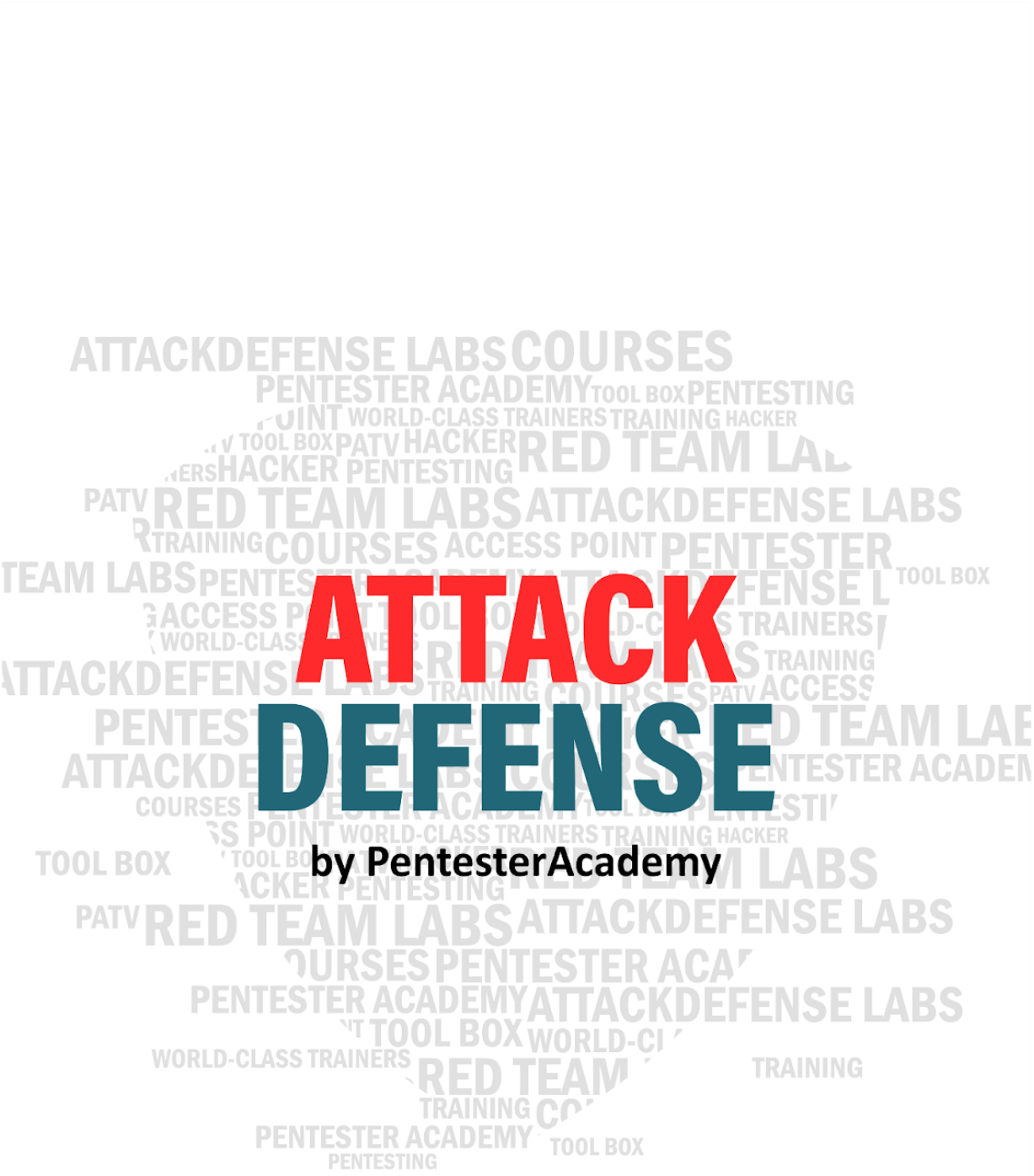
ATTACK
DEFENSE
by PentesterAcademy

Name	T1087: Account Discovery I
URL	https://attackdefense.com/challengedetails?cid=1766
Type	MITRE ATT&CK Linux : Discovery

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 for user root and admin.

Solution:

Step 1: Check the user details on the machine.

Commands: cat /etc/passwd

```
root@attackdefense:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
admin:x:999:999:admin:/home/admin:/bin/sh
```

Step 2: Check the user password details on the machine.

Command: cat /etc/shadow

```
root@attackdefense:~# cat /etc/shadow
root:$6$9n0syS4r4AlYijVL$t4v4BQH/CYxc6r5UwcWHRxyxPWHW892HSLcngdu.9xZPcyUTReCUt7nEeNQ.Un.9jCVLlmZFZkWwfXu8Lm/ej1:18346:0:99999:7:::
daemon:*:18275:0:99999:7:::
bin:*:18275:0:99999:7:::
sys:*:18275:0:99999:7:::
sync:*:18275:0:99999:7:::
games:*:18275:0:99999:7:::
man:*:18275:0:99999:7:::
lp:*:18275:0:99999:7:::
mail:*:18275:0:99999:7:::
news:*:18275:0:99999:7:::
uucp:*:18275:0:99999:7:::
proxy:*:18275:0:99999:7:::
www-data:*:18275:0:99999:7:::
backup:*:18275:0:99999:7:::
list:*:18275:0:99999:7:::
irc:*:18275:0:99999:7:::
gnats:*:18275:0:99999:7:::
nobody:*:18275:0:99999:7:::
_apt:*:18275:0:99999:7:::
admin:$6$Ckr6fYR6wHbACzjl$C8xPgUAzcRDUKHxgLFbaR9xiYFVOePvcV2OFiCar7HewitIMsnBRp0pCTj.Ue/pOjPLyhVCqdic/JD8ZWQU1D/:18346::::::
root@attackdefense:~#
```

Step 3: Run john the ripper on the saved file and use the dictionary file mentioned in the challenge.

Command: john --wordlist=100-common-passwords.txt /etc/shadow

```
root@attackdefense:~# john --wordlist=100-common-passwords.txt /etc/shadow
Created directory: /root/.john
Loaded 2 password hashes with 2 different salts (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
chicago          (root)
friendship       (admin)
2g 0:00:00:00 100% 3.773g/s 181.1p/s 362.2c/s 362.2C/s 242424..74k&^*nh#$
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@attackdefense:~#
```

Password for user root: chicago
Password for user admin: friendship

References:

1. Account Discovery (https://attack.mitre.org/techniques/T1087)