CSAW'22

Red Team Competition

Hackers targeted « RedNews Channel » last week. This attack is part of the massive attack set observed against media, diplomatic, governmental and public sector for the last two weeks. Though the aim of this cybersecurity attack is still unclear, the company believes hackers also breached sensitive data during this attack.

You are in charge of the investigation, your mission is to perform a « red team » audit to find :
- The identity of the hacker who attacked « RedNews Channel ».
- The cyber kill chain : How he managed to penetrate the IT of « RedNews Channel ». How he modified the « flash news overlay » under the live RedNews Channel.
- The reason why he performed this attack, the company believes the hacker has been sponsored.

To be able to perform these tasks, you receive the authorization to :

- connect to all private or public IT servers of « RedNews Channel » (for example : newsX.rednews.media – replace X with the number of your team)
- perform the investigation of any materials or server under « rednews.media » or « fakebouc.com » you can discover during this investigation.

Previous investigator reports that someone called « darkHat » boasted about this attack on a public account on this social media : http://wwwX.fakebouc.com – replace X with the number of your team). (It seems that the password of darkHat is easily guessable).
In order to connect to this site, the previous investigator used the following account :

Name : RED_Inspector
Password : azerty

The success of your mission will be evaluated with the report audit you have to produce during this investigation.

Good Luck,

WARNING : In order to reserve the evidence, you are not allowed to destroy any server, or materials, so don't forget to backup any data you will use.