Mason Competitive Cyber

Linux, Scripting, and Regex

News since last meeting

- Equifax CIO and CSO Retiring
  - Knew about vulnerability in Apache Struts Web Framework
  - Didn’t patch in time

- AWS EC2 billing now by the minute

- Navy to investigate possibility of cyber attack that led to ships crashing

CSAW

- Online
- Guest speaker from Kudu Dynamics going over problems in the Advanced section
  - That’s happening next week

Upcoming CTFs & Events

- BackdoorCTF
  - September 23 6:30pm to September 24, 6:30pm
  - Online

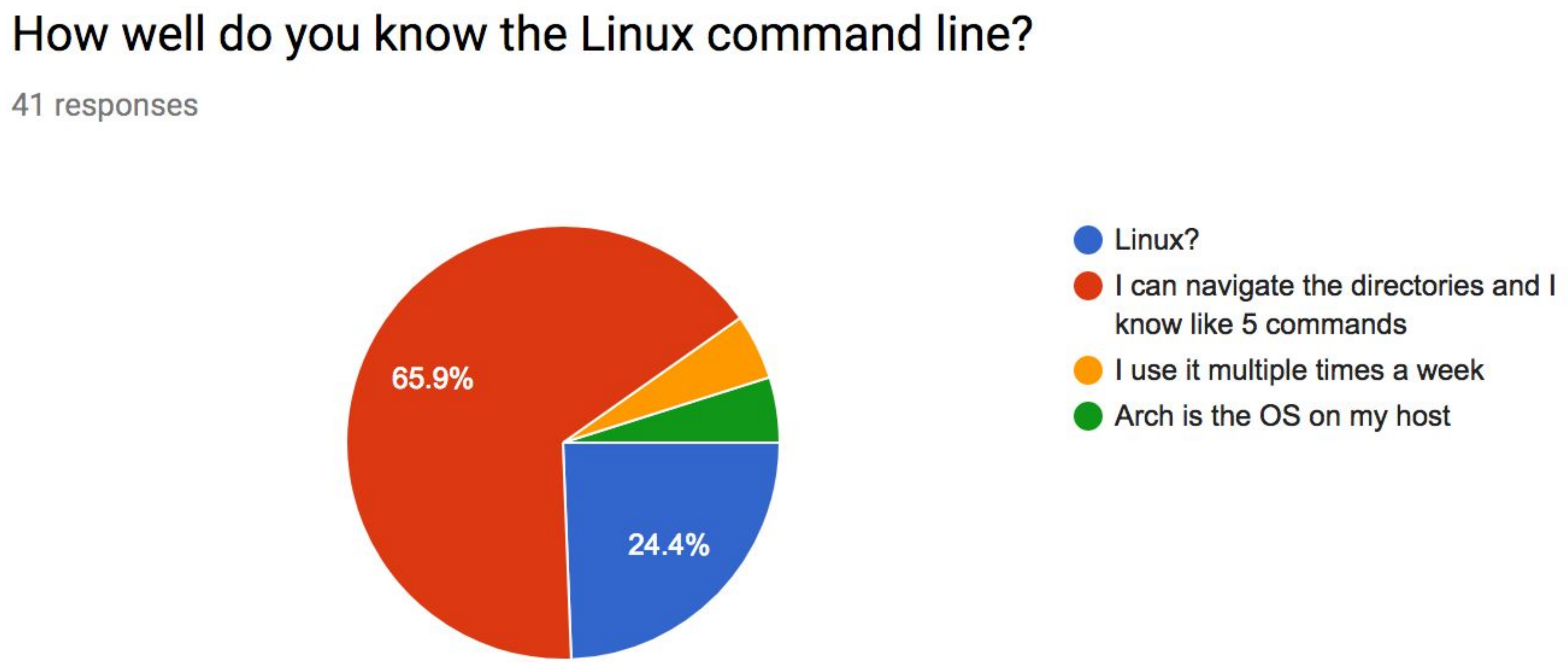
- DefCamp CTF Quals
  - September 30 8am to October 1, 8am
  - Online

- Capital One Wargame
  - October 3rd, 6-9pm
  - In-person 1680 Capital One Dr, McLean, VA
  - Winning individual/team gets an Echo Dot

Today’s Plan

- Linux
  - Commands useful in CTFs
- Scripting
  - Bash & Python
- Regex
  - Regular Expressions
  - Use in scripting & CTFs

Linux



How well do you know the Linux command line?

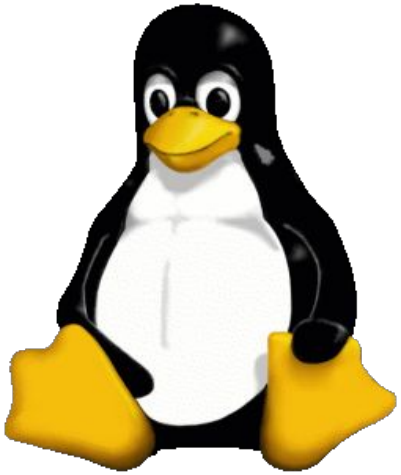
41 responses

- 24.4% → you have some catching up to do

Linux

- Operating System
  - Different distros (distributions)
- More reliant on command line than Windows

- Don’t have Linux?
  - MasonCC Virtual Machine
  - go.gmu.edu/masonccvm
    - Kali
    - SIFT (forensics tools)
    - CTF tools (stegsolve, xortool, etc.)



- linuxjourney.com
  - If you don’t use linux multiple times a week, go here

Linux in CTFs

- Reverse Engineering & pwning problems often use ELFs
  - Executable and Linkable Format
  - ^Doesn’t work on Windows

- file
  - file command gives you file format

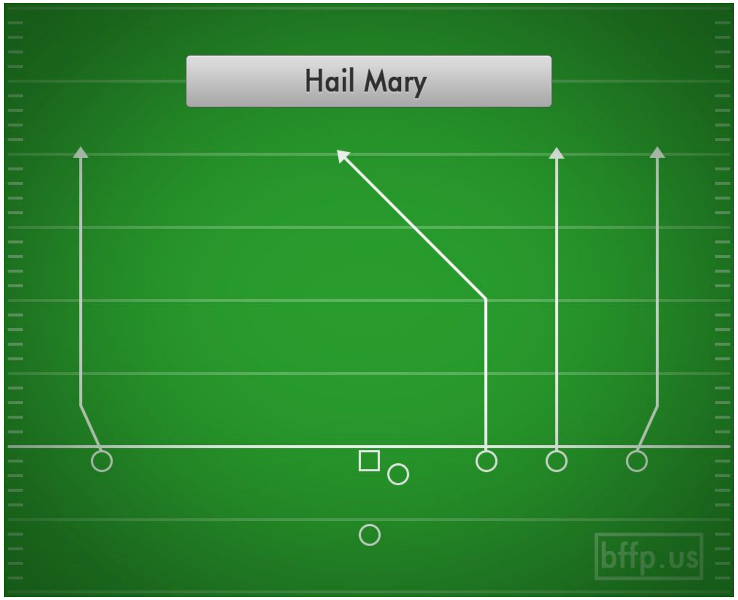
- strings
  - command that outputs printable strings in file
  - Easy RE challenges
  - .pcap
  - tool output

Linux in CTFs

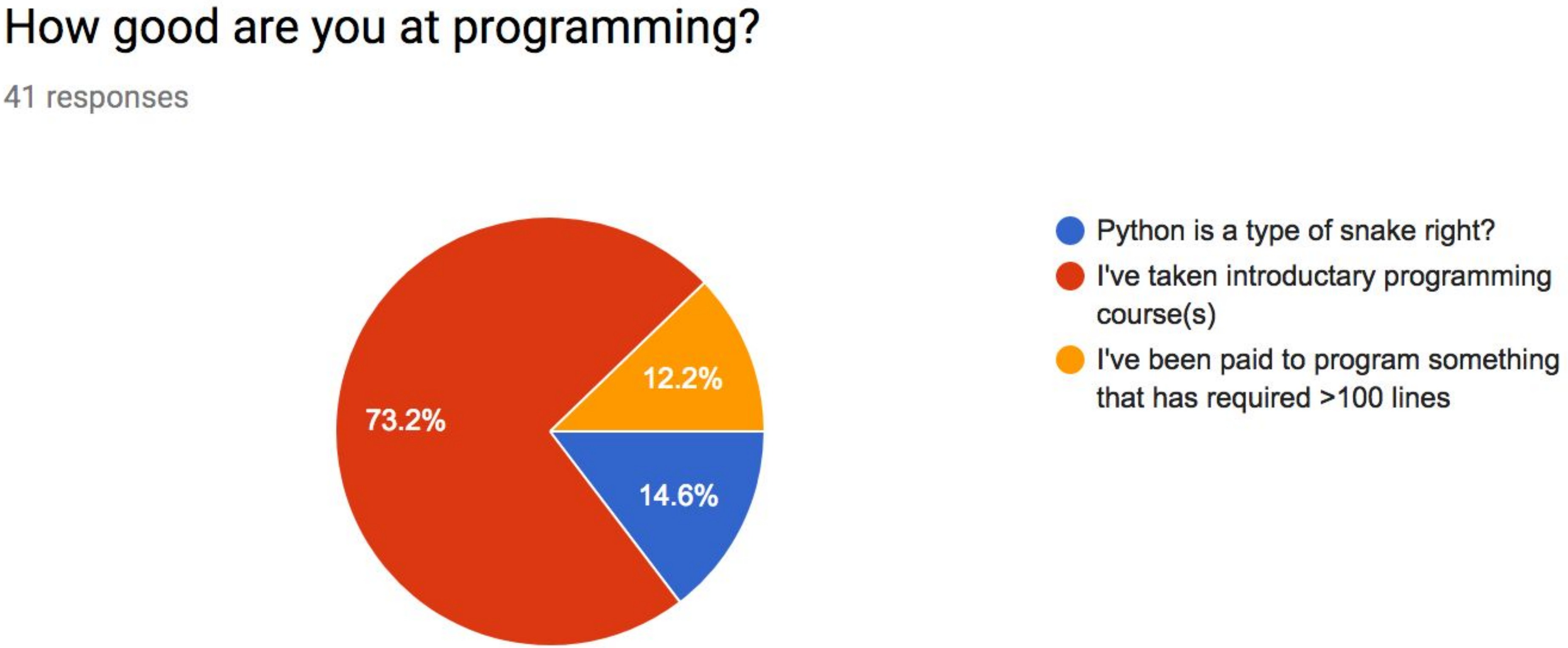
- grep
  - search file(s)
  - “-i” means ignore case

- strings capture.pcap
  - huge dump
  - too much info

- strings capture.pcap | grep -i flag
  - searches for “flag” in strings
  - only works on easy challenges



Scripting

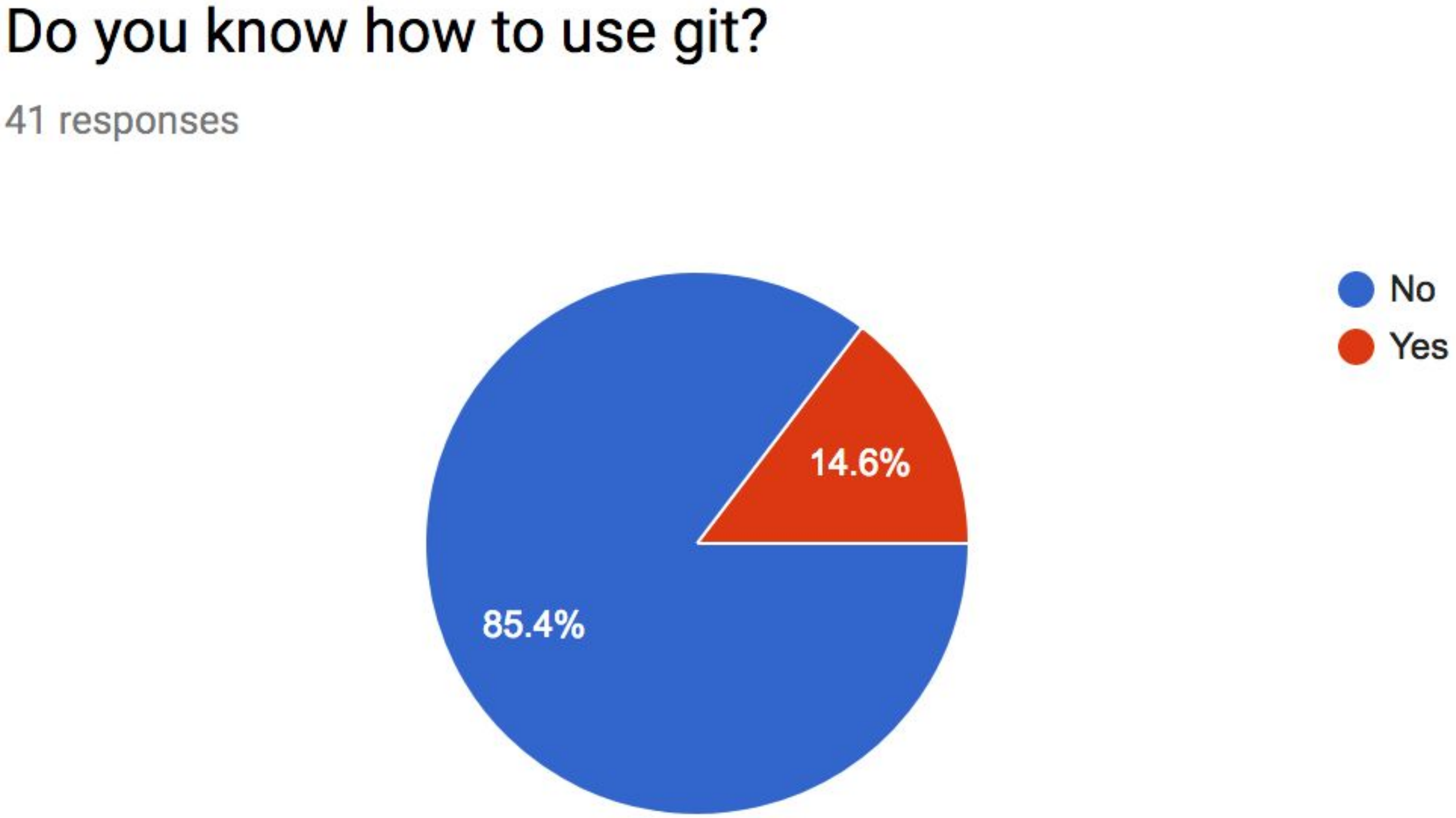


How good are you at programming?

41 responses

- CS112 != proficiency in Python

Scripting



Do you know how to use git?

41 responses

- try.github.io

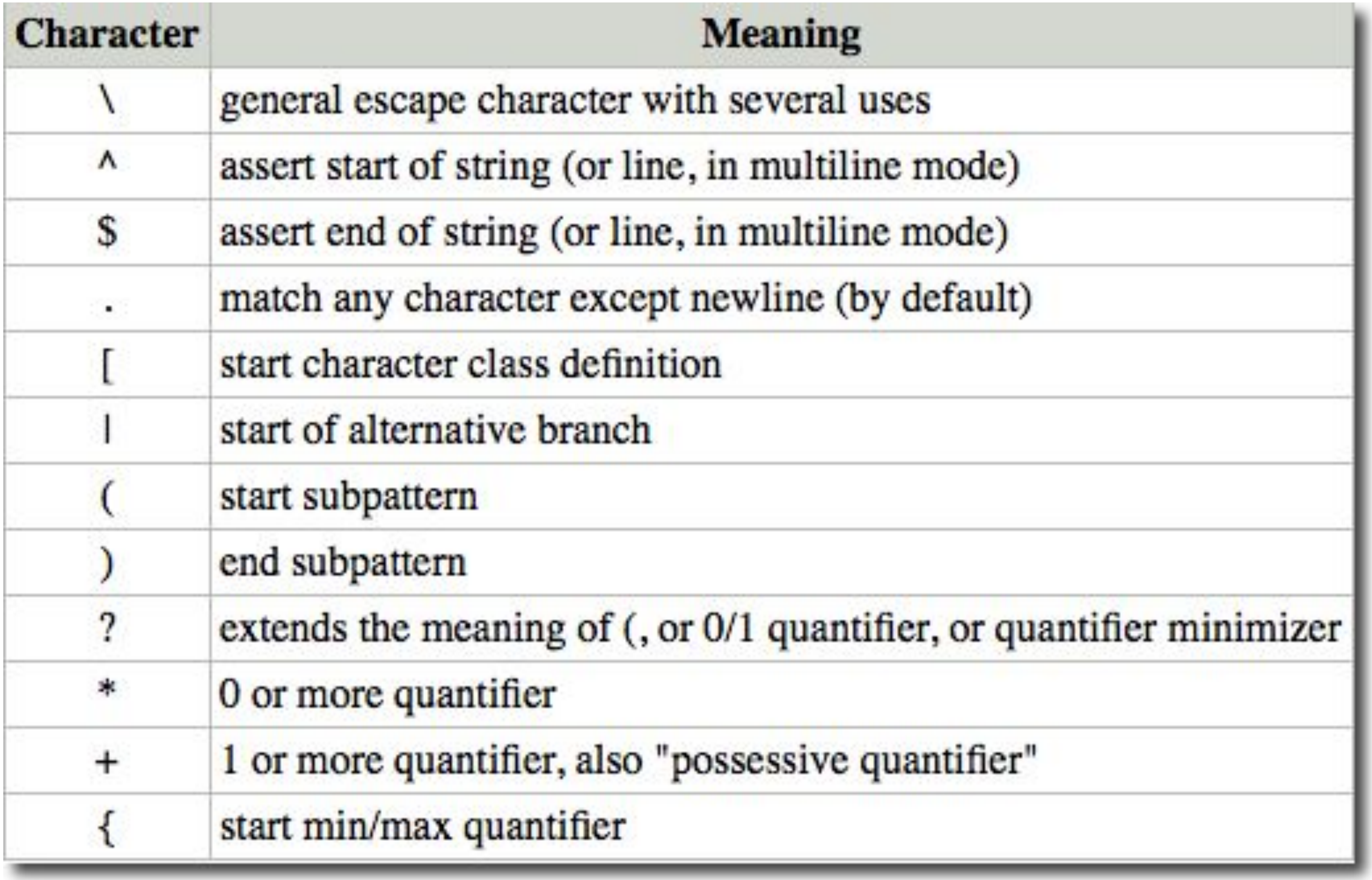
Regex

- Regular Expressions
- Patterns

- regexone.com
  - if you’ve never used regex

- alf.nu/RegexGolf
  - if you’ve used regex before

Regex



Character	Meaning
\	general escape character with several uses
^	assert start of string (or line, in multiline mode)
$	assert end of string (or line, in multiline mode)
.	match any character except newline (by default)
[	start character class definition
|	start of alternative branch
(	start subpattern
)	end subpattern
?	extends the meaning of (, or 0/1 quantifier, or quantifier minimizer
*	0 or more quantifier
+	1 or more quantifier, also "possessive quantifier"
{	start min/max quantifier

Challenges

- linuxjourney.com
  - If you know 0 linux and want to work on that
- overthewire.org/wargames/bandit
  - general linux challenges
- regexone.com
  - beginner regex
- alf.nu/RegexGolf
  - advanced regex
- go.gmu.edu/920
  - challenges involving everything we talk about today

Proud Sponsors

Thank you to these organizations who give us their support:

BATTELLE

It can be done™