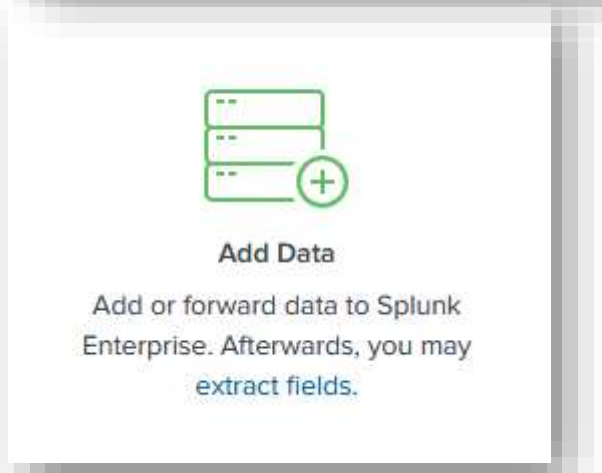
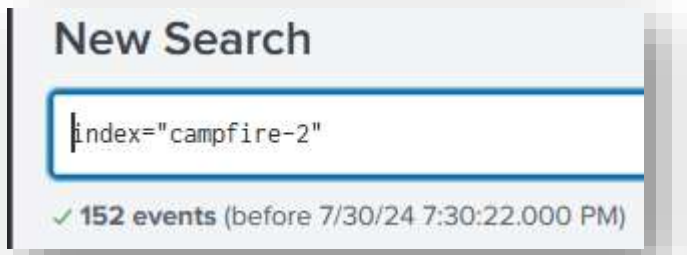
HTB sherlocks – Campfire-2

Write up by Chanan Shenker

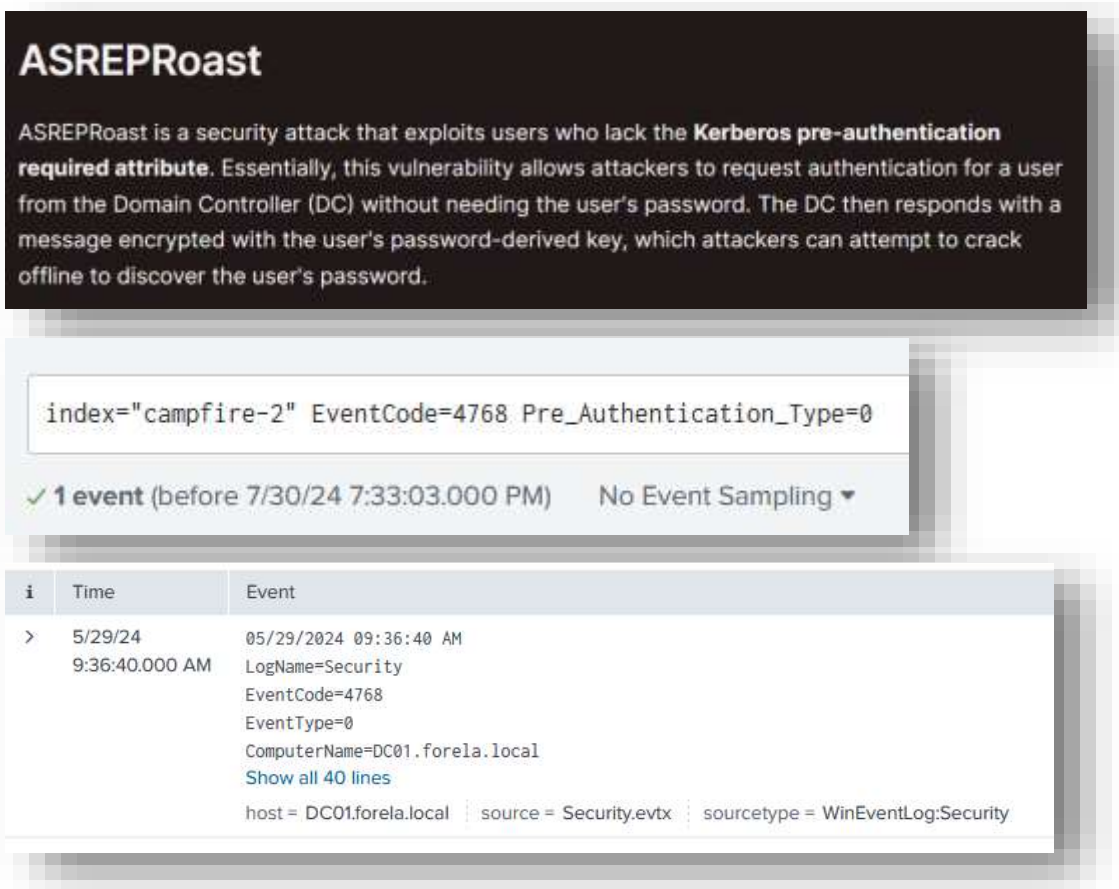
- Start:

- To start we get a event log file. So I fired up splunk and loaded the logs into splunk.
- Splunk is a SIEM (Security information and event management) software which lets you organize and gather all different types of logs and filter, moderate, organize and more. Its used by SOC analysts so they can sift through the grand amount of logs each computer produces and detect threats correctly and thoroughly.
- so with Splunk I added the log file, created a new index so I can easily search through the logs and started to search .
- As you can see total amount of logs is 152



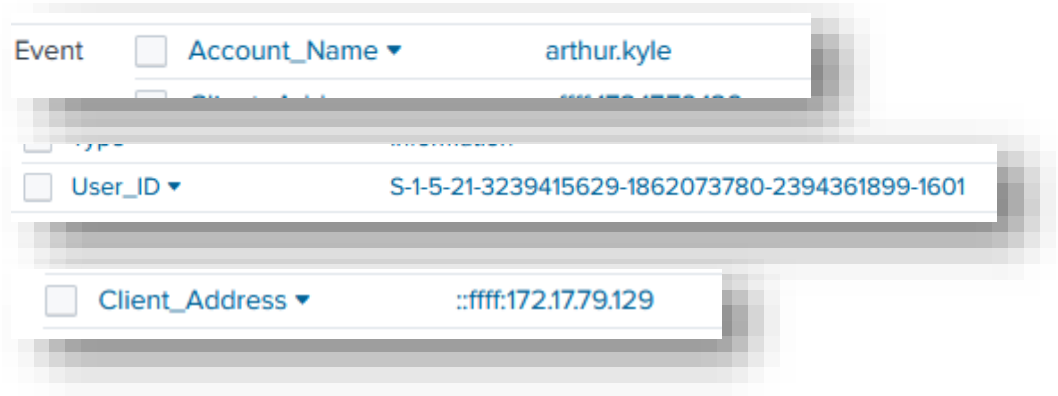


- Task 1: When did the ASREP Roasting attack occur, and when did the attacker request the Kerberos ticket for the vulnerable user?
- When searching up what asrep roasting attack is I found a page by hack tricks explaining that it is when a user lack the Kerberos pre authentication requirements and an attacker can request a ticket which is encrypted with the users password and attempt to crack it offline.
- So I searched for event id 4768 which is triggered when a Kerberos ticket is requested, and I searched for a pre authentication type of '0' which indicates no pre authentication required



- All I found was this one event so I converted the time to UTC time and gota right answer.
- Answer 1: 2024-05-29 06:36:40

- Tasks 2, 3 &4:
- I bunched these question together because they all involve the same event.
- When looking through the event we can find information like, the user being targeted the SID of the user and the IP address of the workstation that was used.



- Answer 2: arthur.kyle
- Answer 3: S-1-5-21-3239415629-1862073780-2394361899-1601
- Answer 4: 172.17.79.129

- Task 5:We do not have any artifacts from the source machine yet. Using the same DC Security logs, can you confirm the user account used to perform the ASREP Roasting attack so we can contain the compromised account/s?
- So for this it took me a bit of time but then I remembered that in the last task we looked for the IP address of the machine that the ticket was requested from, so lets add that to out search

- When searching for the address I only found 2 events, one was the original event we analyzed and the second was event id 4769 that is triggered by a Kerberos ticket being requested. So when looking in we see that the user that requested it was happy.Grunwald
- Answer 5: happy.grunwald