Network Monitoring, Management and Automation

Linux Basics

npNOG 5

Dec 8 - 12, 2019

Our chosen platform

- Ubuntu Linux
  - LTS = Long Term Support
  - no GUI, we administer using ssh
  - Ubuntu is Debian underneath
- There are other platforms you could use:
  - CentOS / RedHat, FreeBSD, ...
- This isn't a UNIX admin course, but some knowledge is necessary:
  - Worksheets are mostly step-by-step
  - Please help each other or ask us for help

You need to be able to...

- Be `root` when necessary
  $ sudo <cmd>
- Install packages
  $ sudo apt-get install <pkg>
- Edit files
  $ sudo nano /etc/mailname
  $ sudo vi /etc/mailname
- Check for the process "apache"
  $ ps auxwww | grep apache
- Start/Stop/Status of services
  $ systemctl [start|stop|status] <NAME>

nano editor

- Ctrl-x y “n” quit without saving
- Ctrl-x y “y” to quit and save
- Ctrl-g for help
- Ctrl-w for searching
- Cursors work as you expect

vi editor

- The default editor for all UNIX and Linux distributions
- Can be difficult to use
- If you know it and prefer to use vi please do
- We provide a PDF reference in the materials

Other tools

- Terminate foreground program:
  - ctrl-c
- Browse the filesystem:
  - cd /etc
  - ls
  - ls -l
- Delete and rename files
  - mv file file.bak
  - rm file.bak

Viewing files

Sometimes files are viewed through a pager program (“more”, “less”, “cat”). Example:

- man sudo
- Space bar for next page
- “b” to go backwards
- “/” and a pattern (/text) to search
- “n” to find next match
- “N” to find previous match
- “q” to quit

Using ssh

Configuring and using ssh incorrectly will guarantee a security compromise…

The wrong way:

- Using simple passwords for users
- Allowing root to login with a password
- In reality – allowing any login with a password

The right way:

- Disable all password access
- Disable root access with password
- Some disable root access completely

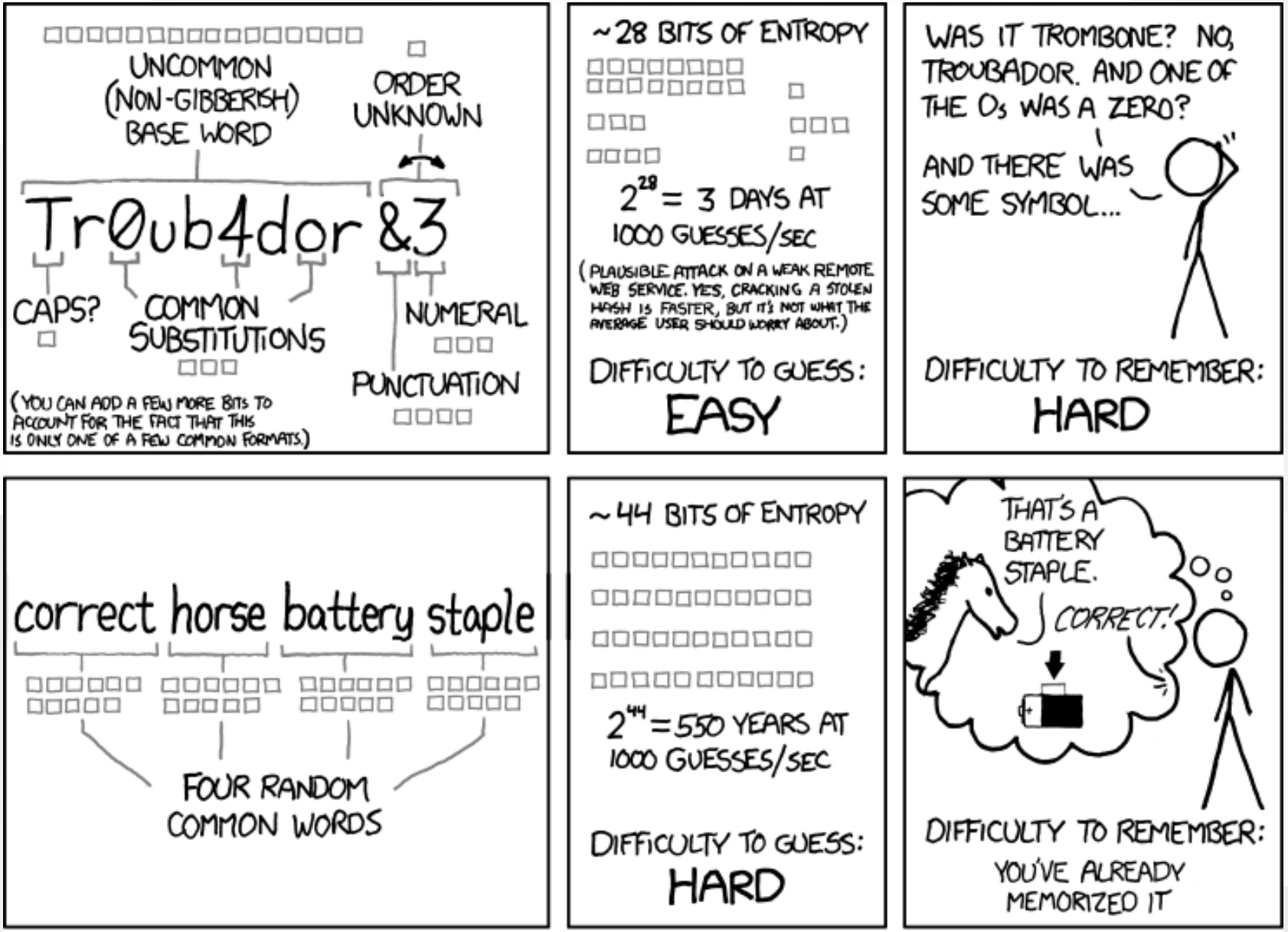
Using ssh: our way

For class we will compromise.

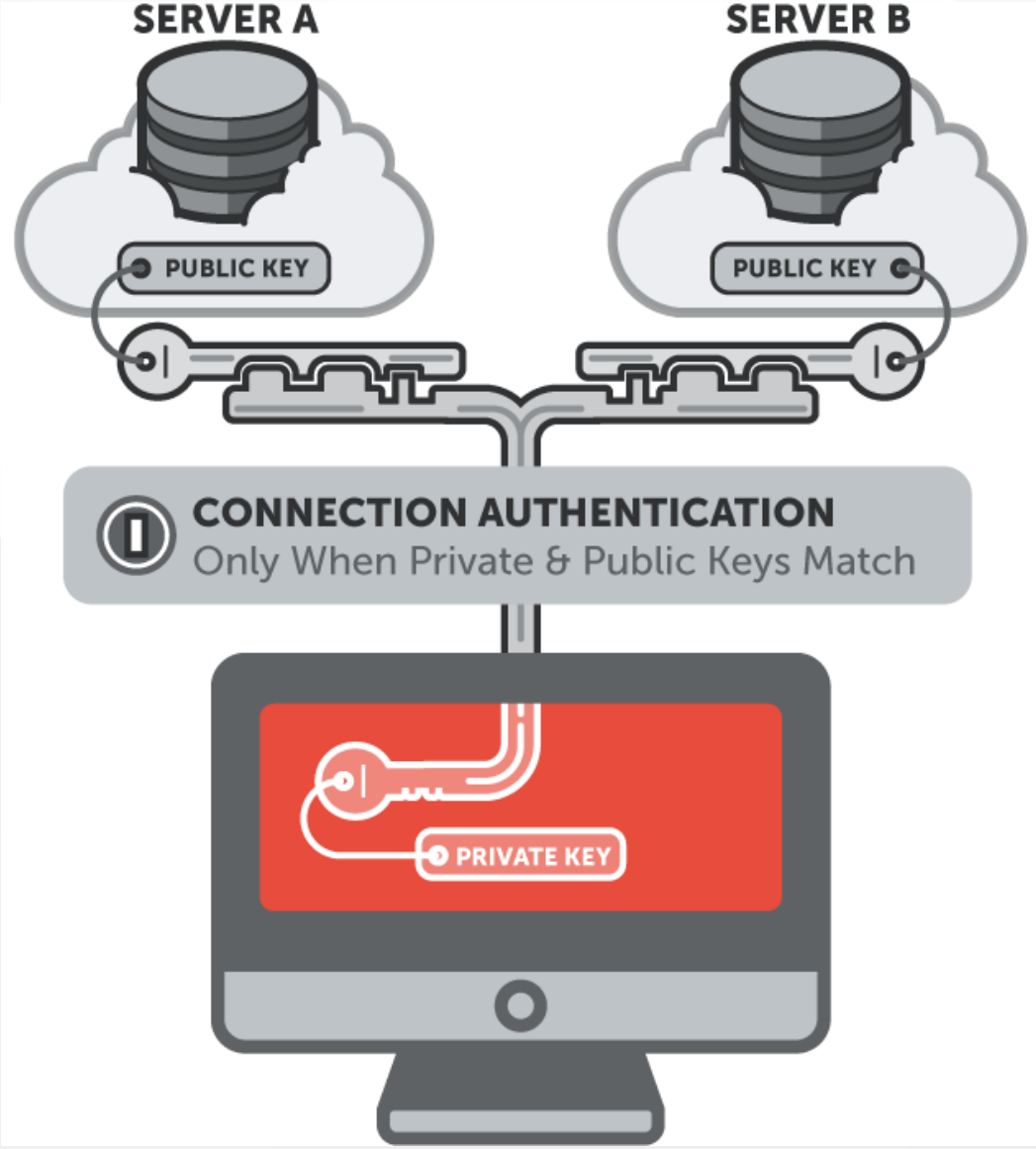
Our way:
– Allow user login with improved passwords
– Allow root login with ssh keys only

Understanding password strength, see next slide…*

* https://xkcd.com/936/


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS:
EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER:
HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS:
HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER:
YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

No Passwords are better



Improve password for `lab` user

Method 1 (moderately strong)

- 8 characters or more
- Not a word in any language
- A mix of numbers, upper and lower case
- Include some punctuation characters

Method 2 (stronger)

- Use four words of 6 characters, or more
- Use unrelated words

Examples (do not use these!)

1. Tr0ub4dor&3
2. CorrectHorseBatteryStaple

Using ssh to connect to your VM

- Login to your virtual machine using ssh
  - On Windows use putty.exe
  - Connect to vmX-gY.lab.workalaya.net as user sysadm
  - We'll do that now…
- Accept Public Key when prompted
- Windows users can download putty from http://www.lab.workalaya.net and connect
- Instructors will now assist everyone to connect

Change `lab` user password

Logged in as user `lab` do:

```
$ passwd
changing password for lab.
(Current) UNIX password:  <enter current password>
Enter new UNIX password: <enter new password>
Retype new UNIX password: <confirm new password>
```

If everything goes well you will see the message:

```
passwd: password updated successfully
```

Finish initial VM configuration

Now we'll do our initial VM configuration, including:

- Software package database update
- nano editor software installation
- Install network time protocol service and update time
- Install mail server and utilities
- Practice using logs
- Practice using man