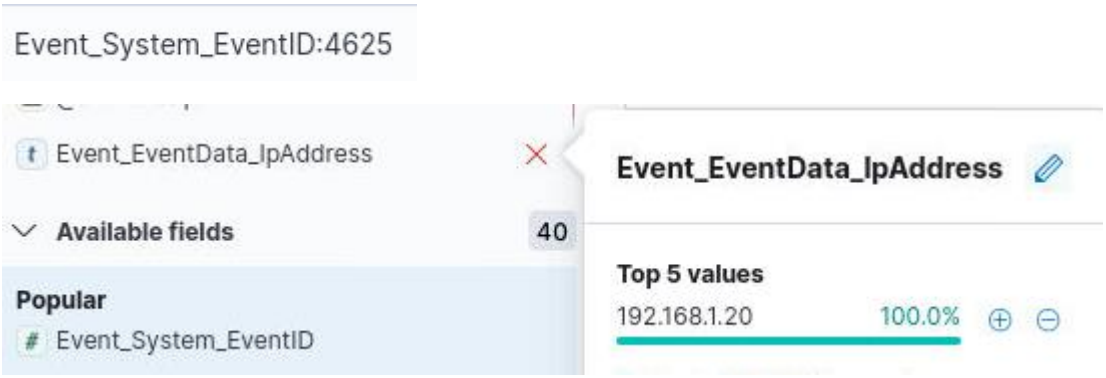
Blue Team Labs Online: SOC Alpha 2

The following writeup is for SOC Alpha 2 on Blue Team Labs Online, it's an easy lab that involves analysing Windows Event Logs using ELK. This is an easy lab more aimed towards those just starting out with Elastic search and is part of a series. In comparison to SOC Alpha 1, this investigation is slightly more difficult, although in my opinion, is way more enjoyable. You get exposed to investigating broader questions, unlike the previous investigation that gave time frames, and alert context.

Scenario: You are provided with use-cases to conduct some proactive searches in ELK. Answer the following questions by using the information provided in README.txt.

Hunt 1 (1/3) - What is the IP address from which the suspicious brute force traffic is seen? (Format: X.X.X.X)

Based on the question, we will need to look for an IP address with repeated failed login attempts. For context, each failed authentication attempt generates an event log with a event ID 4625. In order to look for any brute force attempt, we can filter for this event ID and focus on the Event_EvebtData_UpAddress field:

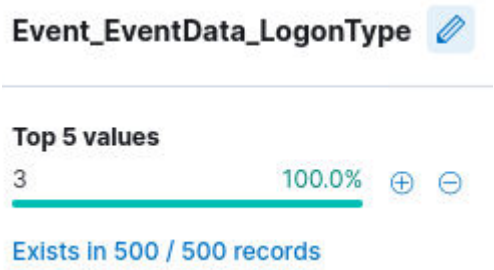


Luckily for us, there is only one IP address, which has 1804 failed authentication attempts for user nightmare.

Answer: 192.168.1.20

Hunt 1 (2/3) - What is the observed logon type? (Format: Logon Type Name)

When a user attempts to authenticate to a Windows host, the generated log includes a field for logon type. Logon type indicates the way the user attempts to authenticate to the host (interactive, over RDP, etc). If you take a look at the Event_EventData_LogonType field, the only value is 3:



3 is for Network logon, which occurs when a user logs on to a computer over the network.

Answer: Network

Hunt 1 (3/3) - What is the time of the first successful logon after the brute force? (Format: Format:DD-MM-YYYY hh:mm:ss)

A successful authentication generates an event log with event ID 4624. Therefore, we can filter for this ID and the username “nightmare”:

As you can see, on the 14th of April, 2021, the attacker successfully authenticated as the username “nightmare”.

Answer: 14/04/2021 10:56:30

Hunt 2 (1/2) - What is the full command used for bypassing the defender scan on the malicious file? (Format: powershell.exe ... Full Command (Do not include the file path))

Based on the question, we are likely looking for a command that adds an exclusion for the malicious file, that way, defender will not scan it. After a quick google, it seems like the Add-MpPreference cmdlet is used to add an exclusion for Windows Defender. We can easily filter for this like as follows:

As you can see, the threat actor is creating an exclusion, in this case its for chroma.exe located in the Downloads folders.

Answer: powershell.exe -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath

Hunt 2 (2/2) - What is the filename of the malicious application? (Format: filename.extension)

We determined the malicious binary in the previous question:

```
-ExclusionPath C:\Users\nightmare\Downloads\chroma.exe
```

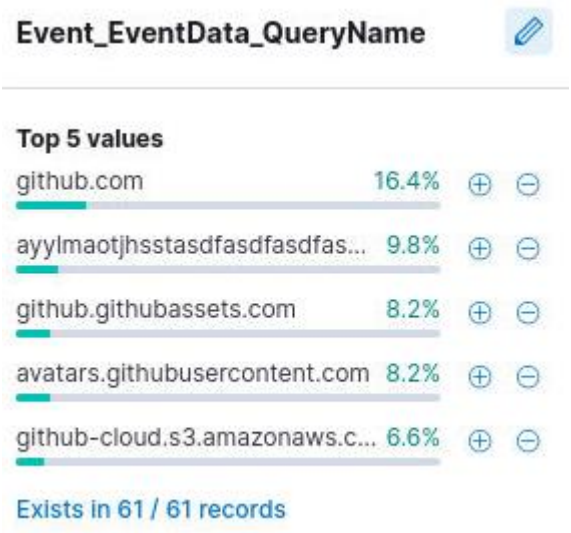
Answer: chroma.exe

Hunt 3 (1/2) - What is the domain name? (Format: domain.tld)

In order to determine the domain name, I am going to look for DNS events (Event ID 22). This event is generated when a process executes a DNS query, aka attempts to resolve a domain name.

```
Event_System_EventID:22
```

If you take a look at the QueryName, we can see a really odd looking domain:




```
ayylmaotjhsstasdfasdfasdfasdfasdfasdfasdf.com
ayylmaotjhsstasdfasdfasdfasdfasdfasdfasdf.com
ayylmaotjhsstasdfasdfasdfasdfasdfasdfasdf.com
```

Based on the randomness, you can determine it to be extremely suspicious. It also has 6 detections on VirusTotal.

Answer: ayylmaotjhsstasdfasdfasdfasdfasdfasdfasdf.com

Hunt 3 (2/2) - What is the Execution ProcessID and ThreadID? (Format: pid, tid)

Let's drill down on the identified URL and determine its associated ProcessID and ThreadID:

```
Event_System_EventID : 22 AND Event_EventData_QueryName: "ayylmaotjhsstasdfasdfasdfasdfasdfasdf.com"
```

Event_System_Execution_#attributes_ThreadID	Event_System_Execution_#attributes_ProcessID	Event_EventData_QueryName
4,260	2,724	ayylmaotjhsstasdfasdfasdfasdfasdfasdf.com
4,260	2,724	ayylmaotjhsstasdfasdfasdfasdfasdfasdf.com

Answer: 2724,4260

Hunt 4 (1/1) - What is the full path of the exe used for dumping password? (Format: C:\path\to\file.extension)

To find the exe used for dumping, I am going to search for process creation events (Event ID 1) with the parent command line including explorer.exe. The reason being that I am looking for user executed binaries. We could just search for tools like mimikatz, which 99% of the time will be the password dumping tool in challenges like this, but that is not the correct approach.

```
Event_System_EventID : 1 AND Event_EventData_ParentCommandLine : "*explorer.exe*"
```

Time ↓	Event_EventData_CommandLine
Apr 20, 2021 @ 14:36:03.367430000	"C:\Users\nightmare\Desktop\mimi\x64\mimikatz.exe"
Apr 15, 2021 @ 08:44:47.969234000	"C:\Users\nightmare\Desktop\chroma.exe"
Apr 15, 2021 @ 08:43:57.755922000	"C:\Users\nightmare\Desktop\chroma.exe"

As you can see, the threat actor executed mimikatz, which is a notorious credential dumping tool.

Answer: C:\Users\nightmare\Desktop\mimi\x64\mimikatz.exe