Rootkits

The best way to understand what a rootkit does is to play with one. As with all our labs, these are for educational purposes only. Any use of programs for illegitimate use either intentionally or unintentionally could result in failure of the course as well as legal action.

Make sure all this is done on a DISPOSABLE virtual machine. We will break things. The machine we compromised in the previous assignment would be ideal.

Virtualbox users could take a snapshot of your vm so it is easier to rollback after you are done.

Look at submission instructions below for what to turn in

Linux Rootkit 1

- I only tested on the 14.04 install.
- Download this file
  - ungzip and untar in your home folder.
- Note that within the bin folder of the above extracted directory, there exists a binary called `login`. A malicious user would try to replace this `rootkitted` version of the `login` binary with the `login` program found in the `/bin` directory of your OS installation.
- We need to replace the program `/bin/login` with the rootkitted version. Prior to doing so, observe what currently happens when you provide an invalid username/password combination to the *real* login program.
  - create a directory called `/bin/backup`
  - copy `/bin/login` into `/bin/backup`
  - copy the rootkitted version into `/bin`
- Test the *new* login program. Easiest way is just to :
  - `/bin/login`
- Observe what happens as you input valid/invalid username/password combinations.
- Note that the primary reason a hacker would want to replace the login binary is so that they can login.
  - try the password `satori` with any of your existing usernames, create a user called 'user1' with whatever password you want and try the login using `satori`, observe what happens.
  - Try the username/password combination `rewt`/`satori`, what happens?
- Explore another binary that you can overwrite.

Linux Rootkit detection

- Leave your *modified* version of login in the `/bin` directory.
  - Install chkrootkit
  - `sudo apt-get install chkrootkit`
  - run chkrootkit, it should detect that the `login` is INFECTED
- Install `rkhunter`, see if it can detect more?
- Replace the INFECTED login with the original, rerun chkrootkit and rkhunter, observe.
  - `cp /bin/backup/login /bin/`
- Take a look at the README file inside of the lrk4 directory. What other programs could you try to overwrite? Why would you want to overwrite things such as `ls` or `du`?

TO submit

- Screenshot showing output of rootkitted login binary
- Screenshot of rkhunter (sample)
- Screenshot of chkrootkit (sample)
- Write a short paragraph of your conclusions about rootkits. Prevention? Detection?

Linux Troubleshooting

- If having problems with rootkit, may have to issue this command: `# init 3`