SSH CLIENT TRICKS AND TIPS

Andrew Denner

Central Iowa Linux User's Group

March 2023

ABOUT ME

- Software Developer by day
- Sleepless diaper changer by night
- Somehow still the president of CIALUG
- Social:
  - Twitter: @adenner
  - Mastadon: https://hachyderm.io/@adenner
- https://denner.co

CLIENT SIDE SSH TRICKS-LEVEL SETTING

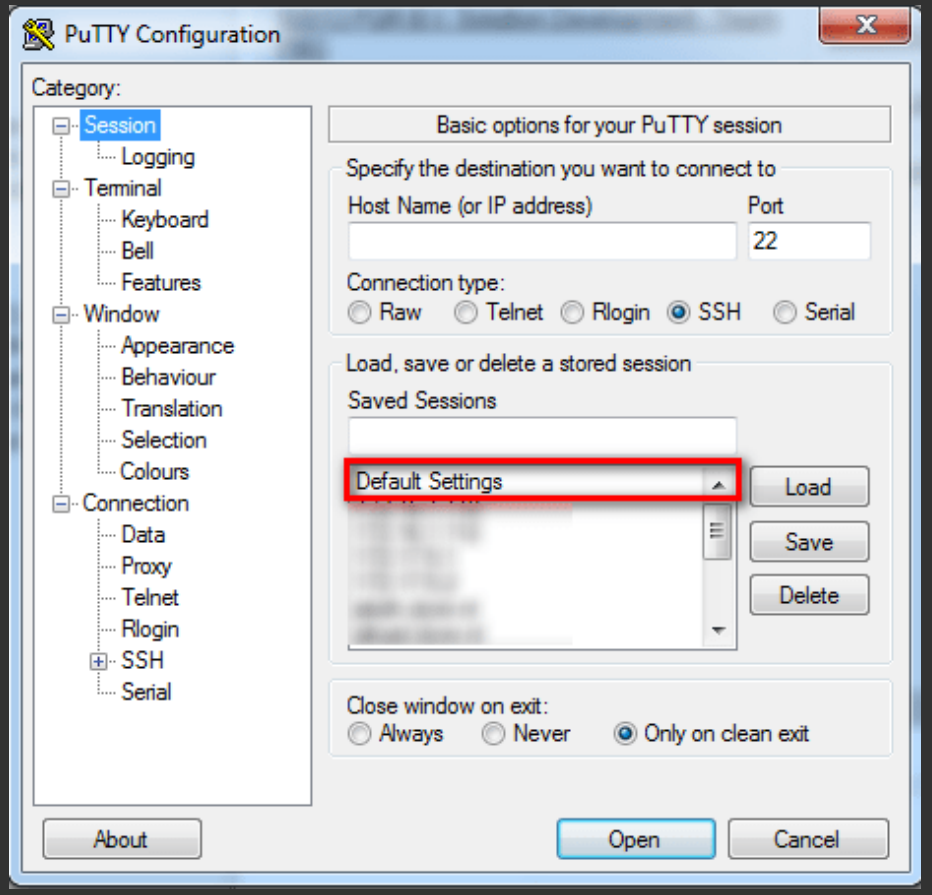
- See last month's talk for server-side stuff (thanks Jared)
- Server Side: Ubuntu Jammy
- Client side: Debian running on a chrome book (showing nothing needs to be fancy)

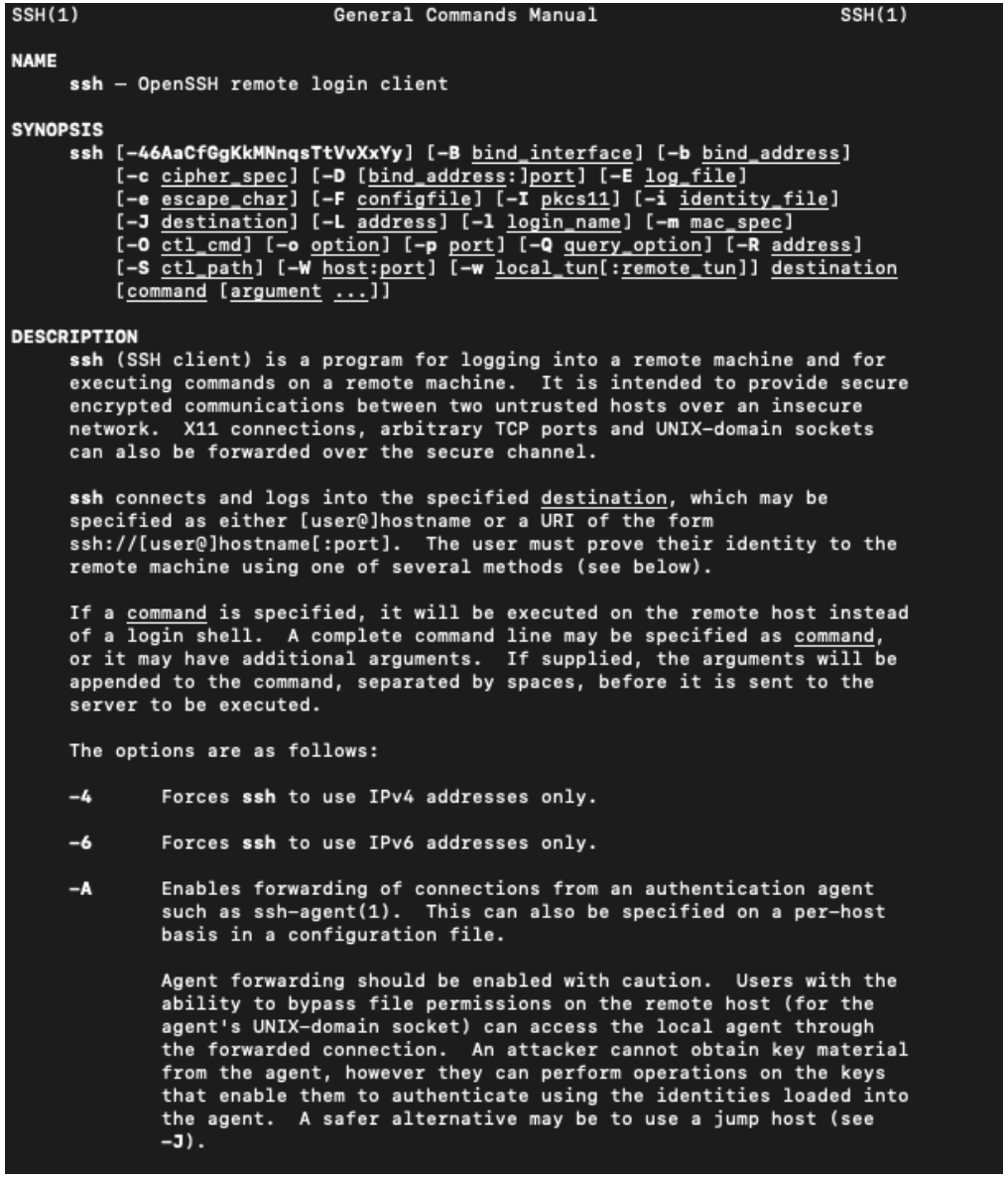
HISTORY

- "Secure Shell Protocol"
- Before was telnet and rsh and rlogin (don't talk about kerb telnet)
- SSH 1995 Tatu Ylönen Helsinki University of Technology in Finland. University network was victim of password sniffing attack
- Version 2 "Secsh" in 2006 Uses Diffie–Hellman key exchange and multiple sessions over one connection

HOW DO I GET IT?

- May be already installed?
- sudo apt install openssh-client
- Windows now has in shell/powershell
- Historically putty was a windows option? (not really needed now)





SSH(1) General Commands Manual SSH(1)

NAME

ssh — OpenSSH remote login client

SYNOPSIS

ssh [**-46AaCfGgKkMNnqsTtVvXxYy**] [**-B** *bind_interface*] [**-b** *bind_address*]
[**-c** *cipher_spec*] [**-D** [*bind_address*:]*port*] [**-E** *log_file*]
[**-e** *escape_char*] [**-F** *configfile*] [**-I** *pkcs11*] [**-i** *identity_file*]
[**-J** *destination*] [**-L** *address*] [**-l** *login_name*] [**-m** *mac_spec*]
[**-O** *ctl_cmd*] [**-o** *option*] [**-p** *port*] [**-Q** *query_option*] [**-R** *address*]
[**-S** *ctl_path*] [**-W** *host*:*port*] [**-w** *local_tun*[:*remote_tun*]] *destination*
[*command* [*argument* ...]]

DESCRIPTION

ssh (SSH client) is a program for logging into a remote machine and for executing commands on a remote machine. It is intended to provide secure encrypted communications between two untrusted hosts over an insecure network. X11 connections, arbitrary TCP ports and UNIX-domain sockets can also be forwarded over the secure channel.

ssh connects and logs into the specified *destination*, which may be specified as either [user@]hostname or a URI of the form ssh://[user@]hostname[:port]. The user must prove their identity to the remote machine using one of several methods (see below).

If a *command* is specified, it will be executed on the remote host instead of a login shell. A complete command line may be specified as *command*, or it may have additional arguments. If supplied, the arguments will be appended to the command, separated by spaces, before it is sent to the server to be executed.

The options are as follows:

-4 Forces **ssh** to use IPv4 addresses only.

-6 Forces **ssh** to use IPv6 addresses only.

-A Enables forwarding of connections from an authentication agent such as ssh-agent(1). This can also be specified on a per-host basis in a configuration file.

Agent forwarding should be enabled with caution. Users with the ability to bypass file permissions on the remote host (for the agent's UNIX-domain socket) can access the local agent through the forwarded connection. An attacker cannot obtain key material from the agent, however they can perform operations on the keys that enable them to authenticate using the identities loaded into the agent. A safer alternative may be to use a jump host (see **-J**).

MAN SSH

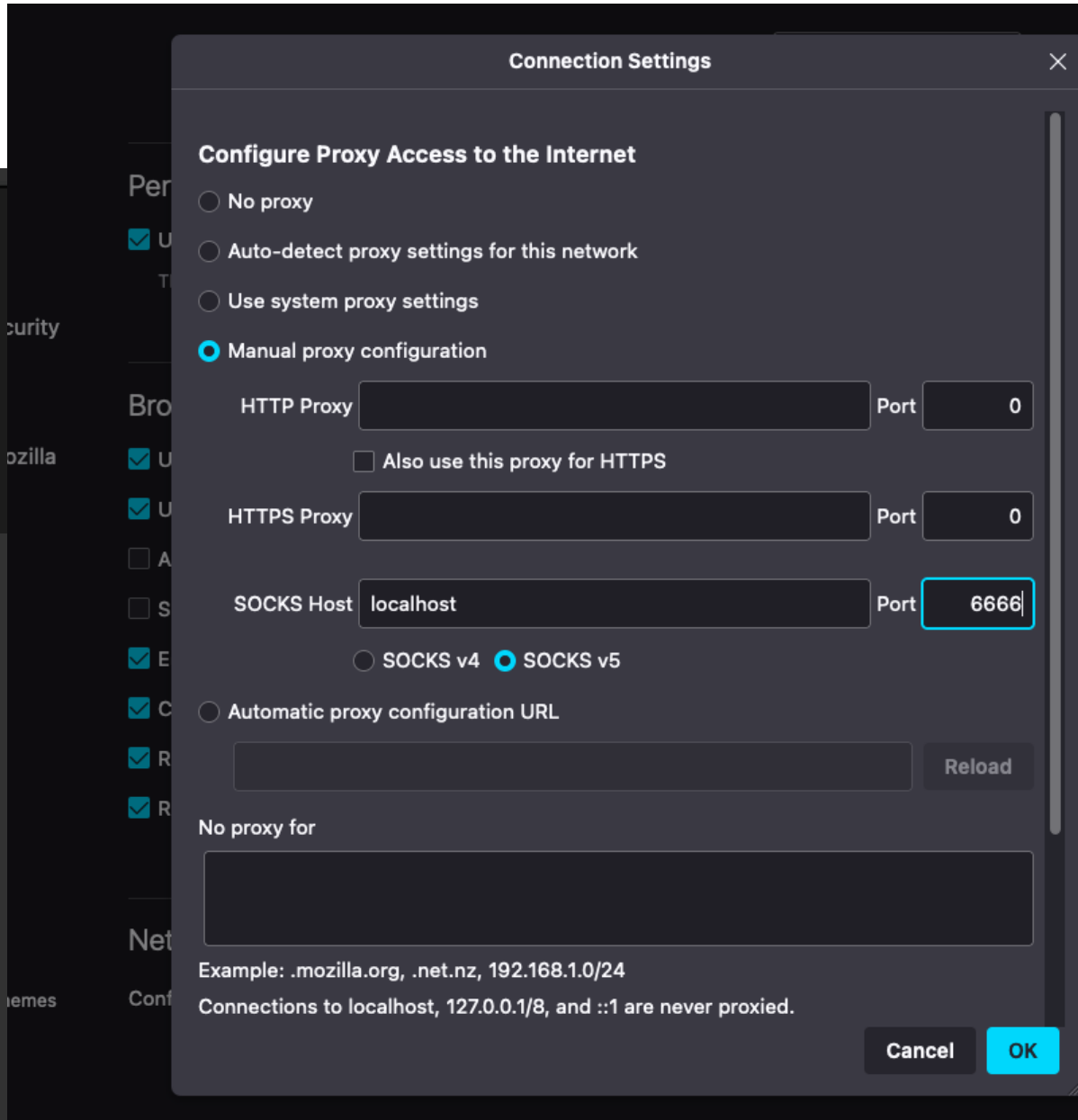
ANATOMY OF THE COMMAND

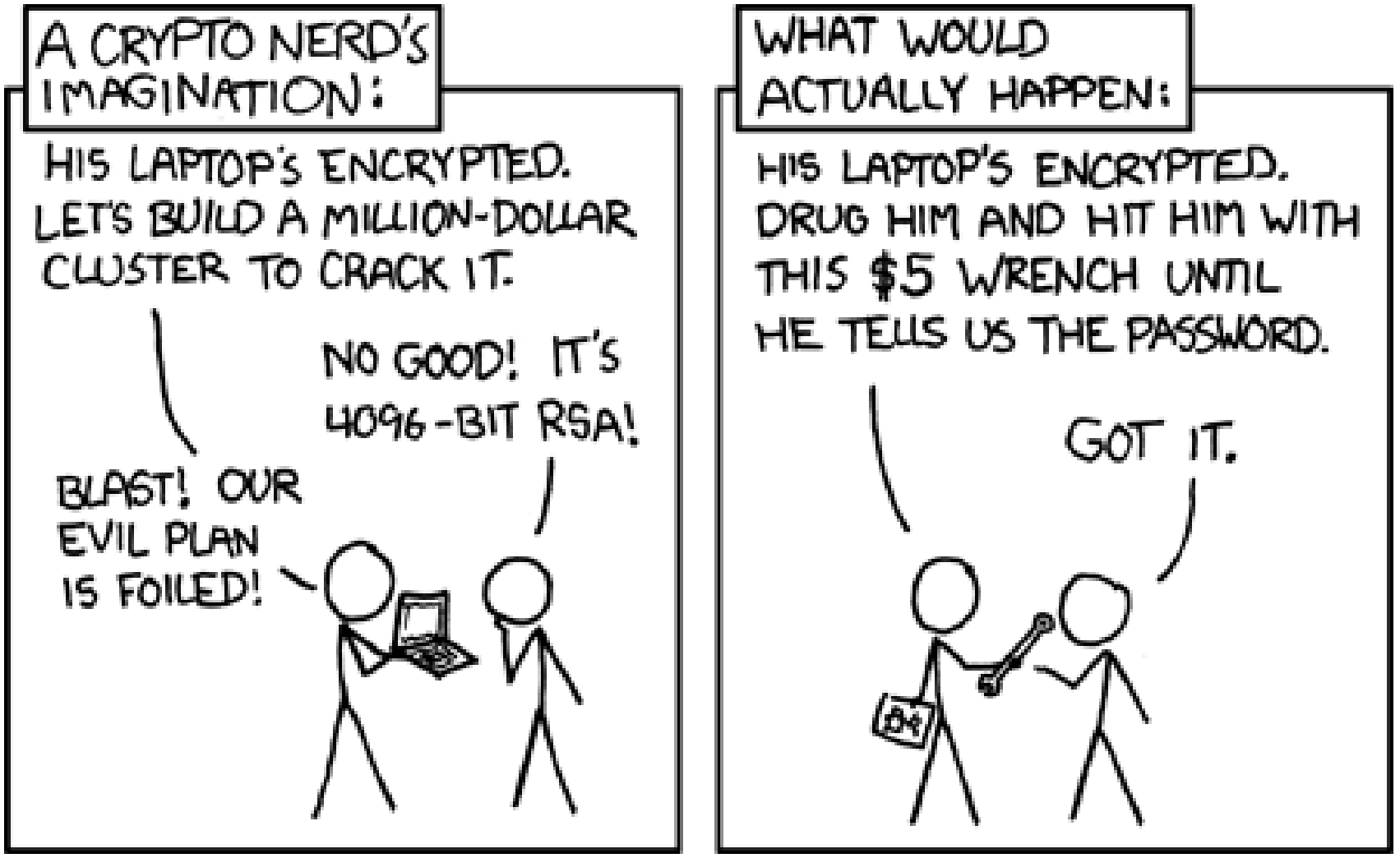
- localhost:~$ ssh -v -4 –X –D 6666 -L 9999:127.0.0.1:80 -p 22 -C adenner@remoteserver whoami
  - -v verbose
  - -4 -6 use ipv4/6
  - -X x11 forwarding –Y trusted x11 forwarding
  - -D 6666 port forwarding (dynamic application level port forwarding) (socks)
  - -L 9999:127.0.0.1:80 port forward from remote localhost:80 to port 9999
  - -p port (default of 22)
  - -C compression
  - User (default to current user)
  - RemoteServer (dns or ip name of server to connect to)
  - Remote command to run

TRICK 1: SOCKS PROXY

```
[adenner@Andrews-Mini ~ % ssh -D 6666 adenner@10.0.0.10
[adenner@10.0.0.10's password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-58-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sun Mar 12 08:41:59 PM UTC 2023
```

```
localhost:~$ proxychains rdesktop $RemoteWindowsServer
```

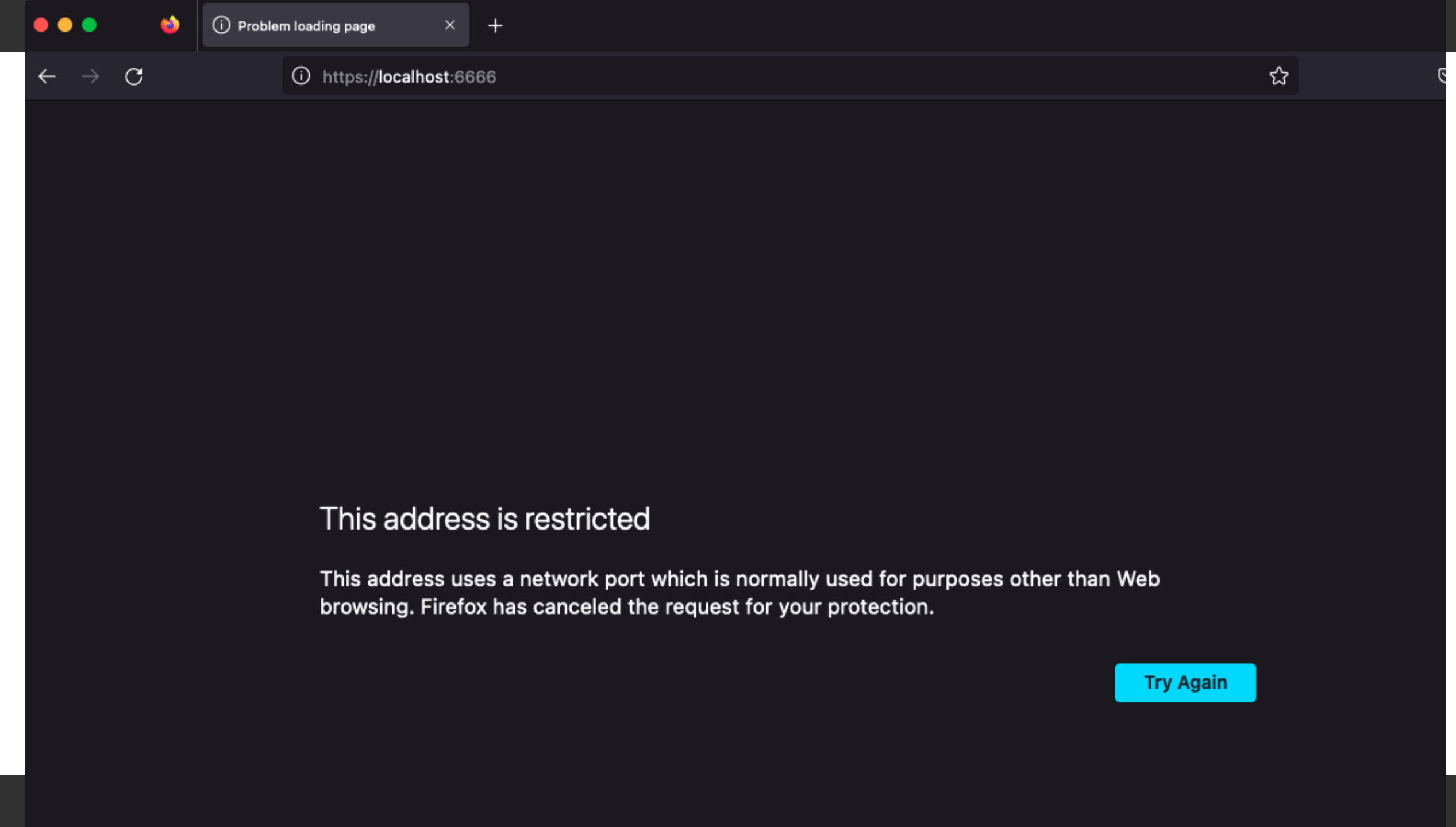


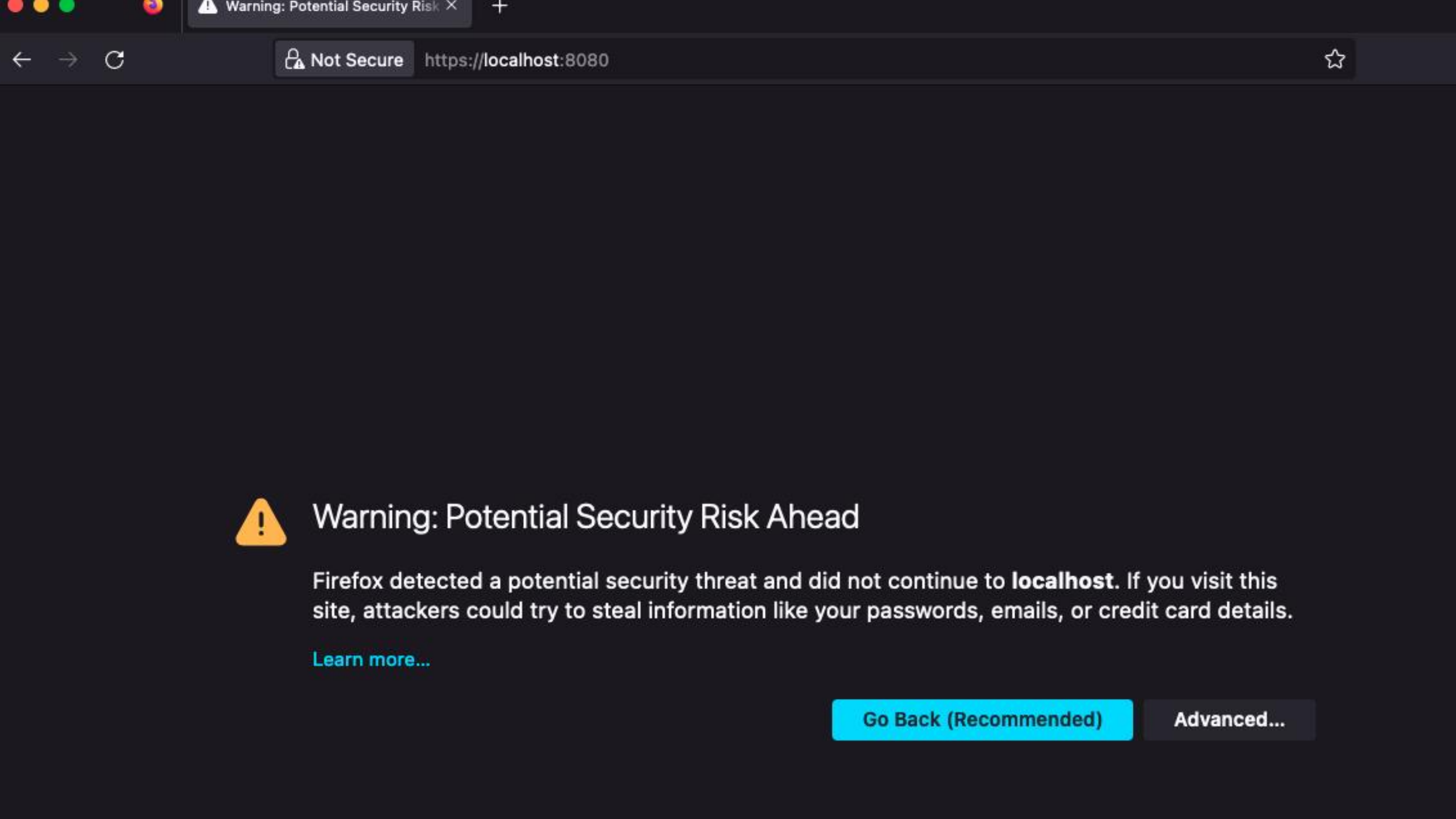


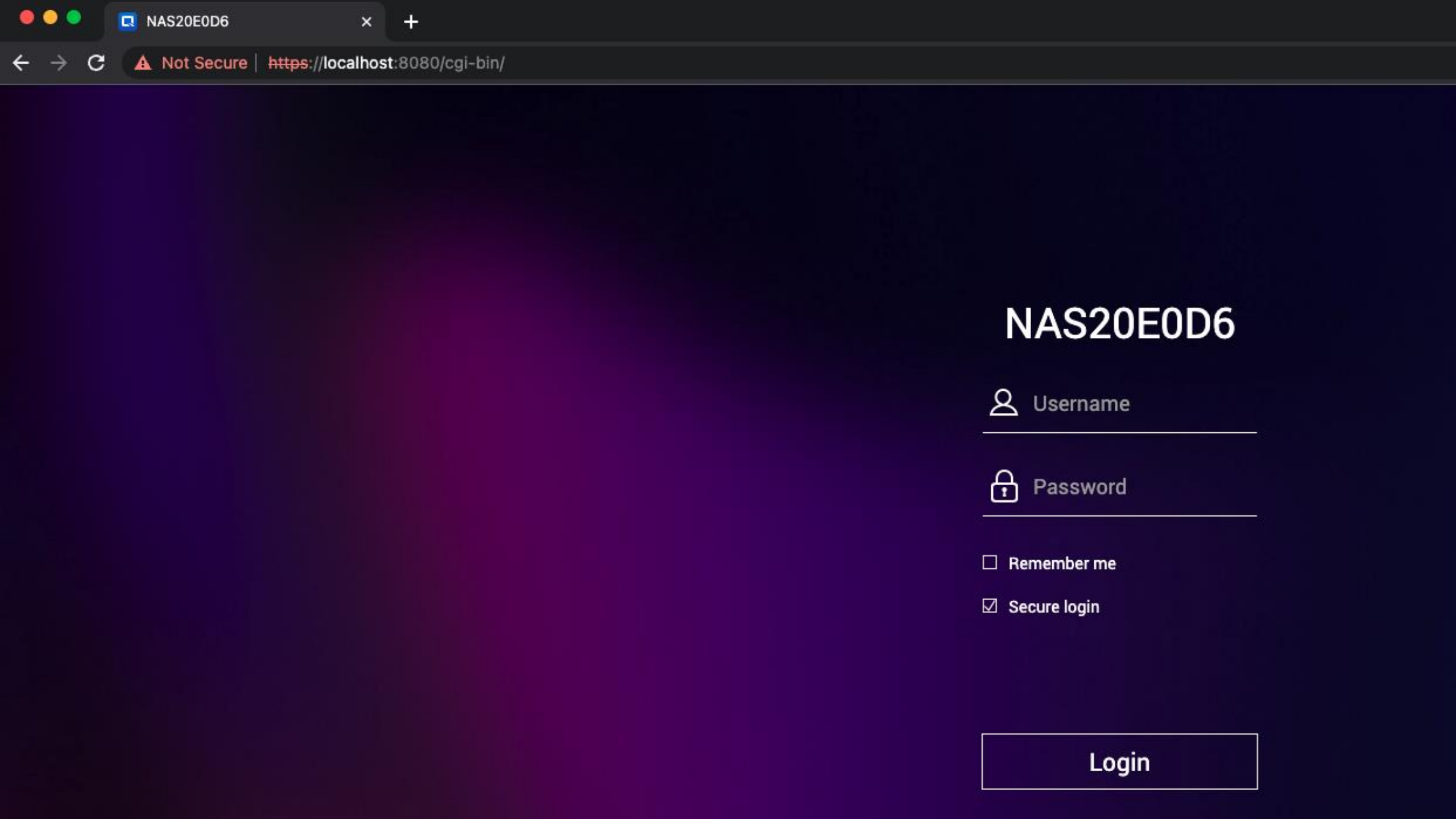
https://xkcd.com/538/

TRICK2: SSH TUNNEL

```
[adenner@Andrews-Mini ~ % ssh -L 6666:10.0.0.8:443 10.0.0.10
[adenner@10.0.0.10's password:
 Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-58-generic x86_64)

  * Documentation:  https://help.ubuntu.com
  * Management:     https://landscape.canonical.com
  * Support:        https://ubuntu.com/advantage

   System information as of Sun Mar 12 08:58:23 PM UTC 2023

   System load:                    0.0478515625
   Usage of /home:                 0.0% of 1.79TB
   Memory usage:                   7%
   Swap usage:                     0%
   Temperature:                    40.0 C
   Processes:                      225
```


Problem loading page
https://localhost:6666
This address is restricted
This address uses a network port which is normally used for purposes other than Web browsing. Firefox has canceled the request for your protection.
Try Again


Warning: Potential Security Risk
Not Secure
https://localhost:8080
Warning: Potential Security Risk Ahead
Firefox detected a potential security threat and did not continue to localhost. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.
Learn more...
Go Back (Recommended)
Advanced...


NAS20E0D6
Not Secure | https://localhost:8080/cgi-bin/
NAS20E0D6
Username
Password
Remember me
Secure login
Login

TRICK 2.5: REVERSE TUNNEL

```
localhost:~$ ssh  -L 0.0.0.0:9999:10.10.10.10:80 user@remoteserver
```

```
localhost:~$ ssh -v -R 0.0.0.0:1999 192.168.1.100 user@remoteserver
```

TRICK 3: COPY YOUR SSH KEY

```
adenner@Andrews-Mini ~ % ssh-copy-id 10.0.0.10
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/Users/adenner/.ssh/id_ed25519.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
adenner@10.0.0.10's password:

Number of key(s) added:        1

Now try logging into the machine, with:   "ssh '10.0.0.10'"
and check to make sure that only the key(s) you wanted were added.

adenner@Andrews-Mini ~ %
```

ASIDE… GENERATE A KEY

```
adenner@Andrews-Mini ~ % ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (/Users/adenner/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /Users/adenner/.ssh/id_ed25519
Your public key has been saved in /Users/adenner/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:CgoiBUWgZJaNIByt1WYU5sbo/7z4GAaLajM28qLjPkw adenner@Andrews-Mini
The key's randomart image is:
+--[ED25519 256]--+
|BOO o+.          |
|*= +=+           |
|. +.o+           |
| o. .            |
|+  o.   S        |
|oE..+. .         |
|o... +.          |
|=O  . *          |
|X**  o.=.        |
+----[SHA256]-----+
adenner@Andrews-Mini ~ %
```

WHY ED25519?

- New(ish) solution using Edwards-Curve Digital Signature Algorithm (EdDSA)
- Faster to generate and verify
- Mathematically more secure
- Collision Resilience
- Smaller keys
- Not messed with like P-256
- NIST approved (draft added to Special publication 800-186)

TRICK 4: RUN REMOTE COMMAND

```
[adenner@Andrews-Mini ~ % ssh 10.0.0.10 tracepath iastate.edu
 1?: [LOCALHOST]                      pmtu 1500
 1:  Linksys00589                                          3.720ms
 1:  Linksys00589                                          3.587ms
 2:  desm-20-25-126.dialup.netins.net                      5.803ms
 3:  ins-wb1-gi-7-8-42355.desm.netins.net                  5.584ms
 4:  ins-wc4-lo0.wdmn.netins.net                           6.641ms asymm 12
 5:  ins-dc3-lo0.desm.netins.net                           6.584ms asymm 11
 6:  ins-dc2-et-0-0-1-0.desm.netins.net                    6.550ms asymm 10
 7:  ins-dc5-lo0.desm.desm.netins.net                      6.574ms asymm  9
 8:  167.142.66.65                                         5.623ms
 9:  be5248.rcr21.dsm01.atlas.cogentco.com                 5.585ms
10:  be2640.ccr42.ord01.atlas.cogentco.com                14.516ms
11:  be2124.rcr21.ord04.atlas.cogentco.com                13.640ms
12:  38.32.97.242                                         18.286ms asymm 11
```

TRICK 4.5: DO IT IN BULK (GNU PARALLEL)

```
adenner@k8master:~$ sudo apt install parallel
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libllvm13 libvulkan1 libxcb-randr0 linux-headers-5.15.0-57 linux-headers-5.15.0-57-generic linux-image-5.15.0-57-generic
  linux-modules-5.15.0-57-generic linux-modules-extra-5.15.0-57-generic mesa-vulkan-drivers
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  sysstat
Suggested packages:
  ash csh fish ksh tcsh zsh isag
The following NEW packages will be installed:
  parallel sysstat
0 upgraded, 2 newly installed, 0 to remove and 4 not upgraded.
Need to get 2,434 kB of archives.
After this operation, 4,521 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 sysstat amd64 12.5.2-2ubuntu0.1 [487 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu jammy/universe amd64 parallel all 20210822+ds-2 [1,947 kB]
Fetched 2,434 kB in 1s (4,682 kB/s)
Preconfiguring packages ...
Selecting previously unselected package sysstat.
(Reading database ... 150800 files and directories currently installed.)
Preparing to unpack .../sysstat_12.5.2-2ubuntu0.1_amd64.deb ...
Unpacking sysstat (12.5.2-2ubuntu0.1) ...
Selecting previously unselected package parallel.
Preparing to unpack .../parallel_20210822+ds-2_all.deb ...
Adding 'diversion of /usr/bin/parallel to /usr/bin/parallel.moreutils by parallel'
Adding 'diversion of /usr/share/man/man1/parallel.1.gz to /usr/share/man/man1/parallel.moreutils.1.gz by parallel'
Unpacking parallel (20210822+ds-2) ...
Setting up sysstat (12.5.2-2ubuntu0.1) ...
```

TRICK 4.5: DO IT IN BULK (GNU PARALLEL)

- cat hosts.txt | parallel -I% --max-args 1 ssh root@% apt update
  - Each host to run command on is listed in hosts.txt
- **parallel > commands.txt**
  - **Each line in commands.txt is another command to execute**
    i.e. ssh root@foo apt-get update
    ssh root@bar apt-get update
    etc.

TRICK 5: REMOTE FOLDER COPY

- tar -cvj /datafolder | ssh remoteserver "tar -xj -C /datafolder”
- ssh user@remoteserver "tar -jcf - /path/to/backup" > dir.tar.bz2

- (or just use RSYNC/SCP) see trick 5.5/5.6

TRICK 5.5: USE SCP

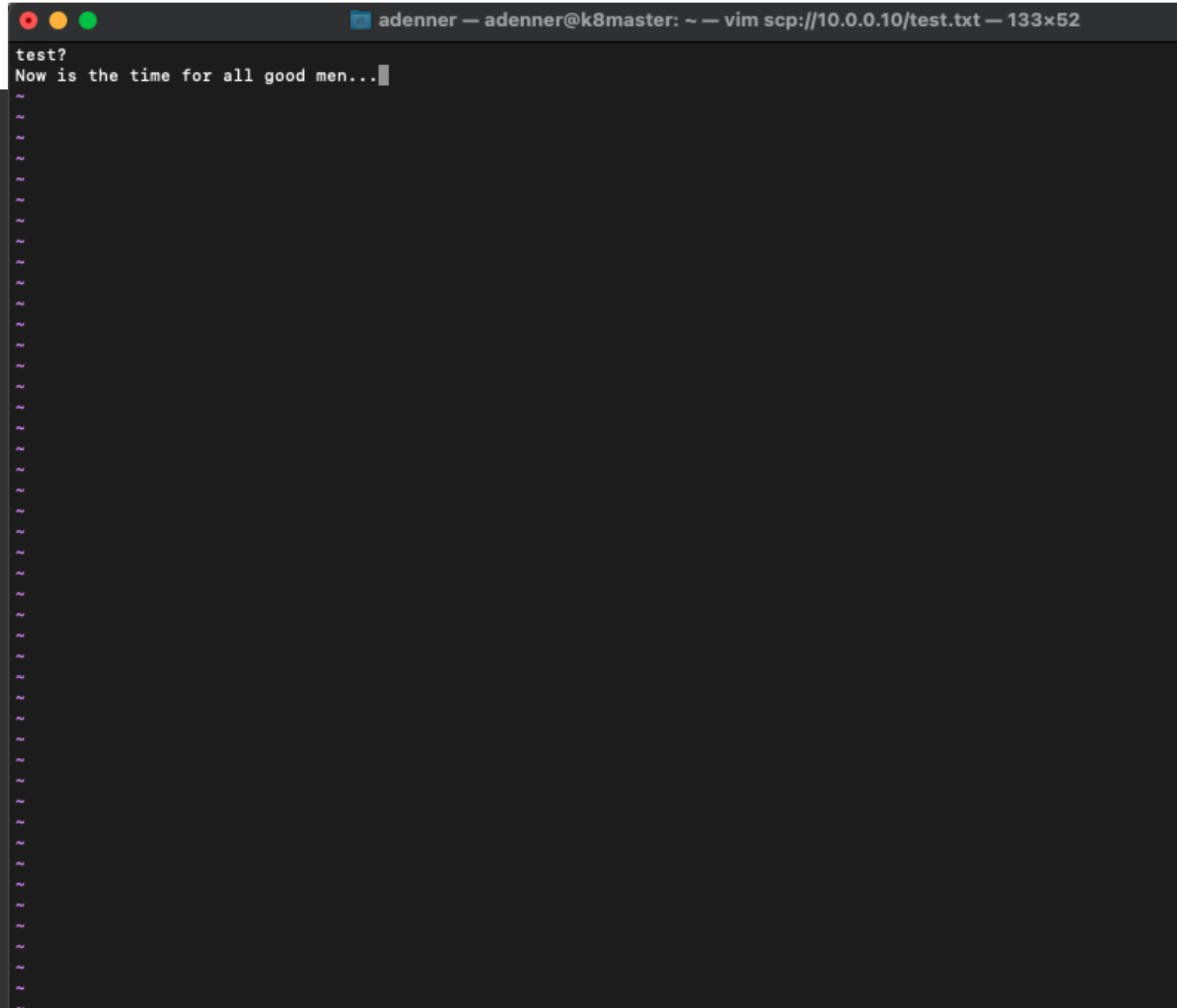
```
SCP(1)                          BSD General Commands Manual                          SCP(1)

NAME
     scp — OpenSSH secure file copy

SYNOPSIS
     scp [-346ABCOpqRrsTv] [-c cipher] [-D sftp_server_path] [-F ssh_config] [-i identity_file] [-J destination] [-l limit]
         [-o ssh_option] [-P port] [-S program] source ... target

DESCRIPTION
     scp copies files between hosts on a network.

     It uses ssh(1) for data transfer, and uses the same authentication and provides the same security as a login session.

     scp will ask for passwords or passphrases if they are needed for authentication.

     The source and target may be specified as a local pathname, a remote host with optional path in the form [user@]host:[path],
     or a URI in the form scp://[user@]host[:port][/path].  Local file names can be made explicit using absolute or relative
     pathnames to avoid scp treating file names containing ':' as host specifiers.

     When copying between two remote hosts, if the URI format is used, a port cannot be specified on the target if the -R option
     is used.

     The options are as follows:

     -3      Copies between two remote hosts are transferred through the local host.  Without this option the data is copied di-
             rectly between the two remote hosts.  Note that, when using the original SCP protocol (the default), this option se-
             lects batch mode for the second host as scp cannot ask for passwords or passphrases for both hosts.  This mode is
             the default.

     -4      Forces scp to use IPv4 addresses only.

     -6      Forces scp to use IPv6 addresses only.
```

TRICK 5.6 USE RSYNC

```
rsync(1)                                    User Commands                                    rsync(1)

NAME
       rsync - a fast, versatile, remote (and local) file-copying tool

SYNOPSIS
       Local:
           rsync [OPTION...] SRC... [DEST]

       Access via remote shell:
           Pull:
               rsync [OPTION...] [USER@]HOST:SRC... [DEST]
           Push:
               rsync [OPTION...] SRC... [USER@]HOST:DEST

       Access via rsync daemon:
           Pull:
               rsync [OPTION...] [USER@]HOST::SRC... [DEST]
               rsync [OPTION...] rsync://[USER@]HOST[:PORT]/SRC... [DEST]
           Push:
               rsync [OPTION...] SRC... [USER@]HOST::DEST
               rsync [OPTION...] SRC... rsync://[USER@]HOST[:PORT]/DEST)

       Usages with just one SRC arg and no DEST arg will list the source files instead of copying.

       The   online   version   of   this   manpage   (that   includes   cross-linking   of   topics)   is   available   at   https://down-
       load.samba.org/pub/rsync/rsync.1.

DESCRIPTION
       Rsync is a fast and extraordinarily versatile file copying tool.  It can copy locally, to/from another host over  any  re-
```

TRICK 6: VIM OVER SCP

```
adenner@Andrews-Mini ~ % vim scp://10.0.0.10/test.txt
```



TRCK 7: SSHFS

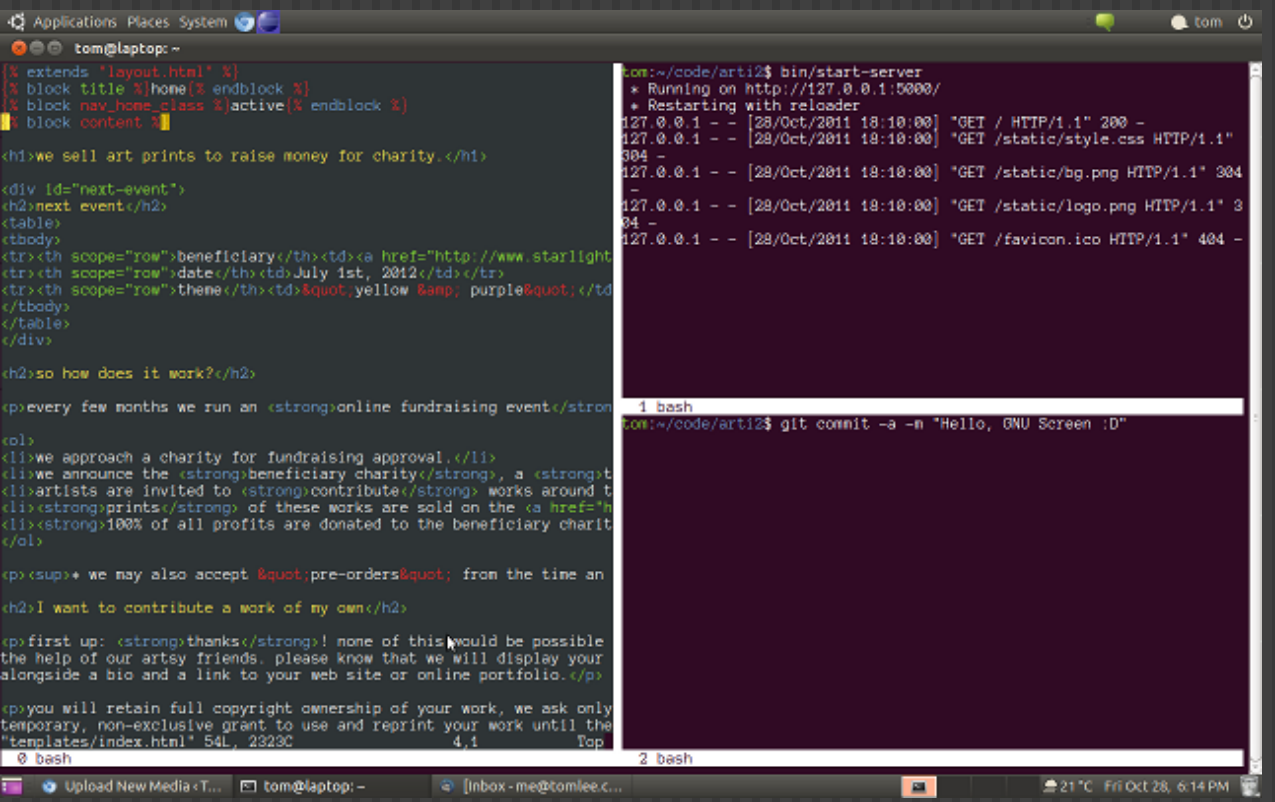
- sshfs user@remoteserver:/media/data ~/data/

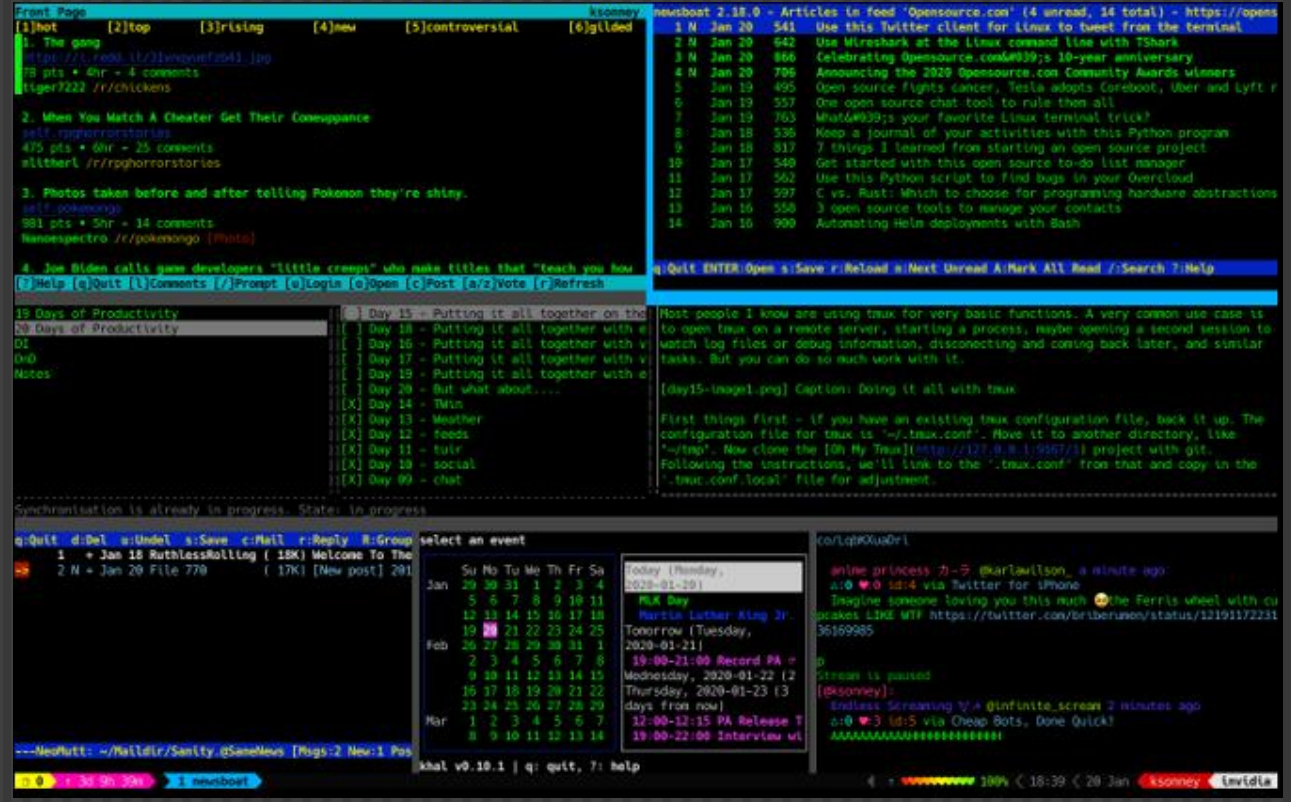
TRICK 8: EXIT ON INTERRUPTION

- ~/.ssh/config
  - ServerAliveInterval 5
  - ServerAliveCountMax 1

TRICK 9: ESCAPE SEQUENCES

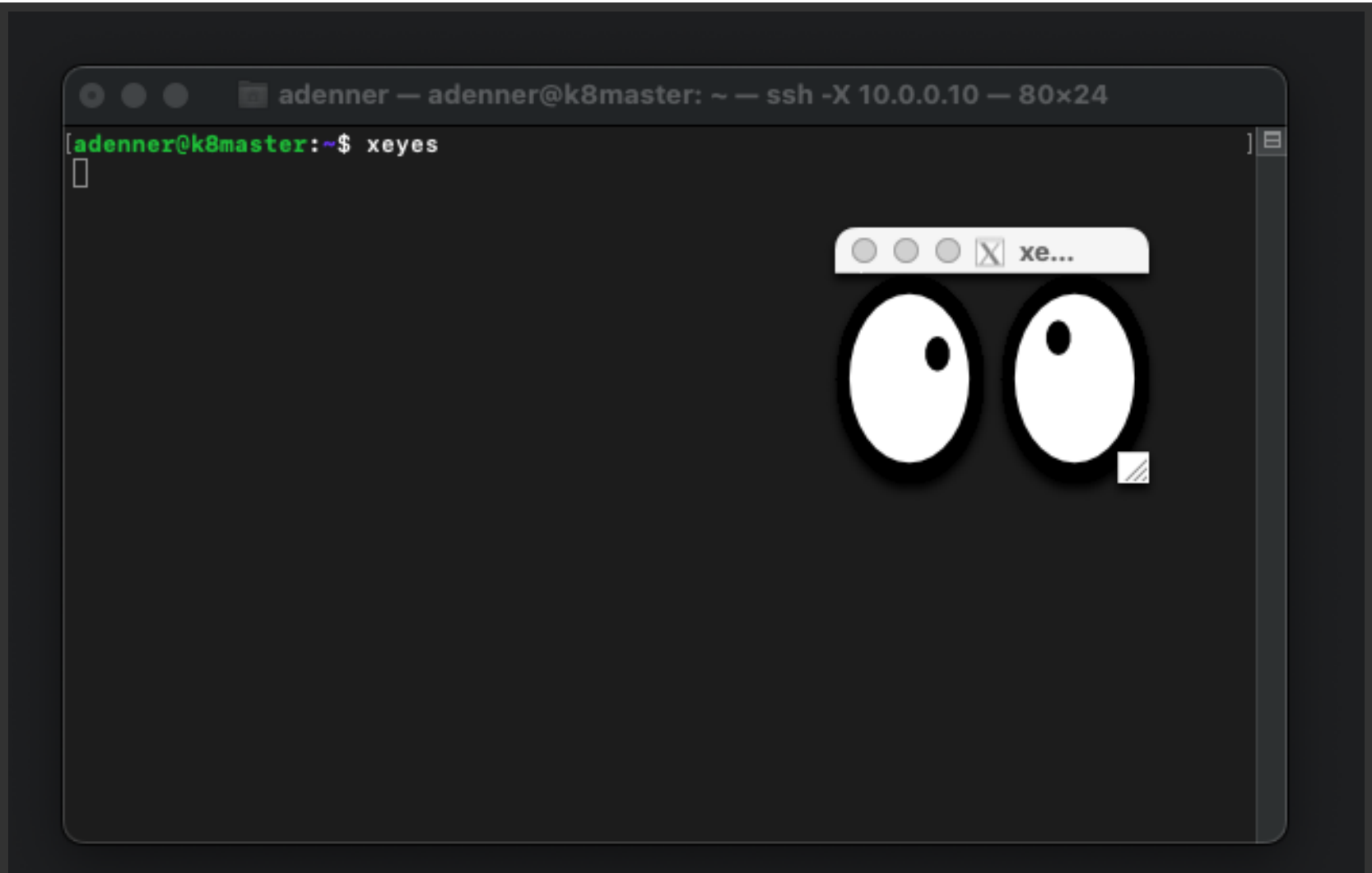
```
adenner@k8master:~$ ~?
Supported escape sequences:
 ~.    - terminate connection (and any multiplexed sessions)
 ~B    - send a BREAK to the remote system
 ~C    - open a command line
 ~R    - request rekey
 ~V/v - decrease/increase verbosity (LogLevel)
 ~^Z   - suspend ssh
 ~#    - list forwarded connections
 ~&    - background ssh (when waiting for connections to terminate)
 ~?    - this message
 ~~    - send the escape character by typing it twice
(Note that escapes are only recognized immediately after newline.)
```



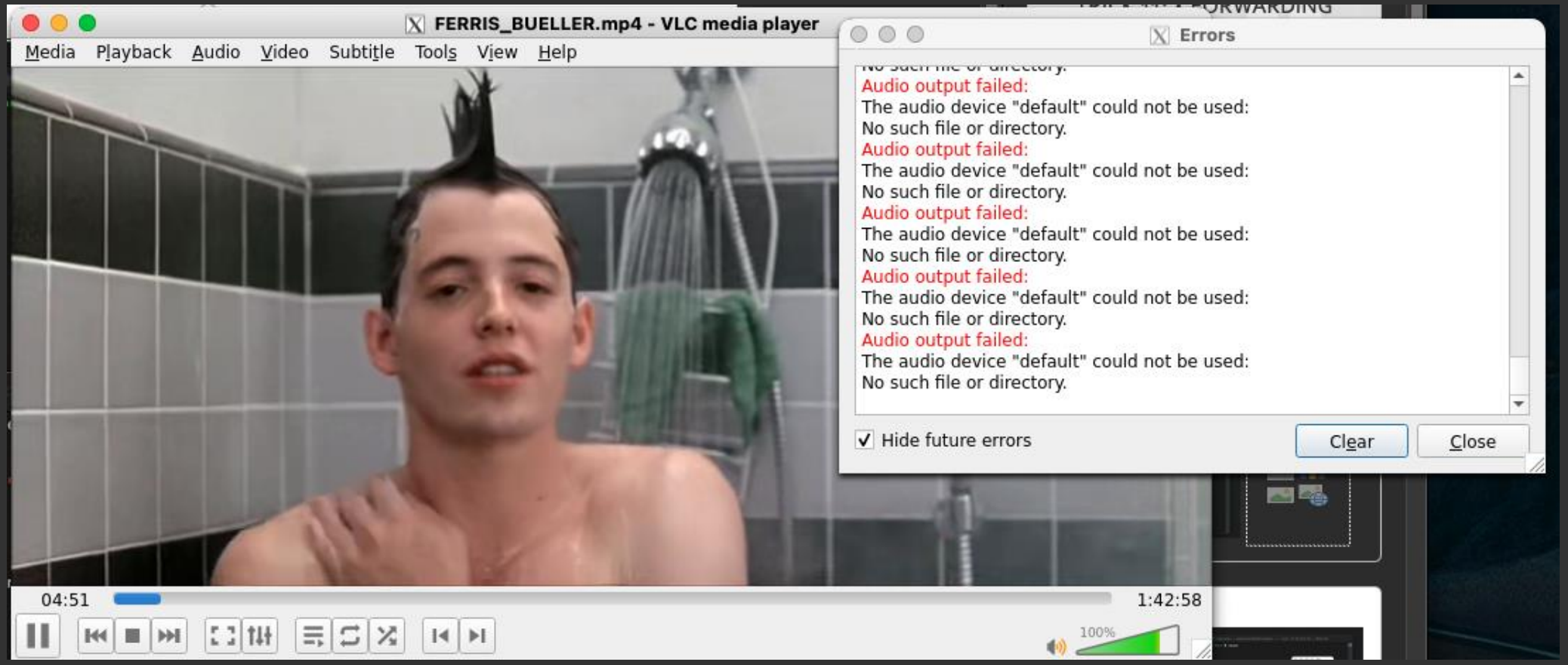


TRICK 10: TMUX OR SCREEN

TRICK 11: X FORWARDING



NOT PERFECT…


FERRIS_BUELLER.mp4 - VLC media player
Media Playback Audio Video Subtitle Tools View Help
04:51
1:42:58
100%
Errors
Audio output failed:
The audio device "default" could not be used:
No such file or directory.
Audio output failed:
The audio device "default" could not be used:
No such file or directory.
Audio output failed:
The audio device "default" could not be used:
No such file or directory.
Audio output failed:
The audio device "default" could not be used:
No such file or directory.
Audio output failed:
The audio device "default" could not be used:
No such file or directory.
Hide future errors
Clear
Close

WHAT DID I MISS?

Let the heckling begin…