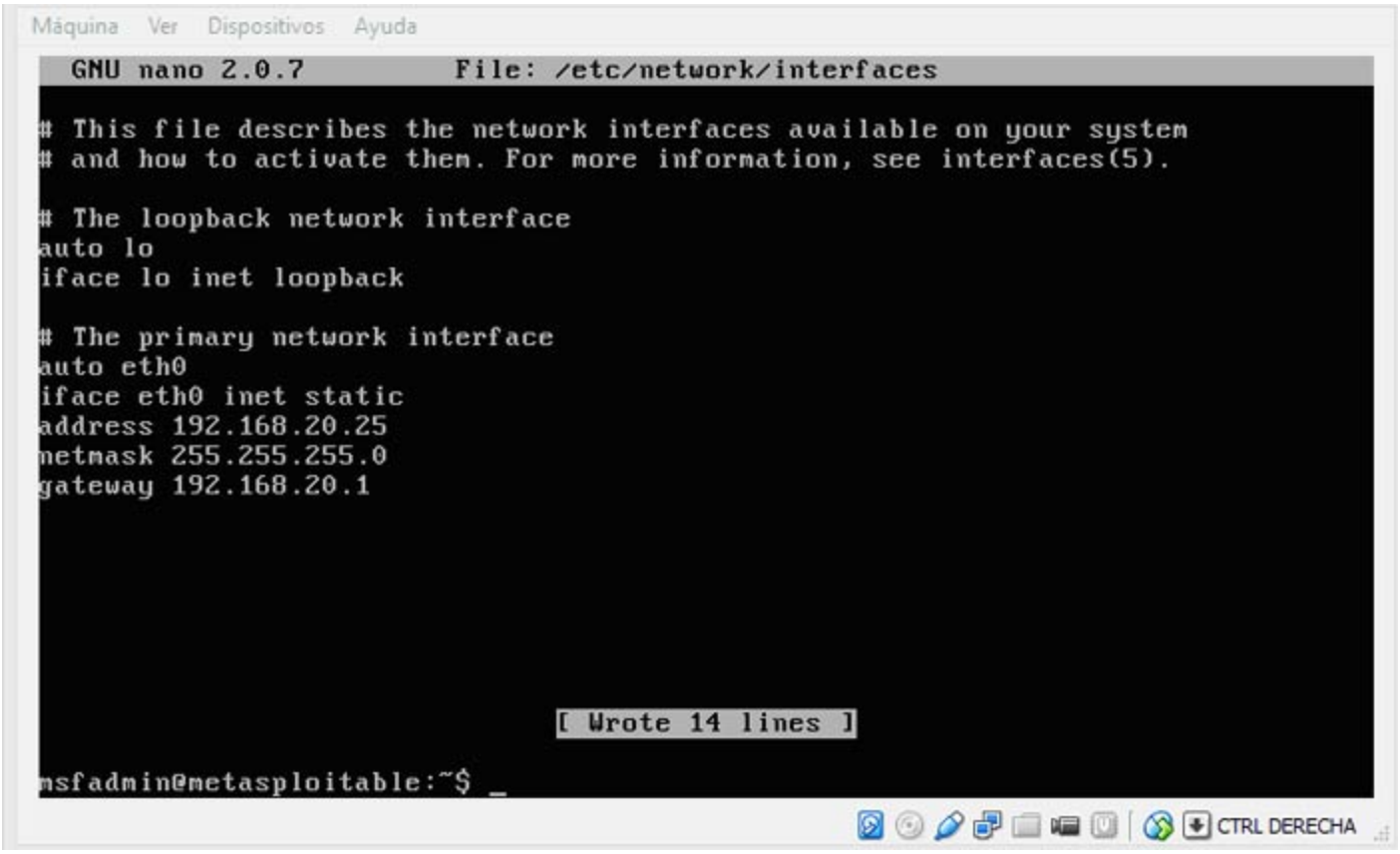
MetaSploit, tomar control de equipos remotos

MetaSploit es una suite o conjunto de programas en realidad. Está diseñada para explotar las vulnerabilidades de los equipos y es sin duda el programa más usado por los mejores hackers del mundo. Dentro de MetaSploit, disponemos de multitud de herramientas y programas para ejecutar en las diferentes vulnerabilidades de cada equipo, a cada una de estas aplicaciones se le llama sploit.

Primero vamos a arrancar nuestra Kali Linux y le configuramos la red con una IP estática dentro del rango de red de la víctima con sudo nano /etc/networw/interfaces.

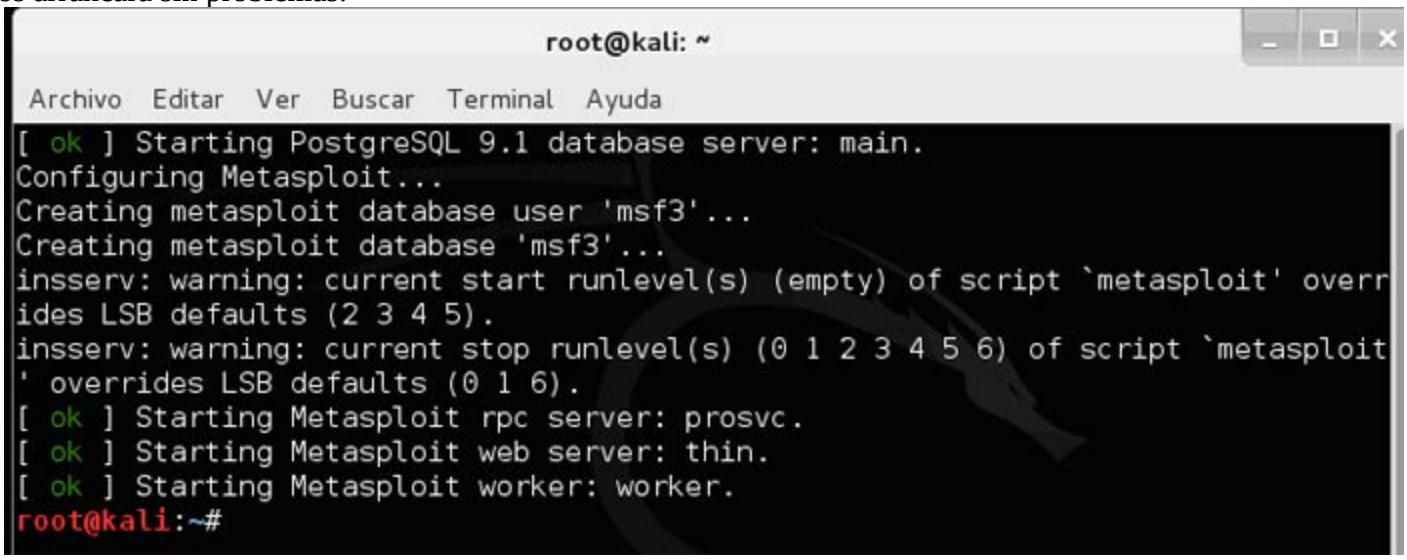


Cada vez que hagamos modificaciones de red, debemos reiniciarla. Si hacemos un ifconfig y sigue sin asignarnos la IP que le hemos puesto, reiniciamos Kali.

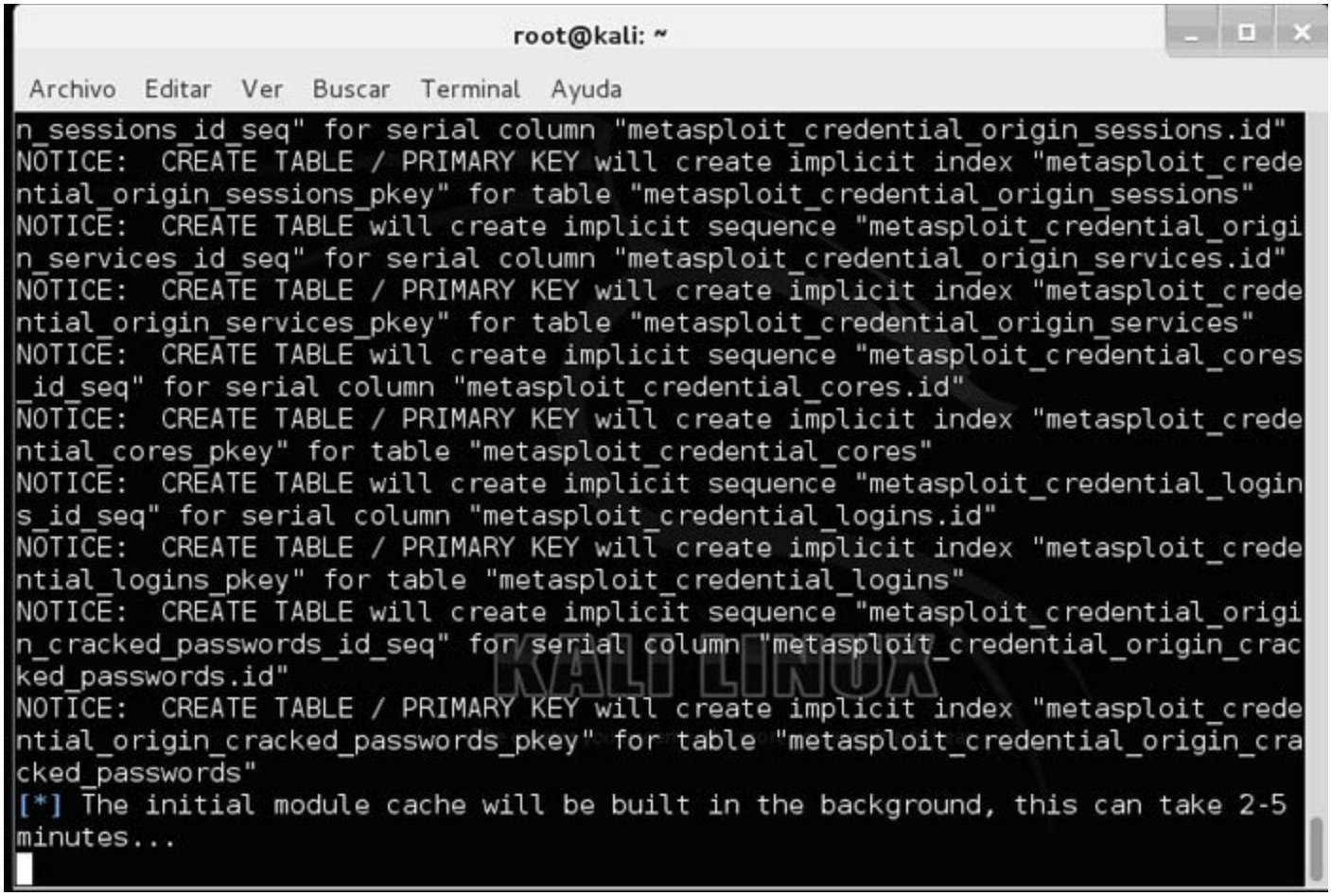
Ahora necesitaremos los logs de algún programa de detección de vulnerabilidades como el Nessus o el Openvas que hayamos usado anteriormente. Existe una guía sencilla de Nesus donde viene como obtenerlo paso a paso.

Abrimos Metasploit en Aplicaciones, Kali Linux, Servicios del sistema, Metasploit, Community pro start.

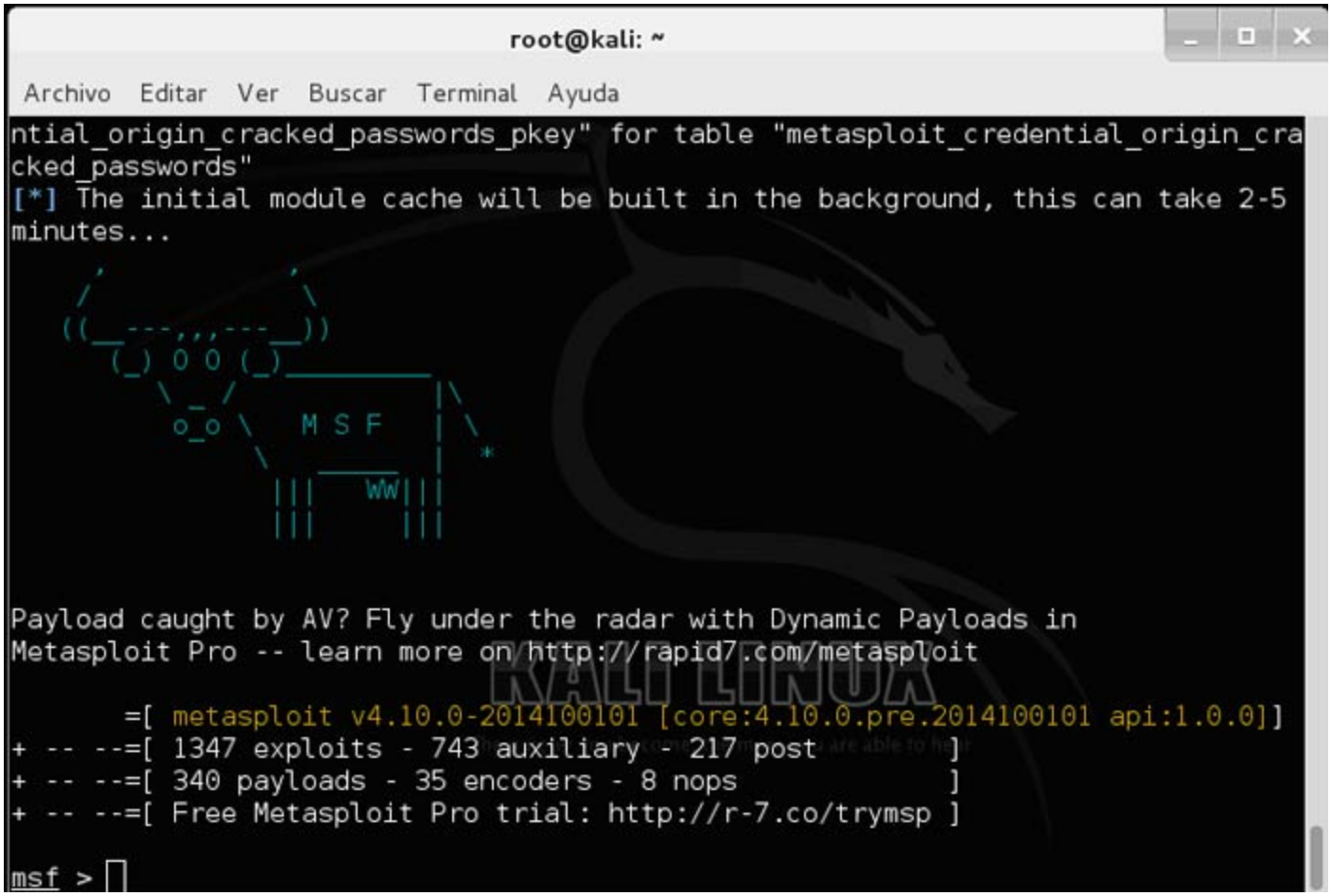
Nos arrancará sin problemas.



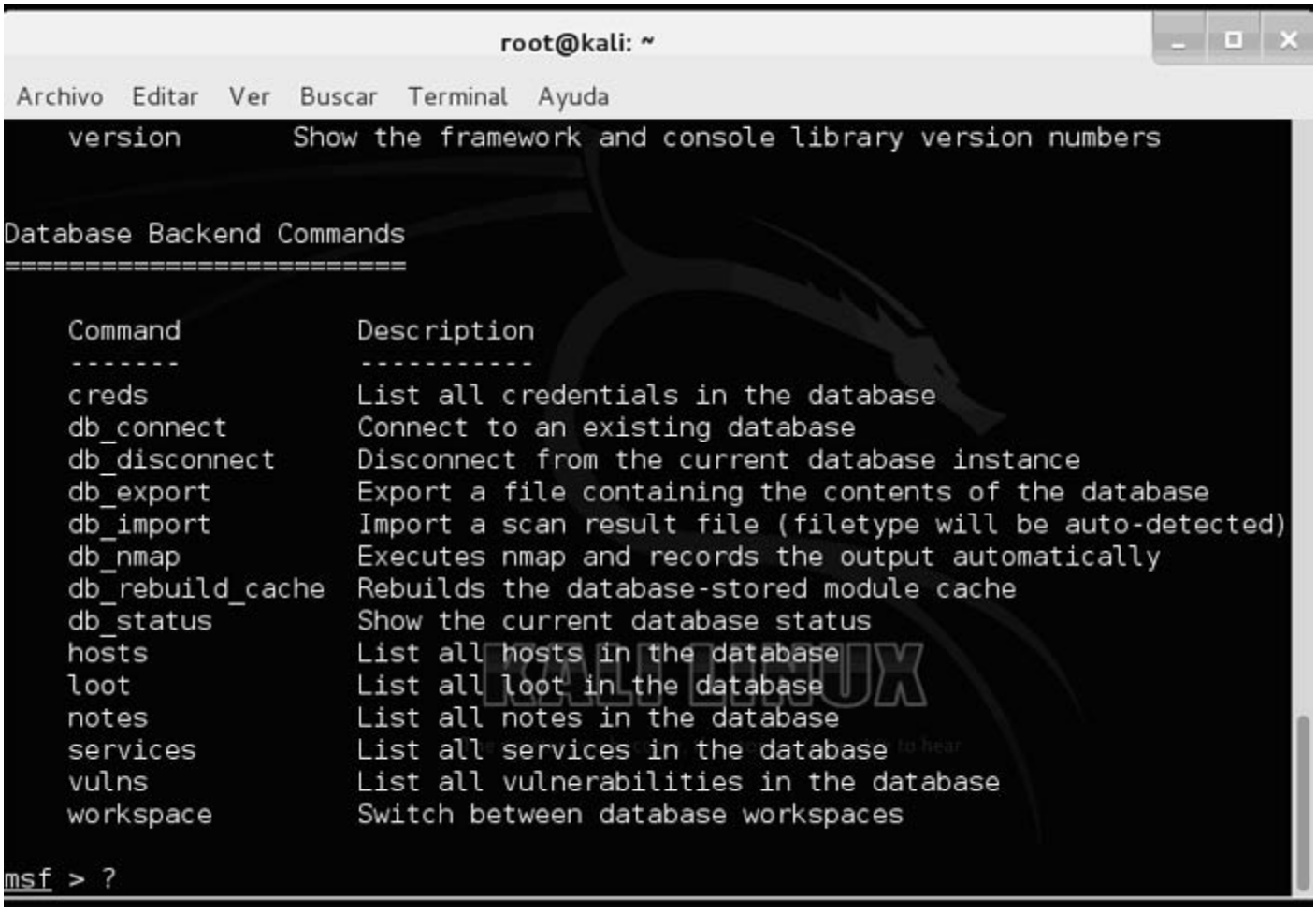
Ahora vamos a crear la consola msf o de Metasploit. Tardará un rato amplio, luego pasado unos minutos empezará a crear las tablas.



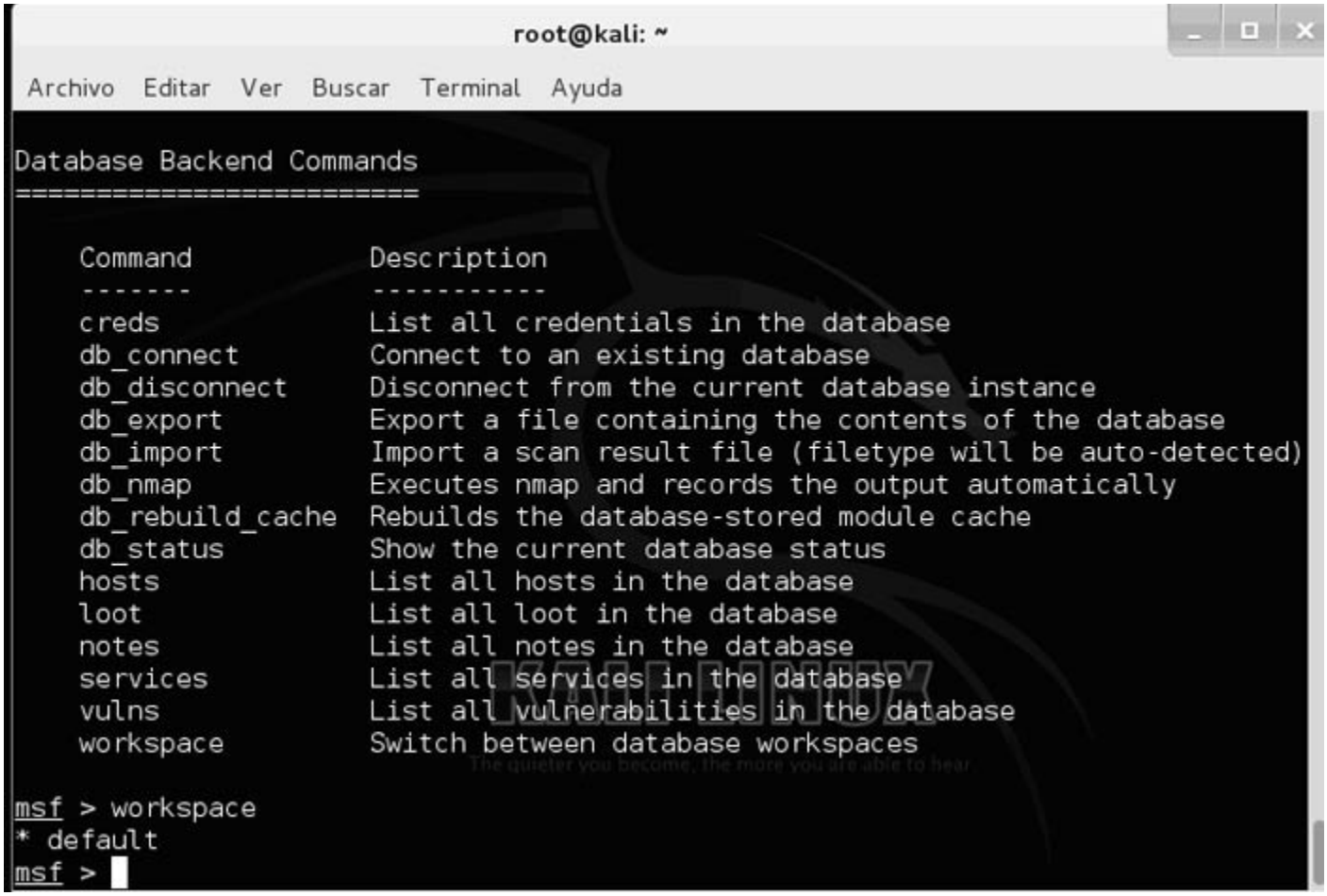
Y finalmente sale la línea de consola.



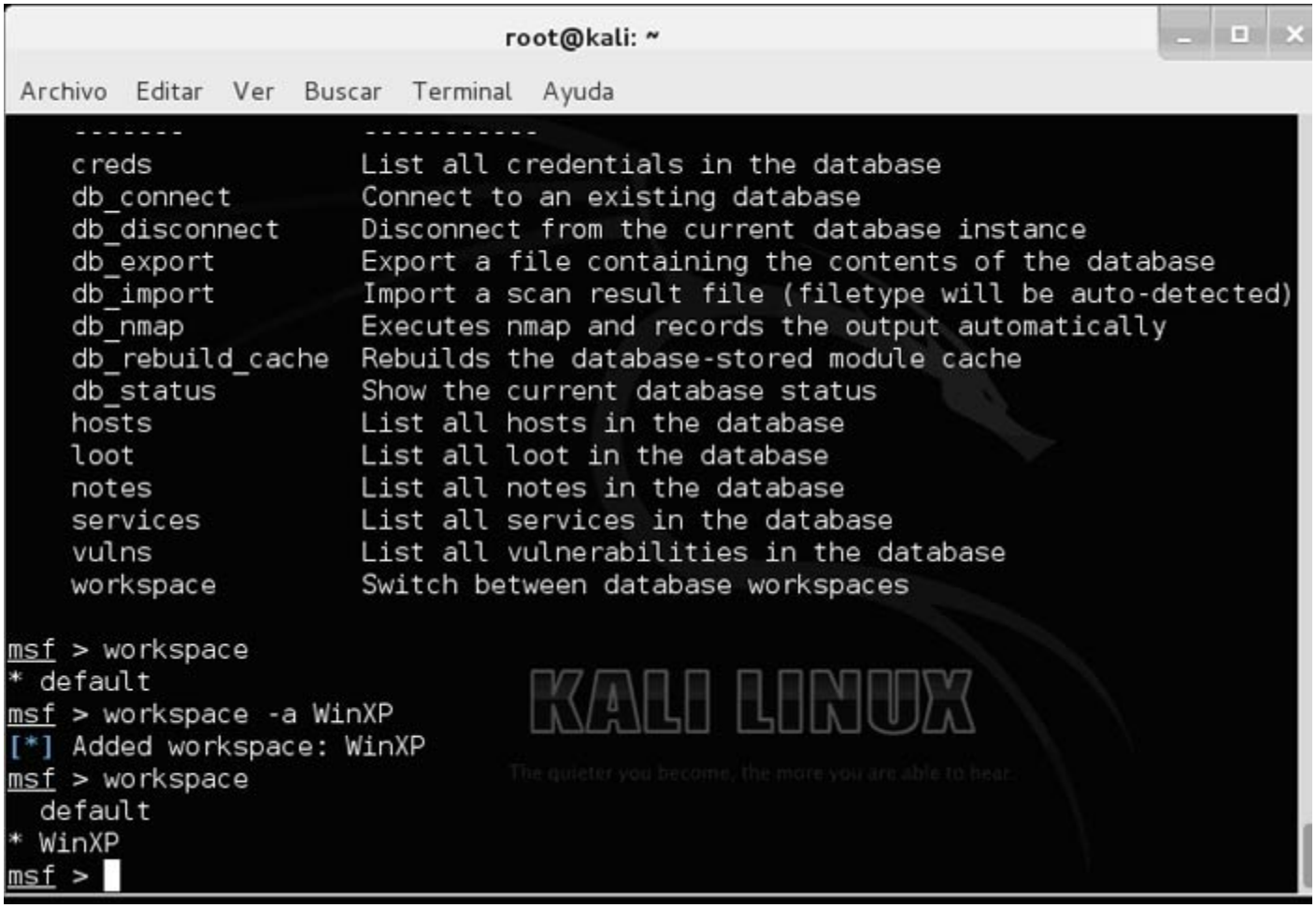
Para ver la lista de comandos usamos la interrogación hacia abajo.



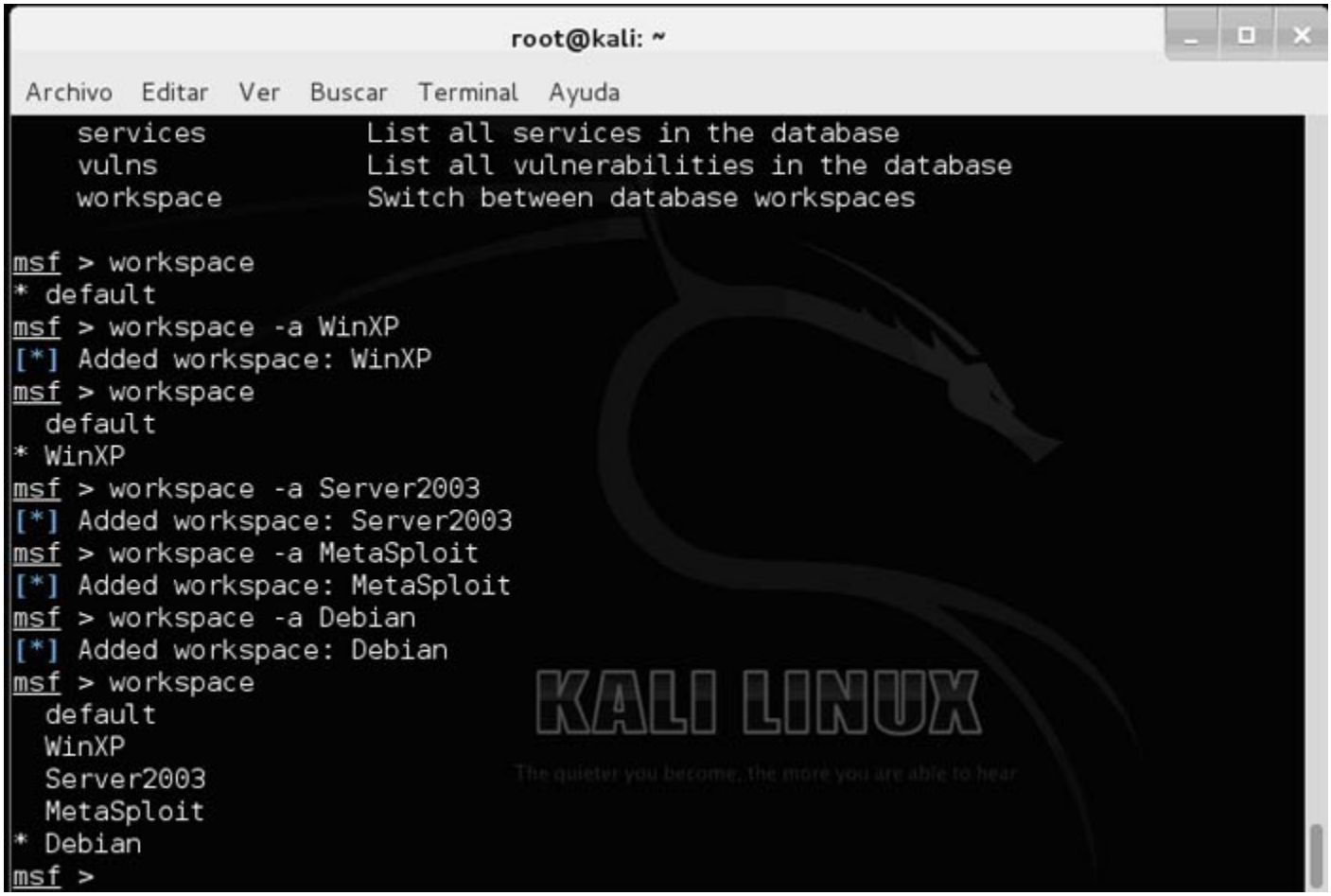
Una cosa importante son los Workspace o lugares de trabajo, si ejecutamos workspace, entra en nuestro entorno de trabajo por defecto.



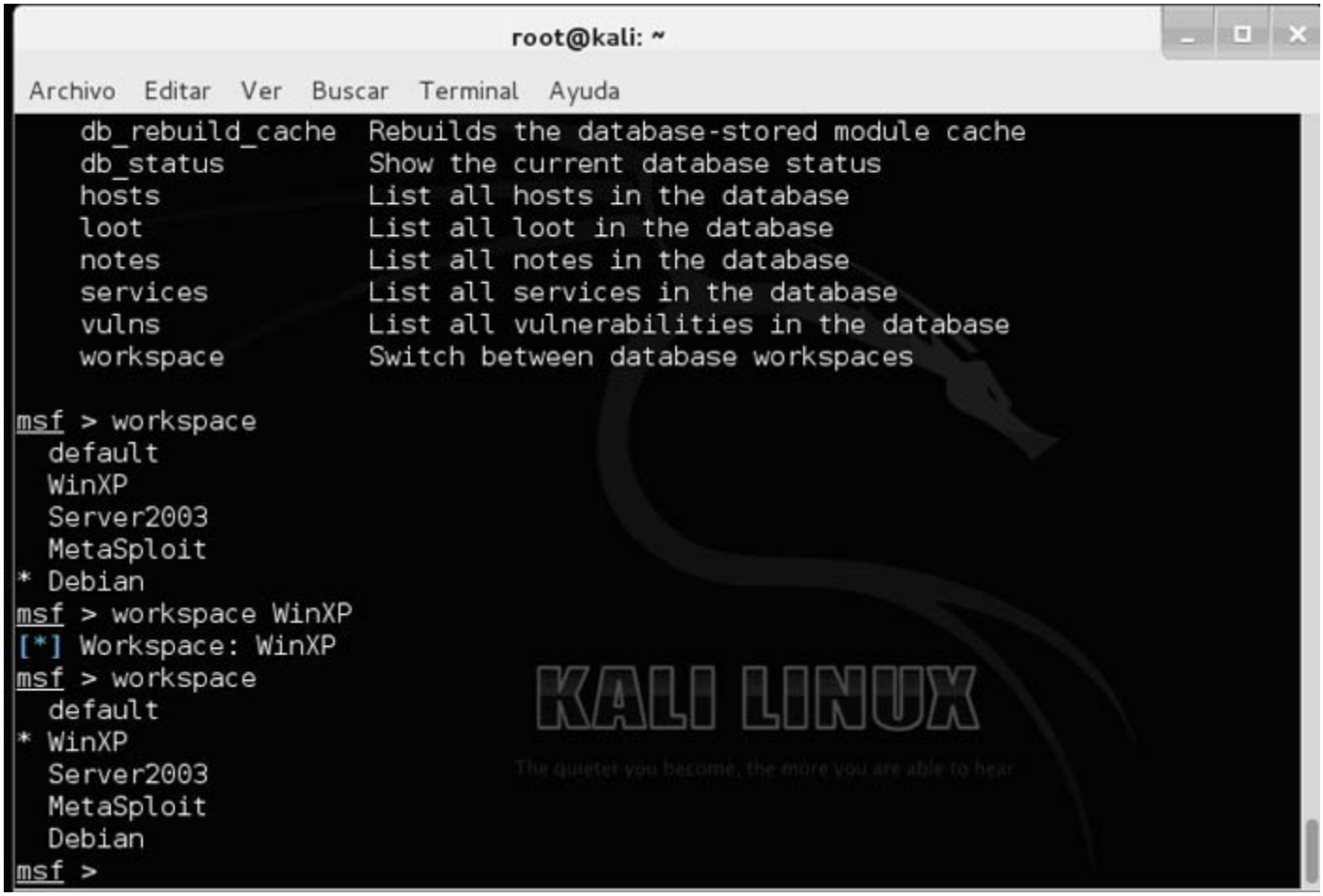
Creamos otro workspace para atacar un Windows XP y vemos que se ha creado. Para ello ponemos workspace –a WinXP.



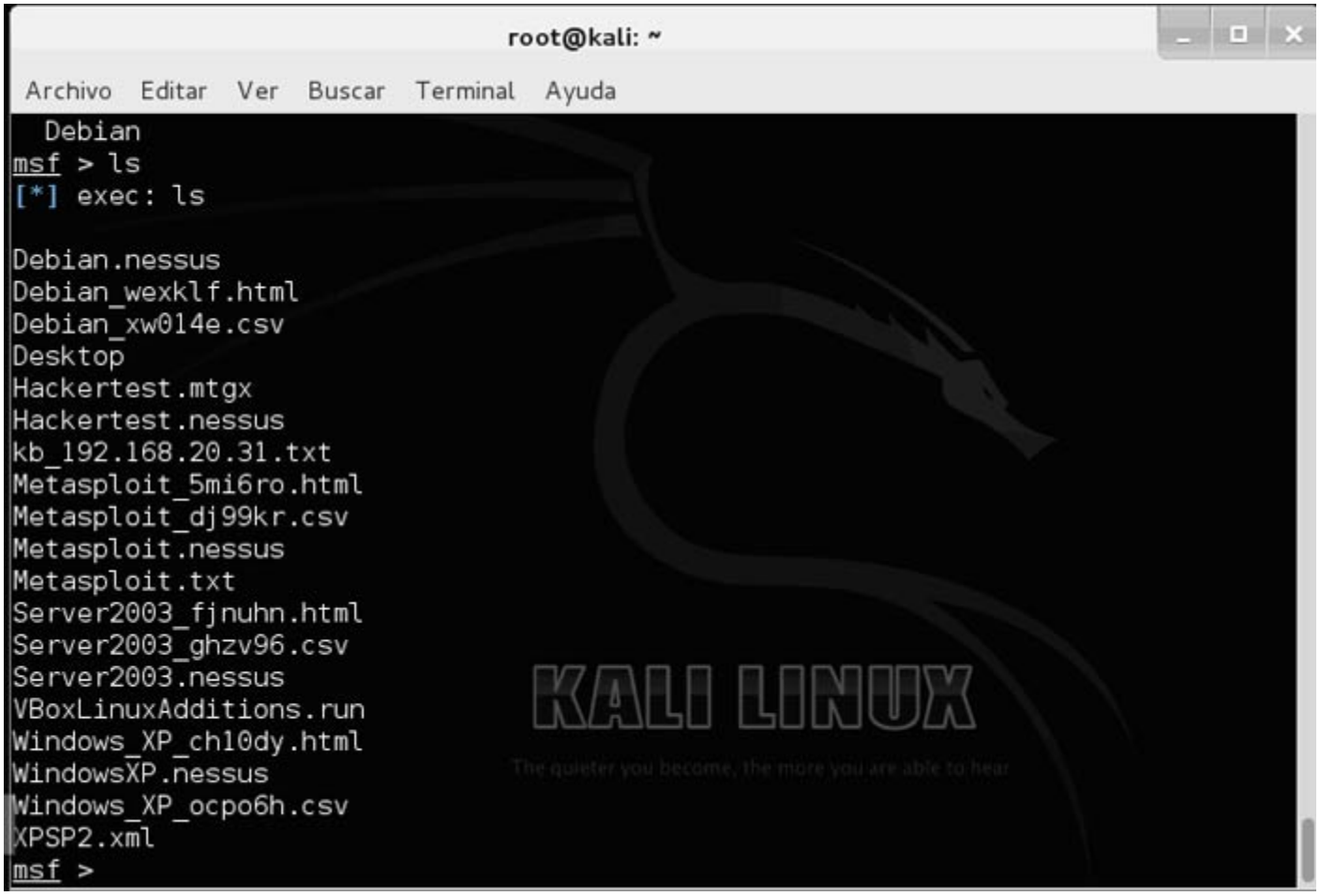
Creamos varios, uno por cada máquina virtual que tengamos y que queramos atacar.



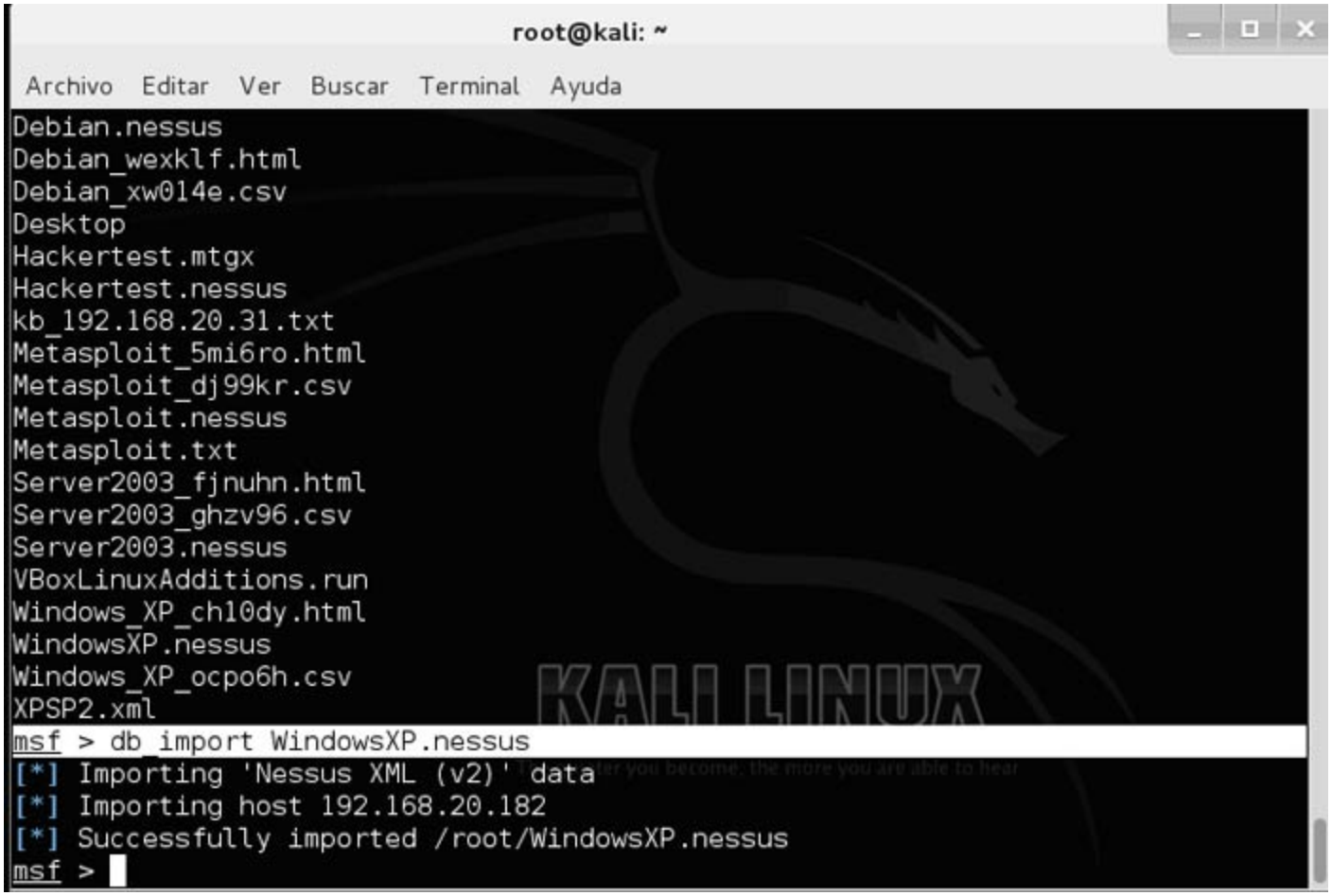
El asterisco marca el que está activo en este momento. Para cambiarlo se hace workspace y el nombre del workspace al que deseamos acceder.



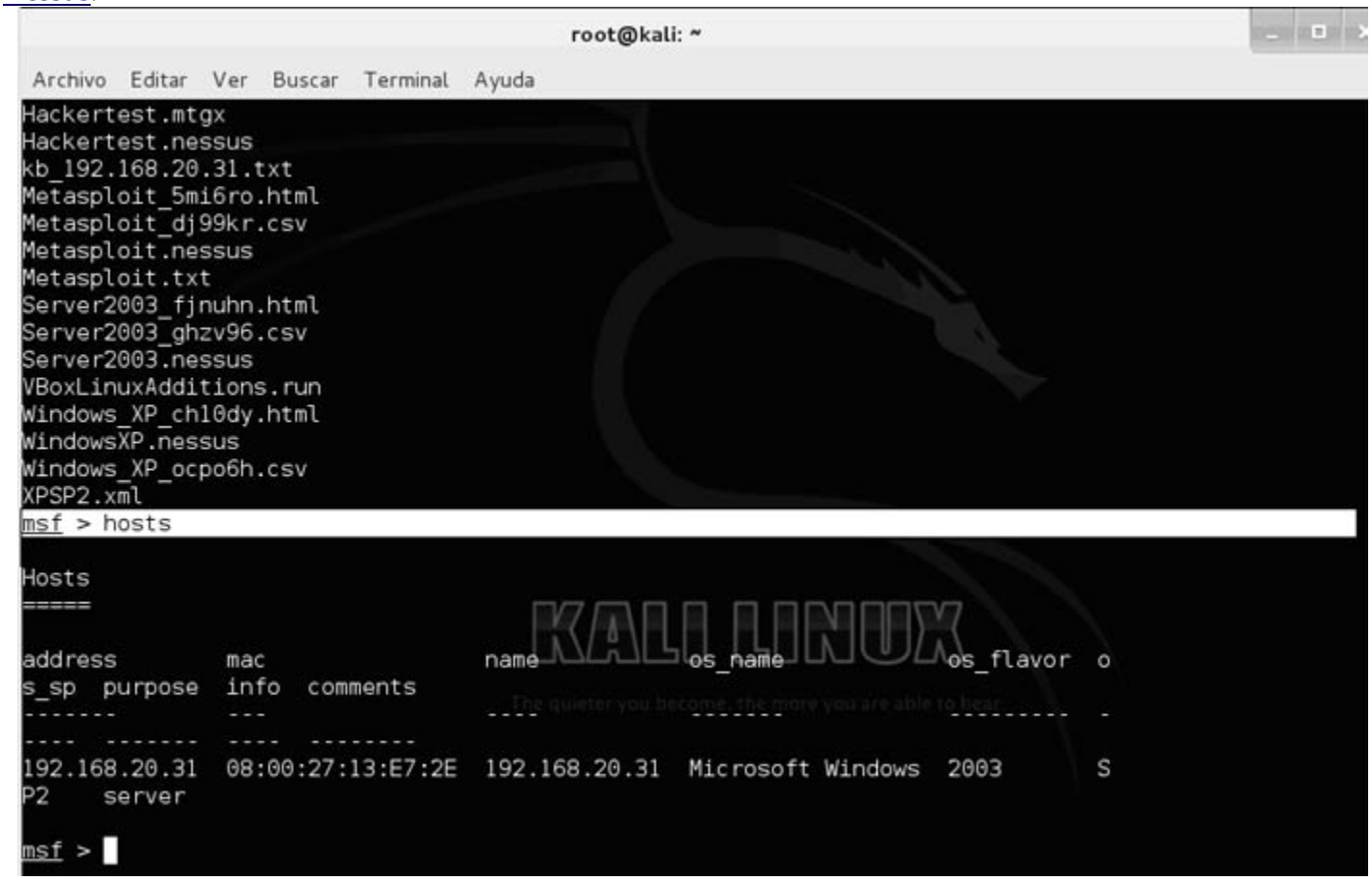
Damos un ls para ver el nombre de los archivos a importar del Nessus que salvé anteriormente. En este caso para no complicarme los metí en el Home del root, que es desde el directorio que me arranca Metasploit.



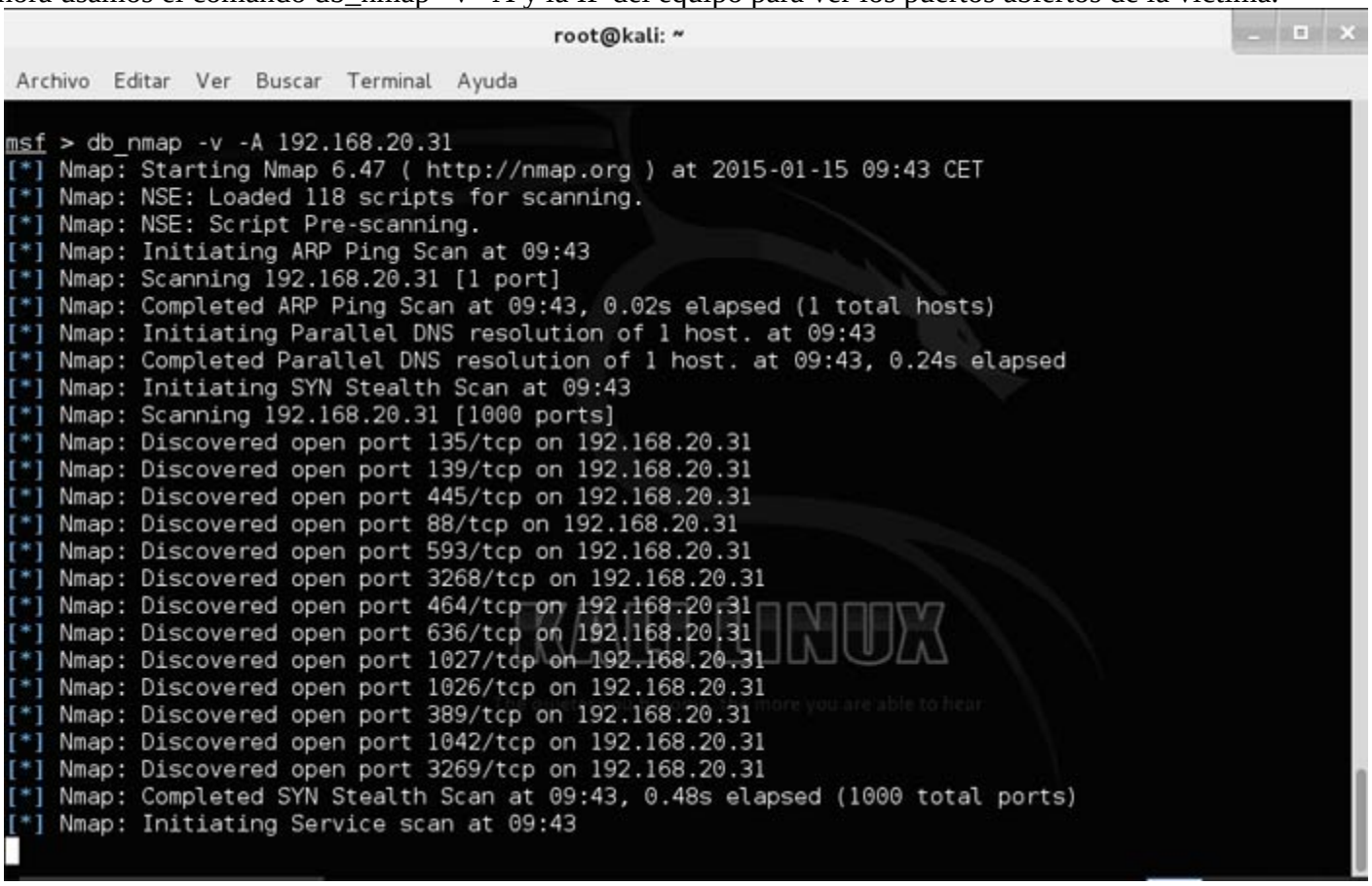
Ahora importamos el archivo del Nesus del Windows XP con el comando db_import al workspace en el que estamos.



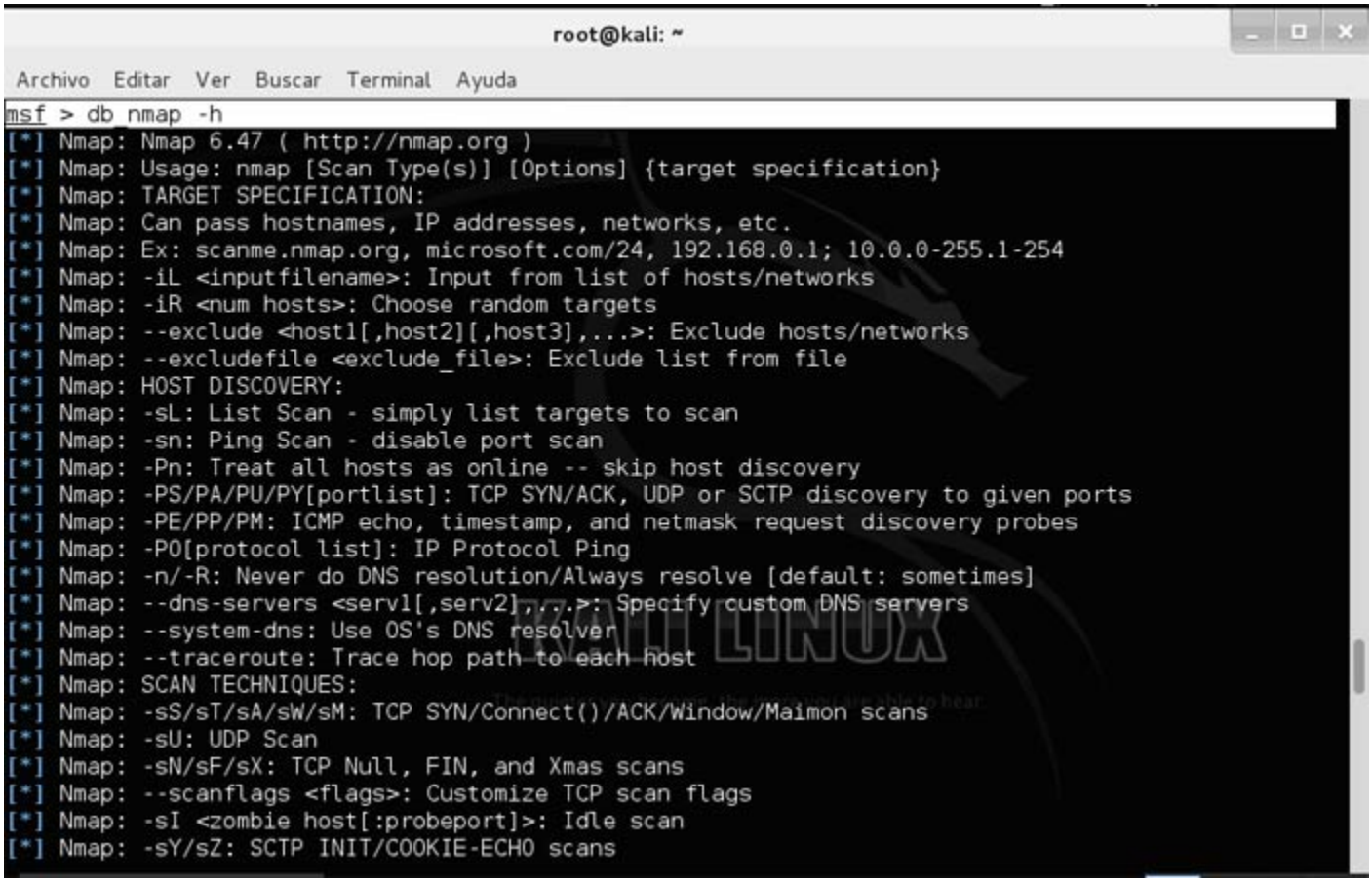
Ahora entramos en el workspace del Server2003 y vemos con el comando hosts los equipos que descubrimos con el Nessus.



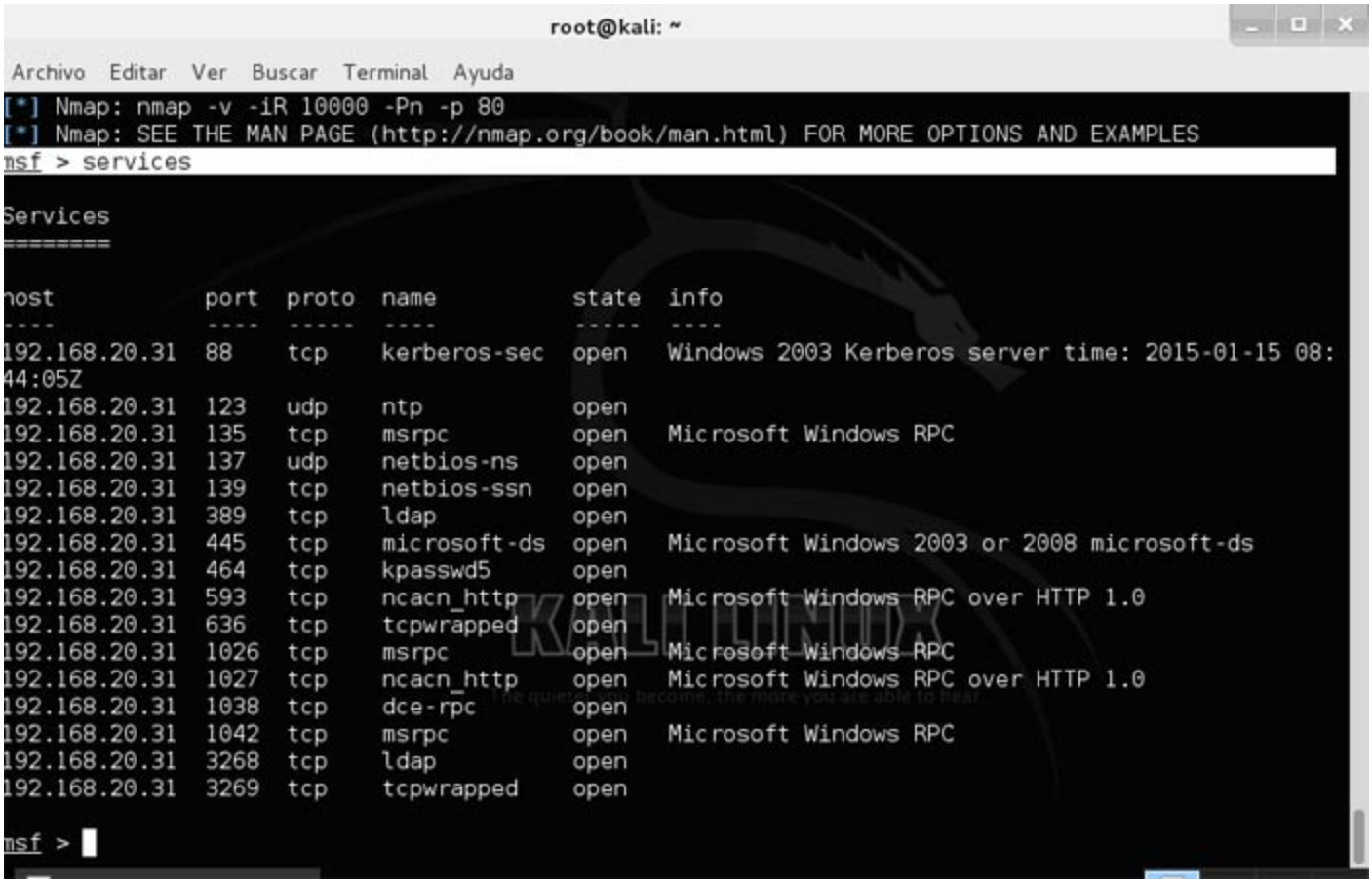
Ahora usamos el comando db_nmap –v –A y la IP del equipo para ver los puertos abiertos de la víctima.



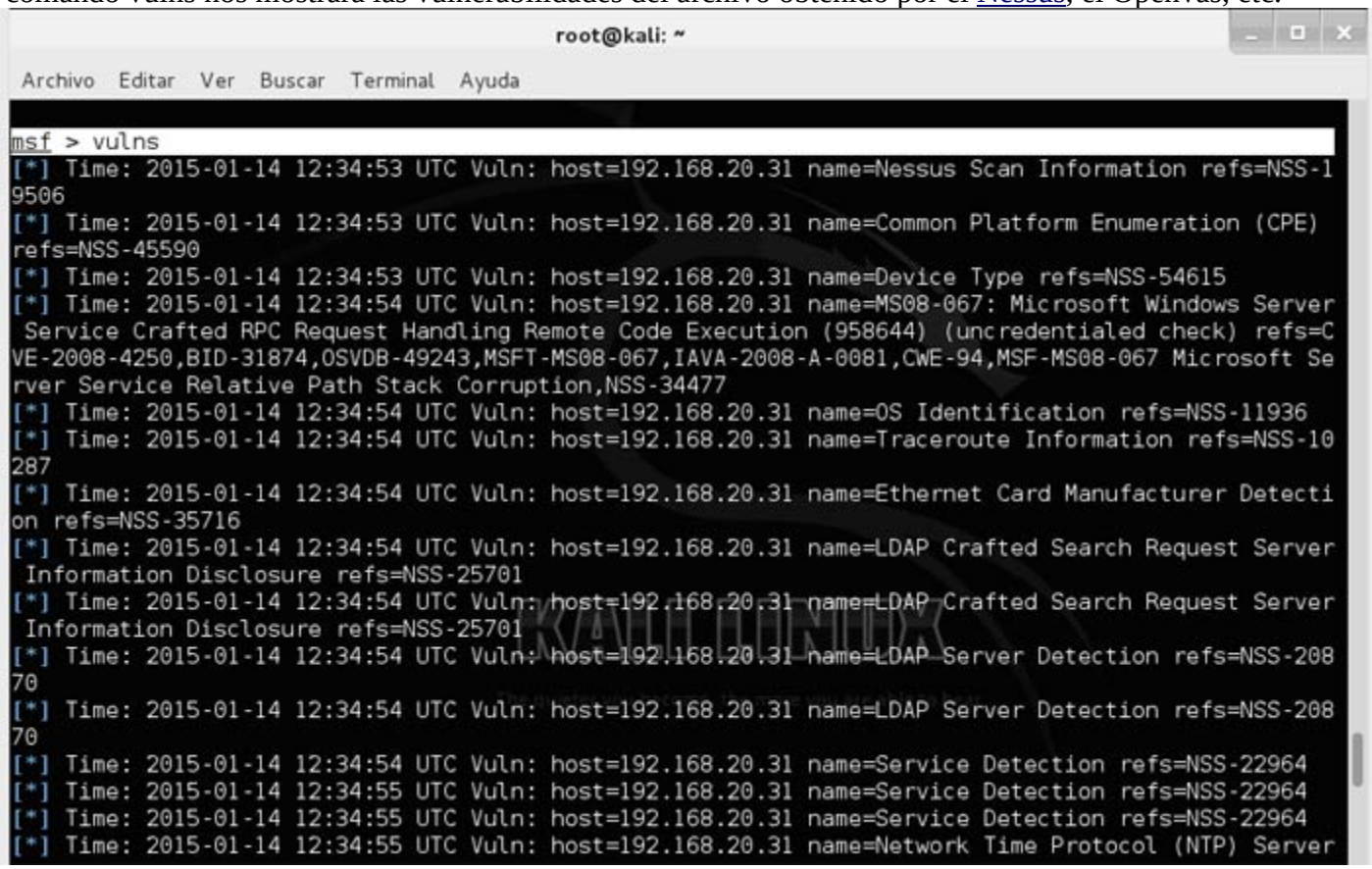
Los comando del db_nmap, son los mismos que con el programa Nmap. En MetaSploit para obtener ayuda de un comando escribimos help comando (ejemplo: help workspace), pero en los externos como es el db_nmap, usaremos comando -h (ejemplo: db_nmap –h).



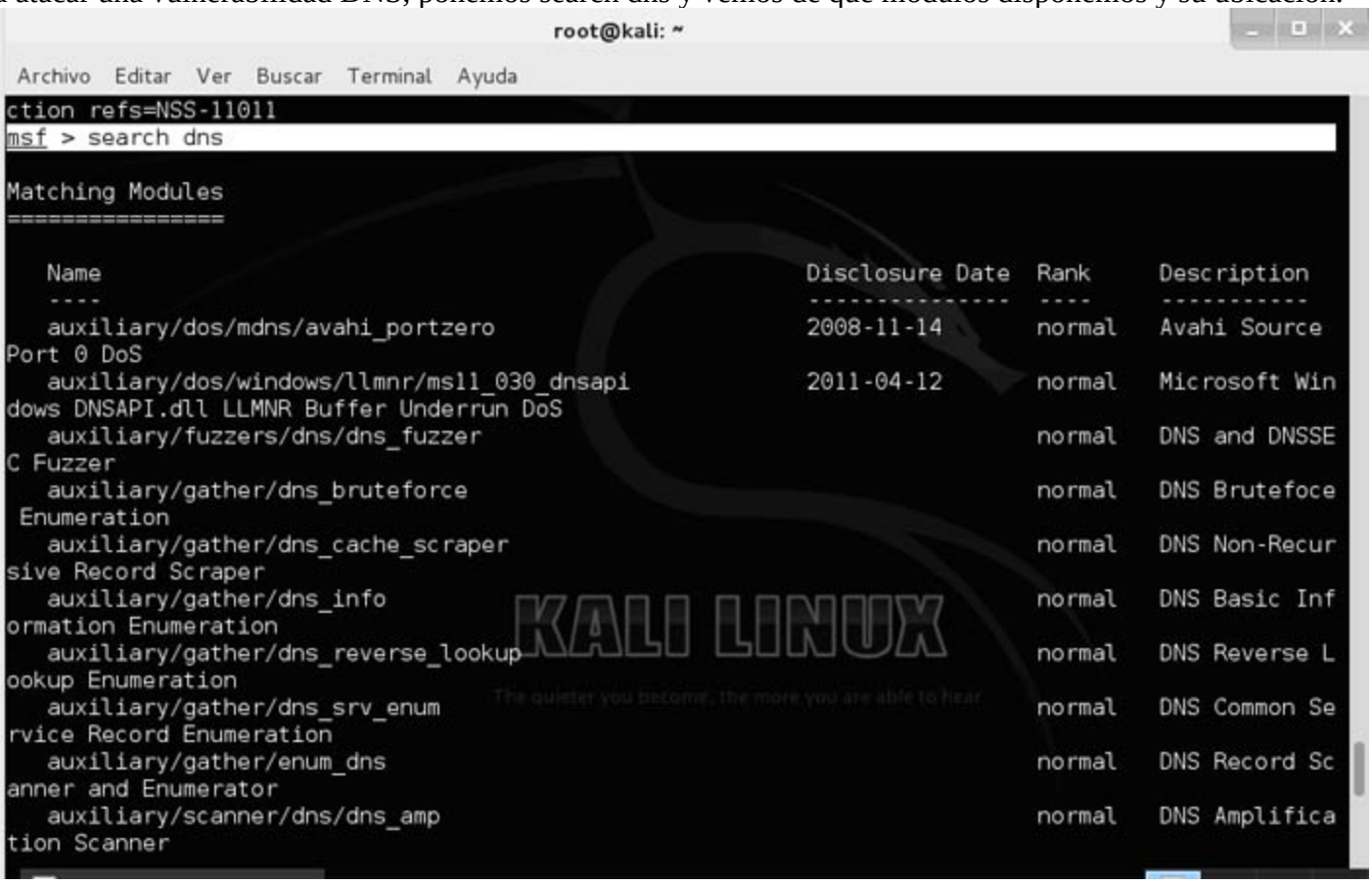
El comando services nos muestra los servicios abiertos de la víctima.



El comando vulns nos mostrará las vulnerabilidades del archivo obtenido por el Nessus, el Openvas, etc.

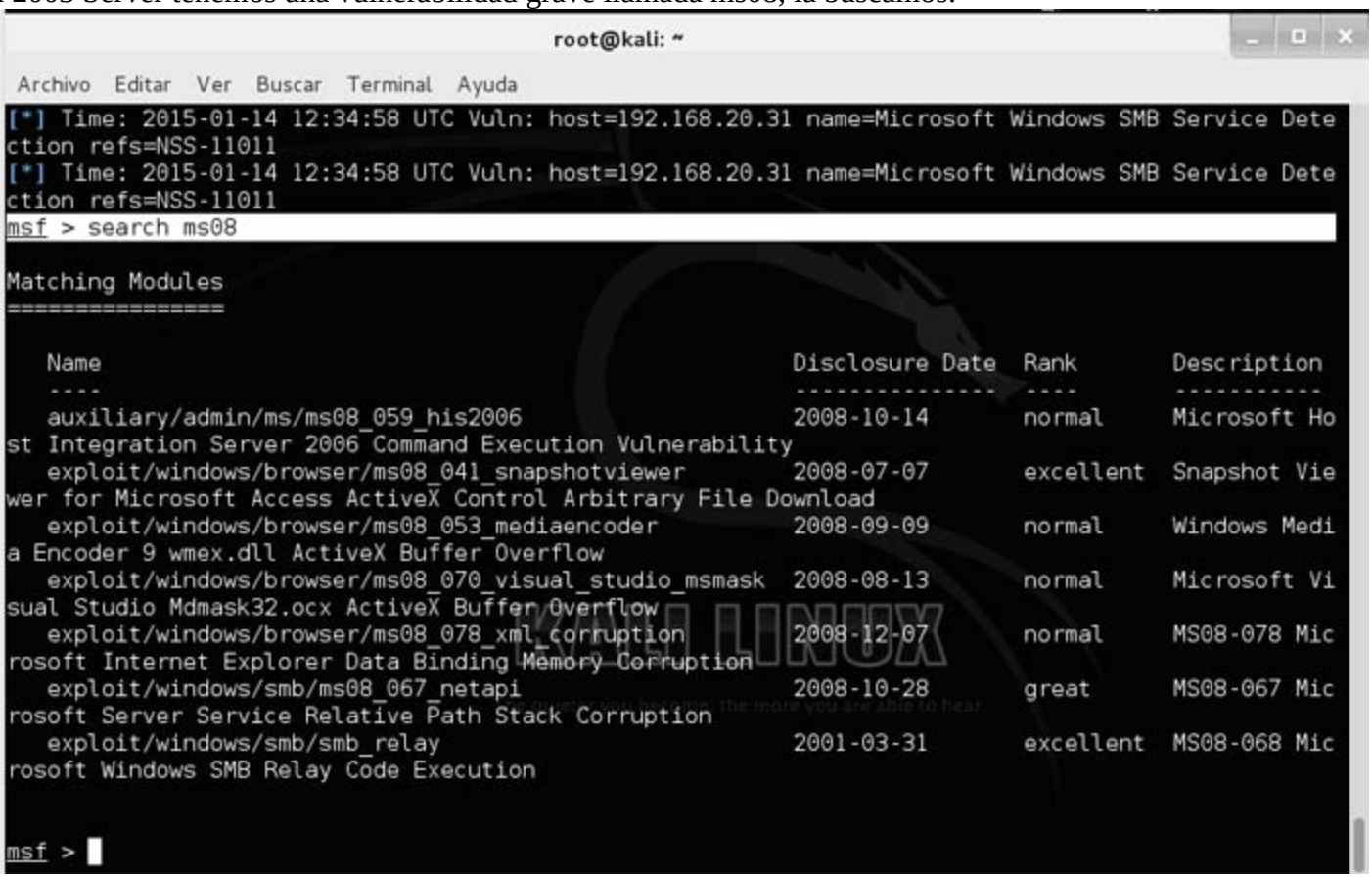


El comando search nos ayuda a buscar módulos del MSF (Metasploit). Por ejemplo, si necesitamos un módulo para atacar una vulnerabilidad DNS, ponemos search dns y vemos de qué módulos disponemos y su ubicación.

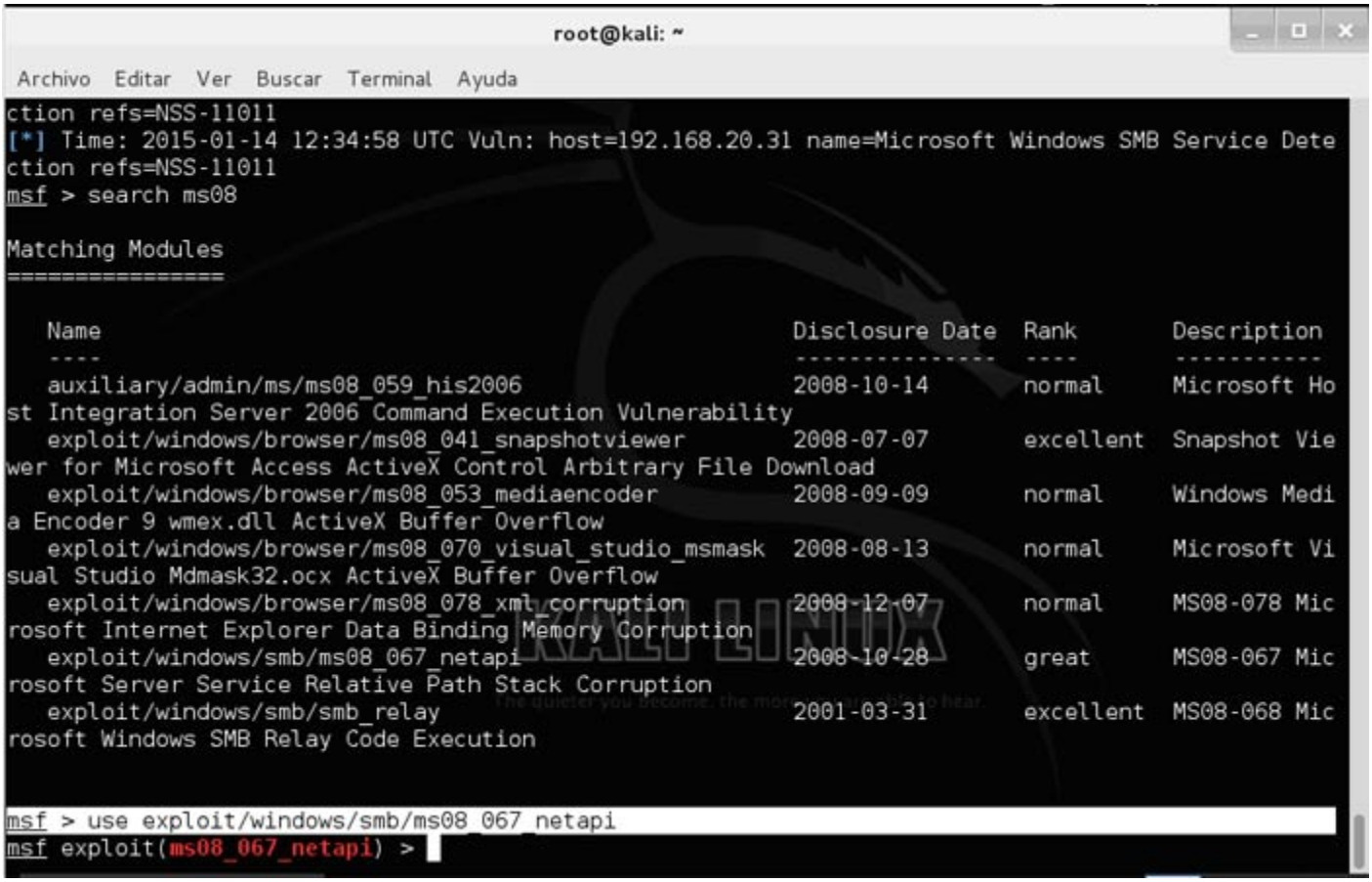


Uno de los exploits mostrados es el exploit/windows7dcerpc7ms07_029_msdns_zonename que explota una vulnerabilidad del DNS de los Windows 2000 y 2003 servers mediante el protocolo RPC en los controladores de dominio. Este exploit realiza un ataque DoS o de denegación de servicio que permite tumbar al servidor.

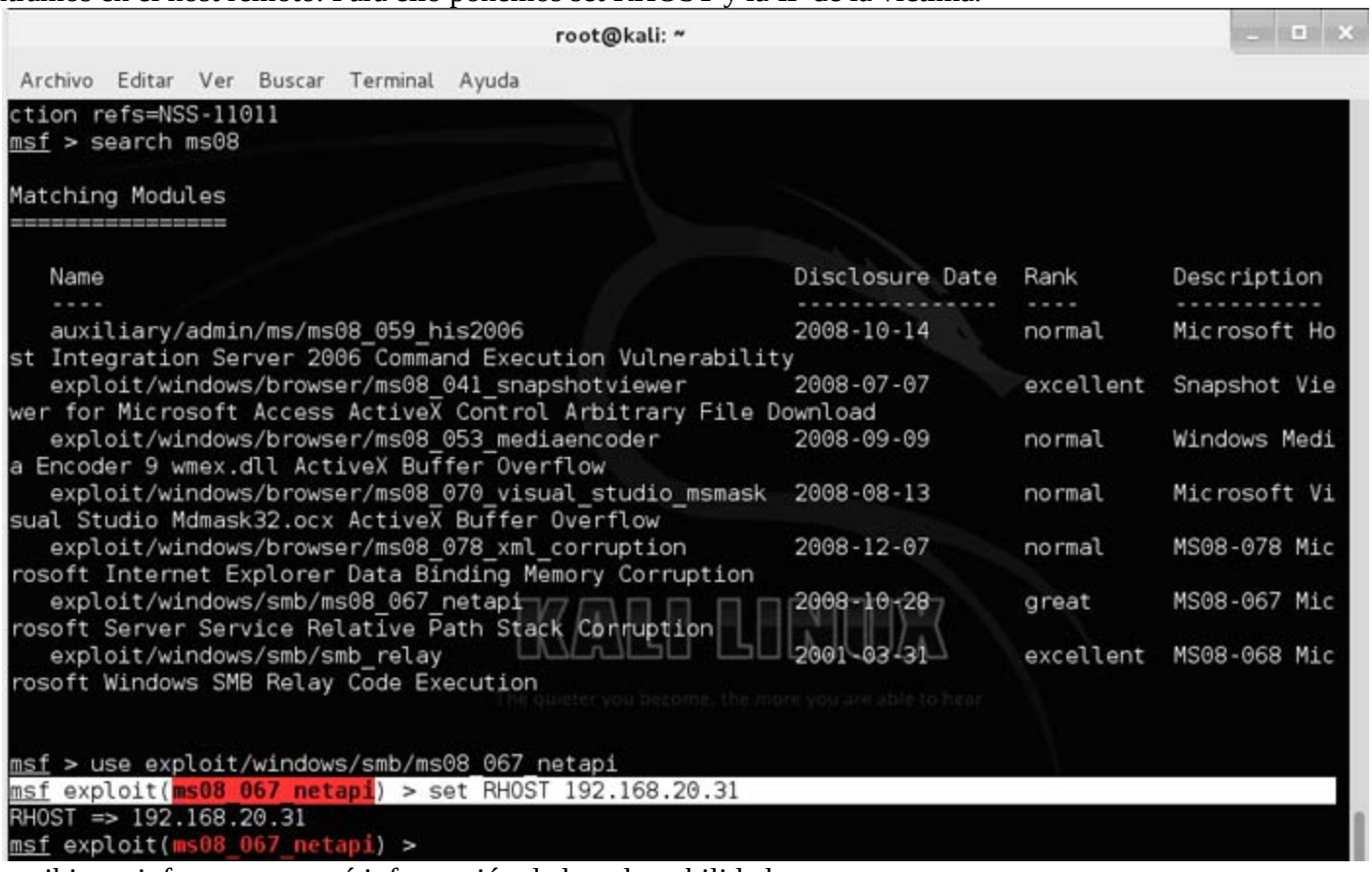
En 2003 Server tenemos una vulnerabilidad grave llamada ms08, la buscamos.



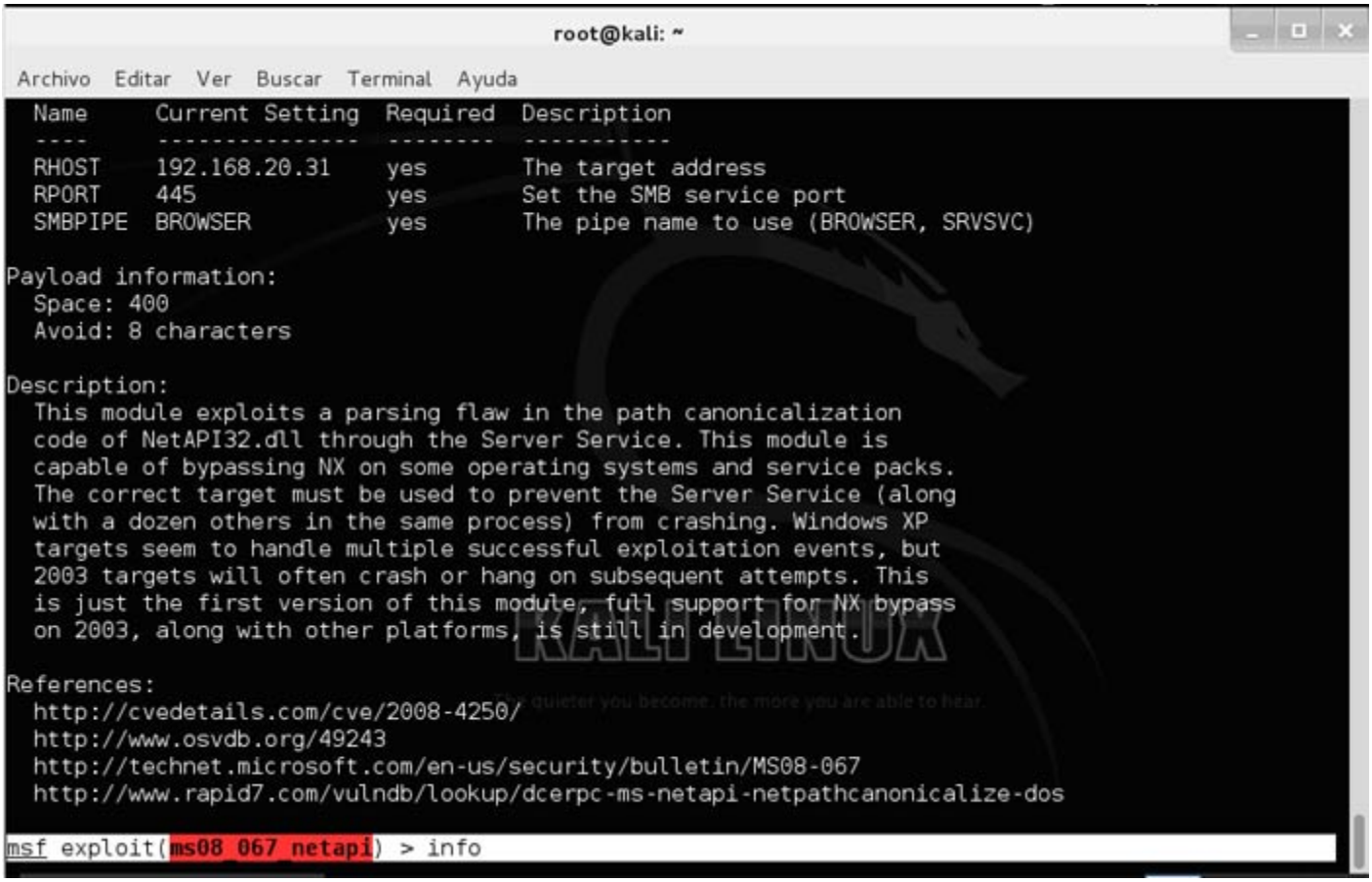
Ahora ejecutamos ese exploit que está en exploit/windows/smb/ms08_067_netapi. Para ello usamos el comando use.



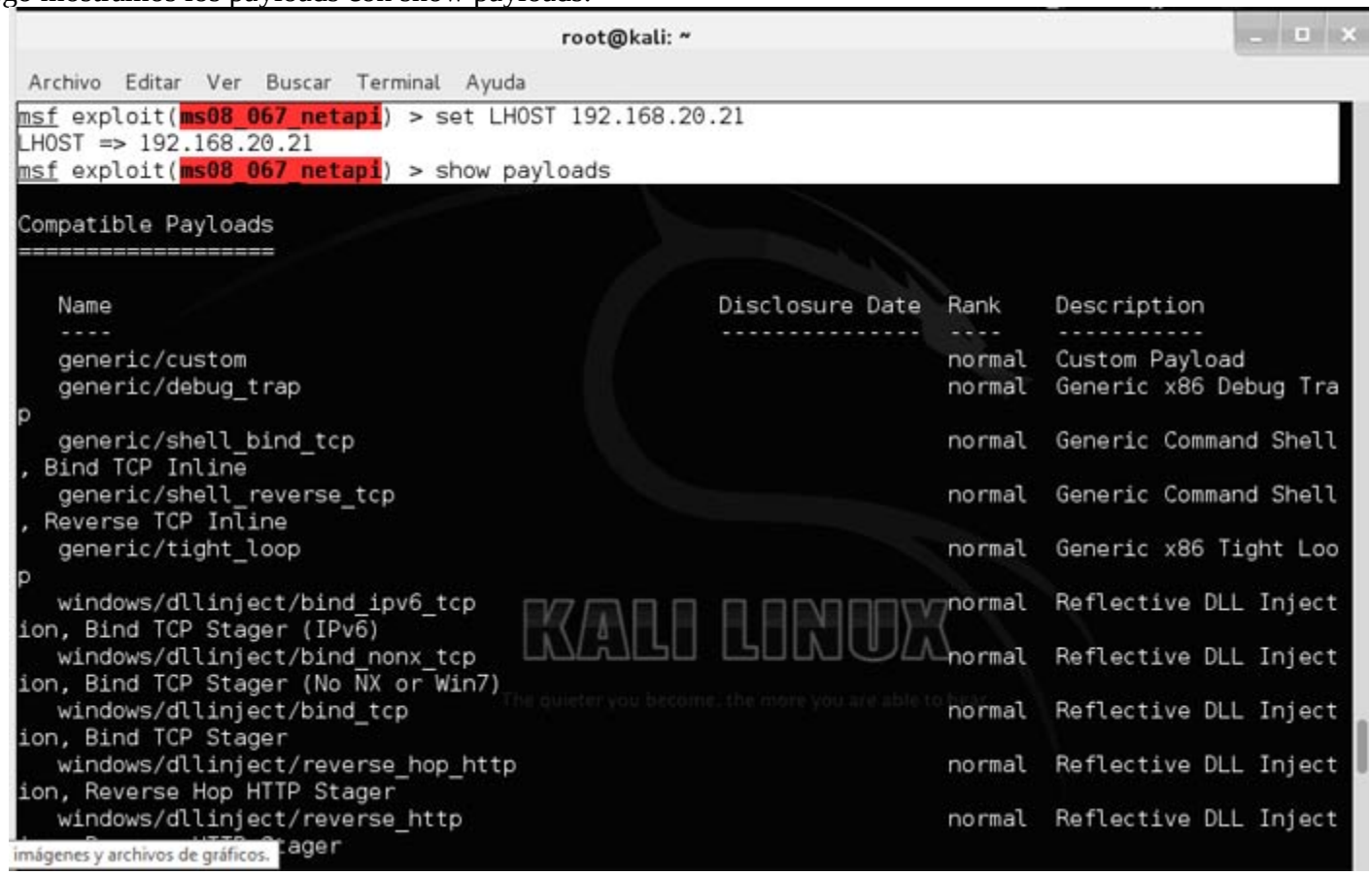
Entramos en el host remoto. Para ello ponemos set RHOST y la IP de la víctima.



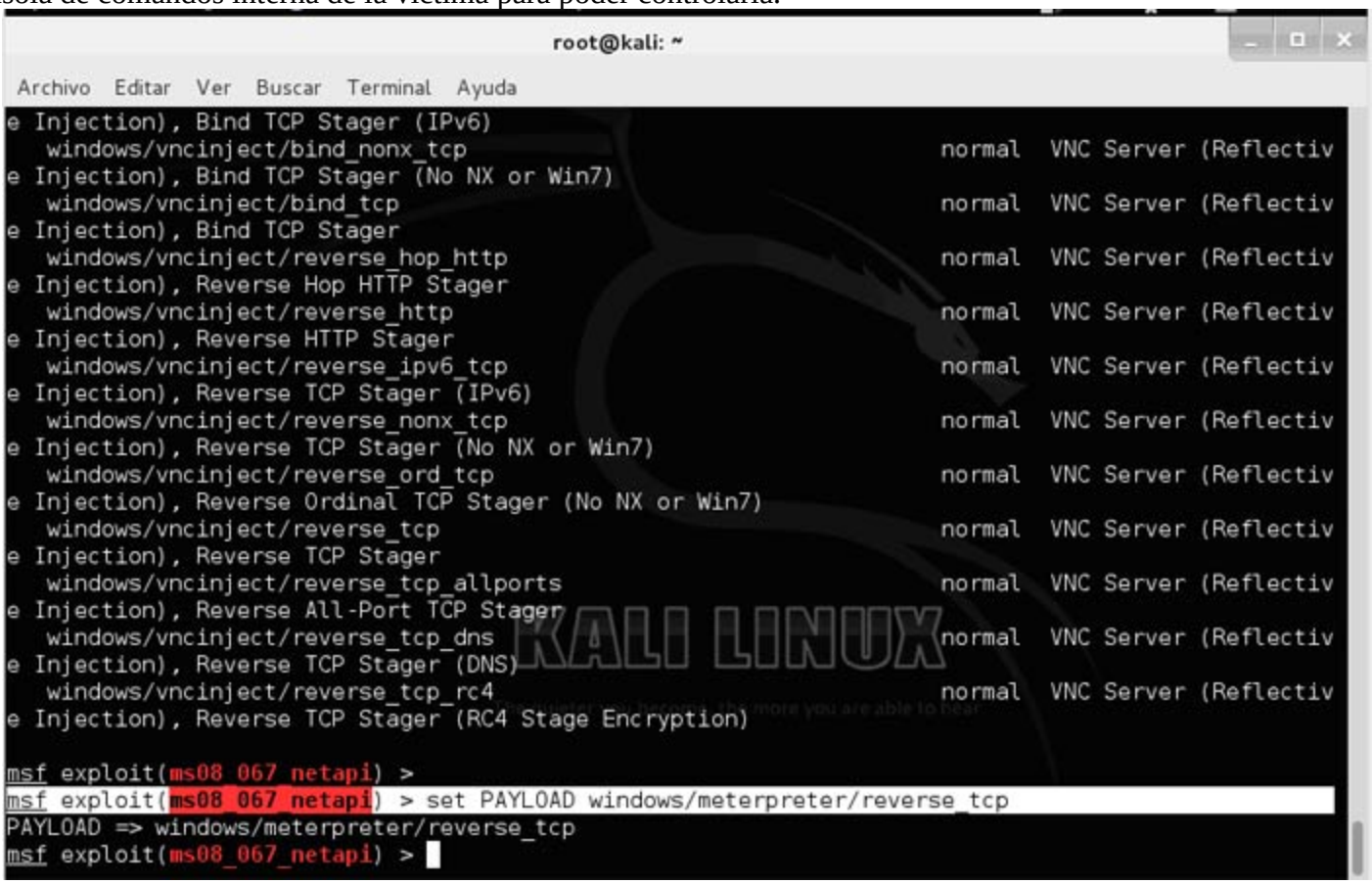
Si ecribimos info nos mostrará información de la vulnerabilidad.



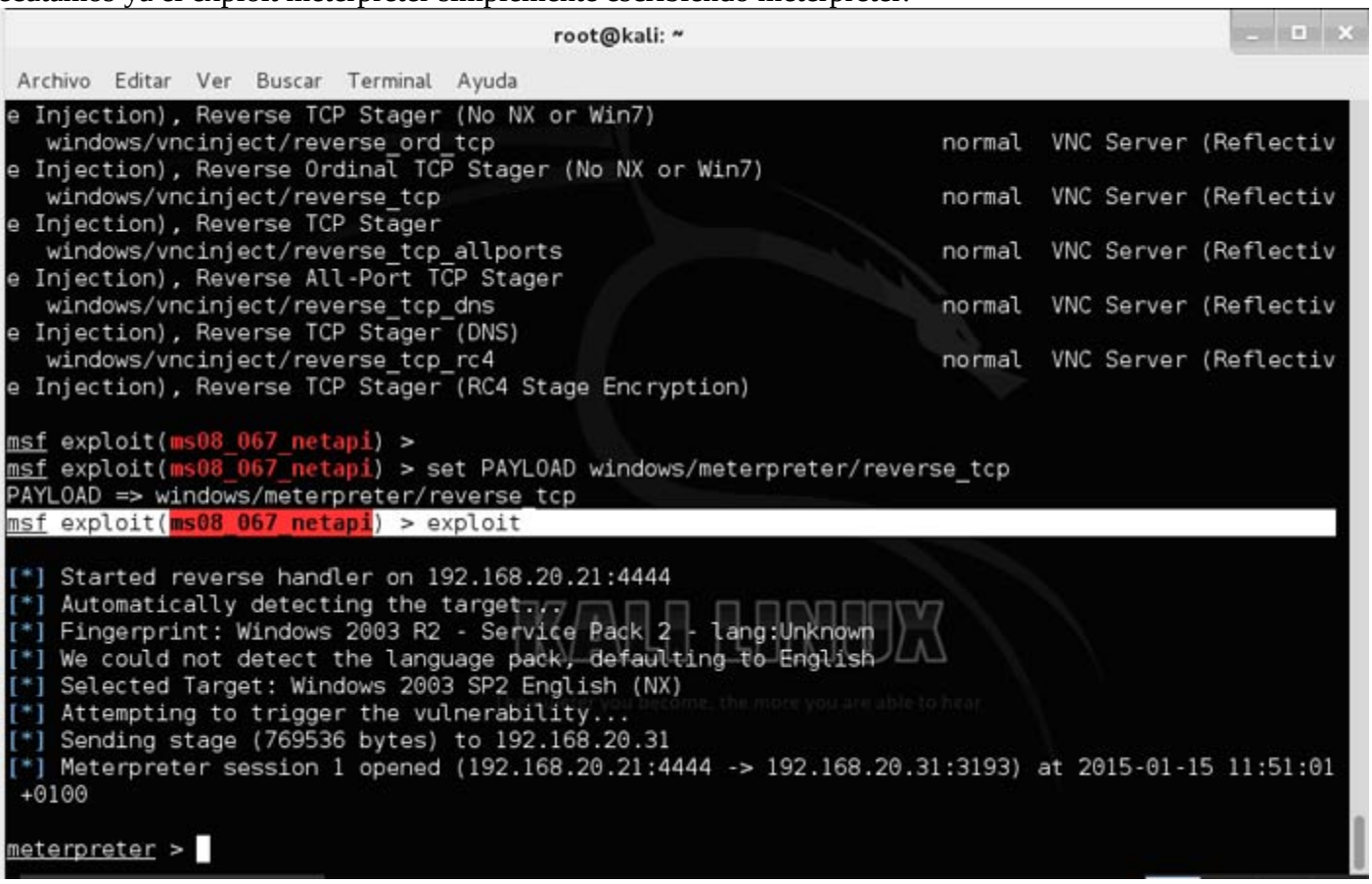
Entramos en nuestro host y vemos que payloads podemos usar. Para ello entramos con set LHOST y nuestra IP, y luego mostramos los payloads con show payloads.



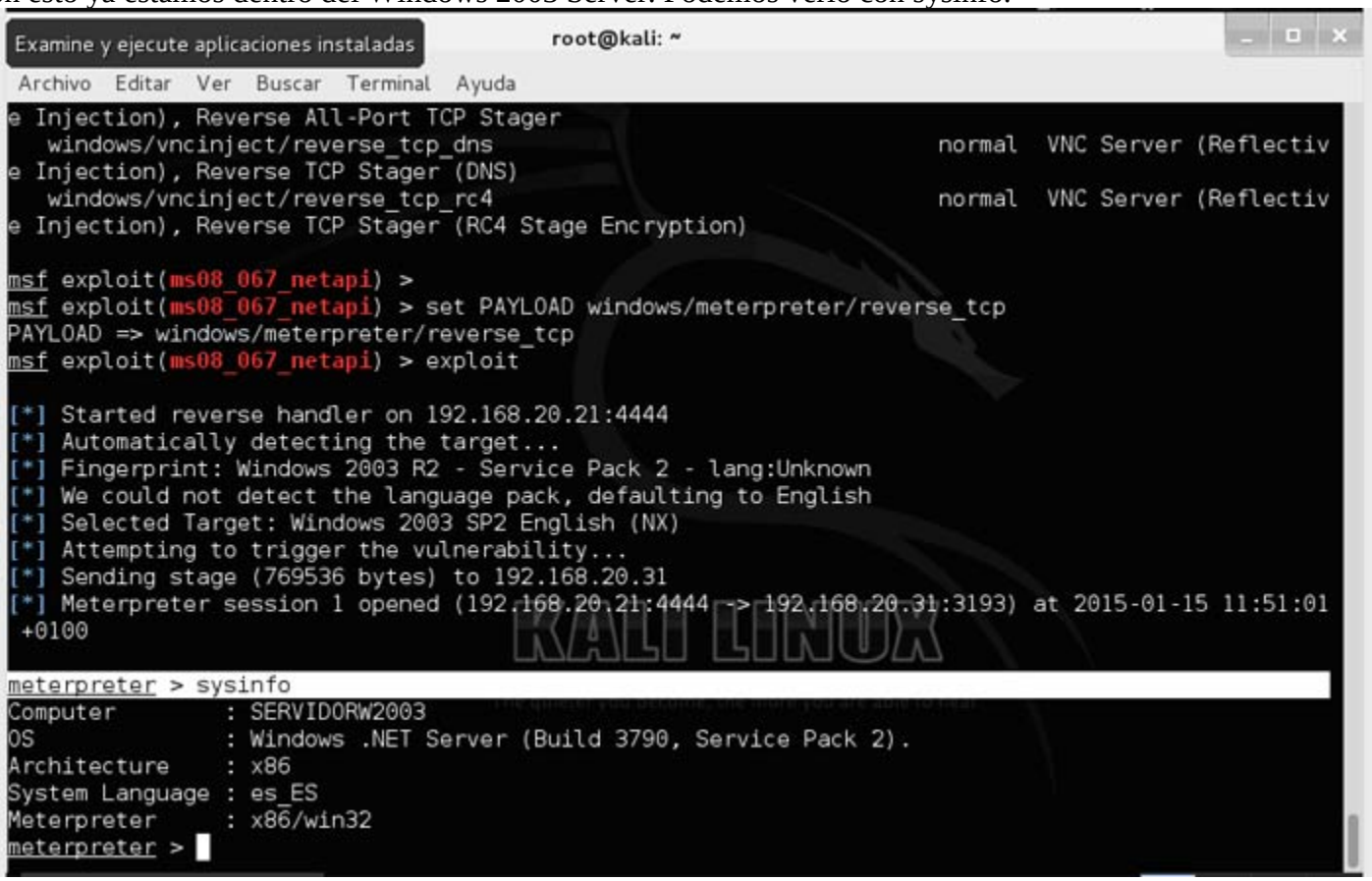
Cargamos el payload meterpreter para controlar la shell del Server 2003. Con esto lo que hacemos es ejecutar una consola de comandos interna de la víctima para poder controlarla.



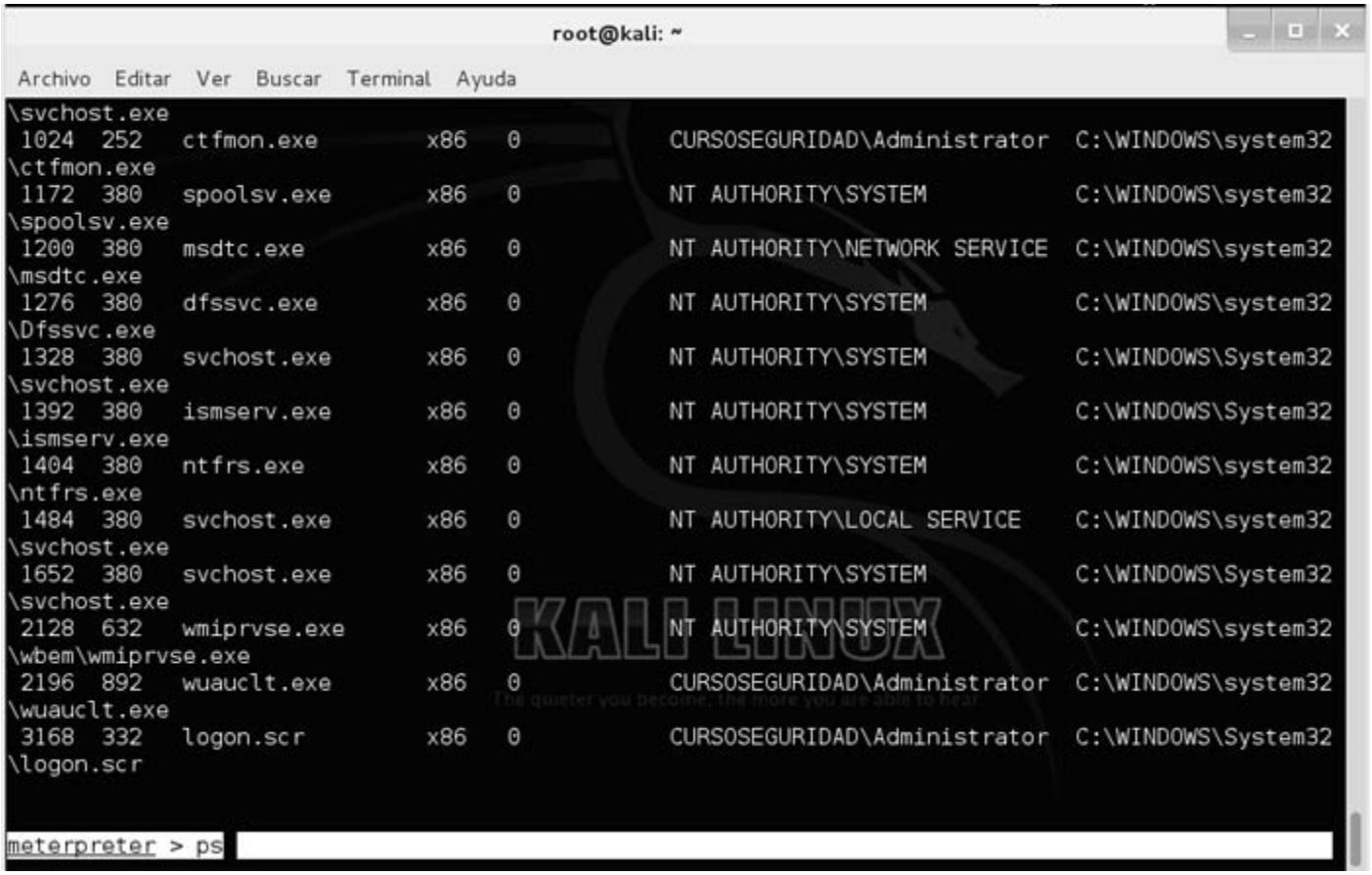
Ejecutamos ya el exploit meterpreter simplemente escribiendo meterpreter.



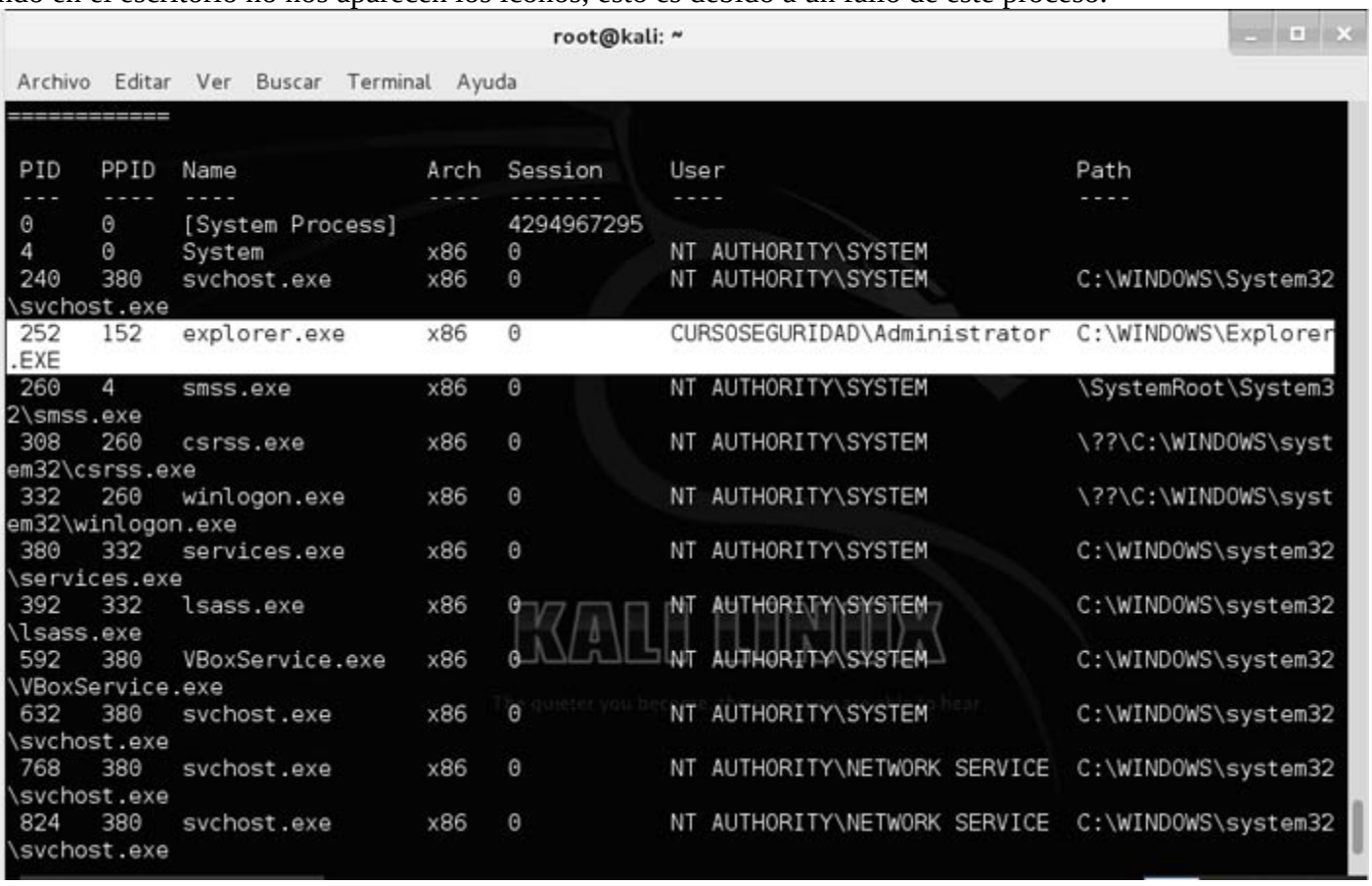
Con esto ya estamos dentro del Windows 2003 Server. Podemos verlo con sysinfo.



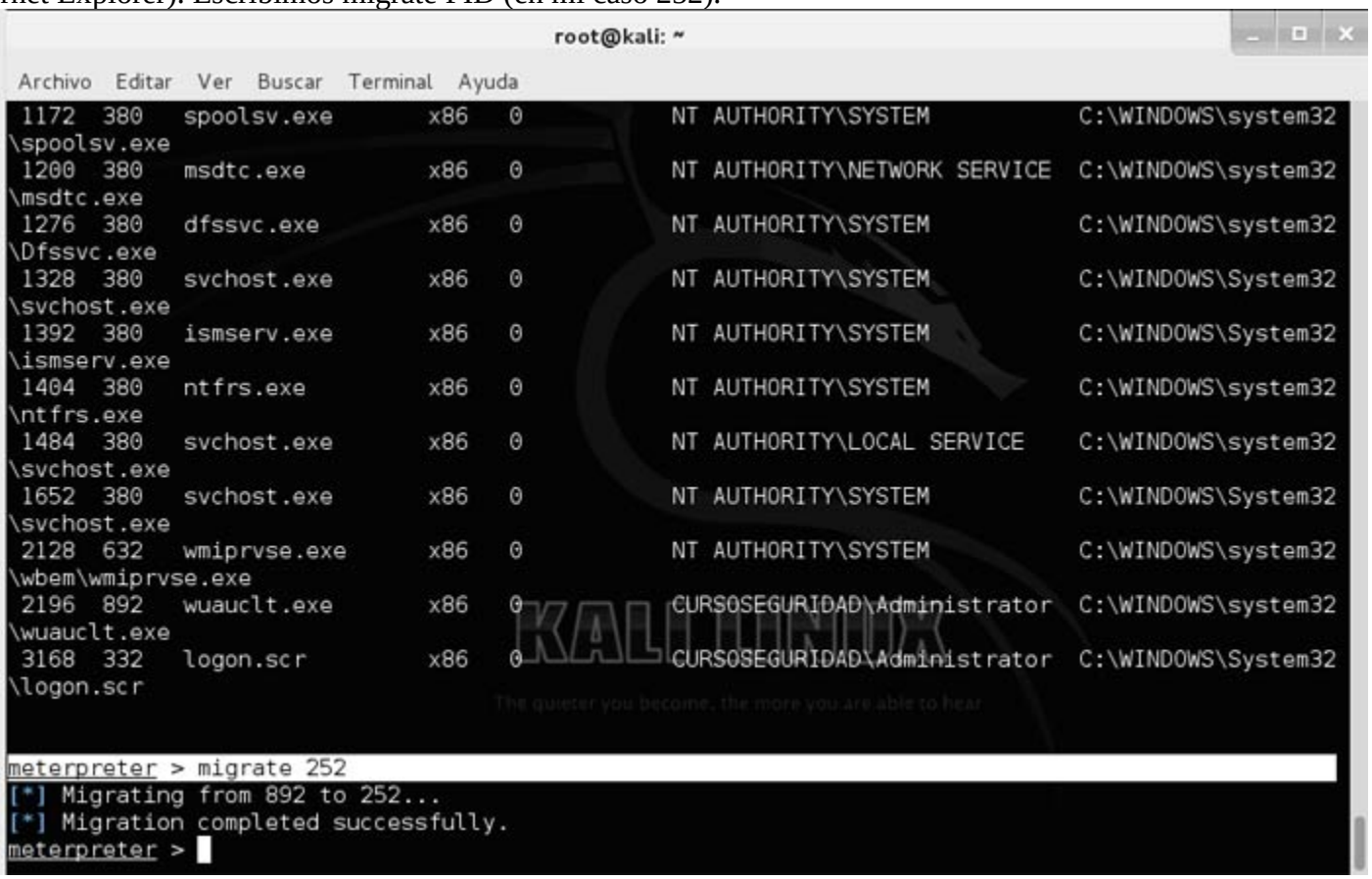
Con ps vemos que procesos está ejecutando el Windows 2003. Nos muestra el ejecutable del proceso y el PID o identificador numérico del proceso.



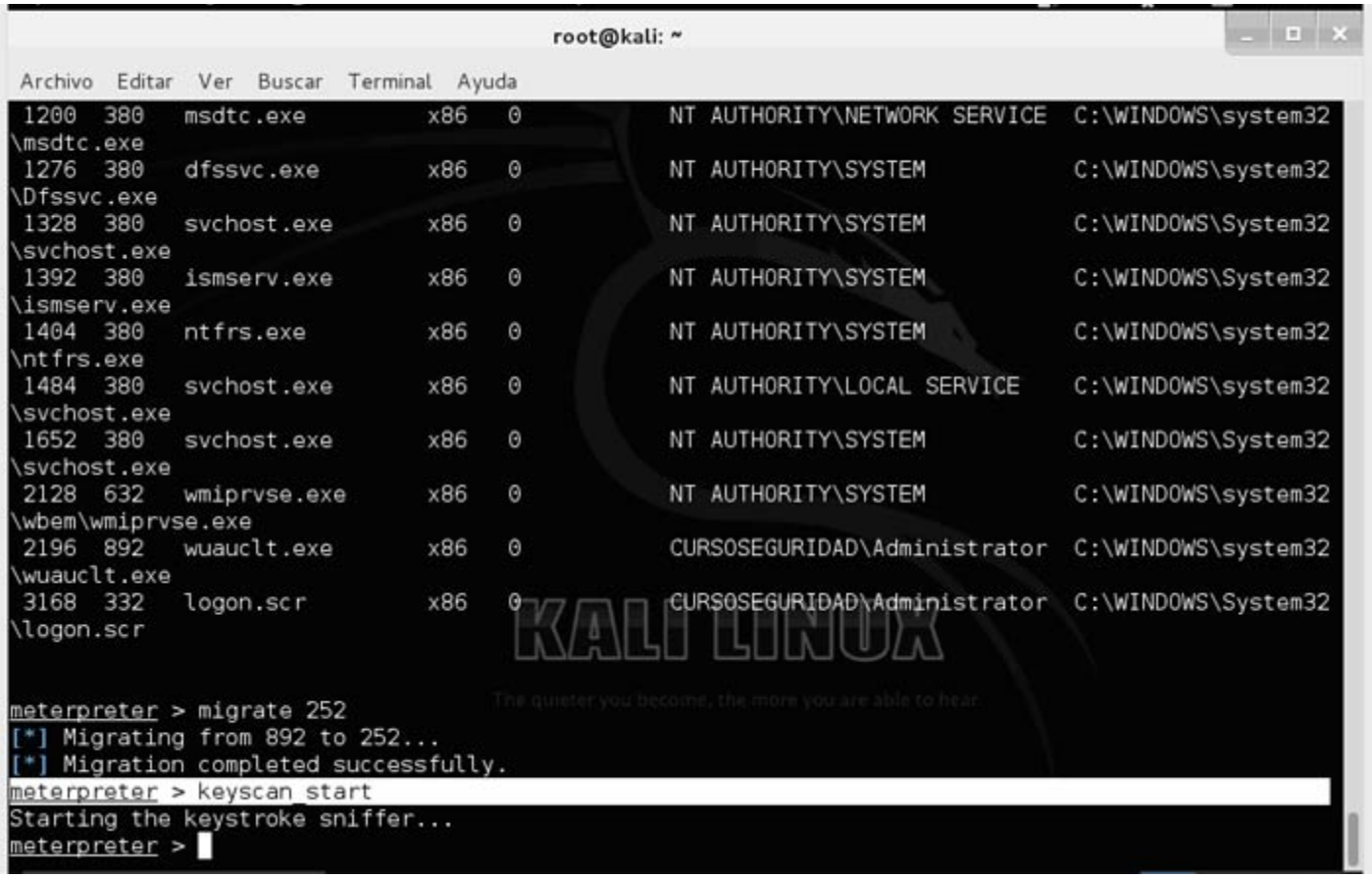
Hay un proceso que es el explorer, lo buscamos y miramos que número de proceso tiene o PID, en este caso el 252. El explorer es el proceso que en los sistemas Windows muestra la interface gráfica. Un claro ejemplo es cuando en el escritorio no nos aparecen los iconos, esto es debido a un fallo de este proceso.



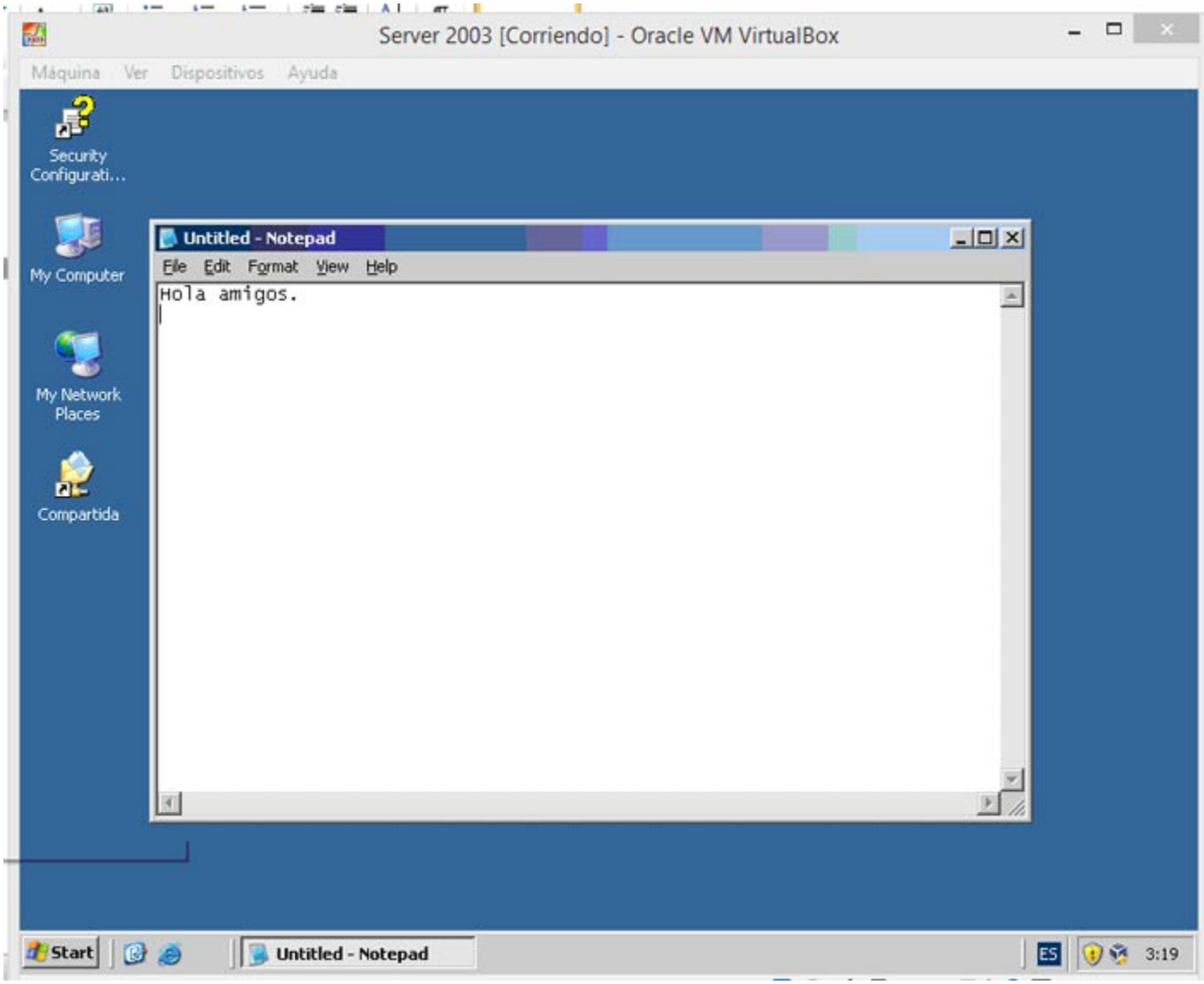
Ahora redirigimos ese proceso hacia nosotros con el comando migrate para controlar su explorer (nada que ver con Internet Explorer). Escribimos migrate PID (en mi caso 252).



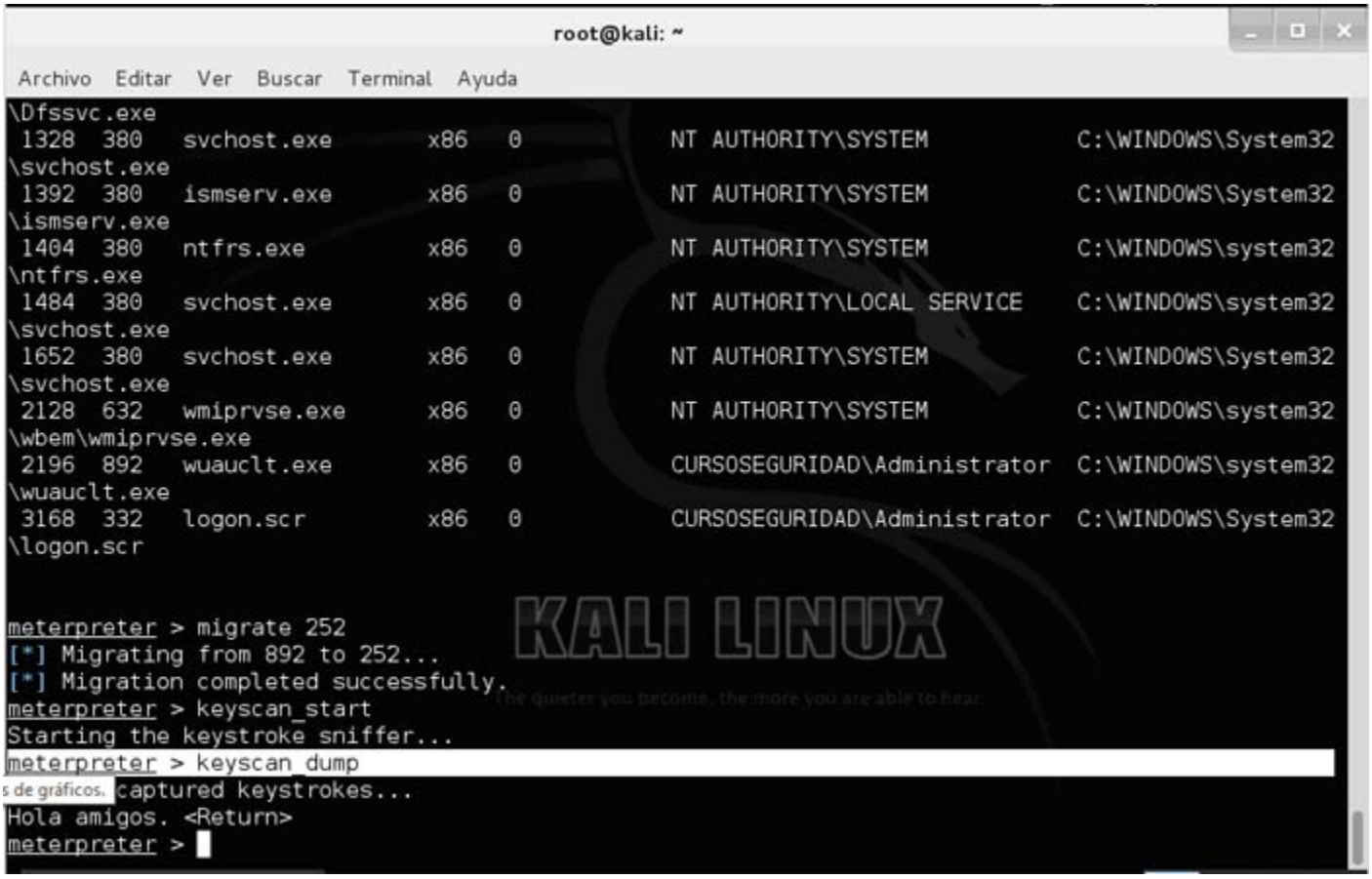
Ahora le vamos a meter un keylogger. Los Keyloggers son programas que nos muestra que está haciendo la víctima. Lo normal es que muestren todas las pulsaciones del teclado, inclutendo contraseñas. Muchos Keyloggers nos permiten configurarlos para que cada cierto tiempo nos mande a un correo electrónico que le indiquemos toda esa información, incluso con pantallas de lo que la víctima está viendo. Vamos a usar el keyscan que es muy sencillo, ponemos keyscan_start.



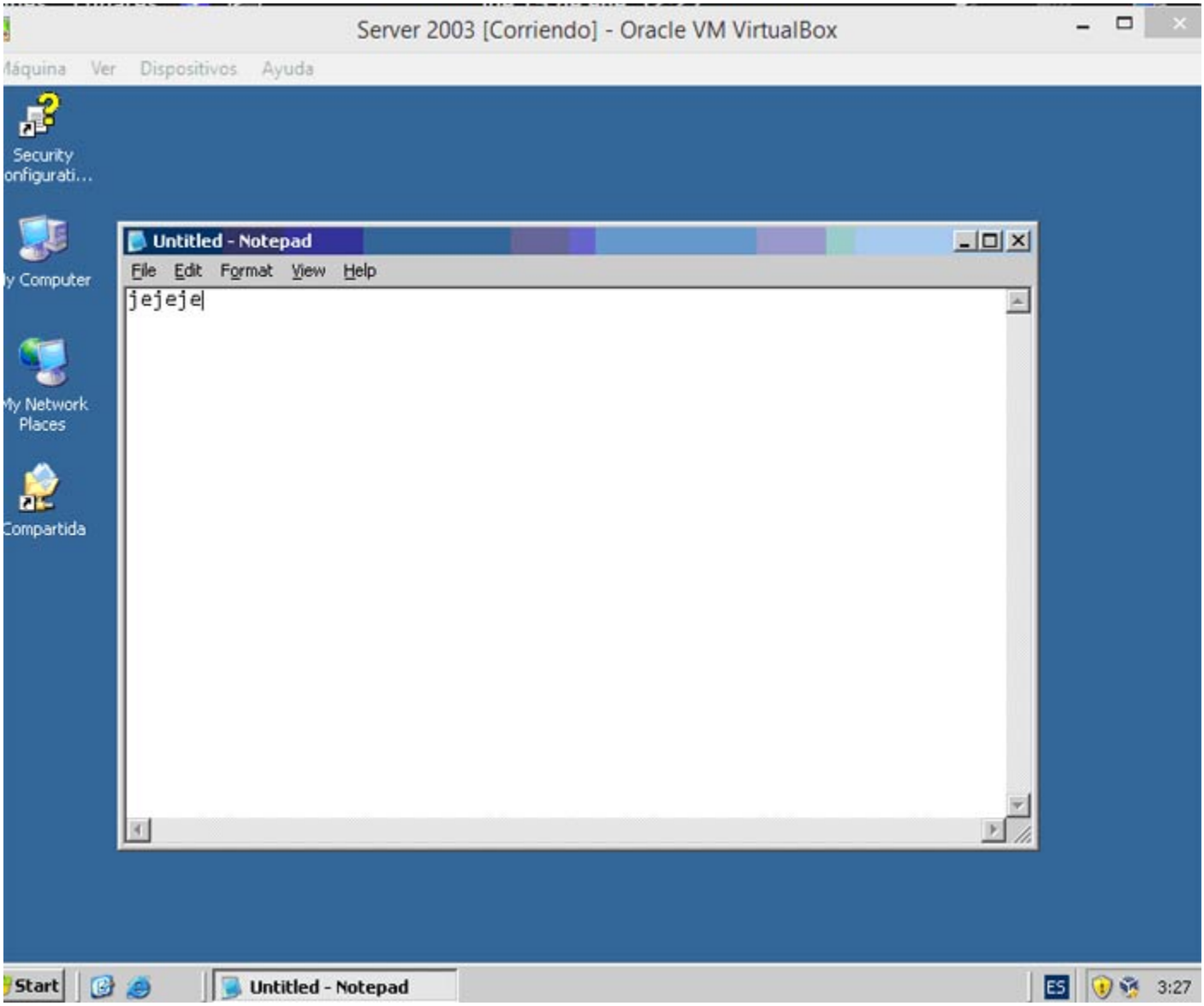
Para ver que realmente nos está funcionando, vamos a hacer también de víctima y abrimos el Windows 2003 y escribimos algo en el notepad, lo que sea.



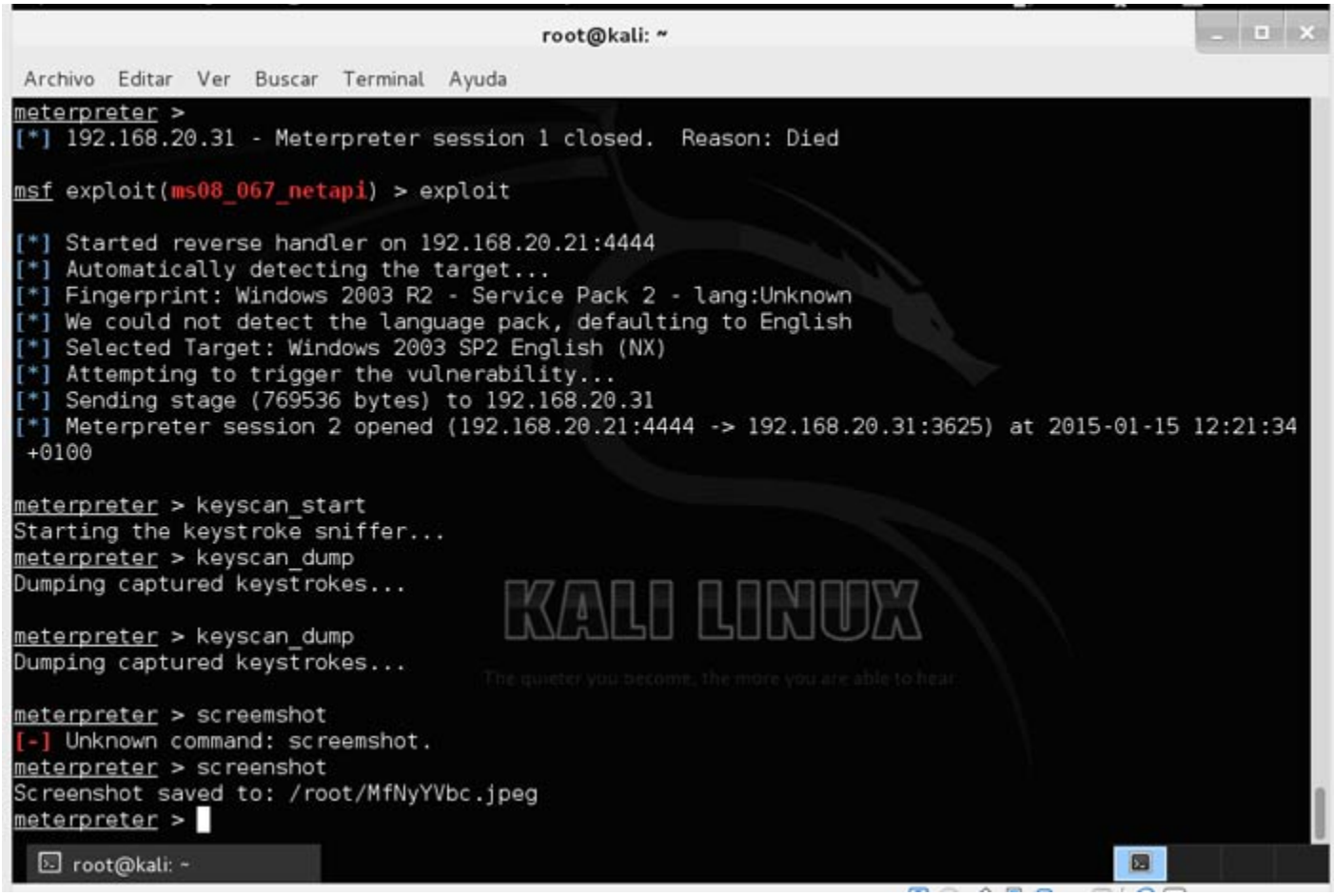
Vamos al Metasploit de nuevo y ecribimos keyscan_dump para que muestre los resultados hasta ese momento y vemos que muestra lo que se puso en 2003 server.



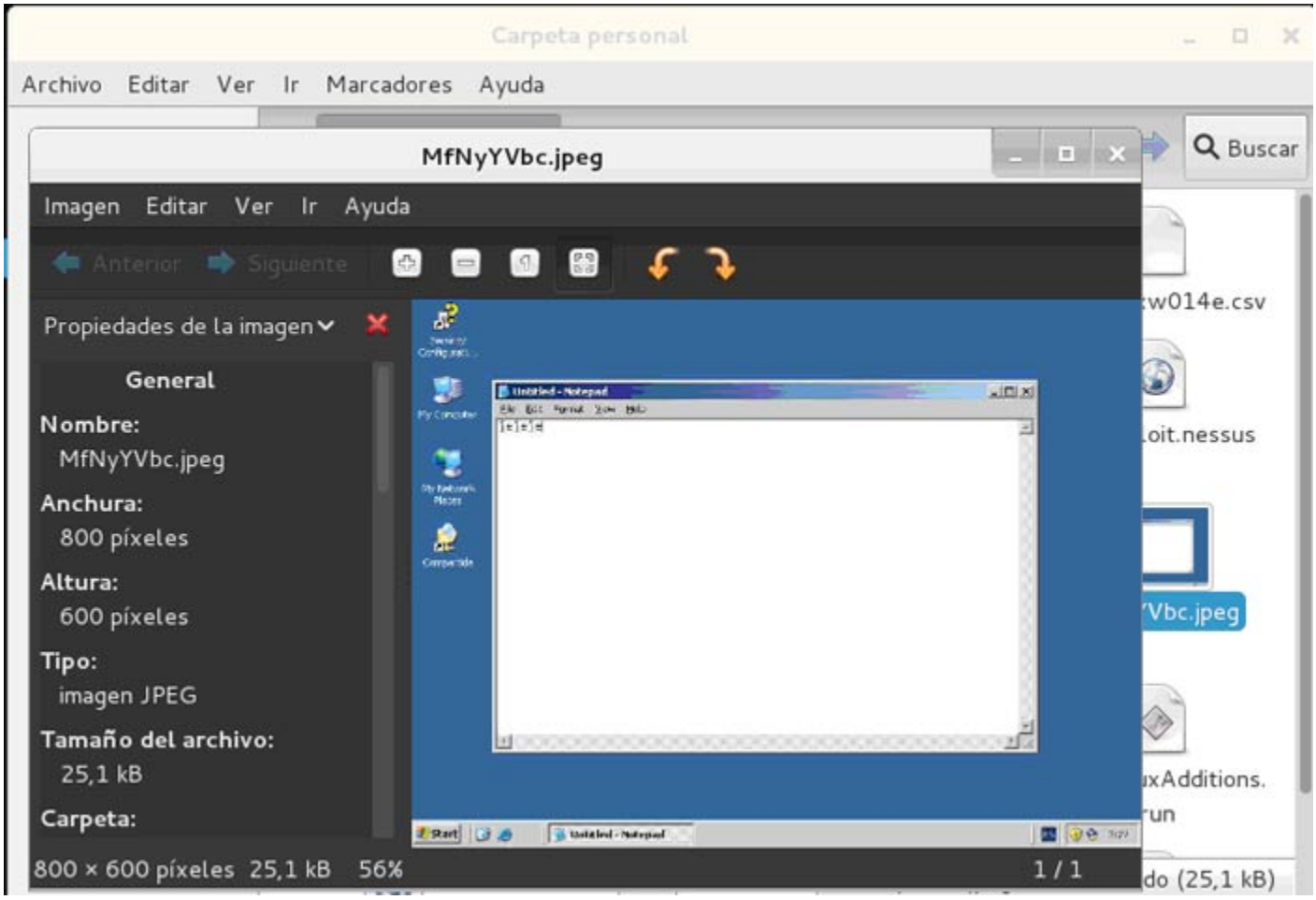
Ahora veremos todo cuanto escriba por el teclado nuestra víctima.
En el server hacemos lo que sea, como escribir algo en un block de notas.



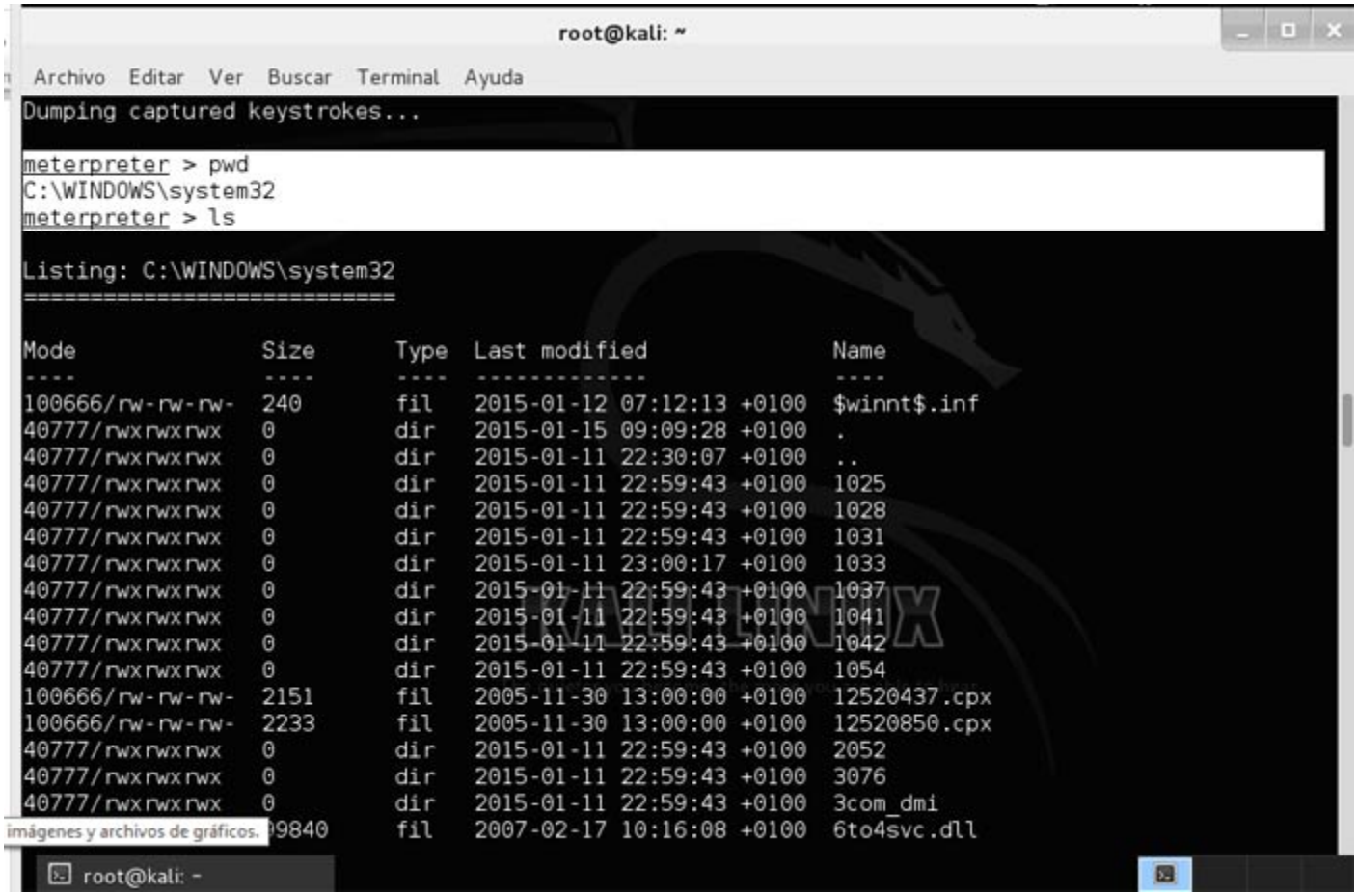
Ahora vamos a sacar un pantallazo de lo que está haciendo. Para ello usamos el comando screenshot que se encarga de realizar capturas de pantalla.



Esto nos da el directorio donde meterá nuestro pantallazo y el nombre de jpeg. Accedemos desde Kali a ese archivo y abrimos el jpeg. Vemos que sale exactamente la misma pantalla que hay abierta en el Windows 2003.



Ahora en el meterpreter usamos los comandos básicos de linux para movernos dentro del sistema de la víctima. Por ejemplo pwd para ver el directorio del Windows 2003 en el que estamos y ls para listarlo y que nos muestre el contenido.



Ya podemos entrar en su sistema para borrarle archivos del sistema o de datos y matar de un susto al administrador. Metasploit es mucho más amplio, iré ampliando cosillas cuando tenga tiempo, pero antes quiero sacar la guía de Armitage, es una aplicación gráfica para Metasploit que os resultará más sencilla de usar.