CIS6395 (Fall 2021): Final Exam

University of Central Florida
Cliff C. Zou

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 (only keeping the two accounts' lines).

Please download this password hash file associated with this assignment 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 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]:

1. The rockyou.txt.gz is a compressed file. You need to decompress it first. I have introduced this password file in class.
2. 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.
3. A password could be possibly split into two parts when JtR shows the cracking result (see the slides Page 10-11).

2: Online Password Cracking (12 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 '**finalexam**' with the password of '**secret**'. You need to use screenshot image to show how you create such an account using commands.

(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 'finalexam'. 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.

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.

3: Metasploit Compromising Vulnerable WinXP (24 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 **5555**.

(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.

(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.

4: Metasploit Compromising Metasploitable 2 Linux VM (24 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 **5555**. After successful compromise, inside the generated shell, use command to show the IP address of the compromised Metasploitable 2 Linux VM.

(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 **6666**. After successful compromise, inside the generated shell, use command to show the IP address of the compromised Metasploitable 2 Linux VM.

5: Armitage Exploitation (20 points)

Please run your Kali Linux VM, your metasploitable 2 Linux VM, and your vulnerable WinXP VMs together. Make sure they can see each other (i.e., they are in the same LAN). If you have run Armitage on your Kali Linux VM before, please open Armitage, remove all hosts in the Armitage target window, then restart your Armitage to do this assignment. As I introduced in class, you need to first make Armitage workable in your Kali Linux.

(1). Run Armitage on your Kali Linux, then conduct nmap scan (quick scan with OS detect) inside Armitage. Use screenshot image to show the Armitage interface where the target window section will show the two computers' icons with the correct OS information. These two computers should be the metasploitable Linux VM and the WinXP VM.

(2). After completing the above scanning process, use Armitage to either individually or use 'Hail Mary' flooding attack to let Armitage successfully compromise both VMs (in one step or multiple steps) such that their icons should show red light-bolted. Use screenshot image to show the Armitage interface after the attack finishes, and explain how you compromise both VMs.