Shadow Secrets

Introduction and/or Background

Back in the days when the likes of AT&T System V WAS the primary UNIX, passwords were stored as a hashed value right in the passwd file. That was considered 'sufficient security' for quite some time. But the problem was this. In order for the end users to update their passwords they had to have sufficient right into that file to do so. Well that became a problem.

The solution was to move the hash. And that is what they did and became standard configuration on Unix and Linux machines. The hash was removed and replaced with an 'x' in its place. The hash was moved to shadow and the hash stored there. Here are the rights applied to both files:

```
-rw-r--r-- 1 root root 3149 Mar 24 14:24 passwd
-rw-r----- 1 root shadow 1833 Mar 24 14:25 shadow
```

So here is the takeaway. passwd stores account details, name, group, shell to be used. shadow stores the hash password, time of last password change, span of time to change passwords. You can find out more about shadow here.

For the purposes of password discovery one requires both the passwd and shadow file to perform the crack. The two most common tools to perform this is unshadow and john. Both tools are available on the Kali VM. One uses unshadow to unpack the shadow file and associate the hashes with the accounts. Then john is used to perform the password discovery.

John will go thru three phases, simple crack, wordlist, incremental. Each method is increasingly more sophicated in attempting to acquire the password associated with the accounts. Depending on the length and sophication of the original password it can take mere minutes to hours before a solution is arrived at. Fortunately this exercise should take no more than a hour complete in the worst case.

Objectives

In this project/lab the student will:

- Gain familiarity with password recovery

Equipment/Supplies Needed

- As specified in Lab 0.0.1.
- Linux Installation File: Kali

Procedure

Perform the steps in this lab in the order they are presented to you. Answer all questions and record the requested information. Use a Linux Virtual Machine to perform lab activities as directed. Unless otherwise stated, all tasks done as a non-root user. If root access is needed use the sudo or su command.

Assignment

Linux Attack

1 Execute the following:
- 1.a Turn on the Kali VM.
- 1.b Open a Terminal window. Promote to root.
- 1.c Create two new accounts with the adduser command:
  - c.i user: test1, password: qwerty
  - c.ii user: test2, password: 654321

2 Password Preparation
- 2.a Perform the following

```
unshadow /etc/passwd /etc/shadow > /tmp/passwords
```

3 Password Extraction
- 3.a Open directory /tmp
- 3.b Still in Terminal, execute:

```
john -- format=crypt passwords
```

- 3.c The results will not be immediate but eventually results like this will appear --

```
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (crypt, generic crypt(3) [?/6
4])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sh
a512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
kali             (kali)
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 89 candidates buffered for the current salt, minimum 96 needed
for performance.
Warning: Only 87 candidates buffered for the current salt, minimum 96 needed
for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
123456           (test1)
qazwsx           (test2)
3g 0:00:01:06 DONE 2/3 (2022-03-25 16:08) 0.04484g/s 59.87p/s 62.64c/s 62.64C
/s pretty..celtic
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Sample run against linux passwd and shadow files

3.d Take a screen shot of your terminal screen. Add that to your document.

4 Once the process has terminated execute the following:

john -- show passwords

Take a screen shot of the terminal screen. Add that to your document.

Reflection Questions

1 What algorithm was used to store the password in step 2.a?
2 What is the signifigance of '-- format=crypt' in step 3.b?
3 From a security perspective what is the difference between a LM and NTLM hash?

Lab Submissions Proof: Provide screenshots as indicated in the lab; upload your proof to Canvas for grading.

Rubric

Checklist/Single Point Mastery

Concerns Working Towards Proficiency	Criteria Standards for This Competency	Accomplished Evidence of Mastering Competency
	Criteria #1: Screenshot of Brute Force attempt with John (35 points)	
	Criteria #2: Screenshot of Brute Force attempt with John using the show option (35 points)	
	Criteria #3: Answer to reflection question 1 (10 points)	
	Criteria #4: Answer to reflection question 2 (10 points)	
	Criteria #5: Answer to reflection question 3 (10 points)	