**Hacker informático:** introducirse en sistemas ajenos.

**Hacker ético - Pentester**

↪**PENTESTING:** penetrar el sistema

**FASES:**

1. **Reconocimiento (footprinting):** Conseguir la mayor cantidad de información del objetivo
   1. **Técnicas OSINT (Open Source Intelligence)**
      1. Empresa
         1. Búsqueda en Google (Página Web/Foros,redes sociales->DNS/Sitios Web/Personas,documentos->Ip's/Proveedores->Geolocalización/Emails,teléfonos,documentos
         2. Directorios de empresas -> Sede, datos de contacto,…
         3. Compra/venta de datos
         4. Programas de análisis
      2. **Intrusión física:** información de la empresa
      3. **Ingeniería social:** información de los empleados
      4. **Información de redes, direcciones IPs:** Escaneo
   2. **httrack** [**www.scanme.test**](http://www.scanme.test) **-o /home/admin/sitios/scanme**
   3. **wget-r www.scanme.test**
2. **Escaneo (scanning):** sistema operativo, red…
   1. Averiguar hosts activos, servicios, sistemas operativos, aplicaciones…
   2. Subfases:
      1. **Análisis de vulnerabilidades:** saber si esos programas/S.O. tienen vulnerabilidades de las que nos podamos aprovechar. (Hay BBDD en internet de muchísimas vulnerabilidades).
      2. **Enumeración:** mediante protocolos conseguir una lista de usuarios, recursos compartidos… (Ej: tiene una carpeta compartida voy a ver que tiene detrás…)
      3. **Protocolos:**
         1. ICMP: barrido ping: conexión (
         2. TCP/UDP: puertos abierto, cerrado, filtrado (firewall), no filtrado, mixto.
         3. TCP: orientado a conexión (3 way handshake) y confirmado
            1. Persona 1 - SYN: quiero hablar contigo
            2. Persona 2 - SYN+ACK: me ha llegado la petición y la acepto
            3. Persona3 - ACK: me ha llegado la confirmación que quieres hablar conmigo
            4. 6 flags: SYN, ACK, RST, FIN, URG, PSH
            5. Ejemplo: Halfscan→ACK→no se manda si quieres hacer un escaneo para evitar ser detectado (si se completa la comunicación - se registra).
      4. **Network Mapping: nmap [tipo\_escaneo] [opciones] [red/host] ->**
         1. VERSIÓN GRÁFICA: zenmap
         2. **[tipo\_escaneo]**
            1. **-sn (ping)**
            2. **-sU (udp)**
            3. **-sS (tcp half)->** envía la señal de sincronización
            4. **-sT (tcp full)->** funcionamiento normal del TCP
            5. **-sF (tcp fin)->** envía solo la señal de finalización
            6. **-sN (tcp null)->** envía un paquete tcp sin ningún flag activo
            7. **-sX (tcp xmas)->** activa las banderas que no son típicas (URG, PSH)
            8. **-sA (tcp ack)->** envía un mensaje a alguien que no le ha pedido nada.
         3. **[opciones]**
            1. **-v (info)**
            2. **-sV (servicios)**
            3. **-O (sistema operativo)**
            4. **-A (aplicaciones)**
            5. **-Tnº (temporizador, ej. -T4)**

1. **Conseguir acceso (exploit):** fallos de seguridad en el S.O. etc
   1. Hacker malo
      1. Mantener acceso, sacar información, “dañar”
      2. Borrar huellas
   2. Hacker ético
      1. Escribir un informe
      2. Presentar informe de auditoría de seguridad

**TIPOS:**

* Interno: te doy tarjeta de entrada, te creo un usuario dentro de la empresa…
* Externo: sin ninguna facilidad, desde fuera.

**MODALIDADES:**

* Black Box: ataque a ciegas, la empresa no te da nada.
* Grey Box: punto medio entre Black box y White box (parcial)
* White Box: la empresa te facilita datos como el mapa de red o te crea un usuario (facilitación de acceso).

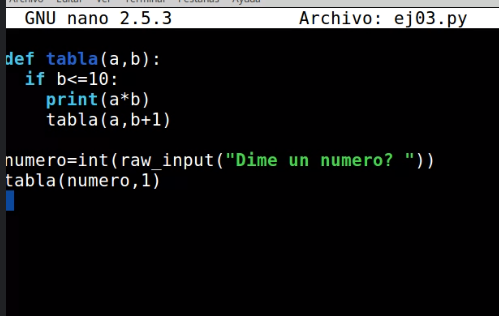
**SERVICIOS ADICIONALES:**

* Ingeniería social: obtener información confidencial a través de la manipulación de usuarios legítimos.
* Wardialing: técnica utilizada durante las décadas de los años 1980 y 1990, que consistía en hacer llamadas a una serie de números de teléfono automáticamente con el fin de encontrar módems conectados y permitiendo la conexión con algún otro ordenador.
* Seguridad física Información pública, nos intentamos hacer con la mayoría y luego filtrar esa información con una herramienta. Filtrar con bash y javascript

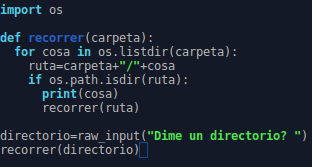
**Osint:** inteligencia de fuentes abiertas

# Python

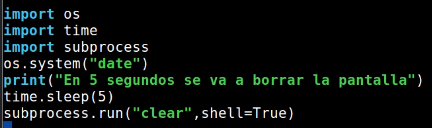
* #comentario
* “”” comentario de varias líneas”””
* **def** **nombre** (variables) ->definir función
* () los paréntesis por si quieres pasar datos
* : para decir que ahí empieza la función
* **print** es como el echo
* **raw\_input** para pedir por teclado
* **input** para versiones nuevas
* **int** para convertir números enteros
* **BUCLES:** llamada a función dentro de otra función, y terminar con un if.



* **import** -> incluir herramientas, ficheros, directorios, librerías
  + **funciones os (librería)**
    - **listdir() ->** para listar el contenido de una carpeta
    - **path.isdir() ->** saber si es un directorio



* + - **system() ->** nos permite ejecutar un comando
    - **otra librerías: subprocess.run ()->** funciona con la versión + actualizada. **Time**

****

*Ejecuta el comando date, luego sleep 5 segundos y borra pantalla.*

* + - **path.join:** para concatenar tanto en windows como en linux -> /linux, \windows
    - **otras librerías: endswith->** acaba en

