|  |
| --- |
| corporacion de estudios tecnologicos del norte del valle |
|  |
| Ataque informático de manera educativa |
| SEGURIDAD EN SISTEMAS DE INFORMACION |
|  |
| **Elkin Ramírez**  **Lorena Sánchez** |
| **18/05/2018** |

|  |
| --- |
| Ataque informático realizado con fines educativos |

Contenido

[1. Introducción . 2](#_Toc514452961)

[1.1 Objetivo 2](#_Toc514452962)

[1.1.1 Alcance 2](#_Toc514452963)

[1.1.2 Objetivos específicos 2](#_Toc514452964)

[2. Resumen ejecutivo 3](#_Toc514452965)

[2.1 Pruebas realizadas 3](#_Toc514452966)

[2.2 Resultado de pruebas 3](#_Toc514452967)

[3. Conclusiones 11](#_Toc514452968)

[3.1 Vista técnica . 11](#_Toc514452969)

[3.2 Vista personal 11](#_Toc514452970)

[4.1 Realizar el cambio de las contraseñas . 12](#_Toc514452971)

1. Introducción   
     
   El presente trabajo comprende el ataque informático que se le realizo de manera educativa a una máquina virtual con vulnerabilidades, para así poder obtener un listado de las vulnerabilidades, usando comandos diferentes para obtener información de dicha máquina.  
   1. Objetivo

Determinar si el Windows xp esta preparado para resistir y detectar un ataque informático desde una red externa.

* + 1. Alcance  
         
       Comprobar las vulnerabilidades en sistema operativo Windows xp
    2. Objetivos específicos
* Conectar por medio de la ip con la maquina
* Obtener información del estado de la maquina
* Realizar la búsqueda de los usuarios

1. Resumen ejecutivo

Las pruebas de penetración tienen como objetivo analizar las vulnerabilidades que tiene el sistema operativo Windows xp , realizándole un ataque informático desde una maquina kali linux.

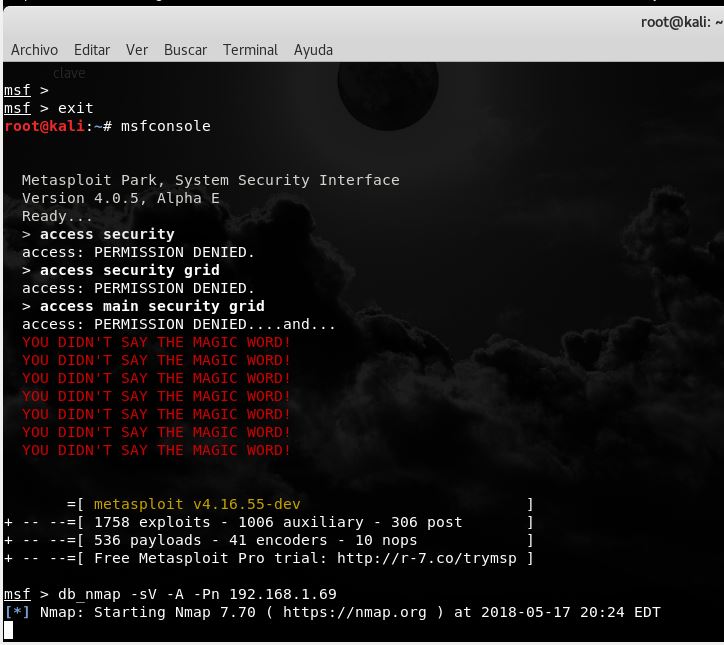
* 1. Pruebas realizadas
* Las pruebas se realizaron mediante los servicios de openvas y postgresql, posterior a eso ingresamos a el metasploit , usando nmap y por medio de la ip logramos ver el estado de la máquina, que sistema operativo es y nos deja visualizar el cliente.
* Ya teniendo acceso y manejo del equipo podemos consultar los servicios por medio del comando “service” , nos muestra los servicios enumerados por la ip de la computadora Windows , los puertos abiertos y que servicio están corriendo por ellos .
* Con el comando “search netapi” podemos visualizar los modulos de la máquina.
* En metasploit utilizamos el use exploit en Windows para poder ingresar y ver los payloads que hay en la máquina.
* Por medio del comando dir en el meterpreter se nos lista los estados con sus respectivos permisos , puertos etc.
* Procesos adicionales  
  1. Resultado de pruebas
* Habilitación de servicios openvas y postgresql , iniciamos el metasploit por medio de mfs console, usamos nmap para conectarnos con la maquina a través de la ip y observar sus estados.  
  

Ilustración 1 openvas, postgresql e iniciación de metasploit

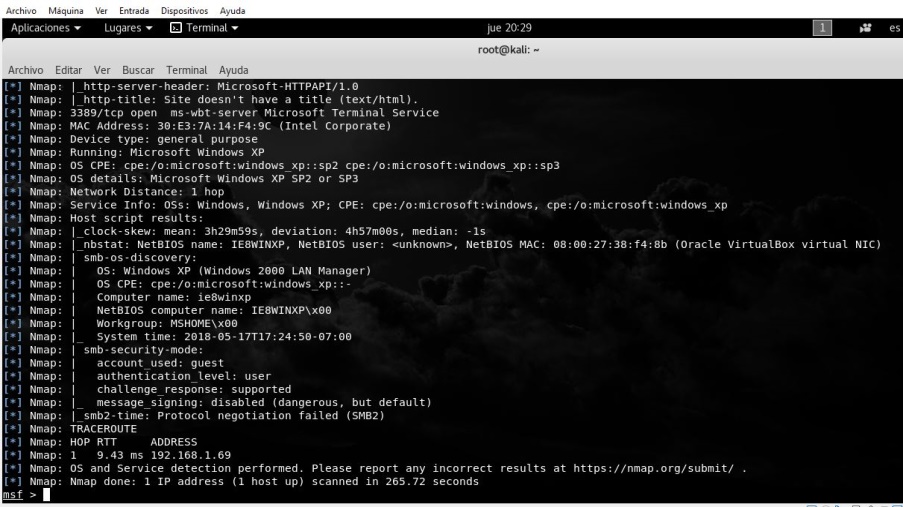


Ilustración 2 Consulta nmap



Ilustración 3 Consulta cliente

* Puertos abiertos y que servicios están corriendo por ellos  
  

Ilustración 4 Service host

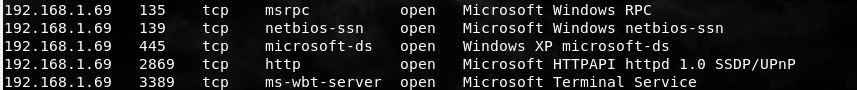


Ilustración 5 Puertos y servicios

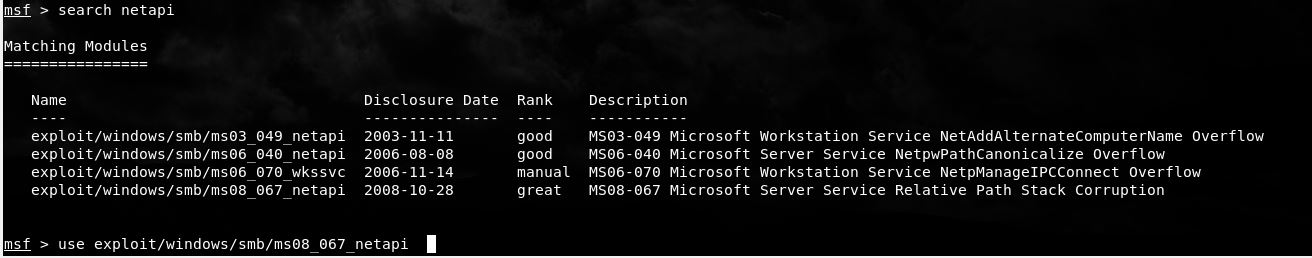
* Módulos de la maquina  
    
  

Ilustración 6 Módulos de la maquina

* Visualización de los Payloads  
    
  

Ilustración 7 Payload 1

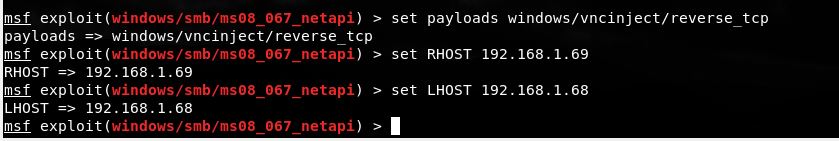
En metasploit utilizamos el use exploit en Windows para poder ingresar y ver los payloads que hay en la máquina.  


Ilustración 8 Payload 2

En esta parte le decimos al kali Linux que ataque tipo reverse a la dirección RHOST 192.168.1.69 desde la dirección LHOST 192.168.1.68

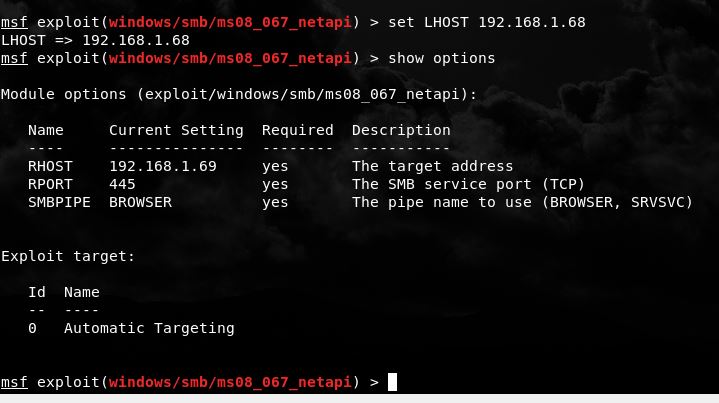
Después de ello me mostrara los servicios   


Ilustración 9 Payload 3

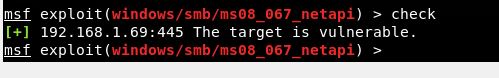
Realizamos un cuequeó para saber si la maquina es vulnerable o no, para esto utilizamos el comando check  


Ilustración 10 Payload 4

Después de haber hecho los análisis realizamos un check para saber si la quina es vulnerable.

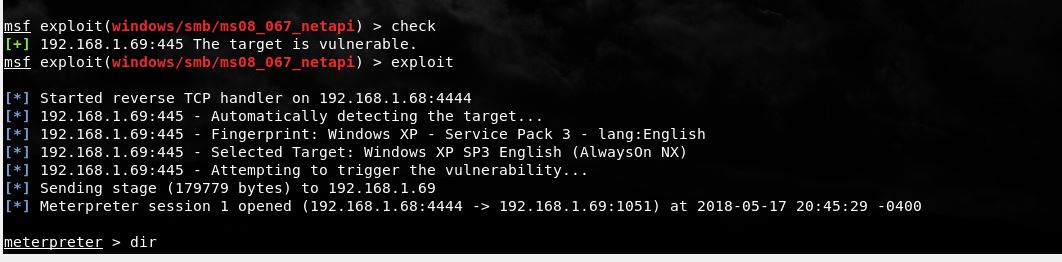
Efectivamente Lo es.  


Ilustración 11 Payload 5

visualización de vulnerabilidades.

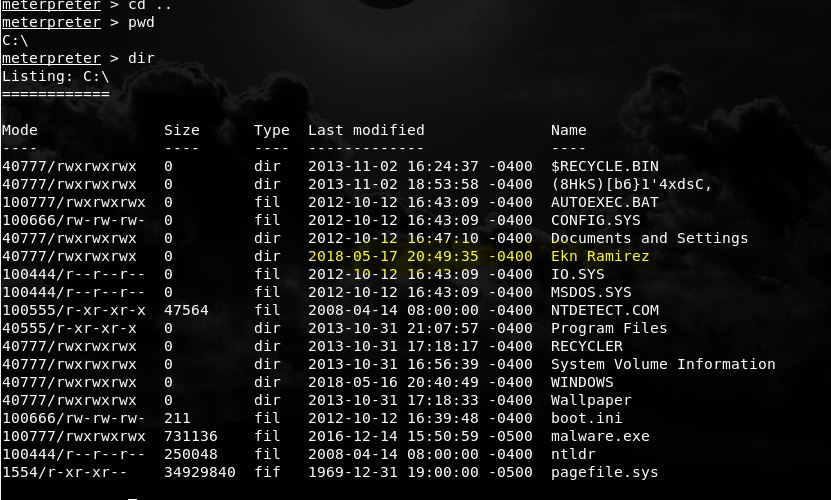
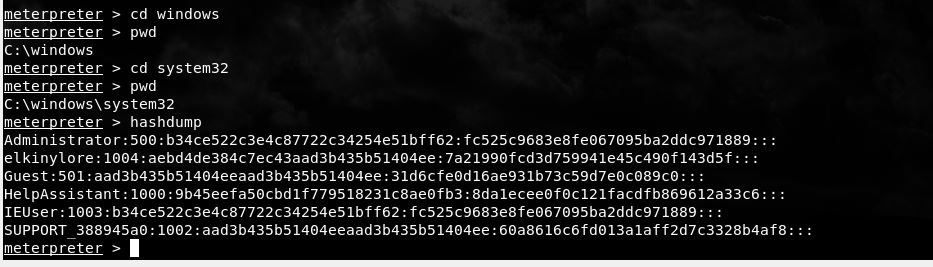
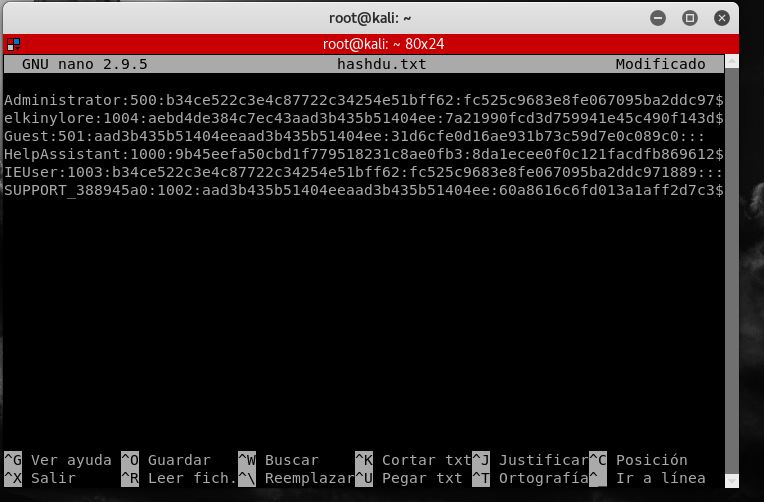
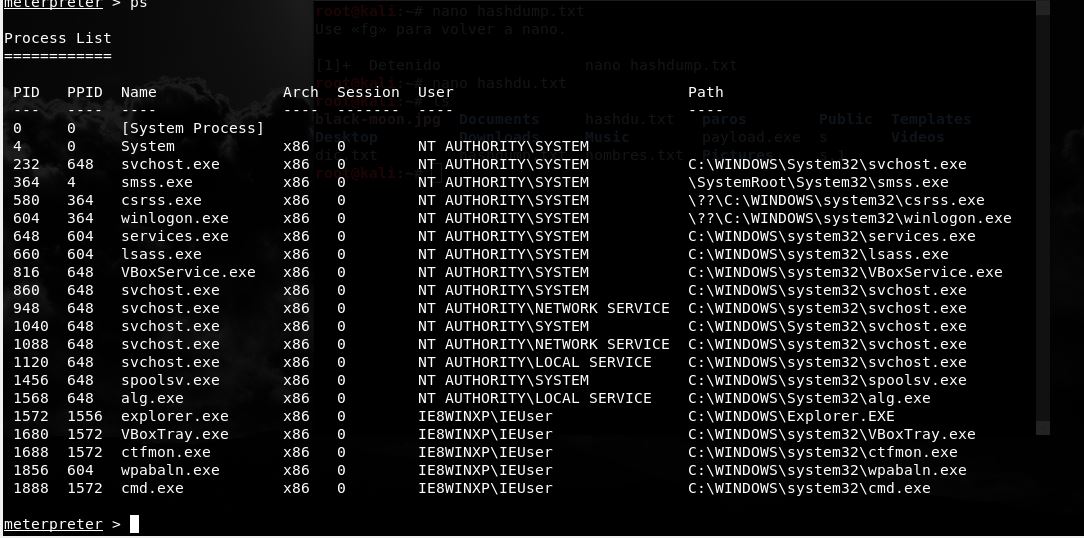
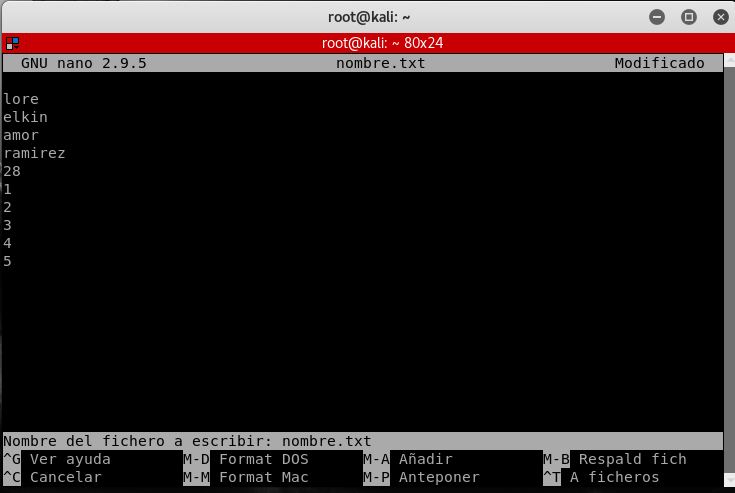
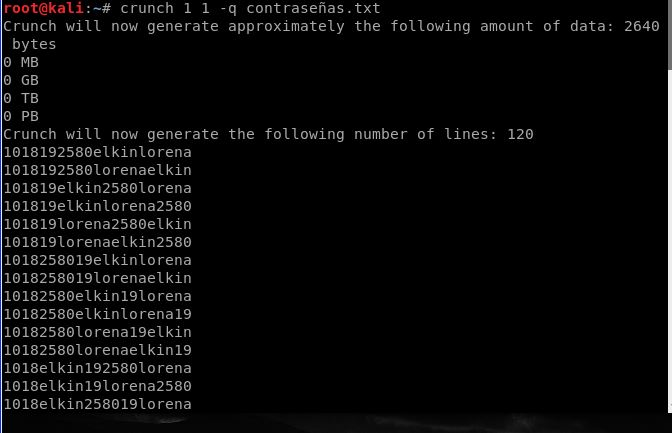
* Uso del dir listar los estados con sus respectivos permisos , puertos etc.  
  

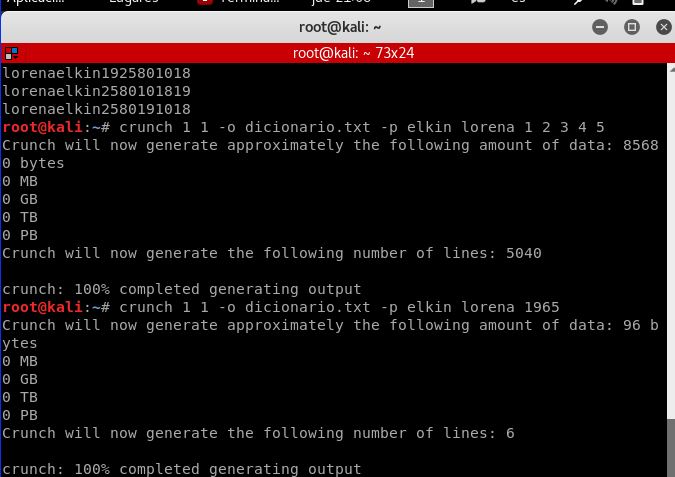
Ilustración 12 Uso del dir

Volvemos a la máquina de Windows y creamos una archivo nuevo en la máquina virtual, en este caso en el disco local C creamos una carpeta con el nombre Ekn Ramírez, volver a realizar el listado por medio del comando de meterpreter Dir y podemos visualizar el nuevo documento ya listado.

* Procesos adicionales  
  Ingresamos a Windows por medio de pwd y realizamos un hashdump en el sistema y nos arroja los nuevos o antiguos usuarios que posee el sistema , en este caso creamos en la máquina virtual de windows un usuario llamado elkinylorena, también nos arroja la contraseña en forma codificada.

También nos arroja los demás usuarios ocmo Administrador, su respectiva contraseña, asi como IEUSER y Helpasistent lso cuales son propio del sistema operativo Xp.  
  
  
  


Dentro de este sudo o editor vamos a crear un diccionario de datos que ya supuestamente conocemos del sistema que deseamos vulnerar.  
  
Creamos el diccionario de datos.

Creamos diccionario nuevo puesto que el otro que llamamos nombres.txt nos daba un diccionario de 36420 posibles contraseñas , el cual lo cambiamos por este llamado contraseñas.txt el cual nos arroja un total de 2640 posibles contraseñas, basadas en todas las combinaciones posibles por el diccionario de datos.  


1. Conclusiones
   1. Vista técnica   
        
      El acceso a internet tiene ventajas como lo son acceso a información entrenamiento entre otros, pero también pone en riesgo su integridad como persona, empresa u organización, ya que si no se protege o no cierran los puertos de accesos a los equipos pueden verse enredados en un mal momento si no se detecta a tiempo.
   2. Vista personal

Con esta actividad de ataque informativo podemos concluir que hay muchas manera de vulnerar la información de cualquier persona desde su ordenador personal con el solo hecho de conéctanos a una red ya se de nuestros hogares, si no se tiene las precauciones necesarias para no caer en este proceso relativamente sencillo ya que se puede obtener información de cualquier persona y hacer uso malicioso de ella.

1. Anexos
   1. Realizar el cambio de las contraseñas   
       Se puede filtrar información personal en las tareas realizadas, puede quedar el rastro del equipo y nos pueden realizar un daño a nosotros mismos.