**Demo 1: Attack on Windows Defender via Disabling MIC**

Show that Microsoft Defender is active and can detect malware:

1. Run ProcessHacher to show Windows Defender integrity level and privileges.
2. Activate filtering: Run ProcMon and add filter
   1. Press: CTRL + L
   2. Add Path: "C:\adfsl2022\mimikatz\mimikatz\_trunk\x64\mimikatz.exe"
3. Run CMD with admin privilege;
4. Run “cd C:\adfsl2022”
5. Run batch “clear\_extract\_and\_check.bat”
6. Windows Defender reacts and detects malware
7. Show that CMD cannot found file:  
   Wait 20 secs

|  |
| --- |
| **C:\adfsl2022\mimikatz\mimikatz\_trunk\x64\mimikatz.exe** |
| '"C:\adfsl2022\mimikatz\mimikatz\_trunk\x64\mimikatz.exe"' is not recognized as an internal or external command, operable program or batch file. |

|  |
| --- |
| **>dir "C:\adfsl2022\mimikatz\mimikatz\_trunk\x64"** |
| there is no mimikatz.exe |

1. 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.

*Proofed that Windows Defender is running and can detect malware.*

**Attack on Windows Defender via Disabling MIC**

1. Patch Integrity Level for Windows Defender
   1. Run dbgview64   
      activate Capture Kernel (Ctrl+K)
   2. Run mem\_attacker\_console
      1. Run the “patch\_integrity MsMpEng.exe” – command
   3. Run batch “clear\_extract\_and\_check.bat” again
   4. Show that now CMD returns  
      “The system cannot execute the specified program.”
   5. Relaunch ProcessHacher to show updated integrity level for Windows Defender.
   6. Move to the ProcMon to show how the app is blocked
      1. Search “**906**” to locate “0xC0000906”
      2. Show that cmd fails to create files with error 0xC0000906.
      3. This time the file is not deleted, but the app cannot be launched.
      4. Each time cmd tries to run mimikatz.exe – the OS returns 0xC0000906.