LAB

7

Cracking Password

By the end of this section, you should be able to:

- To understand the method to break password
- Applied wordlist generator tool to create list of possible passwords
- Demonstrate brute force password breaking method on ftp service
- Demonstrate the use of rainbow attack and password cracker tool

7.1 Cracking Password

One of the methods of gaining access to a machine is Password cracking. Password Cracking is the process of recovering passwords from the transmitted data over a network or data that is stored in a machine. In a penetration testing, cracking password can be used to check how secure the password mechanism in the machine or to check how easy a password can be break. Whereas, for a hacker this method is used to crack password for unauthorized access. Generally a passwords can be cracked manually or with automated tools that guessing the password until the correct password is found.

There are five Password cracking techniques, namely, Dictionary attack, Brute Forcing attack, Hybrid attacks, Syllable attack and Rule-based attack. Each of the technique's description is presented in table 1.

Table 1: Password Cracking Techniques Description

Password Cracking Techniques	**Description**
Dictionary attack	Guessing the password by referring to list of word in a dictionary.
Brute Forcing attack	Guessing the password by testing any possible combination of characters.
Hybrid attacks	By using words in dictionary added with symbols, characters or numbers.
Syllable attack	Combination of brute force and dictionary attack
Rule-based attack	This type of technique make used the information about the password in guessing the password.

7.2 Brute Forcing Attacks

A brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found.

Task 1

Generating wordlist.

1. To start brute forcing attack, we need to create a list of word by combining characters, number and symbol.
2. One method to create a list of possible word combination is by using crunch tool.
3. Start Kali linux and open a terminal, type in the following command to view the manual to used crunch

   ```
   crunch -h
   ```

4. To generate a list of word that have 4 characters with a combination of ‘a’,’b’,’c’,’1’,’2’ and ‘3’, the command is

   ```
   crunch [min] [max] [list of possible
   combination] -o [output file]
   crunch 4 4 abc123 -o wordlist.txt
   ```

5. Open the wordlist.txt and you will see a list of 4 characters with the combination of abc123.

Brute Forcing FTP Service.

1. In order to start brute forcing an ftp service, you need to prepare these two virtual machines in a same network setting.
    - Kali Linux with NAT setting
    - Metasploitable 2 with NAT setting
2. Switch on the two VM's and ping each other IP, if you are successfully ping each other than proceed to the next steps.
3. In the Kali VM open a zenmap and scan the services on Metasploitable 2 machine, you should be able to see the FTP service is running on port 21.
4. Create two text files on your Kali Desktop with the content below:-

    user.txt

    ```
    admin
    msfadmin
    user
    raju
    AhChai
    Ismai
    ```

    pass.txt

    ```
    msfadmin
    user
    admin1
    admin
    abc123
    root
    ```

5. The more you write on the two files the longer it takes to brute force the service.
6. Once you have created the two files, open a terminal and type in the command below to view the manual to used the brute forcing tool hydra.

```
hydra -h
```

7. To start brute forcing the ftp service, type in the following command

```
hydra -L [path/user.txt] -P [path/pass.txt] [IP address of your metasploitable] ftp
```

8. Wait a few second and you will be able to see the list of FTP service account and password.

7.3 Rainbow Table Attacks

One method to improve security of password is by encrypting the password stored in a machine or during the password is transmitted over the network. This approach protects the password from easily being read or captured by attacker. The password can be hashed or encrypted using secure algorithm before it stored or transmitted. For example Windows Operating systems stored it user's password in LM/NT hash, where as Linux stored it password in hash and salt. So even though an attacker get the file that is storing the user account list and password still it will no be able to read the password in plain text.

However, this mitigation approach is not 100% unbreakable, a technique called Rainbow Table attack can assist attacker to break this encrypted password storage. A rainbow table attack uses a rainbow table that consist of hash value used to gain authentication by cracking the password hash. It is a precomputed dictionary of plaintext passwords and their corresponding hash values that can be used to find out what plaintext password produces a particular hash.

For an example, to break a password for windows account, an attacker will first collect the SAM file in windows. A SAM in windows consist of the list of username account and its LM/NT password hashes. The LM/NT hashes of the SAM file is then compared with a rainbow table hashes to get the corresponding plain text characters.

Task 2

Rainbow attack on window 7 using Ophcrack.

1. Start this task by preparing the following requirement.
   - Download Kali Live (Not installer) ISO from:-
     - https://www.kali.org/downloads/
   - Download Ophcrack Table From:
     - https://ophcrack.sourceforge.io/tables.php
     - Choose Vista proba free (581MB)
   - Create two or more user account in Windows 7 VM choose and set an easy password to the account ,ideally with less than 6 characters
2. Unzip the Ophcrack table into a USB drive
3. Once the user account is created on the Windows 7 VM shutdown the VM.
4. From the VMware Menu, choose [VM] | [settings]. Choose [CD/DVD] device setting and on the connection options , click on [use ISO image file]. Browse to the Kali Live ISO file that you have download and then click [OK]
5. Next step is to boot your windows 7 VM into Kali Live , to do this the VM need to boot from the CD/DVD of your VM.

6. To boot from the CD/DVD Click on Vmware menu [VM] | [Power] | [Power On to Firmware]. You will go to the bios interface of the VM, then set your boot device to cd/dvd and exit with save changes.
7. Your VM will boot into the KALI live OS.
8. On your KALI live Desktop you will see an icon of a disk mount, this icon is the disk of your windows. If you double click on the disk icon you will see the whole folder of your windows 7 OS.
9. To get the user account and password of windows 7, open an Ophcrack tool. Click the kali application button choose [Password Attacks] | [Ophcrack]
10. On the ophcrack menu choose [Load] | [Encrypted SAM], then browse the windows 7 disk mount to [WINDOWS] folder | [SYSTEM32] folder | [Confg] folder and click on [OK]. You will see a list of user account and password in NT hashes on the ophcrack interface.
11. To crack the password, connect the USB drive containing the Ophcrack rainbow table to your VM. On VMware menu choose [VM] | [Removable Devices] | [Your USB Drive]. Do use a USB drive that support Version 2.0.
12. Then on the Ophcrack menu choose [Tables], you will see a list of Ophcrack rainbow table list. On the bottom of the list there is a [install] button, click on the button and browse to your rainbow table folder on the usb drive and click [OK].
13. Click [OK] again and you will see the name of your rainbow table on the interface of Ophcrack.

14. To Crack the password, go the Ophcrack menu and choose [Crack]. Ophcrack will start do the rainbow attack and will take a few minutes before you see the plain password on the screen.

- **For a step by step demonstration, please refer to the video manual prepared by your instructor.**

Review Question

By using an appropriate tool, crack a zip file given by the instructor.