CS 378 Final Project Report:
Automating SMB Mounting

Dustin Huang, Godfrey Macasero, Aish Shashidhar, Allen Zhang

November 28, 2018

1 What is our Tool?

Our tool is an automation service that allows mounting onto a SMB server with the ability to crack the required password needed to access the server. To run this tool, the following parameters are needed.

- Mounting location
- Windows Server Name
- Username
- Password (Optional)
- Copy(Optional)

Commands

Run the script with the password flag if the password is known. If no password is passed in the parameter, the tool will brute force the password.

Password Known: *python3 smbattack –mountloc ./mount –serverIP SMB-Server –username admin –password password –copy True/False*

Password Unknown (Brute Force): *python3 smbattack –mountloc ./mount –serverIP SMB-Server –username admin –copy True/False*

2 How does it work?

A. Password Cracking

Hydra is a network logon cracker tested on multiple well-known protocols, including smb. It is a brute force password cracker which tries multiple passwords with a given username to crack the password.

B. Finding the Mount Point

Smbclient is a samba client that has an interface like ftp. It is a tool that can be used to test connectivity in a Windows share. We use this to find out the name of the mount point using the -L tag with the IP address of the user we are trying to get files from.

C. Mounting the SMB Directory

Cifs(Common Internet File System) is a particular implementation of the Server Message Block protocol, created by Microsoft. We chose to use this instead of smbfs because it is not maintained anymore.

3 What problems did we encounter?

- Syntax Errors - We decided to use the argparse library to help us pass arguments to external calls (hydra, smbclient, etc). We ran into a problem where the arguments were seemingly being passed incorrectly despite the syntax being correct. The issue was resolved when we realized that adding one compound argument(such as -p password) was not the same as adding two arguments(-p and password separately).
- Unable to find smb mount point - Another issue was when we were trying to search for the mounting point using smb client we could not figure out the issue so we just had to reset our vm with Windows.
- SMB mounting created a symlink instead of a copy
- Figuring out why mounting did not work (it had to be in the bridged connection)
- Setting up the windows smb client was very difficult. When we set up the shared folder on a client, it would work correctly with our tool sometimes, and other times give us errors, like *NT_STATUS_REVISION_MISMATCH*.
- There isnt a lot of documentation on these errors, or any indication why the client is unstable. We are using SMB1 for this software because it is insecure. Because SMB1 is outdated software, we concluded that this bug is likely something Microsoft has not spent time fixing, and thus is unstable.

4 What can we improve?

A. Automate more parts of Process

Automate Nmap so it finds all the IP addresses that have port 445 open. Use crackmapexec to find all the users in the shared network

B. Salted Passwords

Hydra only handles unsalted passwords. A stronger password cracking tool would be John The Ripper. If we can access a password hash on the SMB mount point, we would be able to use John to crack that hash.

C. Graceful Mount Point access

Right now, our tool is generating a file to store the mount point(s) of the SMB server, then parsing the file to mount the mountpoint(s). A sleeker solution would do this in memory, instead of saving this information to disk. The difficulty is that the output is the result of a unix function call, and all of this information needs to be stored somewhere, not sent to stdout. This is only available for very recent versions of python3.

(https://stackoverflow.com/questions/4760215/running-shell-command-and-capturing-the-output)

D. Graceful Error Handling

Right now, if an error occurs while trying to find the mountpoint of the server, we send the output back to the user. To improve the usability of our tool, our group could provide detailed suggestions depending on the error the server sent back.