2021

Ataques y contramedidas

FRANCISCO JAVIER LÓPEZ CALDERÓN

UT 7. Amenazas, Ataques y fraudes en SI

P7.1 – Footprinting: Hacking con buscadores hacer 1 -2 - 3

Objetivo

Utilizar técnicas de **footprinting** para obtener información y analizarla posteriormente.

Consideraciones previas

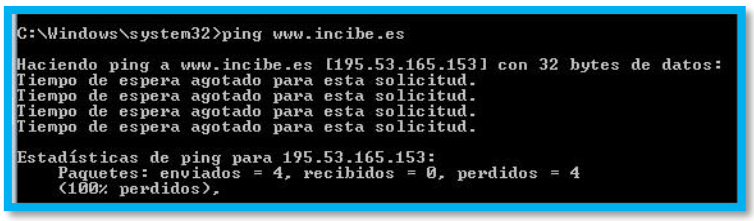
Footprinting es una **técnica legal**, con la que se trata de obtener toda la información posible, del sistema, de la red o usuario objetivo. Para ello nos podemos ayudar de toda la información pública que existe, acudiendo a documentos que tienen metadatos, a las redes sociales, medios de comunicación, etc... Esta recogida de información últimamente se conoce como OSINT (Open Source Intelligence), esto es básico para ingeniería social.

Para buscar información podemos

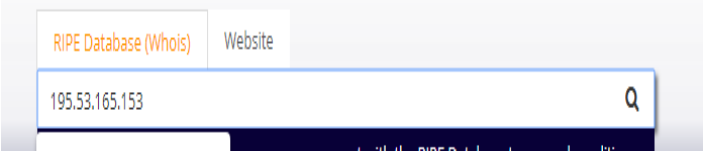
- Usar los buscadores, haciendo búsquedas avanzada en Google (Google hacking) o utilizando Shodan que es un buscador más específico.
- Utilizar herramientas para buscar metadatos, puedes mirar Foca.
- Obtener la información a partir de un dominio, una página que ayuda es dnsstuff.
- APIs de redes sociales, que permiten automatizar la recogida.

Ejercicio 1-----Analizar datos utilizando las siguientes webs

1. Realizamos un ping : www.incibe.es



2. Por ejemplo: si hemos obtenido su dirección: 195.53.165.153:
3. Utilizamos la web ripe.net y ponemos la ip obtenida



4. Ripe Database Query y obtenemos resultados como, por ejemplo:

5. Registrarse en https://www.shodan.io/ . Ponemos la Ip de la red y buscamos más información

Que conclusión sacamos?

El servidor se encuentra en España y pertenece a “Telefónica de España”
Este tipo de páginas, nos muestra información útil sobre las direcciones IP seleccionadas

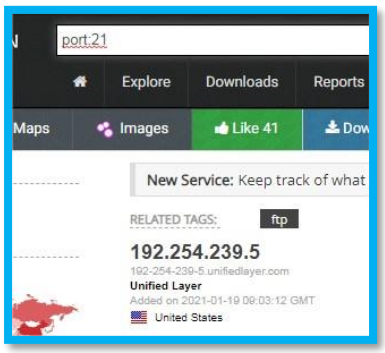
Ejercicio2----Google Hacking

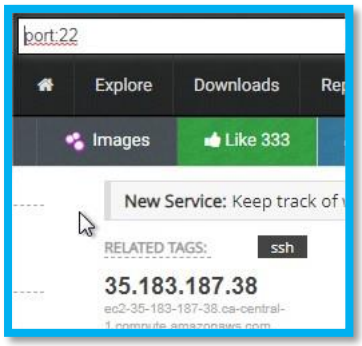
Shodan es un motor de búsqueda que le permite al usuario encontrar routers, servidores, … conectados a Internet a través de una variedad de filtros. Sus rastreadores monitorizan las cabeceras HTTP, FTP, SSH y otros protocolos mostrando información que otros buscadores no muestran.

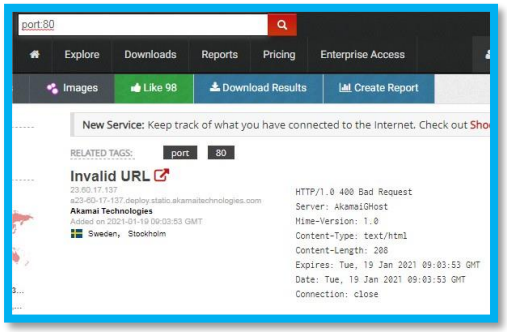
Permite utilizar los siguientes filtros:

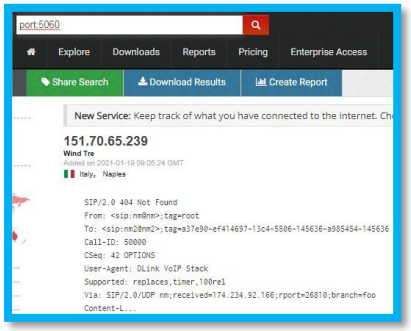
- **city**: búsquedas basadas en una localización
- **country**: búsquedas basadas en un país
- **geo**: búsquedas basadas en coordenadas
- **hostname**: búsquedas basadas en nombres
- **net**: búsquedas basadas en IPs
- **os**: búsquedas basadas en sistemas operativos
- **port**: búsquedas basadas en puertos abiertos
- **before/after**: búsquedas basadas en condiciones temporales

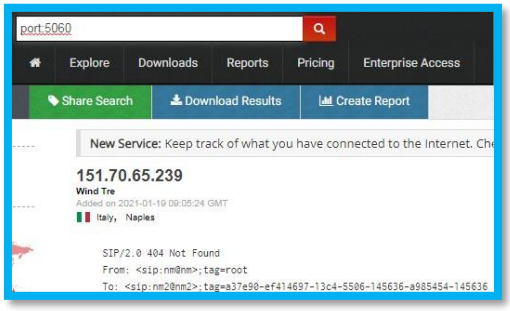
1. Registrarse en https://www.shodan.io/ para acceder a las funciones disponibles.
2. Busca servidores que escuchen en puertos 21(FTP), 22(SSH), 80(HTTP), 161(SNMP) y 5060 (SIP).



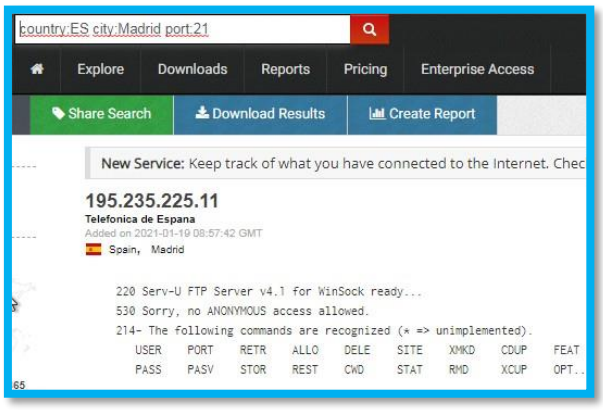






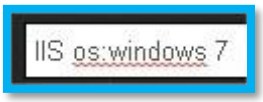


3. Busca servidores FTP en Madrid

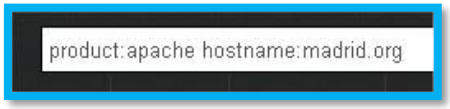


4. Busca servidores web con apache en España

5. Busca servidores IIS7 que corran en Windows



6. Busca servidores apache el dominio madridorg



7. Busca equipos en subred 216.219.0.0/16

8. Buscar servidores apache en subred 216.219.0.0/16

9. Busca puntos de acceso en España

10. Busca cámaras web D-link en China