Scanner SMB Auxiliary Modules a11y.text Scanner SMB Auxiliary Modules pipe_auditor a11y.text pipe_auditor The pipe_auditor scanner will determine what named pipes are available over SMB. In your information gathering stage, this can provide you with some insight as to some of the services that are running on the remote system. msf > use auxiliary/scanner/smb/pipe_auditor

```
msf auxiliary(pipe_auditor) > show options

Module options:

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS                      yes       The target address range or CIDR identifier
   SMBDomain  WORKGROUP        no        The Windows domain to use for authentication
   SMBPass                     no        The password for the specified username
   SMBUser                     no        The username to authenticate as
   THREADS    1                yes       The number of concurrent threads

msf auxiliary(pipe_auditor) > To run the scanner, just pass, at a minimum, the RHOSTS value to the
module and run it. msf auxiliary(pipe_auditor) > set RHOSTS 192.168.1.150-160
RHOSTS => 192.168.1.150-160
msf auxiliary(pipe_auditor) > set THREADS 11
THREADS => 11
msf auxiliary(pipe_auditor) > run

[*] 192.168.1.150 - Pipes: \browser
[*] 192.168.1.160 - Pipes: \browser
[*] Scanned 02 of 11 hosts (018% complete)
[*] Scanned 10 of 11 hosts (090% complete)
[*] Scanned 11 of 11 hosts (100% complete)
[*] Auxiliary module execution completed
```

We can see that running the scanner without credentials does not return a great deal of information. If, however, you have been provided with credentials as part of a pentest, you will find that the pipe_auditor scanner returns a great deal more information.

```
msf auxiliary(pipe_auditor) > set SMBPass s3cr3t
SMBPass => s3cr3t
msf auxiliary(pipe_auditor) > set SMBUser Administrator
SMBUser => Administrator
msf auxiliary(pipe_auditor) > run

[*] 192.168.1.150 - Pipes: \netlogon, \lsarpc, \samr, \browser, \atsvc, \DAV RPC SERVICE, \epmapper, \eventlog, \InitShutdown, \keysvc, \lsass, \ntsvcs, \protected_storage, \scerpc, \srvsvc, \trkwks, \wkssvc
[*] Scanned 02 of 11 hosts (018% complete)
[*] 192.168.1.160 - Pipes: \netlogon, \lsarpc, \samr, \browser, \atsvc, \DAV RPC SERVICE, \epmapper, \eventlog, \InitShutdown, \keysvc, \lsass, \ntsvcs, \protected_storage, \router, \scerpc, \srvsvc, \trkwks, \wkssvc
[*] Scanned 04 of 11 hosts (036% complete)
[*] Scanned 08 of 11 hosts (072% complete)
[*] Scanned 09 of 11 hosts (081% complete)
[*] Scanned 11 of 11 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(pipe_auditor) > pipe_dcerpc_auditor a11y.text pipe_dcerpc_auditor
```

The pipe_dcerpc_auditor scanner will return the DCERPC services that can be accessed via a SMB pipe.

```
msf > use auxiliary/scanner/smb/pipe_dcerpc_auditor
msf auxiliary(pipe_dcerpc_auditor) > show options

Module options:

   Name       Current Setting    Required  Description
   ----       ---------------    --------  -----------
   RHOSTS     192.168.1.150-160  yes       The target address range or CIDR identifier
   SMBDomain  WORKGROUP          no        The Windows domain to use for authentication
   SMBPIPE    BROWSER            yes       The pipe name to use (BROWSER)
   SMBPass                       no        The password for the specified username
   SMBUser                       no        The username to authenticate as
   THREADS    11                 yes       The number of concurrent threads

msf auxiliary(pipe_dcerpc_auditor) > set RHOSTS 192.168.1.150-160
RHOSTS => 192.168.1.150-160
msf auxiliary(pipe_dcerpc_auditor) > set THREADS 11
THREADS => 11
msf auxiliary(pipe_dcerpc_auditor) > run

The connection was refused by the remote host (192.168.1.153:139).
The connection was refused by the remote host (192.168.1.153:445).
192.168.1.160 - UUID 00000131-0000-0000-c000-000000000046 0.0 OPEN VIA BROWSER
192.168.1.150 - UUID 00000131-0000-0000-c000-000000000046 0.0 OPEN VIA BROWSER
192.168.1.160 - UUID 00000134-0000-0000-c000-000000000046 0.0 OPEN VIA BROWSER
192.168.1.150 - UUID 00000134-0000-0000-c000-000000000046 0.0 OPEN VIA BROWSER
192.168.1.150 - UUID 00000143-0000-0000-c000-000000000046 0.0 OPEN VIA BROWSER
```

```
192.168.1.160 - UUID 00000143-0000-0000-c000-000000000046 0.0 OPEN VIA BROWSER
...snip... smb2 a11y.text smb2 The smb2 scanner module simply scans the remote hosts and
determines if they support the SMB2 protocol. msf > use auxiliary/scanner/smb/smb2
msf auxiliary(smb2) > show options

Module options:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target address range or CIDR identifier
   RPORT    445              yes       The target port
   THREADS  1                yes       The number of concurrent threads

msf auxiliary(smb2) > set RHOSTS 192.168.1.150-165
RHOSTS => 192.168.1.150-165
msf auxiliary(smb2) > set THREADS 16
THREADS => 16
msf auxiliary(smb2) > run

[*] 192.168.1.162 supports SMB 2 [dialect 255.2] and has been online for 618 hours
[*] Scanned 06 of 16 hosts (037% complete)
[*] Scanned 13 of 16 hosts (081% complete)
[*] Scanned 14 of 16 hosts (087% complete)
[*] Scanned 16 of 16 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smb2) > smb_enumshares a11y.text smb_enumshares The smb_enumshares module,
```

as would be expected, enumerates any SMB shares that are available on a remote system. msf >

```
use auxiliary/scanner/smb/smb_enumshares

msf auxiliary(smb_enumshares) > show options


Module options (auxiliary/scanner/smb/smb_enumshares):


   Name             Current Setting  Required  Description

   ----             ---------------  --------  -----------

   LogSpider        3                no        0 = disabled, 1 = CSV, 2 = table (txt), 3 = one liner (txt)

(Accepted: 0, 1, 2, 3)

   MaxDepth         999              yes       Max number of subdirectories to spider

   RHOSTS                            yes       The target address range or CIDR identifier

   SMBDomain        .                no        The Windows domain to use for authentication

   SMBPass                           no        The password for the specified username

   SMBUser                           no        The username to authenticate as

   ShowFiles        false            yes       Show detailed information when spidering

   SpiderProfiles   true             no        Spider only user profiles when share = C$

   SpiderShares     false            no        Spider shares recursively

   THREADS          1                yes       The number of concurrent threads

   USE_SRVSVC_ONLY  false            yes       List shares only with SRVSVC


msf auxiliary(smb_enumshares) > set RHOSTS 192.168.1.150-165

RHOSTS => 192.168.1.150-165

msf auxiliary(smb_enumshares) > set THREADS 16

THREADS => 16

msf auxiliary(smb_enumshares) > run
```

```
[*] 192.168.1.154:139 print$ - Printer Drivers (DISK), tmp - oh noes! (DISK), opt -  (DISK), IPC$ - IPC Service (metasploitable server (Samba 3.0.20-Debian)) (IPC), ADMIN$ - IPC Service (metasploitable server (Samba 3.0.20-Debian)) (IPC)
Error: 192.168.1.160 Rex::Proto::SMB::Exceptions::ErrorCode The server responded with error: STATUS_ACCESS_DENIED (Command=37 WordCount=0)
Error: 192.168.1.160 Rex::Proto::SMB::Exceptions::ErrorCode The server responded with error: STATUS_ACCESS_DENIED (Command=37 WordCount=0)
[*] 192.168.1.161:139 IPC$ - Remote IPC (IPC), ADMIN$ - Remote Admin (DISK), C$ - Default share (DISK)
Error: 192.168.1.162 Rex::Proto::SMB::Exceptions::ErrorCode The server responded with error: STATUS_ACCESS_DENIED (Command=37 WordCount=0)
Error: 192.168.1.150 Rex::Proto::SMB::Exceptions::ErrorCode The server responded with error: STATUS_ACCESS_DENIED (Command=37 WordCount=0)
Error: 192.168.1.150 Rex::Proto::SMB::Exceptions::ErrorCode The server responded with error: STATUS_ACCESS_DENIED (Command=37 WordCount=0)
[*] Scanned 06 of 16 hosts (037% complete)
[*] Scanned 09 of 16 hosts (056% complete)
[*] Scanned 10 of 16 hosts (062% complete)
[*] Scanned 14 of 16 hosts (087% complete)
[*] Scanned 15 of 16 hosts (093% complete)
[*] Scanned 16 of 16 hosts (100% complete)
[*] Auxiliary module execution completed
```

msf auxiliary(smb_enumshares) > As you can see, since this is an un-credentialed scan, access is denied a most of the systems that are probed. Passing user credentials to the scanner will produce much different results. msf auxiliary(smb_enumshares) > set SMBPass s3cr3t

```
SMBPass => s3cr3t
msf auxiliary(smb_enumshares) > set SMBUser Administrator
SMBUser => Administrator
msf auxiliary(smb_enumshares) > run

[*] 192.168.1.161:139 IPC$ - Remote IPC (IPC), ADMIN$ - Remote Admin (DISK), C$ - Default
share (DISK)
[*] 192.168.1.160:139 IPC$ - Remote IPC (IPC), ADMIN$ - Remote Admin (DISK), C$ - Default
share (DISK)
[*] 192.168.1.150:139 IPC$ - Remote IPC (IPC), ADMIN$ - Remote Admin (DISK), C$ - Default
share (DISK)
[*] Scanned 06 of 16 hosts (037% complete)
[*] Scanned 07 of 16 hosts (043% complete)
[*] Scanned 12 of 16 hosts (075% complete)
[*] Scanned 15 of 16 hosts (093% complete)
[*] Scanned 16 of 16 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smb_enumshares) > smb_enumusers a11y.text smb_enumusers The smb_enumusers
scanner will connect to each system via the SMB RPC service and enumerate the users on the
system. msf > use auxiliary/scanner/smb/smb_enumusers
msf auxiliary(smb_enumusers) > show options

Module options:

  Name       Current Setting  Required  Description
  ----       ---------------  --------  -----------
  RHOSTS                    yes       The target address range or CIDR identifier
  SMBDomain  WORKGROUP       no        The Windows domain to use for authentication
  SMBPass                   no        The password for the specified username
  SMBUser                   no        The username to authenticate as
  THREADS    1               yes       The number of concurrent threads

msf auxiliary(smb_enumusers) > set RHOSTS 192.168.1.150-165
RHOSTS => 192.168.1.150-165
msf auxiliary(smb_enumusers) > set THREADS 16
THREADS => 16
msf auxiliary(smb_enumusers) > run

[*] 192.168.1.161 XEN-XP-SP2-BARE [  ]
[*] 192.168.1.154 METASPLOITABLE [ games, nobody, bind, proxy, syslog, user, www-data, root,
news, postgres, bin, mail, distccd, proftpd, dhcp, daemon, sshd, man, lp, mysql, gnats, libuuid,
backup, msfadmin, telnetd, sys, klog, postfix, service, list, irc, ftp, tomcat55, sync, uucp ] (
LockoutTries=0 PasswordMin=5 )
[*] Scanned 05 of 16 hosts (031% complete)
[*] Scanned 12 of 16 hosts (075% complete)
[*] Scanned 15 of 16 hosts (093% complete)
[*] Scanned 16 of 16 hosts (100% complete)
[*] Auxiliary module execution completed
```

We can see that running the scan without credentials, only the Linux Samba service coughs up a listing of users. Passing a valid set of credentials to the scanner will enumerate the users on our other targets.

```
msf auxiliary(smb_enumusers) > set SMBPass s3cr3t
SMBPass => s3cr3t
```

```
msf auxiliary(smb_enumusers) > set SMBUser Administrator
SMBUser => Administrator
msf auxiliary(smb_enumusers) > run

[*] 192.168.1.150 V-XPSP2-SPLOIT- [ Administrator, Guest, HelpAssistant, SUPPORT_388945a0 ]
[*] Scanned 04 of 16 hosts (025% complete)
[*] 192.168.1.161 XEN-XP-SP2-BARE [ Administrator, Guest, HelpAssistant, SUPPORT_388945a0, victim ]
[*] 192.168.1.160 XEN-XP-PATCHED [ Administrator, ASPNET, Guest, HelpAssistant, SUPPORT_388945a0 ]
[*] Scanned 09 of 16 hosts (056% complete)
[*] Scanned 13 of 16 hosts (081% complete)
[*] Scanned 15 of 16 hosts (093% complete)
[*] Scanned 16 of 16 hosts (100% complete)
[*] Auxiliary module execution completed
```

msf auxiliary(smb_enumusers) > Now that we have passed credentials to the scanner, the Linux box doesnâ€™t return the set of users because the credentials are not valid for that system. This is an example of why it pays to run a scanner in different configurations. smb_login a11y.text smb_login Metasploitâ€™s smb_login module will attempt to login via SMB across a provided range of IP addresses. If you have a database plugin loaded, successful logins will be stored in it for future reference and usage. msf > use auxiliary/scanner/smb/smb_login

```
msf auxiliary(smb_login) > show options

Module options (auxiliary/scanner/smb/smb_login):

   Name           Current Setting                 Required  Description
   ----              ---------------                    --------  -----------
   ABORT_ON_LOCKOUT  false                              yes       Abort the run when an account lockout
is detected
   BLANK_PASSWORDS   false                              no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                  yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                              no        Try each user/password couple stored in the
current database
   DB_ALL_PASS       false                              no        Add all passwords in the current database to
the list
   DB_ALL_USERS      false                              no        Add all users in the current database to the
list
   DETECT_ANY_AUTH   true                               no        Enable detection of systems accepting
any authentication
   PASS_FILE         /usr/share/wordlists/fasttrack.txt  no        File containing passwords, one per line
   PRESERVE_DOMAINS  true                               no        Respect a username that contains a
domain name.
   Proxies                                              no        A proxy chain of format
type:host:port[,type:host:port][...]
   RECORD_GUEST      false                              no        Record guest-privileged random logins to
the database
   RHOSTS                                               yes       The target address range or CIDR identifier
   RPORT             445                                yes       The SMB service port (TCP)
   SMBDomain         .                                  no        The Windows domain to use for authentication
   SMBPass                                              no        The password for the specified username
   SMBUser                                              no        The username to authenticate as
   STOP_ON_SUCCESS   false                              yes       Stop guessing when a credential works
```

```
for a host
   THREADS          1                              yes       The number of concurrent threads
   USERPASS_FILE                                   no        File containing users and passwords
separated by space, one pair per line
   USER_AS_PASS      false                         no        Try the username as the password for all
users
   USER_FILE                                       no        File containing usernames, one per line
   VERBOSE           true                          yes       Whether to print output for all attempts
```

You can clearly see that this module has many more options that other auxiliary modules and is quite versatile. We will first run a scan using the Administrator credentials we found.

```
msf auxiliary(smb_login) > set RHOSTS 192.168.1.150-165
RHOSTS => 192.168.1.150-165
msf auxiliary(smb_login) > set SMBPass s3cr3t
SMBPass => s3cr3t
msf auxiliary(smb_login) > set SMBUser Administrator
SMBUser => Administrator
msf auxiliary(smb_login) > set THREADS 16
THREADS => 16
msf auxiliary(smb_login) > run

[*] Starting SMB login attempt on 192.168.1.165
[*] Starting SMB login attempt on 192.168.1.153
...snip...
[*] Starting SMB login attempt on 192.168.1.156
[*] 192.168.1.154 - FAILED LOGIN () Administrator :  (STATUS_LOGON_FAILURE)
[*] 192.168.1.150 - FAILED LOGIN (Windows 5.1) Administrator :  (STATUS_LOGON_FAILURE)
[*] 192.168.1.160 - FAILED LOGIN (Windows 5.1) Administrator :  (STATUS_LOGON_FAILURE)
[*] 192.168.1.154 - FAILED LOGIN () Administrator : s3cr3t (STATUS_LOGON_FAILURE)
[-] 192.168.1.162 - FAILED LOGIN (Windows 7 Enterprise 7600) Administrator : (STATUS_ACCOUNT_DISABLED)
[*] 192.168.1.161 - FAILED LOGIN (Windows 5.1) Administrator :  (STATUS_LOGON_FAILURE)
[+] 192.168.1.150 - SUCCESSFUL LOGIN (Windows 5.1) 'Administrator' : 's3cr3t'
[*] Scanned 04 of 16 hosts (025% complete)
[+] 192.168.1.160 - SUCCESSFUL LOGIN (Windows 5.1) 'Administrator' : 's3cr3t'
[+] 192.168.1.161 - SUCCESSFUL LOGIN (Windows 5.1) 'Administrator' : 's3cr3t'
[*] Scanned 13 of 16 hosts (081% complete)
[*] Scanned 14 of 16 hosts (087% complete)
[*] Scanned 15 of 16 hosts (093% complete)
[*] Scanned 16 of 16 hosts (100% complete)
[*] Auxiliary module execution completed
```

msf auxiliary(smb_login) > The smb_login module can also be passed a username and password list in order to attempt to brute-force login attempts across a range of machines. root@kali : ~ # cat users.txt Administrator

dale

chip

dookie

victim

jimmie root@kali : ~ # cat passwords.txt password

god

password123

s00pers3kr1t

s3cr3t We will use this limited set of usernames and passwords and run the scan again. msf

```
auxiliary(smb_login) > show options


Module options:


   Name              Current Setting  Required  Description

   ----              ---------------  --------  -----------

   BLANK_PASSWORDS   true             yes       Try blank passwords for all users

   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5

   PASS_FILE                          no        File containing passwords, one per line

   RHOSTS                             yes       The target address range or CIDR identifier

   RPORT             445              yes       Set the SMB service port

   SMBDomain         WORKGROUP        no        SMB Domain

   SMBPass                            no        SMB Password

   SMBUser                            no        SMB Username

   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host

   THREADS           1                yes       The number of concurrent threads

   USERPASS_FILE                      no        File containing users and passwords separated by space,
one pair per line

   USER_FILE                          no        File containing usernames, one per line

   VERBOSE           true             yes       Whether to print output for all attempts


msf auxiliary(smb_login) > set PASS_FILE /root/passwords.txt

PASS_FILE => /root/passwords.txt

msf auxiliary(smb_login) > set USER_FILE /root/users.txt

USER_FILE => /root/users.txt

msf auxiliary(smb_login) > set RHOSTS 192.168.1.150-165
```

```
RHOSTS => 192.168.1.150-165

msf auxiliary(smb_login) > set THREADS 16

THREADS => 16

msf auxiliary(smb_login) > set VERBOSE false

VERBOSE => false

msf auxiliary(smb_login) > run


[-] 192.168.1.162 - FAILED LOGIN (Windows 7 Enterprise 7600) Administrator :

(STATUS_ACCOUNT_DISABLED)

[*] 192.168.1.161 - GUEST LOGIN (Windows 5.1) dale :

[*] 192.168.1.161 - GUEST LOGIN (Windows 5.1) chip :

[*] 192.168.1.161 - GUEST LOGIN (Windows 5.1) dookie :

[*] 192.168.1.161 - GUEST LOGIN (Windows 5.1) jimmie :

[+] 192.168.1.150 - SUCCESSFUL LOGIN (Windows 5.1) 'Administrator' : 's3cr3t'

[+] 192.168.1.160 - SUCCESSFUL LOGIN (Windows 5.1) 'Administrator' : 's3cr3t'

[+] 192.168.1.161 - SUCCESSFUL LOGIN (Windows 5.1) 'Administrator' : 's3cr3t'

[+] 192.168.1.161 - SUCCESSFUL LOGIN (Windows 5.1) 'victim' : 's3cr3t'

[+] 192.168.1.162 - SUCCESSFUL LOGIN (Windows 7 Enterprise 7600) 'victim' : 's3cr3t'

[*] Scanned 15 of 16 hosts (093% complete)

[*] Scanned 16 of 16 hosts (100% complete)

[*] Auxiliary module execution completed
```

msf auxiliary(smb_login) > There are many more options available that you should experiment with to fully familiarize yourself with this extremely valuable module. smb_lookupsid a11y.text smb_lookupsid The smb_lookupsid module brute-forces SID lookups on a range of targets to determine what local users exist the system. Knowing what users exist on a system can greatly speed up any further brute-force logon attempts later on. msf > use

```
auxiliary/scanner/smb/smb_lookupsid

msf auxiliary(smb_lookupsid) > show options


Module options (auxiliary/scanner/smb/smb_lookupsid):


   Name       Current Setting  Required  Description

   ----       ---------------  --------  -----------

   MaxRID     4000             no        Maximum RID to check

   RHOSTS                      yes       The target address range or CIDR identifier

   SMBDomain  .                no        The Windows domain to use for authentication

   SMBPass                     no        The password for the specified username

   SMBUser                     no        The username to authenticate as

   THREADS    1                yes       The number of concurrent threads



Auxiliary action:


   Name   Description

   ----   -----------

   LOCAL  Enumerate local accounts


msf auxiliary(smb_lookupsid) > set RHOSTS 192.168.1.150-165

RHOSTS => 192.168.1.150-165

msf auxiliary(smb_lookupsid) > set THREADS 16

THREADS => 16

msf auxiliary(smb_lookupsid) > run
```

```
[*] 192.168.1.161 PIPE(LSARPC) LOCAL(XEN-XP-SP2-BARE -
5-21-583907252-1801674531-839522115) DOMAIN(HOTZONE - )
[*] 192.168.1.154 PIPE(LSARPC) LOCAL(METASPLOITABLE -
5-21-1042354039-2475377354-766472396) DOMAIN(WORKGROUP - )
[*] 192.168.1.161 USER=Administrator RID=500
[*] 192.168.1.154 USER=Administrator RID=500
[*] 192.168.1.161 USER=Guest RID=501
[*] 192.168.1.154 USER=nobody RID=501
[*] Scanned 04 of 16 hosts (025% complete)
[*] 192.168.1.154 GROUP=Domain Admins RID=512
[*] 192.168.1.161 GROUP=None RID=513
[*] 192.168.1.154 GROUP=Domain Users RID=513
[*] 192.168.1.154 GROUP=Domain Guests RID=514
[*] Scanned 07 of 16 hosts (043% complete)
[*] 192.168.1.154 USER=root RID=1000
...snip...
[*] 192.168.1.154 GROUP=service RID=3005
[*] 192.168.1.154 METASPLOITABLE [Administrator, nobody, root, daemon, bin, sys, sync, games,
man, lp, mail, news, uucp, proxy, www-data, backup, list, irc, gnats, libuuid, dhcp, syslog, klog, sshd,
bind, postfix, ftp, postgres, mysql, tomcat55, distccd, telnetd, proftpd, msfadmin, user, service ]
[*] Scanned 15 of 16 hosts (093% complete)
[*] 192.168.1.161 XEN-XP-SP2-BARE [Administrator, Guest, HelpAssistant, SUPPORT_388945a0,
victim ]
[*] Scanned 16 of 16 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
msf auxiliary(smb_lookupsid) > By way of comparison, we will also run the scan using a known set of user credentials to see the difference in output. msf auxiliary(smb_lookupsid) > set SMBPass s3cr3t
SMBPass => s3cr3t
msf auxiliary(smb_lookupsid) > set SMBUser Administrator
SMBUser => Administrator
msf auxiliary(smb_lookupsid) > run

[*] 192.168.1.160 PIPE(LSARPC) LOCAL(XEN-XP-PATCHED - 5-21-583907252-1801674531-839522115) DOMAIN(HOTZONE - )
[*] 192.168.1.161 PIPE(LSARPC) LOCAL(XEN-XP-SP2-BARE - 5-21-583907252-1801674531-839522115) DOMAIN(HOTZONE - )
[*] 192.168.1.161 USER=Administrator RID=500
[*] 192.168.1.160 USER=Administrator RID=500
[*] 192.168.1.150 PIPE(LSARPC) LOCAL(V-XPSP2-SPLOIT- - 5-21-2000478354-1965331169-725345543) DOMAIN(WORKGROUP - )
[*] 192.168.1.160 USER=Guest RID=501
[*] 192.168.1.150 TYPE=83886081 NAME=Administrator rid=500
[*] 192.168.1.161 USER=Guest RID=501
[*] 192.168.1.150 TYPE=83886081 NAME=Guest rid=501
[*] 192.168.1.160 GROUP=None RID=513
[*] 192.168.1.150 TYPE=83886082 NAME=None rid=513
[*] 192.168.1.161 GROUP=None RID=513
[*] 192.168.1.150 TYPE=83886081 NAME=HelpAssistant rid=1000
[*] 192.168.1.150 TYPE=83886084 NAME=HelpServicesGroup rid=1001
[*] 192.168.1.150 TYPE=83886081 NAME=SUPPORT_388945a0 rid=1002
[*] 192.168.1.150 TYPE=3276804
NAME=SQLServerMSSQLServerADHelperUser$DOOKIE-FA154354 rid=1003
[*] 192.168.1.150 TYPE=4 NAME=SQLServer2005SQLBrowserUser$DOOKIE-FA154354 rid=1004
...snip...
[*] 192.168.1.160 TYPE=651165700
NAME=SQLServer2005MSSQLServerADHelperUser$XEN-XP-PATCHED rid=1027
[*] 192.168.1.160 TYPE=651165700
NAME=SQLServer2005MSSQLUser$XEN-XP-PATCHED$SQLEXPRESS rid=1028
[*] 192.168.1.161 USER=HelpAssistant RID=1000
[*] 192.168.1.161 TYPE=4 NAME=HelpServicesGroup rid=1001
[*] 192.168.1.161 USER=SUPPORT_388945a0 RID=1002
[*] 192.168.1.161 USER=victim RID=1004
[*] 192.168.1.160 XEN-XP-PATCHED [Administrator, Guest, HelpAssistant, SUPPORT_388945a0,
ASPNET ]
[*] 192.168.1.150 V-XPSP2-SPLOIT- [ ]
[*] Scanned 15 of 16 hosts (093% complete)
[*] 192.168.1.161 XEN-XP-SP2-BARE [Administrator, Guest, HelpAssistant, SUPPORT_388945a0,
victim ]
[*] Scanned 16 of 16 hosts (100% complete)
[*] Auxiliary module execution completed
```

msf auxiliary(smb_lookupsid) > You will notice with credentialed scanning, that you get, as always, a great deal more interesting output, including accounts you likely never knew existed. smb_version a11y.text smb_version The smb_version scanner connects to each workstation in a given range of hosts and determines the version of the SMB service that is running. msf > use auxiliary/scanner/smb/smb_version

```
msf auxiliary(smb_version) > show options
```

```
Module options:

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   RHOSTS                      yes       The target address range or CIDR identifier
   SMBDomain  WORKGROUP        no        The Windows domain to use for authentication
   SMBPass                     no        The password for the specified username
   SMBUser                     no        The username to authenticate as
   THREADS    1                yes       The number of concurrent threads

msf auxiliary(smb_version) > set RHOSTS 192.168.1.150-165
RHOSTS => 192.168.1.150-165
msf auxiliary(smb_version) > set THREADS 16
THREADS => 16
msf auxiliary(smb_version) > run

[*] 192.168.1.162 is running Windows 7 Enterprise (Build 7600) (language: Unknown)
(name:XEN-WIN7-BARE) (domain:HOTZONE)
[*] 192.168.1.154 is running Unix Samba 3.0.20-Debian (language: Unknown)
(domain:WORKGROUP)
[*] 192.168.1.150 is running Windows XP Service Pack 2 (language: English)
(name:V-XPSP2-SPLOIT-) (domain:WORKGROUP)
[*] Scanned 04 of 16 hosts (025% complete)
[*] 192.168.1.160 is running Windows XP Service Pack 3 (language: English)
(name:XEN-XP-PATCHED) (domain:HOTZONE)
```

```
[*] 192.168.1.161 is running Windows XP Service Pack 2 (language: English)
(name:XEN-XP-SP2-BARE) (domain:XEN-XP-SP2-BARE)
[*] Scanned 11 of 16 hosts (068% complete)
[*] Scanned 14 of 16 hosts (087% complete)
[*] Scanned 16 of 16 hosts (100% complete)
[*] Auxiliary module execution completed
```

Running this same scan with a set of credentials will return some different, and perhaps unexpected, results.

```
msf auxiliary(smb_version) > set SMBPass s3cr3t
SMBPass => s3cr3t
msf auxiliary(smb_version) > set SMBUser Administrator
SMBUser => Administrator
msf auxiliary(smb_version) > run

[*] 192.168.1.160 is running Windows XP Service Pack 3 (language: English)
(name:XEN-XP-PATCHED) (domain:XEN-XP-PATCHED)
[*] 192.168.1.150 is running Windows XP Service Pack 2 (language: English)
(name:V-XPSP2-SPLOIT-) (domain:V-XPSP2-SPLOIT-)
[*] Scanned 05 of 16 hosts (031% complete)
[*] 192.168.1.161 is running Windows XP Service Pack 2 (language: English)
(name:XEN-XP-SP2-BARE) (domain:XEN-XP-SP2-BARE)
[*] Scanned 12 of 16 hosts (075% complete)
[*] Scanned 14 of 16 hosts (087% complete)
[*] Scanned 15 of 16 hosts (093% complete)
[*] Scanned 16 of 16 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smb_version) >
```

Contrary to many other cases, a credentialed scan in this case does not necessarily give better results. If the credentials are not valid on a particular system, you will not get any result back from the scan. Next Scanner SMTP Auxiliary Modules Prev Scanner POP3 Auxiliary Modules