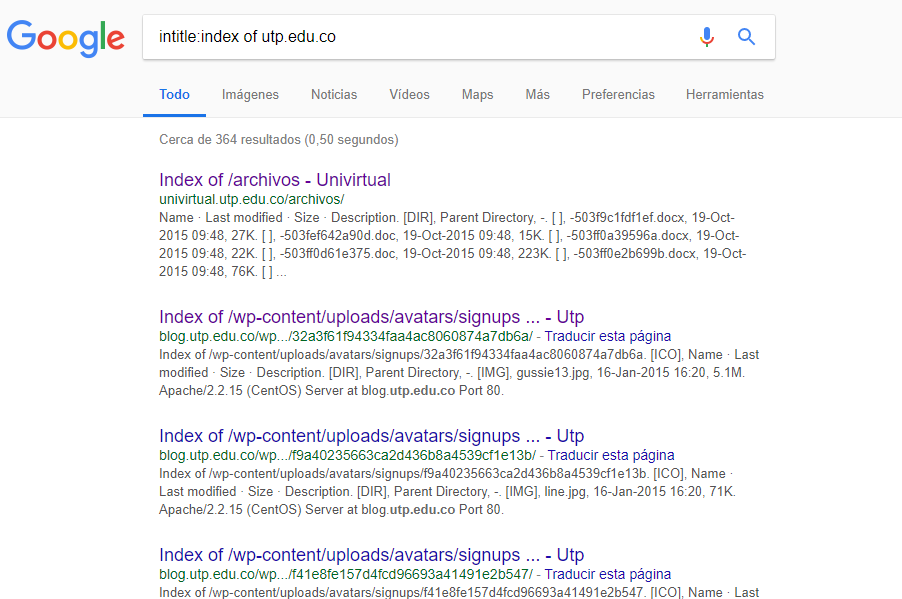
Parcial II

Nombre: Andres Felipe Farfan Hernandez Identificación: 1112779195

Nombre: Mauricio Granada Identificación: 1112768877

1 Búsquedas en Google

Se busca en Google por medio de intitle:index of domino //utp.edu.co



Se encuentra varias opciones donde vamos a escoger una



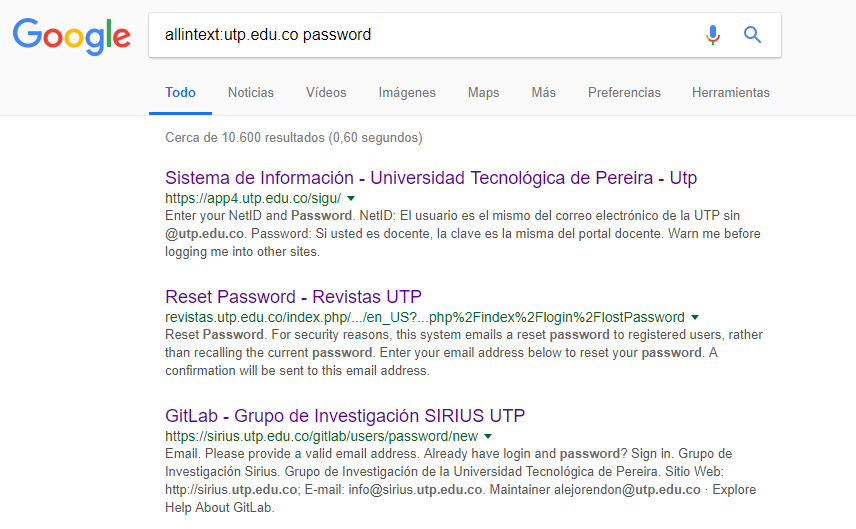
Se observa que se encuentra varios archivos, el cual se pueden ingresar y manipular la información.

Se utiliza la indicación site: utp.edu.co es filetype:pdf

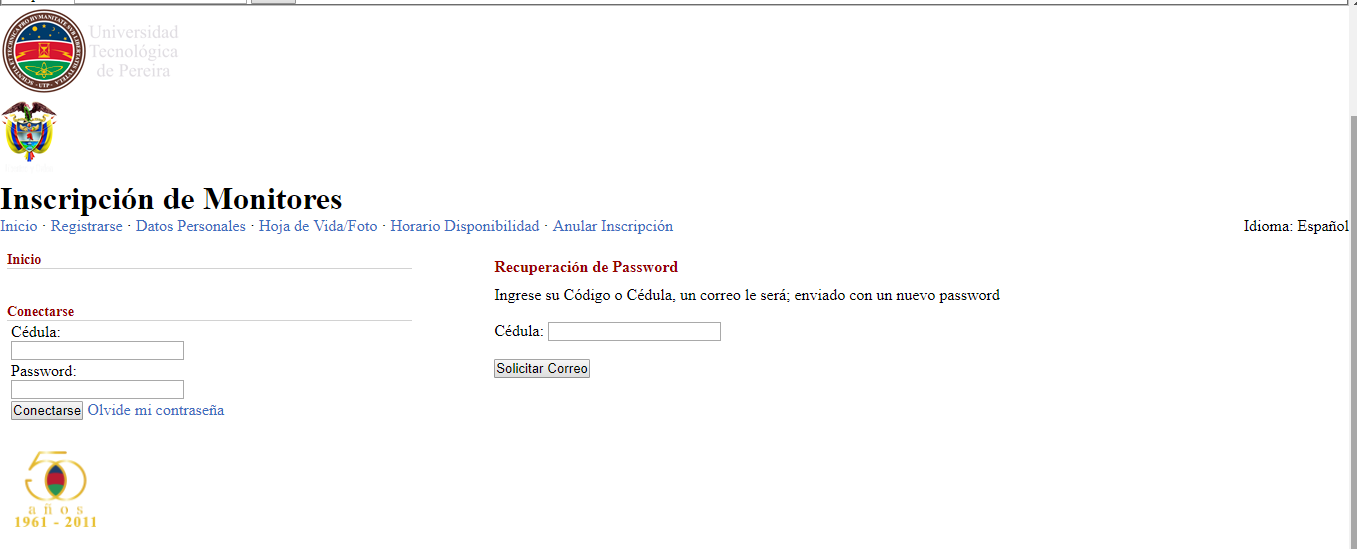


Se encuentra archivos con la extensión pdf

Se utiliza la instrucción allintext:utp.edu.co password

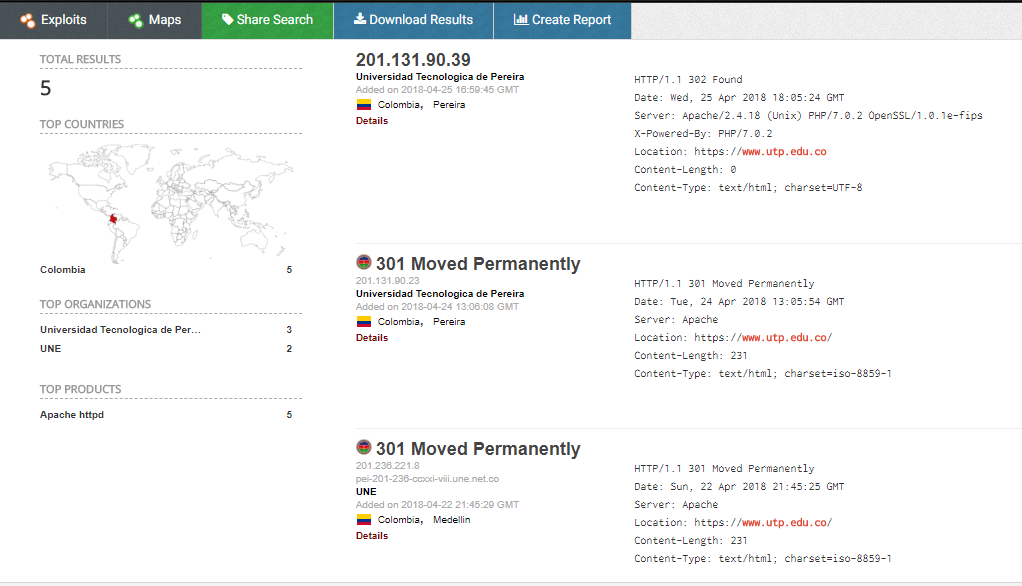


Donde abre páginas de autenticación y que solicite password



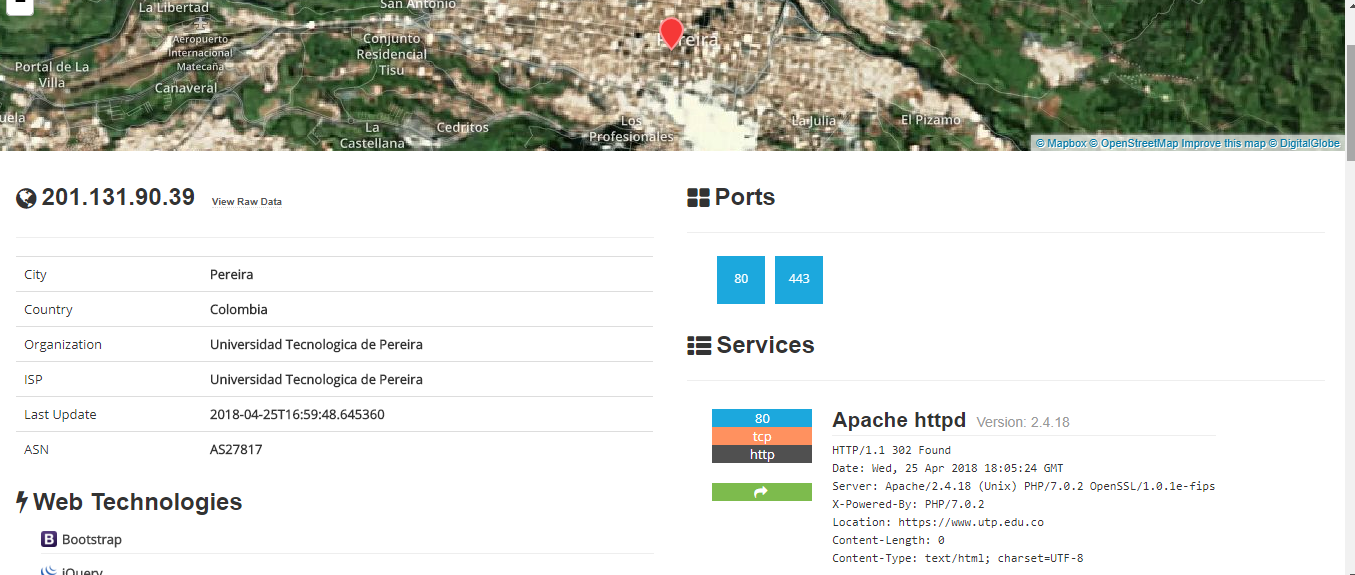
Conclusión: Este tipo de búsquedas permite observar archivos que para una compañía no son de uso público, adicional de la información que no es pública.

2 Se utiliza la pagina shodan.io , y se busca el dominio utp.edu.co



Encontramos que hay 5 resultados donde 3 son de la utp y 2 de UNE

Se observa que de las 5 encontradas el servidor es apache

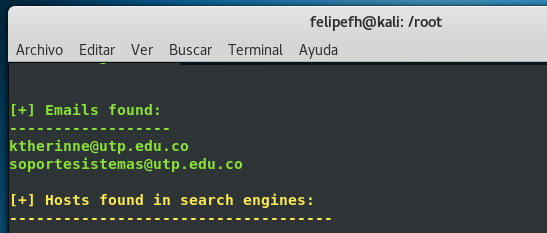


Se encuentra que los puertos utilizados son el 80 y 443

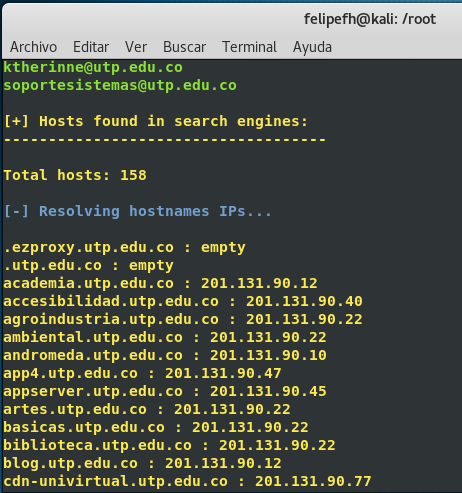
Conclusión: Se encuentra una herramienta que me permite saber que tipo de servidor manejan las compañías o instituciones, el cual puede ser grave, debido a que si no se actualiza, personas maliciosas pueden atacar un servidor o manipular.

3

1. Correos encontrados

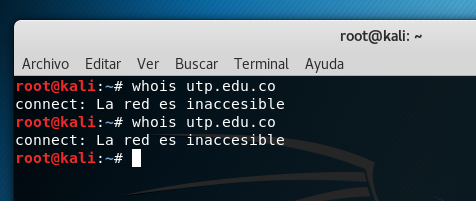


1. Subdominios

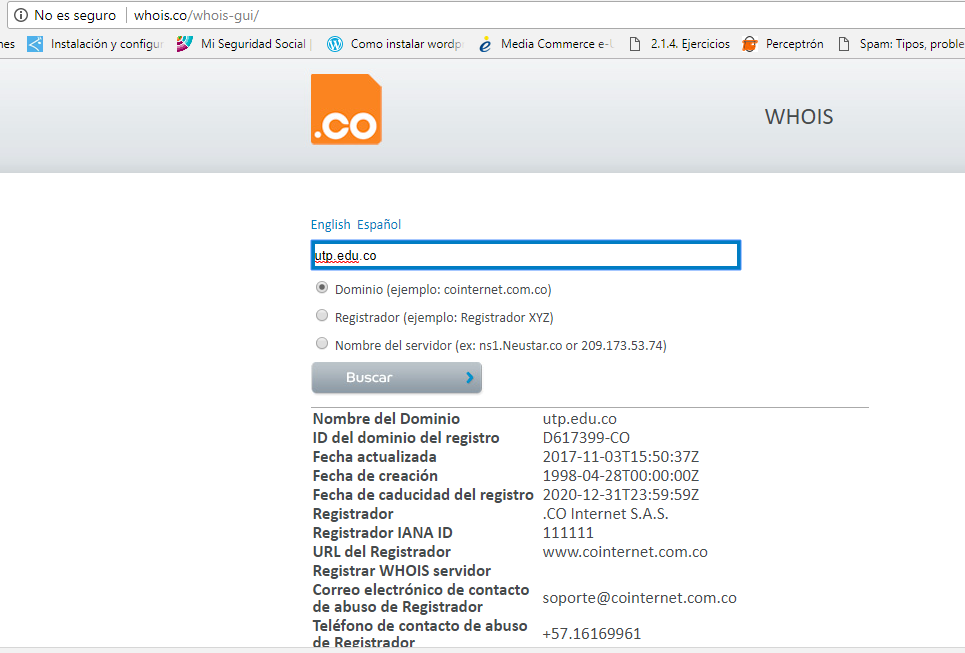


Conclusión: Se observa que se encuentran pocos correos, ya que pueden tener una buena seguridad frente a quien accede a ellos, se verifica los subdominios, el cual también se observa su ip publica, puede que alguno de ellos este vulnerable.

4 whois



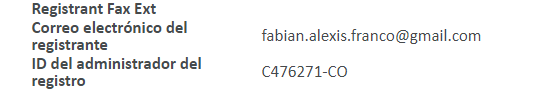
Por medio de Kali no lo resuelve, se procede a verificar por web, el cual se observa que se puede



Registrante



Correo

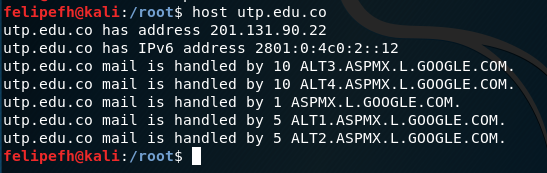


Ubicación



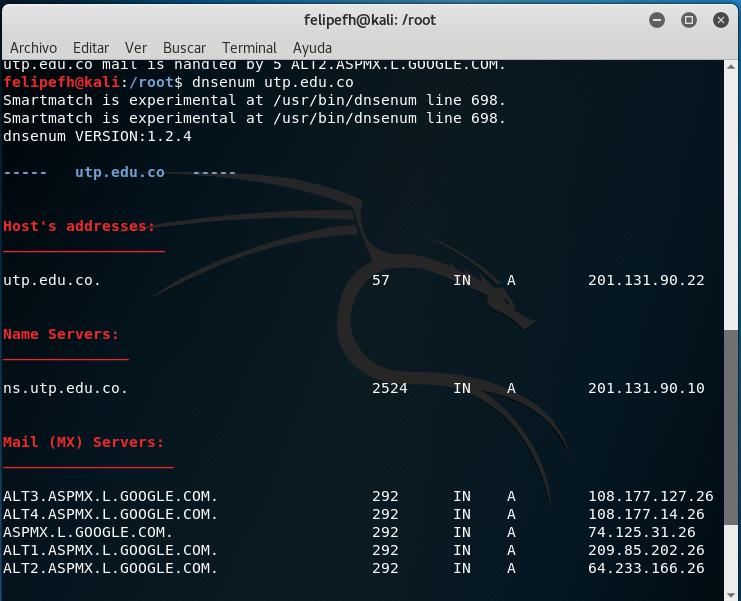
Conclusión: Se observa que se tiene muchos datos que no pueden aparecer, ya que son datos personales o privados.

5 Host



Conclusión: Se observa que tenemos la ip publica, la ip versión 6, y los dominios de correo que son de Google.

6 dnsenum



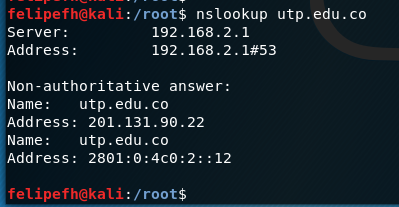
Conclusión: se encuentra con el dominio cpn su respectivo servidor dns, también los dominios de correos con sus direcciones ip de los dns, y también los puertos que utilizan.

7 dnsmap



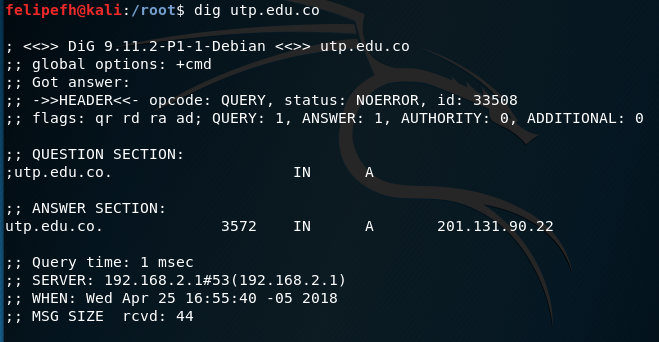
Conclusión: Se demora demasiado, ya que es un ataque de fuerza bruta

8 nslookup



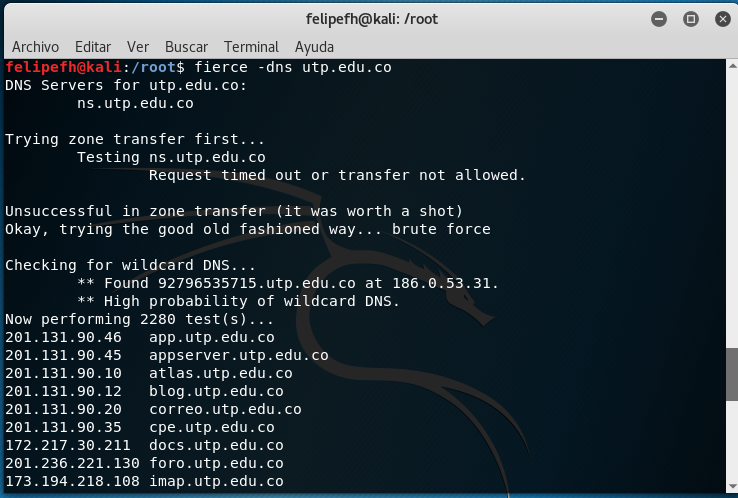
Conclusión: Son las direcciones el cual se resuelve con el servidor dns, también aparece las direcciones ip del dominio y también ipv6.

9 dig



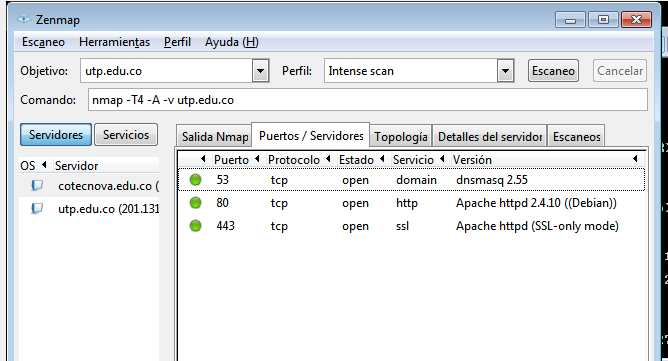
conclusión: Se observa consultas hacia las direcciones DNS, encontrando puertos y el servidor.

10 fierce



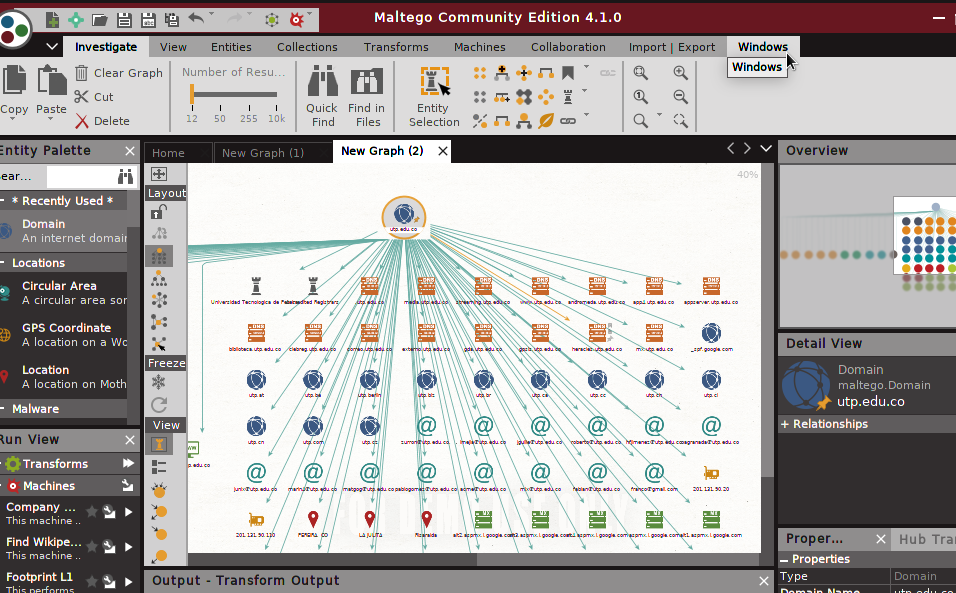
conclusión: Se observa son las ip continuas, o los subdominios del dominio principal.

11 puertos nmap



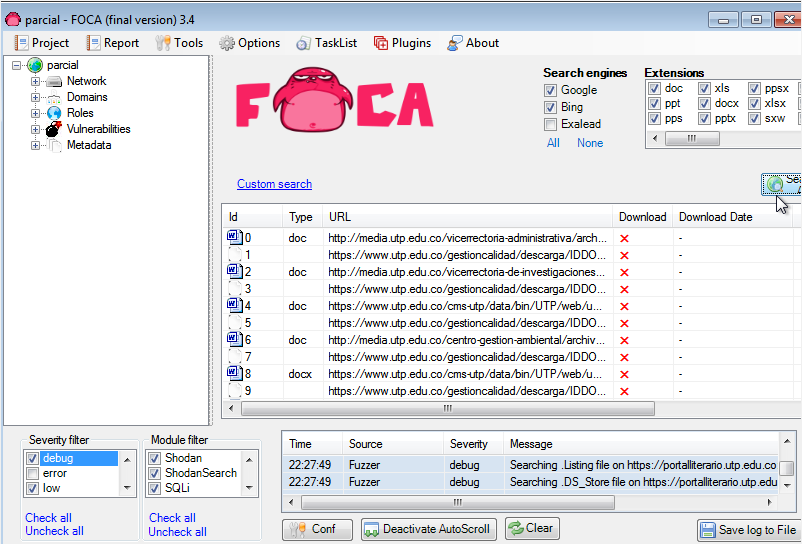
conclusión: Se encuentra 3 puertos activos, el cual corre servicios de apache y servidor mascara dns

13 maltego



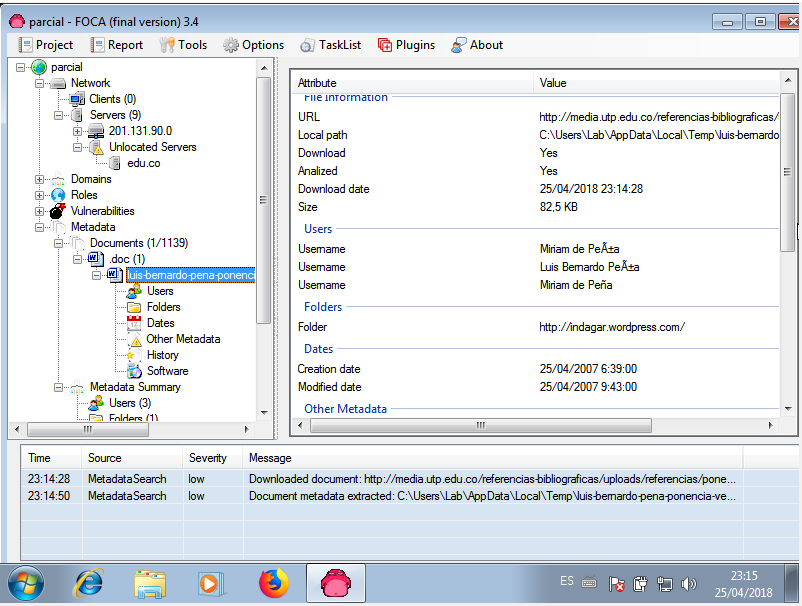
conclusión: Se observa los subdominios y personas

14 foca

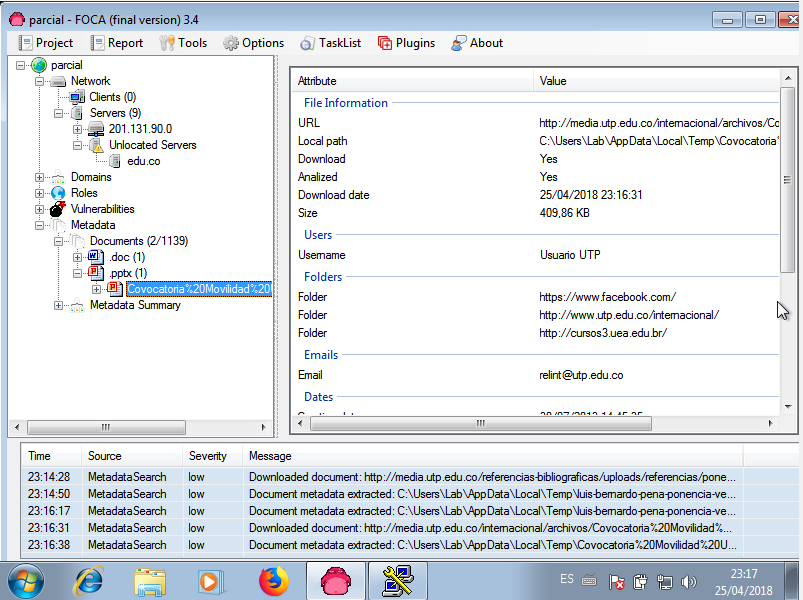


Se analiza el dominio utp.edu.co en foca

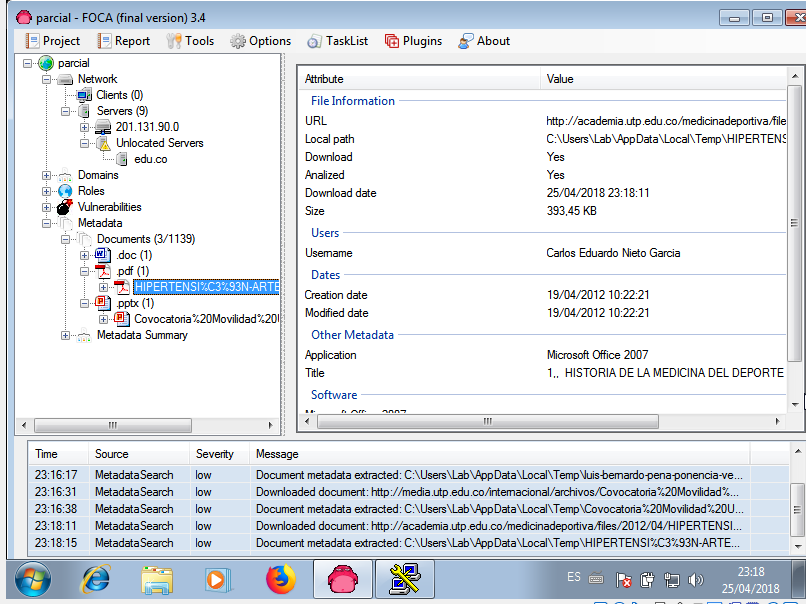
1 archivo



2 archivo

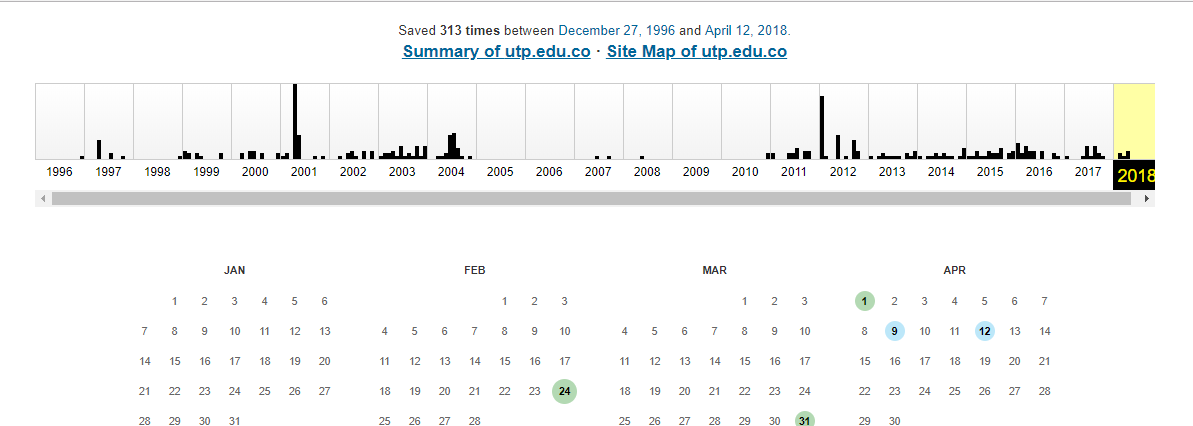


3 archivo

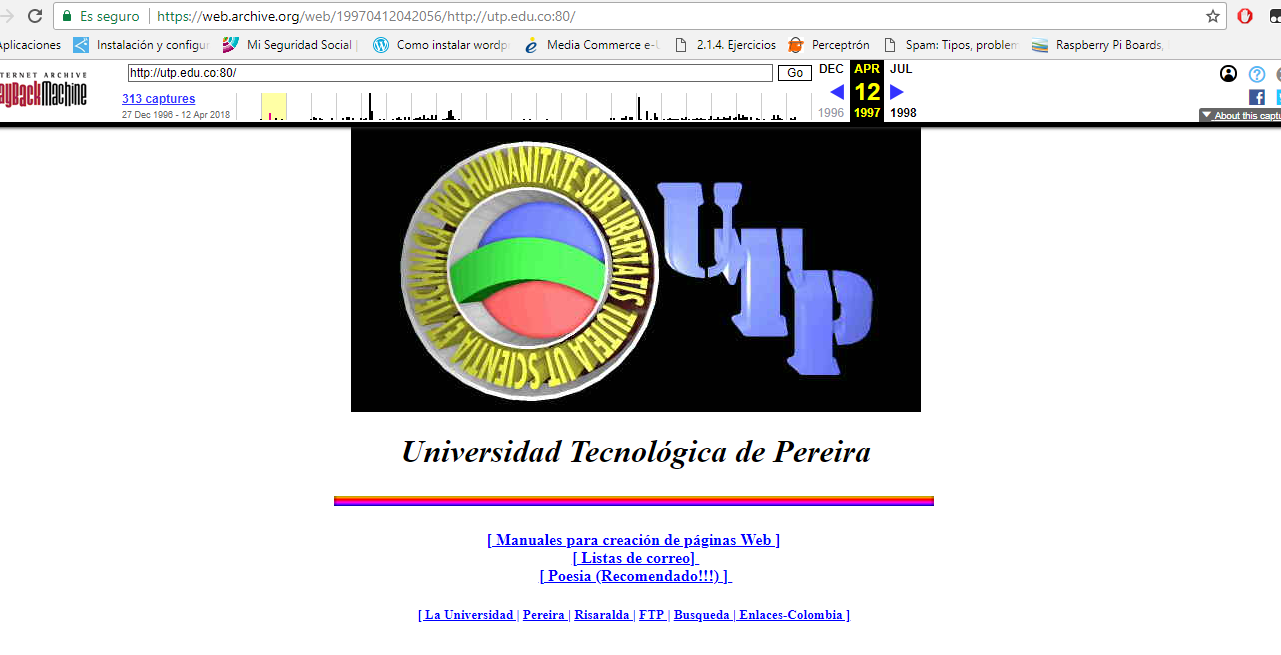


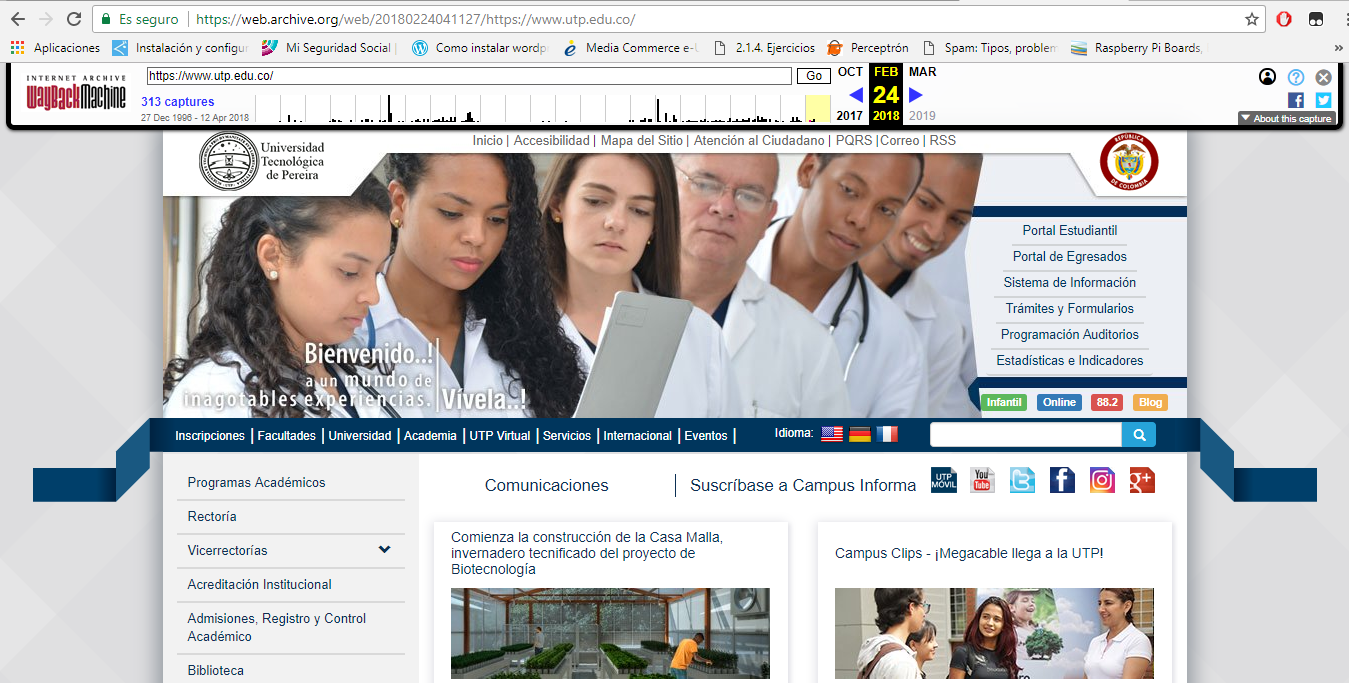
Conclusión: Se observa que hay mucha cantidad de información que consiguió solo con el dominio, 1139 archivos, pero para deducir cual es valiosa es lo complicado, pero se utilizaron 3 diferente tipo de archivos, donde se observa las url, también el directorio de donde saco el archivo, el nombre de usuario, fecha de creación y hora, mucha información que es privada.

15 archive.org



Se observa en orden cronológico

la pagina de la utp en 1997

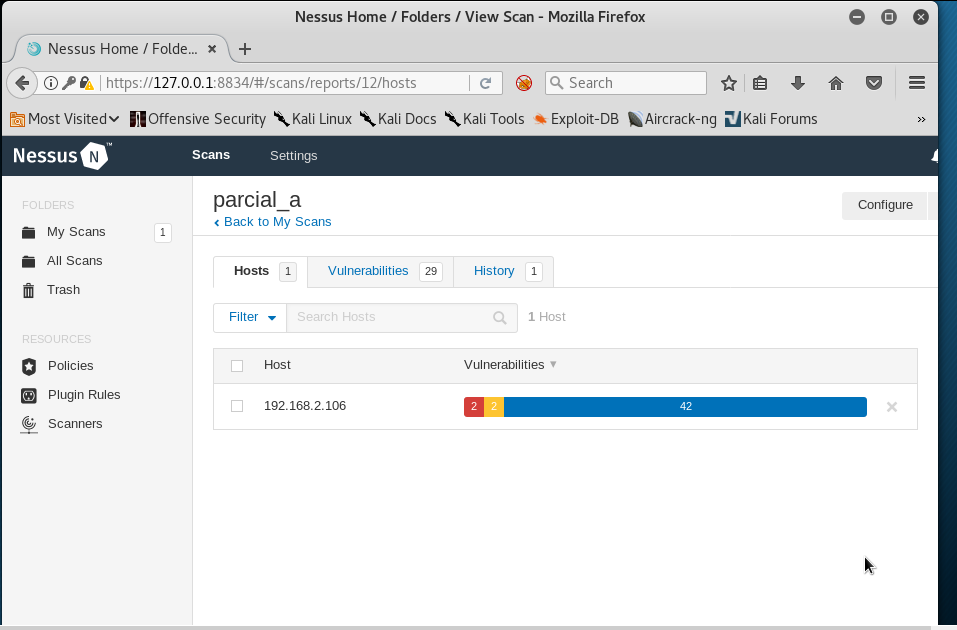


Pagina utp en el 2018

Conclusión: Se observan los cambios en orden cronológico, detallando una mejoría al pasar del tiempo, por medio de la herramienta se puede detectar errores y vulnerabilidades.

16. Nessus

Escaneo básico

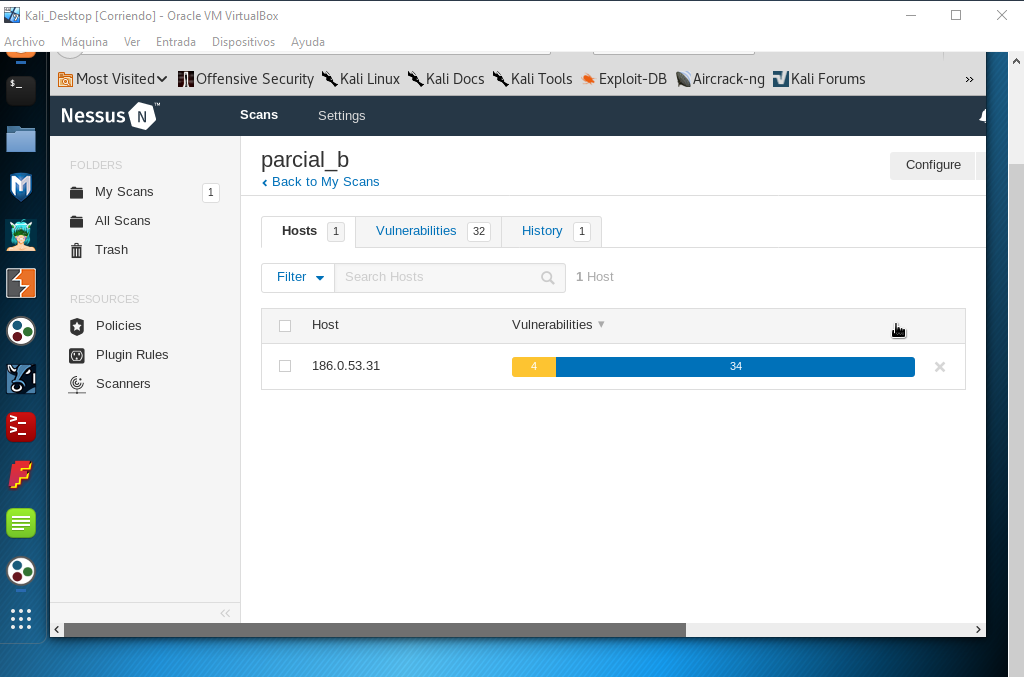


Se realiza escaneo a una ip de la red local, el cual es la máquina virtual de Windows

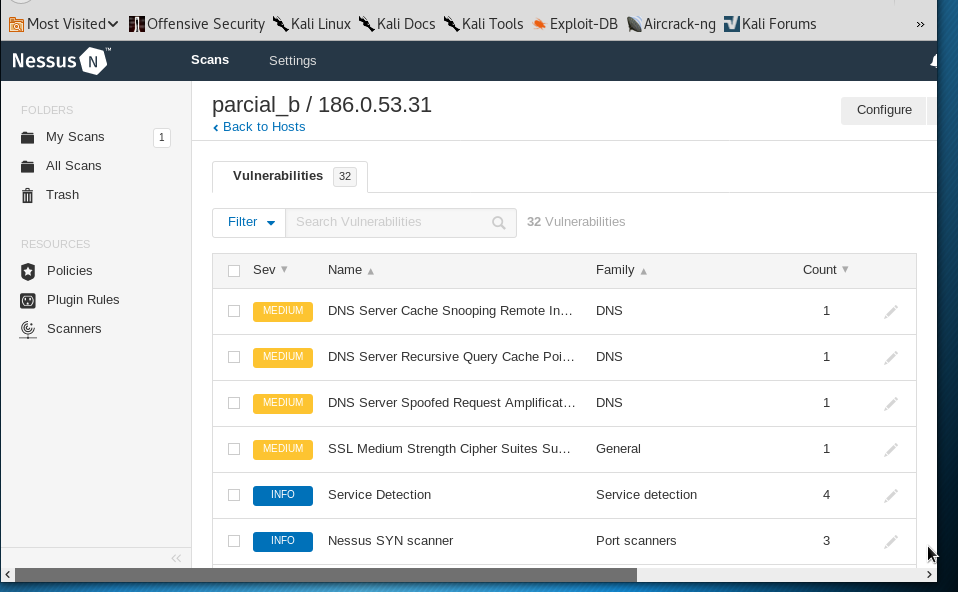


Conclusión: Se observa 2 vulnerabilidades a nivel crítico, y otras 2 a nivel medio, en el cual por ese medio pueden atacar fácilmente sin ser detectados.

Escaneo Avanzado



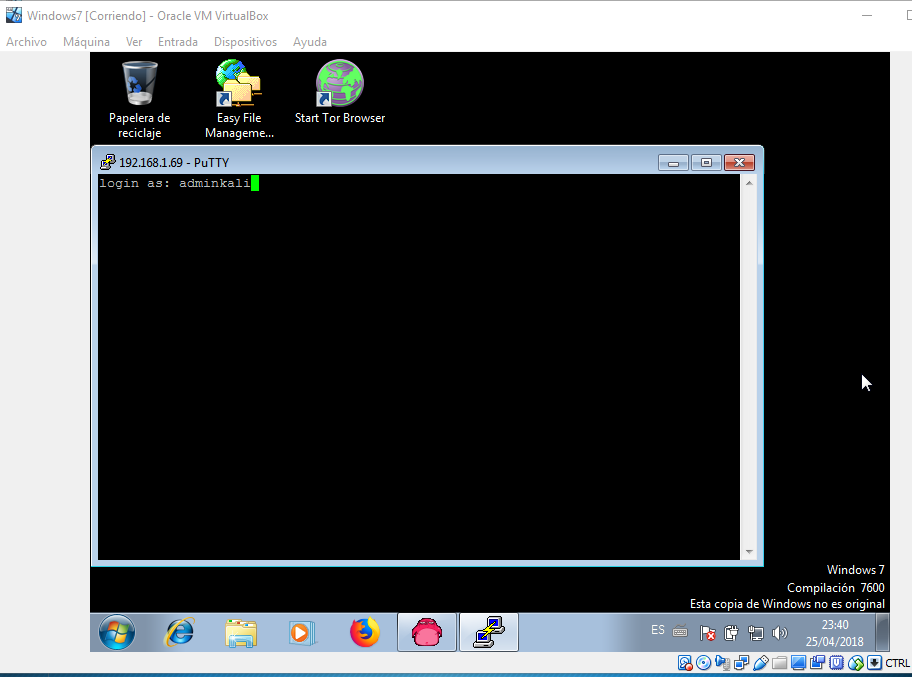
Se escanea una ip publica, la del dominio de cotecnova.edu.co.

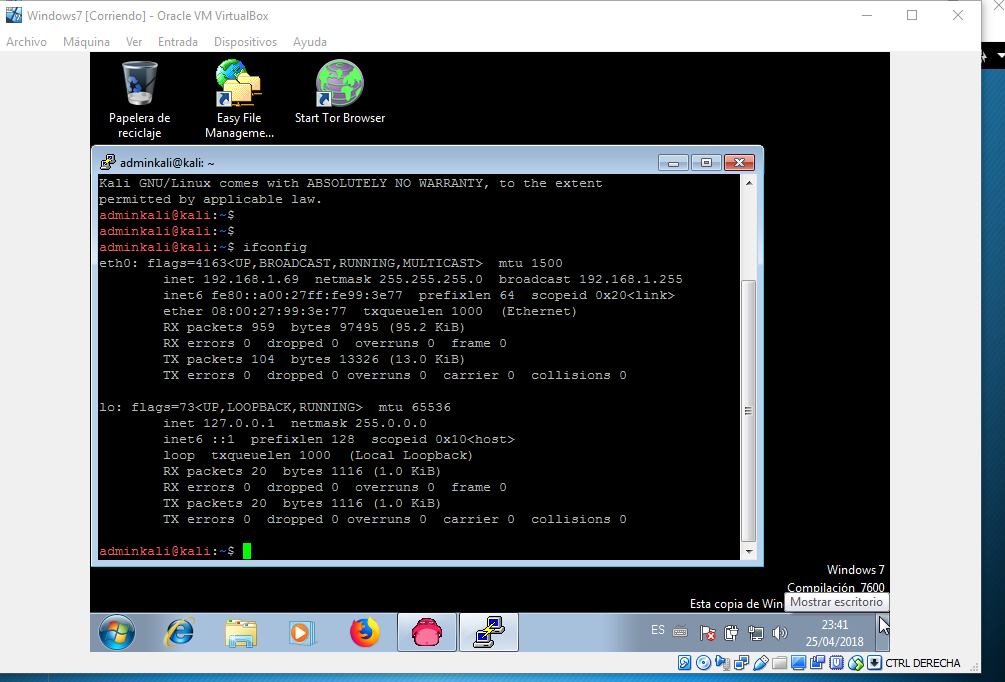


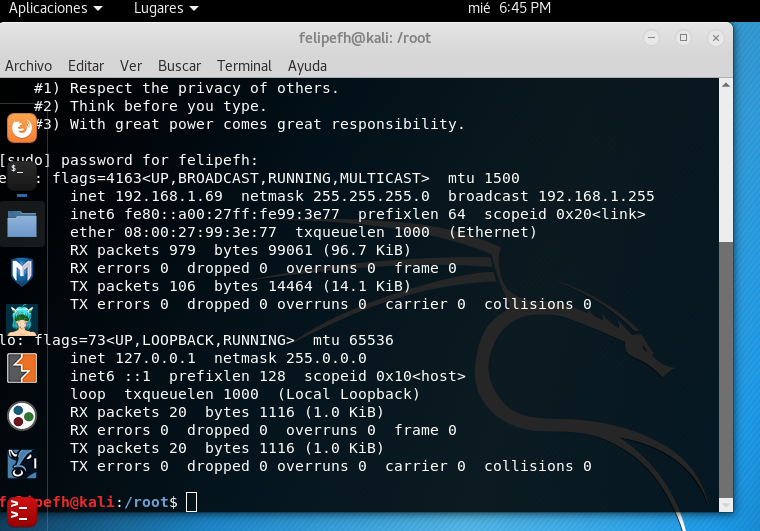
Se observa que hay 4 vulnerabilidades a nivel medio, se puede mitigar, siendo este tipo de direcciones mucho más protegidas, en conclusión las ip de host son mas vulnerables que las ip de los servidores.

17 Anonimato

Tunel



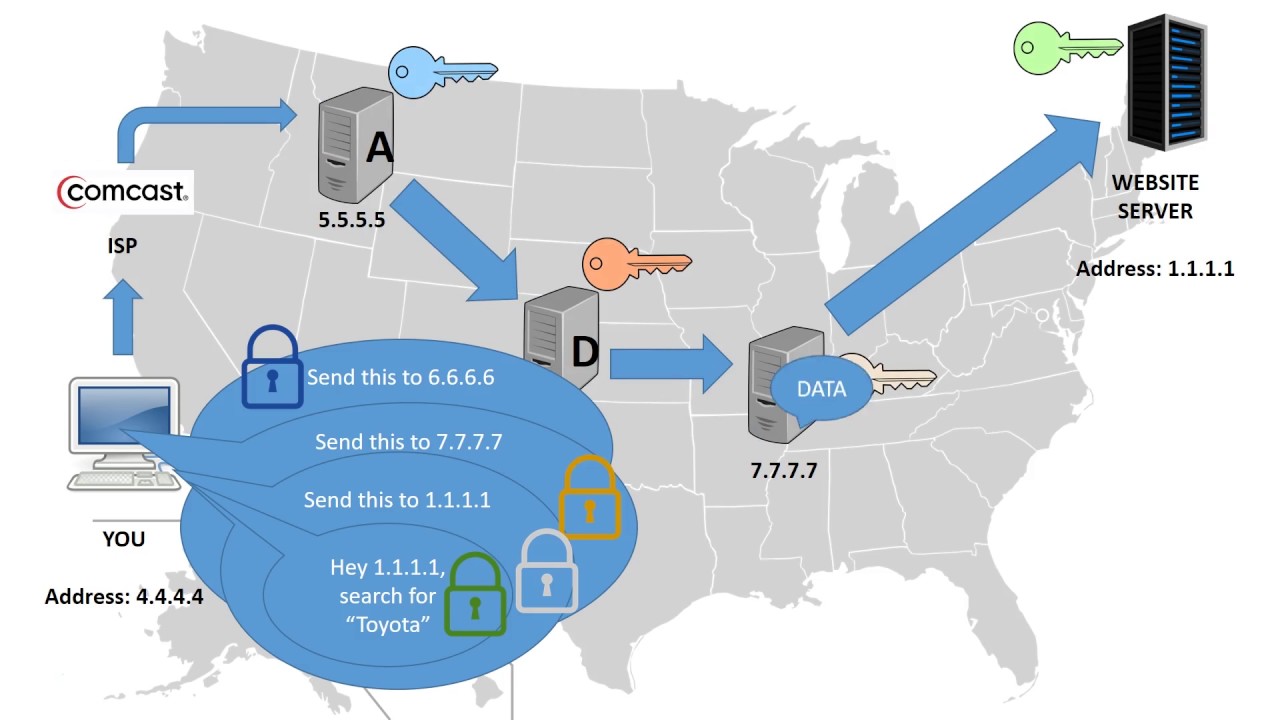




Se observa que es la misma ip la que esta en Kali y la que esta en putty

18. Cuando es necesario usar anonimato y cuando no, grafique un sistema de anonimato ideal.

El anonimato se puede usar si no se van hacer cosas graves se puede utilizar para dar puntos de opinión sobre temas políticos o publicar en blog sobre temas que no está de acuerdo con la empresa y no quiere que el jefe se dé cuenta, no se debe hacer para dar amenazas, chantajes, insultos o robos.



20. Defina con sus propias palabras

a. Obtención de Información

Consiste en adquirir datos almacenados en cualquier fuente.

b. Enumeración de sistemas

Es una agrupación de elementos que representan alguna información.

c. análisis de Vulnerabilidad

Es el proceso por el cual se puede identificar como puede ser atacado un sistema y que tan expuesta esta su información a un ataque de terceros.

d. Explotación de Vulnerabilidad

Se hace mediante un programa para atacar alguna vulnerabilidad puede ser de una base de datos y así poder sacar todos los registros.

e. Post-explotación de vulnerabilidad

Con esto se tienen en cuenta que vulnerabilidades pueden haber y poder corregirlas y así evitar futuros ataques al sistema o base de datos.