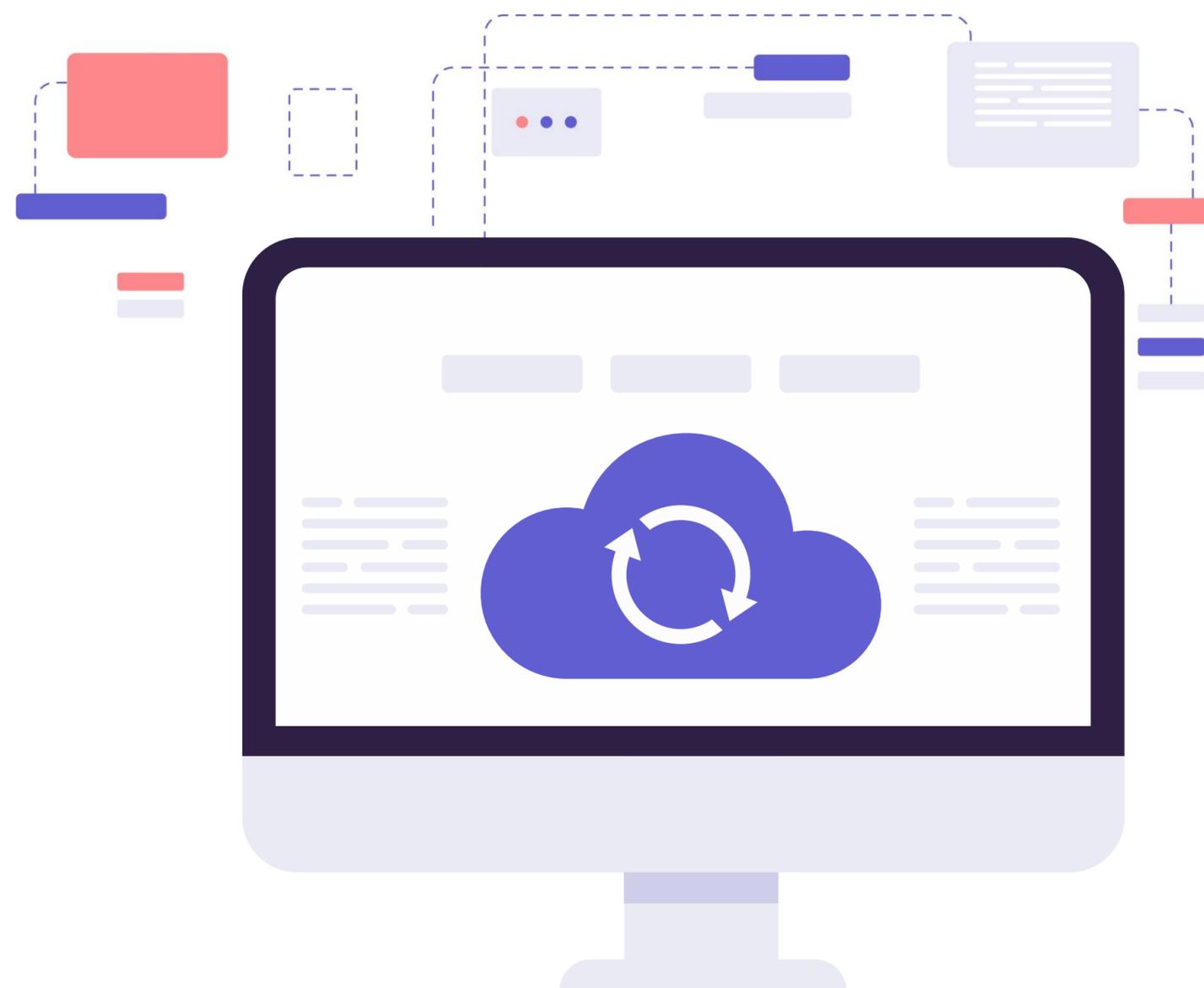


# RECOMENDACIONES DE CIBERSEGURIDAD EN BASE A DETECCIÓN Y ANÁLISIS DE VULNERABILIDADES.

**Módulo 8: Sistemas Operativos de Redes.**

 **Telecomunicaciones**



# Perfil de Egreso - Objetivos de Aprendizaje de la Especialidad

Módulo 1	<p><b>OA1</b> Leer y utilizar esquemas, proyectos y en general todo el lenguaje simbólico asociado a las operaciones de montaje y mantenimiento de redes de telecomunicaciones.</p>	Módulo 6	<p><b>OA8</b> Instalar y configurar una red inalámbrica según tecnologías y protocolos establecidos.</p> <p><b>OA7</b> Aplicar la normativa y los implementos de seguridad y protección relativos al montaje y el mantenimiento de las instalaciones de telecomunicaciones y la normativa del medio ambiente.</p>
Módulo 2	<p><b>OA6</b> Realizar mantenimiento y reparaciones menores en equipos y sistemas de telecomunicaciones, utilizando herramientas y pautas de mantención establecidas por el fabricante.</p> <p><b>OA7</b> Aplicar la normativa y los implementos de seguridad y protección relativos al montaje y el mantenimiento de las instalaciones de telecomunicaciones y la normativa del medio ambiente.</p>	Módulo 7	<p><b>OA5</b> Instalar y configurar una red de telefonía (tradicional o IP) en una organización según los parámetros técnicos establecidos.</p>
Módulo 3	<p><b>OA2</b> Instalar equipos y sistemas de telecomunicaciones de generación, transmisión, repetición, amplificación, recepción, y distribución de señal de voz, imagen y datos, según solicitud de trabajo y especificaciones técnicas del proyecto.</p> <p><b>OA10</b> Determinar los equipos y sistemas de comunicación necesarios para una conectividad efectiva y eficiente, de acuerdo a los requerimientos de los usuarios.</p>	Módulo 8	<p><b>OA3</b> Instalar y/o configurar sistemas operativos en computadores o servidores con el fin de incorporarlos a una red LAN, cumpliendo con los estándares de calidad y seguridad establecidos.</p>
Módulo 4	<p><b>OA9</b> Detectar y corregir fallas en circuitos de corriente continua de acuerdo a los requerimientos técnicos y de seguridad establecidos.</p>	Módulo 9	<p><b>OA10</b> Determinar los equipos y sistemas de comunicación necesarios para una conectividad efectiva y eficiente, de acuerdo, a los requerimientos de los usuarios.</p> <p><b>OA6</b> Realizar el mantenimiento y reparaciones menores en equipos y sistemas de telecomunicaciones, utilizando herramientas y pautas de mantención establecidas por el fabricante.</p>
Módulo 5	<p><b>OA2</b> Instalar equipos y sistemas de telecomunicaciones de generación, transmisión, repetición, amplificación, recepción y distribución de señal de voz, imagen y datos, según solicitud de trabajo y especificaciones técnicas del proyecto.</p> <p><b>OA4</b> Realizar medidas y pruebas de conexión y de continuidad de señal eléctrica, de voz, imagen y datos- en equipos, sistemas y de redes de telecomunicaciones, utilizando instrumentos de medición y certificación de calidad de la señal autorizada por la normativa vigente.</p>	Módulo 10	<p>No está asociado a Objetivos de Aprendizaje de la Especialidad (AOE), sino a genéricos. No obstante, puede asociarse a un OAE como estrategia didáctica.</p>



# Perfil de Egreso – Objetivos de Aprendizaje Genéricos

<p><b>A-</b> Comunicarse oralmente y por escrito con claridad, utilizando registros de habla y de escritura pertinentes a la situación laboral y a la relación con los interlocutores.</p>	<p><b>B-</b> Leer y utilizar distintos tipos de textos relacionados con el trabajo, tales como especificaciones técnicas, normativas diversas, legislación laboral, así como noticias y artículos que enriquezcan su experiencia laboral.</p>	<p><b>C-</b> Realizar las tareas de manera prolija, cumpliendo plazos establecidos y estándares de calidad, y buscando alternativas y soluciones cuando se presentan problemas pertinentes a las funciones desempeñadas.</p>
<p><b>D-</b> Trabajar eficazmente en equipo, coordinando acciones con otros in situ o a distancia, solicitando y prestando cooperación para el buen cumplimiento de sus tareas habituales o emergentes.</p>	<p><b>E-</b> Tratar con respeto a subordinados, superiores, colegas, clientes, personas con discapacidades, sin hacer distinciones de género, de clase social, de etnias u otras.</p>	<p><b>F-</b> Respetar y solicitar respeto de deberes y derechos laborales establecidos, así como de aquellas normas culturales internas de la organización que influyen positivamente en el sentido de pertenencia y en la motivación laboral.</p>
<p><b>G-</b> Participar en diversas situaciones de aprendizaje, formales e informales, y calificarse para desarrollar mejor su trabajo actual o bien para asumir nuevas tareas o puestos de trabajo, en una perspectiva de formación permanente.</p>	<p><b>H-</b> Manejar tecnologías de la información y comunicación para obtener y procesar información pertinente al trabajo, así como para comunicar resultados, instrucciones e ideas.</p>	<p><b>I-</b> Utilizar eficientemente los insumos para los procesos productivos y disponer cuidadosamente los desechos, en una perspectiva de eficiencia energética y cuidado ambiental.</p>
<p><b>J-</b> Emprender iniciativas útiles en los lugares de trabajo y/o proyectos propios, aplicando principios básicos de gestión financiera y administración para generarles viabilidad.</p>	<p><b>K-</b> Prevenir situaciones de riesgo y enfermedades ocupacionales, evaluando las condiciones del entorno del trabajo y utilizando los elementos de protección personal según la normativa correspondiente.</p>	<p><b>L-</b> Tomar decisiones financieras bien informadas, con proyección a mediano y largo plazo, respecto del ahorro, especialmente del ahorro previsional, de los seguros, y de los riesgos y oportunidades del endeudamiento crediticio así como de la inversión.</p>



# Marco de Cualificaciones Técnico Profesional (MCTP) Nivel 3 y su relación con los OAG

## HABILIDADES

### 1. Información

1. Analiza y utiliza información de acuerdo a parámetros establecidos para responder a las necesidades propias de sus actividades y funciones.

2. Identifica y analiza información para fundamentar y responder a las necesidades propias de sus actividades.

### 2. Resolución de problemas

1. Reconoce y previene problemas de acuerdo a parámetros establecidos en contextos conocidos propios de su actividad o función.

2. Detecta las causas que originan problemas en contextos conocidos de acuerdo a parámetros establecidos.

3. Aplica soluciones a problemas de acuerdo a parámetros establecidos en contextos conocidos propios de una función.

### 3. Uso de recursos

1. Selecciona y utiliza materiales, herramientas y equipamiento para responder a una necesidad propia de una actividad o función especializada en contextos conocidos.

2. Organiza y comprueba la disponibilidad de los materiales, herramientas y equipamiento.

3. Identifica y aplica procedimientos y técnicas específicas de una función de acuerdo a parámetros establecidos.

### 4. Comunicación

4. Comunica y recibe información relacionada a su actividad o función, a través de medios y soportes adecuados en contextos conocidos.

## APLICACIÓN EN CONTEXTO

### 5. Trabajo con otros

1. Trabaja colaborativamente en actividades y funciones coordinándose con otros en diversos contextos.

### 6. Autonomía

1. Se desempeña con autonomía en actividades y funciones especializadas en diversos contextos con supervisión directa.

2. Toma decisiones en actividades propias y en aquellas que inciden en el quehacer de otros en contextos conocidos.

3. Evalúa el proceso y el resultado de sus actividades y funciones de acuerdo a parámetros establecidos para mejorar sus prácticas.

4. Busca oportunidades y redes para el desarrollo de sus capacidades

### 7. Ética y responsabilidad

1. Actúa de acuerdo a las normas y protocolos que guían su desempeño y reconoce el impacto que la calidad de su trabajo tiene sobre el proceso productivo o la entrega de servicios.

2. Responde por cumplimiento de los procedimientos y resultados de sus actividades.

3. Comprende y valora los efectos de sus acciones sobre la salud y la vida, la organización, la sociedad y el medio ambiente.

4. Actúa acorde al marco de sus conocimientos, experiencias y alcance de sus actividades y funciones

## CONOCIMIENTO

### 8. Conocimientos

1. Demuestra conocimientos específicos de su área y de las tendencias de desarrollo para el desempeño de sus actividades y funciones.



# Metodología seleccionada

## Simulación de contextos laborales

- Esta presentación les ayudará a poder comprender los conceptos necesarios para el desarrollo de su actividad.

## Aprendizaje Esperado

- **AE5.** Evalúa la seguridad de una red utilizando técnicas de criptografía, reconocimiento, escaneo, proponiendo recomendaciones en un informe de hallazgos y brechas de seguridad encontrados.



# ¿Qué vamos a lograr con esta actividad para llegar al Aprendizaje Esperado (AE)?

**Analizar** vulnerabilidades encontradas, usando técnicas de escaneo.

**Identificar** componentes de un informe técnico de Ciberseguridad.



# Pregunta o actividad para detectar qué saben del tema o atraer el interés de estudiantes al tema...

**¿Se han dado cuenta de la cantidad de ataques que han sufrido las empresas este último tiempo?**

**¿Alguien puede indicar algún ejemplo y lo que sabe al respecto?**



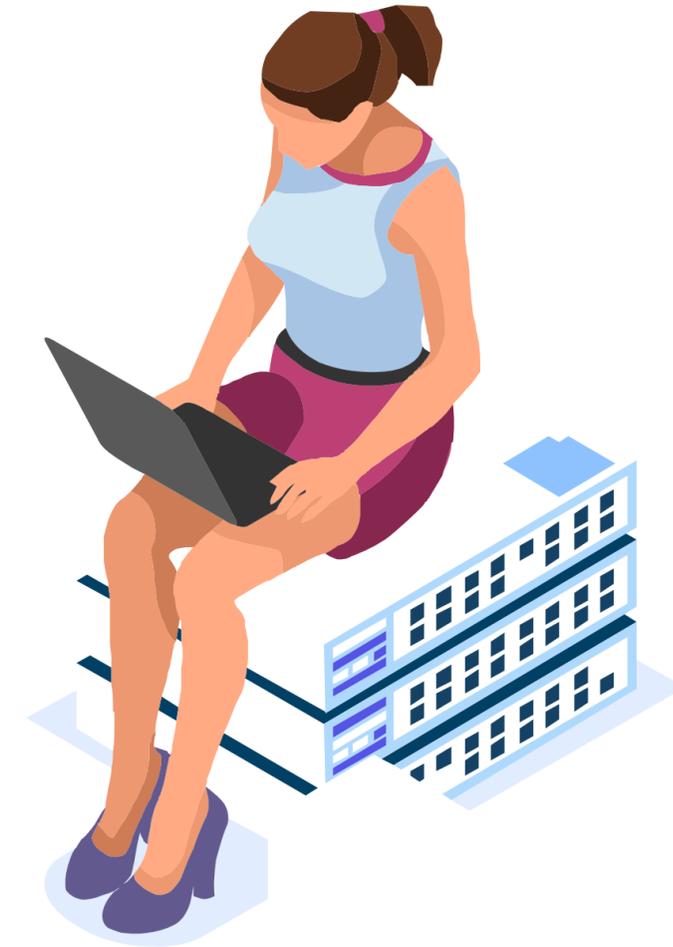
# ¿Qué es la recopilación de información de un sistema informático?

- En el proceso de **pentester (prueba de penetración a un sistema)** es de suma importancia la buena **recopilación de información (footprinting)** de nuestro objetivo, ya que mientras más información logremos obtener de nuestro objetivo, más posibilidades tenemos de ingresar a sus sistemas informáticos.



# ¿Qué información podemos recolectar ?

- Algunos ejemplos de elementos de información que se pueden recolectar son:
  - *Direcciones IP.*
  - *Correos electrónicos.*
  - *Información de los empleados.*
  - *Sistemas operativos utilizados por la empresa.*
  - *Números telefónicos.*

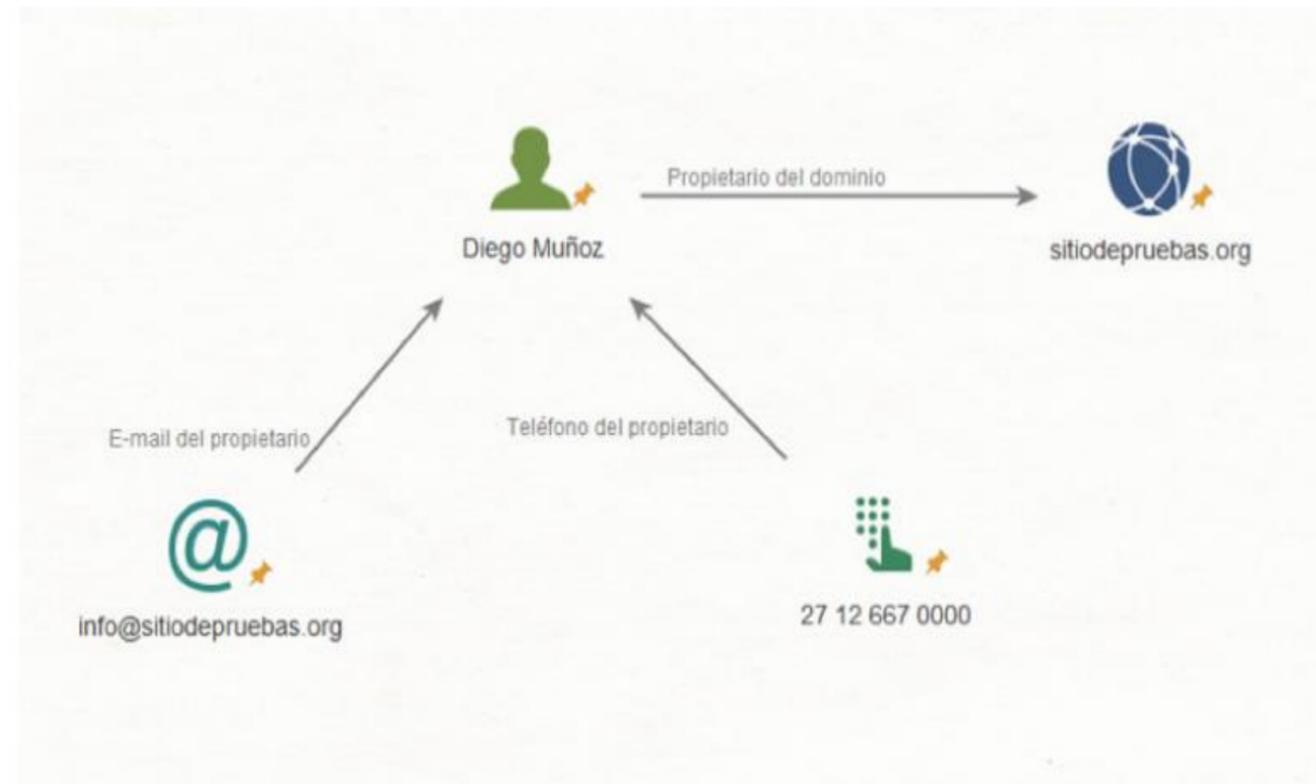


# ¿Qué herramientas existen para recopilar información?

- Existen software para el proceso de recopilar información.

Ejemplos:

- *Software MALTEGO.*
- *TheHarvester.*



Fuente imagen: <https://ciberpatrulla.com/maltego/>

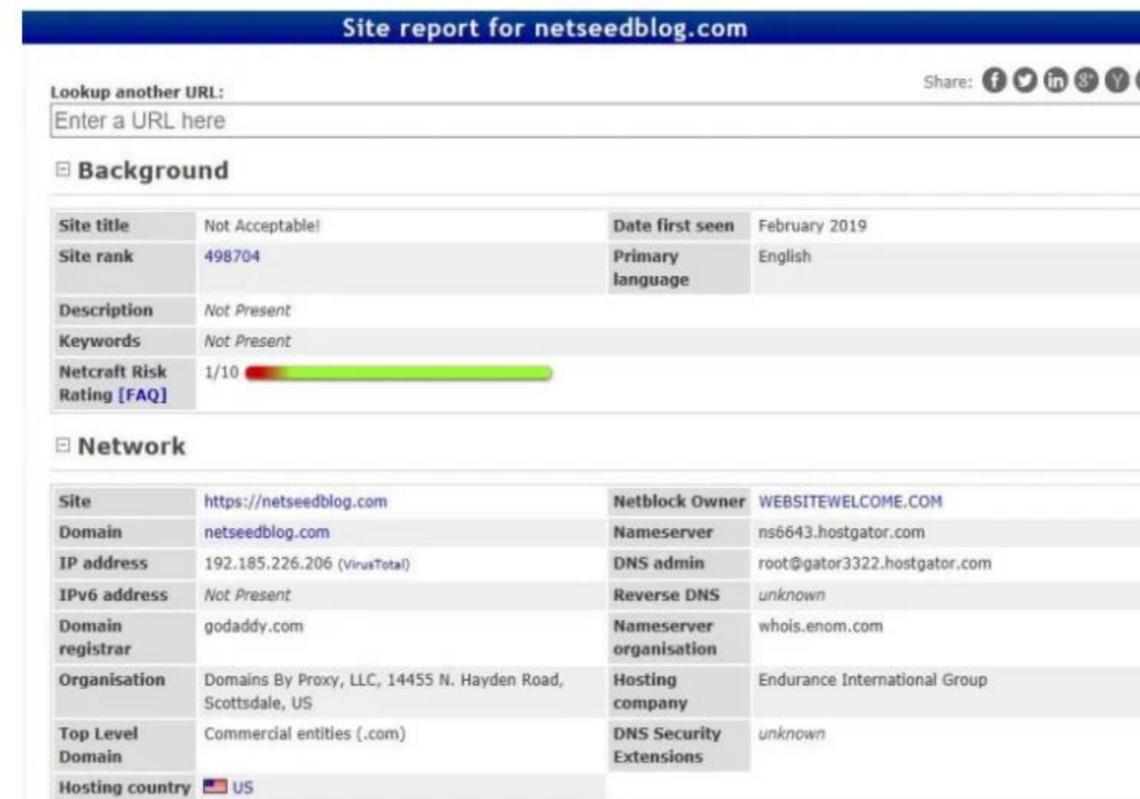


# ¿Existen páginas para poder recopilar información?

- Existen páginas para el proceso de recopilar información.

Ejemplos:

- <https://www.netcraft.com/>
- <https://whois.domaintools.com/>



Site report for netseedblog.com

Lookup another URL:  Share: [f](#) [t](#) [in](#) [g+](#) [y](#) [e](#)

### Background

Site title	Not Acceptable!	Date first seen	February 2019
Site rank	498704	Primary language	English
Description	Not Present		
Keywords	Not Present		
Netcraft Risk Rating [FAQ]	1/10 		

### Network

Site	<a href="https://netseedblog.com">https://netseedblog.com</a>	Netblock Owner	WEBSITEWELCOME.COM
Domain	netseedblog.com	Nameserver	ns6643.hostgator.com
IP address	192.185.226.206 (VirusTotal)	DNS admin	root@gator3322.hostgator.com
IPv6 address	Not Present	Reverse DNS	unknown
Domain registrar	godaddy.com	Nameserver organisation	whois.enom.com
Organisation	Domains By Proxy, LLC, 14455 N. Hayden Road, Scottsdale, US	Hosting company	Endurance International Group
Top Level Domain	Commercial entities (.com)	DNS Security Extensions	unknown
Hosting country	 US		

Fuente imagen: <https://netseedblog.com/security/footprinting-passive-information-gathering/>



# Pregunta de Reflexión

Si tuvieran que recopilar información de un sistema informático:

**¿Qué información sería?  
Indique algunos ejemplos y  
dé razones de su elección.**



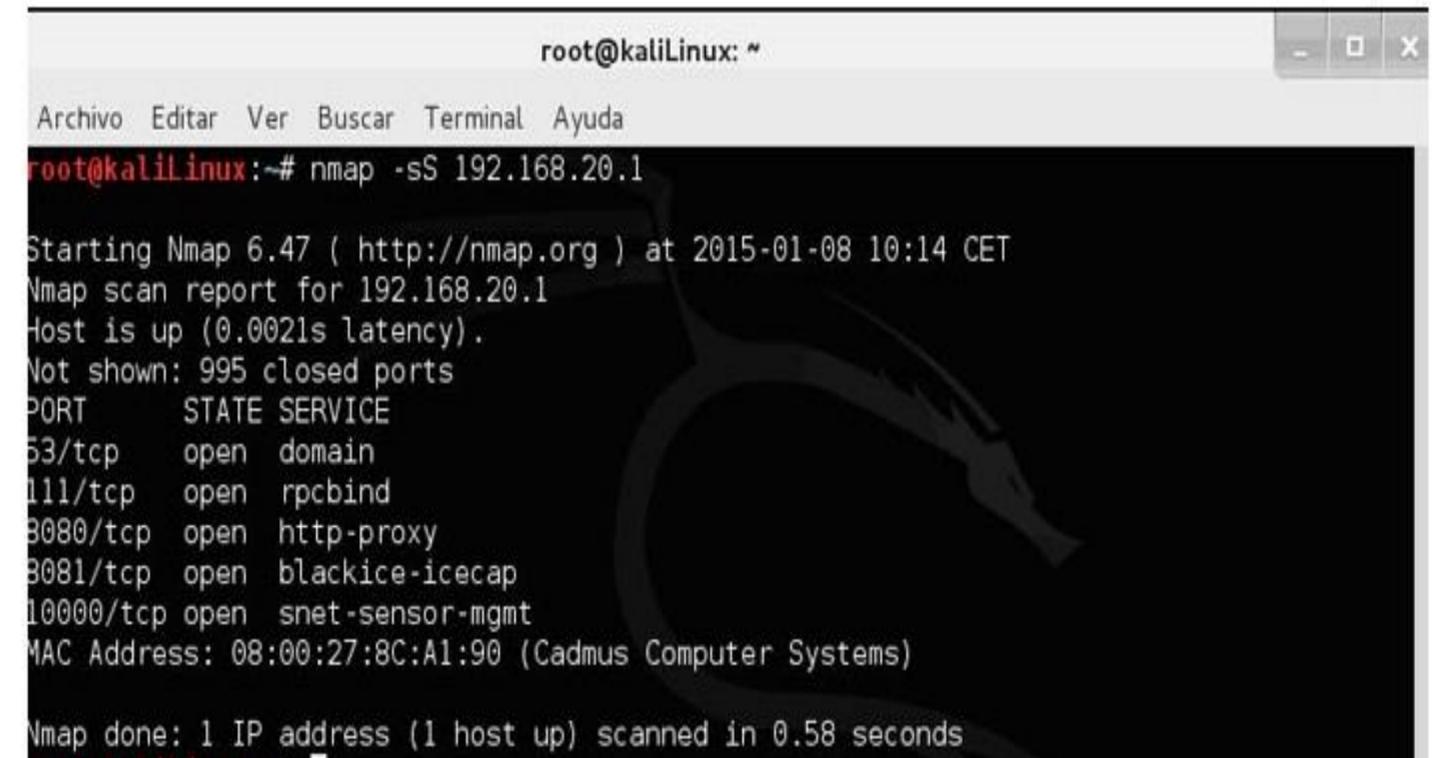
# ¿Qué es la enumeración?

- **Enumeración:** corresponde a tener ya contacto directo con los dispositivos para hacer pruebas e identificar información de ellos.
  - En esta fase trataremos de analizar una aplicación, un equipo, un sistema, unos servicios y sus versiones, sistemas operativos, vulnerabilidades.
  - Con toda esta información podremos entender de mejor manera la estructura del sistema informático.



# ¿Algunos software o herramientas para el proceso de enumeración?

- **Netdiscovery:** Muestra la dirección IP, la MAC, y el fabricante de la tarjeta de red, además de los equipos conectados a la red.
- **NMAP:** Posee varias opciones de información, siendo una de las más utilizadas el Scanner de puertos.
- **Nessus:** Scanner de vulnerabilidades.



```
root@kaliLinux: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
root@kaliLinux:~# nmap -sS 192.168.20.1  
Starting Nmap 6.47 ( http://nmap.org ) at 2015-01-08 10:14 CET  
Nmap scan report for 192.168.20.1  
Host is up (0.0021s latency).  
Not shown: 995 closed ports  
PORT      STATE SERVICE  
53/tcp    open  domain  
111/tcp   open  rpcbind  
8080/tcp   open  http-proxy  
8081/tcp   open  blackice-icecap  
10000/tcp open  snet-sensor-mgmt  
MAC Address: 08:00:27:8C:A1:90 (Cadmus Computer Systems)  
Nmap done: 1 IP address (1 host up) scanned in 0.58 seconds
```

Fuente imagen: <http://www.cursodehackers.com/nmap.html>



# Pregunta de reflexión

**¿Cuál cree que es la vulnerabilidad que genera tener muchos puertos abiertos en un PC?**



# ¿Qué se hace en el proceso de análisis?

- En este proceso y contando toda la información recolectada y numerada, se debe evaluar y tomar las **decisiones correctivas para evitar o mitigar las vulnerabilidades de mi sistema.**
- **Observación:** el contenido específico sobre decisiones correctivas se encuentra disponible en presentación:

*“Recursos compartidos a través de una red de área local:  
vulnerabilidades, matriz de riesgo y plan de acción”*

**En M5\_AE1\_Act2**



# ¿Qué es un informe técnico ?

- Es el documento que se va entregar y donde debe estar toda la información técnica del proceso de recopilación de información.

## Recopilar Información (Footprinting):

- a. Enumeración (scanner de puertos, scanner de vulnerabilidades, etc.).
- b. Análisis de toda esta información.
- c. Recomendaciones de seguridad adecuada, ya sean:
  - *Implementaciones nuevas.*
  - *Políticas de seguridad, etc.*



# Test de intrusión o pentester



# Amenazas y Aspectos Legales

Al tener el conocimiento y las herramientas para detectar y analizar vulnerabilidades, contribuyes a cumplir con las leyes chilenas que resguardan la privacidad de la información. Aquellas personas que utilizan estas herramientas para vulnerar la ciberseguridad de terceros, se ven expuestos a delitos tipificados y penalizados en las leyes chilenas.

**La Ley N° 19.628** regula el trato de los datos de carácter personal, en registros o bancos de datos, por organismos públicos o privados, y es uno de los estatutos normativos más relevantes sobre la materia.

**La Ley 19223** Tipifica Figuras Penales Relativas a la Informática.

**Artículo 2°.-** El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.



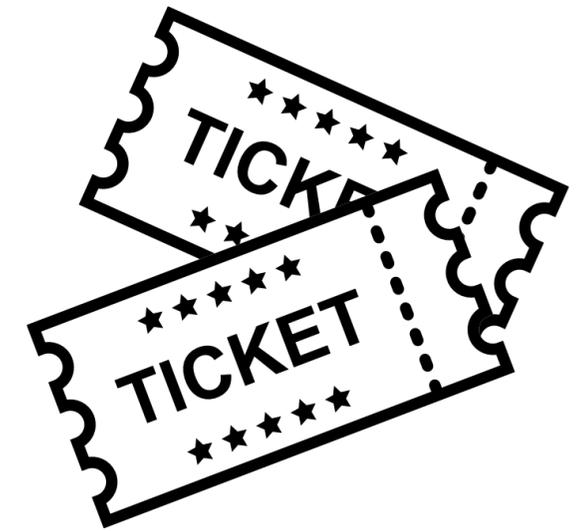
# Ticket de salida

- **Realiza un mapa conceptual** donde incluyas recursos (software) para detectar vulnerabilidades, función específica de cada recurso, elementos que deben ser analizados, amenazas o vulnerabilidades que pueden detectarse y recomendaciones de protección para evitar las vulnerabilidades:

**Alternativa 1:** En lugar de mapa conceptual pueden crear un breve video o un audio con la misma información.

**Alternativa 2:** Pueden transformar la actividad en preguntas a ser respondidas usando las herramientas que se presentan a continuación:

- **Kahoot - Mentimeter - Padlet - Google Forms.**



# REFERENCIAS DE CONTENIDO:

- <https://www.ciscopress.com/store/ccna-cyber-ops-secfnd-210-250-official-cert-guide-9781587147029>
- <https://www.dragonjar.org/>

