CPSC 525/625: Principles of Computer Security (F23)
Instructor: Ryan Henry <ryan.henry@ucalgary.ca>

Name: Alex Stevenson

UCID: 30073617

Worksheet 0x06

Part 1: Keypairs versus passwords

(a) List some potential benefits of using public keys instead of passwords for ssh authentication.

Public keys can't be randomly guessed or deduced by attackers.

Public keys don't allow bots or other users to spam authentication attempts at the server.

(b) List some potential drawbacks of using public keys instead of passwords for ssh authentication.

If you lose access to your public key somehow, or if your private key doesn't match your public key on the server, you get locked out of it with no way to get back in.

(c) Why might you want (or not want) to use a passphrase for an ssh public key?

You may want to use a passphrase for greater security to prevent others from using your private key (cases such as if they have gained access to your computer)

You may not want to use a passphrase because they are tedious to type in every time you want to ssh into something

CPSC 525/625: Principles of Computer Security (F23)
Instructor: Ryan Henry <ryan.henry@ucalgary.ca>

UNIVERSITY OF CALGARY

Name: Alex Stevenson

UCID: 30073617

Part 2: Unix permissions

```
ryan@mocha:~$ ls -l /usr/bin/passwd
-rwsr-xr-x 1 root root 59640 Nov 29 2022 /usr/bin/passwd
ryan@mocha:~$ ls -l /etc/passwd
-rw-r--r-- 1 root root 11928 Sep 17 23:17 /etc/passwd
ryan@mocha:~$ ls -l /etc/shadow
-rw-r----- 1 root shadow 22121 Sep 18 10:32 /etc/shadow
ryan@mocha:~$ ls -l /usr/bin/sudo
-rwsr-xr-x 1 root root 149080 Apr  4 05:56 /usr/bin/sudo
ryan@mocha:~$ ls -l /bin/su
-rwsr-xr-x 1 root root 44664 May 30 09:42 /bin/su
ryan@mocha:~$ ls -l /etc/sudoers
-r--r----- 1 root root 755 Sep 17 22:58 /etc/sudoers
```

(a) The above output is copy-pasted from a real session on mocha. Which of the following files do you think *you* have permissions to `read`? How about to `write`? And to `execute`?

As each of these files belong to user `root` and group `root`, you only have `everyone` permissions.

That is:
Read: `/usr/bin/passwd`, `/etc/passwd`, `/usr/bin/sudo`, `/bin/su`
Write: None
Execute: `/usr/bin/passwd`, `/usr/bin/sudo`, `/bin/su`

(b) Come up with the best justification you can think of for why each of these files has the permissions that it does. (This is not a trick question. There are good reasons these permissions are as they are.)

Anyone can read `/usr/bin/passwd`, `/usr/bin/sudo`, `/bin/su` as they are binaries.
Anyone can read `/etc/passwd` to view the users and groups of the system
Anyone can execute `/usr/bin/passwd` as it allows you to change your password.
Anyone can execute `sudo` or `su` as they require authentication before using if the user is not root.

CPSC 525/625: Principles of Computer Security (F23)
Instructor: Ryan Henry <ryan.henry@ucalgary.ca>

UNIVERSITY OF CALGARY

Name: Alex Stevenson

UCID: 30073617

(c) Who did you team up with for the group activity?:

1. Alex Stevenson
2. Simrat Benipal
3. Francis Nacu

As a group, think critically about the file permissions you saw on the last page. Now, donning your attacker hat, what seem like the most promising avenues for attack? Share your though processes. **I'm not looking for concrete attacks; rather I'm curious where you would start *probing* for potential weaknesses, in light of the information contained above.**

Try reading /usr/bin/passwd to get usernames of different users. Then trying to brute force their passwords in ways that are related to their username.

Otherwise try probing passwd, sudo, su to see if your execute permissions get you anywhere

(d) Designate a member of your breakout group to do the following: By the end of today, post a followup to my Piazza posting that includes your group's responses to prompt 2(c). To assist the TAs in locating your Piazza post, please have each group member enrol in the same group (under the Worksheet 0x06 category) on D2L and designate one member of your group to upload a direct link to you Piazza post to the dropbox for that group.

[And please read/comment on/critique/discuss the ideas given by other groups by replying to their followups!]