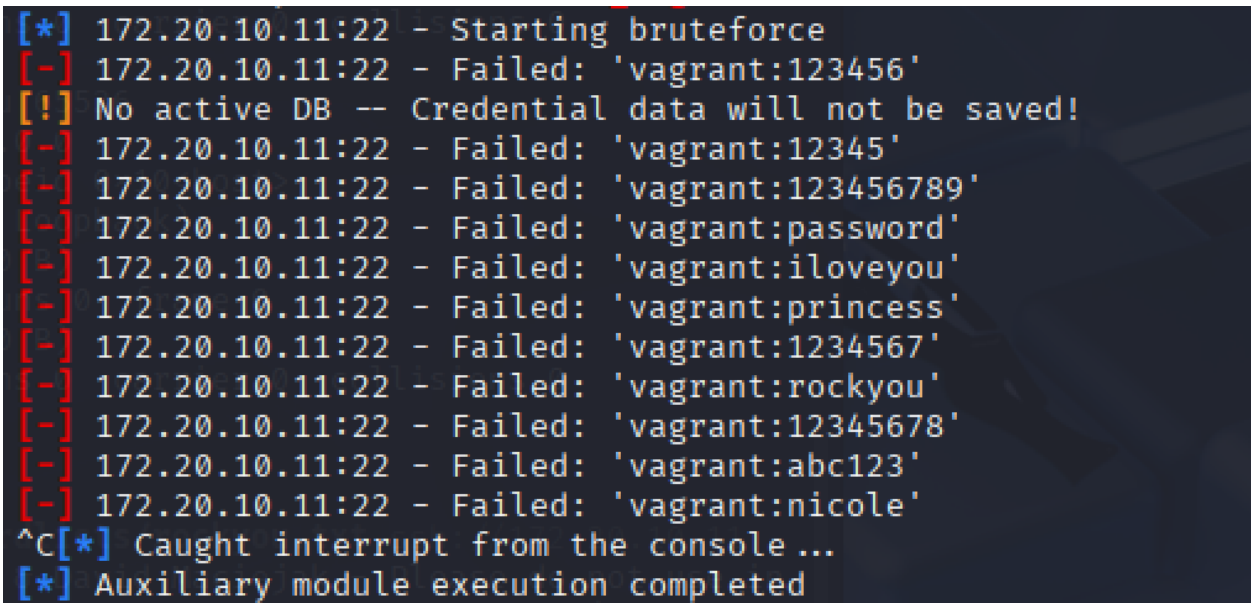
Phase 3: Setup a Suitable Defense Strategy

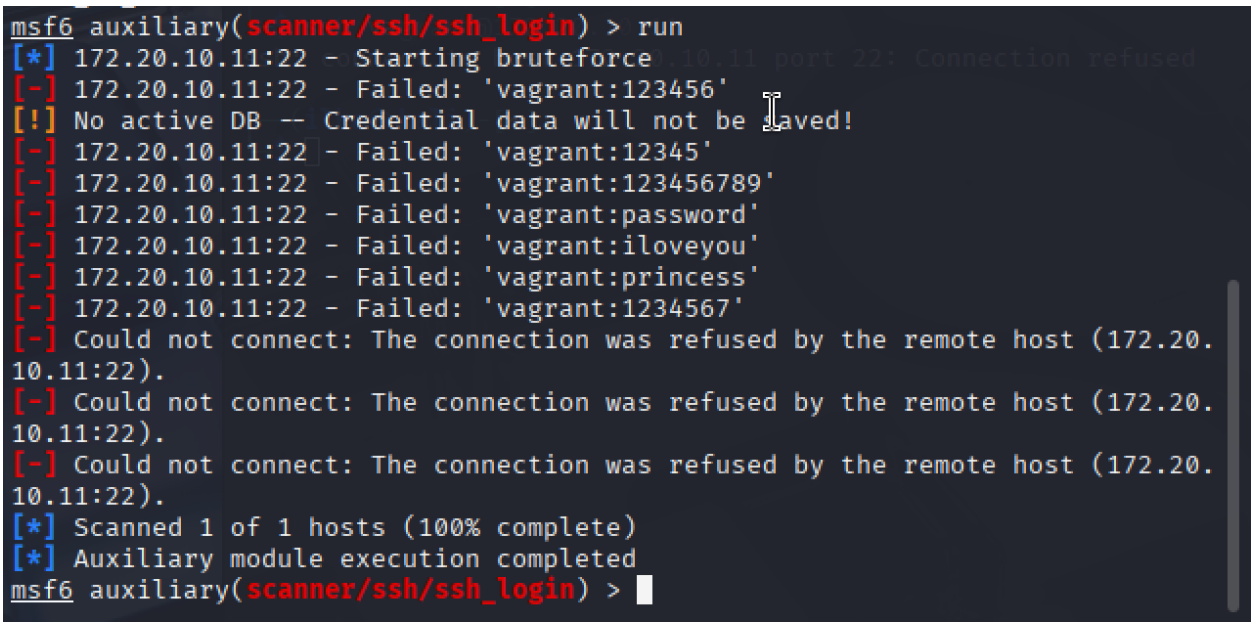
- Showcase the brute force attack on Metasploit trying to get through by trying multiple password combinations until manually stopped.



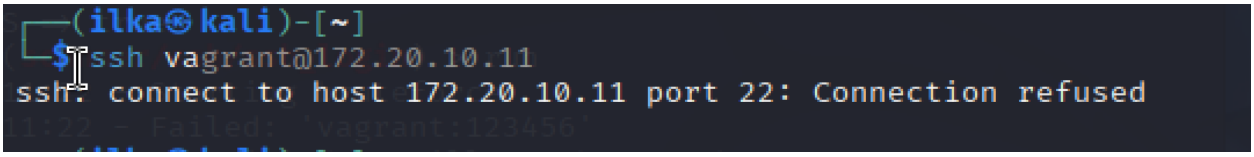
- Use and configure fail2ban jail.local file to ban out ip addresses with repeated tries.
- The parameters are configured such that after 5 attempts at accessing the ssh port the ip will be banned and logged to auth.log for 300 seconds.

```
[sshd]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 5
bantime = 300
```

- Now we can see that the brute force attack is stopped after 7 attempts
- The reason that it didn't stop exactly 7 times is because the log ins are happening quickly and fail2ban polls periodically.



- We can see that the attacker device cannot ssh into the vagrant user victim device.



- We can also see the attacker's ip is blacklisted by fail2ban on the victim's device.