CS349 Computer Security **Handout # 2**
Prof. Lyn Turbak **September 17, 2004**
Wellesley College

Homework 2
Due: 6pm Friday September 24

Note: Lyn will be away at a conference from Fri., Sep. 17 – Wed. Sep. 22 (inclusive). On Tue. Sep. 21, Betsy Masiello '03 will fill in for Lyn in class, where she will lead a discussion on privacy.

Reading:

- Lessig, *The Architecture of Privacy*
- Masiello, *Privacy Implications of Biometric Surveillance: The Destruction of Anonymity* (optional)
- Browse the following websites for "industry" views on privacy: `www.cdt.org`, `www.eff.org`, `www.epic.org`
- There are a number of good books on privacy in the security library in SCI 121B that you may want to skim. Garfinkel's *Database Nation* is particularly interesting.
- Bishop, Chapters 12, 13, 14.1-14.5, 15

Problem 1: Privacy and Security

a. Before doing any of the privacy readings, prepare a (short!) written essay about your own thoughts on the following topic:

> Is digital security or digital privacy a greater concern today (1) to you personally and (2) to society at large?

b. After doing the privacy readings, but before coming to class on Tuesday, Sep. 21, write down how (if at all) the readings have influenced your views on security and privacy.

c. After the privacy discussion on Tue. Sep. 21, write down how (if at all) the class discussion has influenced your views on security and privacy.

Problem 2: Linux System Administration

(Please do not start this problem until after noon on Fri. Sep. 17.) In this problem, you will choose a partner and a machine in the Security Lab (SCI 121B) and become system adminstrators (sysadmins) of that machine. You and your partner will "own" that machine for the rest of the semester.

a. : Choose a Machine

Choose one of the following five machines in 121B, putting a note on it to indicate it is "yours":

- `lion (192.168.1.1)`
- `ocelot (192.168.1.2)`

- `leopard (192.168.1.3)`
- `lynx (192.168.1.5)`
- `tiger (192.168.1.6)`

The number in parentheses is the IP number (network address) of the machine. The machines are networked to each other, but not to the outside world. We will refer to this network as the *security lab network (SLN)*. Since the SLN has no nameserver, the machines will not recognize the English names `lion`, `ocelot`, etc. You will have to use the IP numbers to refer to other machines. For example, to telnet to lion, you execute `telnet 192.168.1.1`. Similarly, when the web servers are enabled (they currently are not), you will use a URL with `192,168.1.1` to access a web page on lion.

There are two other machines in 121B:

- `caribou (192.168.1.4)`: This is a machine currently being reserved for development. You are welcome to use it, but not "take it over". It is the only one of the six SLN machines that has a Zip drive. For this reason, it will often be use to distribute files (such as for the Password Cracking exercise, below).
- `rhodes`: This is the only machine in 121B that is on the regular Wellesley network. It is *not* on the SLN. It provides a way for you to access the "outside world" from 121B. It has a Zip drive, so it can be used in conjunction with `caribou` to download software off the net and install it on SLN machines.

b. : Log into Your Machine

You can log into your machine with superuser privileges via the username `root` and password `toober`. Each machine also has a regular user account with username `guest` and password `anonymous`. By default, you will be provided with a text-based interface to the machine. To get the Gnome X-Windows graphical interface, execute the command `startx`.

c. : Change the Root Password

You wouldn't want anyone else to log into *your* machine with superuser privileges, would you? One of the first things you should do is change the root password using the `passwd` program.[1] This program does some simple checking to prevent you from choosing an easily guessable passsword, but you still need to choose your password with care.

d. : Create Some Accounts

Next you should create some "fake" user accounts with the `useradd` program discussed in class to get experience with account creation. You can set the passwords for these accounts using the `passwd` program and/or the `-p` option to the `useradd` or `usermod` programs. (To generate a DES-style hashed password, used the `crypt.pl` program on the download disk. Accessing files on the download disk is explained in the Password Cracking exercise.) For the purposes of the Password Cracking exercise, you will want some users to have "good" passwords and others to have "bad" (easily crackable) ones.

e. : Play with Linux

As system administrators, you need to gain familiarity with lots of Linux commands. Below are some of the commands you should be familiar with. The list is by no means exhaustive!

[1] You may need to type `Control-C` after changing the password to return to the system prompt.

Many of the commands have lots of options; some of the common options ones are listed. To get documentation on this commands, use `man` and `info`, browse on-line resources, and refer to the many Linux books in the Security Lab. You should also play with pipes (`|`) and input/output redirection (`<`, `>`) and learn a little bit about shell scripts.

```
cat
cd
chmod (-R)
chown (-R)
chgrp (-R)
cp (-R)
du
df
echo
find
grep
gunzip
gzip
info
less
ln (-s)
ls
man
mkdir
more
mount
nice
passwd
popd
ps (-ef)
pushd
pwd
rm (-rf)
scp (-r)
ssh
source
su (-)
tar (-cvf, -xvf)
telnet
top
touch
umount
useradd
usermod
wc
which
whoami
```

Problem 3: Password Cracking

In this problem, you will play with a password cracking program known as "John the Ripper" or just plain John for short.

a. : Download John

In the Security Lab, there is a green Zip disk that we'll call the *download disk* that contains useful files and will be updated throughout the semester. For instance, the download disk currently contains the `john-1.6` directory and the Perl programs `crypt.pl` and `md5.pl`.

To download `john-1.6` onto your machine, take the following steps.

1. Insert the donwload disk into the Zip drive of `caribou`.
2. Log into `caribou` as `guest` (password `anonymous`).
3. Execute `mount /mnt/zip100.0`. This will make the zip disk visible to the file system.
4. From an account on another machine (other than `caribou`), execute:

   ```
   scp -r guest@192.168.1.4:/mnt/zip100.0/john-1.6 .
   ```

   This will copy the whole `john-1.6` directory from the download disk to the remote account.
5. On `caribou`, execute `umount /mnt/zip100.0` to unmount the Zip disk from the file system.
6. On `caribou`, press the green button on the Zip drive to eject the disk.

b. : Use John

The `john` program attempts to crack passwords by generating likely passwords, hashing them, and comparing them to the hashes in the password files. (In Bishop's terms, it is a type 1 dictionary attack.)

Read the documentation on how to use `john` in the `john-1.6/doc` folder. The executable is in `john-1.6/run/john`. For input to `john`, you will need to make a copy of your `/etc/passwd` file that replaces the `x`s with the passwords in `/etc/shadow`. Your should not contain any system usernames, just `root`, `guest`, and your fake users.

Run `john` on the copy of your password file. How well does it do in terms of cracking "bad" passwords?

If you have time, you may want to modify the rules of John so that it can crack more passwords. Read the documentation for more info.

Jennifer Song has lots of experience running `john`. She has offered to answer questions you may have about the program