Lab 5 Report  
Passwords

# Task 1: Password Files

1. What error did you receive when you tried to view the shadow password file without privilege?

more: cannot open /etc/shadow: Permission denied

1. As recorded in item #1 above, you received an error when you tried to view the shadow password file. Why is this error a good thing?

This specific directory uses confidential passwords so, any outsider should

not have access to that. Only the intended user must see that.

1. What is the hash algorithm that was used to store your password information in the password file?

SHA-512

1. What salt value was used to generate your stored hash value?

7voVz3cj

1. When was your password chosen, as reported by the change command?

Jul 07, 2018

1. In item #5 above you recorded the date/time when your password was selected. Why does the system need to keep track of this information?

To make sure that the password is up-to-date and secured.

# Task 2: Dictionary Attacks

1. By examining the passwords in htpasswd-sha1, which users have the same password?

alice:{SHA}A9Z8JjwnpFPvZbKeMDNHJzM8y80=

dave:{SHA}A9Z8JjwnpFPvZbKeMDNHJzM8y80=

1. List the usernames and passwords of any accounts in htpasswd-sha1 that were cracked when using tinylist.txt as the dictionary.

alice password is 'awesome'

dave password is 'awesome'

1. List the usernames and passwords of any accounts in htpasswd-sha1 that were cracked when using biglist.txt as the dictionary.

carol password is '2cute4u'

alice password is 'awesome'

dave password is 'awesome'

bob password is 'password1'

eve password is 'zaq12wsx'

1. Record the displayed statistics when you performed a dictionary attack using biglist.txt as the dictionary.
   1. Number of words tried: 2198690
   2. Number of passwords found: 5
   3. Number of seconds: 6.309
2. When a dictionary attack fails to crack one or more passwords (as was the case in the above cracking attempts), what can be said about those passwords?

Those passwords may use special characters or have many characters or don’t have any meaningful word relation according to any dictionary.

# Task 3: Considering Execution Times

1. Record the displayed statistics when you performed a dictionary attack using biglist.txt on htpasswd-md5.
   1. Number of words tried: 2198690
   2. Number of passwords found: 5
   3. Number of seconds: 6.174
2. Item #12 recorded the time it took to perform a dictionary attack on a file of MD5 digests. Assume there is a hash algorithm called APR1 that is simply 1000 iterations of MD5. If this password file indicated that APR1 had been used instead of MD5, approximately how many seconds would it have taken? Show your work.

Time Taken = factor \* base time

= 1000 \* 6.174 = 6174 seconds

1. Item #12 recorded the time it took to perform a dictionary attack on a file of MD5 digests. If this password file also contained salt values that were used in the creation of the MD5 digests (i.e., it contained the following: username, salt, digest), roughly how many seconds would it have taken? Why?

It would take roughly 8 times as before in item 12, so it might take 6.174 \* 8 = 49.392 seconds. Because, by adding the salt values (length is 8 from the item 4), the password length is getting bigger, so to crack the new appended password, it needs much time as before.

1. Record the output data when using biglist.txt on htpasswd-sha512.
   1. Number of words tried: 2198690
   2. Number of passwords found: 5
   3. Number of seconds: 3.984
2. Referring to the times recorded in #12 and #15, if a system was using MD5 as the hash function for storing password information, but then switched to SHA512, by what percentage would it slow down a dictionary attack (or a brute force attack)? Show your work.

Quite surprisingly, the cracker code took less time to crack the SHA512 hashed password compared with the MD5 hashed ones. So, the percentage would be

= (time taken in MD5 / time taken in SHA512) \* 100

= (6.174 / 3.984) \* 100 = 155 Approx.

So, it was like 55% faster to crack the SHA512 passwords.

1. Review the results of the spreadsheet when 10,000,000,000 passwords/sec was entered. From the point of view of a computer security officer, what conclusions or observations can be made?
2. Record the output data when pre-hashed passwords are used to crack htpasswd-sha1.
   1. Number of words tried: TBD
   2. Number of passwords found: TBD
   3. Number of seconds: TBD
3. Explain why crackPre.py did not try all the words in the dictionary.

# Task 4: Personal Experimentation

1. Record your observations and conclusions from your personal experimentation.

TBD

1. What did you learn from this lab exercise?

TBD

1. How could this lab exercise be improved?

TBD