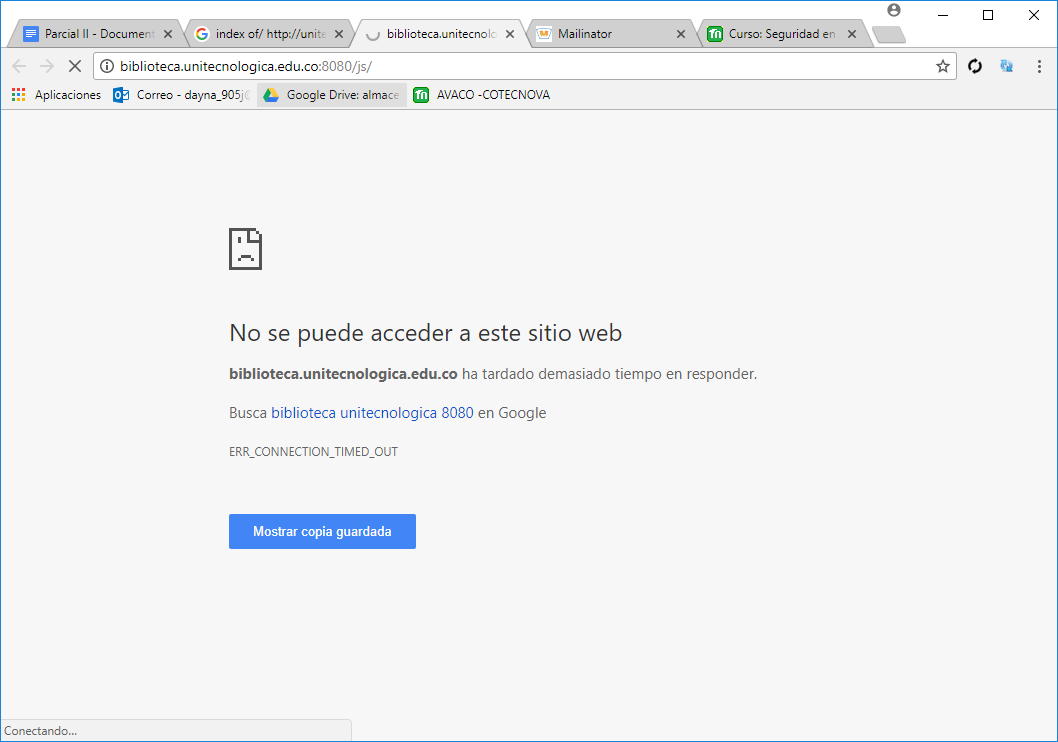
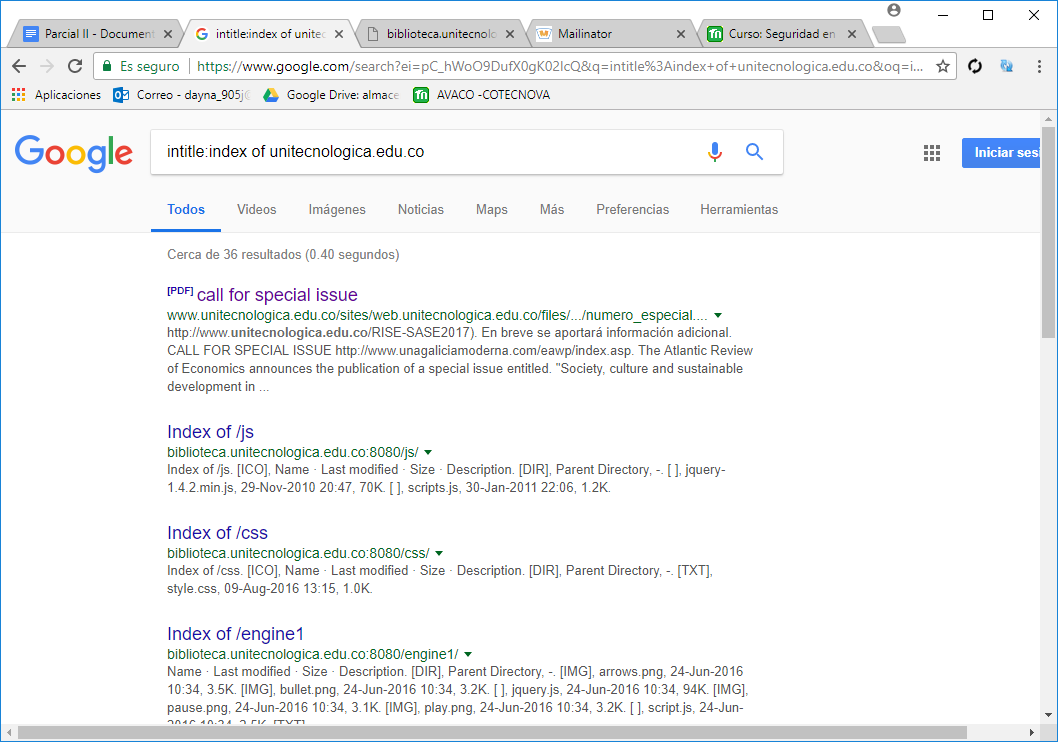
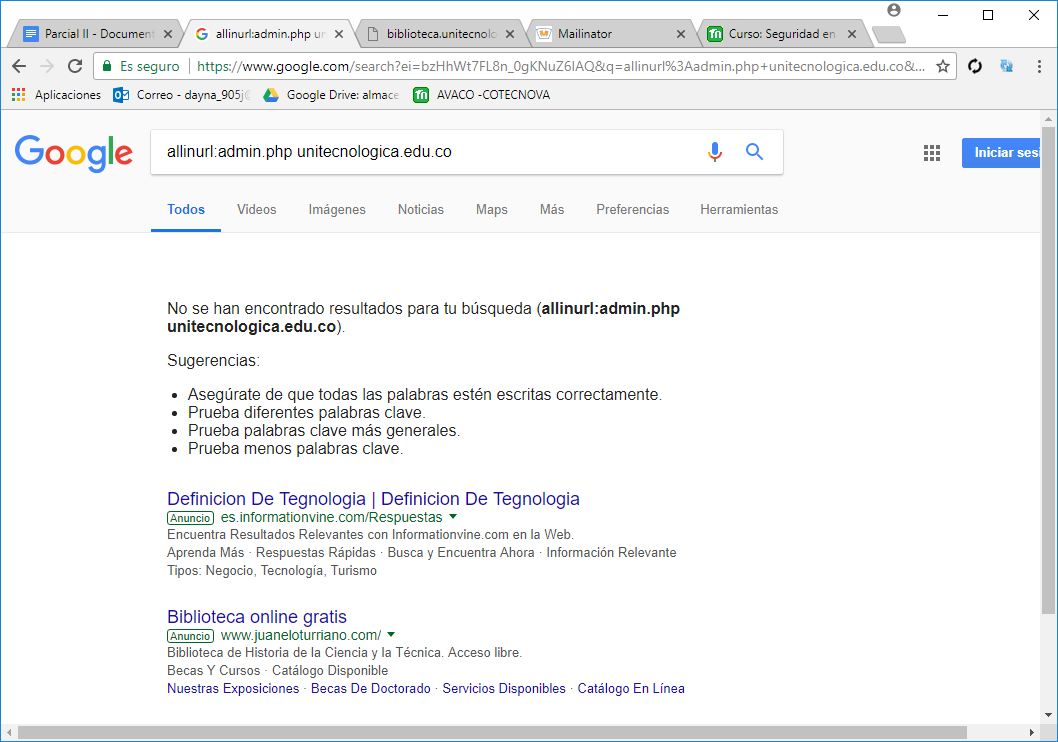
Cristhian urrego Salazar 1.112.775.485

Adrian Vargas 1.112.778.264

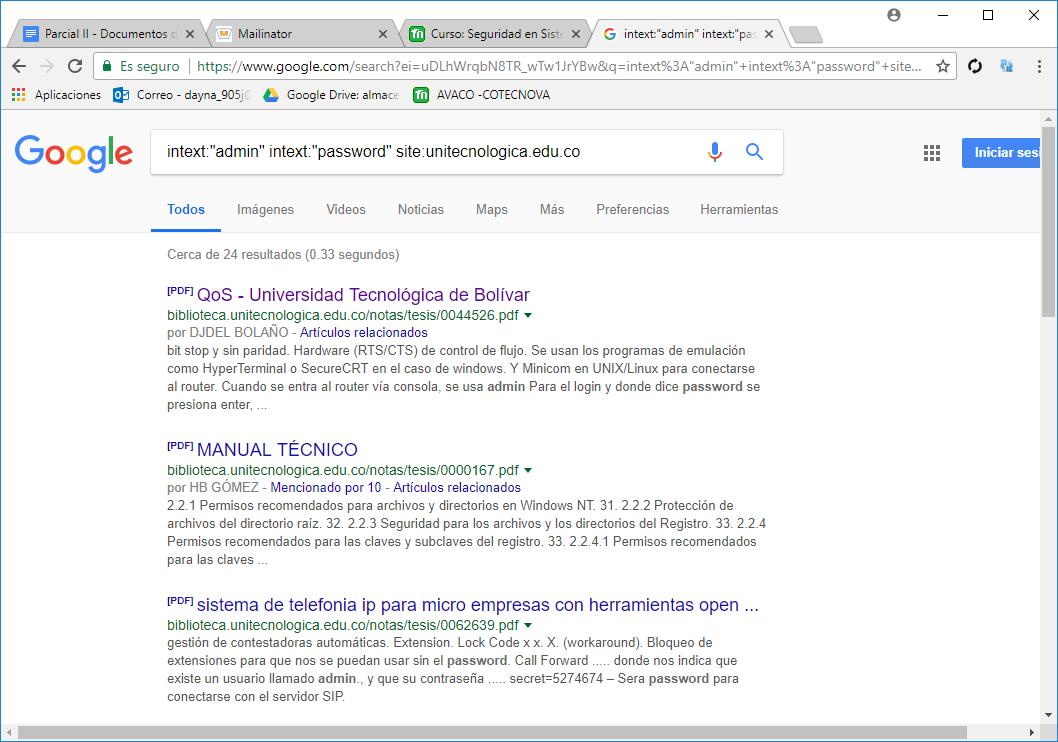
1. Se realiza una búsqueda index of, en los resultados se encuentran enlaces con el puerto 8080 a los cuales se intenta acceder a los sitios sin exito



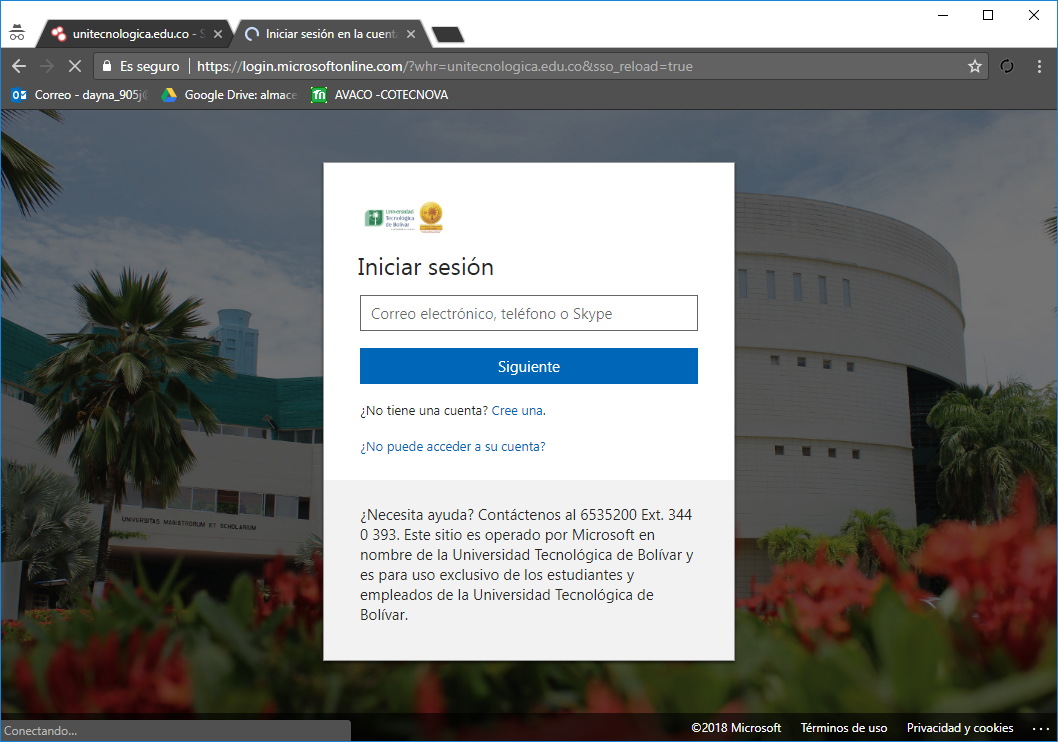
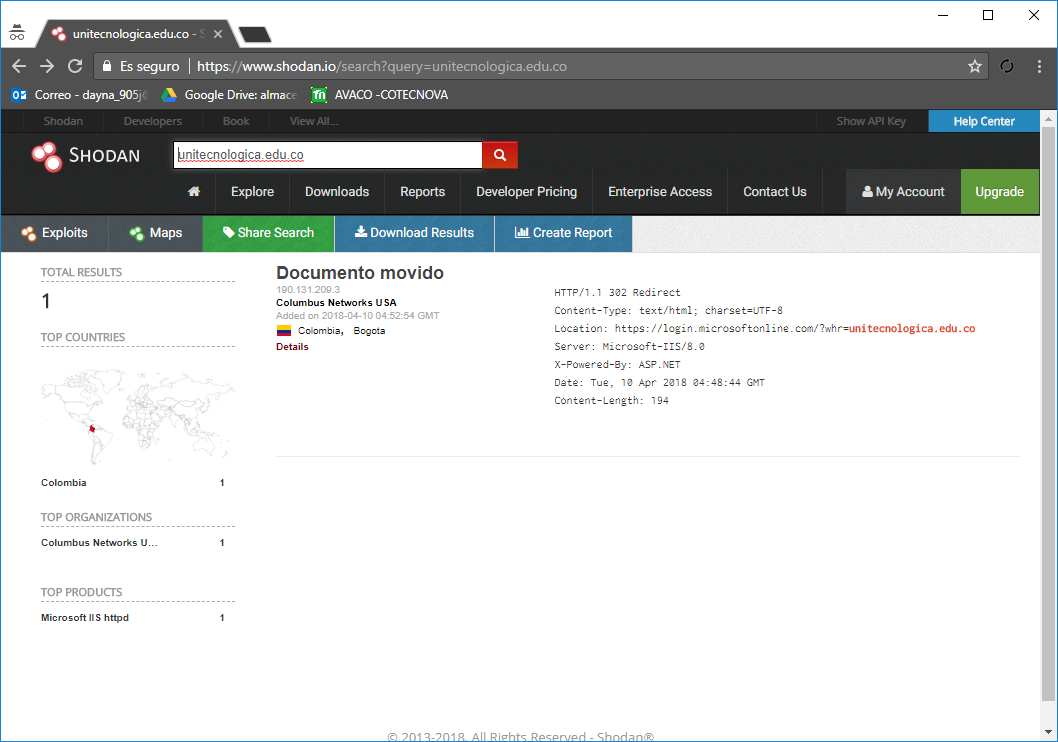
Se realiza una búsqueda del algún archivo admin.php sin éxito:



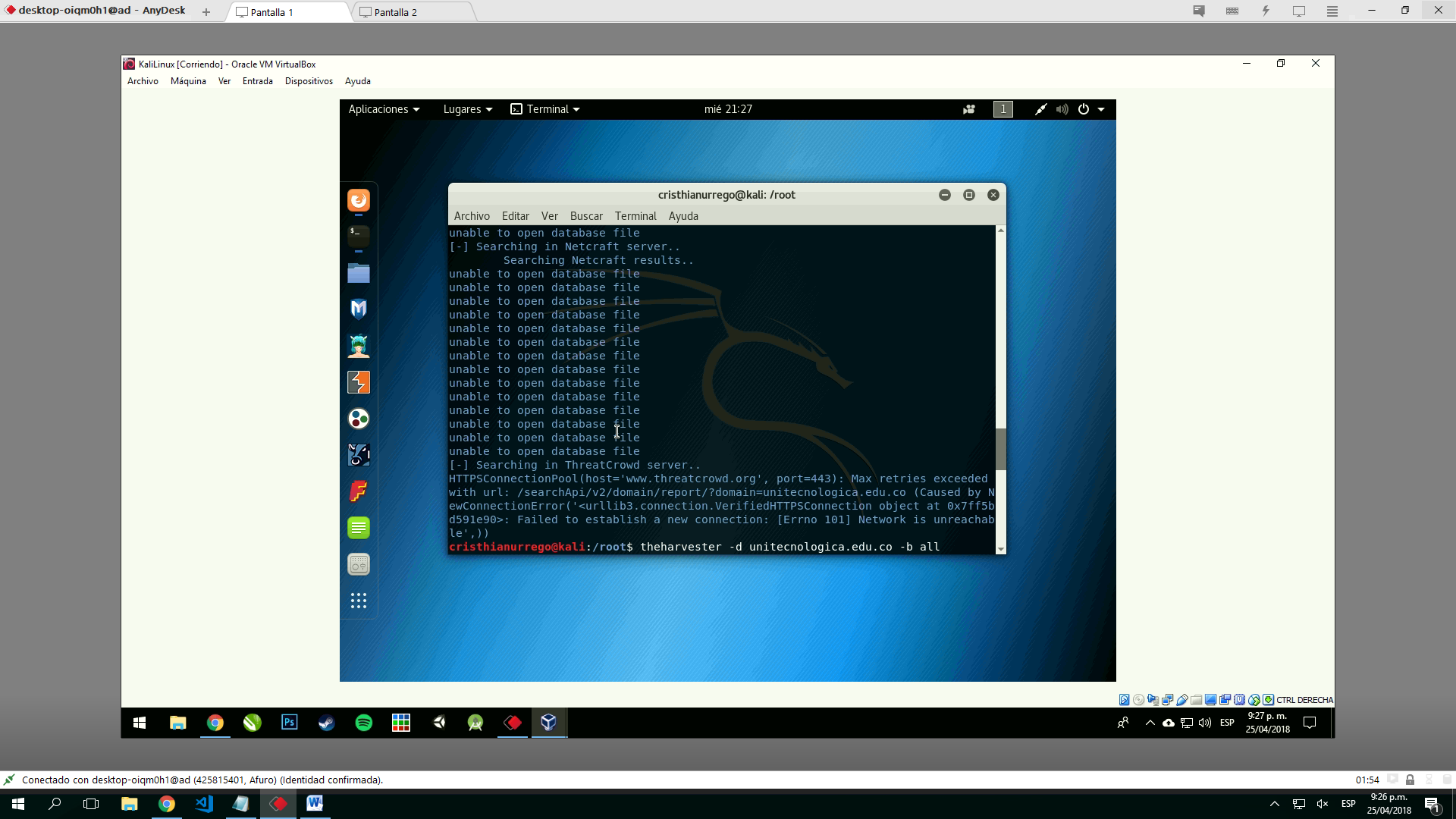
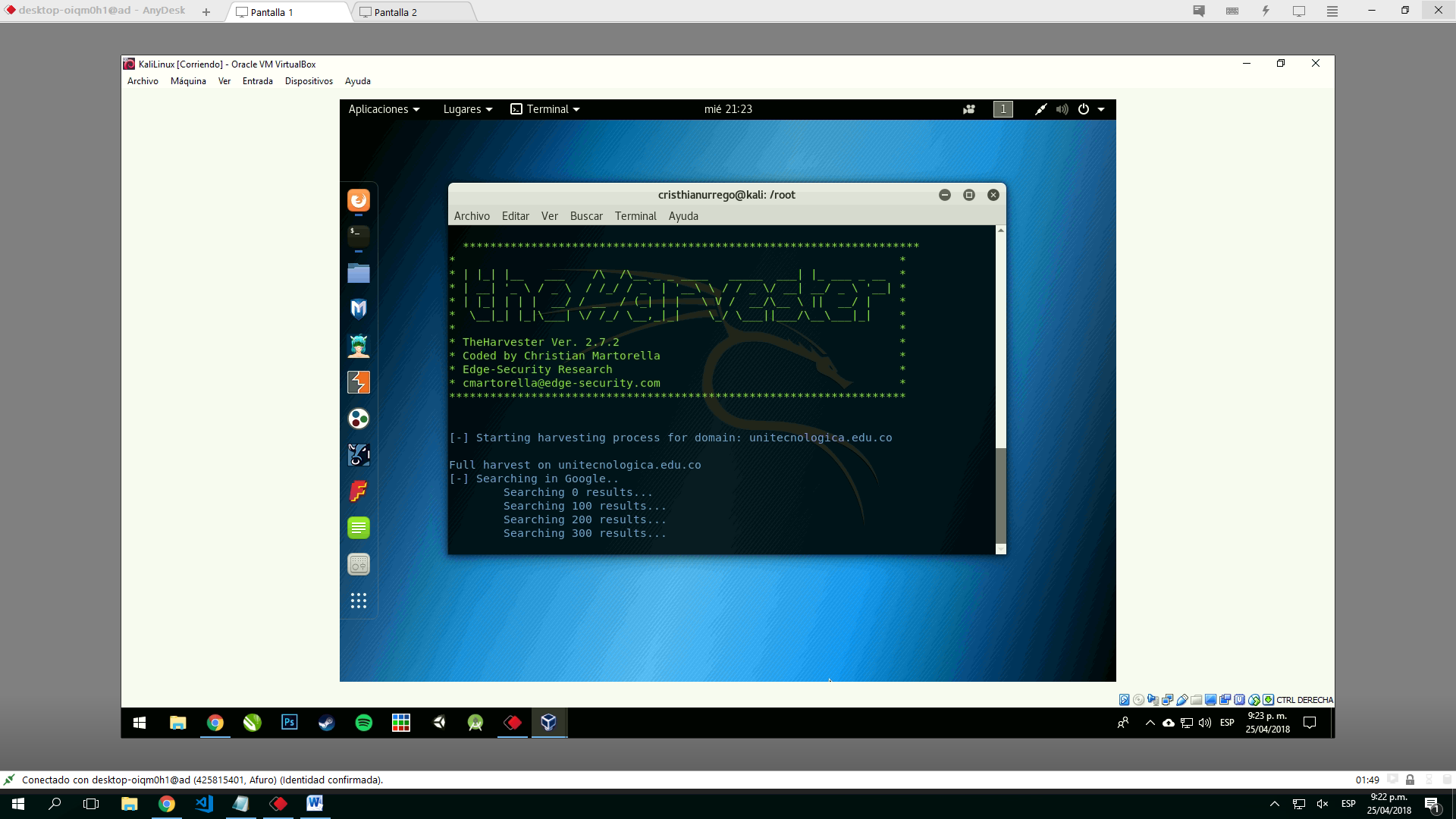
Se realizaron diferentes búsquedas y en general la información resultante son archivos de la biblioteca virtual:



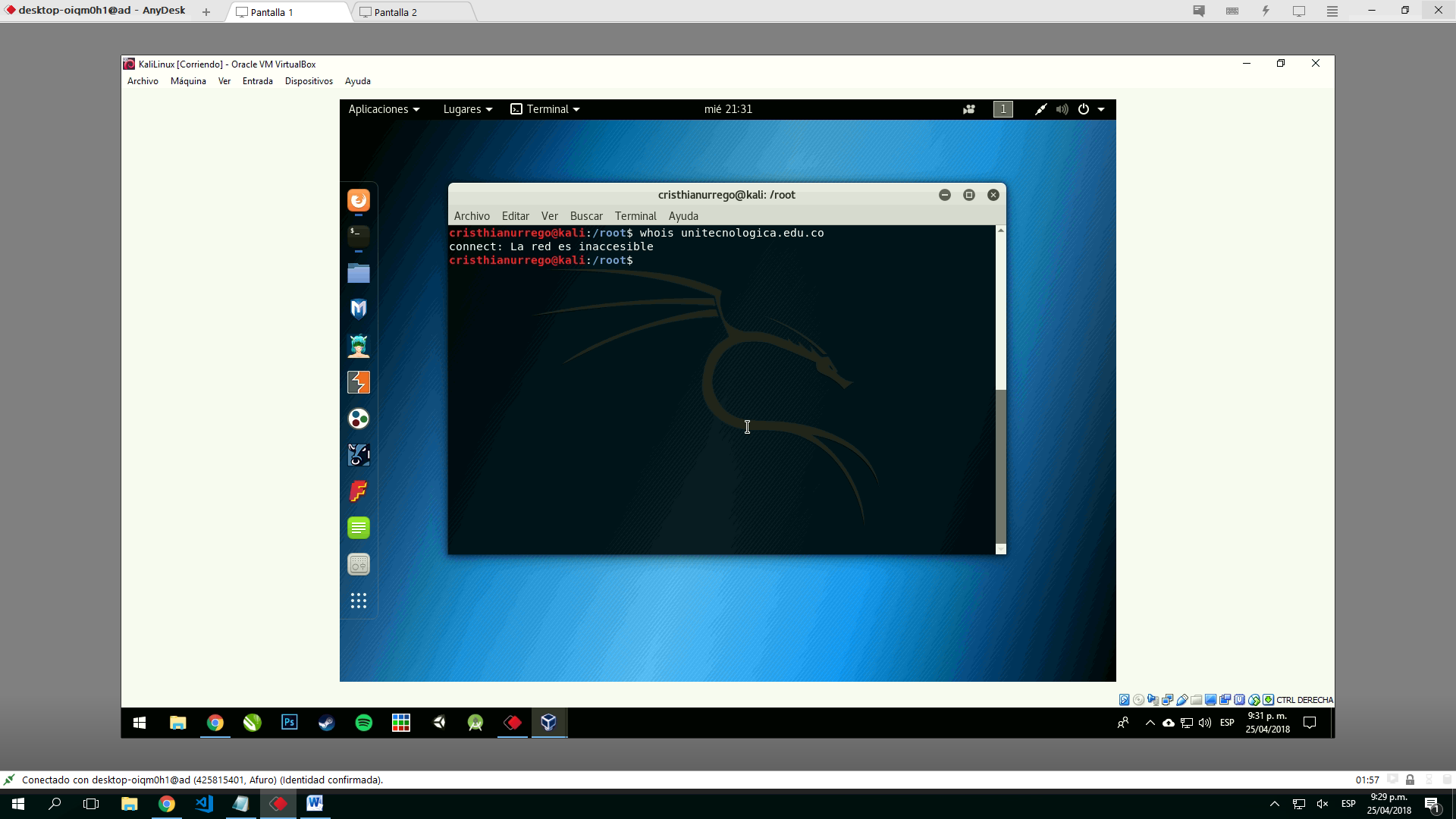
1. Se realizó una búsqueda en shodan en el cual únicamente se encontró una dirección ip que dirigía a la de inicio de correos electrónicos de la universidad.



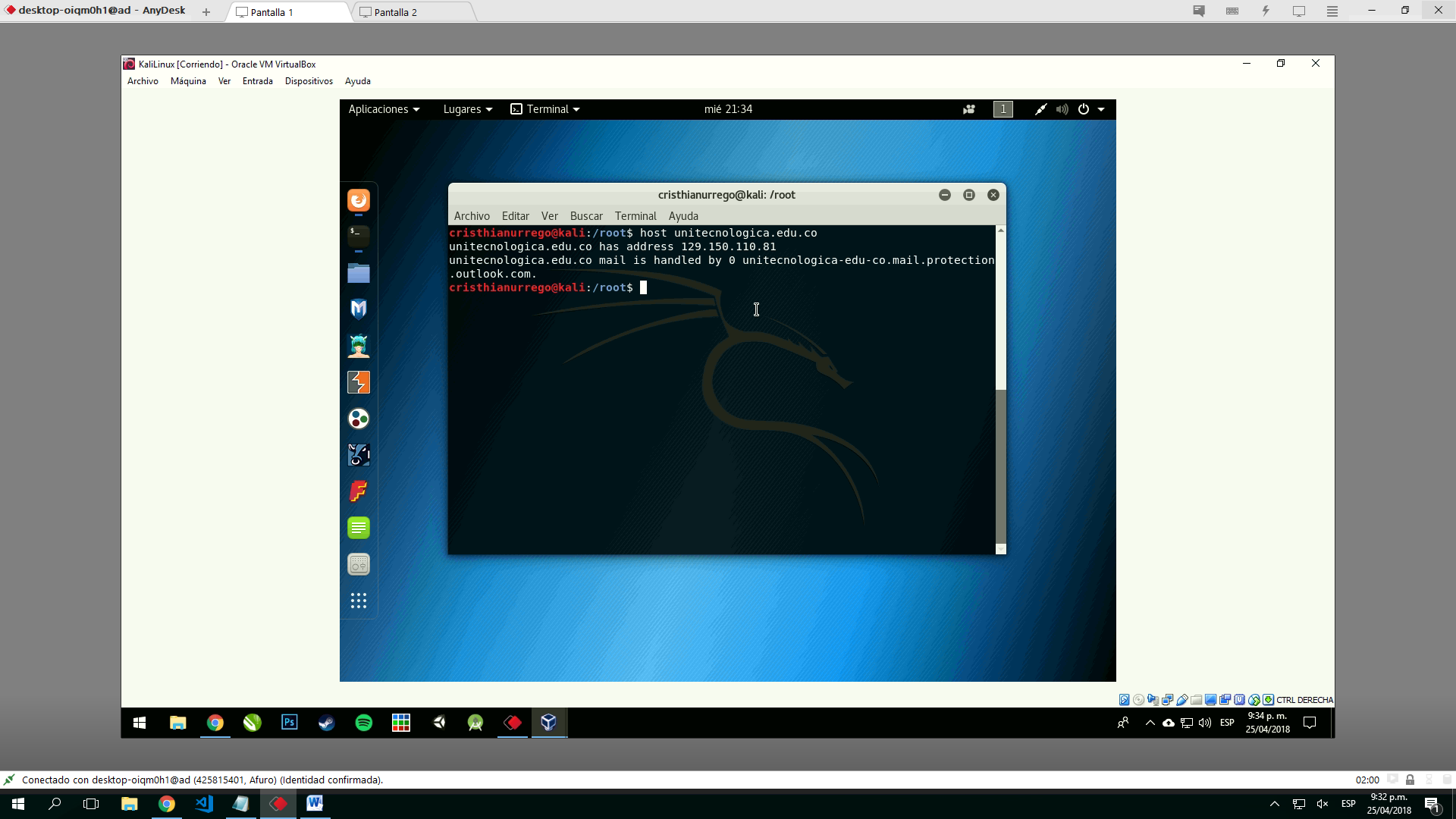
1. Usando theharvester encontró una lista de más de 500 resultados de los cuales fue incapaz de abrir y leer los archivos



1. Se realiza un whois al sitio de la universidad el cual como resultado no permite acceder a la red

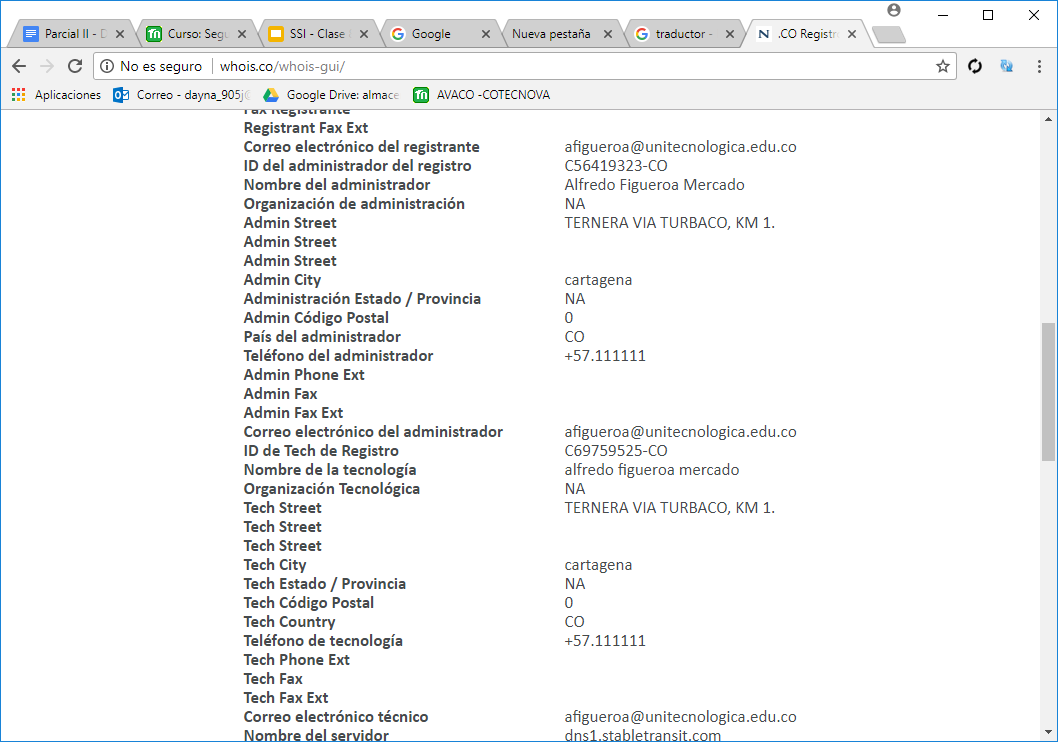


1. Utilizando host en Linux se obtiene la dirección del sitio y el administrador de correos de la universidad

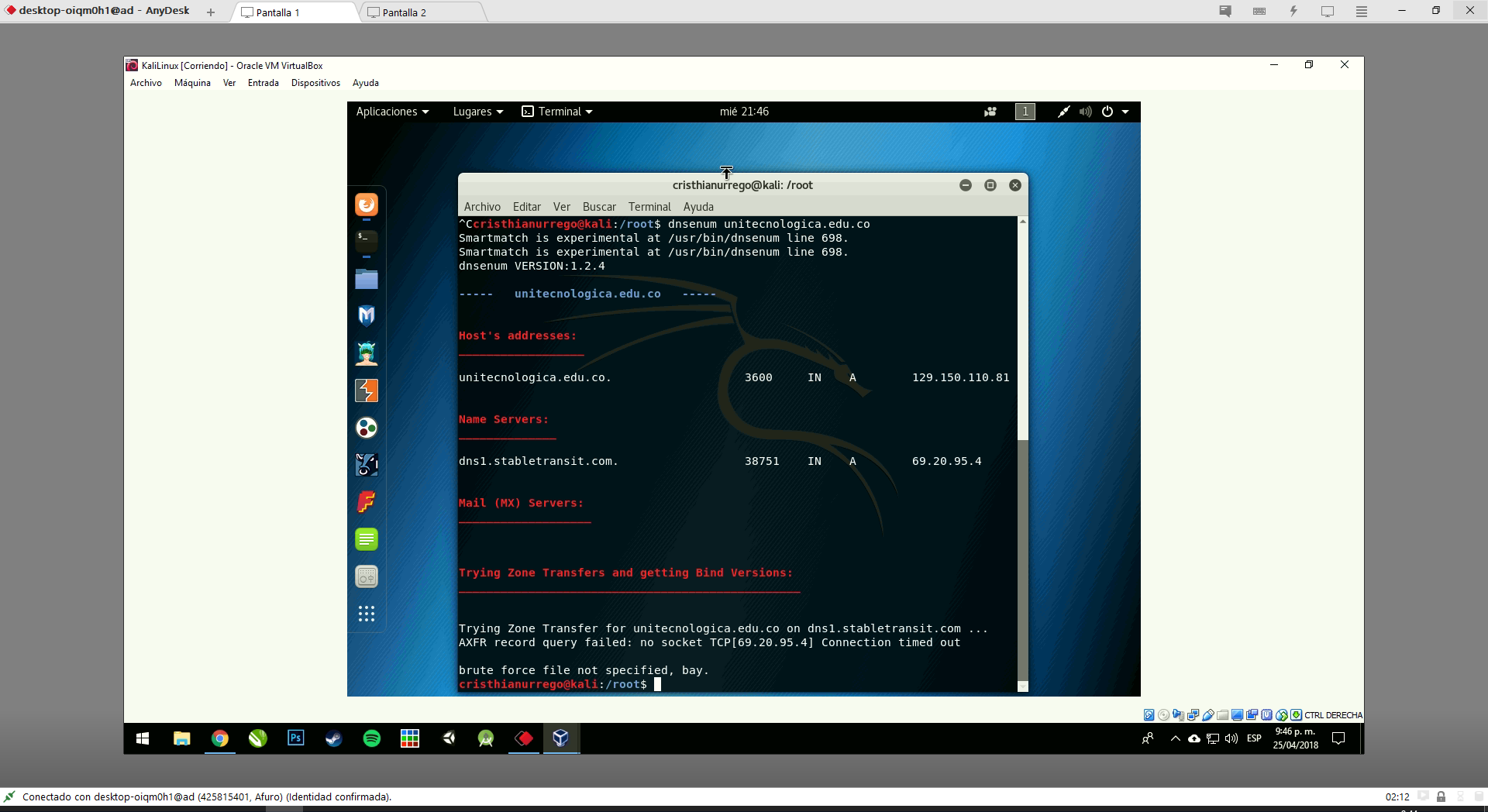


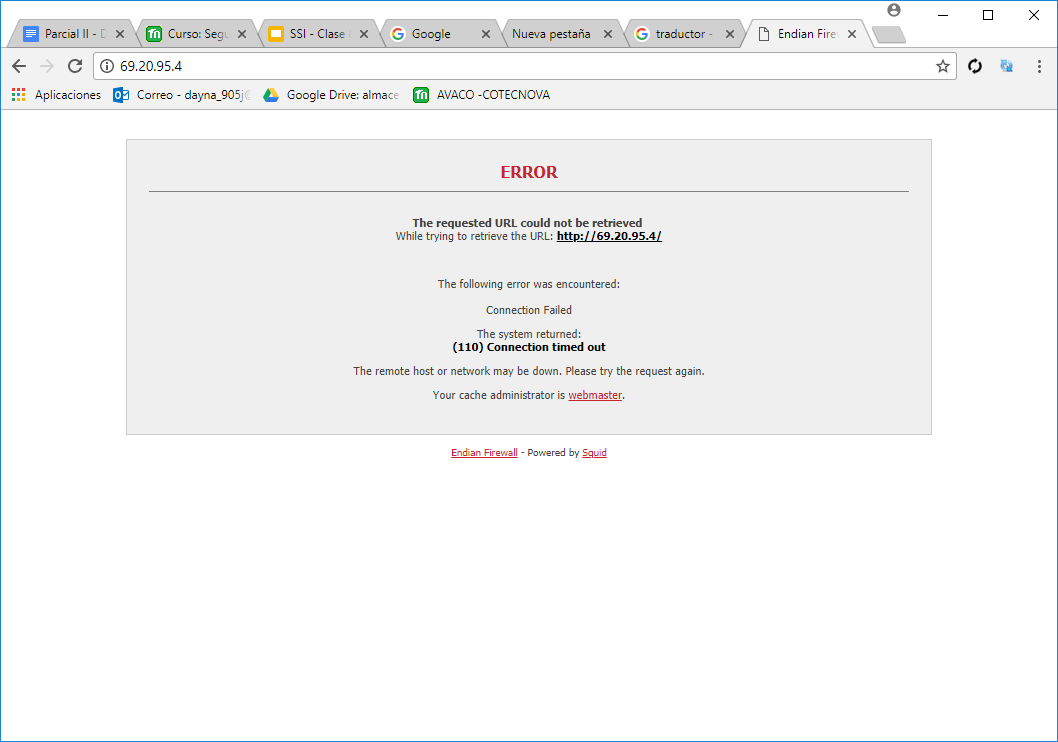
Realizando una búsqueda por whois.co se obtuvo una mayor cantidad de información, ente ellos el nombre del registrante del dominio.



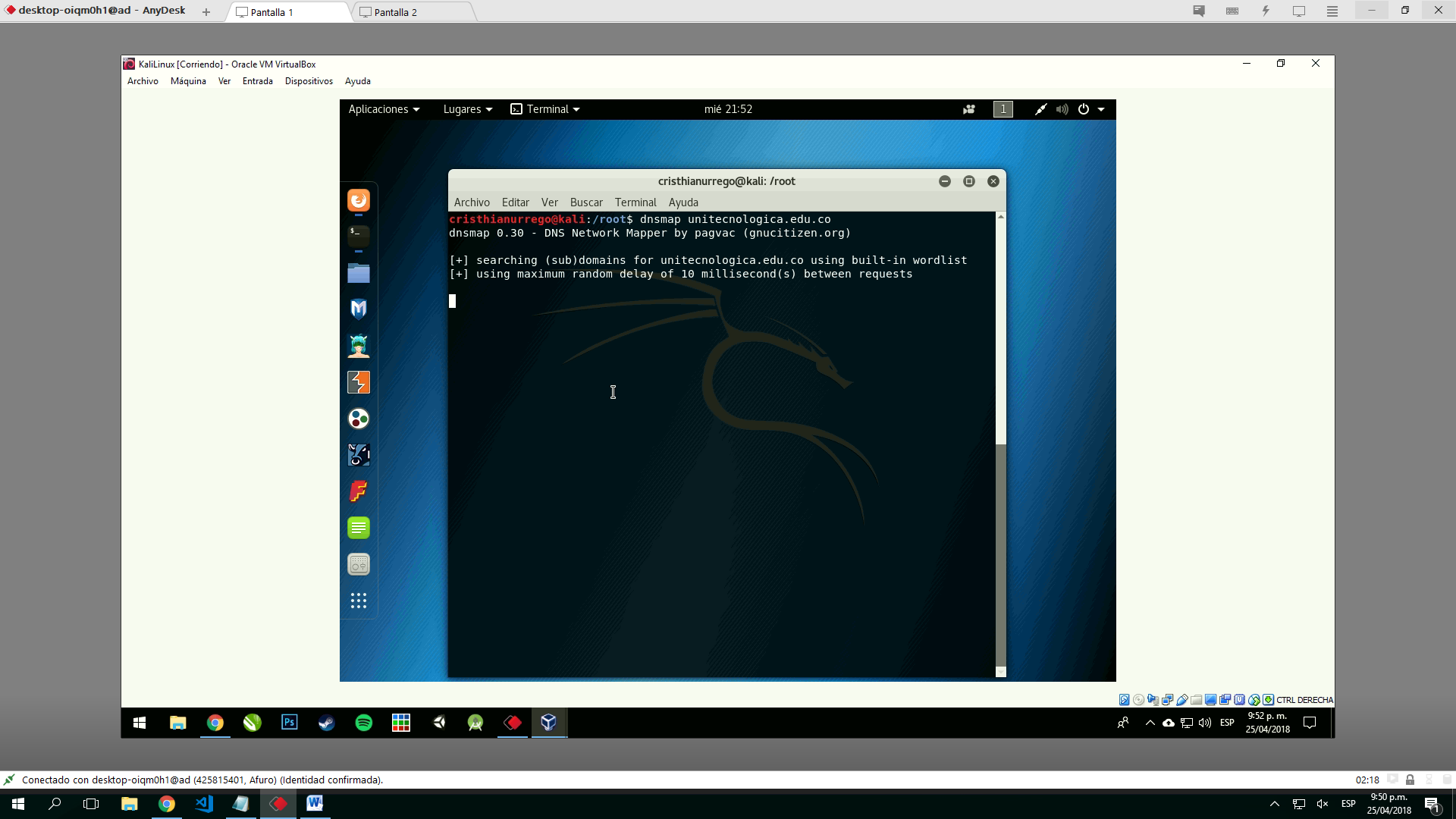


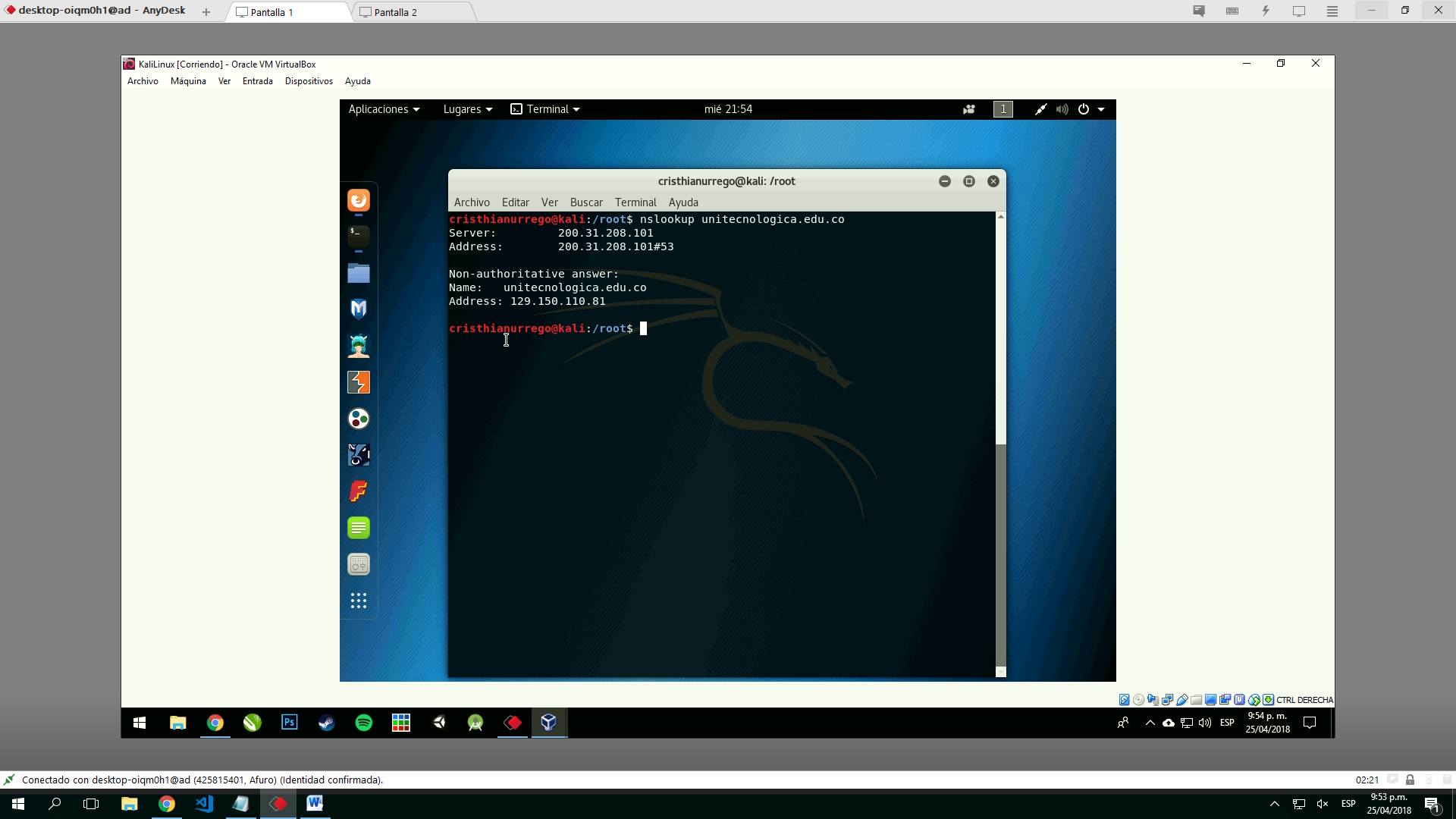
1. Utilizando dnsenum se encontraron dos dirección ip, y accediendo a ellas se encontró con un acceso restrigindo observando que el servidor web cuenta con endian firewall

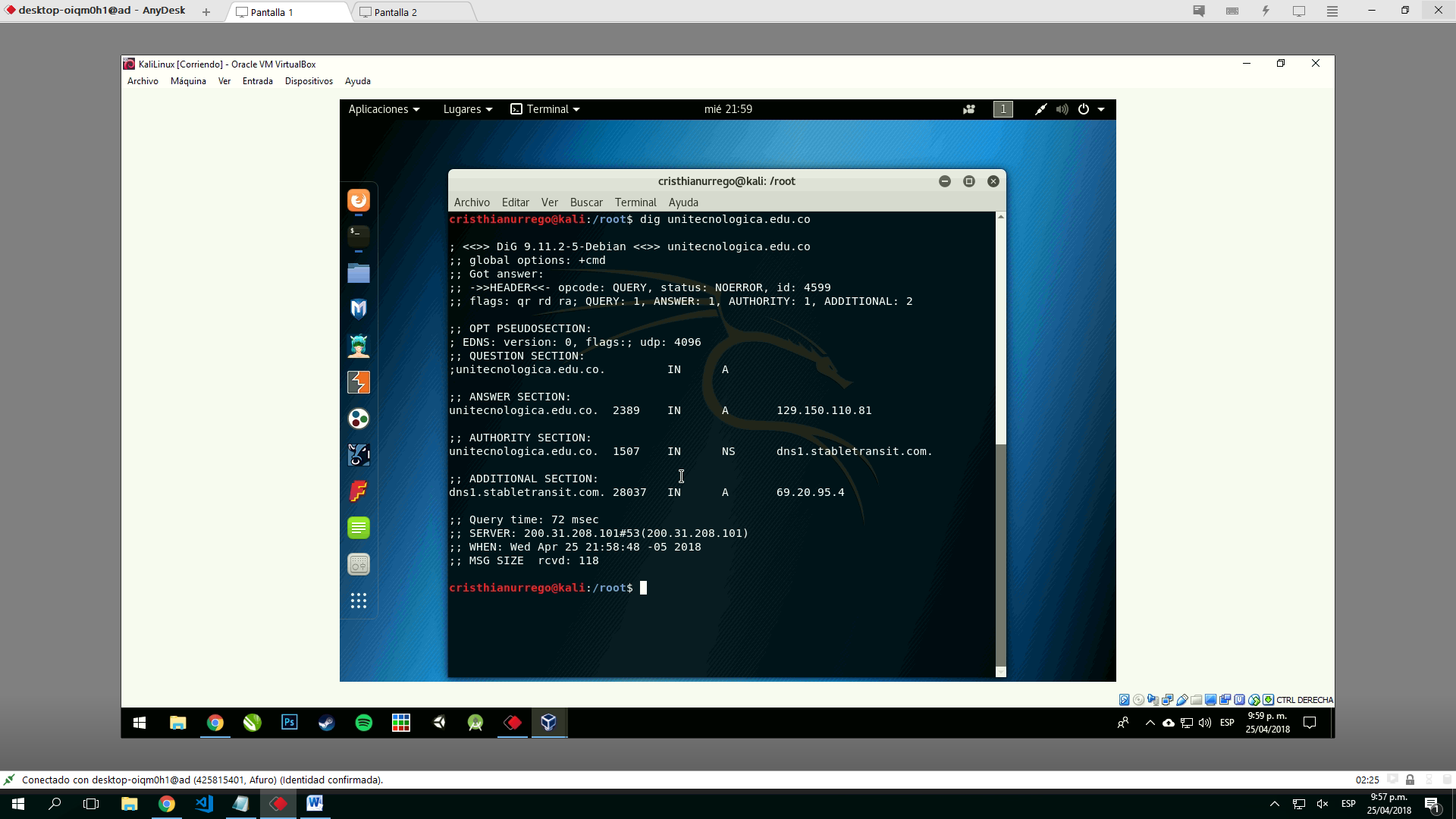




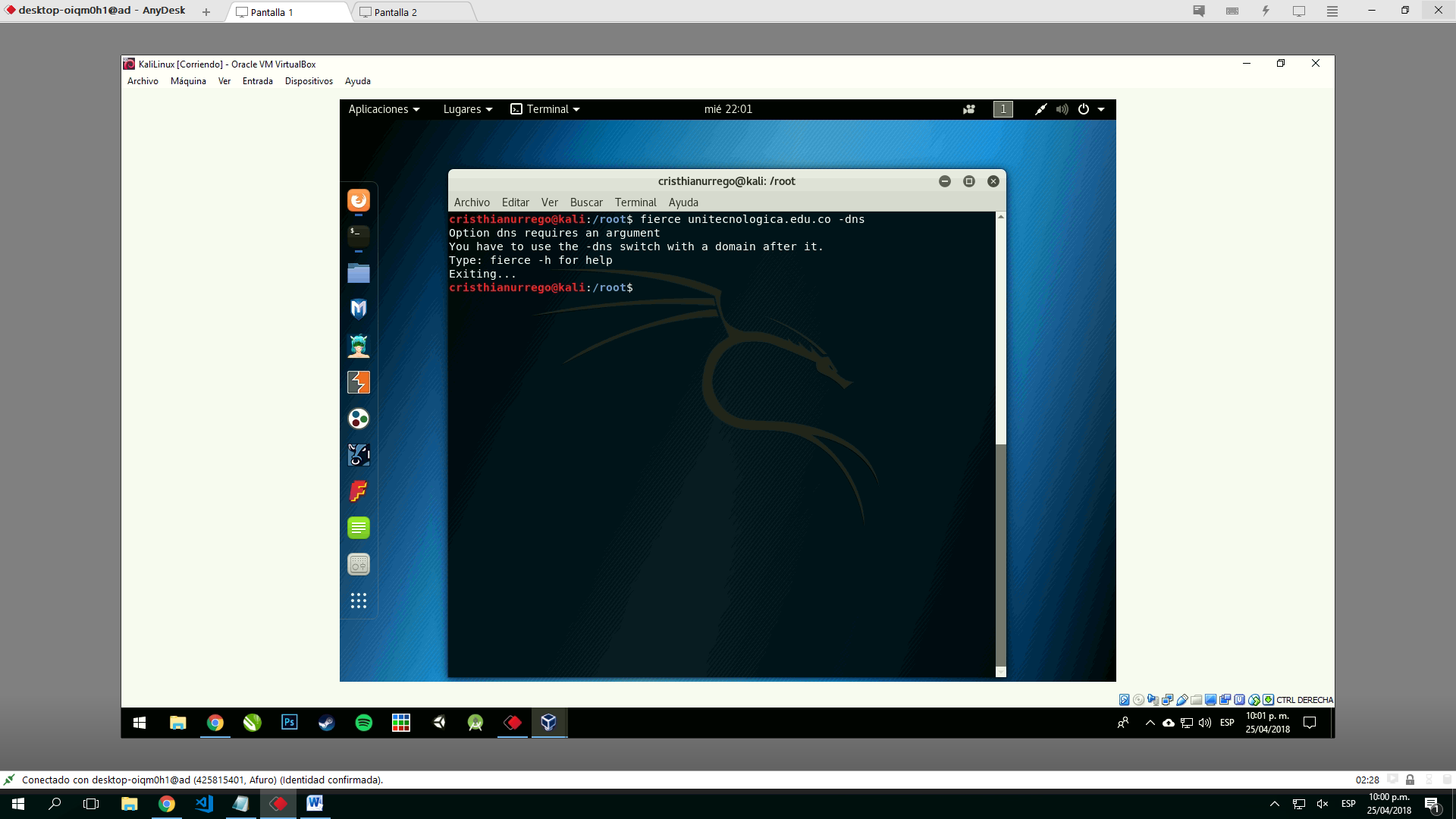
1. No se observa nada anormal



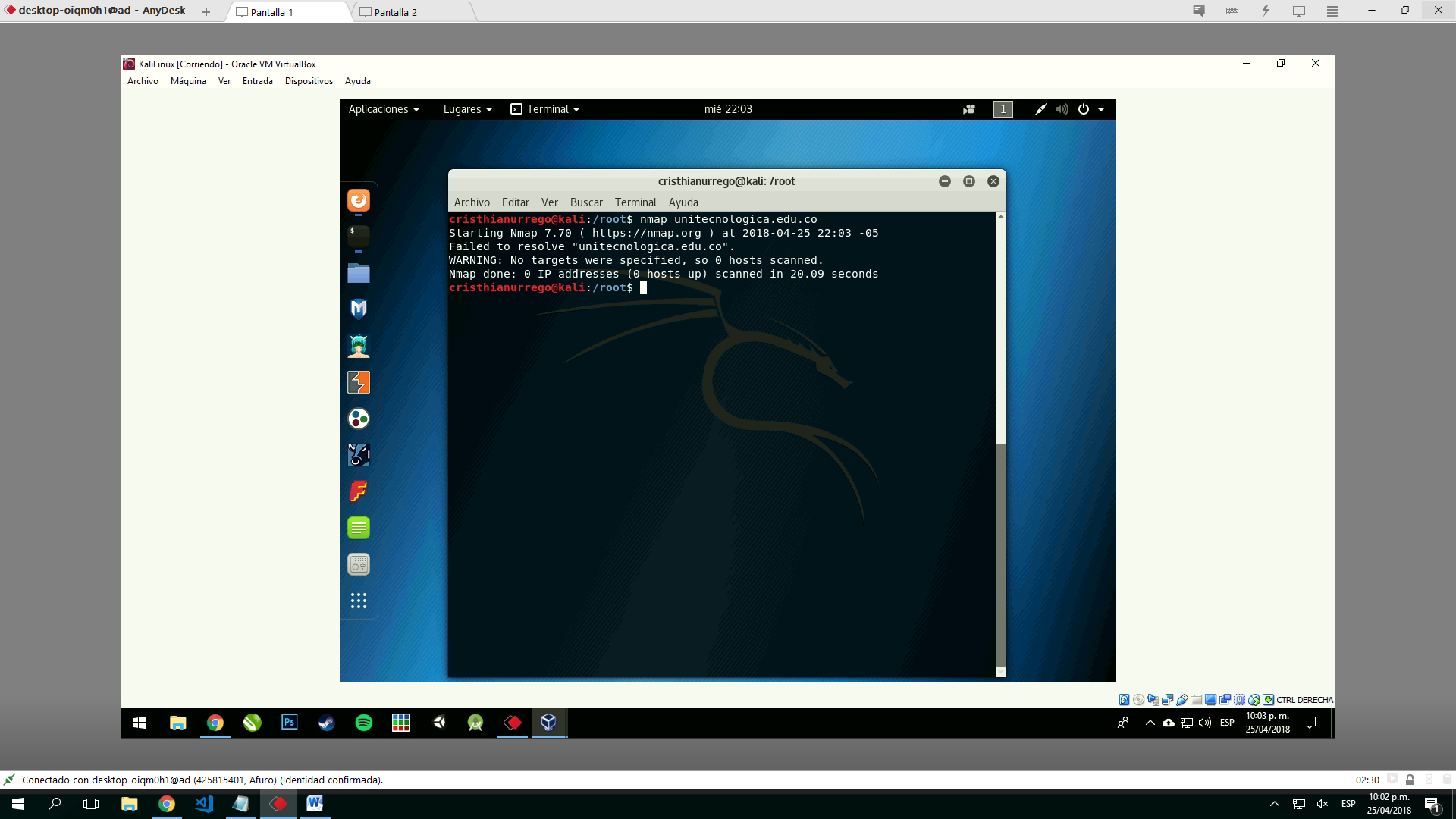
1. se obtiene la direccion de servidor he ip incluido el dominio, no se observa nada anormal
2. no se observa nada anormal



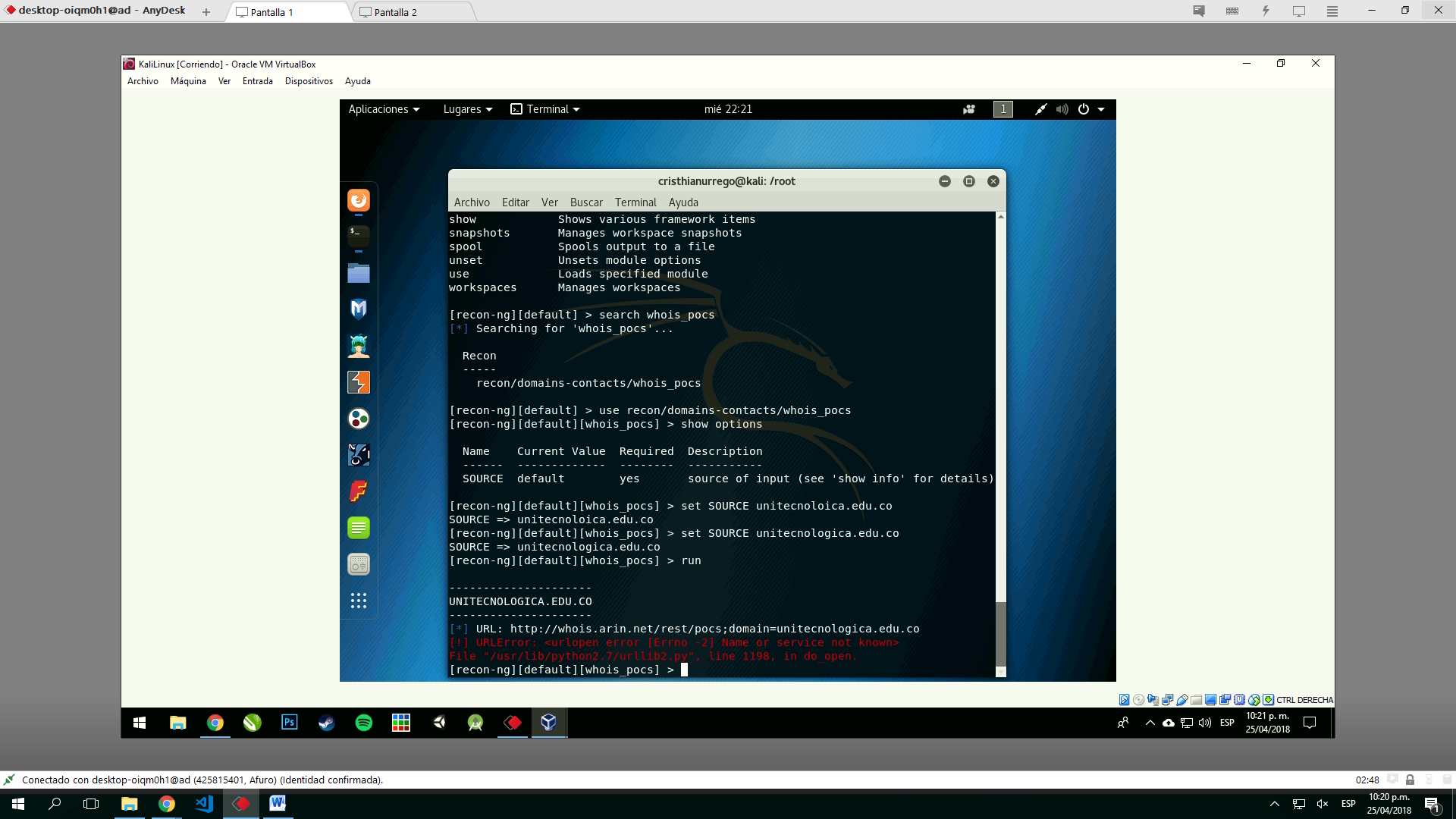
1. no se observa nada anormal



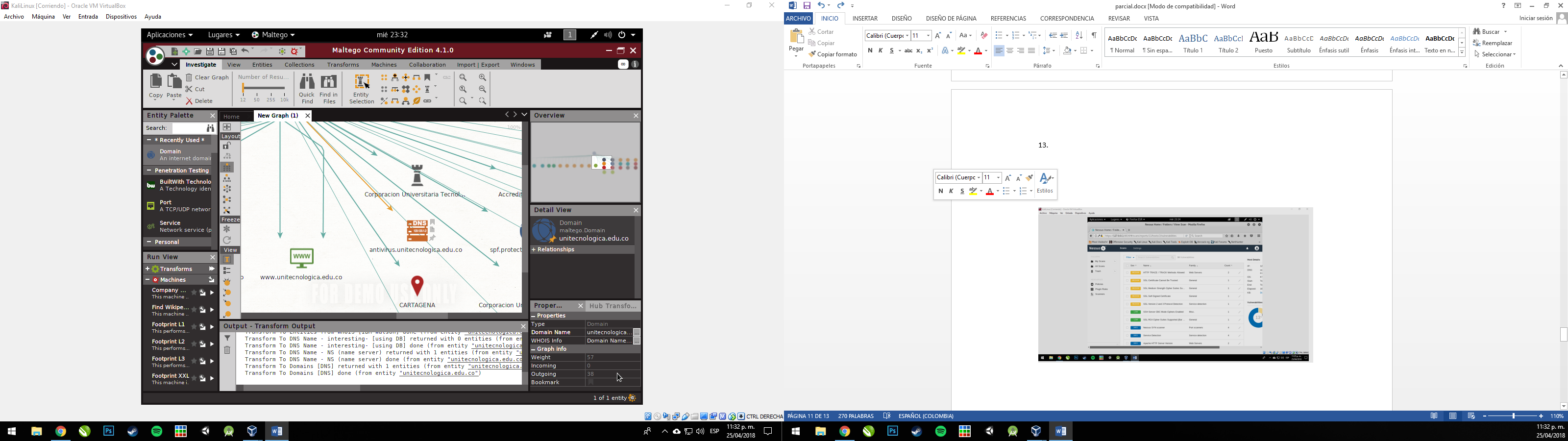
1. nmap no obtuvo resultados



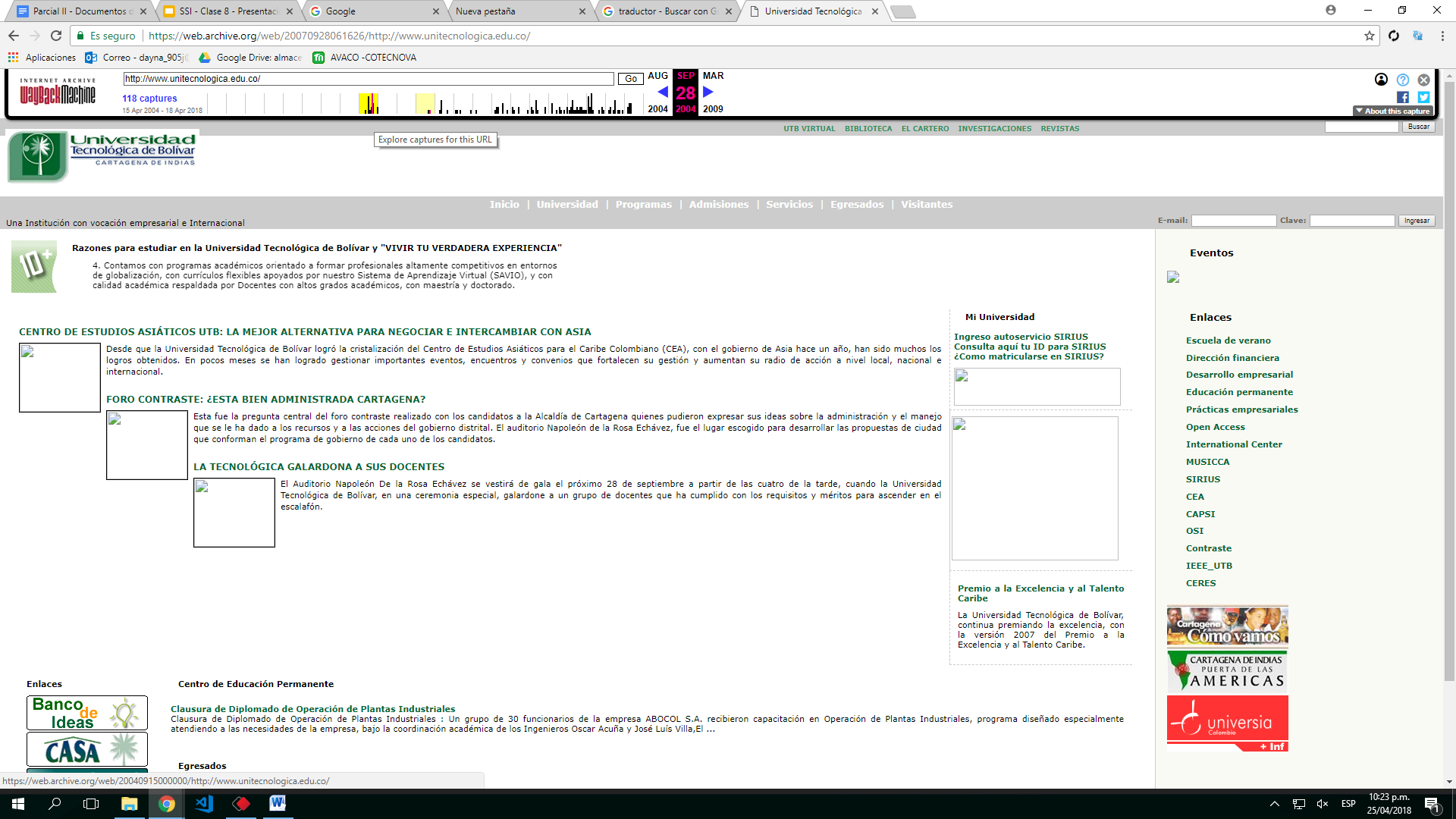
1. no permite el acceso



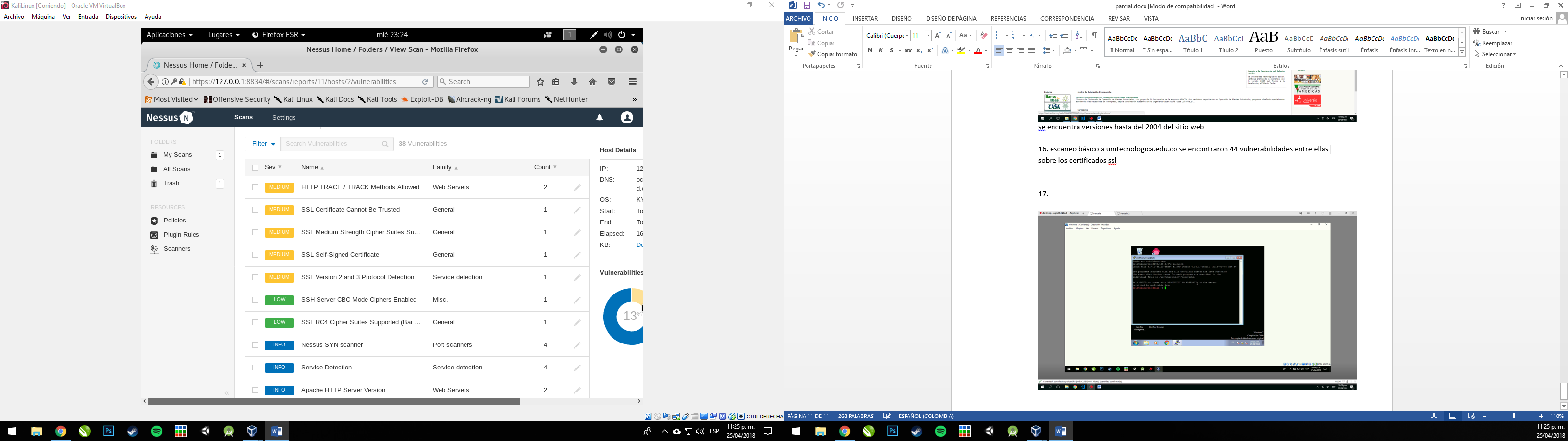
1. utilizando maltengo se obtuvo mayor información que hasta ahora con otras herramientas pero se concluye que no es información sensible, se encuentran algunas cuentas de correo institucionales y teléfonos de la universidad



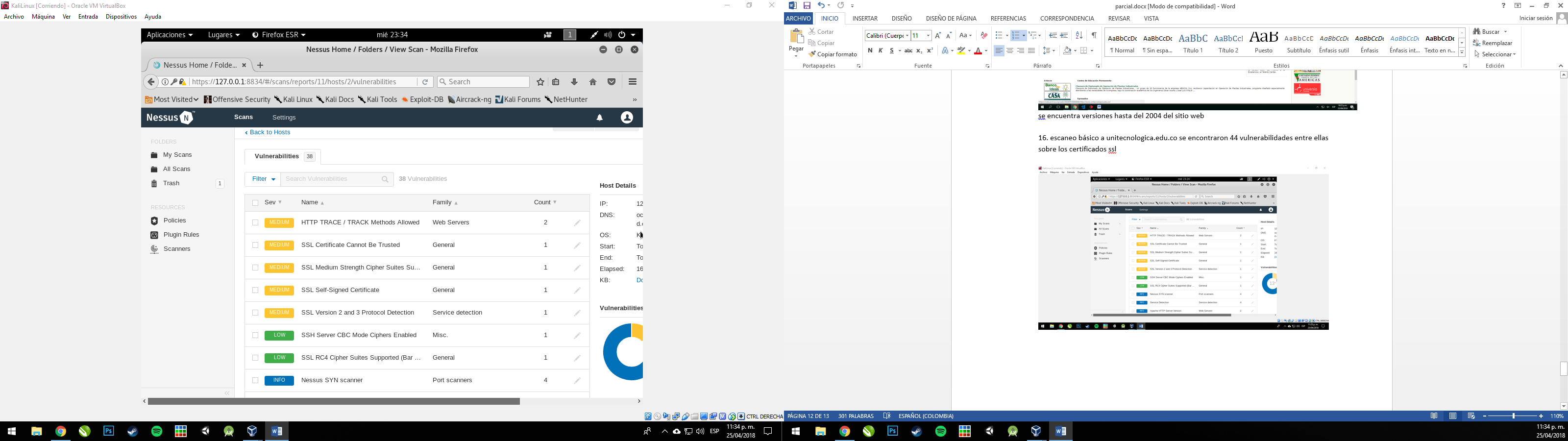
15.

se encuentra versiones hasta del 2004 del sitio web

16. escaneo básico a unitecnologica.edu.co se encontraron 44 vulnerabilidades entre ellas sobre los certificados ssl

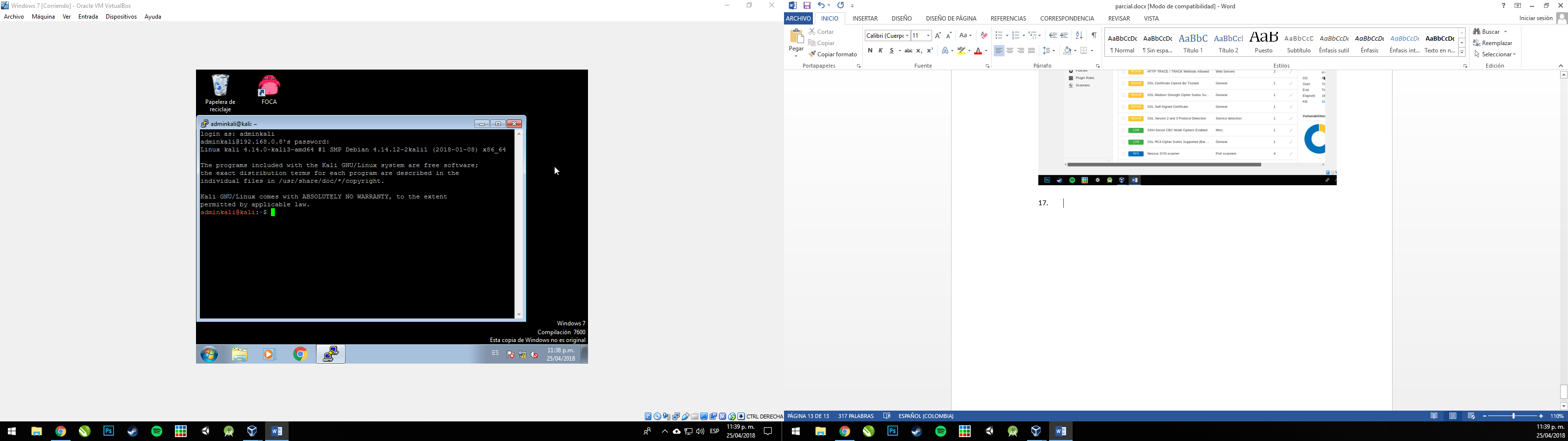


Con el escaneo avanzado se obtiene la misma cantidad de información del sitio de la universidad



17.

Se realiza la conexión a través de putty a la maquina linux



18.

**Funcionamiento cifrado de mensajes**

Clave privada del

emisor

Clave privada del

receptor

19.

|  |  |
| --- | --- |
| Cuadro comparativo | |
| Información más importante | La información mas relevante que obtuvimos de e taller fue que la pagina utiliza una muy buena seguridad ante los ataques que le puedan efectuar. |
| Con que herramientas las obtuvo | Shodan, Email harvesting, whois, host, dnsenum, dnsmap, nslookup, fierce, dig.  Putty |

20.

Obtención definición:

Es la forma en que se procesa, almacena y organiza para su posterior uso por los órganos de elaboración durante la producción de inteligencia.

Enumeración de sistema:

Es un conjunto de símbolos y reglas de generación que permite construir todos los números válidos.

Vulnerabilidad de sistema:

Se puede considerar como debilidad de cualquier tipo afecta y compromete la seguridad de un componente tecnológico.

Explotación de vulnerabilidades:

Se considera como algo que afecta indefinidamente de veces la seguridad de algún programa.

Post-explotación de vulnerabilidades:

Recurso para identificar amenazas informáticas, noticias de interés etc.

21.

Recomendaciones serian pocas sobre la seguridad de la pagina ya que consta con muy pocas vulnerabilidades y algo en constatar son las vulnerabilidades del tipo administrativo ya que cuenta con vencimiento.