Actividad Práctica 2: Fundamentos de Python

HERRAMIENTAS PYTHON PARA HACKING

Hay muchas herramientas para hacking escritas en Python orientadas sobre todo al manejo de paquetes y protocolos de red. Algunas de las librerías Python son:

- **Scapy**
  Esta herramienta tiene dos funciones principales: enviar paquetes y recibir respuestas.
  Puede falsificar o decodificar paquetes de una variedad de protocolos, enviarlos, recibir respuestas, emparejar solicitudes con respuestas y devolver una lista de parejas de paquetes y una lista de paquetes no emparejados. Puede manejar fácilmente las tareas más comunes como el escaneo de la red, el descubrimiento de la red, el rastreo, los ataques, el sondeo, etc.
  Con esto podemos falsificar peticiones o respuestas para recoger información de la red.
  Las principales funciones básicas que deberemos conocer son:
  - ls() : listado de capas disponibles
  - explore() : interfaz gráfica para visualizar capas existentes
  - lsc() : funciones disponibles
  - help() : menú de ayuda.

  Y dentro del grupo de funciones, las más habituales son:
  - send(): envía paquetes a nivel 2.
  - sendp(): envía paquetes a nivel 3.
  - sr(): envía y recibe paquetes a nivel 3.
  - srp(): envía y recibe paquetes a nivel 2.
  - sr1(): envía y recibe solo el primer paquete a nivel 3.
  - srp1(): envía y recibe solo el primer paquete a nivel 2.
  - sniff(): sniffing de paquetes.
  - traceroute(): comando trace route.
  - arping(): Envío de solicitudes 'who-has' ARP para determinar que equipos están levantados en la red.
- **CRYPTOGRAPHY**
  Cryptography es un paquete que proporciona recetas criptográficas a los desarrolladores de Python. Esto incluye encriptación, hashing, generación de números aleatorios, firmas, así como cifrados por bloque y de flujo.
  El hacking ético hace uso de esta funcionalidad para cifrar y descifrar información sensible compartida en Internet.
- **Python-nmap**
  Python-nmap es una librería de Python que ayuda a utilizar el escáner de puertos Nmap. Nmap es una herramienta de administración de redes y auditoría de seguridad. Normalmente se utiliza para descubrir hosts y servicios disponibles en una red, aunque también puede utilizarse para examinar un único host.
  La librería python-nmap sirve como una wrapper de Python para la herramienta Nmap permitiendo acceder, usar y manipular fácilmente las características y funcionalidades de Nmap. La librería no sustituye a la herramienta Nmap, sino que sólo proporciona una interfaz para interactuar con Nmap.
  Ofrece un rico conjunto de características para el escaneo de puertos, el descubrimiento de hosts y TCP/IP fingerprinting (huella digital). Esta librería es una herramienta perfecta para hackers y administradores de sistemas que quieran automatizar las tareas de escaneo de la red y los informes.

GLOSARIO:

Modelo OSI:

El modelo OSI proporciona a los diferentes sistemas informáticos un estándar para comunicarse entre sí.

El modelo OSI se puede entender como un lenguaje universal de comunicación entre sistemas de redes informáticas que consiste en dividir un sistema de comunicación en siete capas abstractas, apiladas en vertical.

Nivel 2:

La capa de enlace de datos (Nivel 2 modelo OSI) se ocupa del direccionamiento físico, de la topología de la red, del acceso a la red (MAC), de la distribución ordenada de tramas y opcionalmente del control del flujo, de la notificación de errores y de la calidad del servicio.

Los concentradores (hubs) actúan exclusivamente a nivel físico (Nivel 1 modelo OSI) y, entre otras cosas, no controlan las colisiones; mientras que los conmutadores (switches) actúan a nivel de enlace, por lo que son capaces de gestionar los paquetes dentro de la red y mandarlos solo a la IP que los solicita.

Nivel 3:

El cometido de la capa de red (Nivel 3 modelo OSI) es hacer que los datos lleguen desde el origen al destino, aun cuando ambos no estén conectados directamente. Para ello se basan en dos aspectos: el direccionamiento y el encaminamiento (utilizando encaminadores (routers), a veces llamados enrutadores).

Adicionalmente la capa de red debe gestionar la congestión de red.

Sniffin:

Es una técnica de hacking que consiste en recopilar todos los datos que pasan por una red. Los programas que está hecho para hacer sniffin se llaman **Sniffers**.

Hasing:

Un hash es el resultado de una función hash, la cual es una operación criptográfica matemática que genera identificadores únicos e irrepetibles a partir de una información dada.

Fingerprinting:

El fingerprinting o la huella digital es toda aquella información sistemática que dejamos sobre un dispositivo informático cada vez que lo utilizamos.

Los datos obtenidos permiten determinar de manera inequívoca el dispositivo empleado y, de esta forma, poder llegar a perfilar y conocer la actividad del usuario, ya sea una persona física o jurídica