**Report**

Task 1:

Task 2:

From the **auth.log** file and the **synthetic\_honeynet\_logs.csv** file we can see that multiple IP addresses attempted logins have some successful login attempts and there are some failed login attempts for every IP client where they want to login as **“admin”,** indicating possible **brute-force** or **reconnaissance activity**.

Some of these IPs later had **successful logins**, including for the **root account**, which strongly suggests **privilege escalation**.

Additionally, new users were created (e.g., a user named **"attacker"**) after root access, which is a common tactic to establish persistence.

This behavior is further supported by the presence of **scheduled cron jobs** tied to these IPs, showing **automated execution of potentially malicious scripts**, such as reverse shells.

Based on this evidence, **each of the listed IP clients demonstrated suspicious and coordinated attacker-like behavior**, including unauthorized access, privilege escalation, user creation, and persistence techniques.

Task 3:

Task 4:

**List of indicators of compromise**

IP addresses:

* 192.168.1.10
* 192.168.1.11
* 203.0.113.5
* 10.0.0.8

(They all share the same potential threat by trying to access protected information and execute many malicious cron jobs)

File path or binaries

* /etc/passwd

Potential act of trying to get password information of the server found in file\_changes file

* /tmp/reverse\_shell.py

An added file into the directory above coming from the cron jobs, attacker embedded in the server, also found in file\_changes file and cron.log file

2 URLs or domain used in the attack

* GET /phpmyadmin/ HTTP/1.1

Task 5: