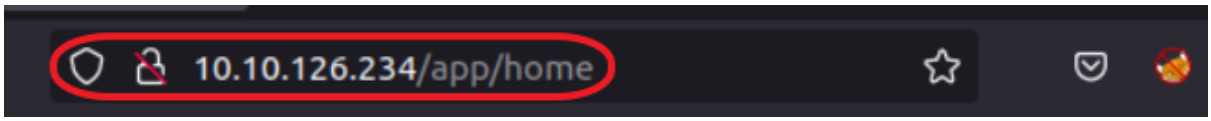
Name:Ramya Ajay

Roll No:CB.ENP2CYS22004 ItsyBitsy

Task - 2 Scenario - Investigate a potential C2 communication alert

- First of all, we go to the site using the machine_ip provided.



- Now we login to the site using the given credentials and we start answering the questions

a) How many events were returned for the month of March 2022?

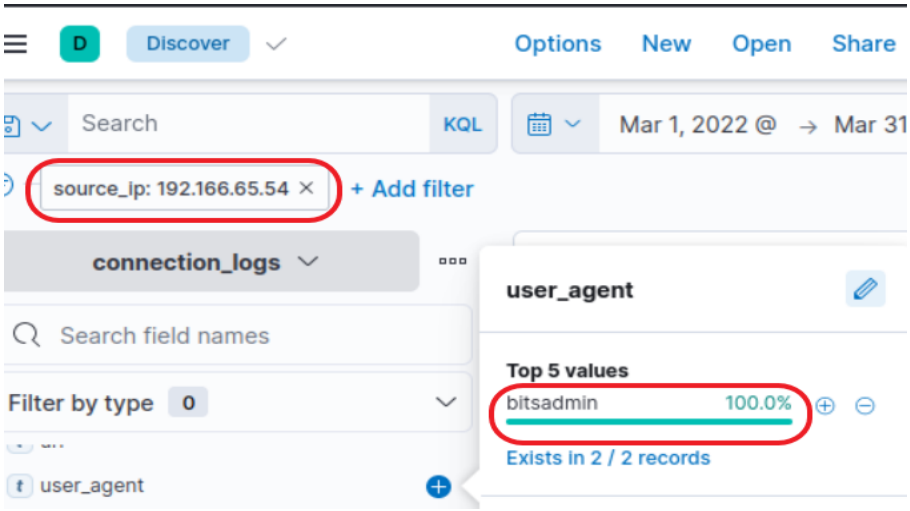
- Here, we filter date from March 1,2022 to March 31,2022 to get the number of hits

b) What is the IP associated with the suspected user in the logs?

- Here ,first we go to the filtertype useragent, and we select the bitsadmin filter which is a suspicious useragent. When we select the agent we get the IP associated to it as

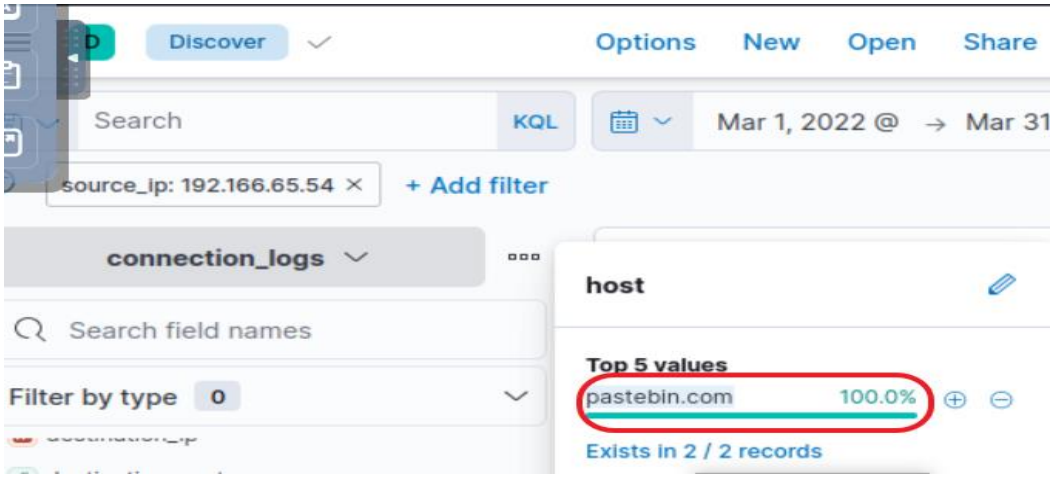
c) The user's machine used a legit windows binary to download a file from the C2 server. What is the name of the binary?

- The answer to this question is the user agent which we acquired in question 2



d) The infected machine connected with a famous filesharing site in this period, which also acts as a C2 server used by the malware authors to communicate. What is the name of the filesharing site?

- When we check the bitsadmin hits, we get the website to be

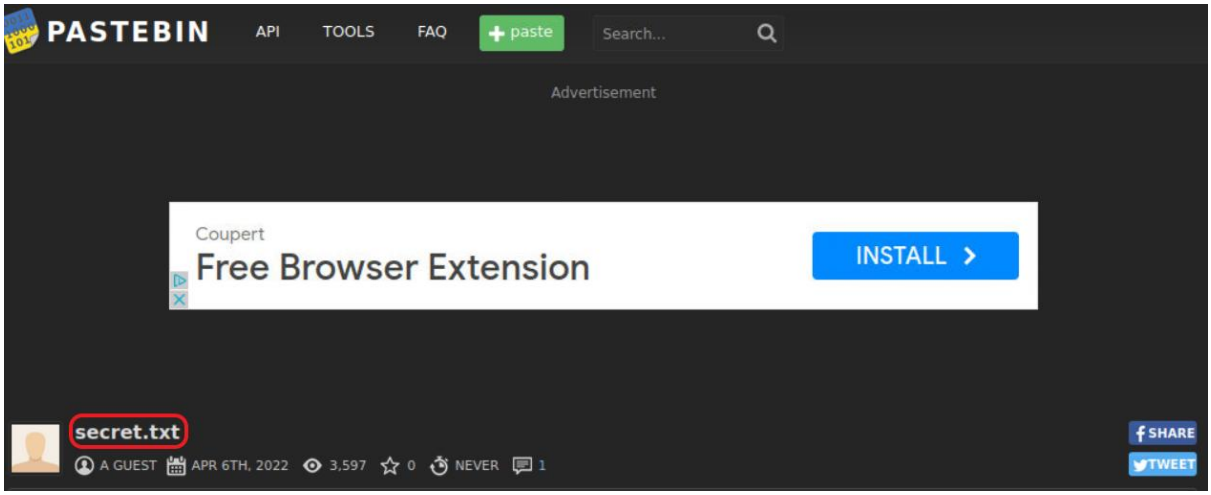


e) What is the full URL of the C2 to which the infected host is connected?

- The full URL of the site to which the infected host is connected is as given pastebin.com/yTg0Ah6a

f) A file was accessed on the filesharing site. What is the name of the file accessed?

- Now we go the URL given and we get the file which was accessed by the infected host



g) The file contains a secret code with the format THM{_____}.

- The page also contains the secret code in it.