**Lab – Brute Force the SMB Password on a Windows Server**

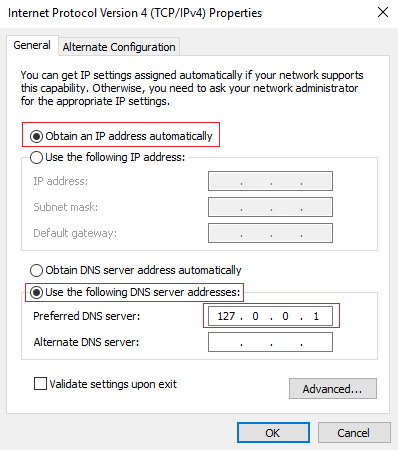
**Overview**

In this lab, you will learn how to brute force the SMB password from a Windows Server configured 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.



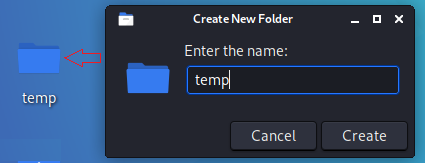
**Begin the lab!**

**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.

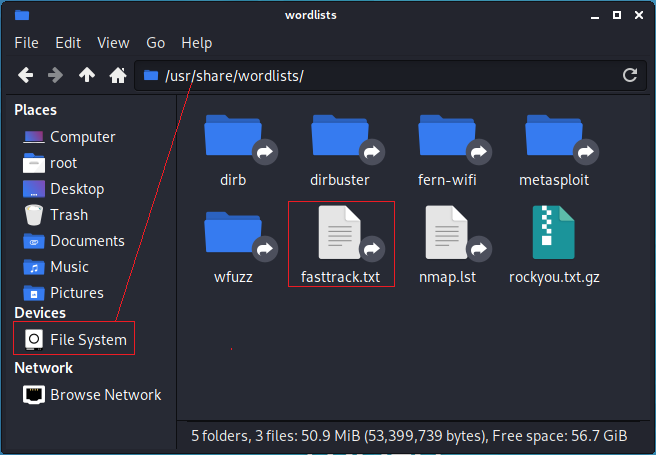
We have one of the two parts we need, the user account. We next need to obtain the password for the user account. For this, we can use the use **auxiliary/scanner/smb/smb\_login** module available in Metasploit.

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**

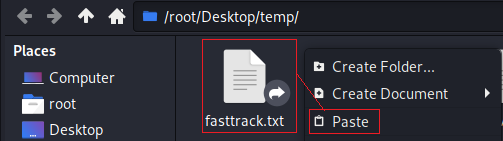
From the Desktop of your Kali machine, open the folder marked **File System**. Browse to the wordlist's directory using the path, **File System/usr/share/wordlists/.** Inside the wordlist's directory, find the wordlist labeled **fasttrack.txt**. Right-click, and from the context menu, select **copy**.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



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.

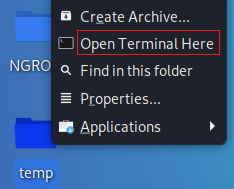
**Add your password to the wordlist**

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.

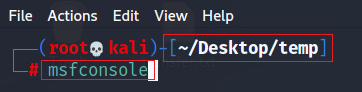


We could attempt to brute force the password with a massive list of passwords, but that would take hours, possibly days.

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.

****

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**.

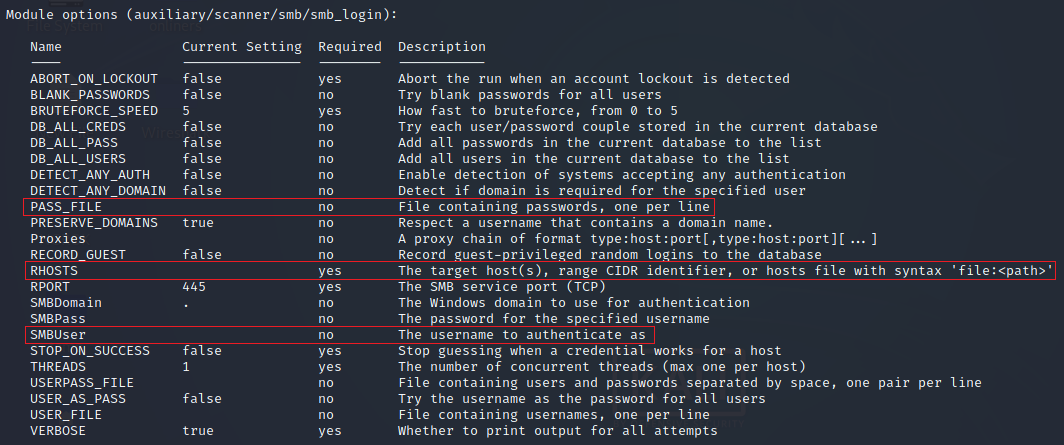


Under options, you will find the three that we need to configure for this module to work.

**PASS\_FILE** – The wordlist that contains an SMB password for the remote target.

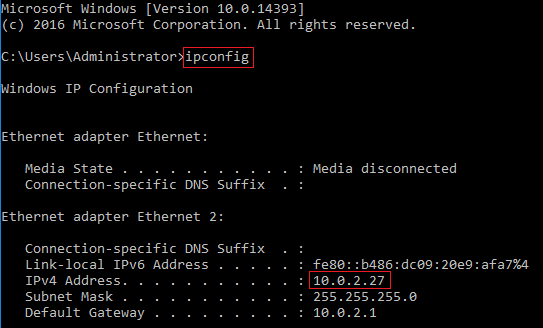
**RHOSTS** – The IP address of the remote target.

**SMBUser** – The user account of an authorized user.



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!



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**

****

**set rhost 10.0.2.27**

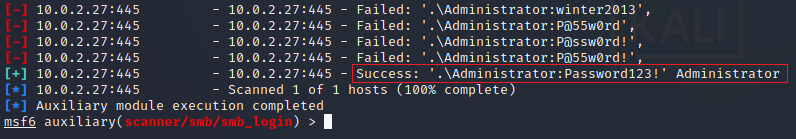
****

**set SMBUser Administrator**

****

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.



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.