**Assignment #5: Lab on Password Cracking Tools (6th Jan 2021)** Objectives

To help you gauge the level of security offered by the typical password systems. The  goal is to crack as many passwords as possible in the inputs described below. This  can take hours on fast laptops/ desktops, if you do not take advantage of multiple  cores or GPU.

Students should be able to:

1. Recognize the limitations of the typical password schemes

2. Sketch the cracking algorithms, and use cracking tools

Background: Required Reading

1. Password Cracking Ideas

2. Some Well Known Cracking Tools

3. ./Word-Lists and Hash-Dumps

4. The following are readily available "word lists" in the context of choosing good  passwords. This is obviously not an exhaustive list. Note also that some files are  populated at multiple sites.

5. https://github.com/danielmiessler/SecLists/ is the security tester's companion. It is a  collection of multiple types of lists used during security assessments. List types include  usernames, passwords, URLs, sensitive data grep strings, fuzzing payloads, and many  more. It includes a collection of password lists. It includes the *RockYou* lists.

6. /usr/share/wordlists/\* of the Kali Linux distribution.

7. http://contest-2010.korelogic.com/wordlists.html wordlists used in "Crack Me If You  Can" contest of DEFCON 2010.

8. https://wiki.skullsecurity.org/Passwords Passwords that were leaked or stolen from  sites.

9. http://gdataonline.com/downloads/

10. http://www.justpain.com/ut\_maps/wordlists/

11. http://weakpass.com/lists

12. http://www.adeptus-mechanicus.com/codex/hashpass/hashpass.php 13. http://www.openwall.com/wordlists/

14. Mark Burnett, Today I Am Releasing Ten Million Passwords, Feb 9, 2015. 1. SubLab-1: Online Password Cracking using Hydra

i. First of all, you are required to change Metasploitable 2 (target machine)  default password to any password of your choice (choose weak password).  ii. Then crack the password of ftp login (running of target machine) using the  following command on Kali Linux (attack machine):

*hydra -l username -P /usr/share/metasploit-framework/data/wordlists/unix\_passwords.txt  ftp://192.168.YYY.YYY –V*

where *username* is the name of the user and *192.168.YYY.YYY* is the IP address of  the target machine.

iii. If password is not found in dictionary (*unix\_passwords.txt*) then include  that password in dictionary then run the command again.

iv. Once the password has cracked, perform the ftp login on attack machine  using the command

*ftp 192.168.YYY.YYY*

v. Download and upload any file from and to target machine.  vi. Repeat the steps from i to iii for ssh login.

vii. Perform secure copy (scp) to copy a file from and to the target machine. **Note: For each step, include a snapshot in the report.**

2. SubLab-2: Cracking MD5 Password Hashes using Hashcat/John the Ripper

MD5 examples shown from machine M1 in the */etc/shadow* file format. Just three  entries.

**student**:$1$l67ia9iK$x80ABcEExHYMVpMx.Bls5.:13749:0:99999:7::: **jsmith**:$1$Y4.kjoQ2$GIuEZcnQVPYi7RPWrQRTE.:14036:0:99999:7::: **jtripper**:$1$WH2SxqnX$rL0J6JYshB3wl6yBm90Bd1:13887:0:99999:7:::

Crack the passwords of *student*, *jsmith*, and *jtripper* and include the screenshot in the  report for each user.

3. SubLab-3: Cracking SHA512 Password Hashes using Hashcat/John the Ripper

Since MD5 is considered "broken", Linux distributions have moved to using salted  *SHA512* password hashes (crypt id 6, i.e., $6$), which are several orders of magnitude  more difficult to brute-force. Example lines from machine M2:

**root**:$6$vPVevCXV$Pj2yIpQhprsMifm7i4X7F6IioqAQxJCyrhNjH4zK0fG YUc2gWjGJjobIwRp7wT5spTlLEywDW0ySmgB0XkVBs/:15401:0:99999:7:::

**ceg442091**:$6$03bKILGu$pgsg2fOTpYyhcPGSaJZfbVEFPgyle5YtGR1wY2Ch uxSv7C4lEfdES26qAXa9UHqt04ap5v0AXF0DuWMXdeaWY0:15295:0:99999:7 :::

**ceg235013**:$6$T6Yj4GYP$MjioJv3VqkU5WOx5gruV2fSHgitkSHMLvSx5M.KL 5JCDsVIVKqf3uo0DGTV.CLar0dW4eV5VYTzbfSi9rA1g8/:15398:0:99999:7 :::

Crack the passwords of *root*, *ceg442091*, *ceg235013* and include the screenshot in  the report for each user.