CYBR 8410 – Distributed System Security – 2021 Spring

Lab 2

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

NUID: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Please follow the requirements and due date specified in the Syllabus to submit your work.

Students need to answer the specified questions in the following lab content and steps, and submit your answers in a PDF or Word file.

You need to describe what you have done and what you have observed; you also need to provide explanation to the observations that are interesting or surprising.

During the lab, if anything is not clear to you, please contact the instructor.

1. **Lab Environment:**

A Linux machine. A virtual machine on Windows/Mac will also be fine.

Cryptography library OpenSSL. We will use openssl commands and libraries. Make sure you have openssl installed on your Linux machine.

Linux Bash.

1. **Lab Content and Steps:**

**2.1 Dictionary attack (35 pts)**

The file “file\_1.txt” contains a list of MD5 values of 100 users’ passwords (there is no salt). We would like to perform a **dictionary attack** to find out their passwords if possible. You need to use the popular passwords listed in the dictionary “rockyoutop1000.txt”. In order to do that, you should write **bash script(s)** to perform your attack. You will also need to record how long your script(s) would take (in seconds). Please refer to Chapter 3.2 in the textbook “Computer Security Principles and Practices” for **offline dictionary attack**.

To compute MD5 values in bash, you will need the “md5sum” command. Please refer to its manual by “man md5sum”.

echo the\_value | md5sum -

Please replace “the\_value” with a specific value you want to computer MD5 on.

1. Please attach your script(s). (20 pts)
2. How many users’ passwords did you find out? (10 pts)
3. How long does/do your script(s) take? (5 pts)

**2.2 Rainbow table (35 pts)**

The file “file\_2.txt” contains a list of hashed passwords with their salts of 100 users. We would like to prepare a **rainbow table** AND perform a **dictionary attack** to find out their passwords if possible. You need to use the popular passwords listed in the dictionary “rockyoutop1000.txt”. In order to do that, you should write **bash script(s)** to prepare the rainbow table and perform your attack. You will also need to record how long your script(s) would take (in seconds). Please refer to Chapter 3.2 in the textbook “Computer Security Principles and Practices” for **rainbow table**.

The format of “file\_2.txt” is

salt,hashedpassword

To compute the hash value from a password and a salt, you will need the “openssl passwd” command. **You must use the “-1” option!** Please refer to its manual by “man openssl”.

openssl passwd -1 -salt salt password

Please replace the “salt” with your salt, and “password” with your password.

1. Please attach your script(s). (20 pts)
2. How many users’ passwords did you find out? (10 pts)
3. How long does/do your script(s) take? (5 pts)
   1. **UNIX password system (20 pts)**

Because of the known risks of the UNIX password system, the SunOS-4.0 documentation recommends that the password file be removed and replaced with a publicly readable file called /etc/publickey. An entry in the file for user A consists of a user’s identifier *IDA*, the user’s public key, *PUa*, and the corresponding private key *PRa*. This private key is encrypted using DES with a key derived from the user’s login password *Pa*, that is, E(*Pa*, *PRa*). When A logs in, the system decrypts E(*Pa*, *PRa*) to obtain *PRa*.

1. The system can verify that Pa was correctly supplied. How? (10 points)
2. How can an opponent attack this system? Please consider all the possibilities. (10 points)