DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

Introducción al hacking ético

Fundamentos de ciberseguridad

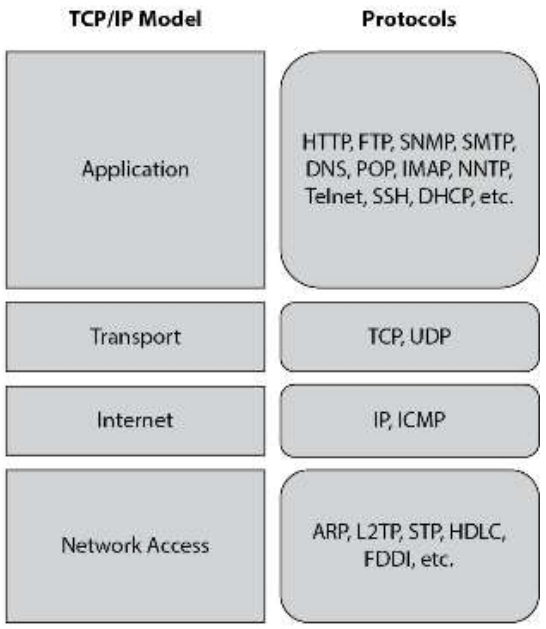
Profesor
Juan Ignacio Iturbe A.

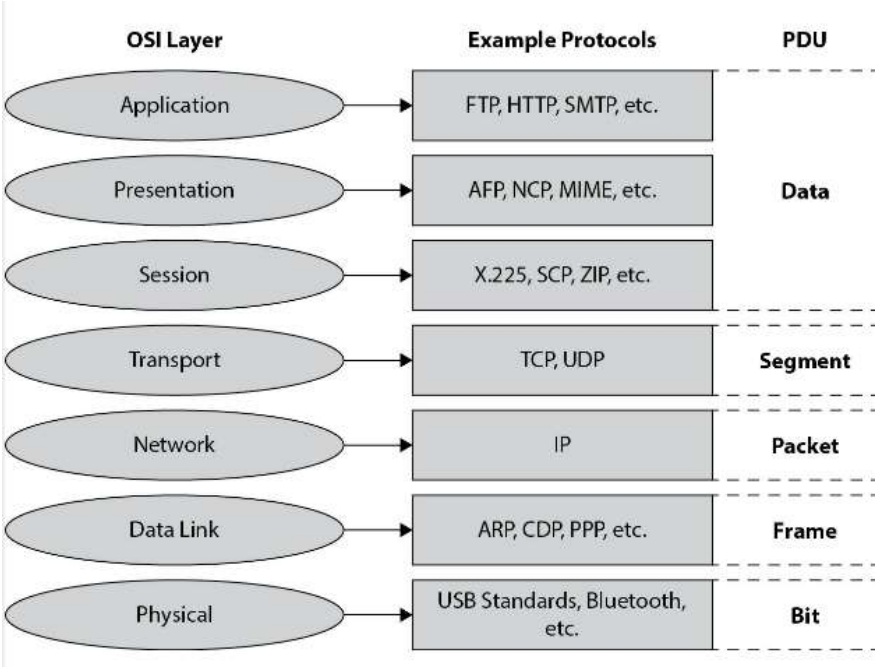
Conocimiento esencial

- Identificar los componentes de una red de computadores TCP/IP.
- Entender elementos básicos de seguridad de la información.
- Entender los pasos de la gestión de incidentes.
- Identificar los fundamentos de las políticas de seguridad.
- Identificar terminología esencial asociada al hacking ético.
- Definir el concepto de hacking ético y las clasificaciones de hackers.
- Describir las 5 etapas del hacking ético.
- Definir los tipos de ataques a sistemas.
- Definir lo tipos de ataques a sistemas
- Identificar las leyes, actos y estándares que afectan la ciberseguridad.

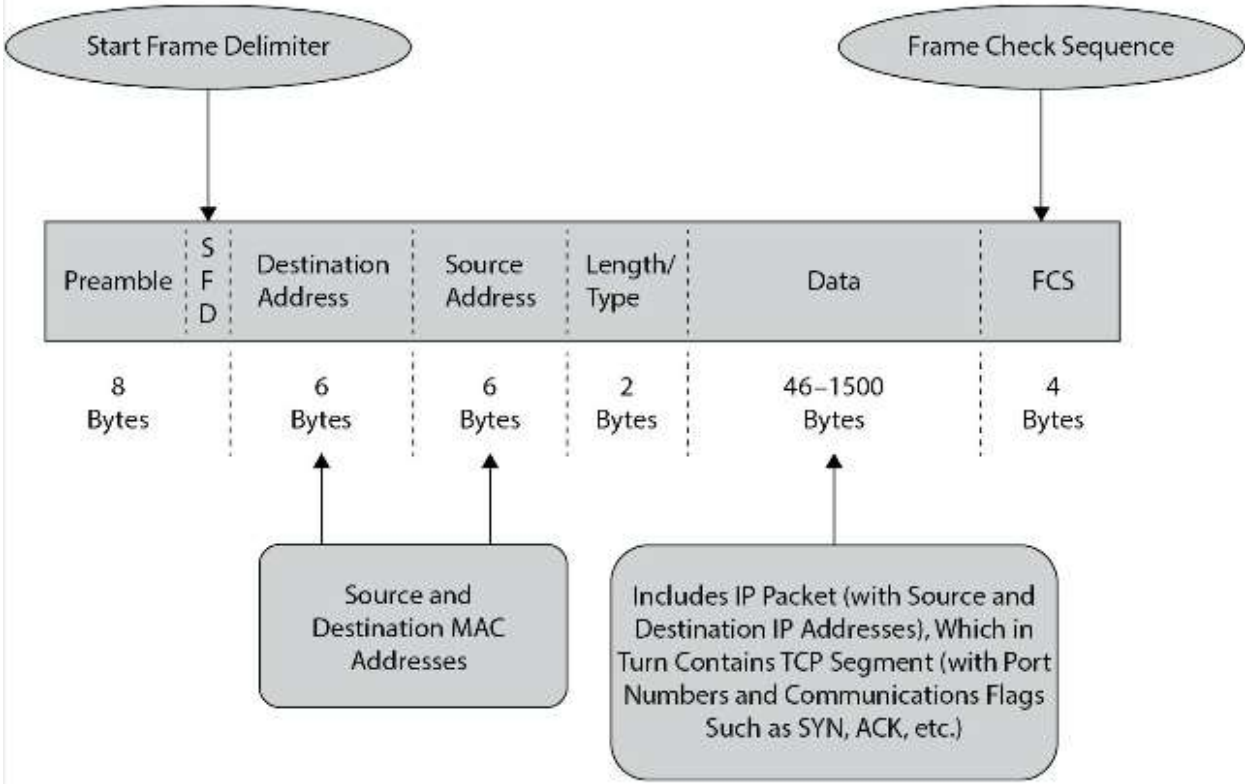
Modelo OSI y TCP/IP

- Deben repasar el modelo de referencia OSI y TCP/IP.



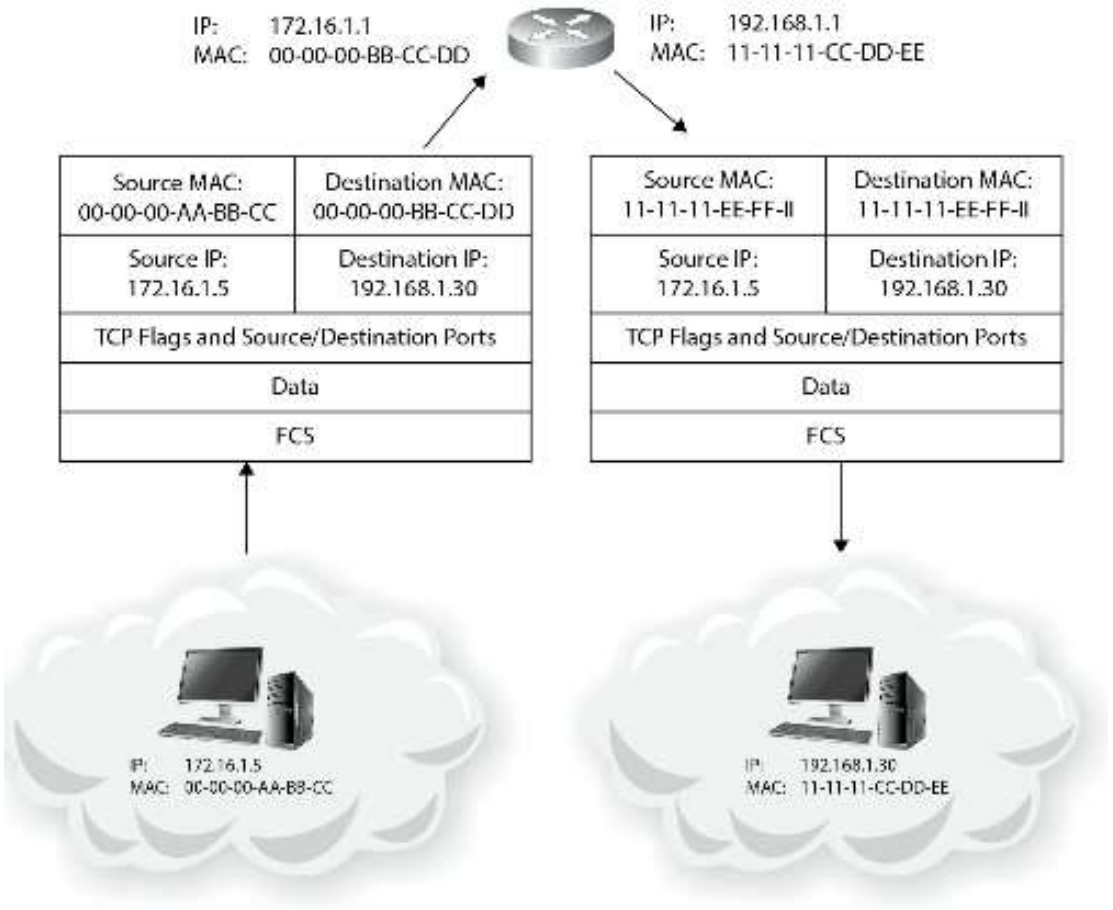


Trama ethernet

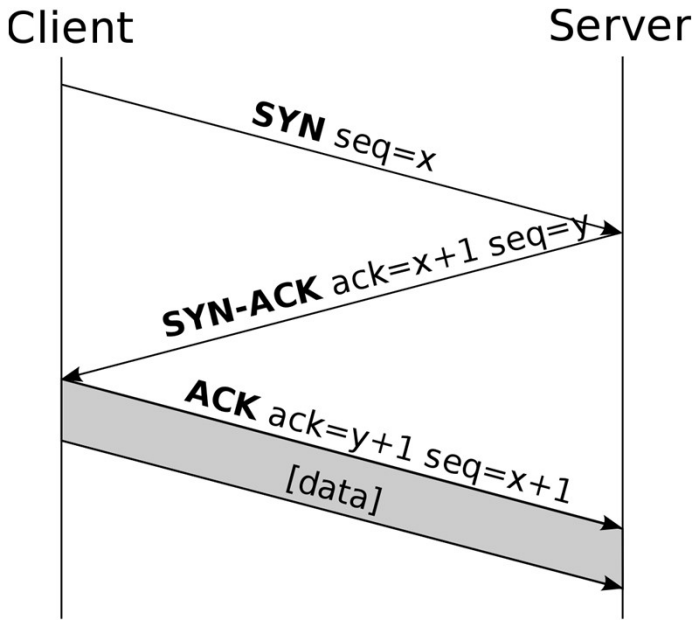


Revisar

- Subnetting
- El funcionamiento del protocolo ARP

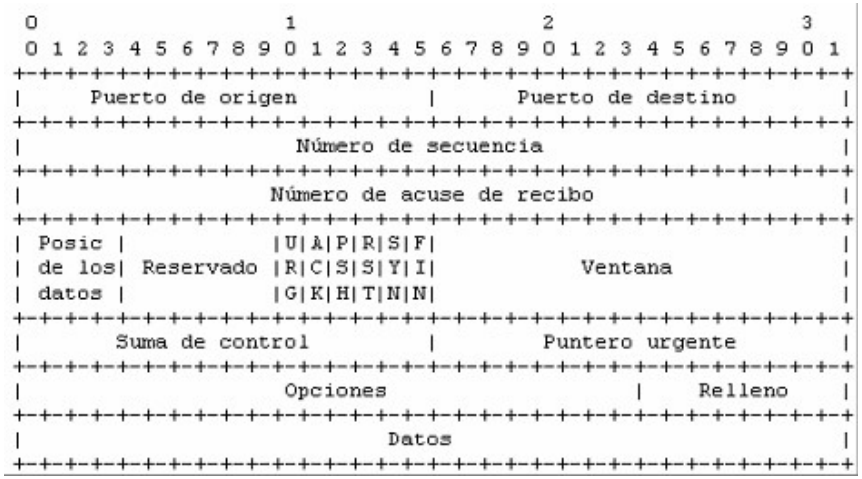


Handshake TCP



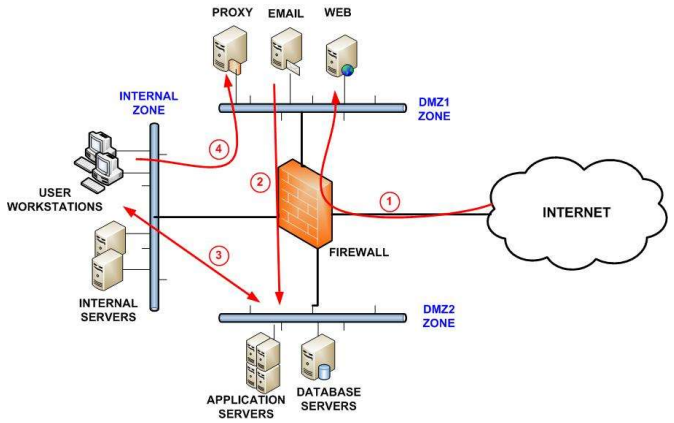
Handshake de tres vías

Cabecera TCP



Zonas de seguridad de red

- Internet: descontrol
- Internet DMZ: zona desmilitarizada, sin armamento.
- Zona de red de producción: muy restringidas y sin usuarios.
- Zona de intranet: que tiene poco o nada de restricciones. Se requieren menos controles internos.
- Zona de red administrada: altamente segura con políticas muy estrictas.



Vulnerabilidades

- Según [1]:

  "Una vulnerabilidad es simplemente una debilidad que puede ser explotada por un atacante para realizar acciones no autorizadas dentro de una computadora o sistema de red."

Recursos sobre vulnerabilidades

Recursos:

- Microsoft Vulnerability Research (technet.microsoft.com)
- Security Focus (www.securityfocus.com)
- Hackerstorm (www.hackerstorm.co.uk)
- Exploit Database (www.exploit-db.com)
- Security Magazine (www.securitymagazine.com)
- Trend Micro (www.trendmicro.com)
- Dark Reading (www.darkreading.com)
- Common Weakness Enumeration (cwe.mitre.org/)

Si se busca cuantificar el peligro o riesgo un una vulnerabilidad en particular:

- Common Vulnerability Scoring System (CVSS, https://www.first.org/cvss/)

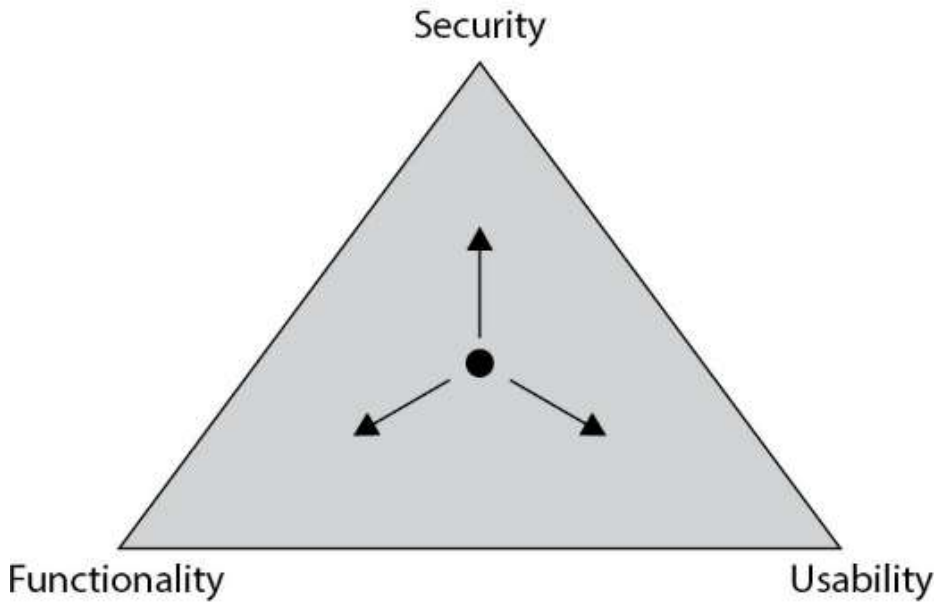
Categorías de vulnerabilidades

- Configuración incorrecta
- Instalaciones predeterminadas
- Desbordamientos de búfer
- Parches faltantes
- Fallas de diseño.
- Fallos del sistema operativo
- Fallas de por pobre codificación de la aplicación
- Servicios abiertos
- Contraseñas predeterminadas

Herramientas para la gestión de vulnerabilidades

- Nessus (www.tenable.com),
- Qualys (www.qualys.com),
- GFI Languard (www.gfi.com),
- Nikto (https://cirt.net),
- OpenVAS (www.openvas.org),
- Retina CS (www.beyondtrust.com).

Para tener en cuenta…



Modelado de amenazas

- El modelado de amenazas se trata de usar modelos para encontrar problemas de seguridad.
- Usar un modelo significa abstraer muchos detalles para proporcionar una visión más amplia, en lugar del código en sí.
- Modela porque le permite encontrar problemas en cosas que aún no ha creado, y porque le permite detectar un problema antes de que comience.
- Consta de cinco secciones:
  - Identificar objetivos de seguridad,
  - Descripción general de la aplicación
  - Descomponer aplicación
  - Identificar amenazas
  - Identificar vulnerabilidades.

Tipos de ataques

- Ataques al sistema operativo
- Ataques a nivel de aplicación
- Ataques de configuración incorrecta
- Ataques Shrink-wrap code

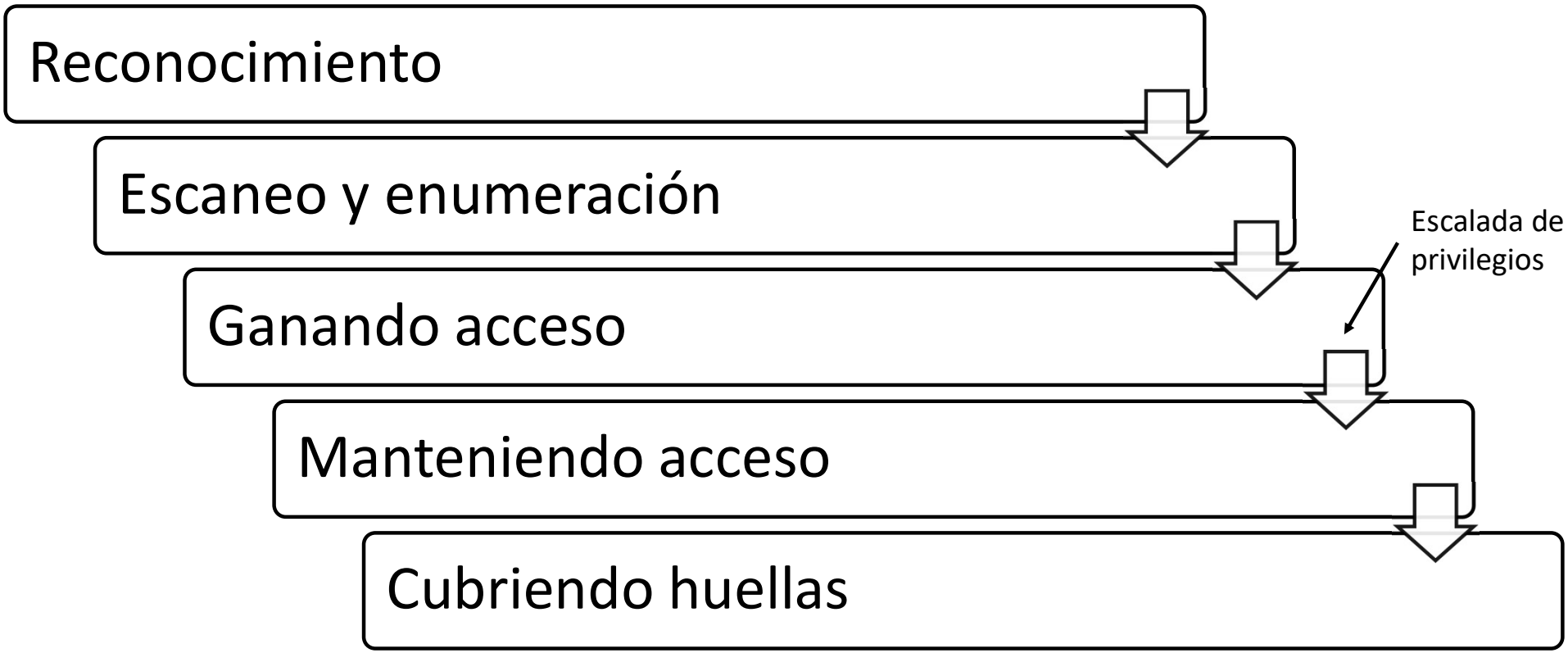
El hacker ético

- Un pirata informático ético es alguien que emplea las mismas herramientas y técnicas que un criminal puede utilizar, con el apoyo y la aprobación del cliente, para ayudar a proteger una red o sistema.
- Un cracker, también conocido como pirata informático malicioso, utiliza esas habilidades, herramientas y técnicas con fines personales o con fines destructivos o, en términos puramente técnicos, para lograr un objetivo ajeno al interés del propietario del sistema.
- Los hackers éticos son empleados por los clientes para mejorar la seguridad.
- Los crackers actúan por su cuenta o, en algunos casos, actúan como agentes contratados para destruir o dañar la reputación del gobierno o de la empresa.

Importante

- Un hacking ético solamente se realiza previa firma de un contrato de servicios con una organización que desea evaluar sus sistemas de seguridad.
- Incluso puede que el contrato incluya una clausula de no daño que prevenga la destrucción o modificación de archivos. Por lo que se llegue solamente a la segunda etapa.
- Probablemente tenga que firmar un NDA (Acuerdo de no divulgación).
- El realizar un hacking sin la autorización de la organización atacada, puede traerle graves consecuencias, ya que puede dañar o sabotear un sistema en producción (Revise ley 19223 sobre figuras penales relativas a la informática)

Fases del Hacking

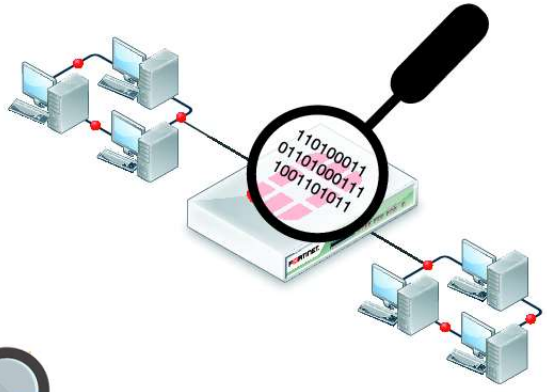


Reconocimiento

- Son los pasos tomados para recopilar evidencia e información sobre los objetivos que desea atacar.
- Se tienen dos tipos:
  - Activo
  - Pasivo

Reconocimiento pasivo

- Implica la recopilación de información sobre su objetivo sin su conocimiento.
- Por ejemplo:
  - Observar el exterior del edificio durante un par de días para conocer los hábitos de los empleados y ver qué medidas de seguridad física se aplican.
  - la ingeniería social
  - el buceo en basureros*
  - Sniffing de redes



Reconocimiento activo

- Utiliza herramientas y técnicas que pueden o no descubrirse, pero pone las actividades del hacker en mayor riesgo de descubrimiento.
- Por ejemplo:
  - Caminar hasta la entrada del edificio o la caseta de vigilancia e intentar abrir la puerta.

```
admin@ip-172-26-0-73:~$ nmap scanme.nmap.org

Starting Nmap 7.40 ( https://nmap.org ) at 2020-07-22 02:48 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.078s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 2.40 seconds
admin@ip-172-26-0-73:~$
```

Enunciado del laboratorio N°1

DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

Bibliografía

1. Walker, Matt. CEH Certified Ethical Hacker All-in-One Exam Guide, Fourth Edition. McGraw-Hill Education.