DEATHCON 2025 Prerequisites - Deconstructing the EDR Evasion Mille-Feuille - Cyb3rhawk

Prerequisites -

- □ Python (Required)
- □ Download Log files (Required)
- □ Download Hunter Python File (Required)
- □ Sysiternals (Optional)
- □ Rust (only if you would like to simulate BYOVD)
- □ Windows 10 SDK (only if you would like to simulate BYOVD)
- □ Sysmon Config (only if you would like to simulate BYOVD)
- □ ETWExplorer (optional) (only if you would like to understand Providers)
- □ Seatlighter executable and .man (only if you would like to generate logs by simulating BYOVD)
- □ Seatligher config (only if you would like to generate logs by simulating BYOVD)
- □ IDA (Optional) (only if you would like to see how a BYOVD look like)
- □ BlackSnufkin BYOVD folder (only if you would like to simulate BYOVD)
- □ Sublime (Optional)

Prerequisites Prep

1. Download Log files - https://drive.google.com/drive/folders/1yILFfCqPleEjhvBM3leg1zfilb9EBwF5?usp=sharing (Required)

2. Download Hunter Python Folder AND Workbook - https://github.com/cyb3rHawk/DEATHCON-2025-Cyb3rhawk-Deconstructing-the-EDR-Evasion-Mille-Feuille- (Required)
3. All the below Items are options if you would like to perform simulatio
4. Download sysinternals and extract them to c:/Program Files/Sysinternals
    a. Open procexp64.exe → accept EULA → check msmpeng.exe for testing
5. Download Rust https://rust-lang.org/tools/install/ and click to install Visual Studio and MSVC v143. This takes good amount of time so please be patient
    a. We also need C++build tools too. Once you install rust, open visual studio → tools → get tools and features → Click Desktop Development C++ and click windows 10 sdk option from the right too → Modify

    b. Check by typing cargo and hit enter
6. Download research-sysmoncofig from Olafhartong https://github.com/olafhartong/sysmon-modular
    a. Install by typing sysmon -i <path_to_sysmon_config>
7. Download SilkETW - https://github.com/mandiant/SilkETW/releases/tag/v0.8
8. Download Seatligher Binary and man file from https://github.com/pathtofile/Sealighter
    a. Instruction on how to install can be found here https://github.com/pathtofile/Sealighter/blob/main/docs/INSTALLATION.md but in a nutshell

    b. Create a folder under `C:\ProgramData` with name “`Seatligher`” - this will be the folder where the JSON events are written to

    c. If you want to write into Windows Event Viewer, Open Command Prompt as Administrator and type

    d. Change config file by replacing

    `"output_format": "file"`

    `"output_filename":"C:\ProgramData\Seatligher\byovd.json"`

    to

    `"output_format": "event"`

e. then proceed to type

```
wevtutil im path/to/sealighter_provider.man
```

```
(Get-WinEvent -LogName "Sealighter/Operational").Length
```

f. Verify if the config is valid and file or events are created by typing

```
sealighter.exe path\to\config.json
```

  a. Hit Control + C to stop the trace

  b. If you get error, please type (admin)

    a. `icacls <path_to_sealighter.exe> /grant "NT SERVICE\EventLog:F”`

9. Download Windbg - https://aka.ms/windbg/download

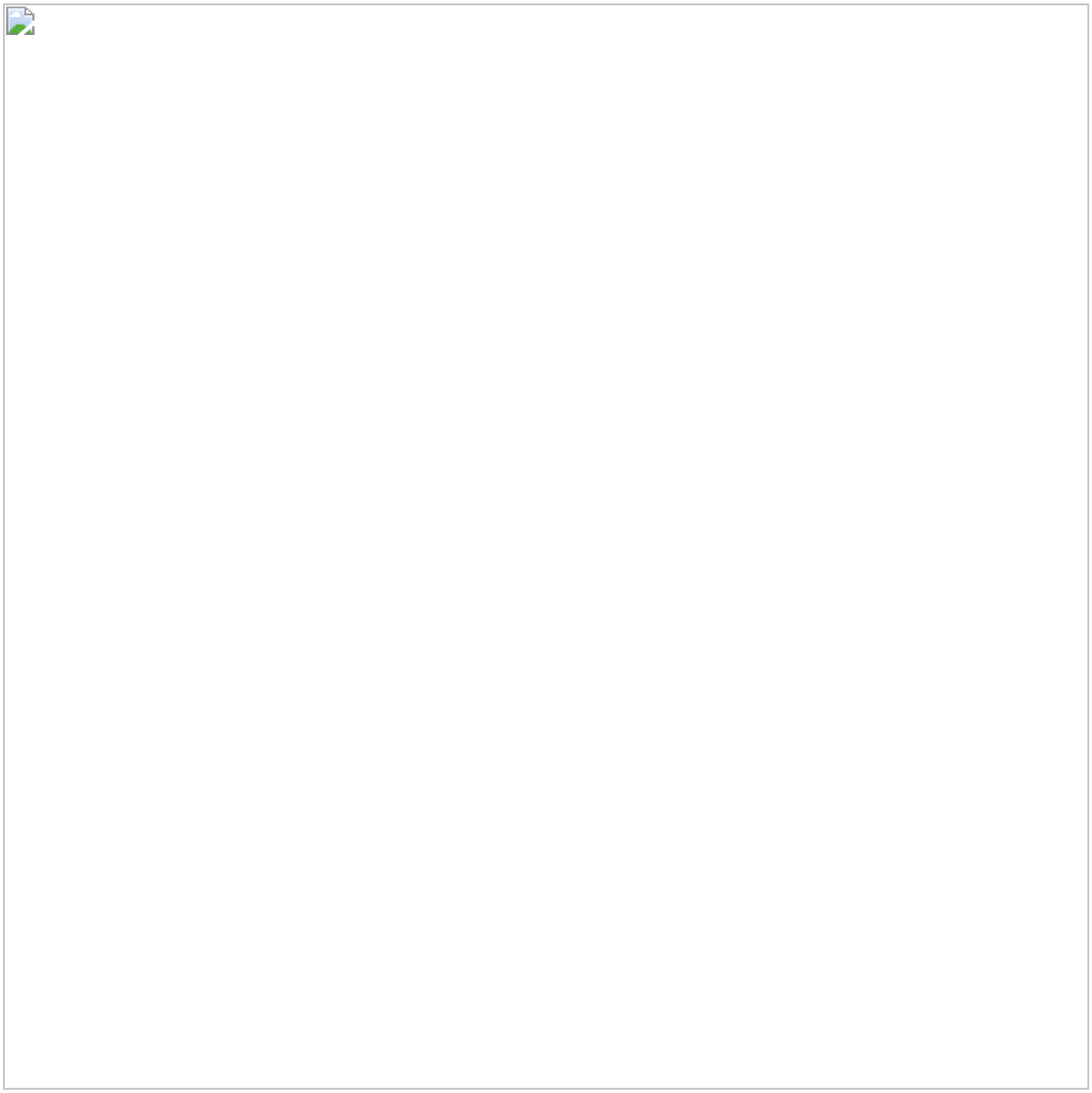
10. Download IDA - You need to have an email to get license and download

11. Download zip file for https://github.com/BlackSnufkin/BYOVD

12. Compile binaries

  a. Open Command Prompt as Administrator

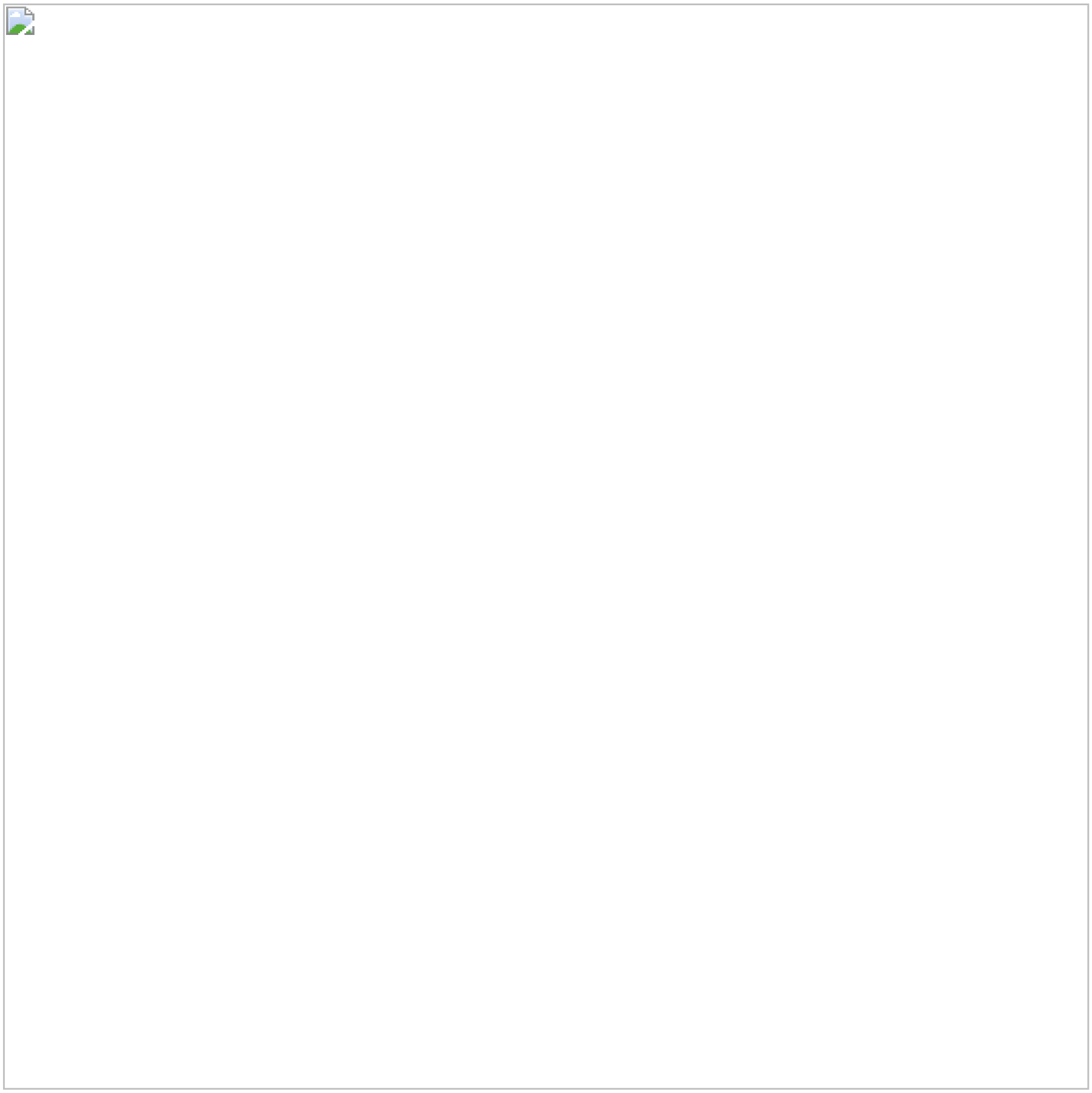
  b. Cd into the BYOD folder (from above download) → NSec-Killer



c. cargo build

If everything goes well, you should have NSec-Killer.exe

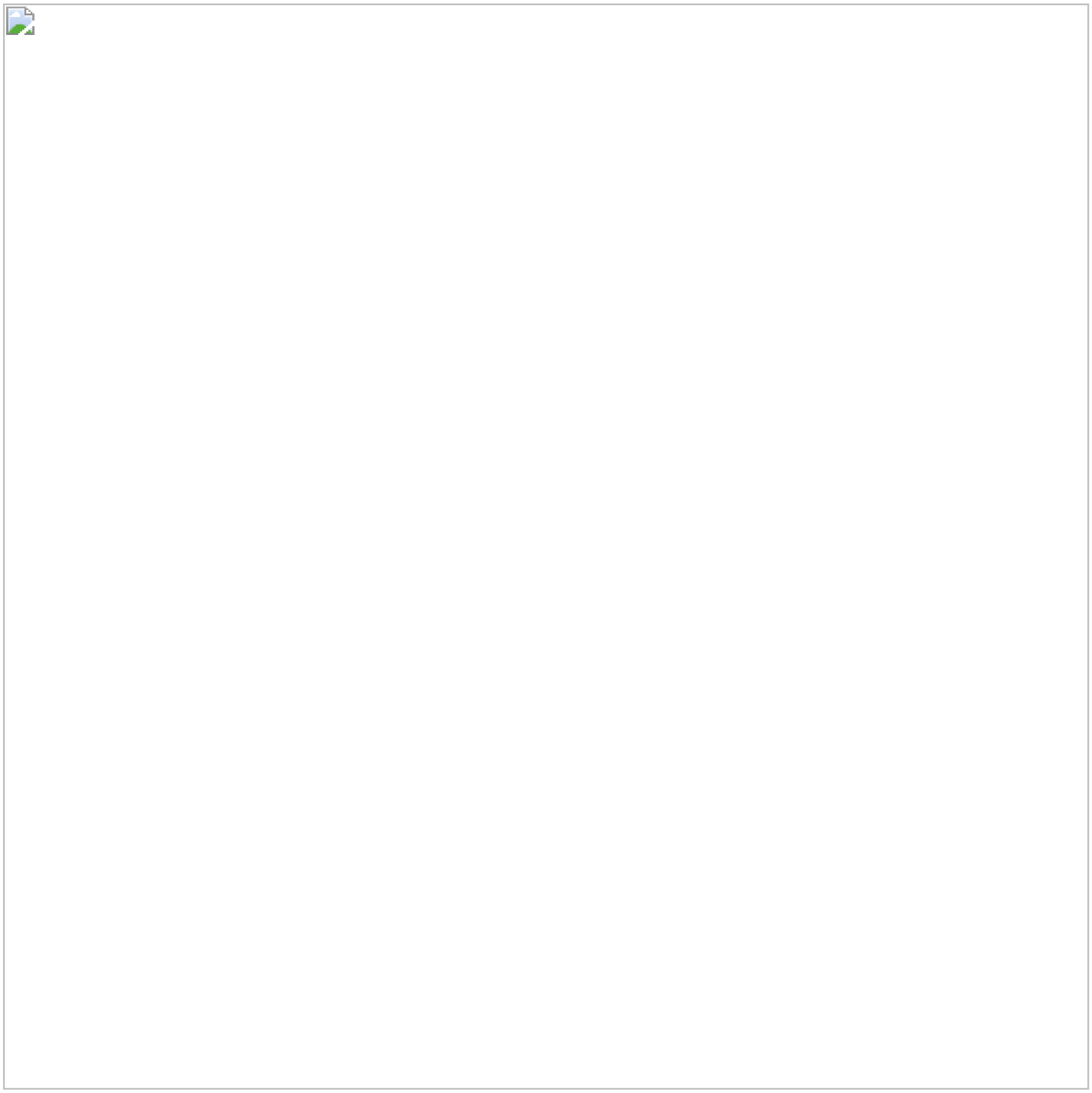
Try NSec-Killer.exe —help



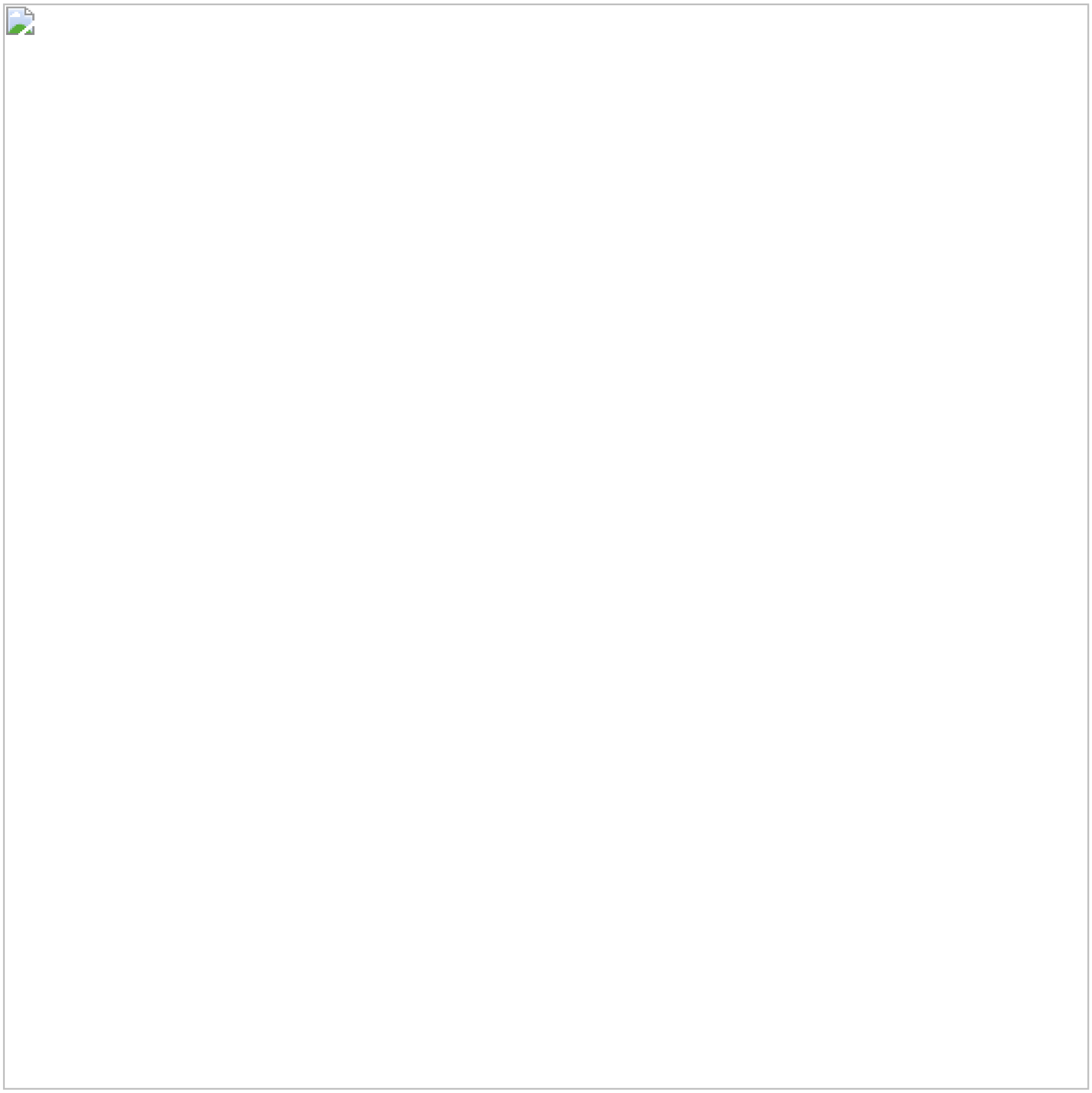
LAYER 1:

This step is not necessary as you already have the JSON file generated using following these steps. However, if you want to replay this in the future or use it for future purposes, please proceed.

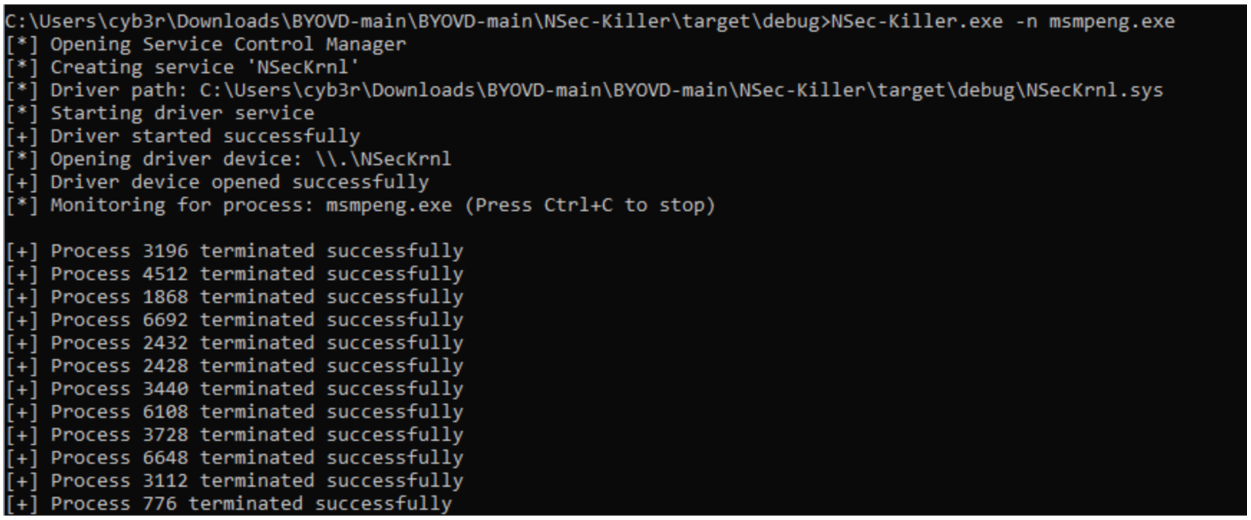
1. Open Command Prompt as Administrator and type (change the file name to the name you downloaded it as)



Wait until you are ready to execute the next step. Once you have both consoles open with necessary commands, hit enter on `sealighter.exe <path_to_config> console`



2. Open another Command Prompt as Administrator and navigate to Nsec-Keller build folder and type
    a. `Nsec-Killer.exe -n msmpeng.exe  -` !! DO NOT HIT ENTER YET! !
    b. After you start the trace (mentioned in the previous step), wait for 30 seconds, hit end enter



```
C:\Users\cyb3r\Downloads\BYOVD-main\BYOVD-main\NSec-Killer\target\debug>NSec-Killer.exe -n msmpeng.exe
[*] Opening Service Control Manager
[*] Creating service 'NSecKrnl'
[*] Driver path: C:\Users\cyb3r\Downloads\BYOVD-main\BYOVD-main\NSec-Killer\target\debug\NSecKrnl.sys
[*] Starting driver service
[+] Driver started successfully
[*] Opening driver device: \\.\NSecKrnl
[+] Driver device opened successfully
[*] Monitoring for process: msmpeng.exe (Press Ctrl+C to stop)

[+] Process 3196 terminated successfully
[+] Process 4512 terminated successfully
[+] Process 1868 terminated successfully
[+] Process 6692 terminated successfully
[+] Process 2432 terminated successfully
[+] Process 2428 terminated successfully
[+] Process 3440 terminated successfully
[+] Process 6108 terminated successfully
[+] Process 3728 terminated successfully
[+] Process 6648 terminated successfully
[+] Process 3112 terminated successfully
[+] Process 776 terminated successfully
```

3. You can wait to see how each msmpeng.exe process is terminated (ideally for couple of time) and Hit Control + C

13. Go back to the console where `sealighter.exe` is running the trace and hit Control + C
    a. This will stop the trace and you should have either Json file at `C:\ProgramData\Seatligher\byovd.json` or logs should be event viewer (depending on what option you choose before)