**How Did I Get Here**

***Log Analysis***

**Challenge:**

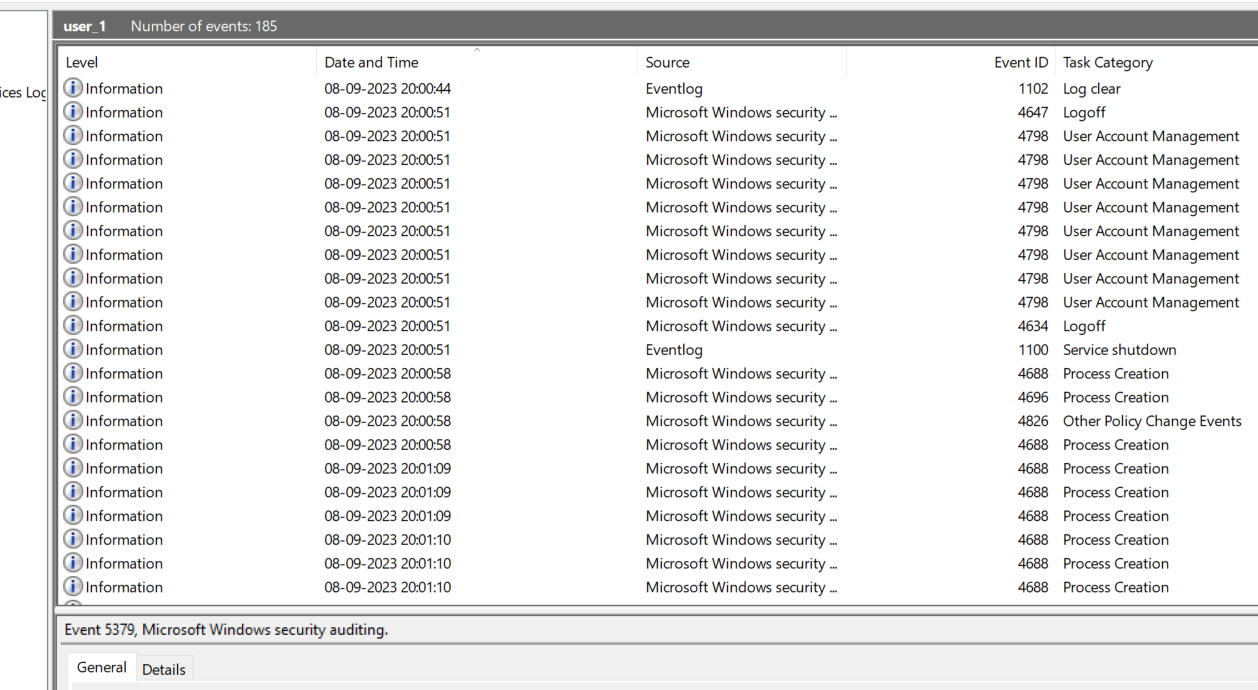
A new user has been created. Can you find the username?

Attached - user.evtx

**Approach:**

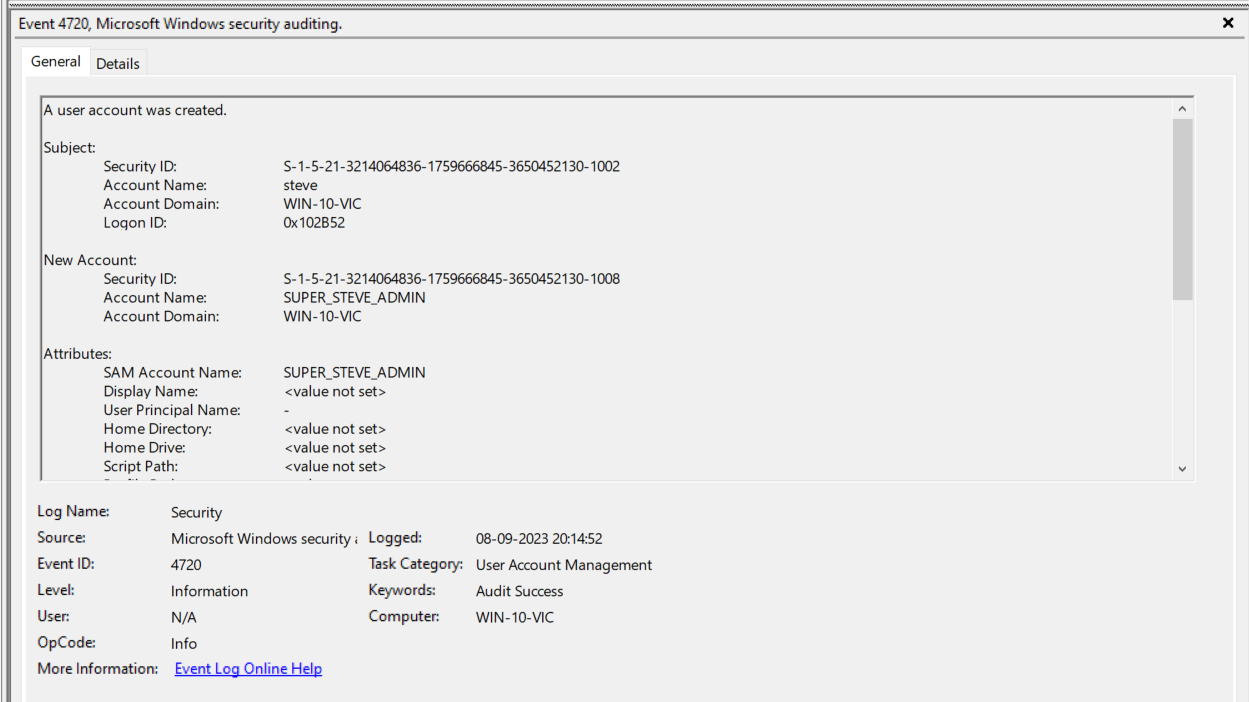
.evtx are basically log files generated by various services. I did not have much knowledge about it, but what’s wrong with viewing it once?

I opened it up using the Event Viewer on windows, and it gave me around 185 events.



Had to make a guess and I believe an action like creating a new account would lie under the task category of “User Account Management”.

Sorted by the “Task Category” and iterated through all the events to finally find this:



Hence the flag:

**Flag: SUPER\_STEVE\_ADMIN**

Congrats!!

Happy Hacking!