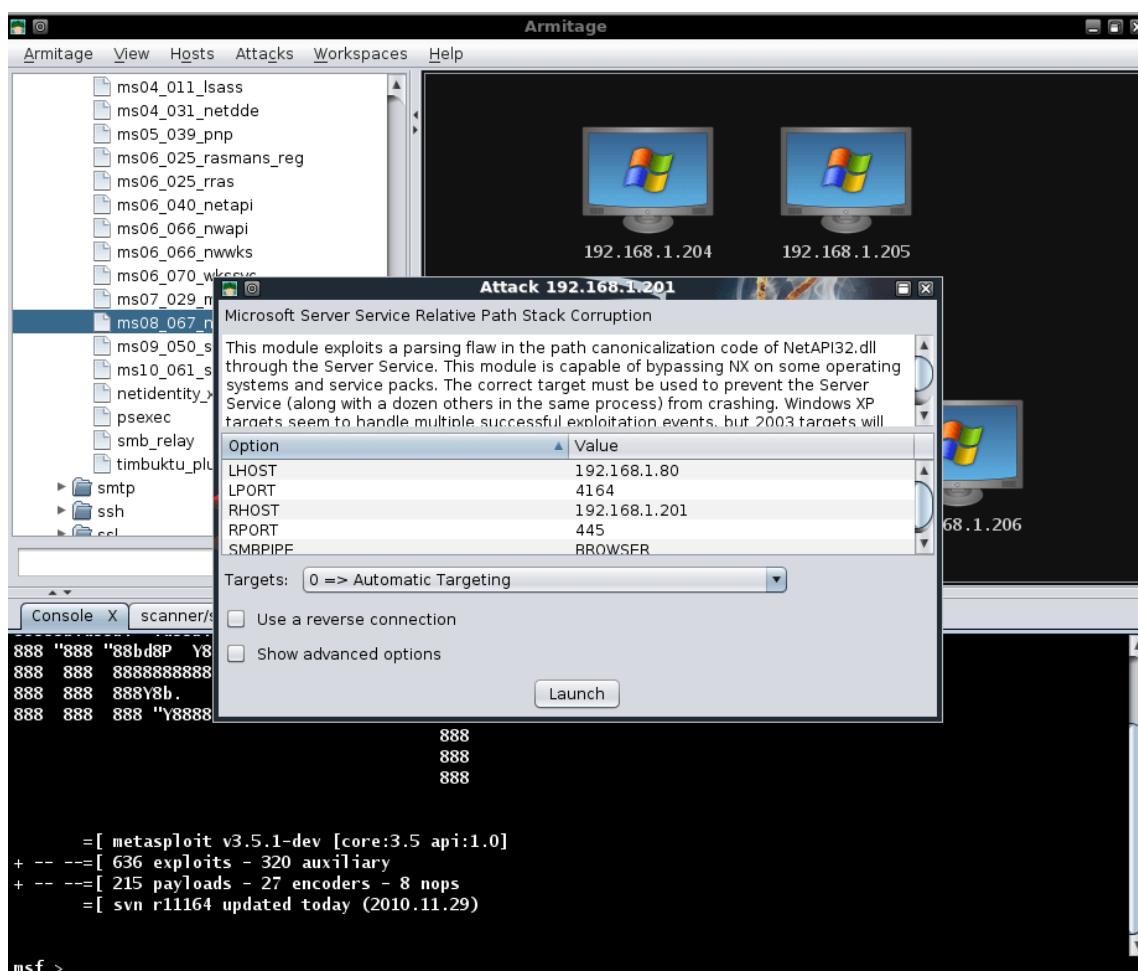


[offensive-security.com](https://www.offensive-security.com)

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

Armitage View Hosts Attacks Workspaces Help

- ms04_011_lsass
- ms04_031_netdde
- ms05_039_pnp
- ms06_025_rasmans_reg
- ms06_025_rras
- ms06_040_netapi
- ms06_066_nwapi
- ms06_066_nwwks
- ms06_070_wkssvc
- ms07_029_msdns_zonename
- ms08_067_netapi**
- ms09_050_smb2_negotiate_func_in
- ms10_061_spoolss
- netidentity_xtierrpcpipe
- psexec
- smb_relay
- timbuktu_plughntcommand_bof
- smtp
- ssh
- smb

192.168.1.204 192.168.1.205

192.168.1.203 192.168.1.201 192.168.1.206

NT AUTHORITY\SYSTEM @ XEN-XP-SP2-BARE

Console X scanner/smb/smb_version X scanner/portscan/tcp X Services X

```

888 888 "88bd8P Y8b888 "88b88k 888 "88b888d88""88b888888
888 888 8888888888888888 .d888888"Y8888b.888 8888888888 8888888888
888 888 888Y8b. Y88b. 888 888 X88888 d88P888Y88. .88P888Y88b.
888 888 888 "Y8888 "Y888"Y888888 88888P'88888P" 888 "Y88P" 888 "Y888
      888
      888
      888

      =[ metasploit v3.5.1-dev [core:3.5 api:1.0]
+ -- --=[ 636 exploits - 320 auxiliary
+ -- --=[ 215 payloads - 27 encoders - 8 nops
      =[ svn r11164 updated today (2010.11.29)

[*] Meterpreter session 1 opened (192.168.1.80:34666 -> 192.168.1.201:4164) at Mon Nov 29 20:57:00 -0500 2010
msf >
  
```

[illegible]

```

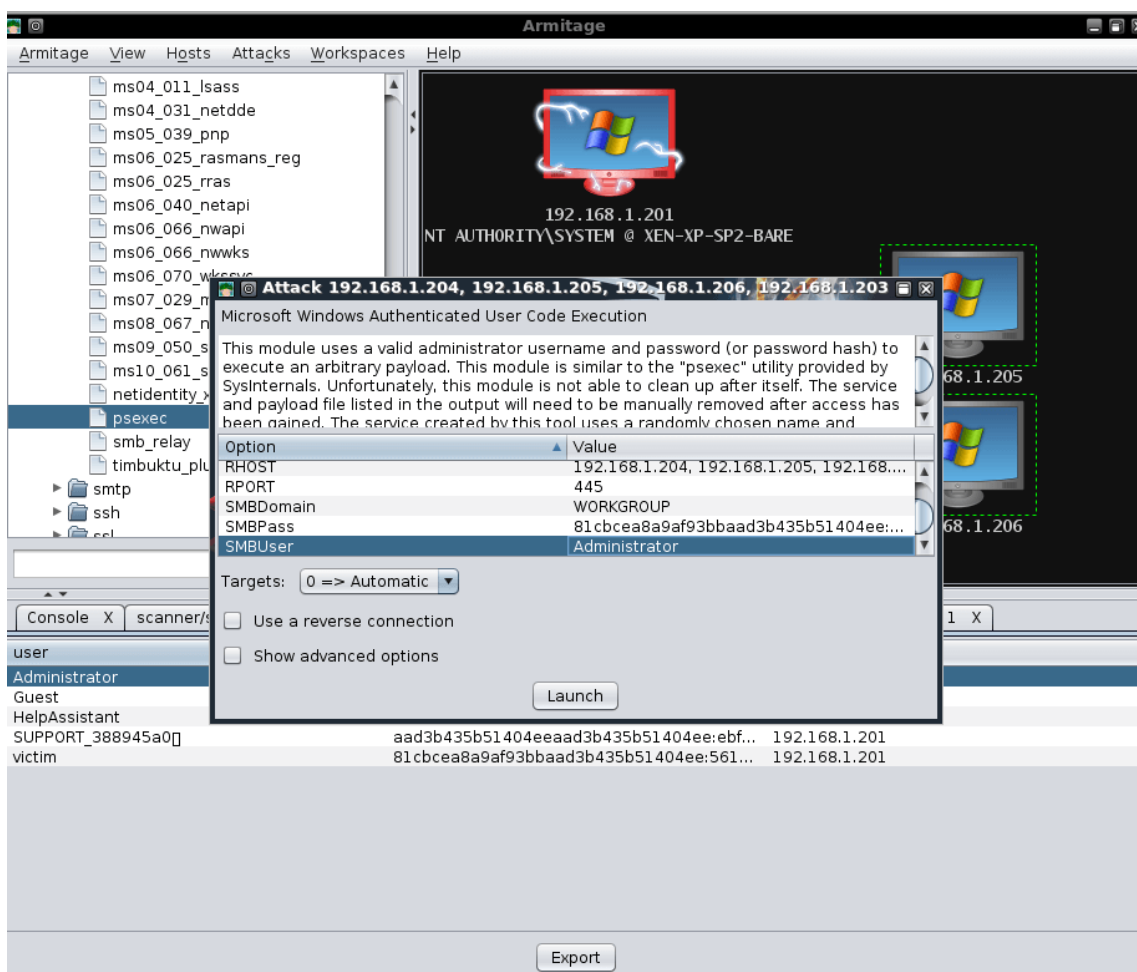
888
888
888

=[ metasploit v3.5.1-dev [core:3.5 api:1.0]
+ -- --=[ 636 exploits - 320 auxiliary
+ -- --=[ 215 payloads - 27 encoders - 8 nops
+ -- --=[ svn r11164 updated today (2010.11.29)

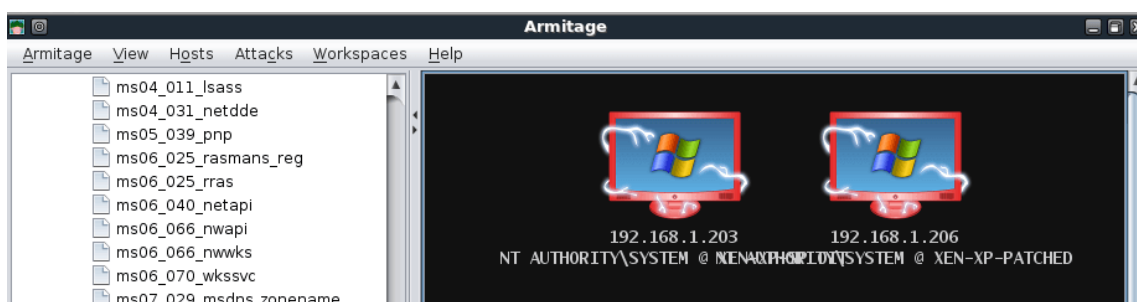
[*] Meterpreter session 1 opened (192.168.1.80:34666 -> 192.168.1.201:4164) at Mon Nov 29 20:57:00 -0500 2010
msf >

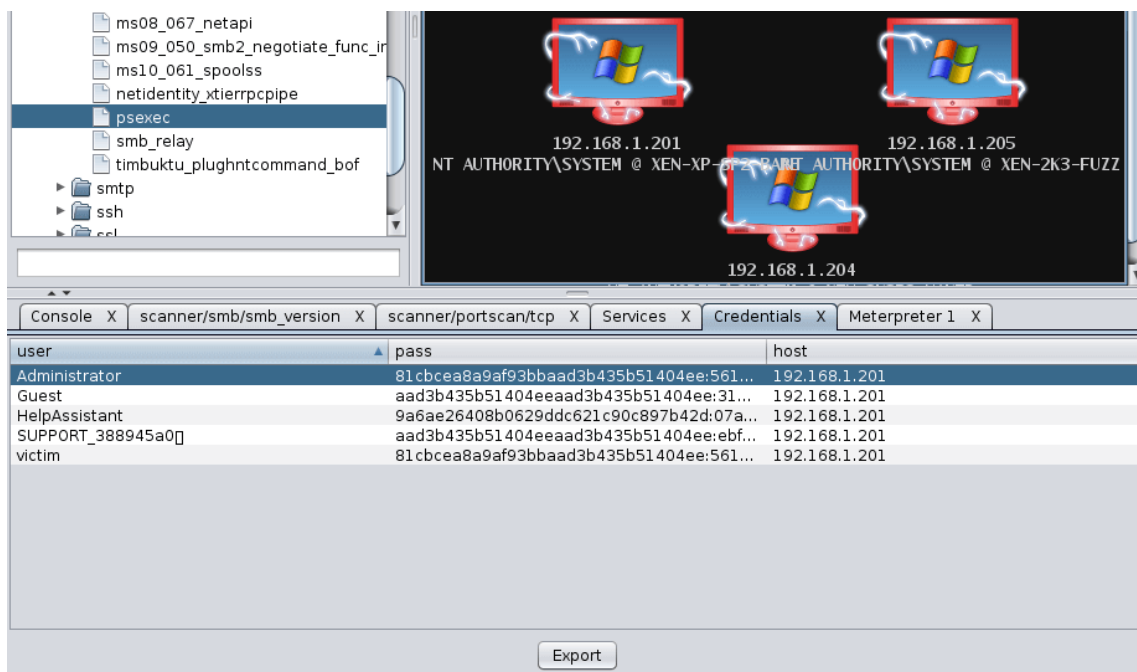
```

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.