Ministerio de Educación
Gobierno de Chile

UNIVERSIDAD CATÓLICA DE TEMUCO

Recomendaciones de Ciberseguridad en base a detección y análisis de vulnerabilidades

Módulo 5: Configuración de la seguridad en redes de área local

Conectividad y Redes

Perfil de Egreso – Conectividad y redes

Módulo 1	**OA1** Leer y utilizar técnicamente proyectos de conectividad y redes, considerando planos o diagramas de una red de área local (red LAN), basándose en los modelos TCP/IP y OSI. **OA3** Instalar y mantener cableados estructurados, incluyendo fibra óptica, utilizados en la construcción de redes, basándose en las especificaciones técnicas correspondientes. **OA7** Instalar y configurar una red inalámbrica según tecnologías y protocolos establecidos.
Módulo 2	**OA2** Instalar y configurar sistemas operativos en computadores personales con el fin de incorporarlos a una red LAN, cumpliendo con los estándares de calidad y seguridad establecidos. **OA11** Armar y configurar un equipo personal, basándose en manuales de instalación, utilizando las herramientas apropiadas y respetando las normas de seguridad establecidos.
Módulo 3	**OA8** Aplicar herramientas de software que permitan obtener servicios de intranet e internet de manera eficiente.
Módulo 4	**OA4** Realizar pruebas de conexión y señales en equipos y redes, optimizando el rendimiento de la red y utilizando instrumentos de medición y certificación de calidad de la señal, considerando las especificaciones técnicas.
Módulo 5	**OA5** Aplicar métodos de seguridad informática para mitigar amenazas en una red LAN, aplicando técnicas como filtrado de tráfico, listas de control de acceso u otras.
Módulo 6	**OA9** Mantener y actualizar el hardware de los computadores personales y de comunicación, basándose en un cronograma de trabajo, de acuerdo a las especificaciones técnicas del equipo.
Módulo 7	**OA10** Mantener actualizado el software de productividad y programas utilitarios en un equipo personal, de acuerdo a los requerimientos de los usuarios.
Módulo 8	**OA6** Aplicar procedimientos de recuperación de fallas y realizar copias de respaldo de los servidores, manteniendo la integridad de la información.
Módulo 9	No esta asociado a Objetivos de Aprendizaje de la Especialidad (OAE), sino a Genéricos. No obstante, puede asociarse a un OAE como estrategia didáctica.

Perfil de Egreso – Objetivos de Aprendizaje Genéricos

A- 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.	**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.	**C-** 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.
D- 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.	**E-** Tratar con respeto a subordinados, superiores, colegas, clientes, personas con discapacidades, sin hacer distinciones de género, de clase social, de etnias u otras.	**F-** 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.
G- 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.	**H-** Manejar tecnologías de la información y comunicación para obtener y procesar información pertinente al trabajo, así como para comunicar resultados, instrucciones e ideas.	**I-** Utilizar eficientemente los insumos para los procesos productivos y disponer cuidadosamente los desechos, en una perspectiva de eficiencia energética y cuidado ambiental.
J- Emprender iniciativas útiles en los lugares de trabajo y/o proyectos propios, aplicando principios básicos de gestión financiera y administración para generarles viabilidad.	**K-** 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.	**L-** 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.

Marco de Cualificaciones Técnico Profesional (MCTP) Nivel 3

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 funcion.
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 acuedo 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.Evalua 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 en contextos laborales

- Esta presentación te servirá para avanzar paso a paso en el desarrollo de la actividad propuesta.

Aprendizaje Esperado

- **5.4** 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.

¿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?

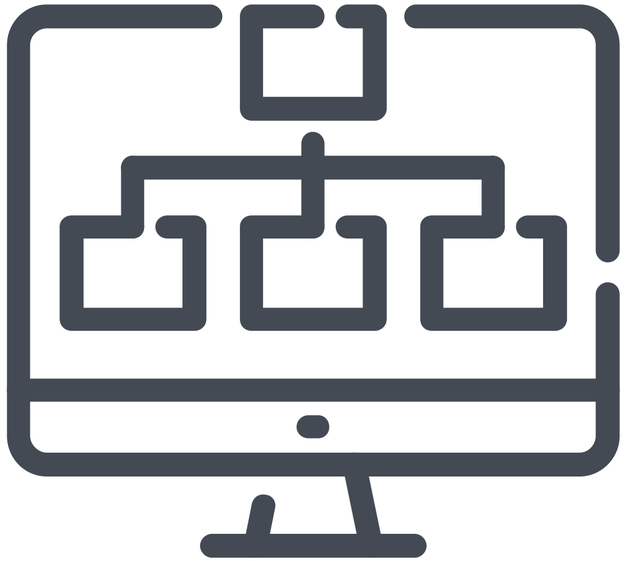
¿Qué es la recopilación de información de un sistema informático?

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 softwares para el proceso de recopilar información.

Ejemplos:

- Software MALTEGO
- TheHarvester

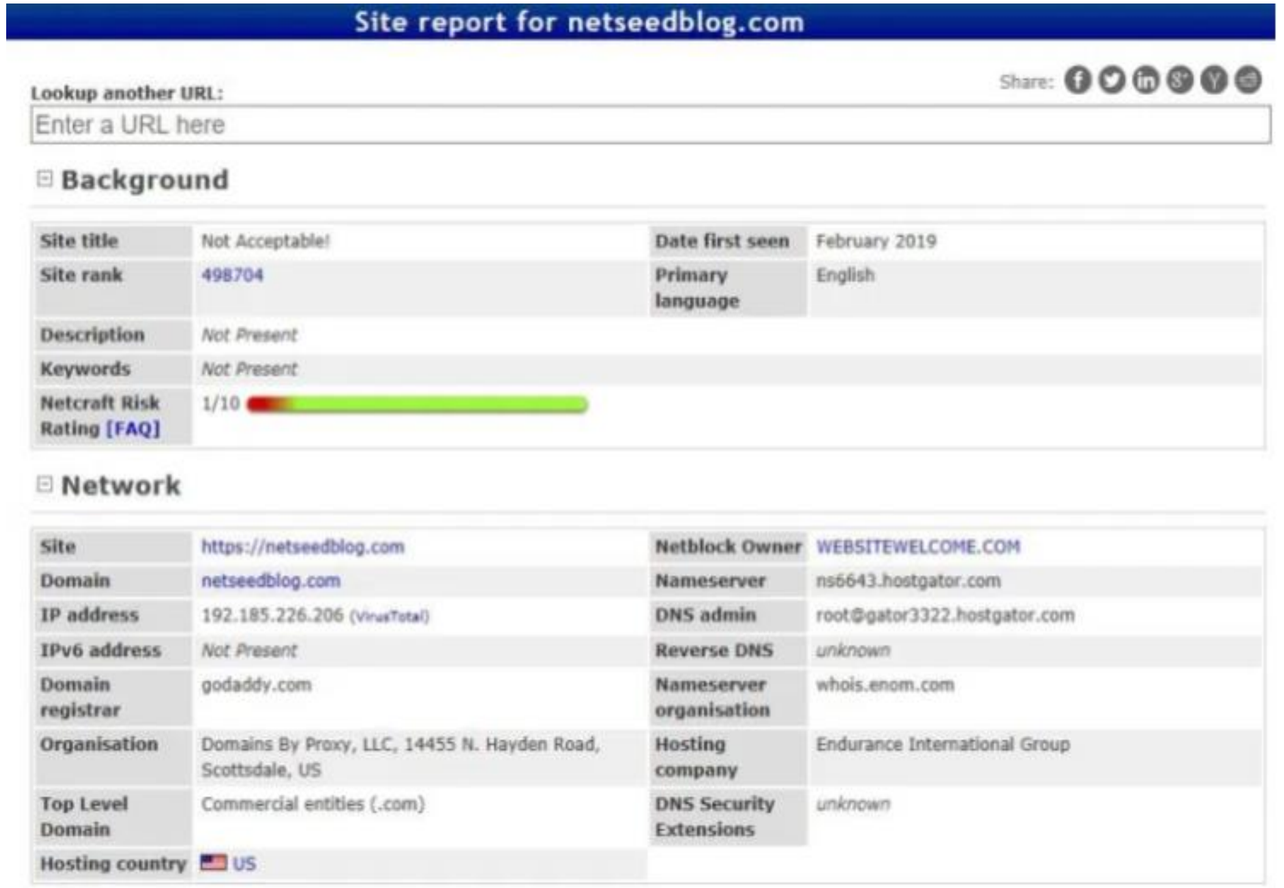
Fuente imagen: https://ciberpatrulla.com/maltego/

¿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:

Enter a URL here

Share:

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	https://netseedblog.com	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.

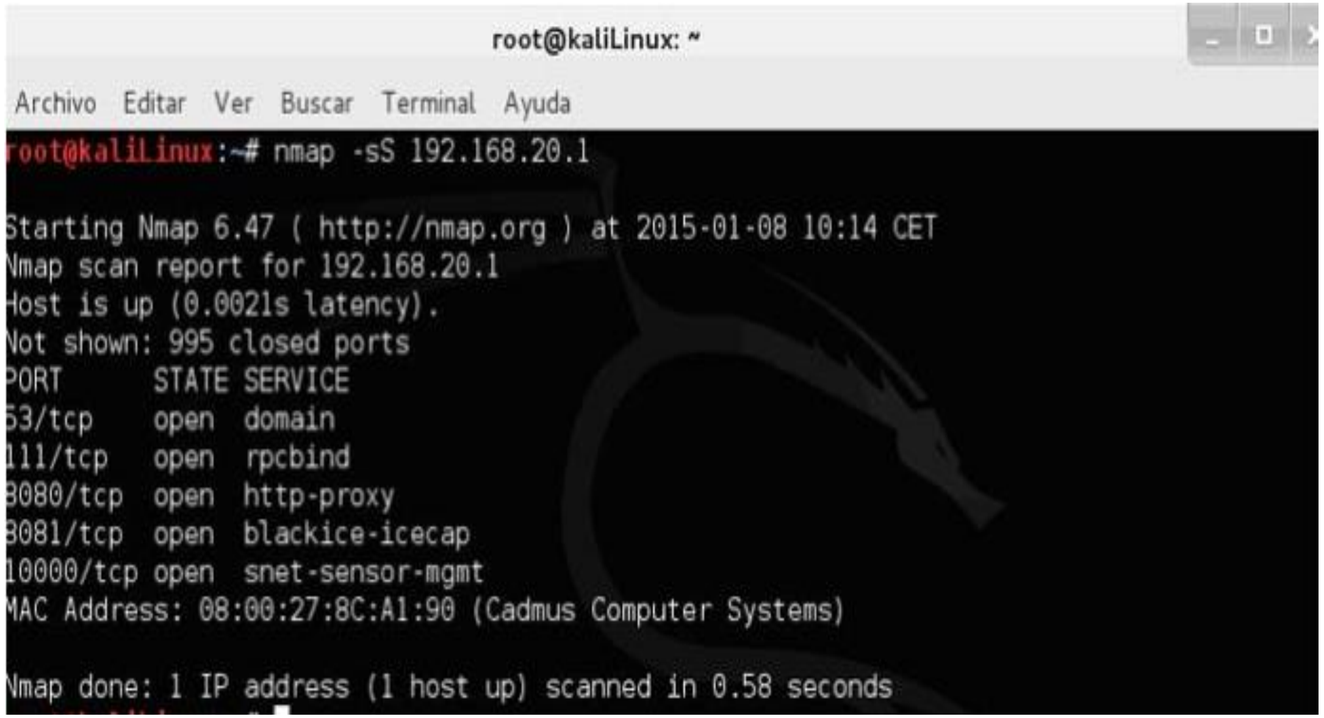
- Con toda esta información podremos entender de mejor manera la estructura del sistema informático.

¿Algunos softwares 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.



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?

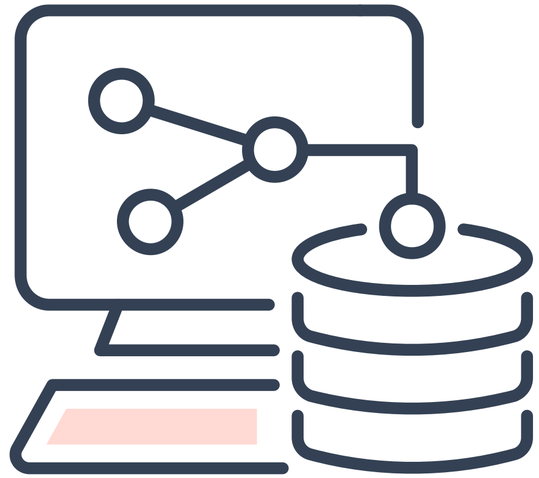
¿Qué es la enumeración?

- 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”.



¿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.

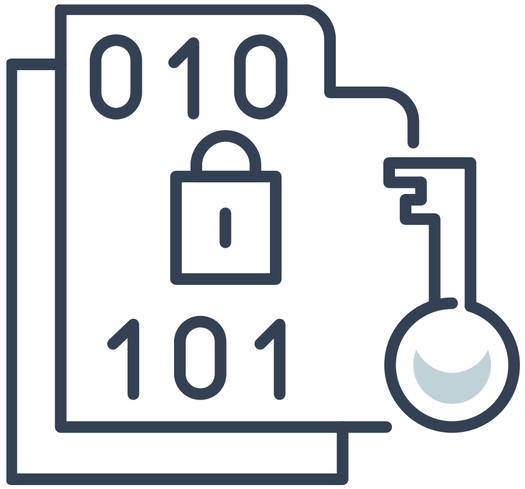
Recopilar Información (Footprinting):

01 **Enumeración (scanner de puertos, scanner de vulnerabilidades, etc.).**

02 **Análisis de toda esta información.**

03 **Recomendaciones de seguridad adecuada ya sean:**

- Implementaciones nuevas.
- Políticas de seguridad, etc.



Test de intrusión o pentester

Fuente imagen: https://integradoresdeti.wordpress.com/2017/08/27/pentesting/

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 19.223** 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

01

Realiza un mapa conceptual donde incluyas recursos (softwares) 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.

Referencias

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

https://www.dragonjar.org