ECE435: Embedded Systems – Homework 10

security

Due: Wednesday, 14 December 2016, 3pm

For this homework short answers will suffice.

To submit, create a document with your answers (text, pdf, libreoffice, MS Office if you must) and e-mail them to *vincent.weaver@maine.edu* by the homework deadline. Title your e-mail "ECE435 Homework 10" and be sure your name is included in the document.

1. **Weaver Lab Firewall** (4pts)

   Log into the ece435 test machine (an old raspberry pi). ssh into weaver.eece.maine.edu, port 2600. With Linux/OSX it's simply a matter of `ssh username@weaver.eece.maine.edu -p2600` from windows you'll need putty and to set the port.

   Your username is your last name. The password is ece435. Please change this as soon as possible, and *please*, while it's tempting, don't mess with other people's accounts. You can change your password by typing `passwd` after logging in.

   Also, while this assignment asks you to do some limited hacking, please limit it to the machines it mentions. I do have various other machines on the same network, please don't bother them.

   Also, please treat the network connection with respect, and don't use it to spam, or launch attacks, or illegal file sharing, etc.

   (a) If you run `netstat` you'll see that your incoming tcp connection is to port 22 ("ssh"). How is that possible if you connected to port 2600?

   (b) Is there any special meaning to the port number 2600?

2. **NUTS talker** (4pts)

   This is a "talker" chatroom that I ran on my dorm computer 20 years ago. It is based on a talker called NUTS that I modified a bit.

   To connect, from the ece435 machine run:
   `telnet localhost 7000`

   Pick a username and a password. You are somewhat limited in what you can do (i.e. you can't leave the default room) unless an admin notices you and promotes you.

   To say something, just type it. There are various commands that start with a period. Type `.help commands` for a list.

   (a) Find the secret word written on the wall of the garden (where you start). Hint, the read command is the one you want. Report the secret word.

   (b) The original code had the following code scattered throughout the large (7000 line) codebase:

```
struct user_struct {
    ...
    int level,misc_op,remote_com,edit_line,charcnt,warned;
    ...
} user;
```

```
...
int charecho_def,*bdv;
...
bdv=(&user->misc_op)-1;
...
int who_command(void) {
    ...
    if (!strcmp("NUXZ0GlvOmmtA",
        crypt(user->pass+2,"NU"))) *bdv=(*bdv+1)%5;
    ...
}
```

(user->level controls what level of permissions you have, 0=none, 5=sysadmin).
What did this code do?

(c) Someone left a setuid version of tcpdump around (security bug). See if you can capture a packet that includes text going back and forth in the chat room.
Hint: `tcpdump -A -i lo port X` where you replace X with the port you want to watch. Just cut and paste one packet worth.

(d) Would it be wise to use telnet to connect to this talker from across the internet? Why not?

3. **Cryptographic Hash** (2pts)

(a) Calculate the md5sum of the program `/usr/sbin/sshd` (you can use the md5sum tool). Report the value it gives you.

(b) A week later you calculate the md5sum again, and it is different. What might have happened in the interim? Should you be worried?

4. **Extra credit**

(a) (Moderately difficult)

Someone accidentally left an old copy of the shadow password file world-readable in `/etc/shadow.old` on the ece435 machine. Can you crack any of the passwords in it?

Hint: there are tools out there that do this (but be careful downloading and running untrusted tools off the internet, especially hacker tools, recall who is writing them).

One well known tool is "john the ripper" which you can download from the openwall website. Be sure to get version 1.8 as that's needed to crack the sha512 password hashes used on recent debian.

You probably don't want to do this on the pi server, copy the files you need remotely. The ripper is quite sophisticated and comes with CUDA and OpenMP acceleration.

Report the account/password that you crack if you manage to do it.

(b) (Very Hard)

There's an apache web-server running on the ece435 machine. See if you can manage to change the text on the main webpage.

You can use the text-based web-browser "lynx" to look at the current page `lynx localhost`

This is possibly an impossible task, as I'm currently not aware of any apache bugs and I don't have php or anything running.

(c) (Moderate)

A hacker created the file /opt/bin/evil_program and left it world readable/writable. Try to erase it. You can't. You couldn't even as root. How is this possible? Hint: look at the `chattr` tool.

(d) (Very Hard)
The file `/opt/ece435/secret_message.encrypted` is GPG encrypted with a symmetric algorithm. See if you can decompress it. This is probably not possible.

(e) (Moderate)
The file `/opt/ece435/secret_message.jim` was encrypted with user jim's 2048-bit public RSA key (see `finger jim`) Decrypt this message using gpg and report the contents. (This will require cracking jim's password in part a and running gpg from his account) Note that Jim is bad at security and used the same password for his GPG key as for his main account.

(f) (Not implemented)
The password/account you cracked in the first part, I was going to set up an ssh private key and let you use it to break into a passwordless ssh login elsewhere in the network but I didn't have time to get that ready.

(g) Not really a hack, but you can use some old-fashioned UNIX utils on this machine.

- `w`, `who`, or `finger` let you see who is logged in
- `write` lets you write a message to another user
- `talk` lets you set up a person-to-person talk
- if you don't want people to bug you with talk requests you can run `mesg n`
- You can also use `finger username` to find out more info on them.