Log Analysis

Auth (Easy)

This challenge evaluates the contestant’s ability to analyze an SSH authentication log. No additional tools are required to solve this challenge, only the ability to infer the meaning of the data in the log.

Question 1 can be solved by finding the hostname, which is listed directly after the timestamp for each entry in the log.

```
Oct 11 10:12:00 myraptor sshd[29459]: Server listening on 0.0.0.0 port 22.
```

Question 2 can be solved by identifying the IP address of the attacker in the first “Failed password” entries.

```
Oct 11 10:12:25 myraptor sshd[29465]: Failed password for harvey from 169.139.243.218 port 57273 ssh2
```

Questions 3 and 4 can be solved in the same way as question 2 by look at the subsequent “Failed password” entries that do NOT come from 169.139.243.218.

Question 5 can be solved by identifying the name of the account that had failed password attempts.

```
Oct 11 10:12:25 myraptor sshd[29465]: Failed password for harvey from 169.139.243.218 port 57273 ssh2
```

Question 6 can be found by searching for the entry that reported a “password” attempt but did not contain “failed”.

```
Oct 11 10:36:59 myraptor sshd[30003]: Accepted password for harvey from 30.167.206.91 port 55326 ssh2
```

Question	Answer
What is the hostname of the SSH server that was compromised?	`myraptor`
What was the first IP address to attack the server?	`169.139.243.218`
What was the second IP address to attack the server?	`56.13.188.38`
What was the third IP address to attack the server?	`30.167.206.91`
What user was targeted in the attack?	`harvey`
From which IP address was the attacker able to successfully log in?	`30.167.206.91`