1: Offline Password Cracking (20 points):

I have created two accounts in WinXP VM, ‘final1’ and ‘final2’, compromised it and got its password hash and put into a text file passHash.txt Download passHash.txt(only keeping the two accounts’ lines).

Please download this password hash file to your Kali Linux VM, and use the John the Ripper offline password cracking tool to find out the passwords for these two accounts. Note that you need to use the ‘rockyou.txt.gz’ dictionary file in Kali Linux in order to crack these two passwords since both passwords exist in this huge dictionary list. Please explicitly answer what are the two passwords, then use screenshot to show how you do it.

[Hint]:

The rockyou.txt.gz is a compressed file. You need to decompress it first. I have introduced this password file in class.

You need to tell JtR program to use this rockyou.txt as the dictionary file. The command option is ‘--wordlist=’. Please google search or type ‘john –help’ in Kali Linux to find how to use it.

A password could be possibly split into two parts when JtR shows the cracking result (see the slides Page 10-11).

Text

Description automatically generated

The two passwords are “ucf2004” and “knight#”.

I used gzip to decompress the rockyou zip file and moved it to the downloads folder and that is why the above command works.

2: Online Password Cracking (20 points):

In class, I have demonstrated how to use Hydra to do online password guessing attack to obtain Metasploitable Linux VM’s user account password by using ssh login cracking.

(1). Run your Metasploitable Linux VM, add a new user account of ‘final’ with the password of ‘secret’. You need to use screenshot image to show how you create such an account using commands.

I did ‘sudo useradd final’ and then ‘sudo passwd final’ and typed in ‘secret’ twice

Below is the bottom output of cat /etc/passwd:

Text

Description automatically generated

(2). On your Kali Linux VM, run Hydra to do online password attack to the ssh service running on the Metasploitable Linux VM, against the new account of ‘final’. Please use the password list file (/usr/share/john/password.lst) for this attack after removing the comment lines in the beginning of this password list file.

Verify that kali vm can ssh into the ‘final’ account:

Text

Description automatically generated

I got the ip address from typing ‘ifconfig’ in metasploitable

Please show the screenshot image of this hydra attack showing both the command line and the result, which should find the correct password ‘secret’ quickly.

Graphical user interface, text

Description automatically generated

Note: If your Hydra does not work (for some students), you can first show the error message screenshot when running Hydra, then use 'ncrack' to do the password cracking and find the password. [Note: ssh from Kali directly to the Metasploitable Linux to login with the 'final' account does not work due to 'key matching' problem without the correct option, but it does not affect the two cracking tools]

3: Metasploit Compromising Vulnerable WinXP (25 points):

Set up your Kali Linux VM and your vulnerable WinXP VM ready (this is the vulnerable WinXP I provided in class, it is still downloadable from my webserver). Make sure they can see each other. Then on Kali Linux VM, run metasploit to attack the vulnerable WinXP by using the MS10-046 ‘drive-by download’ vulnerability. For payload, use the reverse-tcp meterpreter remote shell, and local port should be set to be 5500.

(1). Use screenshot images to show how you use metasploit to successfully compromise your WinXP VM. You need to show all the commands you have used in this compromise.

Text

Description automatically generated

(2). Under the newly created meterpreter shell, display the compromised WinXP IP configuration, and then display the password hash of all accounts in your WinXP. Use screenshot images to show the results.

Text

Description automatically generated

4: Metasploit Compromising Metasploitable 2 Linux VM (35 points)

Set up your Kali Linux VM and your vulnerable Metasploitable 2 Linux VM ready. Make sure they can see each other. Then on Kali Linux VM, run metasploit to attack Metasploitable 2 Linux VM using the following two different vulnerabilities. Use words and screenshot images to illustrate your two attacks.

(1). Use the ‘samba/usermap\_script’ attack module to compromise Metasploitable 2 Linux VM. You must use the ‘cmd/unix/reverse\_netcat’ as the payload, and the local port to be 5005. After successful compromise, inside the generated shell, use command to show the IP address of the compromised Metasploitable 2 Linux VM.

Text

Description automatically generated

(2). Use the ‘unreal\_ircd\_3281\_backdoor’ attack module to compromise Metasploitable 2 Linux VM. You must use the ‘cmd/unix/bind\_perl’ as the payload, and set the local port to be 6006. After successful compromise, inside the generated shell, use command to show the IP address of the compromised Metasploitable 2 Linux VM.

Text

Description automatically generated