Access Control and Password Management Optional Worksheet (for self-study)

1 Overview

The objective of this lab optional worksheet is to further explore set UID and the techniques that an attackers can use to crack the password by a tool called "John the Ripper" to crack the passwords stored in a file in UNIX. Students will recover passwords using different techniques.

2 Lab Environment

Virtual Machine. Cloud Ubuntu VM.

User Accounts Information. `crack-these.txt` is in the `/srv/fit2093files/fit2093lab/` folder.

3 Lab Task: Access Control: SUID Permission

In operating systems, there are many privileged operations that can only be conducted by privileged users. Examples of privileged operations include configuring network interface card, backing up all the user files, shutting down the computers, etc. Without capabilities, these operations can only be carried out by superusers, who often have many more privileges than what are needed for the intended tasks. Therefore, letting superusers to conduct these privileged operations is a violation of the *Least-Privilege Principle*.

Privileged operations are very necessary in operating systems. All `Set-UID` programs invole privileged operations that cannot be performed by normal users. To allow normal users to run these programs, `Set-UID` programs turn normal users into powerful users (e.g. root) temporarily, even though that the involved privileged operations do not need all the power. This is dangerous: if the program is compromised, adversaries might get the root privilege.

We will use an example to show the `Set-UID` permission. First, let us login as the user `sierra` created in the lab by using `su sierra`, and run the following command:

```
passwd
```

The program should run successfully. Look at the file attribute of the program, run `ll /bin/passwd`. The output would look as follows:

```
-rwsr-xr-x 1 root root 68208 Jul 15  2021 /bin/passwd*
```

You will find out that `passwd` is actually a `Set-UID` program with the owner being root, i.e., when you execute `passwd`, your effective user id becomes root, and the running process is very powerful. Look at the third letter access right for owner, the letter is `s` instead of `x` which indicates that the program uses the `Set-UID` when executed.

If there are vulnerabilities in `passwd`, the entire system can be compromised. The question is whether we can remove these privileges from `passwd`.

Let us turn `/bin/passwd` into a non-`Set-UID` program. This can be done via the following command (using superuser privilege):

```
sudo chmod u-s /bin/passwd
```

Run `ll /bin/passwd` again to check file permissions, which would look as follows:

```
-rwxr-xr-x 1 root root 68208 Jul 15  2021 /bin/passwd*
```

Note: Binary files like passwd may locate in different places in different distribution of Linux, use 'which passwd' to locate your passwd program.

Now, run passwd, and see whether you can change the password. Interestingly, the command will not work. This is because passwd needs to open the file /etc/shadow, which is a privileged operation that can only be conducted by root (before capabilities are implemented). That is why passwd has to be a Set-UID program.

4 Lab Task: Cracking Passwords

We will be using the password cracking program John the Ripper for this task. The basic functionality of John the Ripper is to repeatedly try different passwords and hash them until it finds one which matches the hash of the password we are trying to crack. We will use three techniques to crack passwords in this lab, dictionary attack, hybrid attack and combination attack.

1. **Dictionary Attack:** Since the number of passwords could be infinite, brute force attack (testing all possible passwords) will not be a feasible solution unless the password was very short. Instead, we will be more clever by trying a list of more likely passwords first. This is called a dictionary attack. John the Ripper comes with a small dictionary of some typical passwords located in /usr/share/john/password.lst. Take a look at it!. The crack-these.txt file (in the /srv/fit2093files/fit2093lab/ folder) contains account information for 50 users. Now copy the crack-these.txt file to your home directory and run the following commands to perform the dictionary attack

```
% cp /srv/fit2093files/fit2093lab/crack-these.txt ~
% john -w:/usr/share/john/password.lst  ~/crack-these.txt
```

John has created a list of solved passwords in a file john.pot, run cat ~/.john/john.pot to see it. How many of the 50 passwords it was able to crack, what are they, and the time it took?

The output of running john using the given list would be as follows:

```
Loaded 50 password hashes with 50 different salts (descrypt, traditional crypt(3) [DES 32/32])
Press 'q' or Ctrl-C to abort, almost any other key for status
money            (user21)
hello            (user14)
cowboy           (user07)
test             (user29)
blue             (user03)
japan            (user16)
bonjour          (user04)
dog              (user10)
pass             (user24)
www              (user43)
www              (user44)
11g 0:00:00:00 100% 16.41g/s 5286p/s 230391c/s 230391C/s ship..sss
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

the recovered passwords:

```
M.h.0vk3BhbbE:money
VtsKjVbDshURM:hello
```

```
hSWM/OxbN7mLg:cowboy
HNTH57eGshHyQ:test
qOehxlruvN3F6:blue
TviJwR4elCrEk:japan
oPWWjG8dOl7Jk:bonjour
bVbJ8EjFft7Ig:dog
J1KYaW5A7YmTw:pass
NbXi5ONo1R11g:www
krwhufvZUsT/Q:www
```

2. **Hybrid Attack:** A hybrid attack checks for variations of a word or a combination of dictionary words. For example, we could make it append numbers to the end of all the words in the dictionary, such that if the word cat was in the original dictionary, then it would also try the words cat0, cat1, . . . , cat9, cat00, cat01, etc.

   To run this attack execute following commands

   ```
   % john -w:/usr/share/john/password.lst -rules ~/crack-these.txt
   ```

   How many more passwords did the hybrid attack crack? Is there any relationship between what it cracked this time, and those from last time?

   One additional password is found.

   ```
   Loaded 50 password hashes with 50 different salts (descrypt, traditional crypt(3) [DES 32/32])
   Remaining 39 password hashes with 39 different salts
   Press 'q' or Ctrl-C to abort, almost any other key for status
   wwwwww           (user47)
   1g 0:00:00:11 100% 0.08873g/s 12357p/s 471030c/s 471030C/s Sssing
   Use the "--show" option to display all of the cracked passwords reliably
   Session completed
   ```

3. **Combination Attack:** John the Ripper executes dictionary, hybrid, and brute force attacks in combination. Launch a combination attack by executing:

   ```
   % john ~/crack-these.txt
   ```

   How many more passwords did the combination attack crack? how long did it take?
   You can add more passwords in `password.lst` file or download a larger file from Internet, and try again above attacks.

   ```
   Loaded 50 password hashes with 50 different salts (descrypt, traditional crypt(3) [DES 32/32])
   Remaining 38 password hashes with 38 different salts
   Press 'q' or Ctrl-C to abort, almost any other key for status
   Warning: MaxLen = 13 is too large for the current hash type, reduced to 8
   1337             (user18)
   bloody           (user02)
   bread            (user05)
   perro            (user11)
   more             (user22)
   bike             (user01)
   bueno            (user06)
   mind             (user20)
   kaput            (user17)
   ddd              (user08)
   ```

```
tall             (user28)
smc              (user26)
linux            (user19)
dejavu           (user09)
w                (user41)
stir             (user27)
really           (user25)
nauj             (user39)
fido             (user12)
hackme           (user36)
abcdefgh         (user23)
ww               (user42)
22g 0:00:45:24 3/3 0.008075g/s 23063p/s 436618c/s 436618C/s ciiefe..ciiekj
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

I have aborted the process as it was taking too long but you can let it run for longer (seems about 45 minutes or so) if you wish.