Módulo 3. Amenazas en sistemas inteligentes y detección de anomalías

“Cuando se comparte información o datos mediante Internet, atraviesan una serie de dispositivos de red en todo el mundo que forman parte de la Internet pública. A medida que los datos viajan por la Internet pública, existe una posibilidad de que hackers la comprometan o roben. Para evitar esto, los usuarios pueden instalar *software* o *hardware* específicos para garantizar la transferencia segura de datos o información. Estos procesos se conocen como cifrado en **seguridad de redes**”. (García Betancurt, s.f., https://n9.cl/0xshq0)

Es necesario tener un conocimiento mínimo de cómo trabaja la red, cuál es su funcionamiento, qué modos de conexión utiliza, entre otros aspectos. Tener una mirada constante en la red mediante la monitorización es necesario para detectar anormalidades que van desde una mala configuración que ocasiona congestión hasta la detección de algún tipo de ataque.

2. Vulnerabilidades

Referencias

Descarga en PDF

1. Redes

Redes

"El término red hace referencia a un conjunto de sistemas informáticos independientes conectados entre sí, de tal forma que posibilitan un intercambio de datos, para lo que es necesario tanto la conexión física como la conexión lógica de los sistemas" (Aleph, 2021, https://n9.cl/k2r0i). La conexión se establece por medio de protocolos de red, como es el caso de TCP (*transmission control protocol*).

Queda claro que todo el transporte de información se realiza por medio de redes informáticas donde la red de redes, **Internet**, nos permite comunicarnos sin fronteras y la encriptación nos brinda la protección de la información entre el emisor y receptor. Los *hackers* aprovechan cualquier vulnerabilidad presente en la infraestructura crítica para explotarla.

El crecimiento de Internet, el bajo costo de equipos y otros factores determinantes permitieron alcanzar una conectividad permanente y expandieron un ecosistema compuesto por lo tangible e intangible que denominó ciberespacio. Esta heterogénea red compuesta de distintos dispositivos, marcas comerciales, sistemas operativos, aplicaciones, etc., no solo generan beneficios a sus usuarios al compartir información, sino que también las débiles configuraciones de seguridad dejan vulnerabilidades a merced de los ciberdelincuentes. Por lo tanto, entender las características de la red, nos ayudará a comprender la necesidad de conocer los vectores de ataque y la construcción de redes seguras.

Clasificación de redes

En función del tamaño y alcance de la red, realizamos la siguiente clasificación:

- ***Local area networks*** (**LAN**) o red de área local: Se les atribuye a las redes dentro de una organización o establecimiento. Se conectan mediante cable UTP (categoría 5 y 6), fibra óptica. Las redes inalámbricas reciben el nombre de *wireless local área* (WLAN).

- *Metropolitan area networks* (**MAN**) o red de área metropolitana: Se atribuyen a redes de una ciudad. Utilizan como medio de conexión física el cable de red UTP (categoría 5 y 6), fibra óptica e inalámbrica.

- *Wide area networks* (**WAN**) o red de área amplia: Son las que unen ciudades, países, continentes. Se conectan por medio de fibra óptica o inalámbricamente.

Alcances

Cable UTP categoría 5: la norma establece hasta 100 metros.

Cable UTP categoría 6: la norma establece hasta 1000 metros.

Conexión inalámbrica: dependiendo de la antena y su potencia, el rango de cobertura es amplio.

Fibra óptica: cubre grandes rangos, como por ejemplo continentes enteros.

Topología de red

La topología de red no es otra cosa que la forma en que se conectan las computadoras para intercambiar datos entre sí. Las más comunes son:

- **Anillo**: Reduce la posibilidad de fallo de red conectando todos los nodos a un nodo central que puede ser un *router* o *switch*. Por supuesto, la ventaja es que si un nodo falla, la red continuará trabajando sin inconveniente.

- **Estrella**: las estaciones de trabajo o computadoras se encuentran conectadas entre sí en forma de un anillo, es decir, forman un círculo entre ellas. La información viaja en un solo sentido; por lo tanto, si un nodo deja de funcionar, se cae la red.

Lectura sugerida: La siguiente lectura describe las topologías y enlaces desde el punto de vista del modelo de capa OSI que ayudará a dar claridad al conocimiento de vulnerabilidad, propagación, etc.

Universidad de Valencia (s. f.). Redes de comunicación. Topología y enlaces. https://n9.cl/00gxc.

Modelo de interconexión de sistemas abiertos (OSI)

“La comprensión de las redes básicas comienza con el modelo de interconexión de sistemas abiertos.

El modelo OSI (en inglés: *open system interconnection*) estandariza las funciones clave de una red mediante protocolos de red. Esto permite que diferentes tipos de dispositivos de diferentes proveedores se comuniquen entre sí a través de una red.

En el modelo OSI, las comunicaciones de red se agrupan en siete capas lógicas. Dos dispositivos se comunican mediante protocolos estandarizados OSI en cada capa” (Progress Software Corporation, s. f., https://n9.cl/pryub).

Tabla 1: El modelo OSI de siete capas

CAPA	Función de la capa
7 Aplicación	Interactúa con aplicaciones de *software* que implementan un componente de comunicación.
6	Convierte los datos entrantes y salientes de un formato de presentación a otro (cifrado

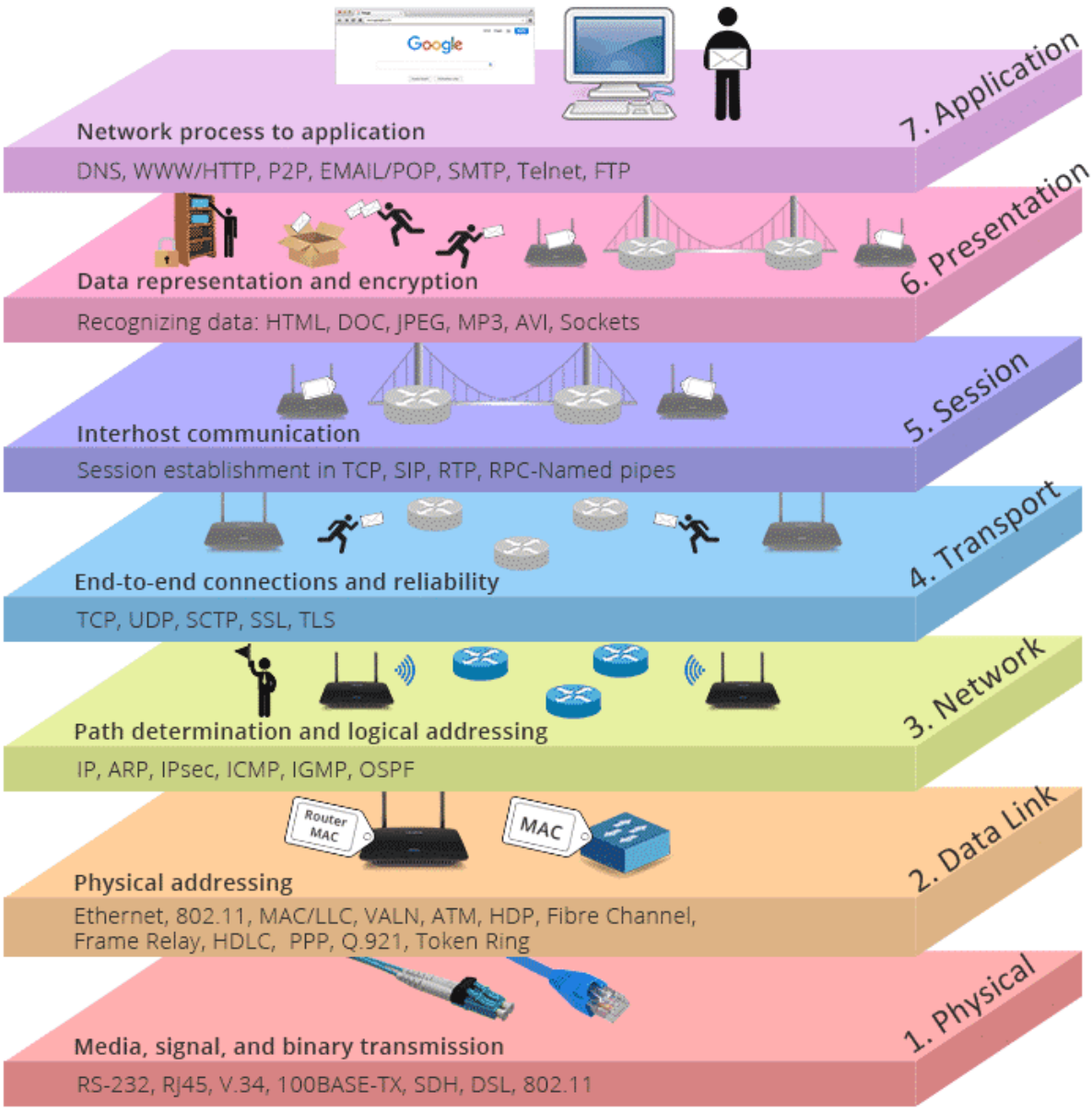
Presentación	de datos, compresión de texto).
5 Sesión	Controla las conexiones entre equipos. Establece, administra y finaliza la conexión.
4 Transporte	Garantiza la transferencia de datos de un origen a un host de destino a través de una o varias redes.
3: Red	Enruta paquetes de datos entre dos nodos en una red utilizando una dirección IP.
2 Enlace datos	Proporciona una conexión confiable entre dos nodos conectados mediante la detección de errores en la capa física.
1 Física	Transmite una secuencia de bits a través de medios físicos tales como coaxial o cable de fibra.

Fuente: Progress Software Corporation, s.f., https://n9.cl/pryub.

“Las capas *datalink* (2), *network* (3) y *application* (7) son las más comunes utilizadas para la supervisión. Los sistemas de monitoreo de red utilizan estas capas para descubrir los dispositivos de la red y cómo están conectados, para generar

mapas de topología de red, y para monitorear la red" (Progress Software Corporation, s. f., https://n9.cl/pryub.).

Figura 1: Las 7 capas del modelo OSI



Fuente: [imagen sin título sobre las 7 capas del modelo OSI], 2021, https://n9.cl/sesam.

Tabla 2: Dispositivos de red comunes

	***Routers*** Los *routers* conectan redes. Por ejemplo, conectar una red privada a Internet. Un *router* actúa como despachador, eligiendo la mejor ruta para que la información viaje. Los *routers* conectan a los usuarios a Internet. Los *routers* son dispositivos de la capa 3 del modelo OSI.
	**Interruptores** Los conmutadores conectan computadoras, impresoras, servidores y otros dispositivos a la red privada. Un conmutador funciona como un controlador que permite que los dispositivos de la red se comuniquen entre sí. Los conmutadores son dispositivos de capa 2.
	***Firewall*** Los *firewall* protegen las redes al controlar el tráfico entrante y saliente en función de las reglas. Esto crea una barrera segura entre una red privada de confianza y una red que no es de confianza, como Internet.
	**Servidores** Las redes entregan aplicaciones e información a los usuarios. Aplicaciones e información en vivo en servidores. Un servidor es una instancia en ejecución o una copia de una aplicación. Los servidores aceptan solicitudes de los usuarios y responden en consecuencia. Por ejemplo, cuando accede a un sitio web, un servidor web "sirve" páginas web a su dispositivo local. Otros ejemplos de servidores son los servidores de correo electrónico y los servidores de bases de datos.

Fuente: Progress Software Corporation, s.f., https://n9.cl/pryub.

¿Cuál es la diferencia entre un switch de capa 2 y un switch de capa 3?

“La diferencia principal entre la capa 2 y la capa 3 radica en la función de enrutamiento. Un *switch* de capa 2 funciona solo con direcciones MAC y no considera la dirección IP ni ningún elemento de capas superiores. Un *switch* de capa 3 realiza todos los trabajos del *switch* de capa 2. Además, el switch de capa 3 puede ejecutar enrutamiento estático y enrutamiento dinámico. En otras palabras, un *switch* de Capa 3 dispone de una tabla de direcciones MAC y de una tabla de enrutamiento IP. Adicional a esto, también controla la comunicación intra-VLAN y el enrutamiento de paquetes entre diferentes VLAN. Un *switch* que solo añade enrutamiento estático se conoce como *layer* 2+ o *layer* 3 Lite. Los *switches* de capa 3, además de los paquetes de enrutamiento, también incluyen algunas funciones que requieren la capacidad de comprender la información de la dirección IP de los datos que ingresan al switch; por ejemplo, identificar el etiquetado del tráfico de la VLAN según la dirección IP en vez de configurar un puerto manualmente. Los *switches* de capa 3 incrementan la potencia y la seguridad en la medida en que se requiera” (Sánchez Castillo, 2018, https://n9.cl/wzj0wn).

Descripción general de redes inalámbricas

Conocer las normas legales de ciberseguridad que rigen en la jurisdicción donde se realizan tareas laborales es fundamental para no caer o ser confundido dentro del rango de actividades ilegales. Algunos países aplican con mayor rigurosidad que otros el uso de ciertas herramientas tecnológicas que podrían ser catalogadas como ciberdelitos o ciberespionaje, ya que incursionar en el acceso no autorizado a información, puertos y protocolos podría causar complicaciones legales.

Toda incursión sobre una red, equipos, infraestructura crítica u otros debe tener la debida autorización y el plan de acción correspondiente. A esto llamamos *hacking* ético.

Los conocimientos de las herramientas dejadas en esta lectura le permiten al futuro profesional tener la experiencia para aportar mejoras al sistema de red que pudieran administrar.

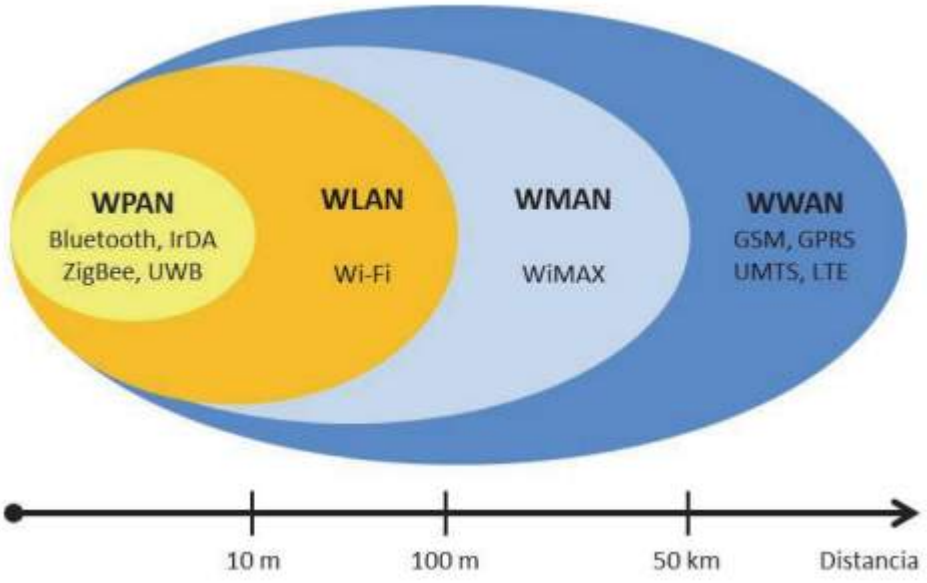
Una de las formas más frecuentes para acceder a Internet es hacerlo por medio de una red inalámbrica pública, algunas sin protección y otras en las que deben escribirse una contraseña. El caso más común para acceder a Internet es conectarse a un *router* inalámbrico en una confitería, biblioteca, vía pública, etc. También hay otros dispositivos que funcionan como *router* o *switch* no inalámbricos y que

brindan acceso a Internet para empresas, entidades gubernamentales, colegios, etc. Cualquiera de estos equipos puede configurarse por medio de una clave o *password*, usando WPA, WPA2, etc.

El acceso a infraestructuras críticas por medio de redes inalámbricas debe analizar y garantizar la seguridad de la conexión y tal vez sea necesario combinarse con el uso de VPN, *firewall*, etc. Para que la red sea más segura.

La configuración de red inalámbrica en un hogar debe configurarse también por medio de una clave y el control de acceso en este caso es a través de un *log* que debe estar habilitado siempre.

Figura 2: Clasificación de redes inalámbricas



Fuente: elaboración propia.

Lectura sugerida

Intel (2021). *Descripción general de redes inalámbricas*. Intel. https://n9.cl/bdk52.

Baca Urbina, G. (2016). *Introducción a la Seguridad Informática*. (Capítulo 5). Grupo Editorial Patria. https://n9.cl/5dcgq.

CONTINUAR

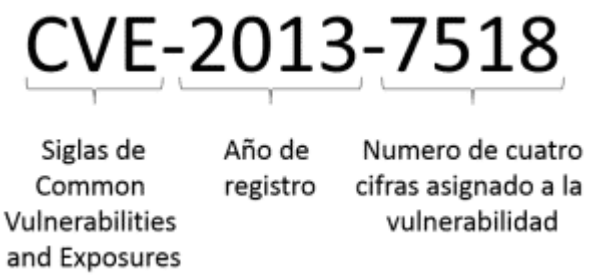
2. Vulnerabilidades

Vulnerabilidades

Las vulnerabilidades y exposiciones comunes (*common vulnerabilities and exposures*, siglas CVE), se encuentran en "una lista de información registrada sobre vulnerabilidades de seguridad conocidas, en la que cada referencia tiene un número de identificación CVE-ID, descripción de la vulnerabilidad, que versiones del software están afectadas, posible solución al fallo (si existe) o como configurar para mitigar la vulnerabilidad y referencias a publicaciones o entradas de foros o blog donde se ha hecho pública la vulnerabilidad o se demuestra su explotación, es definido y es mantenido por The MITRE Corporation" (Carrillo Ledesma y González Rosas, 2020, p. 15).

Puedes visitar el sitio de esta compañía en el siguiente enlace: https://www.cve.org/.

Figura 3: Composición del número de identificación



Fuente: Telefónica Tech, s.f., https://n9.cl/y9sd3.

No todas las vulnerabilidades son reportadas. Muchos investigadores o usuarios descubren alguna que dependiendo de característica u situación pueden o no ser formalizadas.

Los administradores de redes continuamente monitorean toda actividad con el fin de detectar actividades sospechosas y evitar que extraños realicen actos ilícitos aprovechándose de alguna vulnerabilidad. Esta actividad de monitoreo debe ser parametrizada y auditada constantemente por terceros bajo un esquema de trabajo, ya que podrían capturar información sensible que ponga en peligro la infraestructura crítica que tienen que controlar.

Monitoreo de red

El monitoreo de red puede entenderse como la actividad destinada a observar y controlar de forma continua los distintos elementos que la componen, tales como servidores, *firewalls*, *switches*, *routers* y el flujo de datos, entre otros. Esta práctica también se conoce como supervisión de red.

Para analizar su funcionamiento, el *software* especializado envía señales o *pings* a diversos puertos del sistema. Cuando el monitoreo se realiza de manera proactiva, permite detectar y resolver inconvenientes de red de forma anticipada, reduciendo el riesgo de interrupciones del servicio o fallas operativas.

Todo el proceso se desarrolla principalmente en tres pasos:

- **Ping**: esta técnica básica es utilizada por el *software* para probar la disponibilidad de la red.
- **SNMP** (protocolo simple de administración de red): “usa un sistema de llamada y respuesta para verificar los estados de muchos tipos de dispositivos, desde *switches* hasta impresoras. SNMP se puede usar para monitorear el estado y

la configuración de los sistemas" (Crossover, s.f., https://n9.cl/5wmwy).

- **ICMP**: "Los dispositivos de red, como los *routers* y servidores, usan el protocolo de mensajes de control de Internet para enviar información de operaciones por IP y para generar mensajes de error ante fallas de dispositivos" (Crossover, s.f., https://n9.cl/5wmwy).

A continuación, presentamos algunas herramientas de monitoreo de red:

PRTG: Permite determinar los consumos de ancho de banda de la red, monitorear bases de datos, administrar aplicaciones y extraer sus estadísticas detalladas. También lo ayuda a administrar y monitorear servicios de computación en la nube, múltiples tipos de servidores en tiempo real, redes locales como enrutadores, impresoras, estaciones de trabajo, etc. Enlace: https://n9.cl/hjr91.

Nagios Network Analyzer: Proporciona un análisis extenso de su red y fuentes de tráfico junto con las amenazas a la seguridad. Calcula el ancho de banda y permite personalizar el uso. Ayuda a crear informes para resumir las direcciones IP,

la utilización y fuente de ancho de banda, etc. Enlace: https://n9.cl/99fg8.

Ntopng: Obtiene una interfaz web inteligente para explorar información sobre el tráfico histórico y en tiempo real junto con los *hosts* activos. Puede ordenar el tráfico según el protocolo L7, el puerto, la dirección IP, los sistemas autónomos y el rendimiento. Enlace: https://n9.cl/nsk8o.

SolarWinds: NetFlow Traffic Analyzer (NTA). Es una herramienta útil creada para traducir detalles finos en informes y gráficos completos. Monitoreo del ancho de banda: vea los registros de flujo de IPv4 e IPv6 y monitoree aplicaciones como Cisco NetFlow, sFlow, Juniper J-Flow, Huawei NetStream, etc. NTA le ayuda a identificar los mayores recursos que agotan su ancho de banda y otros usos y tráfico de la red. Recopila métricas de tráfico de red de varias fuentes de datos, incluido NetFlow. Enlace: https://n9.cl/nfeaty.

Pandora FMS: “Ha eliminado con éxito los cuellos de botella en los sistemas de red desde 2004. Puede monitorear fácilmente las redes de sus clientes sin acceso externo a través de sus servidores de clientes. Los servidores se implementan rápidamente y se administran de forma

centralizada, a pesar de que no hay conexión directa" (Pathak, 2025, https://n9.cl/253q4). Enlace: https://n9.cl/03e6w.

NetCrunch: "es una plataforma de monitoreo eficiente para varios componentes de red como servidores, enrutadores, servicios de virtualización, cámaras, dispositivos IoT, cortafuegos, y más" (Pathak, 2025, https://n9.cl/253q4). Enlace: https://n9.cl/d6bu1.

OpenNMS: "es una plataforma integrada, de código abierto y de nivel empresarial para la creación de servicios de monitoreo de redes" (Pathak, 2025, https://n9.cl/253q4). Enlace: https://n9.cl/cell7.

Capsa: Herramienta portátil para monitorear, analizar y solucionar problemas de red. Es adecuado tanto para WLAN como para LAN y tiene captura de paquetes y capacidades en tiempo real. Enlace: https://n9.cl/yzwmh.

Zenoss: Permite monitorear todas sus redes virtuales y físicas, incluida la infraestructura local y en la nube. "Extrae, ingiere, correlaciona e indexa sus datos en una arquitectura cohesiva para una inteligencia procesable. Recopila y registra datos de sus sistemas para comprender el estado actual de su infraestructura y aplicaciones" (Pathak, 2025, https://n9.cl/253q4). Enlace: https://n9.cl/dnfanh.

NetXMS: Sistema de monitoreo de red de código abierto. Opera en redes enormes que tienen miles de servidores; por tanto, es escalable, es compatible con Windows y los principales sistemas Unix y ofrece cifrado estándar de la industria para una mejor seguridad y control de acceso. Enlace: https://n9.cl/rfqrjg

Opsview: "Permite ver el uso del protocolo de su red, transferencias de datos, pérdida de paquetes, nodos finales que reciben y transmiten datos, y más. Con Opsview, puede encontrar trampas SNMP, traducirlas a través de SNMP MIB y aplicar reglas para determinar alertas y sus mensajes" (Pathak, 2025, https://n9.cl/253q4). Enlace: https://n9.cl/lgrsk.

LibreNMS: Puede descubrir automáticamente su red mediante SNMP, ARP, BGP, OSPF, LLDP, FDP y CDP. "Ofrece un sistema de alerta altamente flexible y le notifica a través de Slack, IRC, correos electrónicos, etc." (Pathak, 2025, https://n9.cl/253q4). Enlace: https://n9.cl/2j26j.

También existen otros programas que permiten realizar auditorías, *sniffer*, etc. tales como:

Nmap: "Es un programa de código abierto que sirve para efectuar rastreo de puertos, es multiplataforma. Permite la detección de equipos, servicios y sistemas operativos. Estas

funciones son extensibles mediante el uso de *scripts* para proveer servicios de detección avanzados, detección de vulnerabilidades y otras aplicaciones. Además, durante un escaneo, es capaz de adaptarse a las condiciones de la red, incluyendo latencia y congestión de la misma, es difícilmente detectable" (Pathak, 2025, https://n9.cl/253q4). Enlace: https://n9.cl/webnmap.

En el sitio web de Sectools se ofrece una gran cantidad de herramientas *wireless* (enlace: https://n9.cl/8akal). Se mencionan algunas de ellas:

- **Wireshark:** Es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para análisis de datos y protocolos. Enlace: https://n9.cl/owf9f.

- **Zenmap:** Sirve para escanear los puertos y saber cuáles hay abiertos y, de esta manera, evitar problemas a la hora de usar algunos programas o acceder a un servidor. Enlace: https://n9.cl/seqil4

- **Angry IP Scanner:** es una sencilla herramienta que permite obtener la dirección

IP de los equipos ubicados en una determinada red de computadoras. El programa escanea el rango de direcciones que especifiques y muestra la IP de aquellos ordenadores de los que obtiene respuesta. Enlace: https://n9.cl/t3bxf.

- **Metasploit** es un proyecto de código abierto para la seguridad informática que proporciona información acerca de vulnerabilidades de seguridad y ayuda en test de penetración y en el desarrollo de firmas para sistemas de detección de intrusos. Enlace: https://n9.cl/73oqri.

- **Nessus** es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en un demonio o diablo, nessusd, que realiza el escaneo en el sistema, y nessus, el cliente que muestra el avance e informa sobre el estado de los escaneos. Enlace: https://n9.cl/3ar2cn.

- **OpenVas** es una *suite* de *software*, que ofrece un marco de trabajo para integrar servicios y herramientas especializadas en el escaneo y gestión de vulnerabilidades de seguridad de sistemas informáticos. Enlace: https://n9.cl/rasn5.

- **John the Ripper:** es un programa de criptografía que aplica fuerza bruta para descifrar contraseñas. Es capaz de romper varios algoritmos de cifrado o hash, como DES, SHA-1 y otros. Enlace: https://www.openwall.com/john/.

- **Nikto:** es un escáner de vulnerabilidades de línea de comandos de *software* gratuito que escanea los servidores web en busca de archivos / CGI peligrosos, *software* de servidor desactualizado y otros problemas. Realiza comprobaciones genéricas y específicas del tipo de servidor. Enlace: https://n9.cl/vvwf2.

- **Ettercap** es un interceptor/*sniffer*/registrador para LAN con *switch*. Sirve en redes LAN conmutadas, aunque es utilizado para auditorías en distintos tipos de redes. Soporta direcciones activas y pasivas de varios protocolos. Enlace: https://n9.cl/myjjr.

- **OSINT** hace referencia al conjunto de técnicas y herramientas para recopilar información pública, analizar los datos y correlacionarlos, convirtiéndolos en conocimiento útil. Enlace: https://n9.cl/py1z7.

La lista podría seguir, pero la dejaremos aquí, no por una cuestión de preferencia entre algunas herramientas, sino porque se cree haber presentado variedad de opciones. Hay herramientas poderosas en el mercado que, en el uso, pueden infringir normas éticas; por eso, antes de usarlas, debemos tener en claro el propósito de su uso.

Lectura sugerida: Baca Urbina, G. (2016). *Introducción a la seguridad informática*. Capítulo 4 (pp. 142 -184). Grupo Editorial Patria.

Recomendación de la cátedra: Las herramientas anteriormente referenciadas permiten realizar tareas de auditoría, análisis de tráfico, etc. **Se recomienda que nunca intenten realizar acciones ilícitas** con estas o cualquier otra herramienta, siempre deben velar por la privacidad y protección de la información y de la infraestructura crítica.

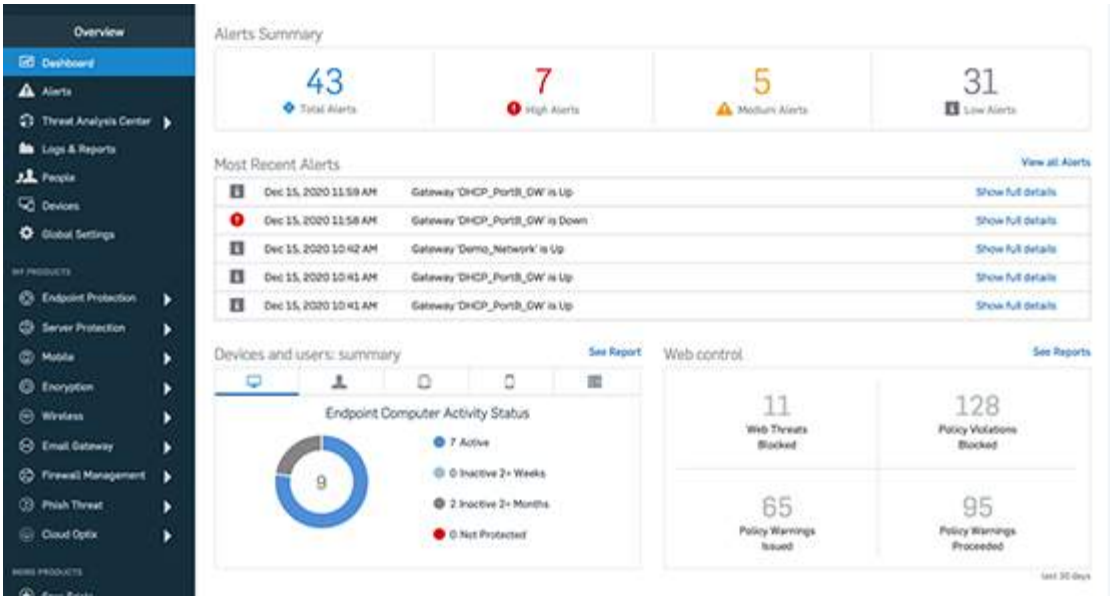
¿Cómo se monitorean las redes?

El monitoreo de red se lleva a cabo por medio de la ejecución de una aplicación que se instala en un equipo, lo provee el *router* / *switch* /etc. y que constantemente monitoriza una red de equipos *host* (computadoras, impresoras, etc.) en busca de componentes defectuosos, lentos, presencia de *malware*, acceso a urls, antivirus desactualizado, etc. Estas

herramientas informan a los administradores de redes la situación que se ha previsto en la configuración.

Este aviso le llega al administrador por medio de un correo electrónico, mensaje de texto, cartel desplegado en la computadora u cualquier otra forma de alarma o notificación que tenga la aplicación. En la actualidad, algunos antivirus brindan este tipo de soluciones que son muy eficientes para el monitoreo de seguridad de la red en las últimas capas del modelo OSI.

Figura 4: Ejemplo de alerta



Fuente: captura de pantalla de Sophos Ltd.

En la imagen anterior observamos que la administración de los servidores, equipos remotos, etc., puede realizarse desde una consola alojada en la nube. Este control permite administrar el acceso, reporte de *malware*, actualización de antivirus, prohibición de acceso a determinadas url, etc.

La selección de la herramienta a usar o recomendar y su instalación, requieren de un análisis minucioso para determinar la factibilidad y llevar a cabo las acciones de planificación. En otras palabras, recomendar un antivirus sin la solidez de una argumentación que amerite un estudio y análisis previo es arriesgarse a hablar sin saber de un tema tan importante como es el de la ciberseguridad.

Para hablar del monitoreo de red, es necesario mencionar al modelo OSI de las siete capas, los dispositivos comunes de comunicación en la red y las cinco funciones de los sistemas de supervisión.

Hacker de sombrero blanco y sombrero negro

“El término sombrero blanco en Internet se refiere a un hacker ético, quien se especializa en pruebas de penetración y en otras metodologías para detectar vulnerabilidades y mejorar la seguridad de los sistemas de comunicación e información de una organización. También se refiere a

personas que no son agresivas o no realizan actividades ilícitas. Un *hacker* ético es un término inventado por IBM. Es utilizado para diferenciar a los piratas informáticos que actúan sin malicia de los que sí, los cuales son más conocidos como *crackers* o *hackers* de sombrero negro". (DesarrolladorSoft, 2021, https://n9.cl/cb2917).

Buenas prácticas

La monitorización de una red es la principal medida de control que, mediante la configuración que ofrece la aplicación o dispositivo, puede ayudar a detectar anomalías en la red.

El advenimiento del almacenamiento en la nube permitió el desarrollo de las redes definidas por *software* (SDN), cuya administración y control puede programarse para cumplir las prestaciones que se necesitan.

Cuando se hace mención a redes y su monitorización, es necesario precisar conceptos como IDS (Intrusion Detection System), IPS (Intrusion Prevention System) y NSM (Network Security Monitoring).

"Un IDS es un sistema pasivo que se encarga de monitorear el comportamiento de una red para detectar e informar

sobre posibles intrusiones no autorizadas, mientras que un IPS es un sistema activo que funciona como una extensión de los IDS y que, además de enviar alertas sobre las detecciones, también puede bloquear la actividad maliciosa dentro de la red —como ataques de fuerza bruta (DDoS) o ataques que buscan la explotación de vulnerabilidades— y crear un registro (*log*) con la intrusión. Todo esto a partir del tráfico, las firmas de archivos, y el análisis heurístico del flujo. Adicionalmente, los IPS permiten agregar políticas y restringir acceso a usuarios y/o incluso aplicaciones" (Confederación de Empresarios de La Coruña, 2021, https://n9.cl/9rbew).

IEM: Security Information and Event Management. Sistemas de correlación de eventos. Son soluciones basadas en reglas, que se encargan de reunir información de registros de los distintos sistemas operativos, servicios y protocolos desplegados, y los analizan en busca de fallas, actividades sospechosas y violaciones de políticas.

OSSIM: *Open source security information management*. Conocidos también como Open Source SIEM, se trata de soluciones con similares características a las que presenta un SIEM, con la ventaja del licenciamiento GPL (General Public Licence).

UTM: Unified Threat Management. Gestión Unificada de Amenazas. Se trata de soluciones que implementan múltiples soluciones de seguridad en una misma herramienta. Algunas de las funcionalidades que incluyen son: *antispam*, *antiphishing*, antivirus, *antispyware*, filtrado de contenidos, IDS/IPS, VPN, por citar algunas.

Firewalls: Cortafuegos. Se trata de soluciones basadas en reglas que controlan el acceso de un recurso desde y hacia una red. Existen versiones de *software* y *hardware*.

Antivirus: Las soluciones antivirus forman también parte de los mecanismos de detección con los que se cuenta en una organización, seguramente con implementaciones más complejas y centralizadas que en un contexto de usuario final.

¿Por qué debo monitorear la red de mi empresa?

“La red es la línea de vida de la infraestructura de TI. Cuando las redes fallan, el flujo de información requerido por las aplicaciones y las operaciones empresariales se detiene.

Las redes son entornos dinámicos. A los administradores de red se les pide continuamente que agreguen nuevos

usuarios, tecnologías y aplicaciones a sus redes. Estos cambios pueden afectar a su capacidad para ofrecer un rendimiento de red coherente y predecible.

Cuando surgen problemas de red, los administradores de red se ven presionados a identificar la causa raíz antes de que afecte a los usuarios, las aplicaciones y el negocio. Esto es más problemático con problemas de rendimiento intermitentes que son difíciles de replicar y diagnosticar" (Progress Software Corporation, s.f., https://n9.cl/pryub).

"A continuación, te daremos 5 razones por las cuales te debe interesar este tema:

1. Evita interrupciones en la red. Monitorear la red brinda visibilidad para detectar problemas antes de que ocurran, mostrando el rendimiento de la misma.

2. Soluciona problemas de manera más eficaz. Monitorear la red simplifica la detección de problemas y muestra de manera mucho más rápida el rendimiento de distintos dispositivos, para así poder detectar los dispositivos problemáticos.

3. Aumenta la seguridad de la red. Monitorear la red proporciona información importante sobre la fuente y la naturaleza del tráfico que fluye en la misma. Supervisando la red es posible detectar tráfico anormal o cambios en el mismo producidos por actividad maliciosa.

4. Permite la escalabilidad y la adaptabilidad a cambios en la red. Cada vez las redes son más complejas y monitorear la red con herramientas flexibles permite supervisar todos los activos y garantizar un rendimiento constante incluso bajo circunstancias cambiantes.

5. Reduce costos y aumenta la satisfacción de los clientes y usuarios. El costo del tiempo de inactividad en una empresa es altísimo por minuto. Pero, además de este costo, las interrupciones en la operación afectan negativamente la satisfacción del cliente. Tener un monitoreo de red permite prevenir problemáticas antes de que se conviertan en emergencias o incidentes graves y afecten tanto a tus servicios internos como externos" (Lara, 2021, https://n9.cl/x11px).

¿Cómo funciona una herramienta de supervisión de red?

“Los sistemas de supervisión de red sondean los dispositivos de red y los servidores en busca de datos de rendimiento mediante protocolos estándar, como:

- SNMP, Protocolo simple de administración de redes.
- WMI, Windows Management Instrumentation.
- Y SSH, Secure Shell para Unix y servidor Linux.

Algunos NMS [sistema de supervisión de red] admiten lenguajes de *scripting* como PowerShell (para crear monitores personalizados para servidores Windows y consultas SQL) para crear monitores personalizados para bases de datos.

Los dos protocolos de monitoreo más utilizados son SNMP y WMI. Proporcionan a los administradores de red miles de monitores para evaluar el estado de sus redes y los dispositivos que hay en ellas”. (Progress Software Corporation, s. f., https://n9.cl/pryub)

Protocolo simple de administración de redes (SNMP)

“Es un protocolo de capa de aplicación basado en IP que intercambia información entre una solución de administración de red y cualquier dispositivo habilitado para SNMP. SNMP es un protocolo estándar que recopila datos de casi cualquier dispositivo conectado a la red, incluidos *routers*, conmutadores, controladores LAN inalámbricos, puntos de acceso inalámbricos, servidores, impresoras y más.

SNMP funciona consultando "objetos". Un objeto es algo sobre lo que un NMS recopila información. Por ejemplo, la utilización de la CPU es un objeto SNMP. La consulta en el objeto de utilización de CPU devolvería un valor que un NMS utiliza para alertar e informar.

Los objetos consultados por SNMP se mantienen en una base de información de administración, o MIB. Un MIB define toda la información expuesta por el dispositivo administrado. Por ejemplo, el MIB para un *router* Cisco contendrá todos los objetos, definidos por Cisco, que pueden ser utilizados para monitorear a ese *router,* tales como la utilización de la CPU, la utilización de la memoria y el estatus de la interfaz.

El objeto de un MIB se cataloga utilizando un sistema de numeración estandarizado. Cada objeto tiene su propio identificador de objeto único o OID.

Algunos NMS proporcionan un navegador MIB. Un navegador MIB permite a los administradores de red navegar a través de un MIB para encontrar objetos adicionales que quieren monitorear en un dispositivo". (Progress Software Corporation, s. f., https://n9.cl/pryub)

Interfaz de máquina de Windows (WMI)

"WMI es un protocolo que se utiliza para supervisar aplicaciones y servidores basados en Windows de Microsoft. WMI es específico de Windows y no supervisa los dispositivos de red ni los servidores que no sean de Microsoft.

WMI tiene una gran biblioteca con miles de contadores de rendimiento. Puede utilizar WMI para supervisar casi cualquier cosa en un servidor Windows que pueda supervisar con SNMP.

Un negativo de WMI es que es más intensivo de recursos para NMS, consumiendo más CPU y memoria para procesar que SNMP". (Progress Software Corporation, s. f., https://n9.cl/pryub)

Buenas prácticas para una red segura

Contraseñas

“Un primer elemento que deben considerar los usuarios es el cambio de las contraseñas generadas por defecto, pues estas pueden encontrarse fácilmente en línea o en los manuales. Un error común es crear una misma para todo, además de ignorar que estas han de ser difíciles de descifrar.

El *hacking* es una práctica cada vez más organizada y sofisticada que utiliza herramientas de gran alcance para probar diferentes combinaciones posibles de palabras, fuera de disponer de datos personales disponibles en la web como fechas de cumpleaños, entre otros, a los que diversos usuarios recurren para formular sus contraseñas.

. . .

Autentificación y cifrado

La autenticación de usuario requiere enviar los nombres de usuario y contraseñas a través de la red, las cuales pueden ser robadas durante esa transferencia. Tradicionalmente, se hace a partir de la codificación de texto no cifrado y base64, los cuales proporcionan acceso libre a quienes monitorean esta red para ver el tráfico, lo que les permite acceder a un dispositivo.

Una táctica menos recurrente es el uso de la autenticación Digest, el cual es un método utilizado para confirmar la identidad de un usuario antes de brindar información sensible. Esta aplica una función criptográfica *hash*, que no es más que un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija.

De esta manera, se crea una cadena alfanumérica única para garantizar que el archivo no haya sido modificado. Esta compara las credenciales *hash* en el dispositivo, sin necesidad de enviar los nombres de usuario y contraseñas reales sobre la red. Todos los productos de Hanwha soportan contraseñas Digest.

Configuración de red

De otro lado, una técnica común y eficaz para blindar aún más una red de seguridad es la separación física de las cámaras y los grabadores de la red corporativa, lo que evita ataques de intrusiones por deficiencias en el acceso. Para ello es recomendable el uso de redes de área local virtual (VLAN), las cuales funcionan en los *switches* de red y segmentan el tráfico basándose comúnmente en los puertos de este, lo que permite la protección por parte de *firewalls*

(cortafuegos) para bloquear el acceso de otros dispositivos en la red.

En ese sentido, el filtrado de la dirección IP (Internet Protocol) es un método para especificar explícitamente quién puede acceder a un dispositivo de red o, por el contrario, denegar el acceso al mismo.

No obstante, la mejor práctica para conectar ubicaciones remotas, tales como múltiples oficinas o trabajadores remotos, es la utilización de una red privada virtual (VPN). Esto crea un canal seguro, encriptado, lo que elimina la posibilidad de fuga de información como nombres de usuario y contraseñas.

Prevención de ataques

En muchos edificios, las tomas de conectores de red pueden estar accesibles; una cámara podría ser desconectada o un cable alterado para tener acceso a la infraestructura de red Ethernet. El estándar 802.1X proporciona control de acceso de red basado en puertos, lo cual requiere un certificado de identificación que se instala en cada dispositivo conectado para tener acceso a la red protegida. De ahí que, cuando un atacante inserta un dispositivo no autorizado en la red, se le niegue el acceso.

Hay una serie de tareas que los administradores de red realizan de forma continua para garantizar la seguridad permanente de sus cámaras y otros dispositivos. Una de las más cruciales es la revisión de todos los cambios al desarrollar, asegurar y aprobar las configuraciones, hacer constantes actualizaciones de software y garantizar que este cumpla con los estándares de seguridad organizacionales.

Al emplear estas mejores prácticas, se puede evitar que los sistemas y dispositivos de todo tipo se conviertan en una puerta abierta para los hackers. Pero, aún más, asegura la integridad y continuidad de la función crítica de algunos de ellos: garantizar la protección de personas y bienes". (OSAO, 2020, https://n9.cl/oqiq3)

Cómo detectar *malware*

Existen herramientas que trabajan con metodologías para detectar malware por medio de reglas; una de ellas se llama SURICATA y, por medio de reglas, puede detectar códigos maliciosos en la red.

Sistemas *honeypot*

Los administradores de red suelen usar un servidor alternativo (señuelo) para que sufra los ciberataques en lugar de los originales. “Esta información ayudaría a consolidar acciones de seguridad para la red que se protege, es decir, esta información debería servirle al equipo de respuesta ante incidentes o al SOC de la organización para implementar los controles o mitigaciones apropiadas.

. . .

Un *honeypot* es un sistema de señuelo en la red, por lo tanto, no hay razón legítima para que los usuarios de una organización intenten acceder a él, lo que hace que sea mucho más fácil detectar ataques, ya que prácticamente cualquier interacción con el equipo puede ser considerada maliciosa. La idea mediante la implementación de este sistema es hacerle creer a un atacante que está apuntando a un sistema real; sin embargo, estará desplegando sus actividades maliciosas en un ambiente controlado por nosotros.

Podemos implementarlos en el interior de nuestra red (delante del *firewall* externo), que puede servir para indicarnos que un atacante ya obtuvo acceso a nuestra red y está intentando realizar un movimiento lateral o bien, en el exterior de nuestra red, para detectar ataques externos. Por

otra parte, podemos tener varios *honeypot* instalados en nuestra red y conformar lo que se conoce como un *honeynet*.

Qué tipos de *honeypot* existen

De interacción alta

Es un servidor que posee servicios reales instalados, al igual que cualquier otro servidor en la organización. Debemos tener cuidado de que esté perfectamente aislado del resto de la red para impedir que un ataque exitoso finalmente le dé acceso a la red al atacante. La información que se genera en este sistema es sumamente detallada.

De interacción media

Tiene algunos servicios básicos, como puede ser un servidor web o FTP, que se pueden programar para dar algún tipo de respuesta al atacante; por ejemplo, devolver un banner del servicio. Más allá de la respuesta básica, los servicios no son reales —emulan servicios reales—; por lo tanto, el atacante no puede obtener acceso al sistema.

De interacción baja

Simula solo algunos servicios de red básicos, como la conectividad TCP/IP, ICMP, NetBIOS, etc. La información que podemos recolectar de este tipo de *honeypot* es mucho más escasa; básicamente, solo podremos saber si alguien está escaneando la red, pero no podremos obtener más información sobre las técnicas o las intenciones detrás de dicha acción. Su implementación en la red es mucho más segura, aunque, por otro lado, un atacante experimentado podría darse cuenta de que el equipo es un señuelo y abandonar sus planes" (Confederación de Empresarios de La Coruña, 2020, https://n9.cl/ytx55a).

De nada serviría la implementación de un *honeypot* en la red si no recolectamos la información que este genera y la utilizamos para fines productivos.

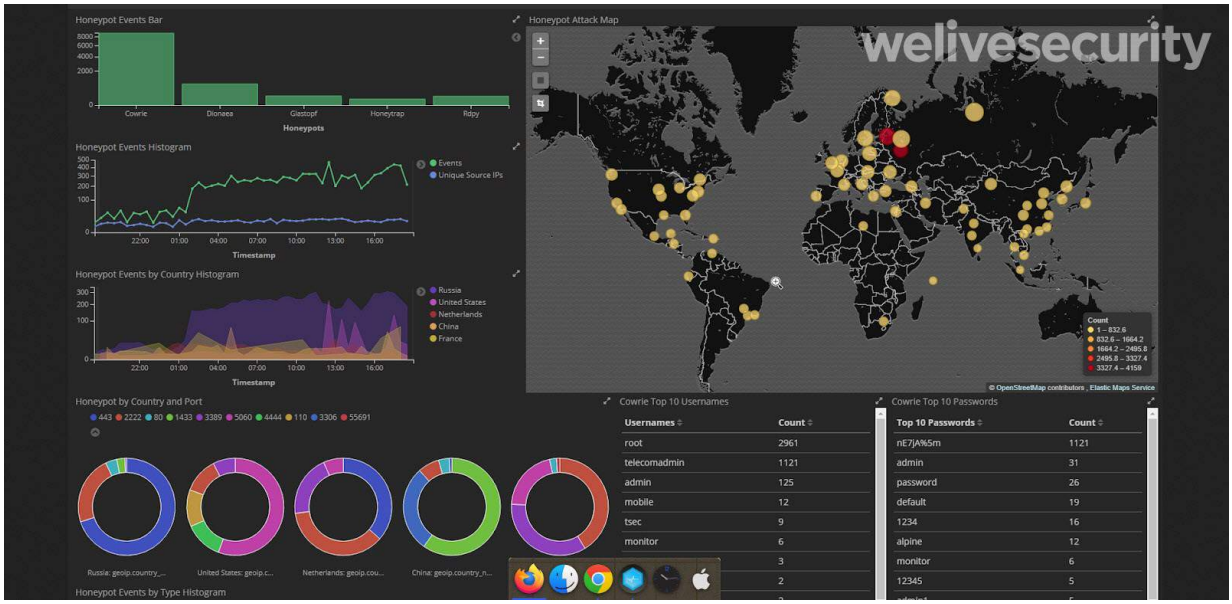
Herramienta *honeypot*: T-Pot

"T-Pot es un desarrollo de código abierto que combina *honeypots* de baja y alta interacción en un único sistema. Su implementación es bastante sencilla (no debería tomar más de 30 minutos en desplegarse) y nos permite emular servicios de red como Android ADB, *hardware* de red vulnerable como *routers*, SCADA, SSH, Telnet, DICOM, Elasticsearch, FTP, RDP, HTTP/S, postgreSQL, MSSQL, POP3, SMTP, SMB, entre otros.

Si bien lo ideal es crear un *honeypot* personalizado con los mismos servicios que se prestan en nuestra red y nada más, T-Pot es una forma más rápida y sencilla de desplegar un *honeypot* si no poseemos el tiempo o los recursos para desarrollar uno propio. Además, puede ser configurado de acuerdo con las necesidades específicas de la organización.

Una de las ventajas es que provee una interfaz gráfica para visualizar la información generada de forma sencilla y la generación de reportes. Puede ser desplegado tanto en máquinas físicas como virtuales" (Confederación de Empresarios de La Coruña, 2020, https://n9.cl/ytx55a).

Figura 5: Mapa de *honeypots*



Fuente: [imagen sin título sobre mapa de honeypots], s. f., https://n9.cl/8wjzp2.

Redes definidas por *software*

Son redes que separan el control *plane* del *data plane*, usadas por empresas como Google, Amazon, entre otras y que permiten una administración centralizada, realizar pruebas de seguridad, entre otras tareas. Aquí solo mencionaremos la existencia de las mismas.

Las redes definidas por *software* (SDN o *software-defined networking*) son una arquitectura de redes ágil y diseñada para agilizar la administración de TI y centralizar el control y ayudar a las organizaciones a seguir el ritmo de la naturaleza dinámica de las aplicaciones actuales. Separa la administración de la red de la infraestructura de red subyacente; por lo tanto, los administradores pueden simplificar el aprovisionamiento de los recursos de la red.

CONTINUAR

Referencias

[Imagen sin título sobre las 7 capas del modelo OSI] (2021). https://www.fs.com/es/blog/tcpip-vs-osi-whats-the-difference-between-the-two-models-28289.html.

[Imagen sin título sobre mapa de honeypots] (s.f.). https://github.com/telekom-security/tpotce.

Aleph (2021). *Qué es una red y tipos de red*. Aleph. https://aleph.org.mx/que-es-una-red-y-tipos-de-red.

Carrillo Ledesma, A. y González Rosas, K. (2020). *Seguridad, Privacidad y Vigilancia*. Facultad de Ciencias, UNAM.

Confederación de Empresarios de La Coruña (2020). *Qué es un honeypot y cómo implementarlo en nuestra red*. CEC. https://www.cec.es/que-es-un-honeypot-y-como-implementarlo-en-nuestra-red/.

Confederación de Empresarios de La Coruña (2021). *Suricata*. CEC. https://www.cec.es/como-detectar-malware-con-reglas-de-suricata/.

Crossover (s.f.). *Servicios de monitoreo de redes – enlaces*. Crossover. https://crossover.co.cr/monitoreo-soc-noc/.

DesarrolladorSoft (2021). *Sombrero blanco - Seguridad Informática*. DesarrolladorSoft. https://blog.desarrolladorsoft.com/2021/10/sombrero-blanco.html.

García Betancurt, Y. (s.f.). ¿Qué es cifrado simétrico? Ceupe. https://www.ceupe.co/blog/que-es-cifrado-simetrico.html.

Lara, C. (2021). *¿Qué es el monitoreo de red y por qué te interesa?* ICorp. https://icorp.com.mx/blog/que-es-el-monitoreo-de-red-y-por-que-te-interesa/.

OSAO (2020). *Prácticas para una red segura*. OSAO. https://osao.com.mx/practicas-para-una-red-segura/.

Pathak, A. (2025). *El mejor software de supervisión de redes para 2025*. Geekflare. https://geekflare.com/es/network-monitoring-software/.

Progress Software Corporation (s.f.). *Introducción al monitoreo de la red*. Progress Software Corporation. https://www.whatsupgold.com/es/que-es-el-monitoreo-de-la-red.

Sánchez Castillo, J. (2018). *Diferencia entre un Switch capa 2 y un Switch capa 3*. JM Systems Perú. https://jmsystemsperu.com/wp/blog-post/diferencia-entre-un-switch-capa-2-y-un-switch-capa-3/.

Telefónica Tech (s. f.). *Ocho siglas relacionadas con las vulnerabilidades (I): CVE*. Telefónica Tech. https://telefonicatech.com/blog/ocho-siglas-relacionadas-con-las-6.

CONTINUAR

Lección 4 de 4

Descarga en PDF