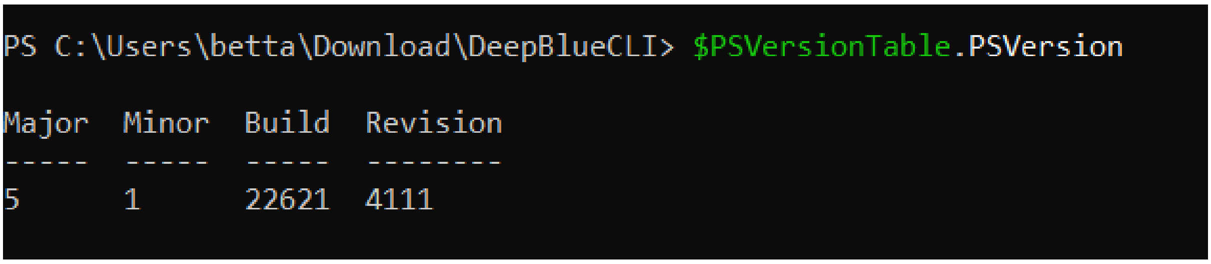
DeepBlueCLI

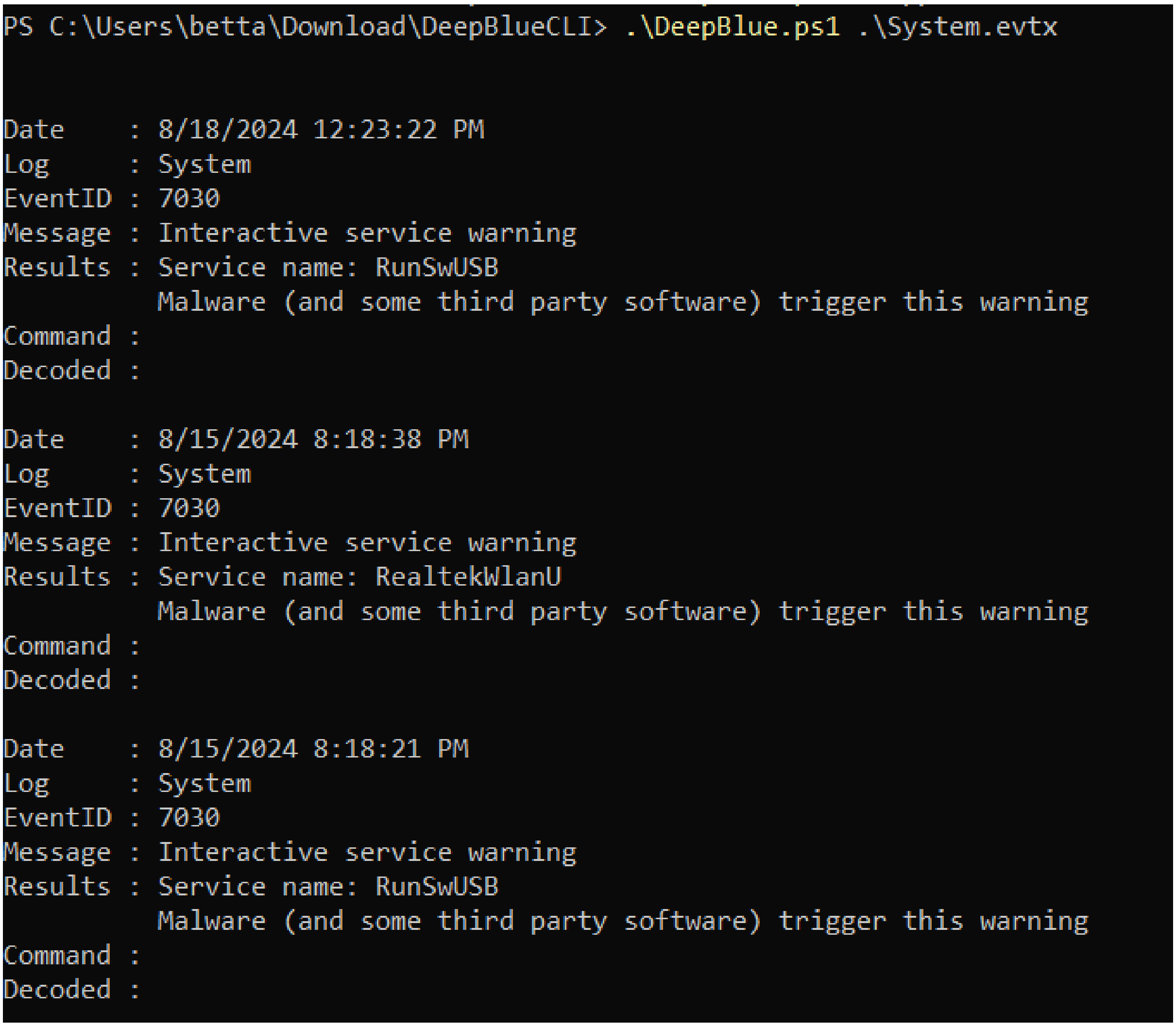
- Install DeepBlueCLI on a Windows virtual machine (VM). Ensure you have PowerShell 5.1 or later installed.



```
PS C:\Users\betta\Download\DeepBlueCLI> $PSVersionTable.PSVersion

Major  Minor  Build  Revision
-----  -----  -----  --------
5      1      22621  4111
```

- Obtain sample Windows Event Logs for analysis. You can use sample logs provided in the DeepBlueCLI repository or generate your own by simulating some activities on your Windows VM.

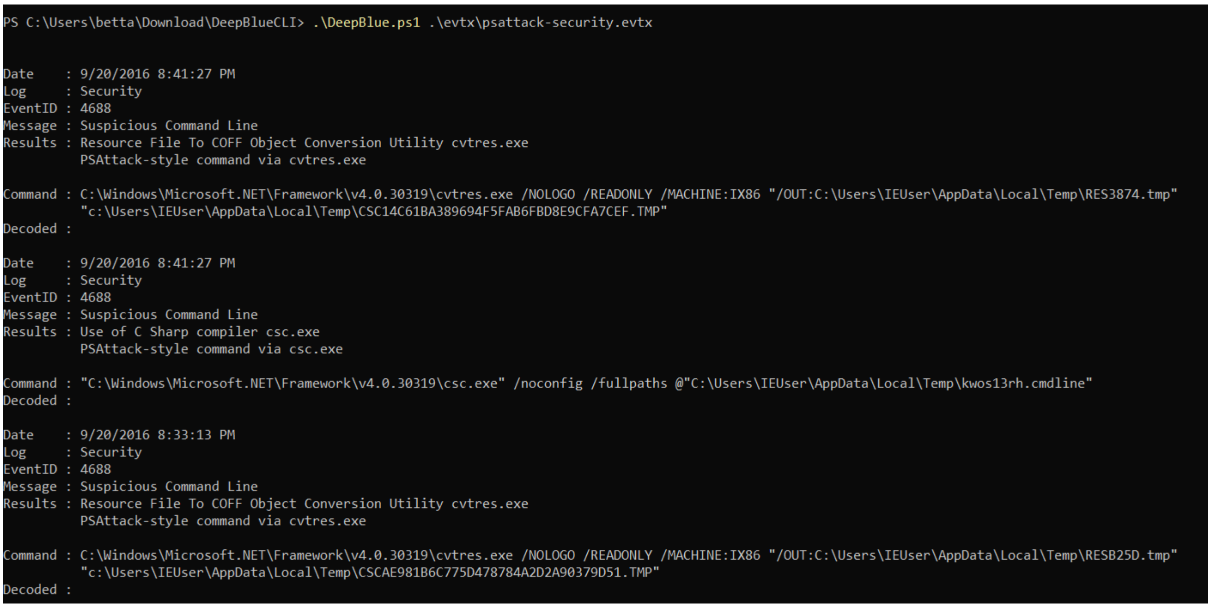


```
PS C:\Users\betta\Download\DeepBlueCLI> .\DeepBlue.ps1 .\System.evtx


Date    : 8/18/2024 12:23:22 PM
Log     : System
EventID : 7030
Message : Interactive service warning
Results : Service name: RunSwUSB
          Malware (and some third party software) trigger this warning
Command :
Decoded :

Date    : 8/15/2024 8:18:38 PM
Log     : System
EventID : 7030
Message : Interactive service warning
Results : Service name: RealtekWlanU
          Malware (and some third party software) trigger this warning
Command :
Decoded :

Date    : 8/15/2024 8:18:21 PM
Log     : System
EventID : 7030
Message : Interactive service warning
Results : Service name: RunSwUSB
          Malware (and some third party software) trigger this warning
Command :
Decoded :
```



```
PS C:\Users\betta\Download\DeepBlueCLI> .\DeepBlue.ps1 .\evtx\psattack-security.evtx


Date    : 9/20/2016 8:41:27 PM
Log     : Security
EventID : 4688
Message : Suspicious Command Line
Results : Resource File To COFF Object Conversion Utility cvtres.exe
          PSAttack-style command via cvtres.exe

Command : C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\IEUser\AppData\Local\Temp\RES3874.tmp"
          "c:\Users\IEUser\AppData\Local\Temp\CSC14C61BA389694F5FAB6FBD8E9CFA7CEF.TMP"
Decoded :

Date    : 9/20/2016 8:41:27 PM
Log     : Security
EventID : 4688
Message : Suspicious Command Line
Results : Use of C Sharp compiler csc.exe
          PSAttack-style command via csc.exe

Command : "C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\IEUser\AppData\Local\Temp\kwos13rh.cmdline"
Decoded :

Date    : 9/20/2016 8:33:13 PM
Log     : Security
EventID : 4688
Message : Suspicious Command Line
Results : Resource File To COFF Object Conversion Utility cvtres.exe
          PSAttack-style command via cvtres.exe

Command : C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\IEUser\AppData\Local\Temp\RESB25D.tmp"
          "c:\Users\IEUser\AppData\Local\Temp\CSCAE981B6C775D478784A2D2A90379D51.TMP"
Decoded :
```

- Familiarize yourself with basic DeepBlueCLI commands.

  Done

- Explore the different types of logs DeepBlueCLI can analyze.

  Done

- Identify key features of the output provided by DeepBlueCLI, such as detecting suspicious activities, failed logins, and abnormal process creations.

  Done

- Analyze the provided sample event logs using DeepBlueCLI. Focus on the following types of logs: Security Logs,System Logs, Application Logs.

  Done

Reporting

1. Based on your analysis, prepare a brief report summarizing your findings. The report should include:

- Details the log analysis performed.
- A summary of the key findings from each type of log.
- Examples of suspicious activities detected.

2. Points to Consider:

- How can DeepBlueCLI be used in a real-world forensic investigation?
  DeepBlueCLI helps in post-incident analysis by detecting anomalies in system and security logs. Investigators can detect threats like malware execution, privilege escalation, or brute-force attacks based on log analysis.

- What are the limitations of using DeepBlueCLI?

  DeepBlueCLI focuses on known indicators, so it may miss highly obfuscated or novel attacks that don't match typical event patterns.

  Requires correlation with other tools or logs (e.g., network logs) to get a fuller picture of incidents.

- What types of suspicious activities can you identify?

  Failed login attempts, which may indicate a brute-force attack.

  Unusual process creation, which might signal malware or malicious scripts being executed.

  Privilege escalation attempts, where an account attempts to gain higher access than it normally has.

  Malware signatures or processes linked to known attacks.

- Are there any failed login attempts or unusual process creations?

  Using DeepBlueCLI, investigators can spot **failed login attempts**, which might suggest brute-force or unauthorized access attempts. Similarly, **unusual process creations**—such as processes that shouldn't typically run on a system—can be identified, often indicating potential malware execution or system compromise.

- Can you identify any patterns that might indicate a security incident?

  Yes, patterns like repeated **failed login attempts**, **execution of uncommon processes**, and **escalation of privileges** could be signs of a security incident. DeepBlueCLI can help reveal such patterns by analyzing different event logs and consolidating the findings into meaningful indicators of a breach or suspicious activity.