**PARCIAL II**

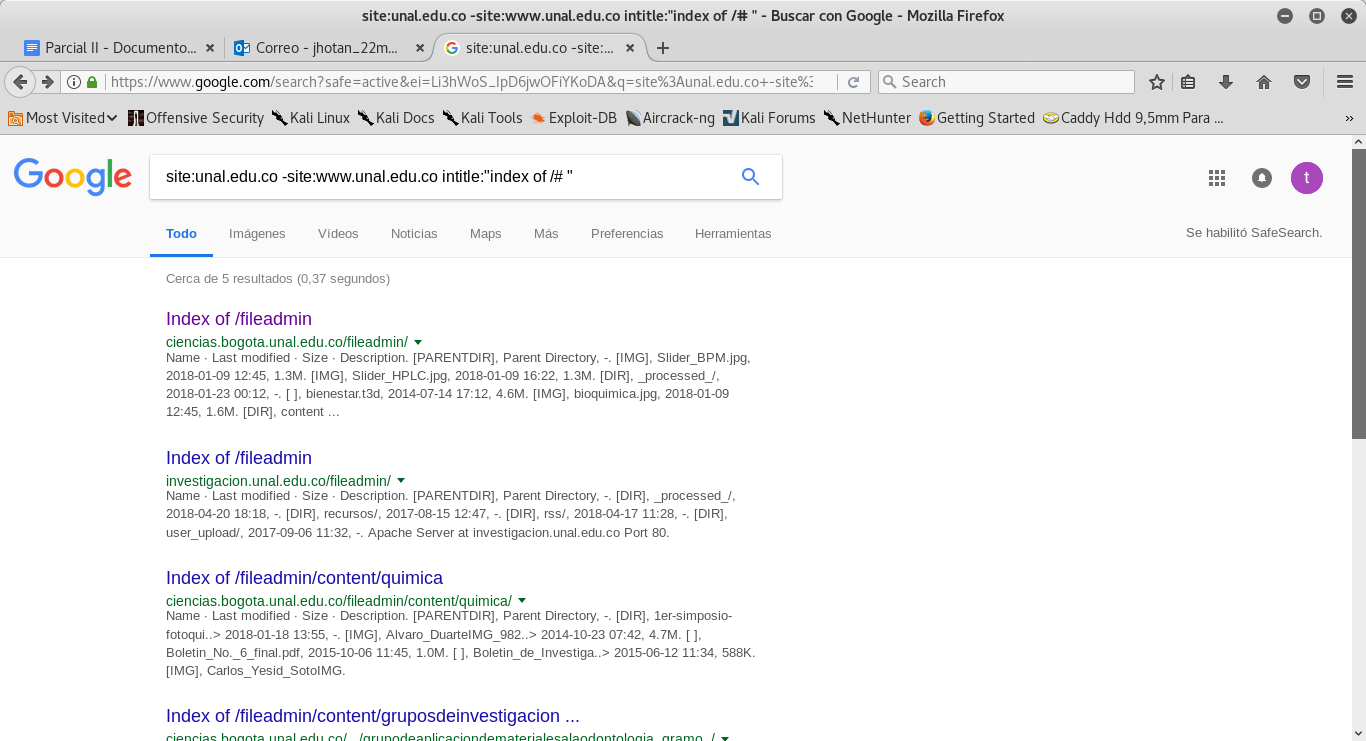
**ASIGNATURA: SEGURIDAD EN SISTEMAS DE INFORMACIÓN**

25 de abril de 2018

Nombre: Natalia Isaza Serrano 1.112.789.882

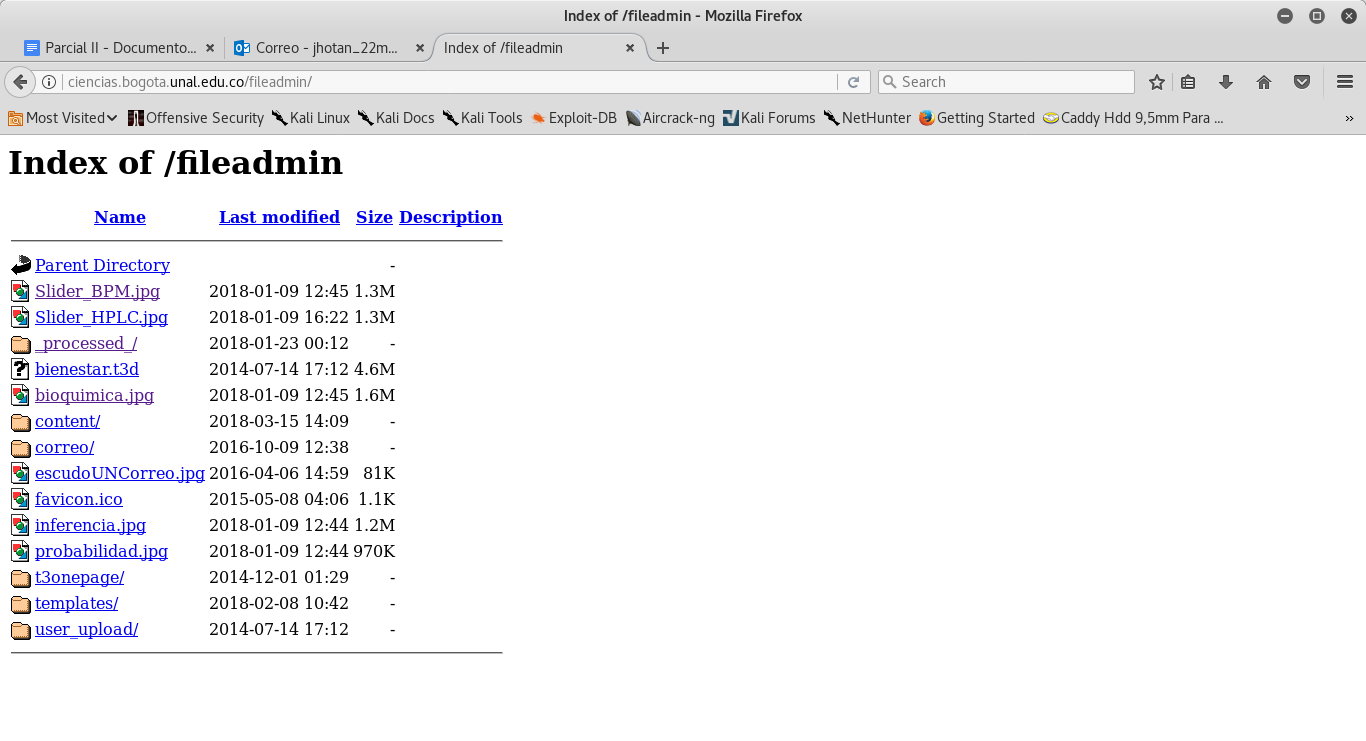
Nombre: Jhonattan Leandro Bedoya 1.112.770.718

1.



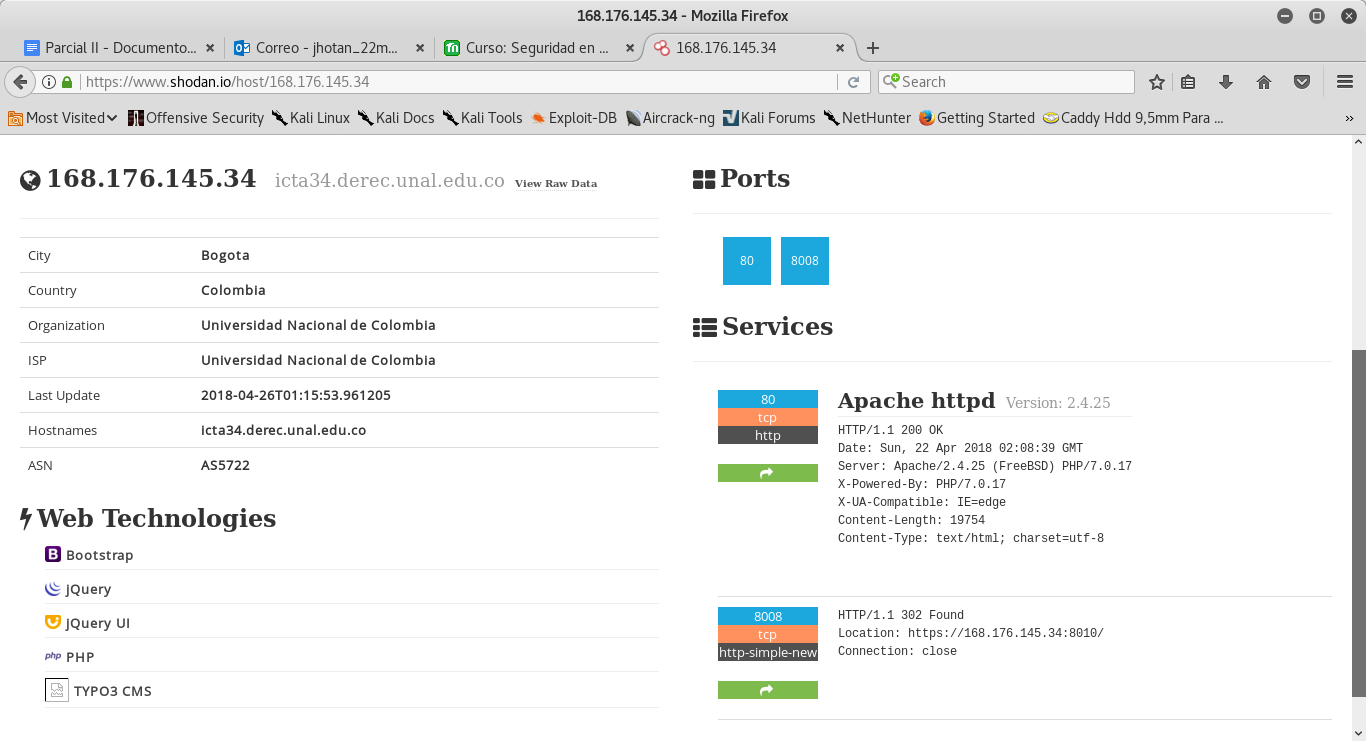
bb

b.

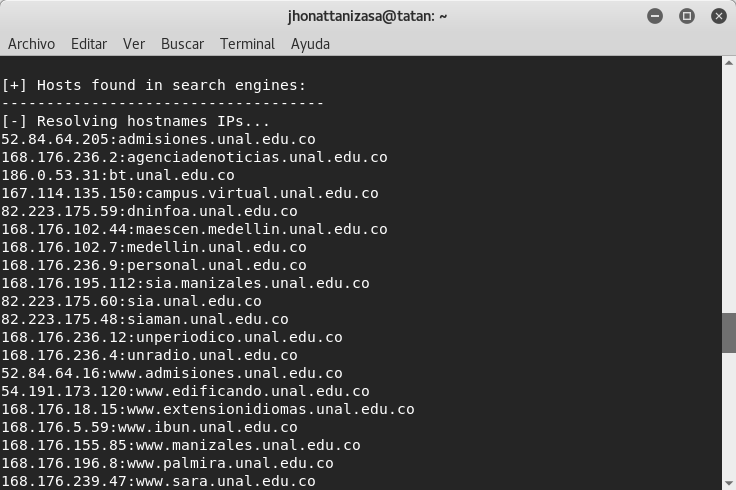


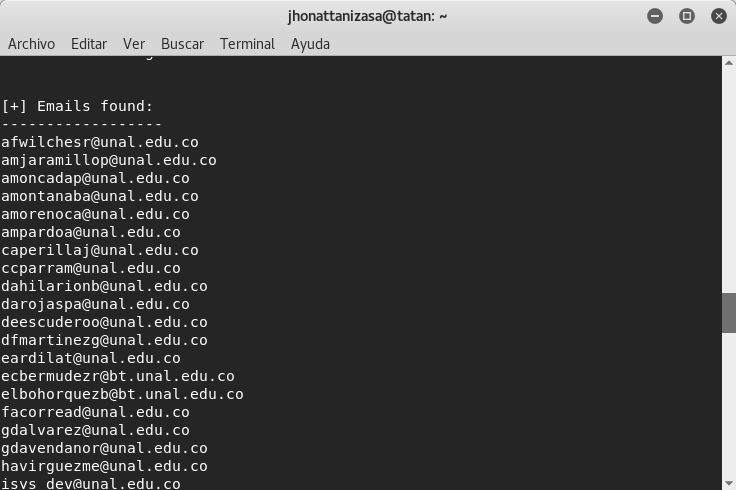
**Conclusión:** Podemos ver que la pagina que hemos visualizado en el navegador se obtiene una vulnerabilidad en el index, lo cual ocasiona que el lugar se puede extraer o verificar documentación.

2.

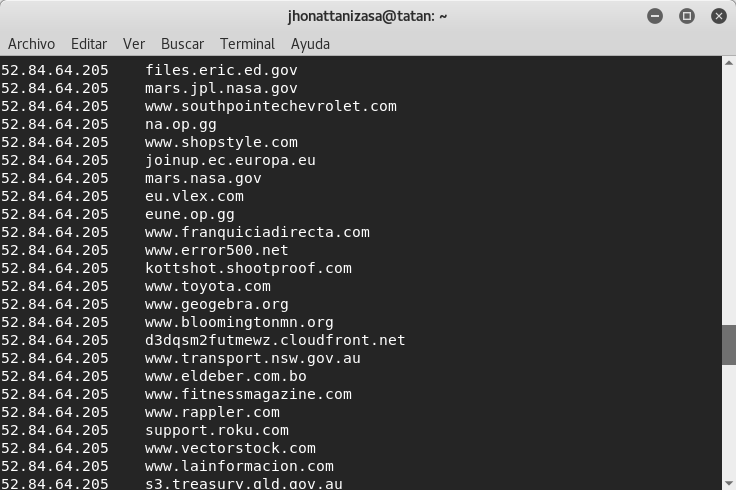


**Conclusión :**  con shodan podemos observar que nos dan información como los puertos, información personal, servicios y plataformas utilizados de este dominio.

3. a.

b. 

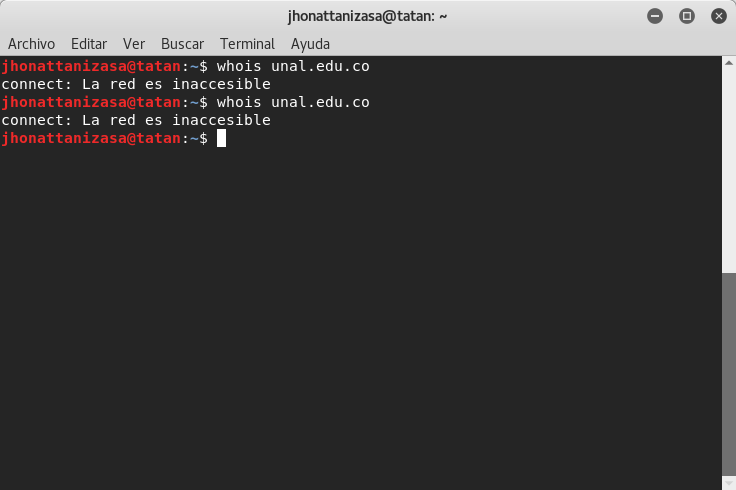
C D E

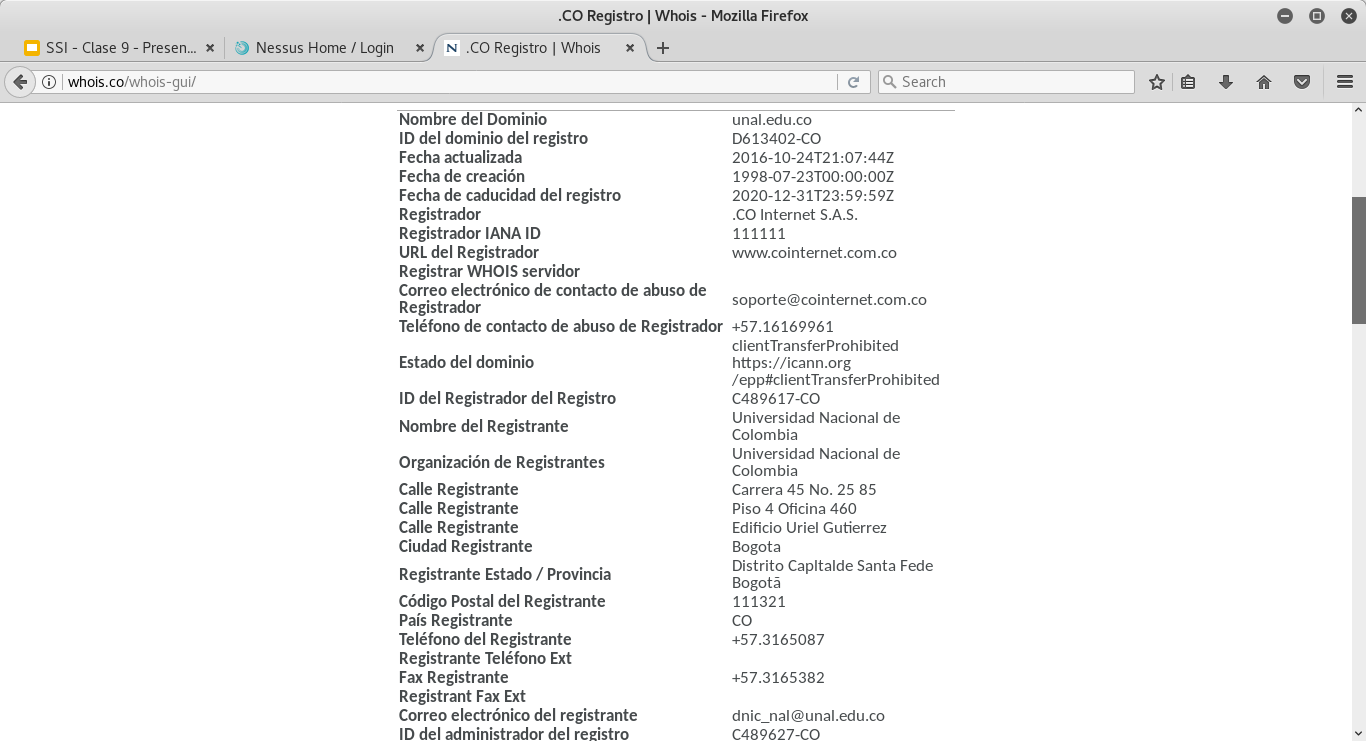


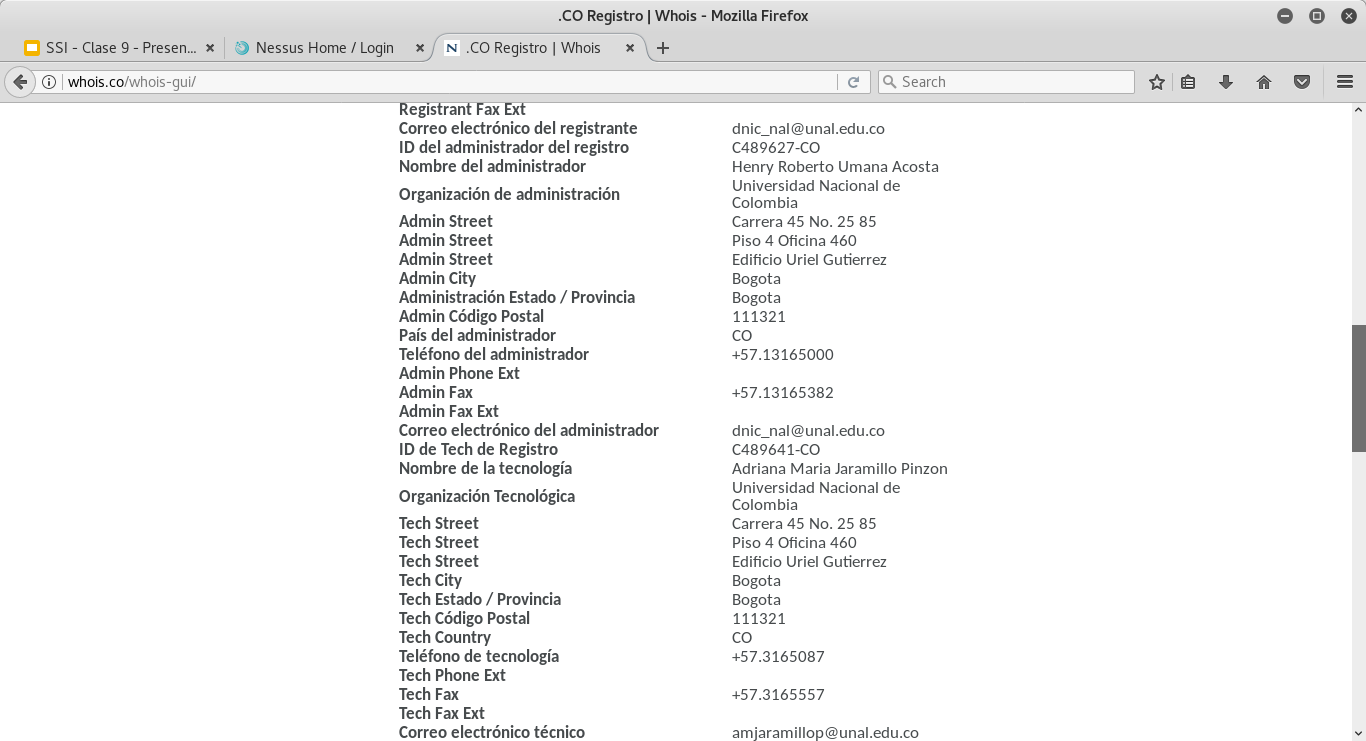
CONCLUSION podemos deducir que en esta parte encontramos bastante información sobre lo relacionado con contactos y link referentes a la universidad

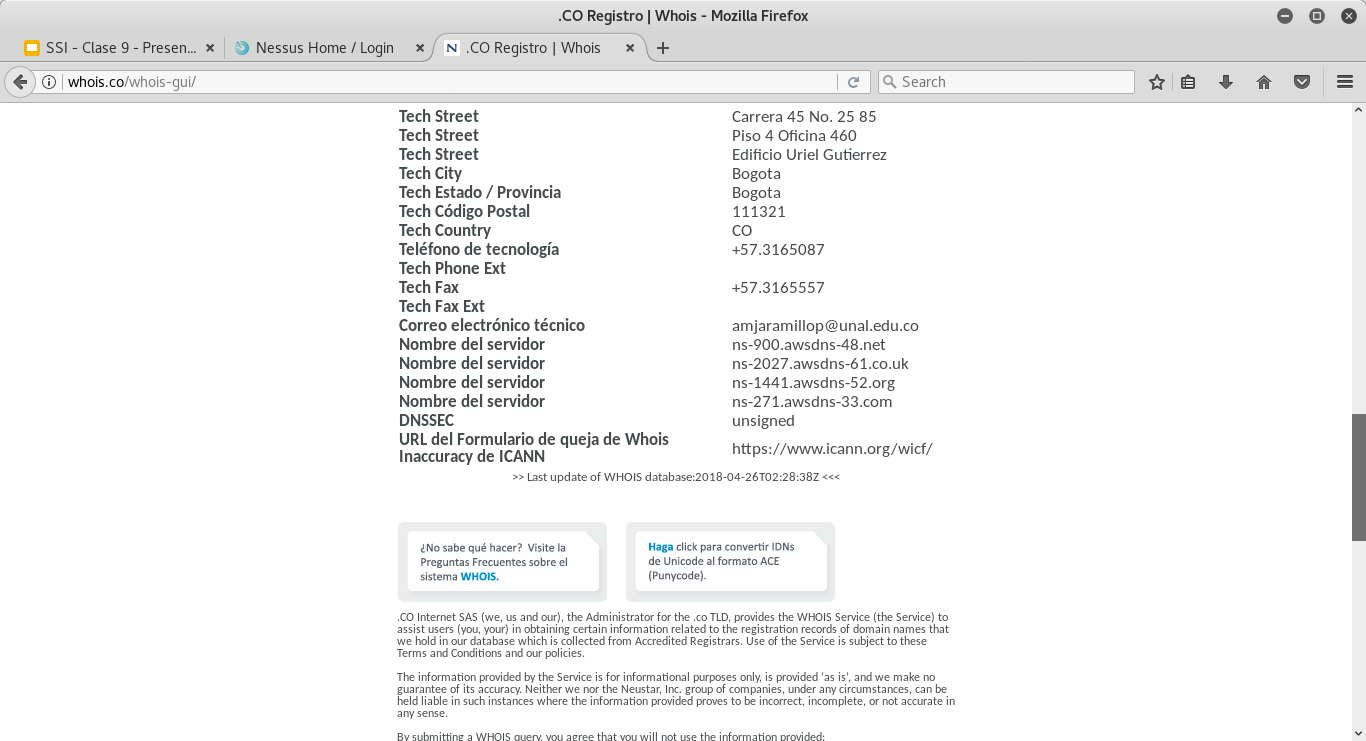
4.

error



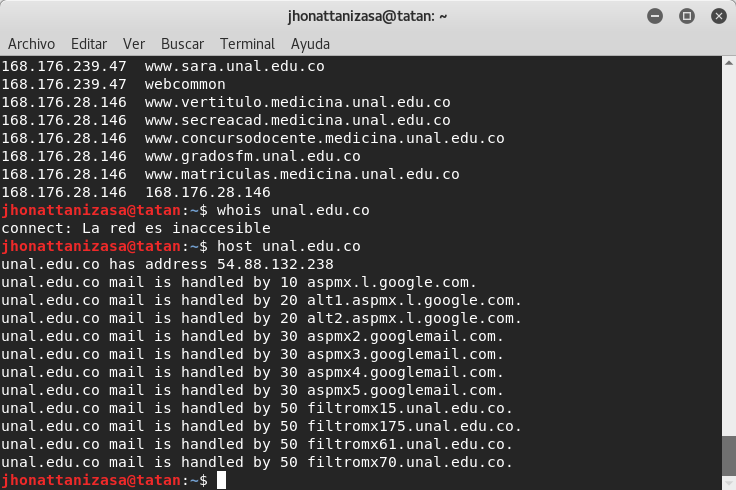




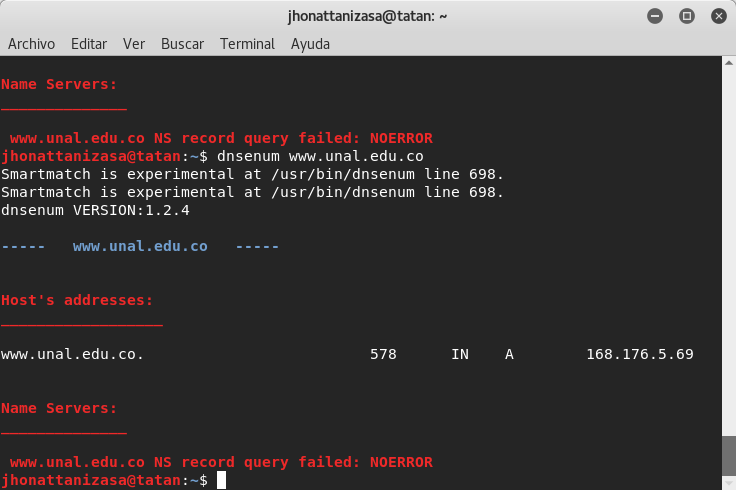


CONCLUSION en esta etapa el whois no sirvió como comando por consola debido a problemas en la red, debimos utilizar la plataforma para ver la información referente a la universidad.

5.

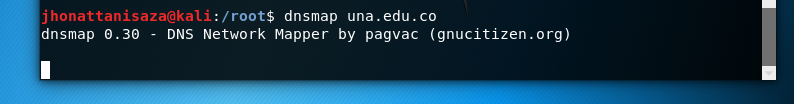


**Conclusión:** nos dan información sobre los tipos de servidores de correos

6. 

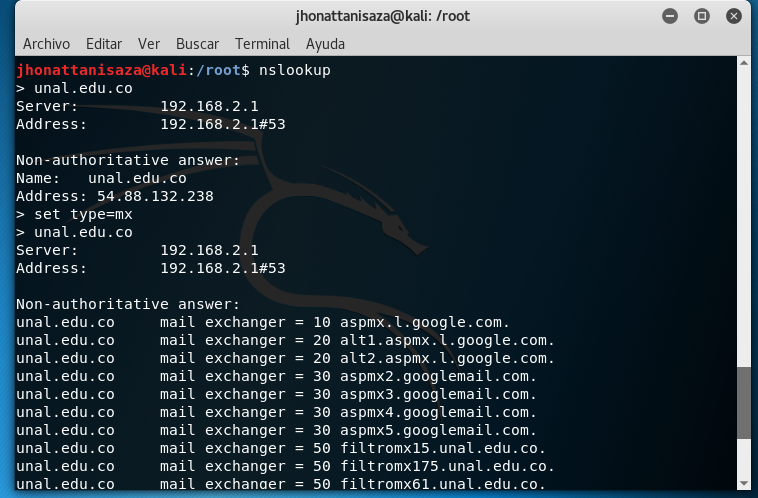
Conclusión: obtuvimos el dominio y a lo ultimo nos muestra un erro en ns record quey faile

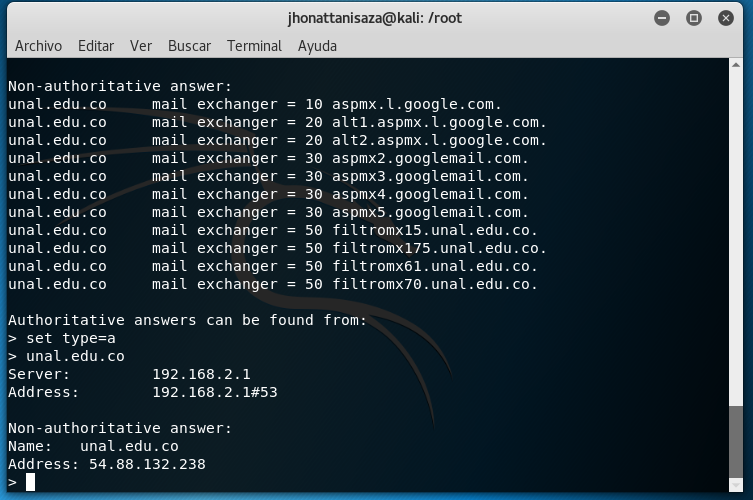
7.

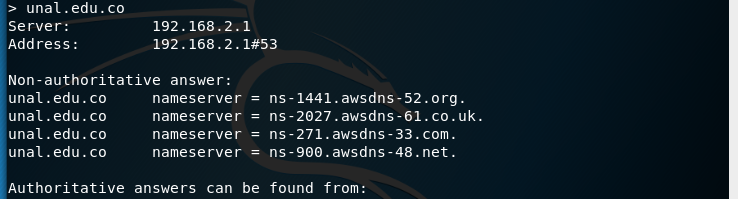


Dnsmap queda pensando y no responde

8.



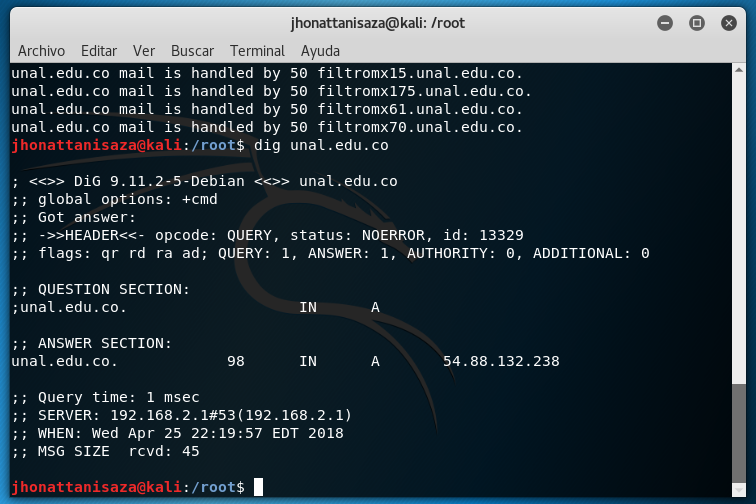




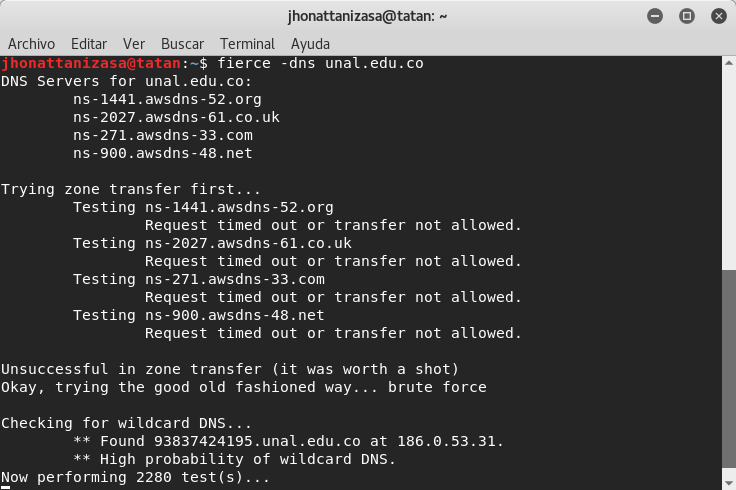
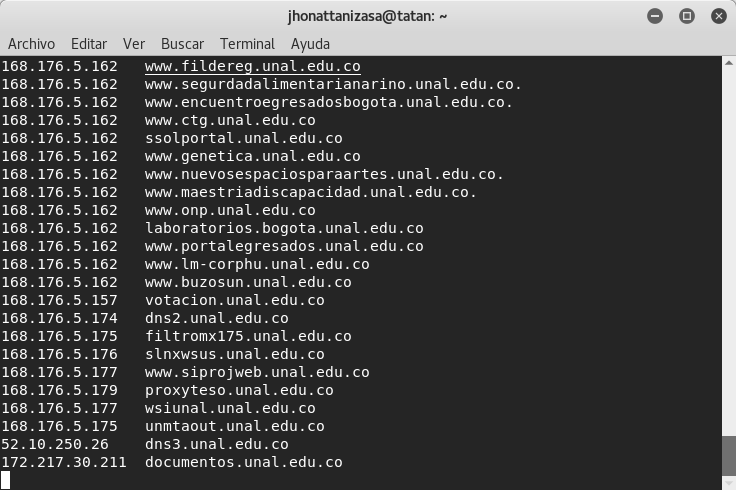


Conclusión : obtuvimos los filtrados del dominio, resgistros de correo,direcciones ip,dns

9.

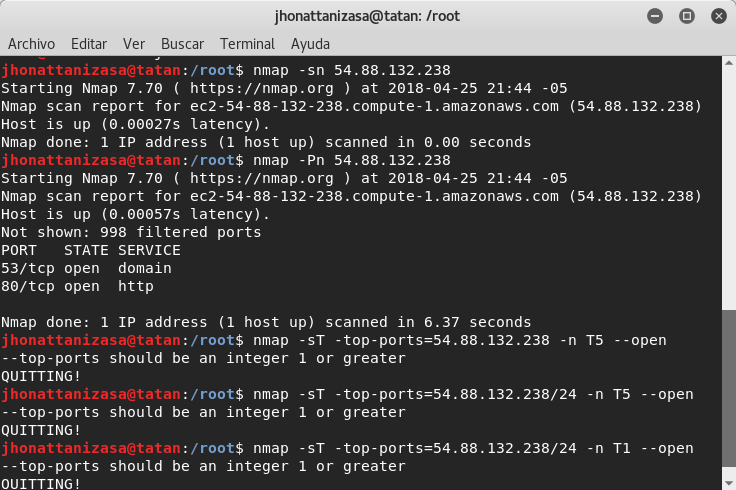


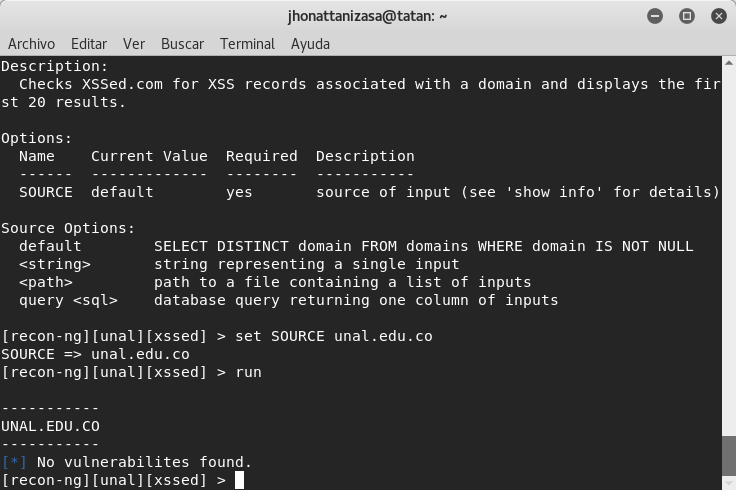
Conclusión: con el dig obtuvimos información del dominio

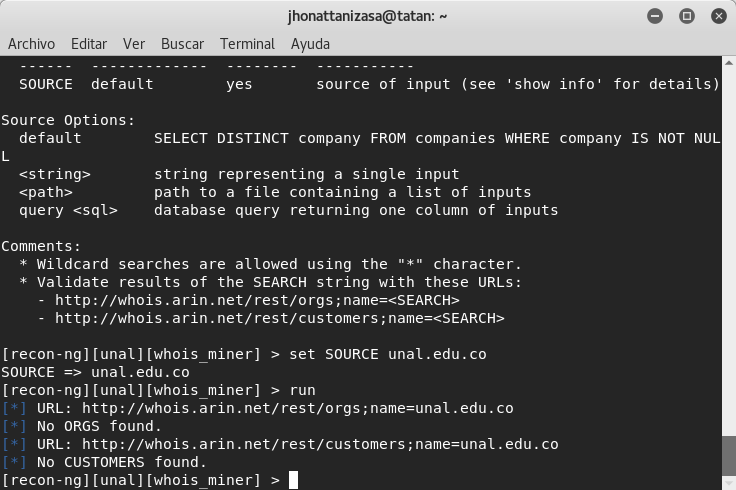
10. 

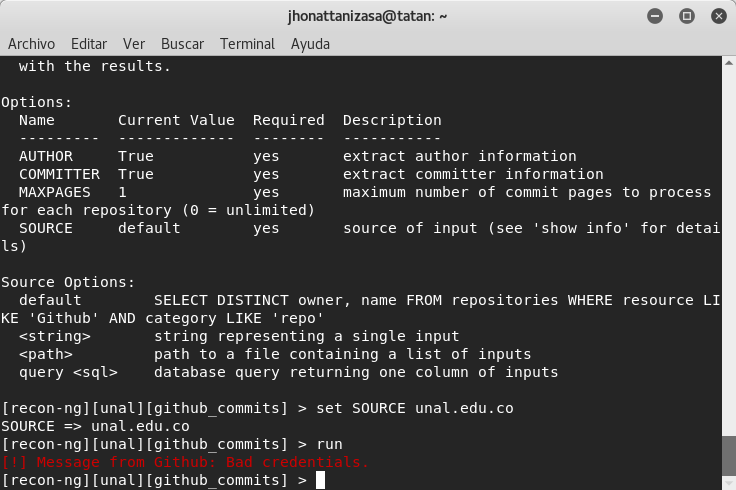
Conclusión: con el firce obtuvimos la informacioncon ataques de fuerza vital

11.

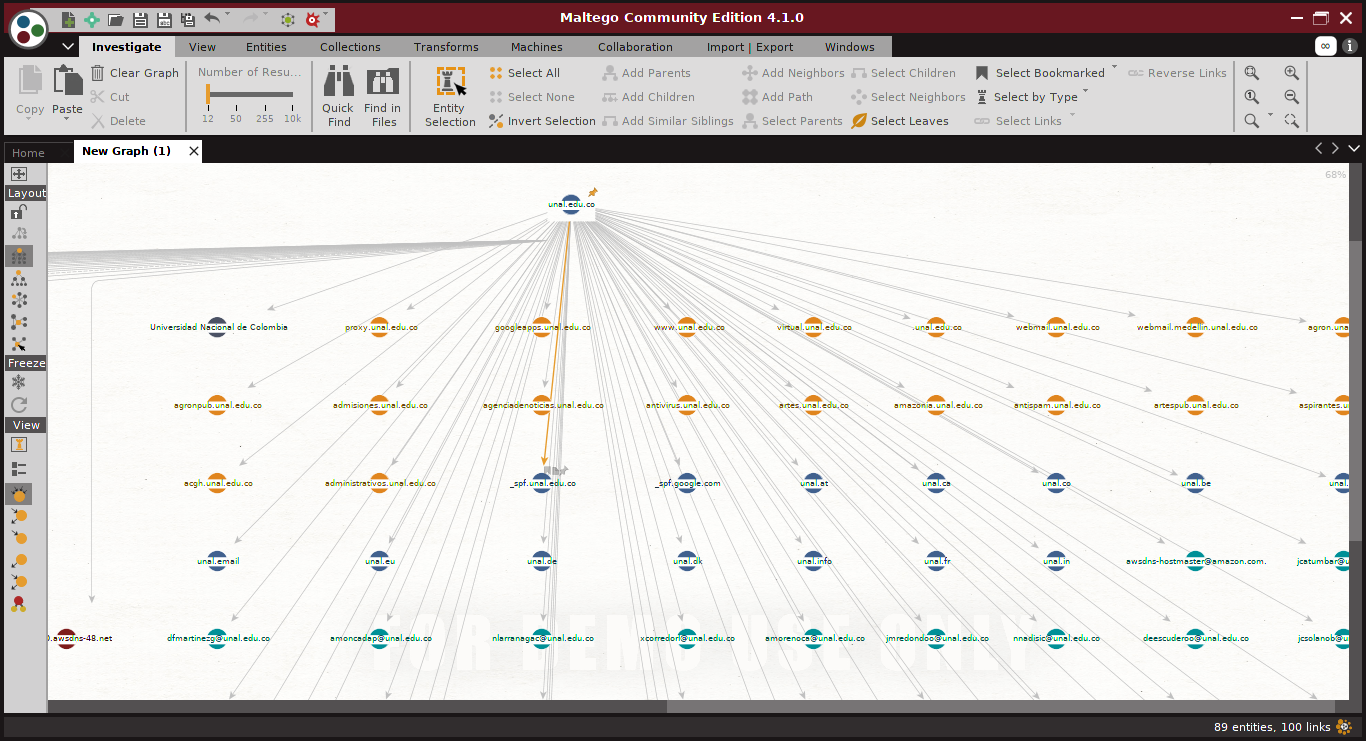


12. 



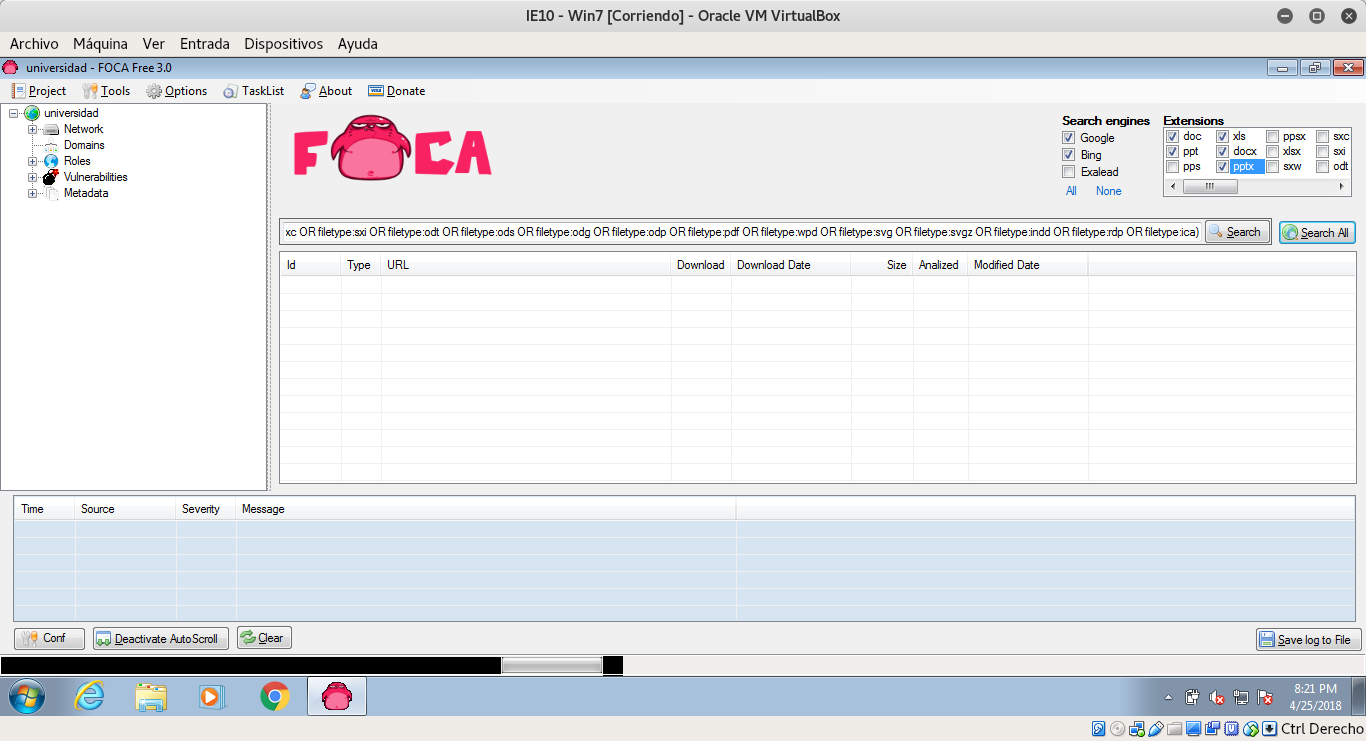


13.

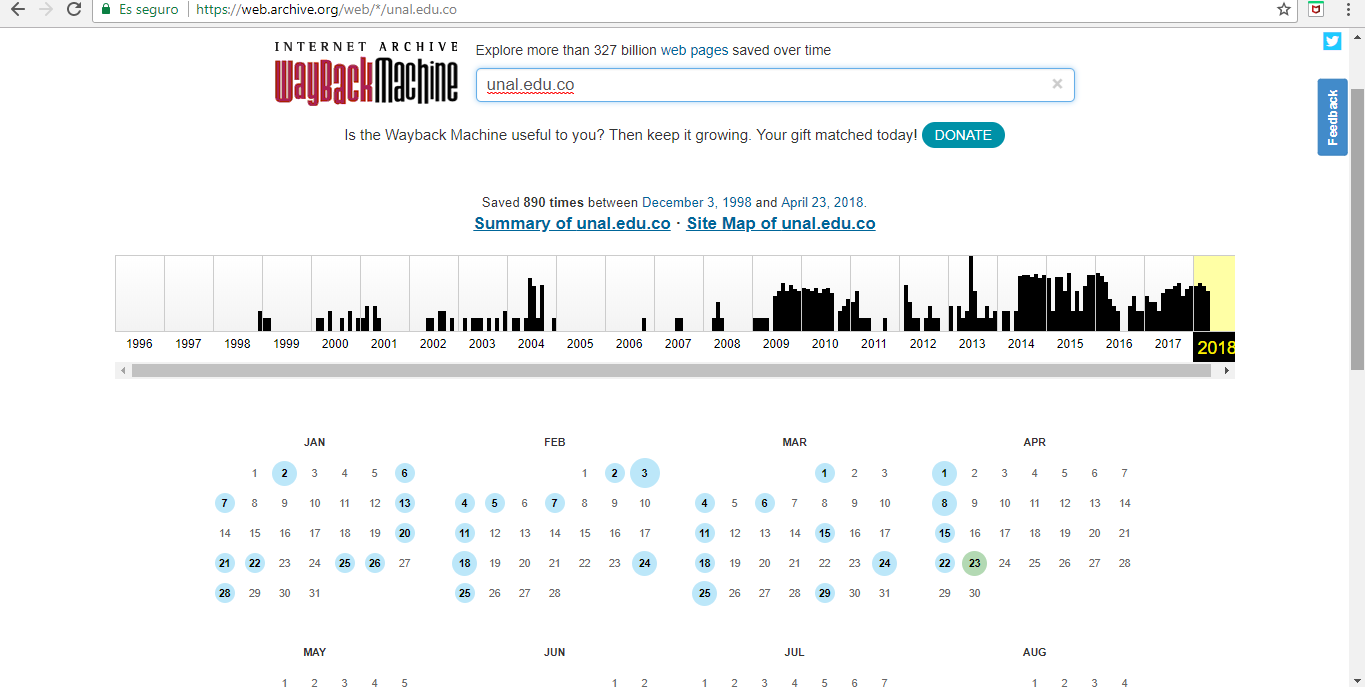


**Conclusión: Maltego** muestra qué tan expuesto esta unal.edu.co en el internet, y pudimos observar que es muy grande la topología de la red, en la cual se debe de buscar el punto débil para explotarlo.

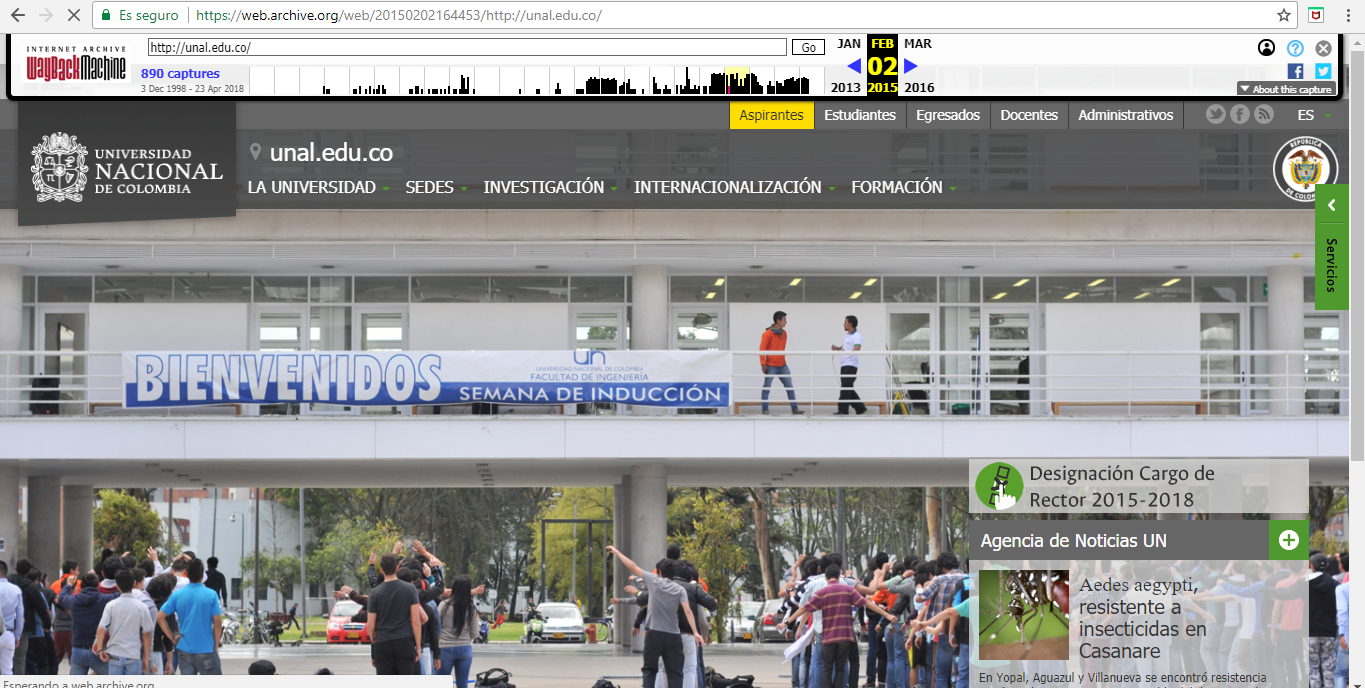
14.



15.

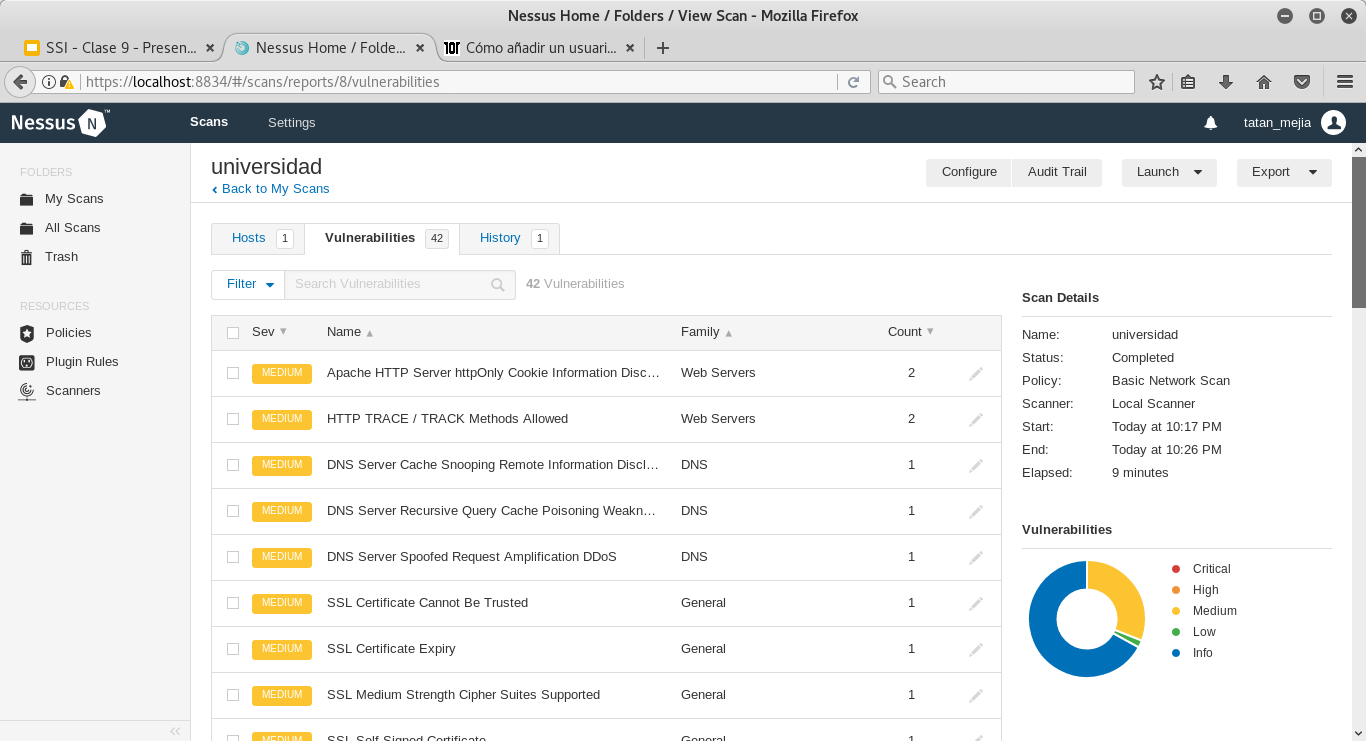




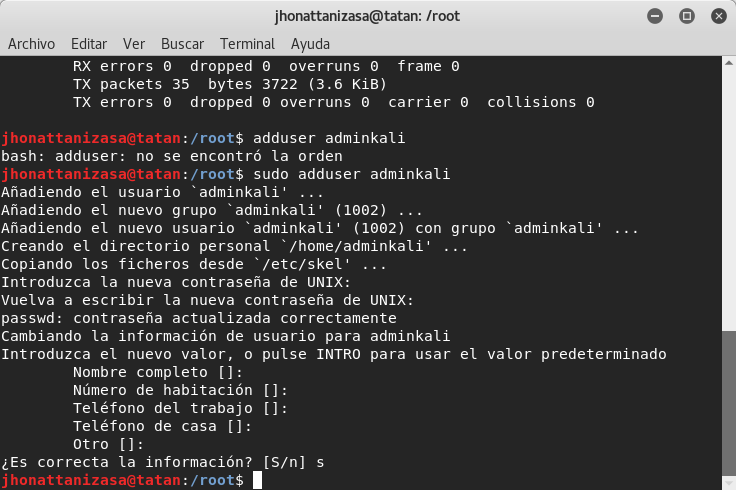


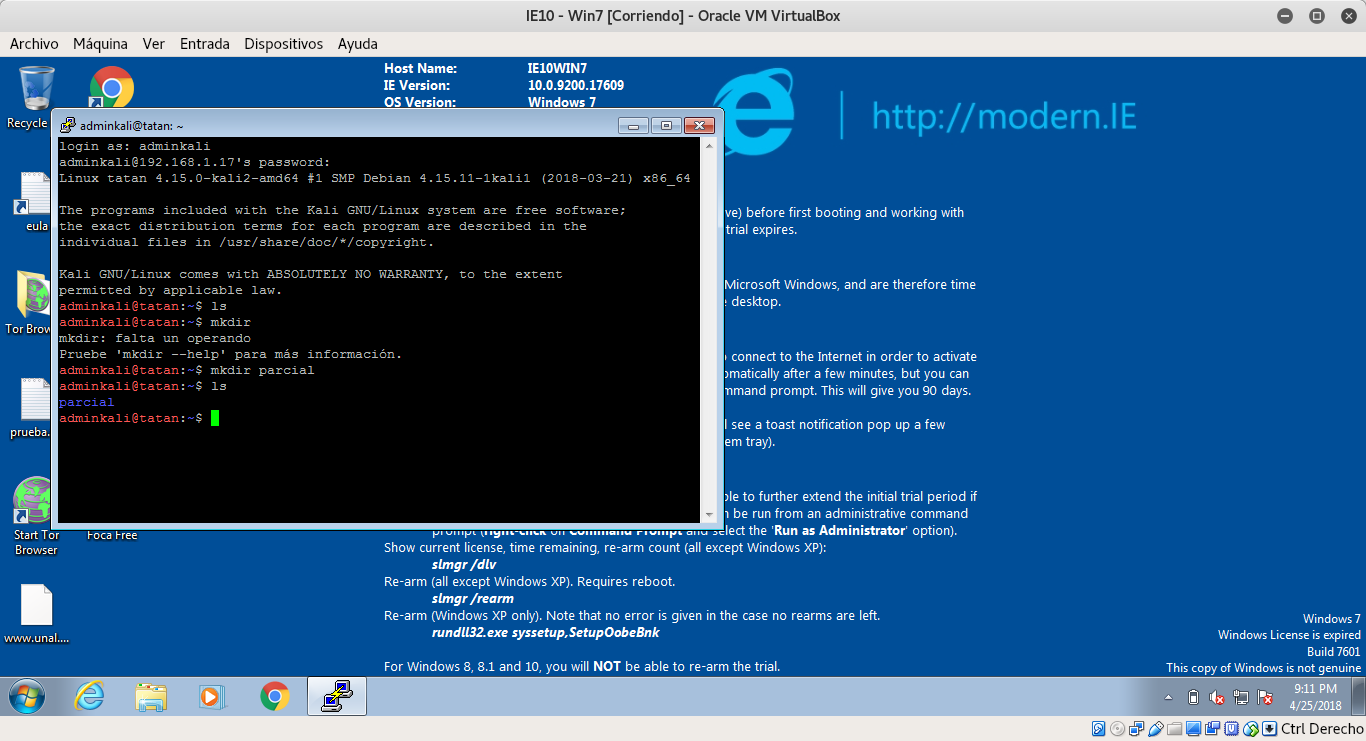


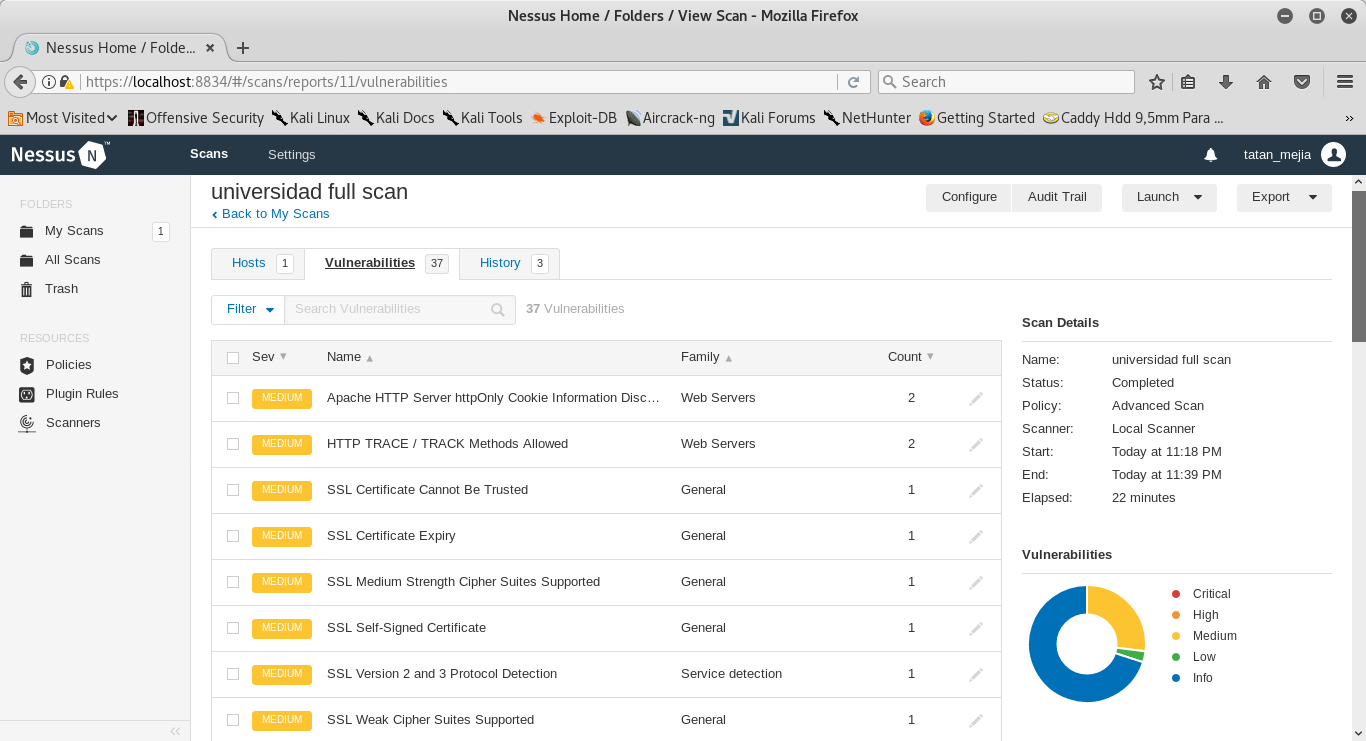
16.

a. 

17

17a. 



b. 

18.

19.

20.

**Obtención de información:**

Etapa del ciclo de inteligencia posterior a la dirección y planificación y anterior a la de producción. Consiste en la adquisición y reunión de información en bruto mediante la explotación de múltiples y variadas fuentes de información por los órganos de obtención, la cual se procesa, almacena y organiza para su posterior uso por los órganos de elaboración durante la producción de inteligencia.

**Numeración de sistema**

es un conjunto de símbolos y reglas de generación que permiten construir todos los números válidos en el sistema a escanear.

**Análisis de vulnerabilidades:** método en el cual se procede a realizar las debilidades encontradas ya que con ello se dara inicio el como afrontar dicha vulnerabilidad o aprovecharla.

**Explotación de vulnerabilidades:** método en el cual serealiza la exploración de dicha vulnerabilidad para determinar el grado de incidencia.

**Post-explotacion de vulnerabilidades:**  método que se realiza después de ser realizada dicha investigación de vulnerabilidad para asi determinar el nivel de aprovechamiento.

21. Despues de toda la información recolectada se puede proceder a dar un informe detallado de las vulnerabilidades encontradas , para asi determinar de que manera poder minimizar dichos problemas, luego de ello proceder a brindarle el apoyo e información pertinente de como tener una buenas practicas informáticas.