**Demo 2: Attack on Windows Defender via Disabling MIC & Token Revoking**

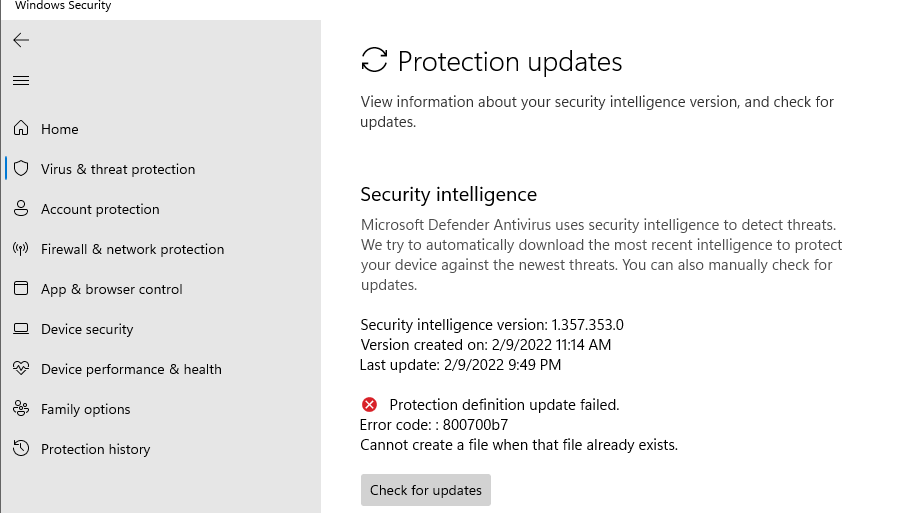
1. Show that Windows Defender is active and can detect malware
   1. Run ProcMon and add filter
      1. Add filter: CTRL + L
      2. Add Path: "C:\adfsl2022\mimikatz\mimikatz\_trunk\x64\mimikatz.exe"
   2. Run CMD with admin privilege;
   3. Run “cd C:\adfsl2022”
   4. Run batch “clear\_extract\_and\_check.bat”   
      Show that CMD cannot found file
   5. Windows Defender reacts and detects malware
   6. Move to the ProcMon to show how the files is deleted:
      1. Search “setdispo” to locate “SetDispositionInformationFile”
      2. After that the “CreateFile” returns “DELETE PENDING”
      3. And finally, the file mimikatz.exe is removed and cannot be found.
      4. Clear ProcMon output.
2. Patch Integrity Level & Revoke Token for Windows Defender
   1. Run dbgview64
   2. Run mem\_attacker\_console
      1. Run the “patch\_integrity MsMpEng.exe” – command
      2. Run the “revoke\_privileges MsMpEng.exe” – command
   3. Run batch “clear\_extract\_and\_check.bat” again

|  |
| --- |
| **privilege::debug**  **lsadump::lsa /inject** |

* 1. Show that now mimikatz.exe has been successfully launched;
  2. Run the following command to show that mimikatz can dump hashes:
  3. Move to the ProcMon to show that the app is not blocked now:
     1. Search “**load**” to locate “Load Image”
     2. Show that now mimikatz is running successfully.
  4. Open Windows Security:

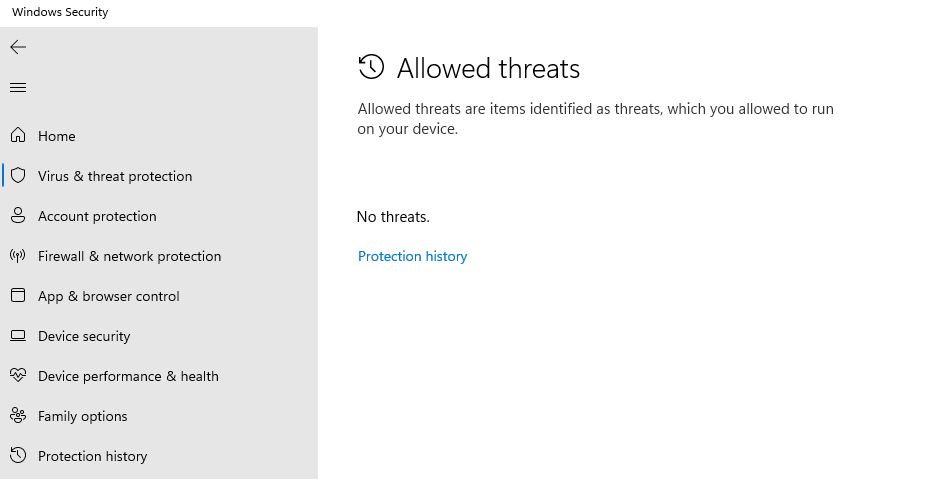
Open Windows Security

Virus & threat protection → Virus & threat protection updates → Protection updates:



They are blocked ☺

Virus & threat protection → Allowed Threads



There are no allowed threads ☺

Let’s wait for 10 hours.