Sherlock: Brutus

* + - Very Easy

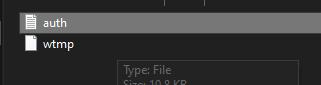
# Challenge Description :

**In this very easy Sherlock, you will familiarize yourself with Unix auth.log and wtmp logs. We'll explore a scenario where a Confluence server was brute-forced via its SSH service. After gaining access to the server, the attacker performed additional activities, which we can track using auth.log. Although auth.log is primarily used for brute-force analysis, we will delve into the full potential of this artifact in our investigation, including aspects of privilege escalation, persistence, and even some visibility into command execution.**

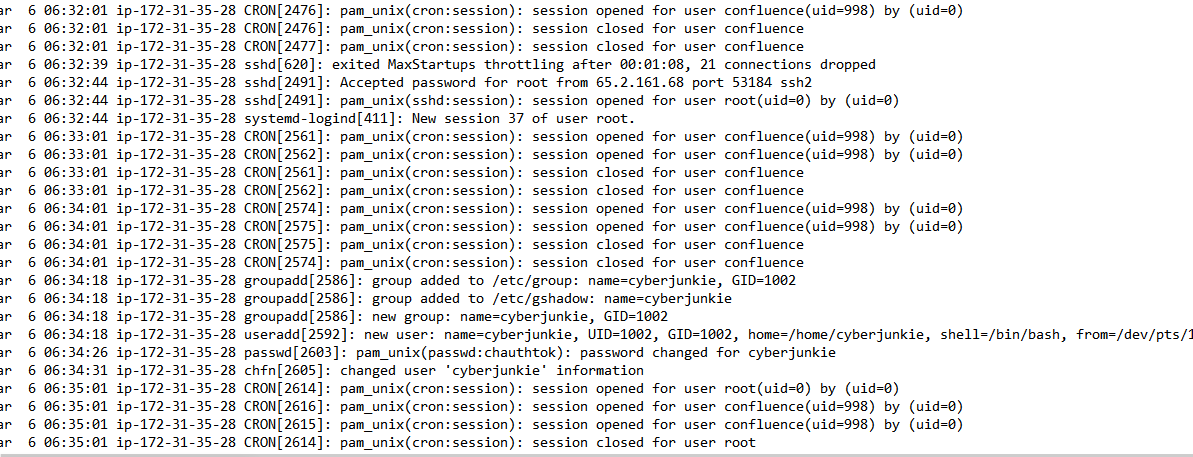
**Just Answer 8 Tasks**

# Getting Down to the Task:

* **First download the ZIP file and extract the contents of the ZIP, after that start opening the log files based on the challenges description. We are only given two files from the ZIP.**

****

* **The [Auth.log] file is the first one we open. Upon scrolling down we find the answer to most of the tasks.**

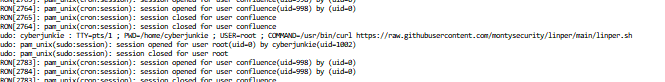
****

* **This should answer Task [ 1-7 ]**

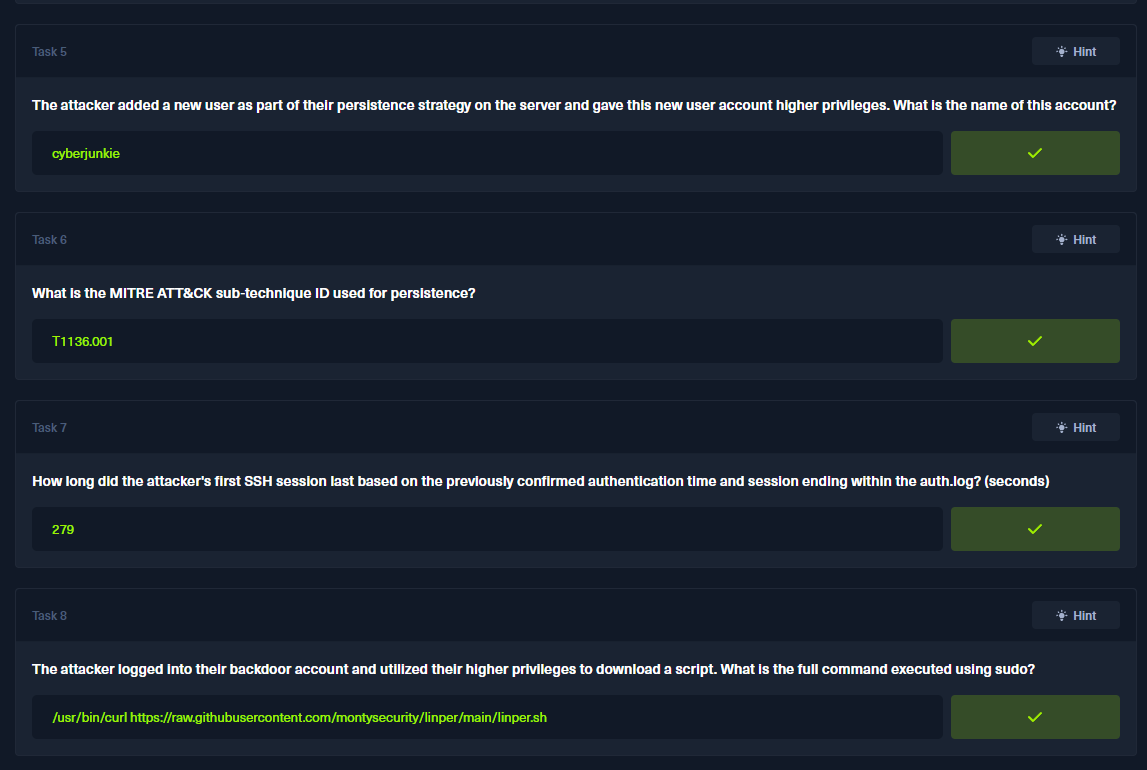
**If you stuck on Task 6 rely on this**

**[**[**MITRE Attack Techniques**](https://attack.mitre.org/techniques/enterprise/)**]**

* **Further down we get the answer to Task 8**

****

****

****

**Sherlock Brutus - Birdo**