Blue Team Labs Online: Deep Blue

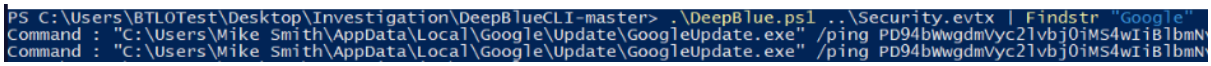
The following writeup is for Deep Blue on Blue Team Labs Online, it's an easy lab that involves analysing Windows Event Logs using DeepBlueCLI and Event Viewer. This investigation is a great way to begin practicing Event Log analysis.

Scenario: A Windows workstation was recently compromised, and evidence suggests it was an attack against internet-facing RDP, then Meterpreter was deployed to conduct 'Actions on Objectives'. Can you verify these findings?

You have been provided with the Security.evtx and System.evtx log exports from the compromised system - you should analyze these, NOT the Windows logs generated by the lab machine (when using DeepBlueCLI ensure you're providing the path to these files, stored inside \Desktop\Investigation\.

Using DeepBlueCLI, investigate the recovered Security log (Security.evtx). Which user account ran GoogleUpdate.exe?

To answer this question, we can simply execute DeepBlueCLI and filter for the string "Google":



As you can see in the output, the user account is Mike Smith (you can see the username in the file path).

Answer: Mike Smith

Using DeepBlueCLI investigate the recovered Security.evtx log. At what time is there likely evidence of Meterpreter activity?

If we run the same command as done previously and save the output to a file, it makes it much easier to analyse the generated alerts. At 4/10/2021 10:48:14 AM, we can see a possible use of Meterpreter:

```
Date    : 4/10/2021 10:48:14 AM
Log     : Security
EventID : 4688
Message : Suspicious Command Line
Results : Metasploit-style cmd with pipe (possible use of Meterpreter 'getsystem')

Command : cmd.exe /c echo rztbzn > \\.\pipe\rztbzn
Decoded :
```

Answer: 4/10/2021 10:48:14

Using DeepBlueCLI investigate the recovered System.evtx log. What is the name of the suspicious service created?

Fortunately for us, there are only two alerts generated from the System.evtx file:

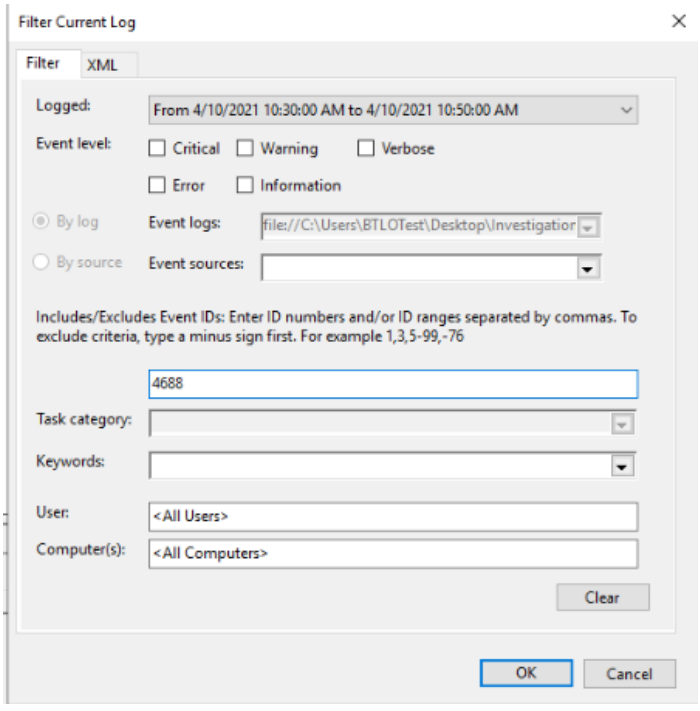
```
Date    : 4/10/2021 10:48:14 AM
Log     : System
EventID : 7045
Message : Suspicious Service Command
Results : Service name: rztbzn
          Metasploit-style cmd with pipe (possible use of Meterpreter 'getsystem')

Command : cmd.exe /c echo rztbzn > \\.\pipe\rztbzn
Decoded :

Date    : 4/9/2021 8:45:03 PM
Log     : System
EventID : 104
Message : System Log Clear
Results : The System log was cleared.
Command :
Decoded :
```

In the Results field for the first alert, we can see that a service named rztbzn was created.

Answer: rztbzn

Investigate the Security.evtx log in Event Viewer. Process creation is being audited (event ID 4688). Identify the malicious executable downloaded that was used to gain a Meterpreter reverse shell, between 10:30 and 10:50 AM on the 10th of April 2021.

Before we try to identify the malicious executable, let's apply some filters based on the context given in this question:



After applying this filter, we can see 39 events, making it far easier to analyse. After looking through some of the events, we can see that Mike Smith executed serviceupdate.exe:

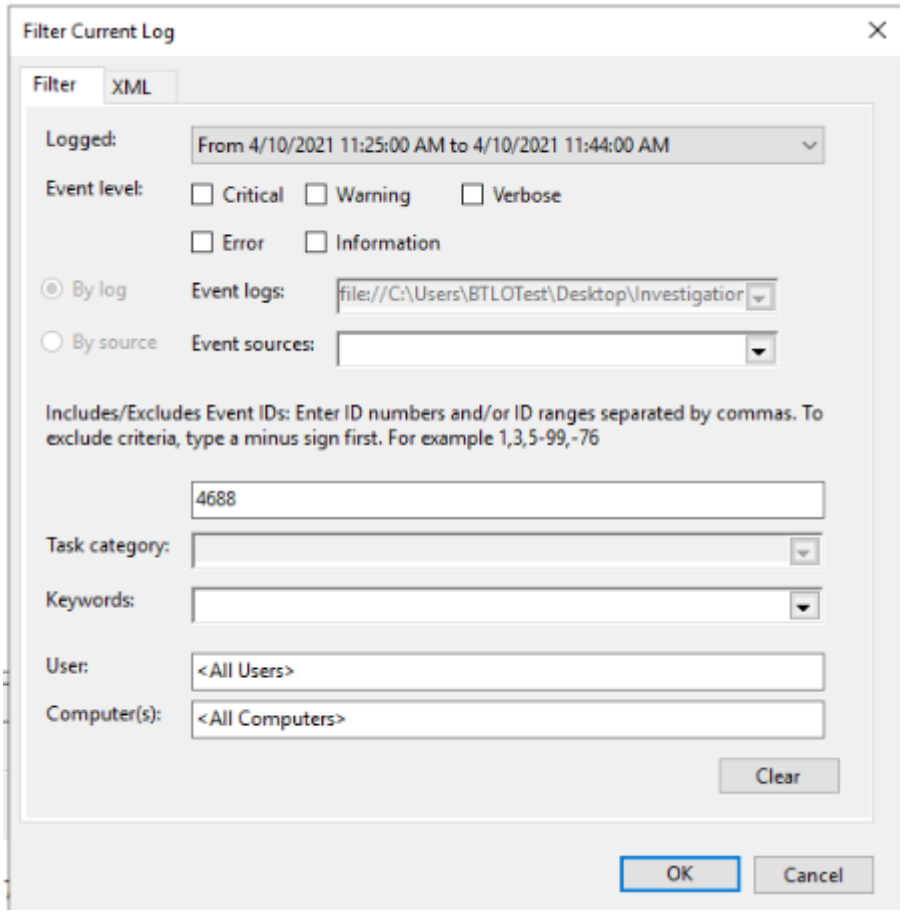
NewProcessName C:\Users\Mike Smith\Downloads\serviceupdate.exe
TokenElevationType %%1937
ProcessId 0x51c
CommandLine "C:\Users\Mike Smith\Downloads\serviceupdate.exe"

This would obviously warrant further investigation, however, after looking at the other executables, this seems the most suspicious.

Answer: Mike Smith, seerviceupdate.exe

It's also believed that an additional account was created to ensure persistence between 11:25 AM and 11:40 AM on the 10th April 2021. What was the command line used to create this account? (Make sure you've found the right account!)

Once again, let's create a filter based on the given context:



NewProcessName C:\Windows\System32\net.exe
TokenElevationType %%1937
ProcessId 0x96c
CommandLine net user ServiceAct /add

Answer: net user ServiceAct /add

What two local groups was this new account added to?

CommandLine	net localgroup administrators ServiceAct /add
CommandLine	net localgroup "Remote Desktop Users" ServiceAct /add

Answer: administrators, Remote Desktop Users