Hacking with Linux networking command line tools

Xiaolin Wang

December 31, 2021

Contents

1 Caution

- You must submit your report as a `tar ball` in which the following files should be included:

  1. Your report in either `Emacs Org` or `Markdown` format, and a HTML file generated from your `org` or `md` file.

     Tips:

     – In Emacs, press `C-c C-e h h` to export HTML file from your org file;

     – For `Markdown` to HTML, you can try `markdown`, `pandoc`, `cmark`, whatever.

     – This page itself is generated from an org file (proj-week.org). You can take it as an example.

     – Report template: `org file`, `html file`, `markdown file`

  2. your bash script for a HTTP demostration;

  3. a `ttyrec` file recording your operations (`man ttyrec`);

---

  1. Here's how ::

     (a) make a directory, e.g. 20201159xxx. In this directory, try very hard to make all the files available.

```
mkdir  20201159xxx
cd 20201159xxx
emacsclient tmux-http.sh # write your script
emacsclient 20201159xxx.org # this is your report
vim 20201159xxx.md # in markdown format
ttyrec http-demo.ttyrec # make your demo screencast
```

(b) make a tar ball.

```
cd ..
tar zcf 20201159xxx.tgz 20201159xxx
ls -l # make sure your tar ball is smaller than 1MB in size
```

(c) upload the `tgz` file to our moodle site.

- Here is a short tutorial about writing lab report: `tutorial.ttyrec`. To view it:

  ```
  ttyplay  tutorial.ttyrec
  ```

  Feel free to make your own `ttyrec` file while doing this lab work. For example:

  ```
  ttyrec  20201159xxx-http.ttyrec
  ttyrec  20201159xxx-email.ttyrec
  ttyrec  20201159xxx-ftp.ttyrec
  ```

- **Deadline:** *<2021-10-31 Sun>*
  - Submit your report as a `tgz` file here. In your `tgz` file, there must be:
    1. your report in `org` or `markdown` format
    2. your report in HTML format
    3. your bash script for demostrating a HTTP session
    4. one or more `ttyrec` files for demostrating whatever you did
  - Late reports will be penalized 20% per day.

- MS-word file will **NOT** be accepted. Cheating will result in automatic failure of this work.

2 tmux, nc, ip, tcpdump, ss, nmap, curl

Here are the bash scripts I used in the class for demostrating how some protocols work.

- TCP three-way handshake
- UDP
- SMTP (need a SMTP server)
- FTP (need a FTP server)

Your tasks (Deadline: *<2021-10-31 Sun>*)

1. Run the above scripts to get familar with these tools, and get a thorough understanding about these protocols;
2. Packet analysis. Upon running the following command:

   ```
   sudo tcpdump -ilo -nnvvvxXKS -s0 port 3333
   ```

   the following packet is captured:

   ```
   08:34:10.790666 IP (tos 0x0, ttl 64, id 12824, offset 0, flags [DF],
   proto TCP (6), length 64)
   127.0.0.1.46668 > 127.0.0.1.3333: Flags [P.], seq 2400005725:2400005737,
   ack 373279396, win 512, options [nop,nop,TS val 3259949783 ecr 3259896343],
   length 12
       0x0000:  4500 0040 3218 4000 4006 0a9e 7f00 0001  E..@2.@.@.......
       0x0010:  7f00 0001 b64c 0d05 8f0d 2e5d 163f caa4  .....L.....].?..
       0x0020:  8018 0200 fe34 0000 0101 080a c24e e2d7  .....4.......N..
       0x0030:  c24e 1217 6865 6c6c 6f20 776f 726c 640a  .N..hello.world.
   ```

   (a) Tell me the meaning of each option used in the previous command;

   (b) Please analyze this captured packet and explain it to me as detailed as you can.
3. Write a similar script showing how HTTP works (you need `curl`);
4. Record your HTTP demo session with `ttyrec`.