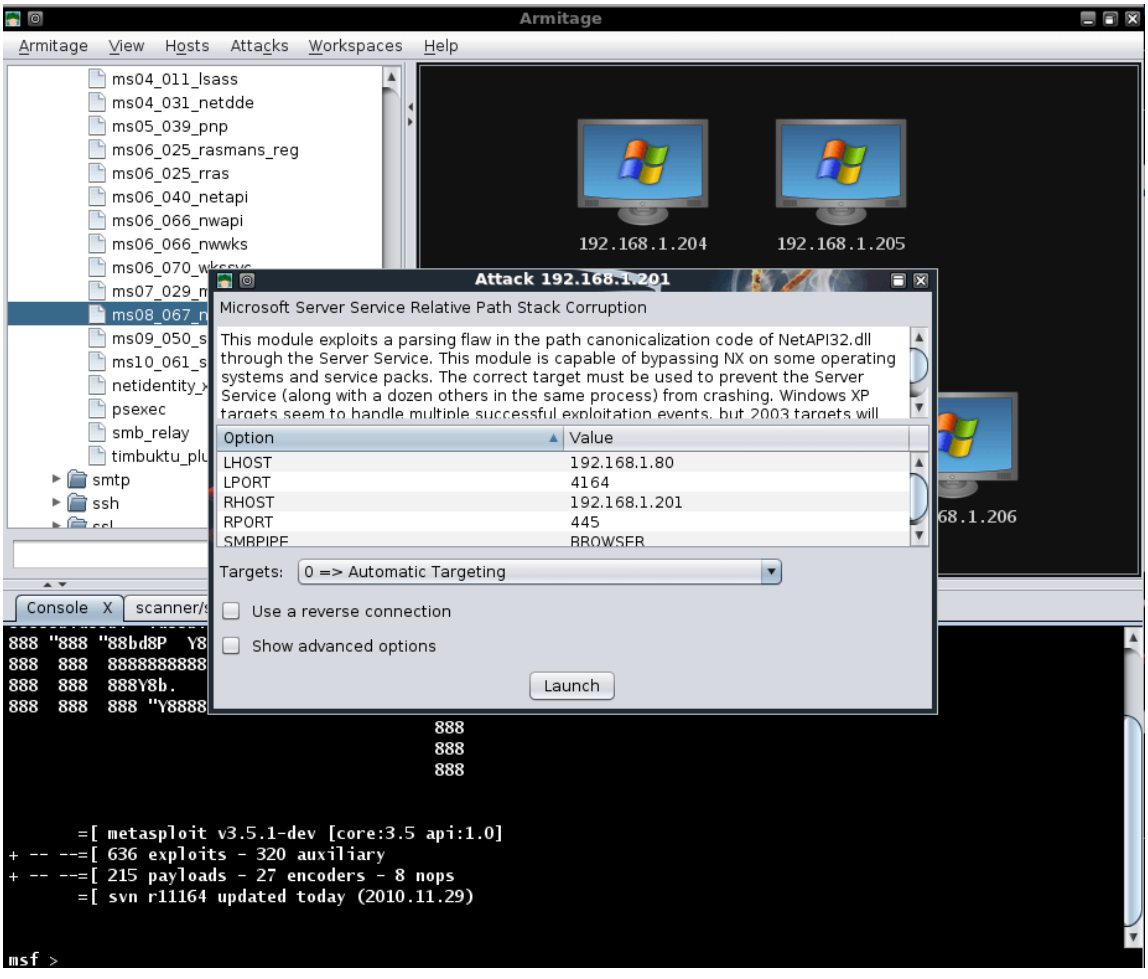
offensive-security.com

Armitage Exploitation | Offensive Security

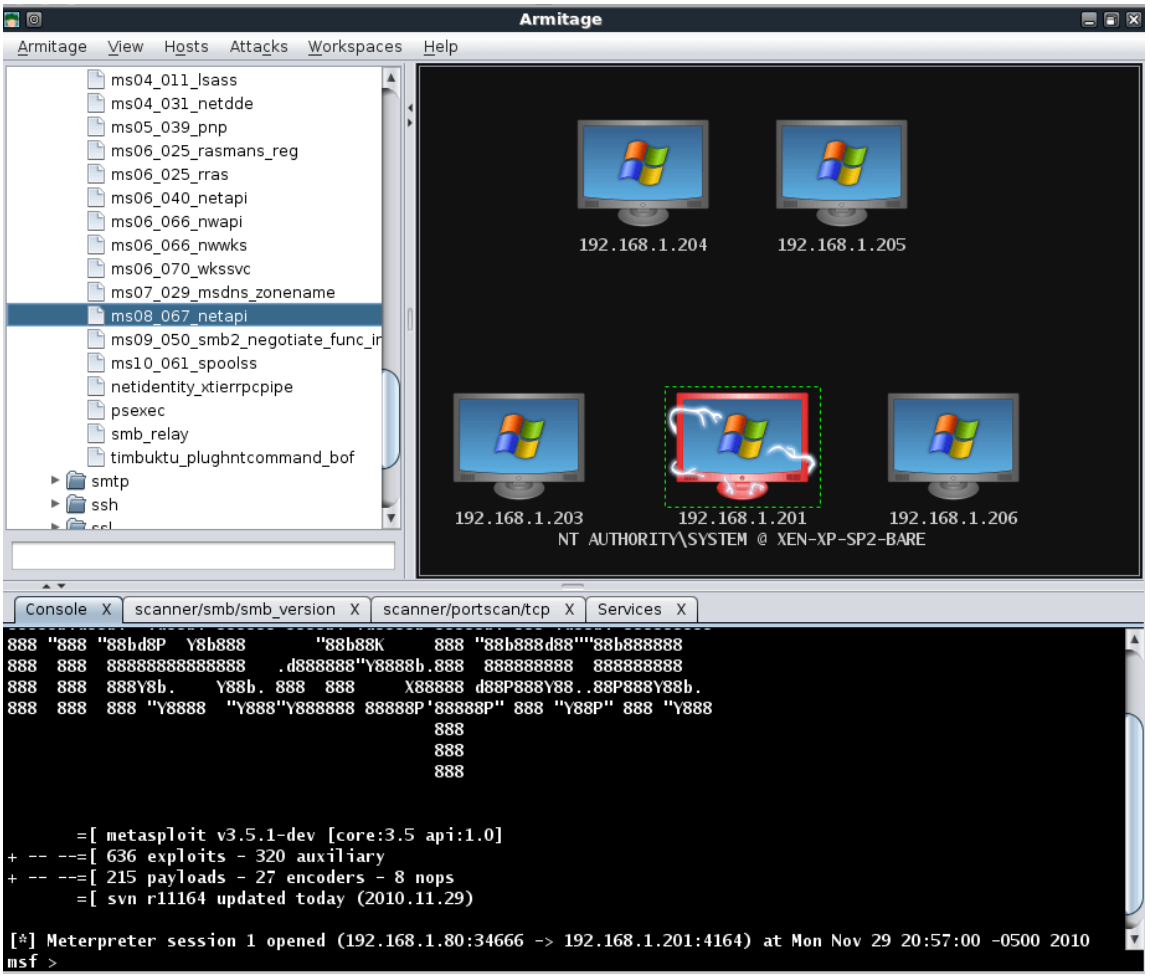
2 minutos

In the scan we conducted earlier, we see that one of our targets is running Windows XP SP2 so we will attempt to run the exploit for MS08-067 against it. We select the host we would like to attack, find the exploit in the tree, and double-click on it to bring up the configuration for it.

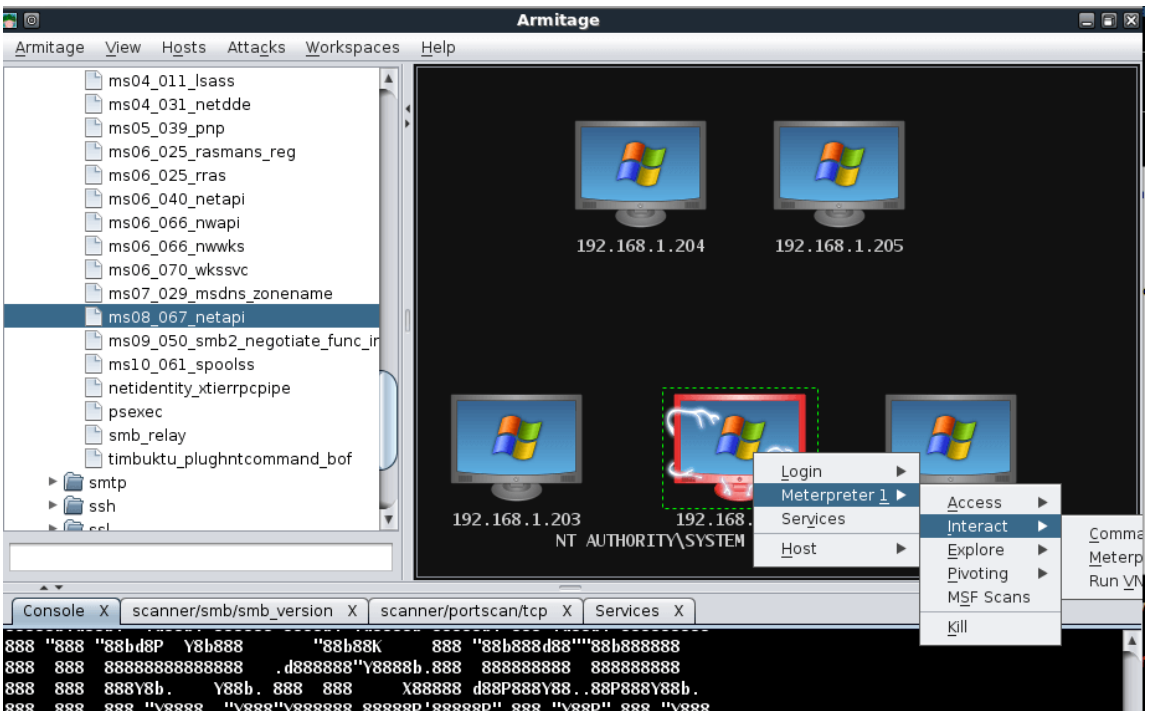


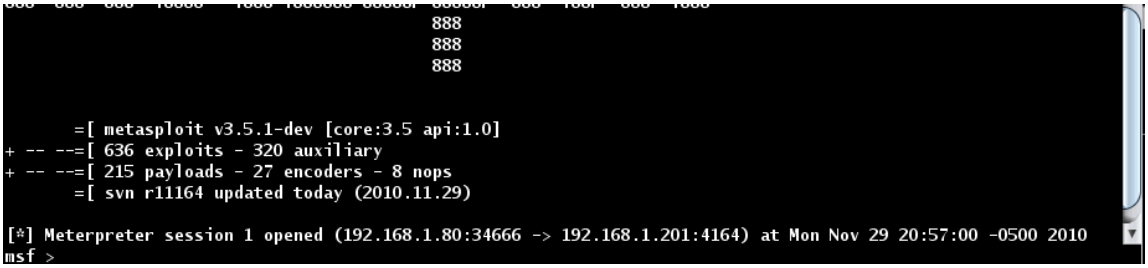
As with our selective scanning conducted earlier, all of the necessary configuration has been setup for us. All we need to

do is click ‘Launch’ and wait for the Meterpreter session to be opened for us. Note in the image below that the target graphic has changed to indicate that it has been exploited.

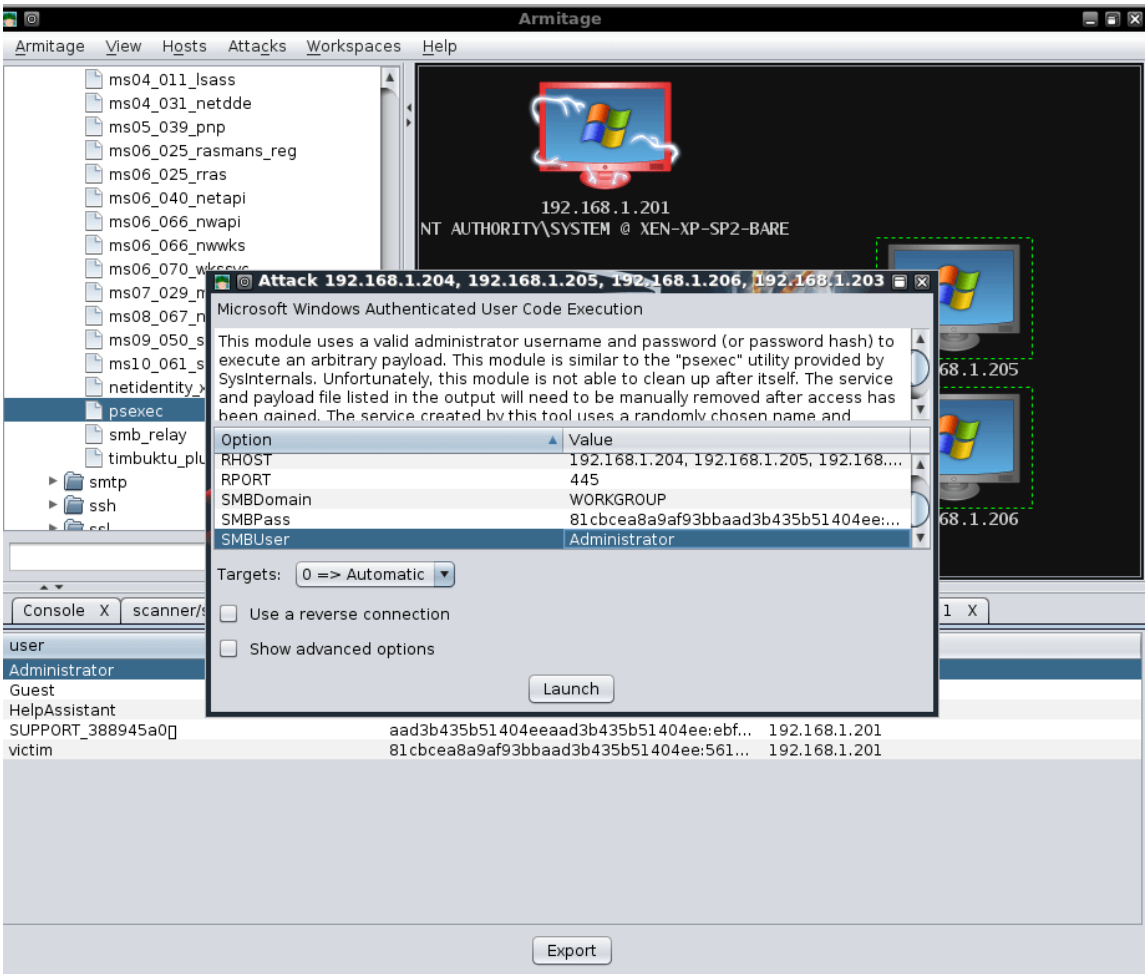


When we right-click on our exploited host, we can see a number of new and useful options available to us.

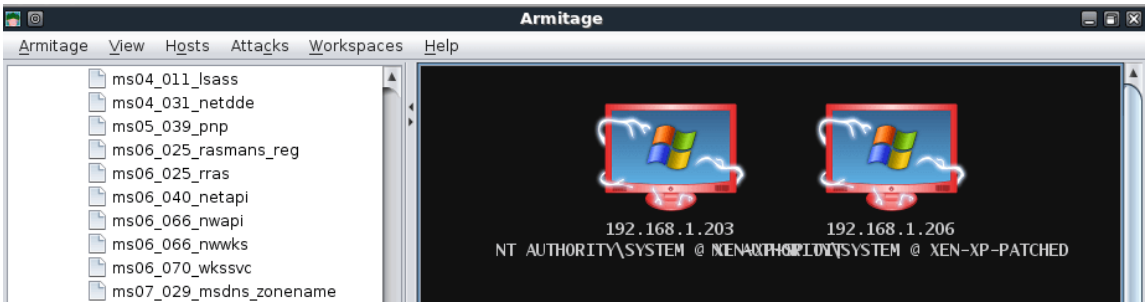


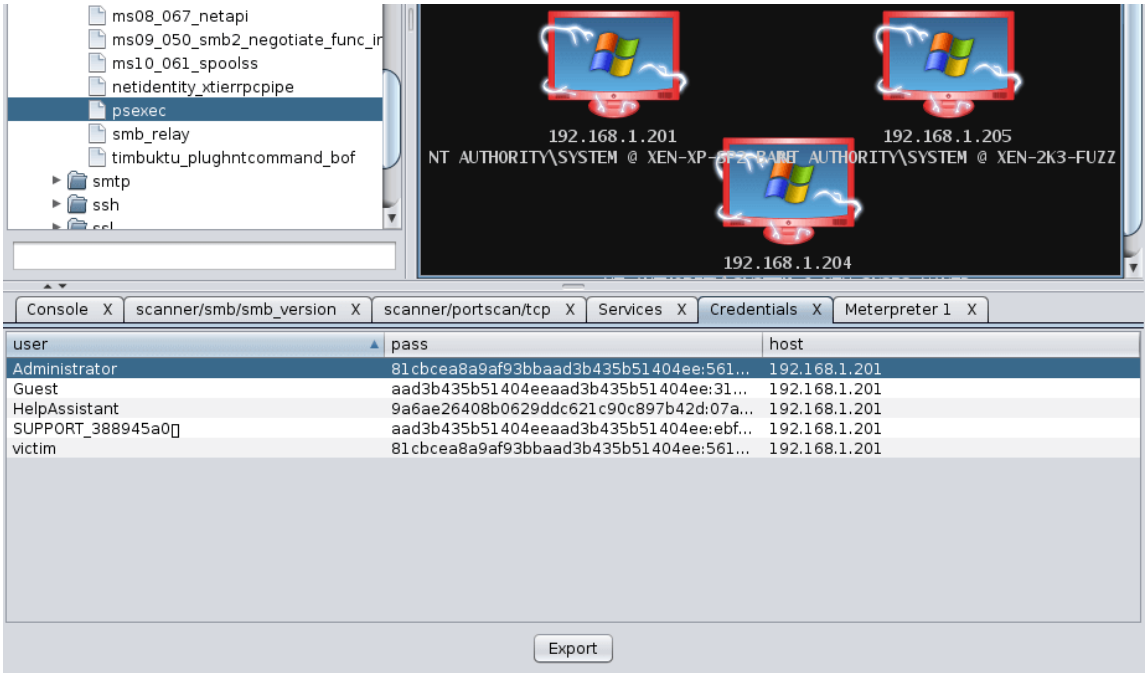


We dump the hashes on the exploited system in an attempt to leverage password re-use to exploit the other targets. Selecting the remaining hosts, we use the **psexec** module with the Administrator username and password hash we already acquired.



Now we just click ‘Launch’ and wait to receive more Meterpreter shells!





As can be plainly seen from this brief overview, Armitage provides an amazing interface to Metasploit and can be a great timesaver in many cases. A static posting cannot truly do Armitage justice but fortunately, the author has posted some videos on the Armitage Website that demonstrates the tool very well.