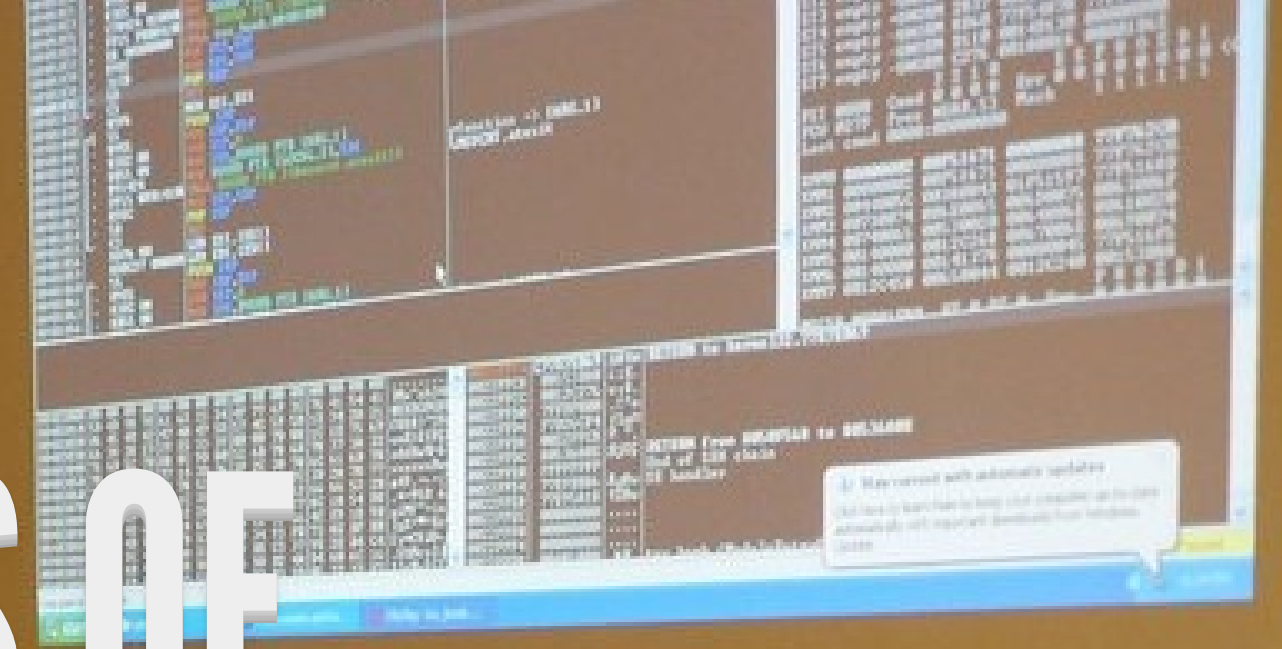


TWO YEARS OF MONTREHACK

Olivier Bilodeau



PLAN

- What
- Why
- How (When, Where, Who)
- Lessons
- Tools and techniques
- What's next?

HI I'M OLIVIER BILODEAU



**YOU MIGHT REMEMBER ME FROM
TALKS SUCH AS "HOW (NOT) TO SUCK
AT CTF" AND BEING DRUNK AT HACKFEST**

\$ WHOAMI

Malware Researcher at ESET

Passionate about infosec and open source

Did [many talks](#), much lulz and luv for the community

Father of two

[@obilodeau](#)

SHAMELESSPLUG

Hacker Jeopardy Saturday at \$something pm

WHAT

Monthly workshop where we work on solving "Capture-the-Flag"* challenges

<http://montrehack.ca>

*: infosec stuff not counter strike

Archives of past challenges on our Website



Archives

By date

- >> [NorthSec 2015 Warm-up Party!](#), 18 May 2015
- >> [Network Forensics BKP Riverside 2015](#), 20 April 2015
- >> [adctf 2014 password-checker](#), 16 March 2015
- >> [Android Forensics CySCA2014](#), 16 February 2015
- >> [Microcorruption initiation](#), 19 January 2015
- >> [Brad Oberberg \(CSAW Finals 2013\)](#), 15 December 2014
- >> [Secure webmail and lost data](#), 17 November 2014
- >> [Web Get \\$SHELL](#), 20 October 2014
- >> [NorthSec Smartcards](#), 15 September 2014
- >> [Social meetup / Rencontre sociale](#), 18 August 2014
- >> [NorthSec Thank You Mr ISP](#), 19 May 2014
- >> [NorthSec 2014 Pre-Party!](#), 21 April 2014
- >> [Boston Key Party Reverse Engineering](#), 17 March 2014
- >> [Hackfest 2013 Web Challenges](#), 17 February 2014

Android, Crackme, Cryptography, Exploit, Forensic,
Hardware, IOS, Linux, Network, Reverse-Engineering, SQL
Injection, Steganography and Web

Covered International and Local CTFs

Advent Calendar CTF, Boston Key Party, CySCA, CSAW,
Hackfest, NorthSec, PlaidCTF, Hack.lu

We feature some of the Web's gems in order to present our challenges

JAVASCRIPT

CRYPTOGRAPHY



NO CHALLENGES THIS MONTH

ONLY BOOZE

**I'LL JUST LEARN TO USE GDB
AND THEN DO THE CHALLENGE**



FLAG:24803472805

BACK IN MY DAY



XSS WAS A FEATURE

Jurassic Park, System Security Interface
Version 4.0.5, Alpha E
Ready...

> access main program

access: PERMISSION DENIED.

> access main security

access: PERMISSION DENIED.

> access main program grid

access: PERMISSION DENIED.....AND.....

YOU DIDN'T SAY THE MAGIC WORD!

YOU DIDN'T SAY THE MAGIC WORD!

YOU DIDN'T SAY THE MAGIC WORD!

YOU DIDN'T SAY THE MAGIC WORD!

YOU DIDN'T SAY THE MAGIC WORD!

YOU DIDN'T SAY THE MAGIC WORD!

YOU DIDN'T SAY THE MAGIC WORD!

YOU DIDN'T SAY THE MAGIC WORD!

YOU DIDN'T SAY THE MAGIC WORD!

YOU DIDN'T SAY THE MAGIC WORD!

YOU DIDN'T SAY THE MAGIC WORD!

HACKFEST



RETALIATION

PERFECT CHALLENGES




**FOR YOUR BLACKHAT / DEFCON
HANGOVER**

SO YOU'RE TELLING ME

**THAT YOU DESIGNED YOUR OWN CRYPTO
SYSTEM?**

But montrehack is also...

A photograph of a group of men sitting at a bar in a dimly lit restaurant. The men are engaged in conversation. The foreground shows a wooden table with a napkin and a glass. The background features a bar counter and hanging lights.

a place to meet celebrities

WHY

Be better at CTF

Because we sucked at Defcon Quals

CISSP Groupies Score: 2600

Logout

Download client and connect FTW:

40 197.217.85:9999 (udp)

fake client

Pwn3d It!

grab bag	/urandom	binary 133tness	pwnables	forensics
100	100	100	100	100
200	200	200	200	200
300	300	300	300	300
400	400	400	400	400
500	500	500	500	500

Leaders

- Hates Irony (4900)
- PPP (4800)
- 侍 (4400)
- sutegoma2 (4400)
- Shellphish (4400)
- TwoSixNine (4400)
- European Nopsled Team (4200)
- More Smoked Leet Chicken (4100)
- our name sucks (4100)
- ACME Pharm (4100)
- WOWHACKER-PLUS (4100)
- Routards (3900)
- Zomg Pwnies (3900)
- bobsleigh (3900)
- Occupy EIP (3800)
- KAIST GoN (3800)
- disekt (3800)
- Neg9 (3600)
- blue-lotus (3600)
- LSE (3500)

Complete [scoreboard](#)

We didn't really succeeded at that

In fact its more about **routine** and **doing**

True story bro

HOW

Someone proposes a challenge

We work on it

He presents his solution after 3 hours

We go for beer after

Participants must bring laptops

Hack in ad-hoc teams

Make friends (optional)

WHEN

3rd Monday of every month*

*: certain restrictions apply, see website for details

WHERE

Notman house, UQAM or Google offices

then Benelux

WHO

Pierre-Marc Bureau, Sebastien Duquette, Marc-Etienne
M.Leveillé and myself

SHOUT-OUTS

DEFCON



Alexandre Rimthong for the montrehack name

Past presenters: Taher Azab, Xavier Garceau-Aranda, Pierre-Marc Bureau, Marc-Etienne M. Leveillé, Charles F. Hamilton, Philippe Arteau, Pierre-David Oriol, Marc-André Labonté, Sébastien Lorrain, Mathieu Lavoie, Benjamin Vanheuverzwijn, Sébastien Duquette, Gabriel Tremblay, Jonathan Marcil, Laurent Desaulniers, François Proulx and myself

A FEW AWARDS SHOULD GO TO

Most montrehack attended without actually working on the challenges

Our very own NorthSec President Mr Gabriel Tremblay



Longest challenge explanation

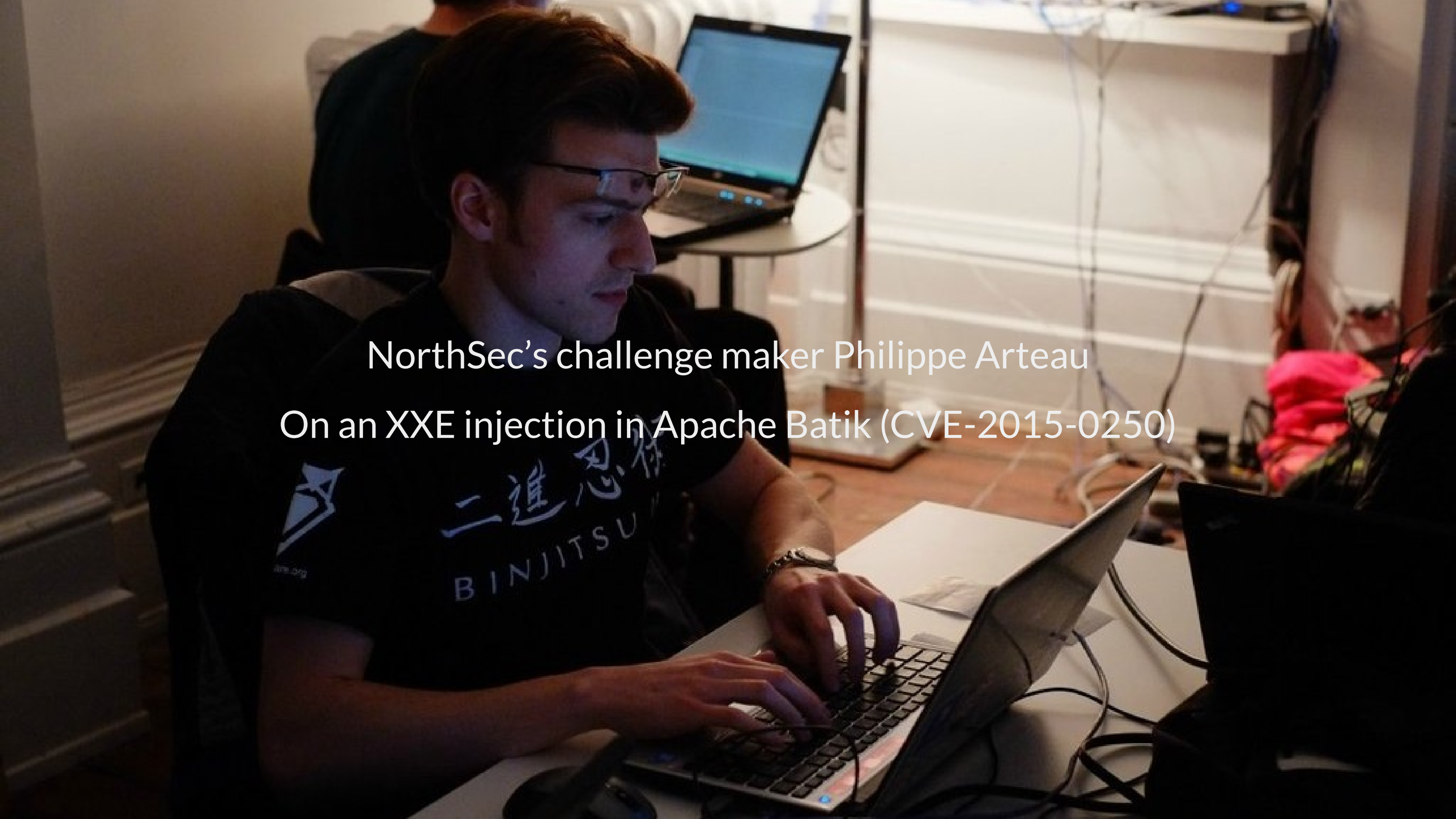
Going 3x over allocated timeslot



NorthSec's Logistics VP Mr. François Proulx

His challenge and explanation was good though

Making us secretly exploit a 0-day vulnerability in some
library



NorthSec's challenge maker Philippe Arteau
On an XXE injection in Apache Batik (CVE-2015-0250)

LESSONS

LESSON #0

Co-maintainership doesn't work

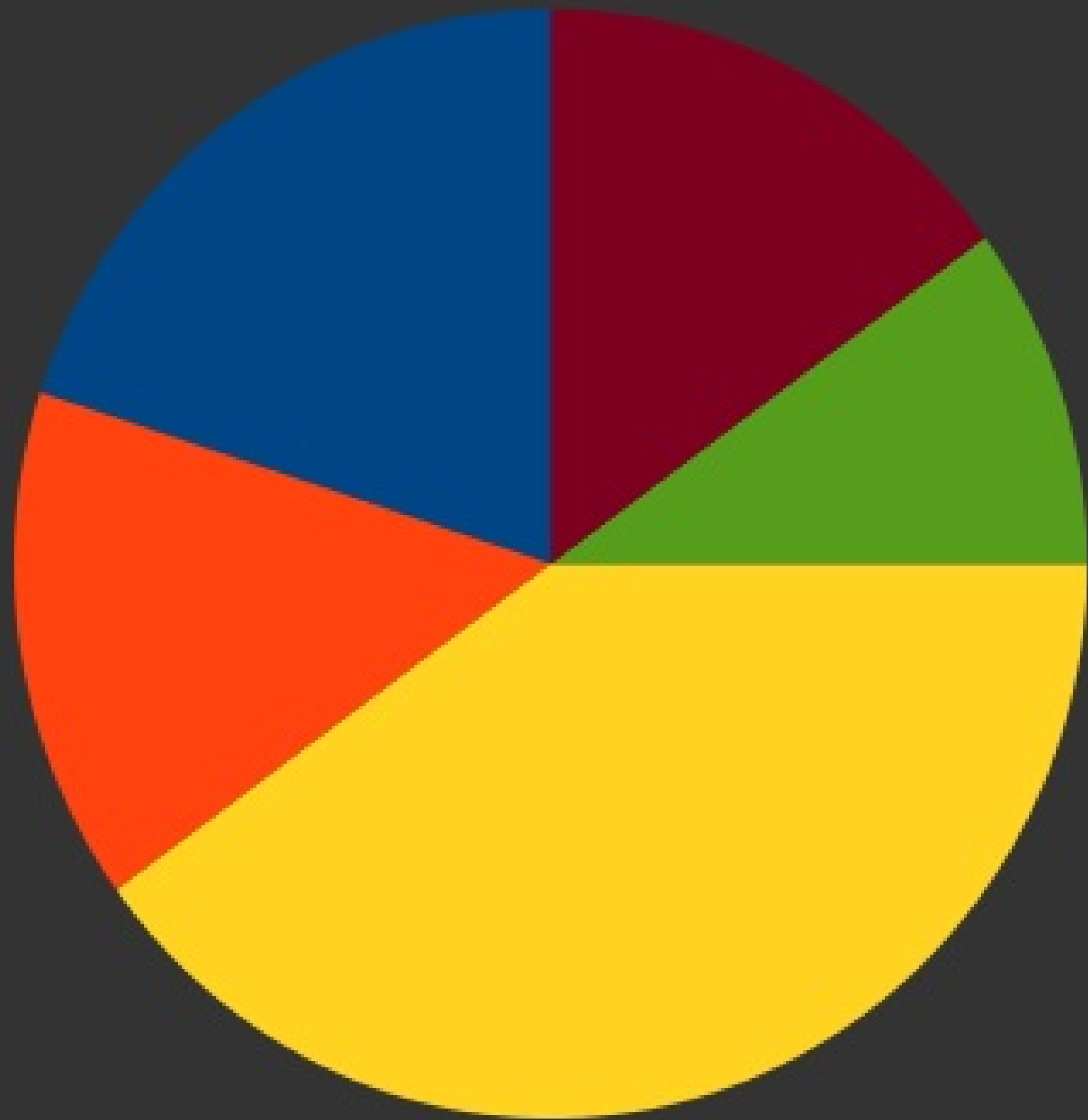
LESSON #1

We accidentally offended several communities

We're sorry

LESSON #2

It takes time



■ Update website

■ Copy / paste on social networks

■ Find the 'right' funny picture

■ Book a venue

■ Find someone to present

LESSON #3

Having checkpoints along a complex challenge is a good thing

TOOLS AND TECHNIQUES

There are no single tools or techniques

The END

Learn a scripting language

Accumulate snippets of codes and re-use them, expand them
over time

but preferably python3

Use ipython and ipython notebook

No plain gdb

fancy `.gdbinit` or `p3da`

From time to time try [radare2](#) instead of a pirated IDA Pro

Wireshark is da bomb and learn tshark

Especially `-T fields -e data` and then some piping into python with `fileinput` module for further processing.

Web: Burp or Owasp ZAP

Use vagrant for disposable VMs

Learn to use a powerful text-editor like `vim`, `sublime` or
`emacs`

Preferably `vim`

Learn to use the developers tools of your browser

WHAT'S NEXT?

Sponsored by the Benelux for a free beer after the workshop

BENELUX

No breaks this summer

Next month we get a Googler from Seattle

Defcon Quals 2015 challenge: wibbly wobbly timey wimey

PARTICIPATE!

We want you to come to montrehack

We want you to **present** at montrehack!

We want you to **sponsor** montrehack!

Best way: present or create a challenge!

- Mailing list:
<https://groups.google.com/forum/#!forum/montrehack>
- Twitter: <https://twitter.com/montrehack>
- Other places: facebook, google+
- Getting involved:
<https://groups.google.com/forum/#!forum/montrehack-meta>

You can easily **contribute** and participate

QUESTIONS?

Thanks for your time!

@montrehack, @obilodeau

NO LOGS = NO CRIME