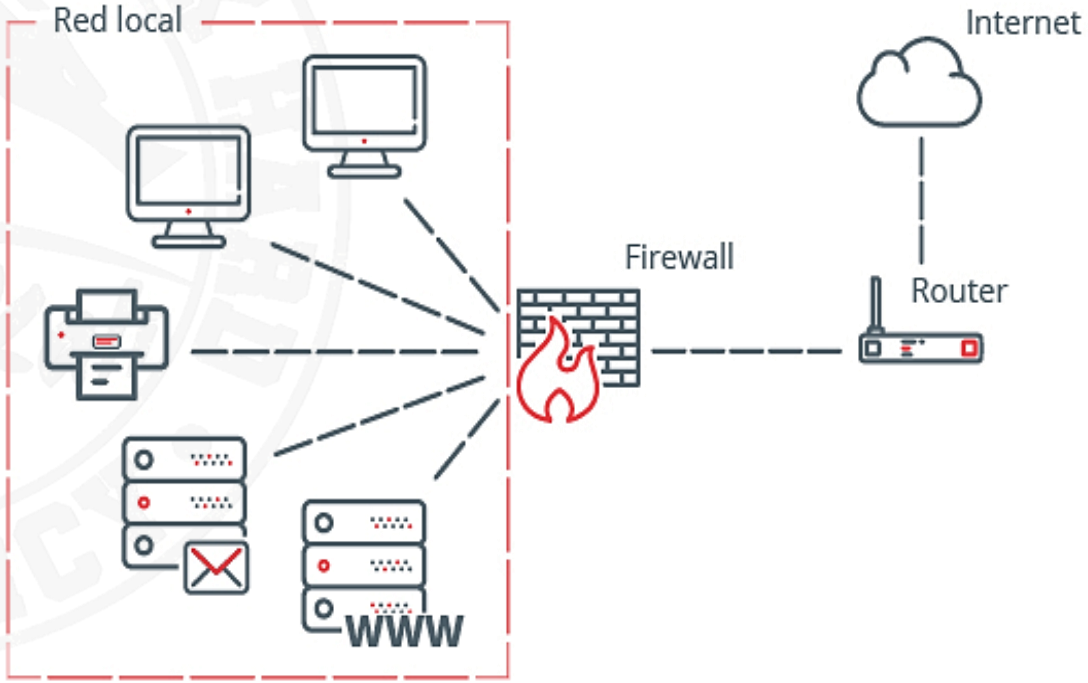


Fuente: https://learn.microsoft.com/es-es/azure/web-application-firewall/ag/ag-overview

Reglas de un firewall

- **Una serie de reglas de filtrado indican qué tipos de comunicaciones son**
  - **Permitidas** (`ALLOW`)
  - **Rechazadas** (`REJECT`)
  - **Descartadas** (`DROP`)
    - Rechazada **sin dar aviso al remitente**
  - En la imagen se permiten conexiones desde cualquier lugar utilizando IPv4 o IPv6
    - ¡Pero solo a los puertos 22 (`ssh`) o 80 (`http`)!

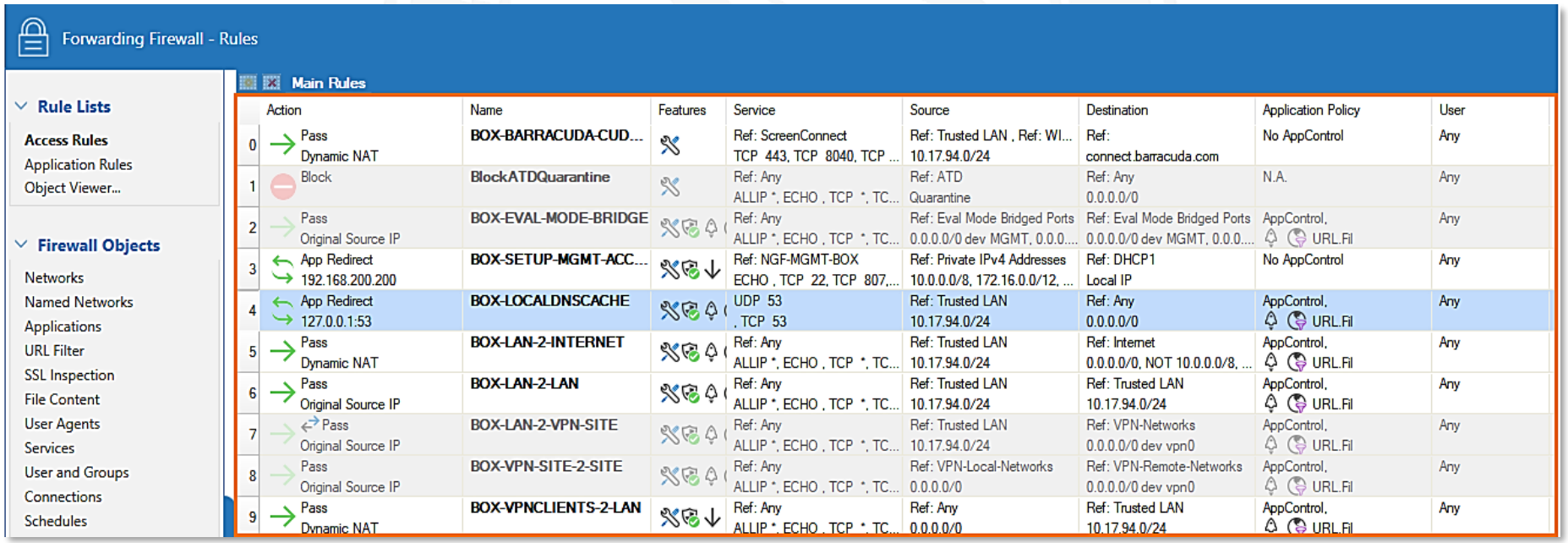
```
Status: active

To                         Action      From
--                         ------      ----
22                         ALLOW       Anywhere
80                         ALLOW       Anywhere
Apache                     ALLOW       Anywhere
22 (v6)                    ALLOW       Anywhere (v6)
80 (v6)                    ALLOW       Anywhere (v6)
Apache (v6)                ALLOW       Anywhere (v6)
```



Fuente: https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

Reglas de un firewall: Ejemplos

- **Las reglas de un firewall operan con tripletas (IP, puerto, protocolo):**
  1. *"La IP 192.168.3.10 solo puede acceder a este servidor cuando se conecta al puerto 22 mediante el protocolo TCP*": **solo esa máquina puede conectarse al servidor a través de SSH (22). El resto de las conexiones se descartan**
  2. *"El tráfico TCP entre 192.168.10.0/24 y 192.168.25.0/24 sólo se permite a través del puerto 3306*": **Las conexiones MySQL (puerto 3306) solo son posibles entre cualquier máquina de la red *192.168.10.10* a cualquier máquina de la red *192.168.10.25***
  3. *"El tráfico TCP/UDP desde cualquier dirección IP solo se permite a la dirección 192.168.59.15, puerto 443*": **El tráfico de Internet sólo puede conectarse a ese servidor web mediante HTTPs (puerto 443)**

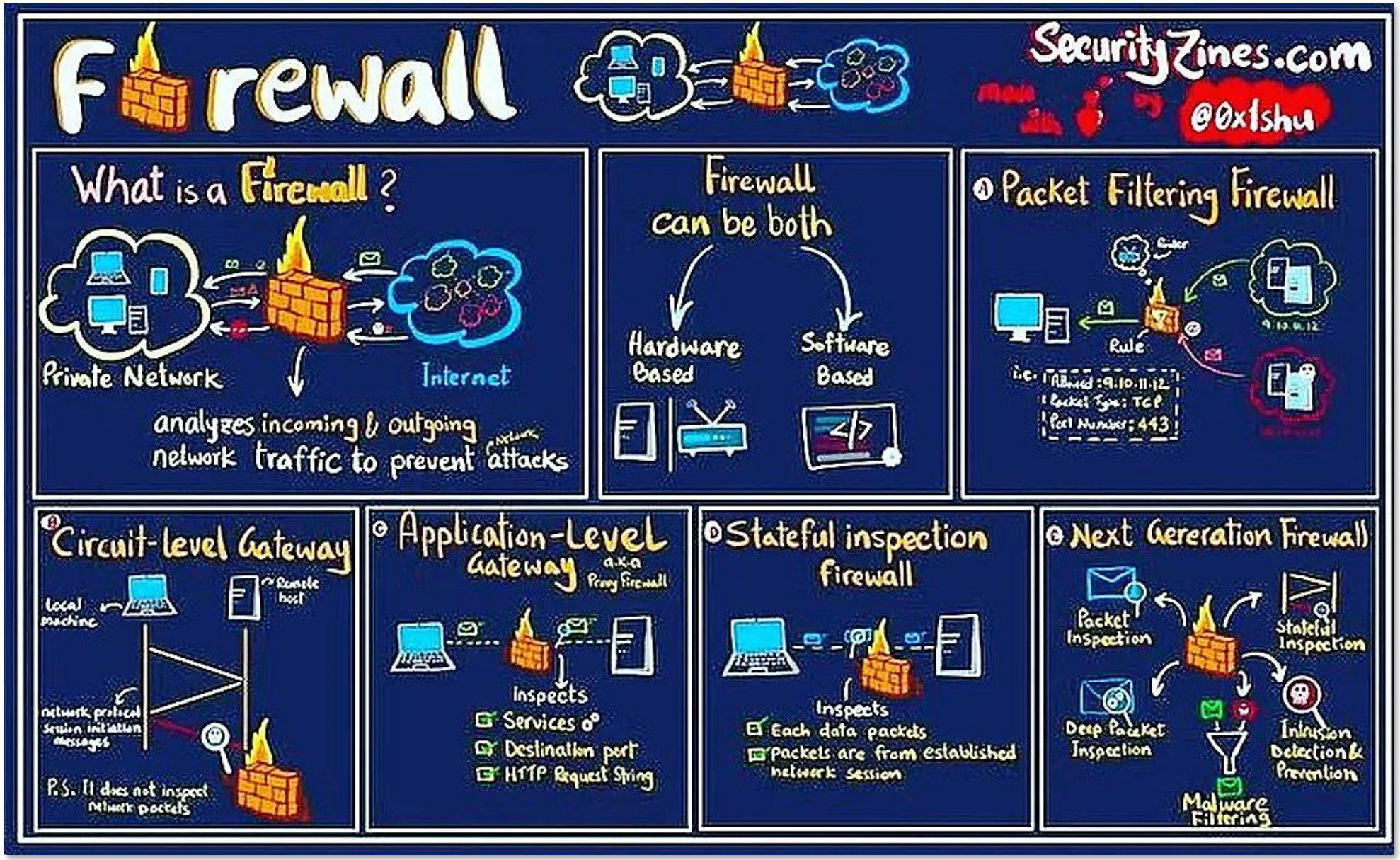


Fuente: https://campus.barracuda.com/product/cloudgenfirewall/doc/79463228/firewall-rule-list-interface-and-icons

Host firewalls vs Perimetral firewalls

- **Todo dispositivo debería tener un firewall instalado con reglas adecuadas**
  - Estos se llaman **firewalls de host** (por ejemplo, iptables de ASR y su interfaz, ufw)
  - Normalmente con un enfoque de **lista de permitidos** para el tráfico entrante
    - **Todo el tráfico entrante se elimina a menos que se permita explícitamente**
    - **El tráfico saliente** (conexiones iniciadas en la propia máquina al exterior) **normalmente está permitido**
  - Las reglas 1 y 3 de los ejemplos anteriores son reglas típicas de firewall de host
- **Cuando los firewalls pueden restringir las conexiones entre diferentes redes o zonas, se denominan firewalls perimetrales**
  - Normalmente, hardware personalizado o distribuciones de Linux que solo implementan la funcionalidad de firewall
  - Por lo general, descarta todas las conexiones no permitidas explícitamente entre dos redes, bidireccionalmente
  - Son una "**primera línea de defensa**"
    - Si se rompe, los atacantes tendrán acceso a la red restringida
  - La regla 2 del ejemplo anterior es una regla típica de firewall perimetral

RESUMEN: FIREWALLS

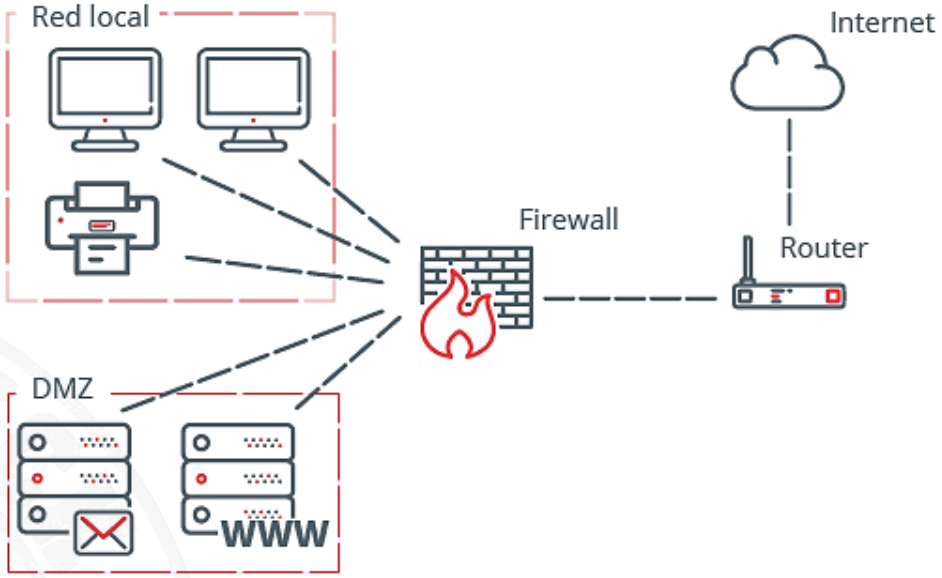


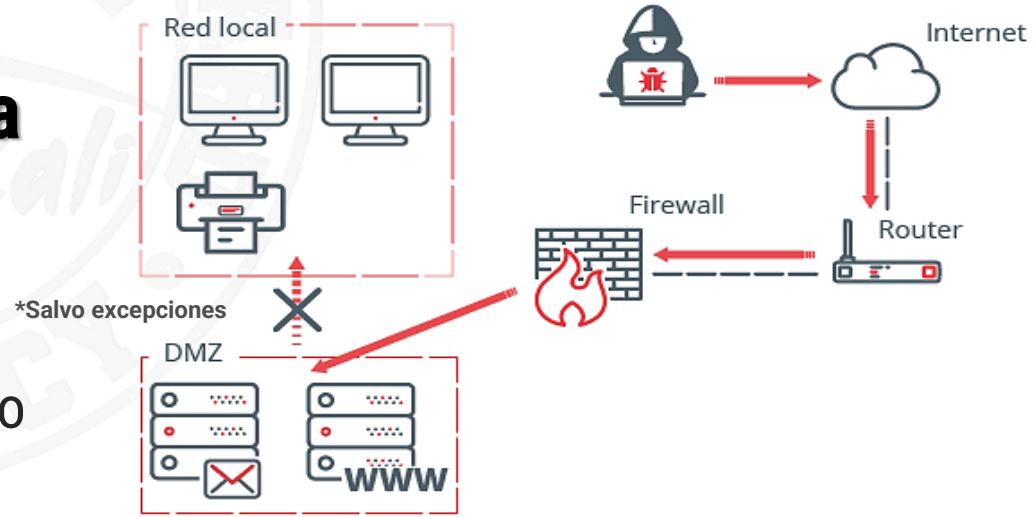
Los Next Generation Firewalls combinan muchas funcionalidades en un solo producto. Son los más modernos (y caros), pero entender en detalle lo que hacen necesita un curso de redes específico ☹

DEMILITARIZED ZONES (DMZS)

Seguridad de Sistemas Informáticos

- Son **zonas de red aisladas** dentro de la red interna de una empresa
- Deben contener todos los recursos que sean accesibles desde internet
  - Servidores web, servidores de correo electrónico...
- **Se implementan con cortafuegos (perimetrales)**
- Los servidores dentro de una DMZ permiten conexiones **tanto desde Internet como desde la red local de la empresa**
  - Las conexiones de la DMZ a la red local normalmente están prohibidas **(se pueden hacer excepciones)**
  - Si un servidor de la DMZ se ve comprometido, el acceso a los datos importantes en la LAN es muy complicado
    - Los de la DMZ son más propensos a verse comprometidos
    - Al tener mayor exposición a amenazas





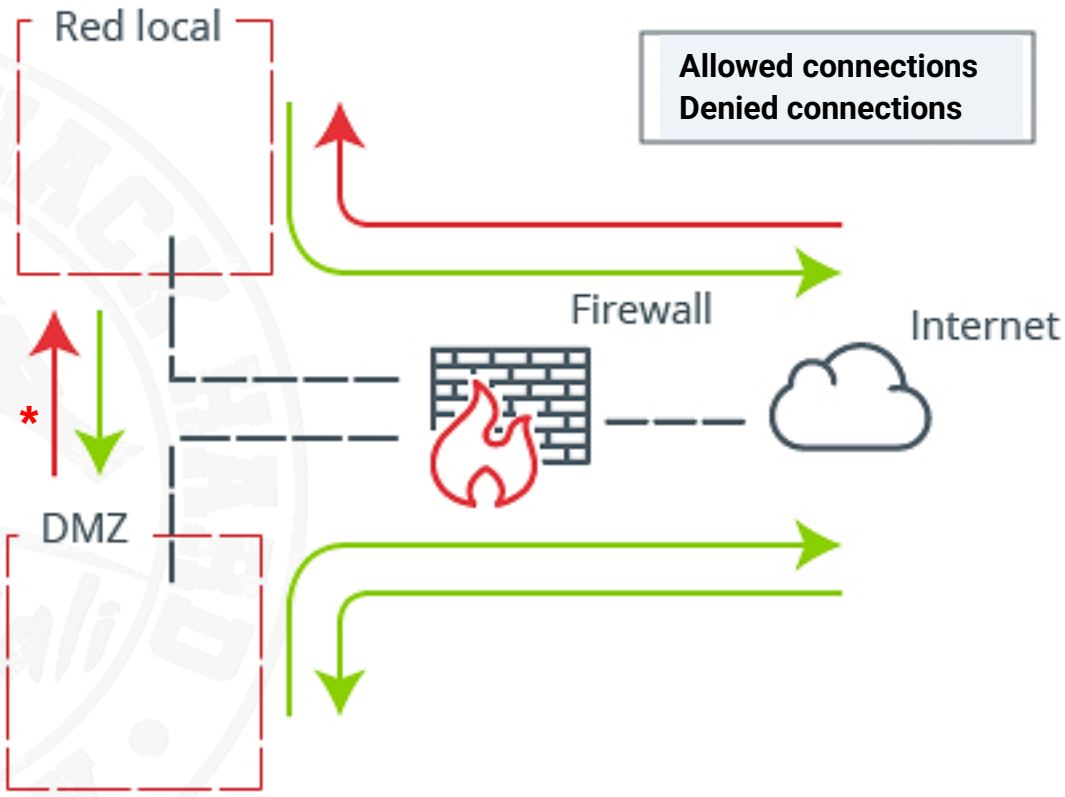
Fuente: https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

DEMILITARIZED ZONES (DMZS)

Source network	Destination network	Action
Internet	DMZ	Allow
Internet	LAN	Deny
DMZ	Internet	Allow
DMZ	LAN	Deny*
LAN	DMZ	Allow
LAN	Internet	Allow

*Se puede permitir el acceso a ciertos puertos, servicios o máquinas desde máquinas específicas

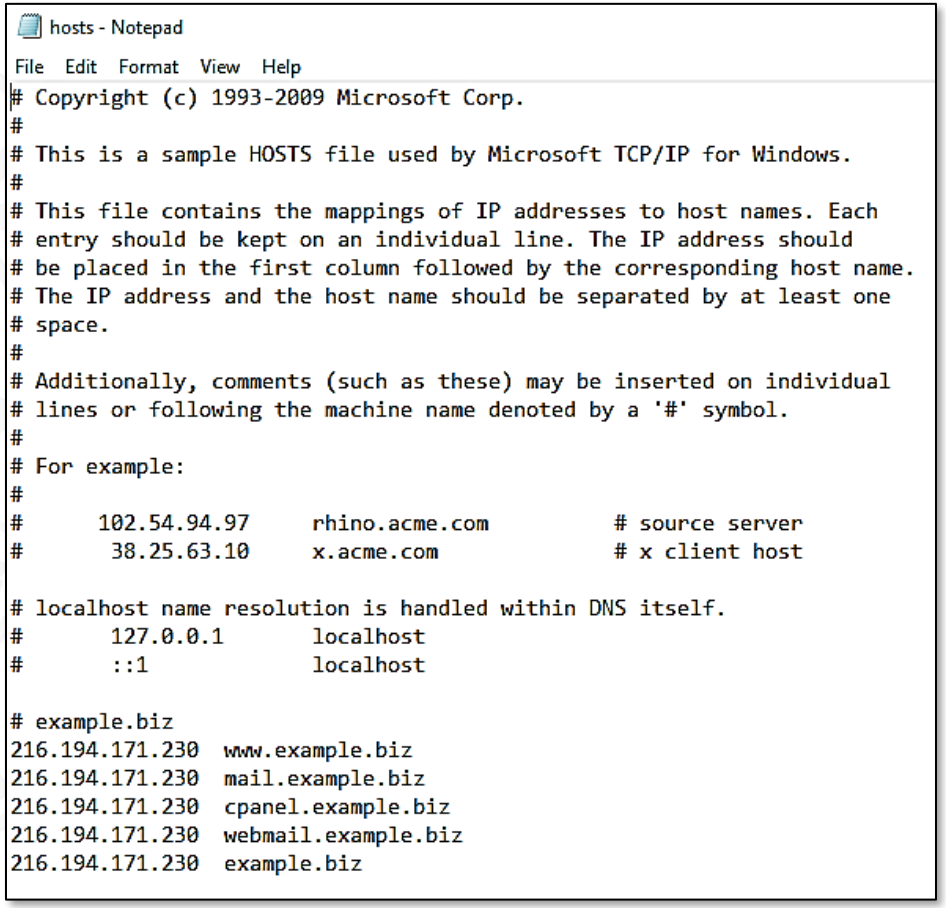
- **Los firewalls son necesarios para implementar una DMZ**
  - Establecen segmentos de red
  - Permiten o desautorizan las comunicaciones entre ellos
- **La tabla muestra la acción recomendada con el tráfico de red que proviene y va hacia diferentes segmentos de red**



Fuente: https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

Ficheros Host

- **Archivo local para para la traducción de nombres de dominio a IPs**
  - Descrito en ASR
  - Todo lo que se pone en este archivo será consultado y resuelto primero
    - ¡Antes de hacer cualquier consulta a un DNS remoto!
    - Si la información del nombre está aquí, se resuelve **y no se utiliza el DNS**
- **Presente en los principales SO**
  - Linux: `/etc/hosts`
  - Windows: `C:\Windows\System32\drivers\etc\hosts`
- **Se podría utilizar para implementar filtros locales de nombres DNS de una manera sencilla**
  - https://github.com/StevenBlack/hosts
  - Es un bloqueador de URL maliciosas para **CUALQUIER** programa de nuestra máquina que haga conexiones remotas



¿Crees que lo has entendido todo? ¡Autoevalúate!

?

- **Eres capaz de hacer lo siguiente**
  - *Entender que hay muchos protocolos de red y que cada uno tiene una función*
    - *Y que un firewall puede bloquear por protocolo, impidiendo de esta forma todos los servicios asociados*
  - *Saber distinguir cada tipo de firewall típico: PF, SPI y Proxy, de host, perimetral...*
  - *Entender adecuadamente lo que te permiten hacer las reglas de un firewall*
    - *Y la capacidad de control del tráfico de la que te dotan*
  - *Comprender adecuadamente el concepto de DMZ*
  - *Entender para que sirve un fichero host y su relación con los DNS*

< Ir al Índice

Fuente: Bing Chat AI

Ataques de red >

Diseños inseguros >

SNI >

Principios de diseño general de redes seguras

Como crear una red realmente segura

*Iconos por Bing Chat AI

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?

En este bloque aprenderás

- Los distintos **tipos de ataques de red** típicos existentes
- Como están **evolucionando los ataques** de red en la actualidad
- Qué medidas puedes tomar **contra ellos**
- El concepto de **Zero Trust**
- Diseños de red **conceptualmente inseguros**

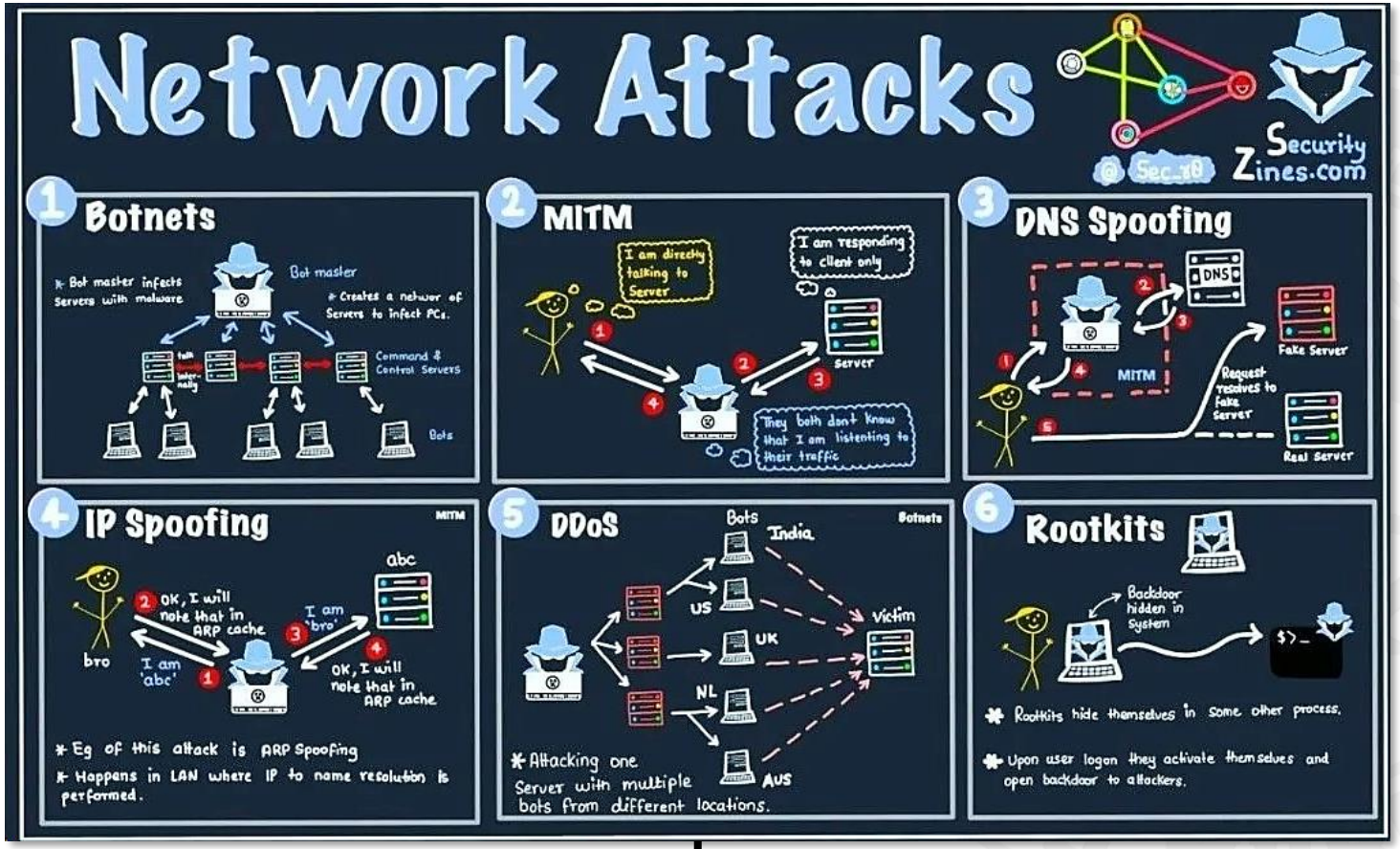
Ataques de red

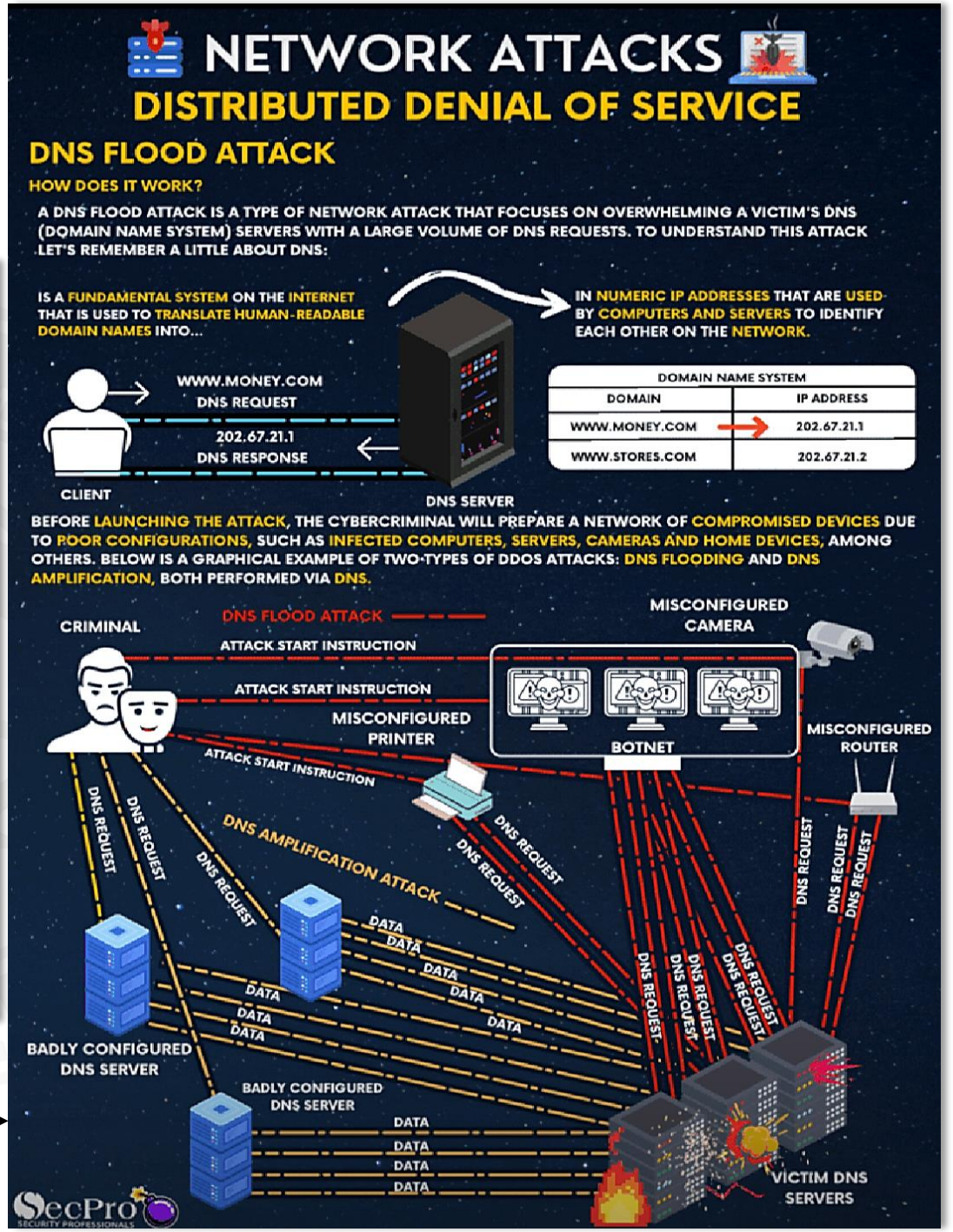
Como se ataca a las redes hoy día

*Iconos por Bing Chat AI

TIPOS DE ATAQUES DE RED TRADICIONALES

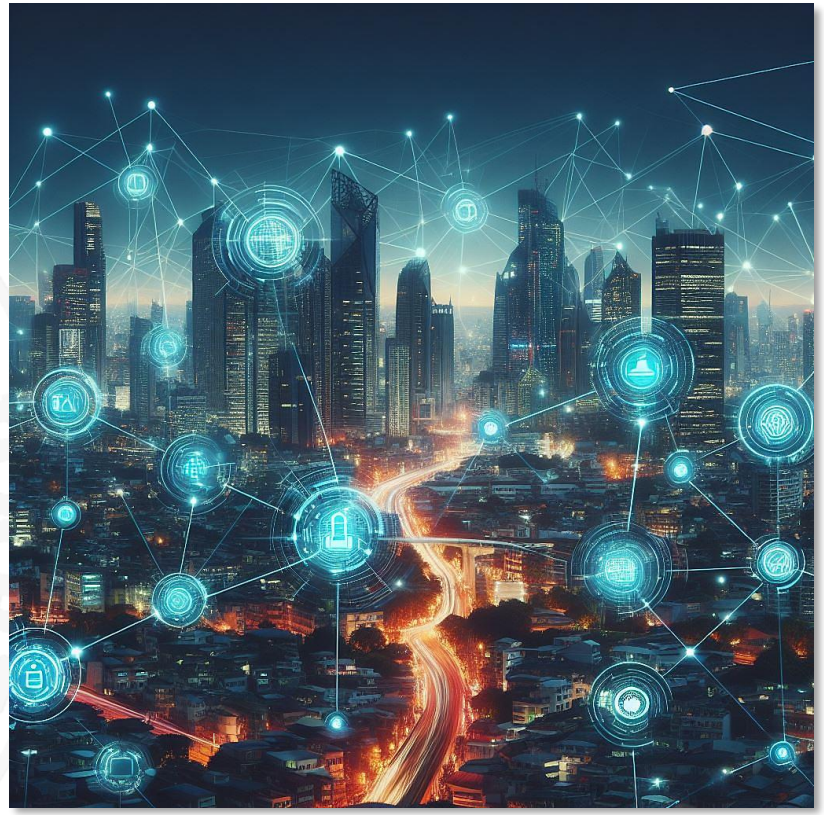
Seguridad de Sistemas Informáticos





Ataques de red hoy

- **Los ciberataques buscan explotar el eslabón más débil de una red**
- **Tradicionalmente las defensas más fuertes se ponen en el perímetro de una red**
  - Es decir, en las máquinas que gestionan el tráfico con máquinas de otras redes
  - Firewalls con estado, sistemas de detección de intrusiones (IDS), segmentación de acceso a las redes, VLANs...
  - Mayor concienciación de los empleados acerca de su existencia y uso aceptable
  - Las defensas de las máquinas "de dentro de la red" (endpoints) eran **más débiles**
    - El paradigma era que las defensas perimetrales eran suficientes
- **El perímetro ya no es el objetivo principal**
  - Entonces, *¿qué se ataca hoy en día en las redes?*



En un mundo interconectado, el perímetro de la red de cada negocio suele tener ya hoy en día unas defensas muy fuertes. Fuente: IA de Bing Chat

ATAQUES DE RED HOY

Escenarios de tipo “traiga su propio dispositivo” (BYOD - Bring Your Own Device)

- **Los empleados usen sus dispositivos personales para trabajar (puede aumentar la productividad)**
- Pero da a los atacantes nuevos puntos de entrada a una red
- Indetectables para muchas defensas perimetrales: el dispositivo se mete dentro del perímetro

Teletrabajo

- **Los avances tecnológicos (y la pandemia) aumentaron su uso**
- Pero podría eliminar la eficacia de las herramientas de seguridad perimetral
  - Los equipos de los empleados en su casa **no están cubiertos por ellas**...
- La conexión a través de VPN se salta la mayoría de estas defensas
  - Ya que la comunicación cliente - red no puede inspeccionarse
- El malware se puede "inyectar" desde el ordenador cliente a la red de la empresa

Fuente: IA de Bing Chat

Aplicaciones en la nube

- **El 83% de las cargas de trabajo empresariales se han trasladado a la nube en la década 2020**
- Sin una forma de asegurar las conexiones a estas aplicaciones se podría comprometer la red
- ¡Independientemente de la inversión en ciberseguridad perimetral!

ATAQUES DE RED HOY

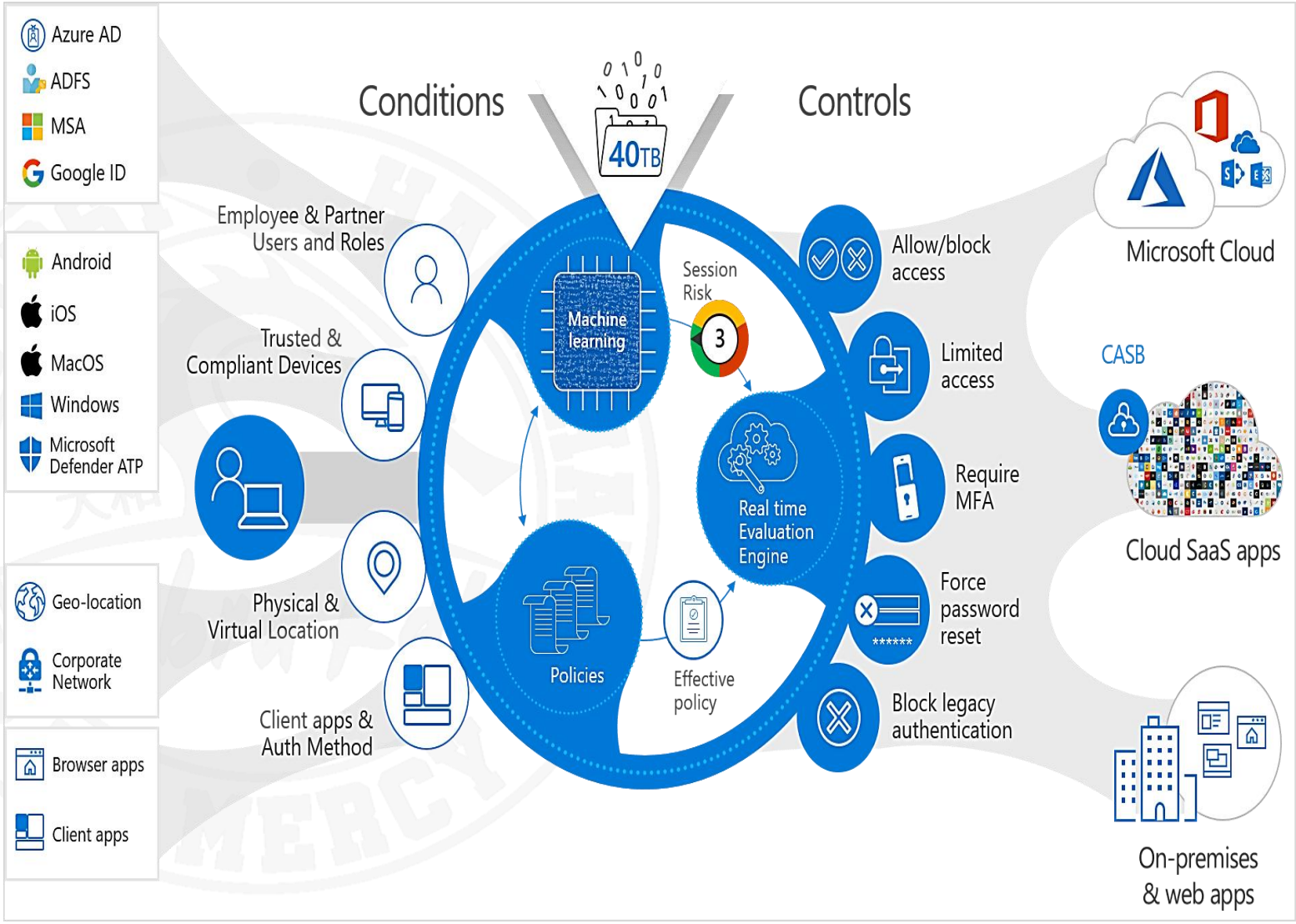
- **Los atacantes ya no emplean enfoques tradicionales para entrar en las defensas perimetrales**
- **Ahora atacan dispositivos finales (endpoints) (de usuarios/empleados)**
  - Típicamente comprometiendo la actividad de un navegador de internet vulnerable
  - Y usando la ingeniería social (combinando con OSINT, **Trabajos en Grupo**)
  - El objetivo es obtener credenciales de los empleados, obteniendo acceso a la red de la empresa
- **Esto no es atacar las defensas perimetrales**
  - Sino **hacerse pasar por alguien** que tiene acceso legítimo a la red
  - ¿Recuerdas la estafa de bitcoin de Twitter en 2020? https://en.wikipedia.org/wiki/2020_Twitter_bitcoin_scam
- **Por tanto, detectar estos ataques ("inside jobs") es mucho más difícil**
  - Requiere un tipo de herramienta de seguridad especializada y muy avanzada llamada UEBAs (User and Entity Behavior Analytics - Análisis del comportamiento de usuarios y entidades, ver **Tema 6**)

Ataques de red hoy: ¿Qué hacer?

- Usar un **enfoque multicapa**
- **No deshacerse de las soluciones de seguridad existentes**
  - Las defensas perimetrales son una capa más del enfoque multicapa, pero ya no la única
- Aplicar un nuevo modelo (**Zero trust**)
  - Tanto a las defensas perimetrales como a la estrategia de seguridad de los endpoints
  - En lugar confiar en todo el tráfico interno, **verifica cada usuario y dispositivo que accede a recursos**
  - Ej.: un caso reciente de la NASA relacionado con no aplicar Zero Trust a dispositivos
    - https://www.bbc.com/news/technology-48743043
  - Una implementación popular es Google's BeyondCorp: https://cloud.google.com/beyondcorp?hl=es
- **Asumir que habrá dispositivos que no serán de confianza** accediendo a la red
- **Filtrado de URLs**
  - Restringir el tráfico web para evitar que los usuarios accedan a sitios malintencionados conocidos
  - Cuyo acceso podría comprometer credenciales y dispositivos de conexión
  - Firewalls SPI perimetrales (Pfsense, IPFire...) lo hacen con un plugin Squid proxy o similar (ASR)

¿ZERO TRUST? (CONFIANZA CERO)

- **Sistema de seguridad que solo admite dispositivos que cumplen con unas condiciones**
  - Usuario propietario y rol, red, geolocalización, cumplimiento de seguridad (**Tema 4**), aplicación usada...
- **Comprueba los dispositivos continuamente (no 1 sola vez)**
  - Usando Machine Learning e información en tiempo real (comportamiento del usuario y cambios en el dispositivo)
- **Concede acceso o fuerza la (re)autenticación del cliente**



Fuente: https://www.infusedinnovations.com/blog/secure-modern-workplace/conditional-access/zero-trust-security-concepts-and-microsoft-365

ATAQUES DE RED HOY: ¿QUÉ HACER?

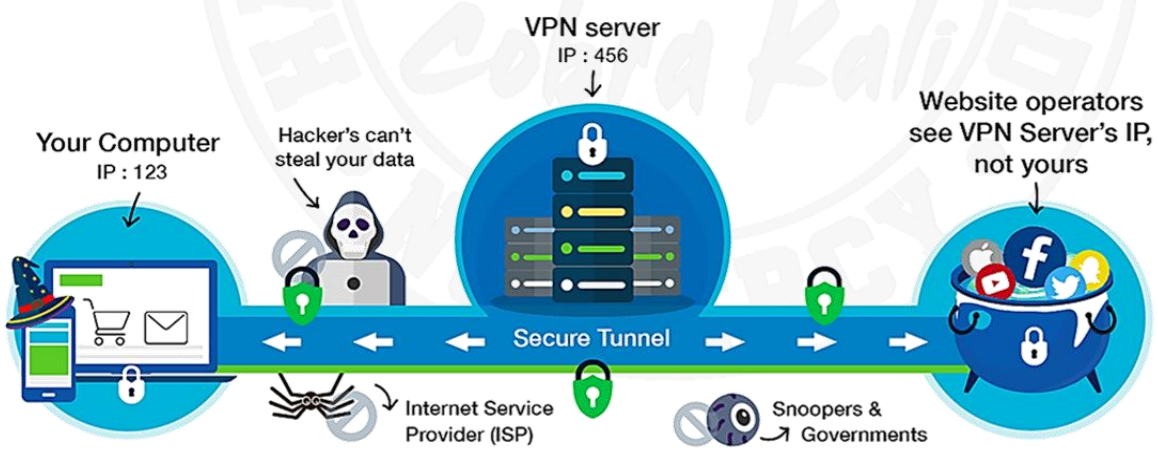
- **Facilitar la detección de anomalías en endpoints**
  - Supervisando continuamente los endpoints buscando actividad sospechosa
  - Y enviar alertas en tiempo real cuando se detecte un comportamiento potencialmente malintencionado
  - **EDR/XDR (Tema 3), Sistemas de detección de intrusiones** (IDS) y **Sistemas de prevención de intrusiones** (IPS), **SIEM**...
    - Ej.: Wazuh, OSSEC Alienvault, Suricata, Snort...
    - Los **SIEM** analizan de forma centralizada los logs de los sistemas para detectar anomalías
  - https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips
- **Aislar el navegador (Ejs.: MVs, una solución de Remote Browser Isolation...)**
  - Protegiendo a los usuarios de ataques Zero-Day, descargas no autorizadas y contenido malicioso...
  - Y en casos de necesitar **máxima privacidad**, usar ToR Browser (red ToR, **Tema 2**)
- **Proteger el acceso a los servicios a través de cortafuegos u otros medios**
  - https://www.tecmint.com/secure-Linux-tcp-wrappers-hosts-allow-deny-restrict-access/

ATAQUES DE RED HOY: ¿QUÉ HACER?

Controlar el acceso remoto

- Asegurar las conexiones remotas con puertas de enlace securizadas y conexiones VPN...
  - Pero no confundir con un servicio VPN tradicional, que solo anonimiza y protege a quien se conecta
  - Necesitamos **una VPN entre el empleado y la organización** (¡como la de Uniovi! ☺)
  - O una **VPN punto a punto** (P2P) que conecta solo los dispositivos que queramos entre ellos como una LAN
  - **Nunca exponer en Internet RDP, el protocolo de escritorio remoto**
- Implementar la autenticación de dos factores para todos los usuarios y dispositivos
- Hacer log todas las sesiones remotas
- En definitiva, implementar una solución y una directiva de acceso remoto altamente segura
  - https://www.ccncert.cni.es/comunicacion-eventos/comunicados-ccn-cert/9638-como-implantar-una-politica-de-acceso-remotoseguro.html

Fuente:
https://blog.360totalsecurity.com/en/how-vpn-works



Una VPN punto a punto, como ZeroTier, es una solución ideal en muchos escenarios al dar acceso seguro + control total del servicio VPN + facilidad de instalación y uso. La otra opción es instalarte un servidor VPN propio (comprado, usando Wireguard...)

➢ Ejercicios **L7B4_VPN, L7B4_VPNP2P**

Diseños de red inseguros

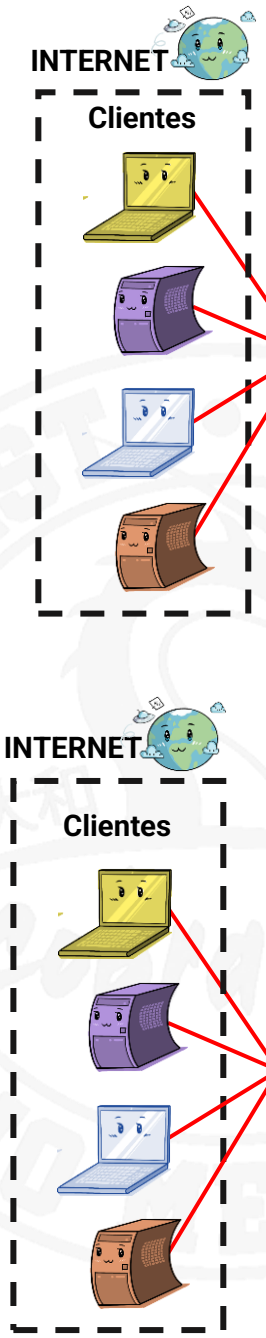
Como NO diseñar una red

*Iconos por Bing Chat AI

Diseños de red inadecuados

Seguridad de Sistemas Informáticos

- Añadir seguridad a infrast. de red las hace más complejas
- Soluciones basadas en 1 servidor con todos los servicios (front, back, SGBD,…) son **inadecuadas**
  - Single Point of Failure al no haber segmentación de red
  - No hay especialización de máquinas que permita optimizar los servicios
  - La protección basada en nube solo arregla parte de los problemas (Ej.: Cloudflare)
  - El hosting en nube es insuficiente, incluso pagando servicios premium
  - El código debe crearse con buenas prácticas de seguridad (Tema 6)



Moviéndose a la nube: "Cloud native" no es una "cura milagrosa"

- **Las soluciones basadas en la nube pueden ser muy caras si no las gestionamos y dimensionamos adecuadamente**
- **Y también pueden tener problemas de seguridad**
  - El código del software alojado en la nube debe crearse siguiendo una metodología/reglas para **el desarrollo seguro de aplicaciones** (**Tema 6**)
  - La **base de datos** puede estar mal configurada o no proteger bien la información confidencial
  - Inconscientemente podemos **"romper" la configuración base de seguridad** que el proveedor de la nube implementa si hacemos modificaciones inadecuadas a la plataforma
    - Necesitamos saber qué estamos haciendo, incluso cuando la nube gestiona la mayor parte de ella
    - Ej.: Desplegar máquinas con hardening CIS (**Tema 4**) y modificar algunos de sus controles de seguridad
  - Debemos saber cómo organizar / configurar correctamente las **comunicaciones** entre las diferentes máquinas que ponemos en la nube, utilizando las herramientas del proveedor
    - Tenemos que estudiar las opciones disponibles para aprovechar las características del proveedor cloud
  - Podríamos tener algo en producción que **no entendemos o controlamos total o completamente**
    - **Es necesario tener conocimientos de ciberseguridad** para sacarle todo el partido a las herramientas

Hacia una solución real

- **El nivel de seguridad de la infraestructura depende de**
  - **El presupuesto** (una seguridad sólida requiere inversiones sólidas)
    - Para implementar segmentación de red (no servidores aislados, sino varios especializados en redes distintas)
    - Para procedimientos de hardening adecuados (**Tema 4**) y hardware de seguridad (EDR/XDR, firewalls, IDS, IPS, SIEMs…vistos más tarde)
  - Capacidad para manejar infraestructuras de diferentes complejidades
  - Criticidad de datos/servicios
  - Regulaciones/certificaciones legales que deben cumplirse, cumplimiento de políticas de software, implementación de SGSI y revisiones de auditorías de seguridad (**Tema 4**)
- **Veamos un ejemplo de una infraestructura segura (y compleja), la SNI**
  - Secure Network Infrastructure
  - Todos o parte de sus elementos se pueden implementar en un proveedor de nube para ahorrar costes de administración / dinero (nubes privadas, públicas, híbridas)

¿CREES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!

?

Eres capaz de hacer lo siguiente

- *Tener claro que, aunque las defensas perimetrales siguen siendo imprescindibles, los ataques modernos se centran en impedir que puedan examinar el tráfico que origina un ataque*
  - *Y que para ello se ataca a los usuarios, dispositivos externos conectados vía VPN, recursos en nube, o cualquier medio que permita saltarse la defensa perimetral*
- *Entender del concepto de Zero Trust*
- *Comprender la importancia y los medios para detectar anomalías*
- *Comprender la importancia y los medios para aislar la navegación o preservar tu privacidad*
- *Entender la diferencia entre un servicio VPN tradicional, la VPN de una organización y una VPN P2P*
- *Tener claro que tener todos los servicios en un solo servidor es un diseño de red inadecuado, y que el diseño debe ajustarse al presupuesto disponible*

Secure Network Infrastructure (SNI)

Cómo diseñar una arquitectura de red segura

*Iconos por Bing Chat AI

¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?

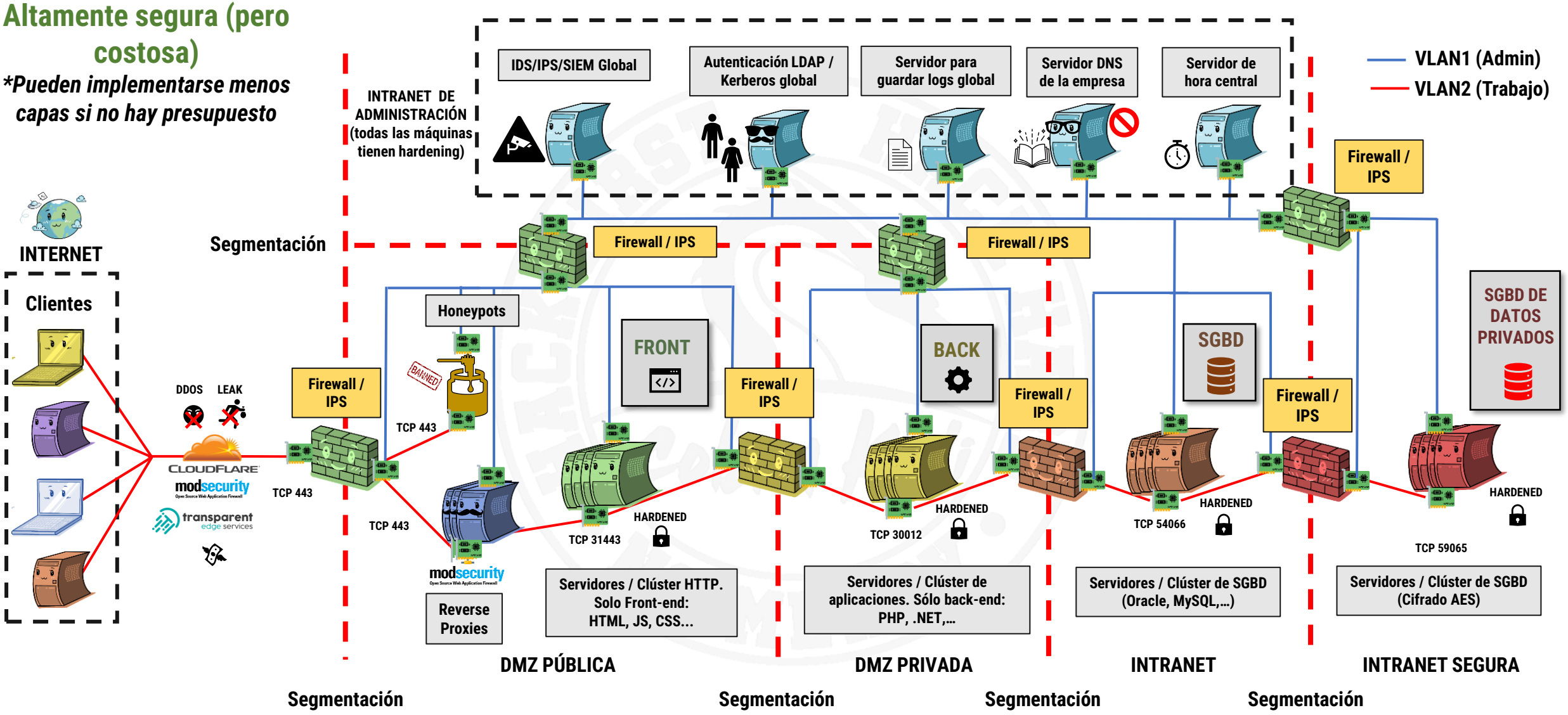
- **En este bloque aprenderás**
  - Como se diseña una infraestructura de **red altamente segura**
  - La enorme **importancia del aislamiento** en capas para la seguridad
  - El concepto de **Honeypot**, **CDN** y **VLAN**
  - La importancia de tener una **red de administración** de la infraestructura totalmente aislada
    - Y sus componentes principales
  - La importancia de la **vigilancia** de endpoints con IDS/IPS
  - Y relacionado con esto, la de **correlacionar todos los eventos** producidos
    - Y **analizarlos** con un SIEM y su relación con un SOC

SECURE NETWORK INFRASTRUCTURE (SNI)

Seguridad de Sistemas Informáticos

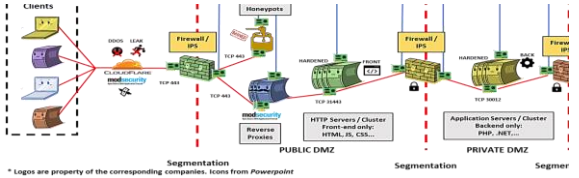
Altamente segura (pero costosa)

Pueden implementarse menos capas si no hay presupuesto



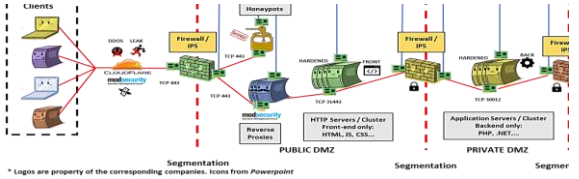
* Los logos son propiedad de sus compañías correspondientes. Iconos de *PowerPoint*. *Esta infraestructura está derivada de:* https://pciguru.files.wordpress.com/2013/12/200511-theultrasecurenetworkarchitecture.pdf

SNI: Componentes principales



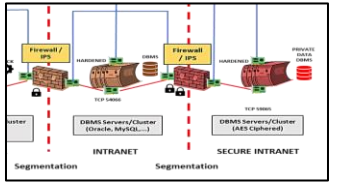
- **Una configuración de base segura para todos los servidores**
  - Los SSOO y los servicios de toda la infraestructura están configurados y protegidos mediante el uso adecuado de un **framework de seguridad** (Ej.: ISO 27001, **Tema 4**)
    - Basado en listas de controles de seguridad validadas (CIS, STIG…)
    - Utilizando políticas de seguridad más estrictas para los servidores orientados al público
  - El código de las aplicaciones debe seguir **metodologías de desarrollo de código seguro** (**Tema 6**)
  - En ambas LANs se deben usar SGBD debidamente protegidos, con los permisos y roles adecuados
  - **Los servidores con un rol crítico no permiten usos interactivos a sus usuarios**
    - Es decir, no uses para eso una máquina donde consultas correo web, navegación, veas vídeos...
- **Firewall de red y de aplicaciones (proxy firewalls-WAF) "externo"**
  - Reducen la amenaza de los ataques a aplicaciones (inyecciones de código...) que los firewalls de red no pueden detectar
  - También se deben utilizar firewalls PF individuales en cada host, abriendo sólo los puertos autorizados: `ufw`, `firewalld`

SNI: Componentes principales



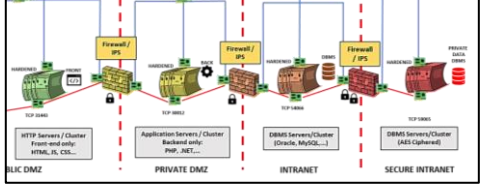
- **Dos DMZ con 2 firewalls SPI/NGFW**
  - **Una pública (cara a internet) y otra privada**
  - Los servidores de la **DMZ pública** contienen **solo la lógica de la interfaz de usuario de la aplicación**
    - Y están aislados (firewall SPI perimetral) de los sistemas con la lógica de aplicación en la DMZ privada
  - Por su parte, los servidores de la **DMZ privada** contienen la **lógica de negocio/aplicación**
    - Código del lado del servidor, PHP, ASP, ...)
    - Y enlaces a sistemas internos para tener capacidades de procesamiento adicionales
  - Esto permite reglas más detalladas para acceder a la lógica de la aplicación
    - Previniendo mejor llamadas no autorizadas a funcionalidades
    - ¡Así los ataques a aplicaciones lo tendrán mucho más complicado!
- **Dos LAN internas con doble cortafuegos SPI/NGFW**
  - **La LAN interna** que contiene los servidores y sistemas accesibles para los empleados
    - Y sistemas que no almacenan información confidencial
  - **La LAN segura**, que contiene servidores con **información cifrada y confidencial**
    - Que podría utilizarse para el robo de identidad u otros fraudes (números de tarjeta de crédito, números de cuenta de cheques, etc.) y por ello **su protección es crítica**

SNI: Componentes principales



- **Una política común de ubicación de los puertos de servicios**
  - Los puertos predeterminados para HTTPS (`tcp/443`) sólo se usan en la DMZ pública
    - **Debe eliminarse el uso de HTTP en toda la infraestructura**
    - Lo necesitamos para que los servidores "cara al público" sean accesibles en las rutas típicas
  - Los servicios web deben utilizar un cifrado adecuado **SIEMPRE**
    - TLS 1.3 si es posible
  - Para todas las demás conexiones a los servicios necesarios **se usarán puertos TCP y UDP no estándar**
    - Esto reduce la posibilidad de que atacantes identifiquen accidentalmente servicios e información
    - Muchos ataques automatizados solo examinan puertos estándar
- **Todos los puertos que no se usen deben estar cerrados**

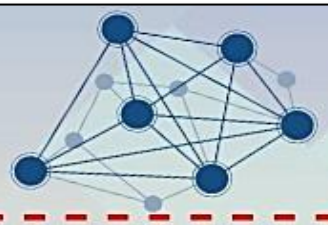
SNI: FIREWALLS



- La configuración de los **firewalls de red** es crítica
  - Configurar **reglas** para **restringir lo más posible y controlar** comunicaciones entrantes y salientes
    - **Reenviando puertos** a otras máquinas para conseguir el mejor **aislamiento de red** posible
  - Requiere un mecanismo fiable para identificar cada servidor con un rol crítico (Ej.: IPs estáticas)
  - Por ejemplo, **el firewall de la red DMZ pública...**
    - Se configuraría solo para permitir el tráfico TCP 80 y 443 entrante y saliente a las direcciones IP de los servidores HTTP orientados al público (reverse proxy / honeypots)
    - Un reverse proxy oculta completamente la arquitectura de red "al otro lado"
  - **Entre la DMZ pública y la DMZ privada...**
    - Sólo se abre el puerto 30012
    - Restringiendo sus comunicaciones a las direcciones IP de los servidores involucrados en nuestro ejemplo
  - **Entre la DMZ privada y la LAN interna...**
    - Sólo se abren los puertos estrictamente necesarios para comunicarse con los distintos servidores
    - Y restringidos a comunicaciones que vengan de direcciones IP específicas autorizadas
  - Igualmente, para el cortafuegos **entre la LAN interna y la LAN segura...**
    - Sólo debe estar abierto el puerto necesario para obtener acceso al servidor SGBD cifrado
    - Y restringido a las direcciones IP permitidas en la LAN interna

➢ Ejercicio **L7B1_FWFORWARD**

HONEYPOTS



What is a Honeypot?
by @SecurityGuill

What is a Honeypot?

- A Honeypot is an "**under surveillance**" system that is **exposed voluntarily** on the internet.
- The goal is to expose devices on the internet (often they are virtual) and to **monitor** them to retrieve information about **attackers**.
- Normally, these are systems to which people should **not have access**, this means that any **traffic arriving on a Honeypot is considered suspicious**.

2 Types of Honeypot

- Honeypot with **Low interaction**: consist of **emulating operating systems** and **services**. Activity is therefore limited to the degree of emulation offered by the honeypot.
- Honeypot with **Strong interaction**: they are different because they often involve the use of **real operating systems** and **real applications**.

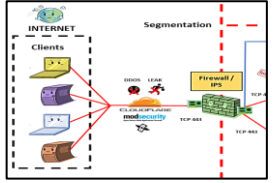
- The risks are many since our device is intended to be **compromised**. One of the advantages of this solution is that it's possible to obtain **more information** about attackers.

Application areas

- The use of a Honeypot can be applied in **two** different environments.
- **Production environment**: the main objective of a production honeypot is to **verify that the security measures are applied**, improve the protection of their network, discover vuln in their applications...
- **Research environment**: the goal is to collect as **much information about attackers** and their procedures. Some data collected: **network traffic**, **files sent** (malwares), **dumps**, what **ports** are most attacked, which **countries** come the attacks...

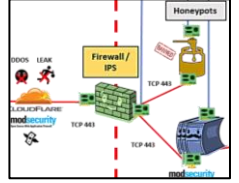
*Follow **@SecurityGuill** on **Twitter** for more about **Infosec** / **Cybersecurity***

SNI: Content Delivery Network (CDN)



- **Servicio basado en la nube que proporciona una capa de seguridad adicional**
  - Las solicitudes al firewall perimetral se filtran en la red de CDNs como CloudFlare o TransparentEdge
- **Proporciona características de seguridad avanzadas**
  - **Protección anti DDoS** completa y muy probada
  - Garantiza **conexiones https adecuadas**
  - **Firewall de aplicaciones web**: `mod_security` con reglas personalizadas
    - Da una protección avanzada contra XSS, inyección SQL, XSRF/CSRF, envenenamiento de parámetros, filtrado de archivos privados...
    - Y fugas de datos debido a una configuración incorrecta
  - Técnicas de "**inteligencia colectiva**" para prevenir nuevas amenazas
  - Protección/bloqueo basado en la reputación contra conexiones de **cliente malintencionadas**
  - Protección contra el **spam de comentarios (comment span)**
  - Protección contra el **hotlinking o el robo de contenido**
  - ...
- **Incluso sólo contratando servicios gratuitos obtenemos un beneficio de seguridad**

SNI: DMZ PÚBLICA

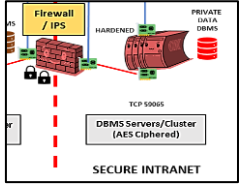


Seguridad de Sistemas Informáticos

- **Es accesible desde el exterior, pero no todo lo que hay dentro de ella**
  - **Proxies inversos + WAF: Las únicas máquinas** visibles tras del cortafuegos perimetral
    - Distribuye las solicitudes a las máquinas adecuadas, según su tipo/puerto dentro de la DMZ pública
    - Esto permite **ocultar el tipo y el número** de servidores desplegados en la DMZ pública
    - **Debe instalarse un WAF en esos servidores** (a menos que paguemos por el a la CDN)
    - Pueden implementar otras medidas de seguridad
      - Bloqueo de intentos de acceso fallidos repetidos para servicios populares: Fail2Ban
      - Bloquear las técnicas de escaneo de puertos, como las implementadas por `nmap`: PortSentry
  - **Honeypot**: Captura intentos de ataque de usuarios o herramientas automatizadas, bloqueando sus IP
    - Podemos derivar intentos de conexión HTTP al honeypot
    - **¡Los servidores reales siempre usarán conexiones cifradas!**
      - Los clientes reales no intentan degradar conexiones HTTPS a HTTP
      - Es una clara indicación de actividades potencialmente maliciosas
    - Abrir puertos asociados a servicios vulnerables conocidos, pero poner el honeypot detrás de ellos
      - Hay software para bloquear los intentos de escaneo a estos puertos "trampa": Portsentry
    - Más recursos sobre honeypots: https://github.com/paralax/awesome-honeypots

➢ Ejercicios **L7B2_FAIL2BAN, L7B2_PORTSENTRY**

SNI: LAN SEGURA

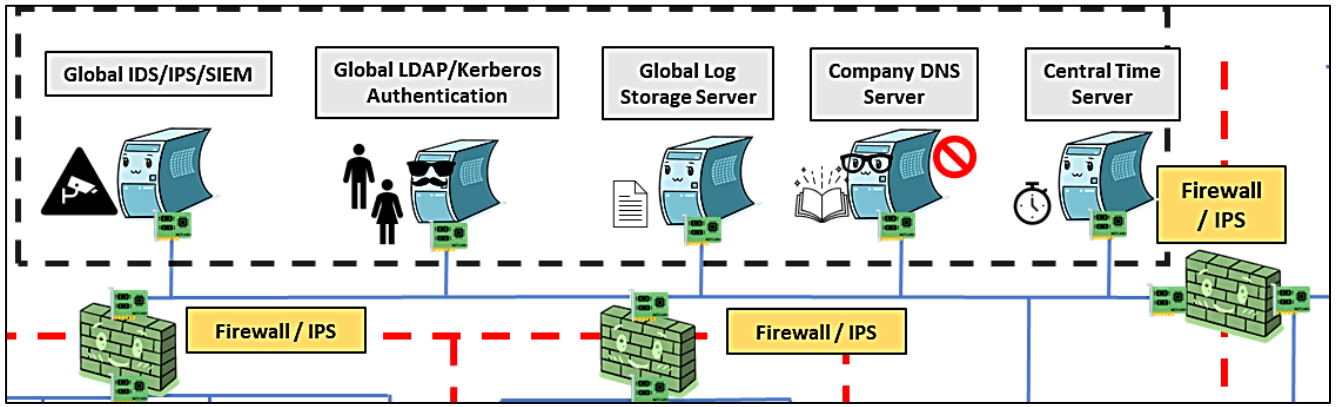


- **Los servidores ubicados en la LAN segura implementan un nivel adicional de seguridad al almacenar solo información cifrada**
- **La clave para proteger los servidores en esta LAN es que esa información...**
  - Venga sólo de lugares autorizados (gracias al cortafuegos)
  - Se cifre y almacene mediante un método de cifrado seguro (AES, ver el **Tema 2**)
  - Sólo se puede recuperar a través **de una política de seguridad muy estricta**
- **Un número muy limitado de sistemas, personal de administración y aplicaciones tienen acceso a estos servidores (y a la propia LAN segura)**
  - Los procesos de las aplicaciones con acceso a estos servidores **están restringidos y supervisados**
    - Para garantizar que solo se procesan los flujos de información adecuados
    - Cuando el acceso se aprueba, la información se descifra para las necesidades de procesamiento
  - Las salidas de información están muy restringidas, documentadas en detalle, filtradas por firewalls
  - También supervisadas y aprobadas por la administración **para cumplir con la ley vigente**

¿CREES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!

?

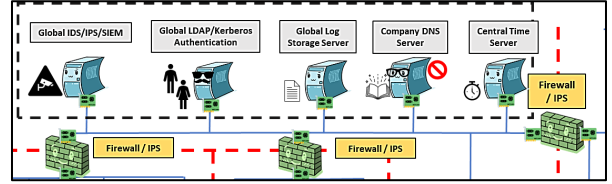
- **Eres capaz de hacer lo siguiente**
  - *Entender que la clave para un diseño de red altamente seguro consiste en la segmentación de redes, aislando diferentes funcionalidades en varias capas*
  - *Tener claro que una primera medida es separar el frontend del backend en un servicio web*
  - *Comprender en qué casos merecería la pena separar los datos almacenados por la aplicación en dos redes independientes*
  - *Entender que debemos situar una gran cantidad de medidas de seguridad en los puntos de la infraestructura que están expuestos a Internet, como WAFs, CDNs, firewalls profesionales...*
    - *Entendiendo de paso la funcionalidad de cada uno de ellos*
  - *Entender la razón por la cual todo servicio que no esté expuesto a Internet debería ofrecerse en puertos no estándar*
    - *Y que todos los demás puertos deberían cerrarse*



LAN de Administración de la SNI

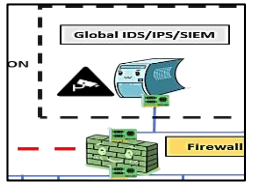
*Iconos por Bing Chat AI

SNI: LAN DE ADMINISTRACIÓN



- **Todos los componentes se supervisan a través de un sistema de gestión y monitorización**
- **Implementado en una LAN de administración protegida, compuesta por**
  - Intrusion Detection/Prevention System(s) (IDS/IPS)
  - Security Information and Event Management (SIEM)
  - Domain Name Services (DNS)
  - Servidores Kerberos (autenticación)
  - Servidor(es) de tiempo
  - Servidor(es) de log centralizado(s) (`syslog`)
- **Todos estos servidores también están separados por cortafuegos de las DMZ y la LAN segura**
  - Para permitir un mejor control y protección

IDS/IPS/SIEM GLOBAL



Seguridad de Sistemas Informáticos

- **Esta arquitectura tiene sistemas de detección de intrusiones basados en red (NIDS) y basados en host (HIDS) correctamente administrados**
  - **Los NIDS** (Suricata, SNORT, Maltrail...) **supervisan subredes críticas en las DMZ y la LAN segura**
    - Esto permite detectar cualquier ataque basado en red o anomalías inesperadas del tráfico de red
    - Se pueden poner NIDS adicionales en otros segmentos de red, pero esto requiere un "tuning" intenso para minimizar alertas falsas positivas y otros problemas
  - Los **HIDS** detectan cambios de archivos, ataques de fuerza bruta, etc. en los servidores
    - Todos los servidores en las DMZ y los de la LAN segura
    - Cualquier servidor que procese información confidencial en la LAN interna
    - Ejemplos de software HIDS popular son: Wazuh, OSSEC, AIDE, Tripwire...
- **Los NIDS y HIDS envían información a la consola de un sistema de detección de intrusiones en la LAN de administración para el seguimiento y la supervisión**
  - Por ejemplo, Alienvault OSSIM (SIEM) es un sistema de gestión de eventos capaz de hacer eso

➢ Ejercicios **L7B3_IDSMALTRAIL, L7B3_WAZUHSCAN**

IDS/IPS

Seguridad de Sistemas Informáticos

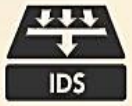
What is IDS & IPS ?

by @ SecurityGuill

What is an IDS?

• An IDS (**Intrusion Detection System**) **analyzes** and **monitors network traffic** for signs that attackers use a **known cyber threat** to **infiltrate** or **steal data** from your **network**.

• IDS systems **compare current network activity with a database of known attacks** to detect various types of behaviors such as security policy violations, malware and port scanners.



• With IDS systems, it is necessary for a human or other system to **take over to review the results** and **determine the actions to be implemented**, which can be a full-time job depending on the amount of traffic generated by day.

Common points

• **Both read network packets** and **compare the contents to a database of known threats.**

Why you need IDS/IPS Technology

• **Conformity reasons** (To prove that you have implemented the necessary means to protect your data)

• To **protect your data** (especially if you collect a **large amount** of **personnal data**)

• **Automation**

What is an IPS?

• An IPS (**Intrusion Prevention System**) acts in the same area of the network as a **firewall**, between the outside world and the **internal network**.

• IPS systems proactively **reject network packet** based on a **security profile** if these packets represents a **known threat**.

• The goal of the IPS is to **capture dangerous packets** and **remove them before they reach their target**.

• It is more passive than an IDS and simply requires **regular updating of the database** to incorporate **new threat information**.

Follow @ SecurityGuill on Twitter for more about Infosec / Cybersecurity

IPS vs IDS

IPS	IDS
IPS is a control system which accepts and rejects a packet based on the ruleset.	IDS is a detection and monitoring tool which do not take action on their own.
IPS	IDS
IPS requires that the database to regularly updated with new threat data.3	IDS requires human or another system to examine results.
IPS	IDS
It should be placed after the firewall device in a network.	IDS should be placed after the firewall.
IPS	IDS
IPS provides detection and reaction support.	IDS provides decoupling detection and reaction functionalities.
IPS	IDS
In IPS, configuration mode is inline mode or as end host.	In IDS, configuration mode is the inline mode, generally on layer 2.

www.educba.com

IDS/IPS

Seguridad de Sistemas Informáticos

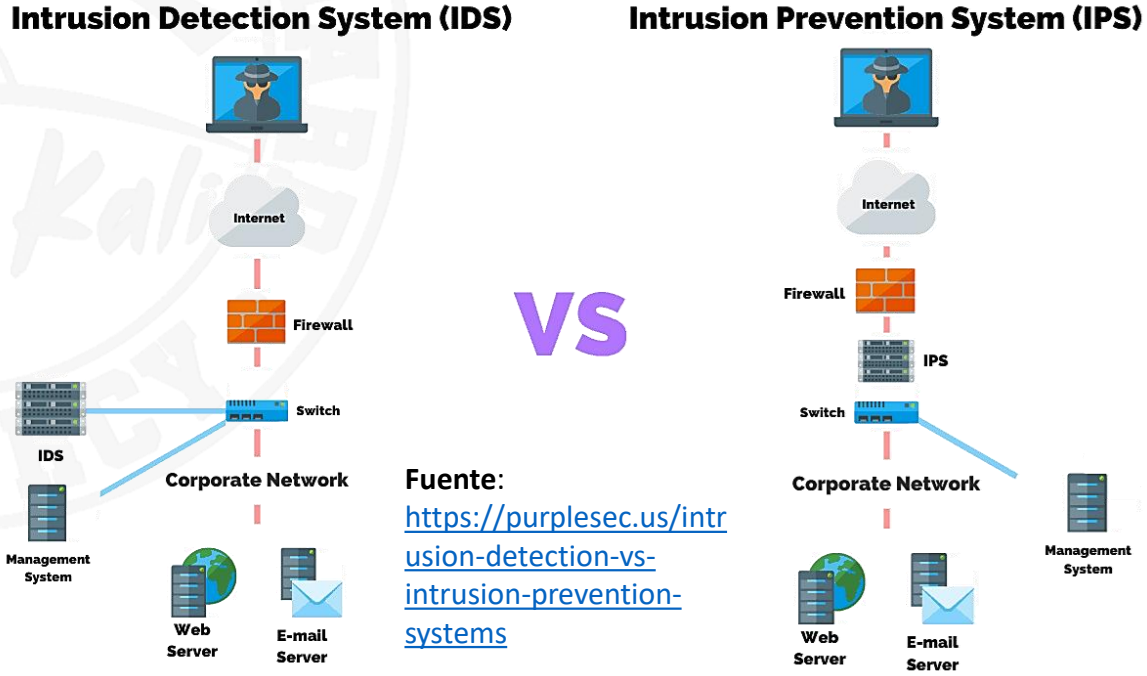
- La seguridad de una infraestructura / equipo no se puede considerar “seria” sin tener estos sistemas
  - Un IDS tiene un carácter **reactivo**: Avisa de lo que detecta, pero no lo bloquea
  - Un IPS tiene carácter **proactivo**: Bloquea lo que detecta
- Ambos sistemas pueden (y deben) **combinarse** en una red
- Requieren “**entrenamiento**” y adaptación a cada contexto para no dar falsos positivos
  - Necesitan “rodaje” para que no interfieran con el tráfico legítimo de una red

IDS Vs IPS

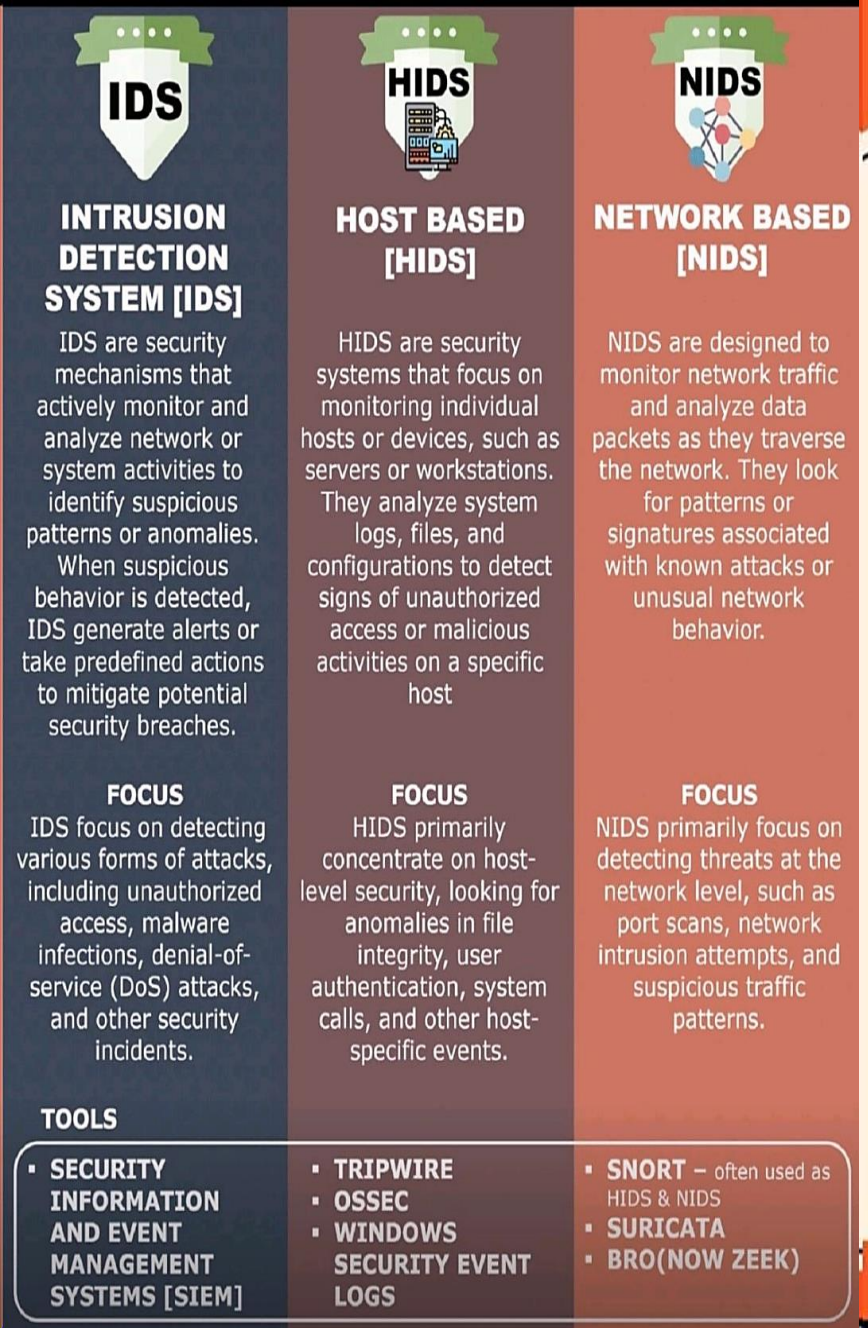
Most organizations have either an IDS or an IPS, and many have both as part of their security information and event management framework.

	IDS	IPS
NAME	Intrusion detection system	Intrusion prevention system
DESCRIPTION	A system that monitors network traffic for suspicious activity and alerts users when such activity is discovered.	A system that monitors network traffic and alerts for suspicious activity, like an IDS, but also takes preventative action against suspicious activity.
LOCATION	A host-based intrusion detection system is installed on the client computer. A network-based intrusion detection system resides on the network.	Located between a company's firewall and the rest of its network.
USE	Warns of suspicious activity taking place, but it doesn't prevent it.	Warns of suspicious activity taking place and prevents it.
FALSE POSITIVE	IDS false positives are usually just a minor inconvenience. Although the IDS incorrectly labels legitimate traffic as malicious, it does not prevent the traffic from entering the network.	IPS false positives can be more serious. When an IPS mistakes legitimate traffic for a threat, it stops the legitimate traffic from entering the network, which could impact any part of the organization, not just the IT team.

Fuente: https://www.linkedin.com/in/sabrinakaur



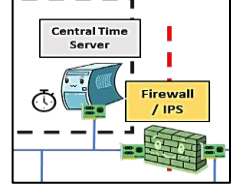
Fuente: https://purplesec.us/intrusion-detection-vs-intrusion-prevention-systems



Fuente: https://www.facebook.com/redback/?locale=az_AZ

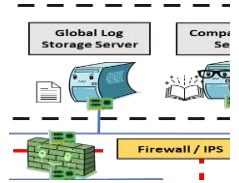
Fuente: https://pe.linkedin.com/posts/luis-gastulo-salazar-081732129_xdr-vs-siem-activity-7046894404757803008-quco

SERVIDOR DE TIEMPO CENTRAL



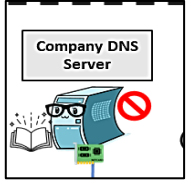
- **Un servidor de hora permite hacer un análisis correcto de la información almacenada en los servidores de log**
- **Determinar qué zona horaria utilizar en la red es vital**
  - Es fundamental tener una zona horaria y control de tiempo único y coherente para todos los dispositivos
  - Para que todas las entradas de todos los logs se puedan **ordenar temporalmente** de forma correcta
  - Especialmente al diagnosticar o identificar un ataque que puede estar ocurriendo contra varios dispositivos en diferentes partes de la red
- **Los dispositivos de infraestructura de red (routers, conmutadores, firewalls, servidores,...), suelen usar Universal Coordinated Time (UTC)**
  - El uso de UTC permite que todos los eventos se muestren en el mismo período de tiempo sin tener que realizar conversiones de zona horaria
- **También evita comportamientos extraños con actualizaciones o archivos del SO**
  - Que ocurren si la hora se desincroniza accidentalmente respecto a servidores externos que interactúan con nuestra infraestructura

SERVIDOR GLOBAL DE ALMACENAMIENTO DE LOGS



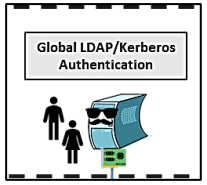
- **Es necesario guardar la información de registro/log del sistema (`syslog`)**
- **De todos los dispositivos de la infraestructura (firewalls, routers, switches, servidores...) y otros sistemas críticos**
  - En un sistema de log centralizado (**Tema 3**)
  - Las grandes organizaciones suelen tener servidores conectados a un Network-Attached Storage (NAS) a través de un Storage Area Network (SAN) de gran capacidad
  - Así se dispone de una gran cantidad de almacenamiento para los logs de toda la infraestructura
- **Todos los dispositivos críticos deben transmitir su información de log al servidor centrar para su conservación y análisis posterior**
  - Análisis que se pueden hacer con técnicas de ML/IA como las que se ven en la asignatura SI
- **Estos sistemas críticos deben registrar tantos eventos exitosos y fallidos como sea posible (el Tema 3 detalla cuáles)**
  - Sólo así podremos tener una imagen completa de los eventos con fines de análisis y diagnóstico
  - También se aplica a los eventos de las aplicaciones que están en nuestra infraestructura (**Tema 6**)

SERVIDORES DNS INTERNOS



- **Configurar un servidor DNS para uso interno proporciona una serie de ventajas**
  - Bloqueo de accesos a sitios malintencionados conocidos (malware, anuncios)
    - **Hay disponibles listas negras de IPs maliciosas conocidas**
      - https://github.com/StevenBlack/hosts, https://blocklistproject.github.io/Lists/
  - Esto es especialmente importante en servidores que permiten el uso interactivo del usuario
    - Como tener un plugin adblocker, pero **que sirve para todos los dispositivos** que pasan a través del DNS
    - Por tanto, reduce la probabilidad de ataques...¡y no solo los basados en navegadores!
  - Ej.: PiHole (https://pi-hole.net/)
- **También podemos bloquear conexiones a ciertos sitios web por otras razones**
  - Las peticiones no bloqueadas se reenvían al DNS del proveedor de servicios de Internet (ISP)
- **Sin embargo, debido a las amenazas potenciales que sufren los servidores DNS, intenta dirigir las consultas de DNS públicas al DNS de tu ISP**
  - Especialmente a **proveedores DNS públicos seguros**, como NextDNS, etc. (**Laboratorio 1**)
  - Pero en este caso haciéndose una cuenta y **usando sus capacidades extendidas**

Autenticación global Kerberos / LDAP



- **El protocolo de autenticación Kerberos es uno de los más seguros**
  - Soportado por los principales SO (ASR detalla más la autenticación)
  - Kerberos utiliza criptografía segura para que un cliente pueda probar su identidad ante un servidor (y viceversa) a través de una conexión de red insegura
  - Tras esto, pueden cifrar sus comunicaciones para garantizar la privacidad y la integridad de los datos
- **Todos los servidores deben usar Kerberos para autenticarse entre sí**
  - Cada sesión individual que tenga transacciones de una aplicación debe generar sus propias claves
  - Para que las sesiones se protejan y cifren individualmente
- **Minimiza ataques AitM, sniffing de paquetes y session hijacking**
  - Proporciona un nivel adicional de seguridad por el cifrado de comunicaciones entre sistemas
  - Incluso si un atacante consigue entrar en la red interna, toda la comunicación está protegida y cifrada
  - Las infraestructuras de Windows Active Directory usan Kerberos como mecanismo de autenticación
- **Se puede usar como complemento la biometría u otro MFA (ver Tema 6)**

¿CREES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!

?

- **Eres capaz de hacer lo siguiente**
  - *Entender que tener una red de administración separada es primordial para mantener un alto nivel de seguridad*
  - *Comprender la función de seguridad que cumplen los IDS, los IPS y los SIEM*
  - *Entender por qué es tan importante tener un servidor de tiempo sincronizado central y único a toda la infraestructura*
  - *Entender por qué es tan importante tener un servidor de almacenamiento de logs central y único a toda la infraestructura*
  - *Comprender qué labor de seguridad puede cubrir un servidor DNS interno*
  - *Comprender para qué sirve el protocolo Kerberos y un LDAP en la infraestructura de una empresa*

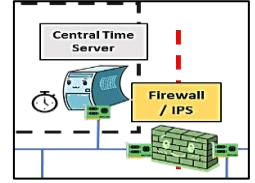
Otras medidas de seguridad de la SNI

*Iconos por Bing Chat AI

SUBREDES

- **Hay varias mejoras que pueden aumentar el nivel de seguridad de la arquitectura**
- **La 1ª medida es extender el uso de varias subredes IP a toda la infraestructura**
  - Y no sólo a la LAN de administración
  - Se pueden usar firewalls **con varias NICs** para aislar diferentes subredes entre capas de red
  - Cada DMZ **pueden tener sus propias subredes IP que no reflejen ninguna otra subred**
    - Es decir, si la subred `10.x.x.x` se usa internamente y la subred privada `192.168.x.x` se usa para la LAN de administración, las DMZ deben utilizar direcciones IP en las subredes `172.16-31.x.x`
  - La LAN segura también debe tener su propia subred IP, no utilizada en ninguna otra
- **El uso de varias subredes IP aumentará la cantidad de enrutamiento y la complejidad de la arquitectura de red**
- **Pero también reducirá significativamente la probabilidad de que un atacante obtenga acceso a los sistemas**
  - Y el tiempo para implementar y afinar mejor las actividades de supervisión de la red

VLANs



- **Las VLANs segregan lógicamente el tráfico de red**
  - **Separan tráfico** en función de su “riesgo”, la calidad de servicio u otras consideraciones. Ej.:
    - Tráfico para el control y monitorización de las operaciones
    - Tráfico interno de LAN diferentes
    - Tráfico y transacciones originados en Internet
- **La VLAN1 se recomienda para control y supervisión**
  - Solo el personal de administración de red, de sistema y de seguridad debe tener acceso a esta VLAN
  - Debe usar direccionamiento IP estático, con un esquema distinto al de cualquier otra red
  - La mayoría de los servidores vienen con varias NIC; una se puede configurar para usar solo la VLAN1
  - Esto permite que el servidor sea monitorizado y controlado a través de una red segura
    - A la que solo el personal de administración de la red y del sistema tiene acceso
- **Se pueden añadir otras VLAN (VoIP, de empleados (navegación, e-mail...), Wi-Fi...**
  - La clave para una buena implementación de VLAN **es planificarlas rigurosamente**
  - Hay ataques que permiten eludir la segregación de VLAN, pero todos ellos se basan en una configuración incorrecta de las VLAN

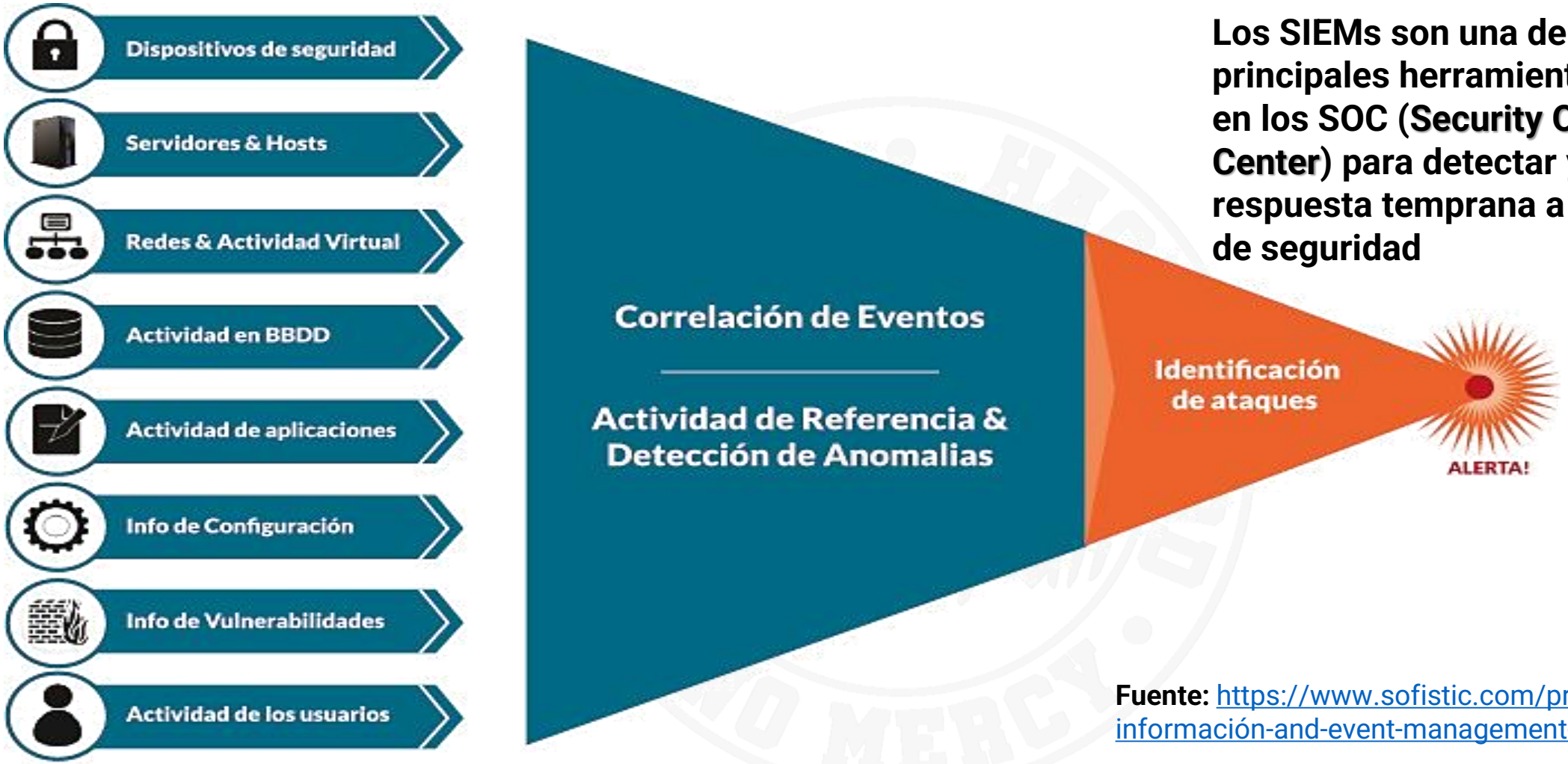
MÁQUINAS VIRTUALES

- **Hoy en día, la mayoría de las infraestructuras de máquinas complejas se crean con máquinas virtuales o contenedores (¡como nuestros laboratorios! ☺)**
- **La capacidad de ejecutar varios SSOO en un sistema informático o en un clúster de equipos maximiza el uso del hardware y simplifica su implementación**
- **Y también tiene ventajas de seguridad: pueden regenerarse**
  - Si un HIDS detecta que un servidor se ha dañado o manipulado, se puede configurar para reiniciar automáticamente el servidor
    - Pero desde una segunda imagen "limpia" intercambiable en caliente, disponible para reemplazar la dañada
  - El sistema reinicia así desde una imagen conocida y no comprometida
    - Y luego se vuelve a poner en servicio
    - Si un atacante compromete el servidor, ¡cualquier rootkit o malware se elimina automáticamente!
      - Porque el servidor siempre se reinicia desde una imagen limpia y conocida
  - Los efectos del ataque se detectan y se eliminan debido a este mecanismo de respuesta

Motor de correlación de un IDS

- Añadir una **aplicación/motor de correlación de syslog/IDS/IPS** sobre el servidor de log centralizado
  - Security Information and Event Management - SIEM
- Buscan patrones en toda la información de log y alertas recibida de todos los componentes de la infraestructura (de los IDS/IPS, distintos servidores...)
  - Estos podrían indicar un ataque o una anomalía de la red que debe ser investigada
  - Los patrones pueden identificarse mediante sistemas de reglas u **otras técnicas de IA** vistas en SI
- Se necesitan reglas apropiadas para dichos motores de correlación
  - **Se requiere mucha planificación y supervisión de la información** para desarrollarlas correctamente
  - Una vez implementadas, estos sistemas pueden reducir significativamente la cantidad de alertas
  - Así los administradores de redes y seguridad puedan centrarse en las amenazas y anomalías más probables (**threat hunting**)

Motor de correlación de un IDS



Los SIEMs son una de las principales herramientas usadas en los SOC (Security Operations Center) para detectar y dar una respuesta temprana a incidentes de seguridad

Fuente: https://www.sofistic.com/productos/security-información-and-event-management-siem/

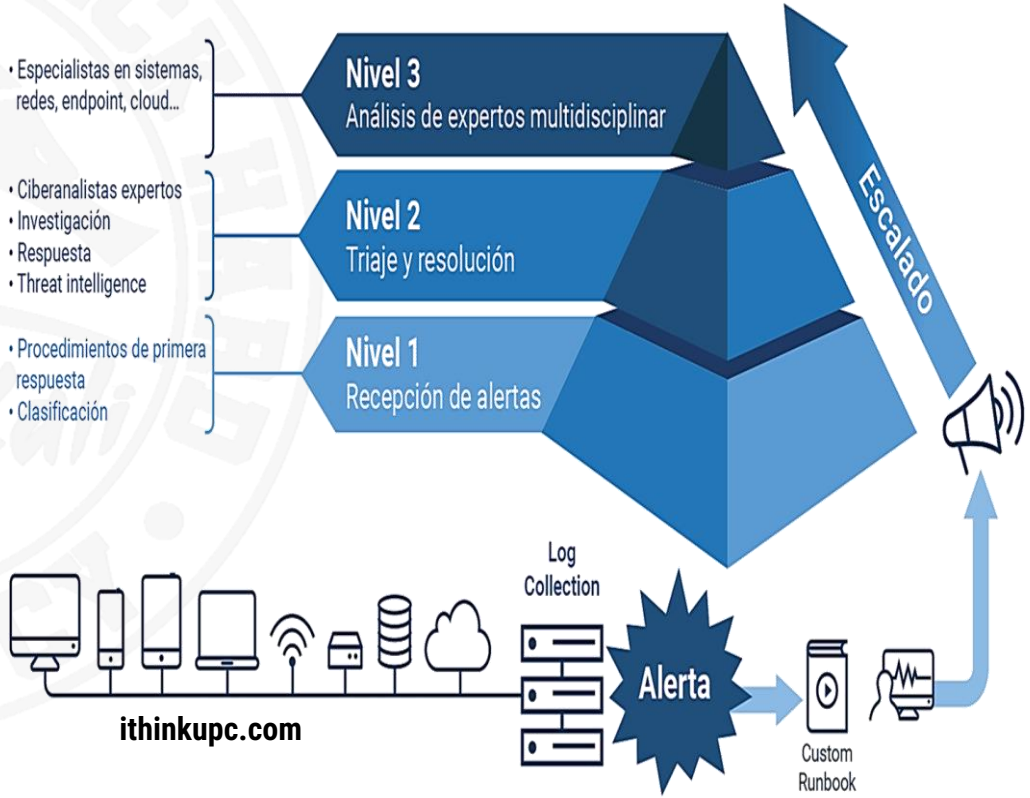
SECURITY OPERATIONS CENTER (SOC)

- Es importante entender que es un SOC y como hace su “vigilancia”,
- ¡Hay muchos puestos de trabajo para trabajar en ellos!

Toda esta información de los sistemas de un cliente se examina en la sala de control del SOC (propio o alquilado) con programas especializados

La detección de una alerta es tratada por los operarios del SOC de acuerdo a procedimientos documentados de respuesta
Si la alerta es grave, “escala” a niveles superiores del SOC para ser tratada adecuadamente
Si es muy grave, escala a nivel 3 donde debe ser tratada por el personal con más conocimiento y especialización

Fuente: https://digitalguardian.com/blog/how-build-security-operations-center-soc-peoples-processes-and-technologies



Fuente: https://blog.elhacker.net/2021/03/que-es-como-funciona-centro-de-operaciones-de-seguridad-soc.html

SOAR (Security Orchestration, Automation & Response)

Seguridad de Sistemas Informáticos

- Conjunto de servicios y herramientas que automatizan la prevención y respuesta contra ciberataques
- Unifica integraciones y define cómo deben ejecutarse las tareas
- Desarrolla un plan de respuesta a incidentes adaptado a las necesidades de una organización
- En otras palabras: proporciona la máxima automatización a la hora de lidiar con incidentes de seguridad

¿CREES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!

?

- **Eres capaz de hacer lo siguiente**
  - *Comprender porque tener diferentes rangos de IPs en las distintas redes es un medio de aislamiento más*
  - *Entender que las VLAN son una forma de aislar completamente el tráfico perteneciente a distintas redes*
  - *Tener claro que el uso de máquinas virtuales es básico también para aislar servicios entre ellos*
  - *Comprender que la correlación entre la información todos los logs recibidos de todos los sistemas, incluyendo el uso de técnicas de IA, es básica para detectar amenazas que estén en marcha en la infraestructura*
    - *Y que esto necesita reglas para poder funcionar correctamente*
  - *Entender que este análisis de la información de log de todos los sistemas es la función de los sistemas SIEM*
    - *Y que los SIEM son una parte muy importante de un SOC*

< Ir al Índice

INTRODUCCIÓN AL PENTESTING DE RED

Como comprobar la seguridad de una red

*Iconos por Bing Chat AI

Fuente: Bing Chat AI

Escaneo activo >

Obtener información >

Otras técnicas >

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

¿QUÉ TE VAS A ENCONTRAR EN ESTE BLOQUE?

En este bloque aprenderás

- Qué es y para qué se usa el **MITRE ATT&CK**, y su relación con los CIS Benchmarks
- La importancia de la **etapa de reconocimiento** para iniciar un ataque
- Cómo hacer un **escaneo activo** de una máquina
- **Otras posibles formas de reconocimiento**

El MITRE ATT&CK

https://attack.mitre.org/

- **Base de conocimientos internacional libre y accesible de tácticas y técnicas de adversarios basadas en observaciones del mundo real**
  - Realista, actualizada, usada mundialmente... la mejor guía para aprender a "atacar"
- **Usada como base para desarrollar threat models específicos (ver Tema 6) y metodologías en todos los sectores y comunidades**
- **Divide las tácticas y las técnicas en 14 etapas**
  - Llamadas adversary lifecycle
- **Describiremos aquí sólo la 1ª: Reconocimiento (Reconnaisance)**
  - Esto cubre las dos primeras etapas de nuestra "kill chain"
  - El resto de las etapas pertenecen a las fases de explotación y post-explotación
    - Se revisarán en el último tema de teoría
- **Aquí veremos una introducción y algunos ejemplos**
  - Pero puedes seguir los enlaces para profundizar en los detalles

MITRE ATT&CK y los CIS Benchmarks

- ¿Te acuerdas de esta parte del Tema 4? (los **CSC Controls**)
  - No te conté toda la verdad...☺
- Cada control técnico de seguridad del CIS está MAPEADO a una técnica del MITRE ATT&CK
  - Aunque solo para las versiones más recientes de los productos…
- ¿Qué significa?
  - ¡Que ahora puedes usar cada control técnico de seguridad del CIS para "**enfrentarte**" a ciertas técnicas del MITRE ATT&CK!
  - **¡Defensa y ataque están así relacionadas!**

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1499, T1499.001	TA0005	M1022

TA0043. Reconnaissance

- El adversario está tratando de recopilar información
- Cualquier cosa que se pueda usar para planificar operaciones futuras y adquirir objetivos
  - Esa información también ayuda en las fases futuras del ciclo de vida del ataque
- La información se puede obtener activa o pasivamente
  - Puede incluir detalles de la organización víctima, su infraestructura o su personal...
- Vamos a describir algunas de estas técnicas técnicas

ATT&CK®

T1595: Active Scanning

Explorando al adversario para obtener información del mismo

*Iconos por Bing Chat AI

T1595: Active scanning

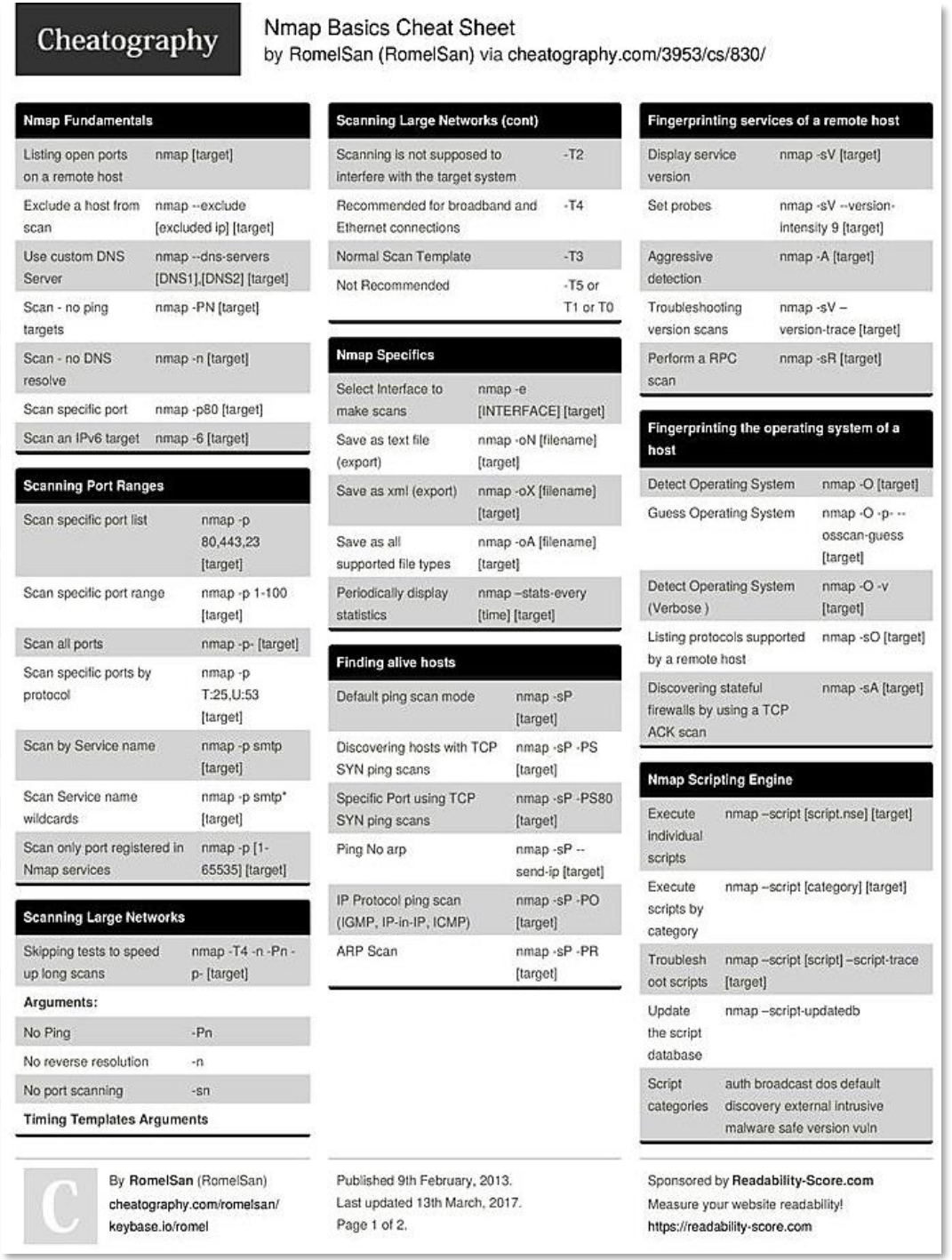
- **El adversario sondea la infraestructura de la víctima a través del tráfico de red**
  - https://attack.mitre.org/techniques/T1595/
  - A diferencia de otras formas de reconocimiento, que no implican una interacción directa con la infraestructura, **esta sí**
  - Escanea bloques de IP y / o vulnerabilidades potenciales
  - Interactúa con la infraestructura de destino tratando de obtener la mayor cantidad de información posible
  - Estos escaneos activos **pueden ser detectados fácilmente** por algunas de las soluciones de seguridad que hemos mencionado: IDS, IPS...

- **Una de las herramientas más populares para hacer escaneo activo es Nmap (el Lab 8-9 se dedicará a esta herramienta)**
- **El software automatizado de escaneo de vulnerabilidades (Seminario 3) también se puede incluir en esta categoría**

TÉCNICAS DE ESCANEO ACTIVO

Seguridad de Sistemas Informáticos

- **Estas técnicas tienen dos objetivos**
  - Localizar sistemas "vivos" (visto en **Tema 1**)
  - Crear un perfil de cada sistema “vivo” para investigarlo
- **Tras un escaneo de Nmap deberíamos saber**
  - Cuántos **puertos** tiene abiertos cada sistema
  - Qué **servicios** se ejecutan detrás de estos puertos
    - Nombre, versión, otra información útil...
  - **Información extendida** de cada servicio
    - Vulnerabilidades potenciales, configuración, ficheros…
- **Los servicios que usan el protocolo HTTP nos dan más opciones de enumeración**
  - Con herramientas especializadas
  - Localizar vulnerabilidades potenciales
    - Generales, especializados por su tecnología (CMS...)...
  - Directorios y archivos comprometedores



Cheatography

Nmap Basics Cheat Sheet
by RomelSan (RomelSan) via cheatography.com/3953/cs/830/

Nmap Fundamentals

Listing open ports on a remote host	nmap [target]
Exclude a host from scan	nmap --exclude [excluded ip] [target]
Use custom DNS Server	nmap --dns-servers [DNS1],[DNS2] [target]
Scan - no ping targets	nmap -PN [target]
Scan - no DNS resolve	nmap -n [target]
Scan specific port	nmap -p80 [target]
Scan an IPv6 target	nmap -6 [target]

Scanning Port Ranges

Scan specific port list	nmap -p 80,443,23 [target]
Scan specific port range	nmap -p 1-100 [target]
Scan all ports	nmap -p- [target]
Scan specific ports by protocol	nmap -p T:25,U:53 [target]
Scan by Service name	nmap -p smtp [target]
Scan Service name wildcards	nmap -p smtp* [target]
Scan only port registered in Nmap services	nmap -p [1-65535] [target]

Scanning Large Networks

Skipping tests to speed up long scans	nmap -T4 -n -Pn -p- [target]
Arguments:	
No Ping	-Pn
No reverse resolution	-n
No port scanning	-sn
Timing Templates Arguments	

Scanning Large Networks (cont)

Scanning is not supposed to interfere with the target system	-T2
Recommended for broadband and Ethernet connections	-T4
Normal Scan Template	-T3
Not Recommended	-T5 or T1 or T0

Nmap Specifics

Select Interface to make scans	nmap -e [INTERFACE] [target]
Save as text file (export)	nmap -oN [filename] [target]
Save as xml (export)	nmap -oX [filename] [target]
Save as all supported file types	nmap -oA [filename] [target]
Periodically display statistics	nmap –stats-every [time] [target]

Finding alive hosts

Default ping scan mode	nmap -sP [target]
Discovering hosts with TCP SYN ping scans	nmap -sP -PS [target]
Specific Port using TCP SYN ping scans	nmap -sP -PS80 [target]
Ping No arp	nmap -sP --send-ip [target]
IP Protocol ping scan (IGMP, IP-in-IP, ICMP)	nmap -sP -PO [target]
ARP Scan	nmap -sP -PR [target]

Fingerprinting services of a remote host

Display service version	nmap -sV [target]
Set probes	nmap -sV --version-intensity 9 [target]
Aggressive detection	nmap -A [target]
Troubleshooting version scans	nmap -sV –version-trace [target]
Perform a RPC scan	nmap -sR [target]

Fingerprinting the operating system of a host

Detect Operating System	nmap -O [target]
Guess Operating System	nmap -O -p- --osscan-guess [target]
Detect Operating System (Verbose)	nmap -O -v [target]
Listing protocols supported by a remote host	nmap -sO [target]
Discovering stateful firewalls by using a TCP ACK scan	nmap -sA [target]

Nmap Scripting Engine

Execute individual scripts	nmap –script [script.nse] [target]
Execute scripts by category	nmap –script [category] [target]
Troubleshoot scripts	nmap –script [script] –script-trace [target]
Update the script database	nmap –script-updatedb
Script categories	auth broadcast dos default discovery external intrusive malware safe version vuln

By **RomelSan** (RomelSan)
cheatography.com/romelsan/
keybase.io/romel

Published 9th February, 2013.
Last updated 13th March, 2017.
Page 1 of 2.

Sponsored by **Readability-Score.com**
Measure your website readability!
https://readability-score.com

Escaneos activos avanzados de Nmap

- **NMap implementa numerosas técnicas de enumeración de sistemas y de escaneo de puertos y servicios**
  - Ej.: `nmap -sS -A -sV -O –p -` ejecuta un **escaneo detallado, pero más lento y detectable**
  - Obtiene la máxima información del objetivo
    - `-sS`: Utiliza el tipo de exploración TCP SYN
      - Potencialmente más eficaz si hay cortafuegos
    - `-A`: Detecta versiones de servicios y del SO, hace un `traceroute`, y lanza varios scripts
    - `-sV`: Sondea los puertos abiertos
      - Para determinar el servicio y la versión del mismo en ejecución
    - `-O`: Habilita la detección de tipo y versión del SO
    - `-p -`: Escanea un rango de puertos
      - `-` escanea todos los puertos, pero podemos especificar un rango

```
root@kali:~# nmap -sS -A -sV -O -p - 192.168.14.2
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-02 13:11 CEST
Nmap scan report for 192.168.14.2
Host is up (0.00029s latency).
```

Puerto/protocolo, estado del puerto, servicio que escucha en él

```
21/tcp  open  ftp         OpenBSD ftpd 6.4 (Linux port 0.17)
22/tcp  open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protoco
l 2.0)
| ssh-hostkey:
|   2048 42:62:a8:1b:16:da:24:bb:52:da:ef:b4:9e:86:87:31 (RSA)
|   256 77:73:2a:b7:4c:8b:97:33:c4:8f:f1:2d:39:97:82:56 (ECDSA)
|   256 b6:46:3e:1c:0d:6b:81:2b:65:e6:aa:56:45:2c:1e:ee (ED25519)
23/tcp  open  telnet      Linux telnetd
80/tcp  open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
MAC Address: 08:00:27:D5:89:36 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: server1804; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1s, deviation: 0s, median: 1s
|_nbstat: NetBIOS name: SERVER1804, NetBIOS user: <unknown>, NetBIOS MAC: <unkno
wn> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: server1804
|   NetBIOS computer name: SERVER1804\x00
|   Domain name: \x00
|   FQDN: server1804
|_  System time: 2019-10-02T11:12:04+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
```

Escaneo activo. Interpretando los resultados de Nmap

Seguridad de Sistemas Informáticos

```
root@kali:~# nmap -sS -A -sV -O -p - 192.168.14.2
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-02 13:11 CEST
Nmap scan report for 192.168.14.2
Host is up (0.00029s latency).
Not shown: 65529 closed ports
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         OpenBSD ftpd 6.4 (Linux port 0.17)
22/tcp  open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protoco
l 2.0)
| ssh-hostkey:
|   2048 42:62:a8:1b:16:da:24:bb:52:da:ef:b4:9e:86:87:31 (RSA)
|   256 77:73:2a:b7:4c:8b:97:33:c4:8f:f1:2d:39:97:82:56 (ECDSA)
|_  256 b6:46:3e:1c:0d:6b:81:2b:65:e6:aa:56:45:2c:1e:ee (ED25519)
23/tcp  open  telnet      Linux telnetd
80/tcp  open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
MAC Address: 08:00:27:D5:89:36 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: server1804; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1s, deviation: 0s, median: 1s
|_nbstat: NetBIOS name: SERVER1804, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: server1804
|   NetBIOS computer name: SERVER1804\x00
|   Domain name: \x00
|   FQDN: server1804
|_  System time: 2019-10-02T11:12:04+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
```

Software concreto (y su versión) que proporciona los servicios FTP y SSH. Muy útil para buscar sus vulnerabilidades / exploits en las BBDD que los enumeran (https://www.cvedetails.com/)

Clave pública de la máquina para distinguirla de otras cuando se realiza la conexión a través de SSH (PKI)

Servidor web / telnet y su versión: igual que los servicios anteriores

Servicio SAMBA (protocolo SMB para compartir archivos de Microsoft, pero su implementación de Linux)

PC estándar (no un teléfono móvil, impresora, dispositivo IoT...) con un Linux en la misma subred que el nuestro (1 salto implica que no hay "salto" entre redes)

Versión de Ubuntu, aunque podría ser falsa. Además, también se puede inferir por las versiones específicas de los servicios expuestos (cada versión del SO suele tener versiones ligeramente diferentes de sus servicios, y podríamos buscar en los repositorios para ver qué versiones se distribuyen con diferentes versiones de un mismo SO). Una vez más, con esto podemos buscar vulnerabilidades específicas de esta versión

Datos de instalación de SMB

El motor de scripts NSE permite sacar el máximo partido a las funcionalidades y versatilidad de NMap. Y recuerda: ¡Puertos abiertos desconocidos pueden indicar la presencia de malware!

Recopilando información técnica y personal

Técnicas para estudiar personas y sitios web

*Iconos por Bing Chat AI

TA0043. Reconnaissance: Técnicas relacionadas con personas

T1592. Gather Victim Host Information

- https://attack.mitre.org/techniques/T1592/
- **Datos administrativos** (por ejemplo: nombre, IP asignada, funcionalidad, etc.)
- **Configuración** (por ejemplo: SO, idioma, etc.)
- Información sobre elementos de hardware, software y firmware
- NMap y Wazuh (con su inventario) pueden proporcionarnos este tipo de información

T1590. Gather Victim Network Information

- https://attack.mitre.org/techniques/T1590/
- **Datos administrativos** (por ejemplo: rangos de IP, nombres de dominio y propiedades DNS, etc.)
- Se suelen usar herramientas especializadas o scripts NSE de Nmap (**Lab 8-9**)
- Detalles sobre su topología y operaciones
  - Dependencias de confianza de una red,
  - Topología de red
  - Dispositivos de seguridad de red (como firewalls)
  - ...

T1592. Gather victim host information / T1590. Gather victim network information

- **Para numerar servicios puedes**
  - Usar **herramientas especializadas** para cada servicio que hayas encontrado
    - Ej.: `dig` (DNS), `Enum4Linux` (SMB), `SNMPWalk` (SMB), `WPScan` (WordPress), `dirb` (páginas web)…
  - Buscar y utilizar **scripts NSE de Nmap** que esté vinculado al nombre del servicio encontrado
    - Consulta las categorías de script recomendadas en los cheatsheets de prácticas
    - `locate *nse* grep <service name>`
    - Y **usa la documentación** de los scripts encontrados para usarlos contra el objetivo
      - https://nmap.org/nsedoc/
    - La mayoría de ellos no sólo realizan tareas de enumeración: también permite explotar vulnerabilidades
    - Para solo tareas de enumeración, es aconsejable buscar la palabra "enum" en la descripción del script
  - Usar **módulos auxiliares de Metasploit** (Metasploit Auxiliary modules , visto en el **Tema 7**)

T1592. Gather victim host information / T1590. Gather victim network information

- **Puedes encontrar más información de la víctima en más sitios, por ejemplo**
  - **Ficheros concretos** de su web que delaten servicios, versiones, información en general...
  - Los endpoints de los ficheros JavaScript que tiene su web
    - Tradicionalmente suelen ser puntos menos protegidos (suelen ignorarse como vía de ataque)
  - Si una organización tiene su código en un **repositorio público** (Ej.: GitHub) es otra vía de ataque
    - Podría **contener información privada** ("hardcoding") (**Seminario 4, Tema 6**)
  - Si se usa **almacenamiento en nube** (Ej.: Amazon S3) también debe revisarse
    - Podría **estar mal configurado** y exponer información privada
- **O puedes considerar "esnifar" (sniff) y analizar el tráfico de red directamente**
  - Wireshark (https://www.wireshark.org/)
    - Ej.: https://null-byte.wonderhowto.com/how-to/spy-traffic-from-smartphone-with-wireshark0198549/
  - Sparrow-Wifi: Analizador gráfico de Wifi para Linux: https://github.com/ghostop14/sparrow-wifi
  - Ehtools Framework: https://github.com/entynetproject/ehtools

➢ Ejercicios **L89B4_SCRIPTSCAN**, **L89B4_JSSCAN**, **L89B4_S3SCAN**, **L89B4_GITHUBSCAN**

TA0043. Reconnaissance: Más técnicas

- **T1589. Gather Victim Identity Information**
  - https://attack.mitre.org/techniques/T1589/
  - Datos personales (por ejemplo: nombres de empleados, direcciones de correo electrónico, etc.)
  - Detalles confidenciales (como credenciales)
- **T1591. Gather Victim Org Information**
  - https://attack.mitre.org/techniques/T1591/
  - Nombres de divisiones/departamentos, ubicaciones físicas,
  - Detalles de las operaciones comerciales (relaciones, business tempo (horas/días de trabajo)...)
  - Roles y responsabilidades de los empleados clave
- **Esta información puede encontrarse en Internet (redes sociales, webs, etc.)**
  - Hay gran cantidad de información sobre personas, empresas, etc.
  - Lo que puede derivar en técnicas de spear phising
  - Todo esto **lo practicaremos en el Trabajo en grupo** (OSINT)

Otras técnicas de reconocimiento

Más técnicas para obtener información de la víctima

*Iconos por Bing Chat AI

TA0043. Reconnaissance: Otras técnicas

T1598. Phishing for Information

- https://attack.mitre.org/techniques/T1598/
- Intentar engañar a los objetivos para que divulguen información, con frecuencia credenciales u otra información procesable
- En este caso el atacante no pretende ejecutar código malicioso
- Los atacantes pueden usar un servicio de terceros de spear phising, un archivo adjunto o un enlace de spear phising
- **Lo veremos en el Trabajo en grupo** (OSINT)

T1597. Search Closed Sources

- https://attack.mitre.org/techniques/T1597/
- La información sobre las víctimas se puede comprar de fuentes y BBDD privadas de buena reputación
  - Como suscripciones de pago a fuentes de datos técnicos / de inteligencia de amenazas (proveedores de inteligencia de amenazas, threat intelligence vendors)
- Pero también se puede comprar de fuentes menos reputadas, como la dark web o los blackmarkets del cibercrimen

TA0043. Reconnaissance: Otras técnicas

T1596. Search Open Technical Databases

- https://attack.mitre.org/techniques/T1596/
- La información sobre las víctimas puede estar disponible en BBDD y repositorios en línea (registros de dominios/certificados...)
- Además, en colecciones públicas de datos/artefactos de red recopilados a partir de tráfico y/o escaneos
  - Esto incluye DNS/DNS pasivo, WHOIS, certificados digitales, CDN, bases de datos de escaneo (**Shodan**, **Censys**)

T1593. Search Open Websites/Domains

- (https://attack.mitre.org/techniques/T1593/)
- La información sobre las víctimas puede estar disponible en varios sitios, como redes sociales o sitios de noticias.
- Además, aquellos que alojan información sobre operaciones comerciales, como empleo o contratos solicitados / ganados
- Esto también incluye motores de búsqueda (**Google Hacking**)

TA0043. Reconnaissance: Técnicas ya descritas

- **Phishing for Information** ya se trató en
  - **Seminario 1**: Phishing contra los usuarios
    - Tinfoleak, Twint, Hunter.io, Social Mapper, Project Sherlock y otras herramientas
  - Los materiales complementarios
    - https://www.researchgate.net/publication/359146160_Las_Ciberestafas_en_la_Actualidad_Formas_de_reconocerlas_y_prevenirlas
    - Describen varias formas de phising y spear phising
- **Search Open Technical Databases** se cubrió en el **Seminario 1** y el **Laboratorio 2**
  - Describiendo Shodan y Censys
- **Search Open Websites/Domains** fue cubierto en
  - **Seminario 1** (código fuente): GitGot, GitGraber y GitRob pueden obtener información sensible
  - Google Hacking fue descrito en el **Seminario 1** y el **Laboratorio 2**
- Todo esto es también parte del **Trabajo en grupo** (OSINT)

¿CREES QUE LO HAS ENTENDIDO TODO? ¡AUTOEVALÚATE!

?

Eres capaz de hacer lo siguiente

- *Entender qué tipo de información contiene el MITRE ATT&CK y para que se usa*
- *Comprender que todos los controles técnicos de seguridad de los **CIS Benchmarks** tienen al final de su definición una tabla que mapea el control con las técnicas, tácticas y mitigaciones para ataque que contiene el MITRE ATT&CK*
- *Entender claramente en qué consiste la etapa de reconocimiento de un ataque, y que parte de la misma conlleva hacer escaneos activos de máquinas*
- ***Sobre los escaneos activos***
  - *Entiendes en qué consisten estos escaneos y el tipo de información que pueden extraer*
  - *Comprendes que existen escaneos básicos y avanzados que obtienen más o menos información, pero a cambio de tardar más tiempo y poder ser detectados por herramientas de vigilancia*
  - *Tener claro que el mayor partido de **NMap**, y explotar su enorme versatilidad, solo es posible aprendiendo a usar su motor de scripts NSE*
  - *Comprendes que la obtención de información de una infraestructura no acaba en sus máquinas o redes, sino que también abarca toda clase de servicios en uso, ficheros, código, almacenamiento en nube, y las personas vinculadas a la misma*
    - *Y que, por tanto, el OSINT de máquinas y personas es una parte integral de esta labor de reconocimiento*

TEMA 5
SEGURIDAD PERIMETRAL Y DE RED

Fuente: Bing Chat AI

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo