

TWO YEARS OF MONTREHACK

Olivier Bilodeau



PLAN

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

HI I'M OLIVER 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 \$omething 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 \\$HELL](#), 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

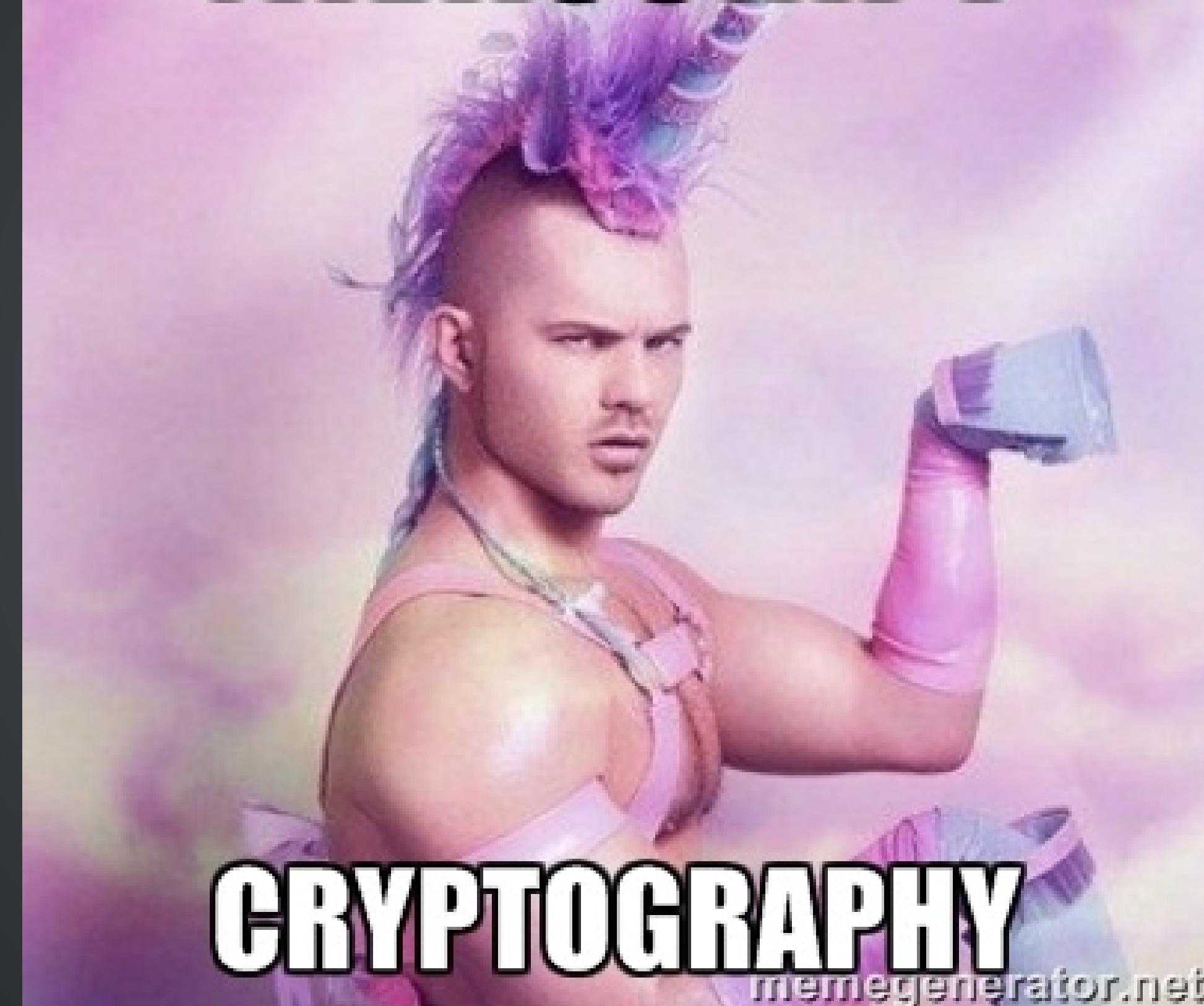
Android, Crackme, Cryptography, Exploit, Forensic,
Hardware, IOS, Linux, Network, Reverse-Engineering, SQL
Injection, Steganography and Web

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



KSS WAS A FEATURE

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

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 people sitting at a bar counter in a dimly lit bar. The scene is filled with warm, ambient lighting from overhead lamps. In the foreground, a person's arm and hand are visible on the left, resting on the bar. Behind them, several men are seated at the bar, engaged in conversation. One man in the center is wearing glasses and a dark t-shirt, looking towards the camera. Another man to his right is seen from behind, wearing a white t-shirt. The bar counter is made of wood and has a dark, polished finish. In the background, there are more patrons and some decorative elements like small flags or signs. A bright, out-of-focus light source on the right side creates a strong lens flare.

a place to meet celebrities

WHY

Be better at CTF

Because we sucked at Defcon Quals

Diutinus Defense Technologies Inc.

CISSP Groupies Score: 2600

[Logout](#)



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, Sébastien Duquette, Marc-Etienne
M. Leveillé and myself



SHOUT-OUTS

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

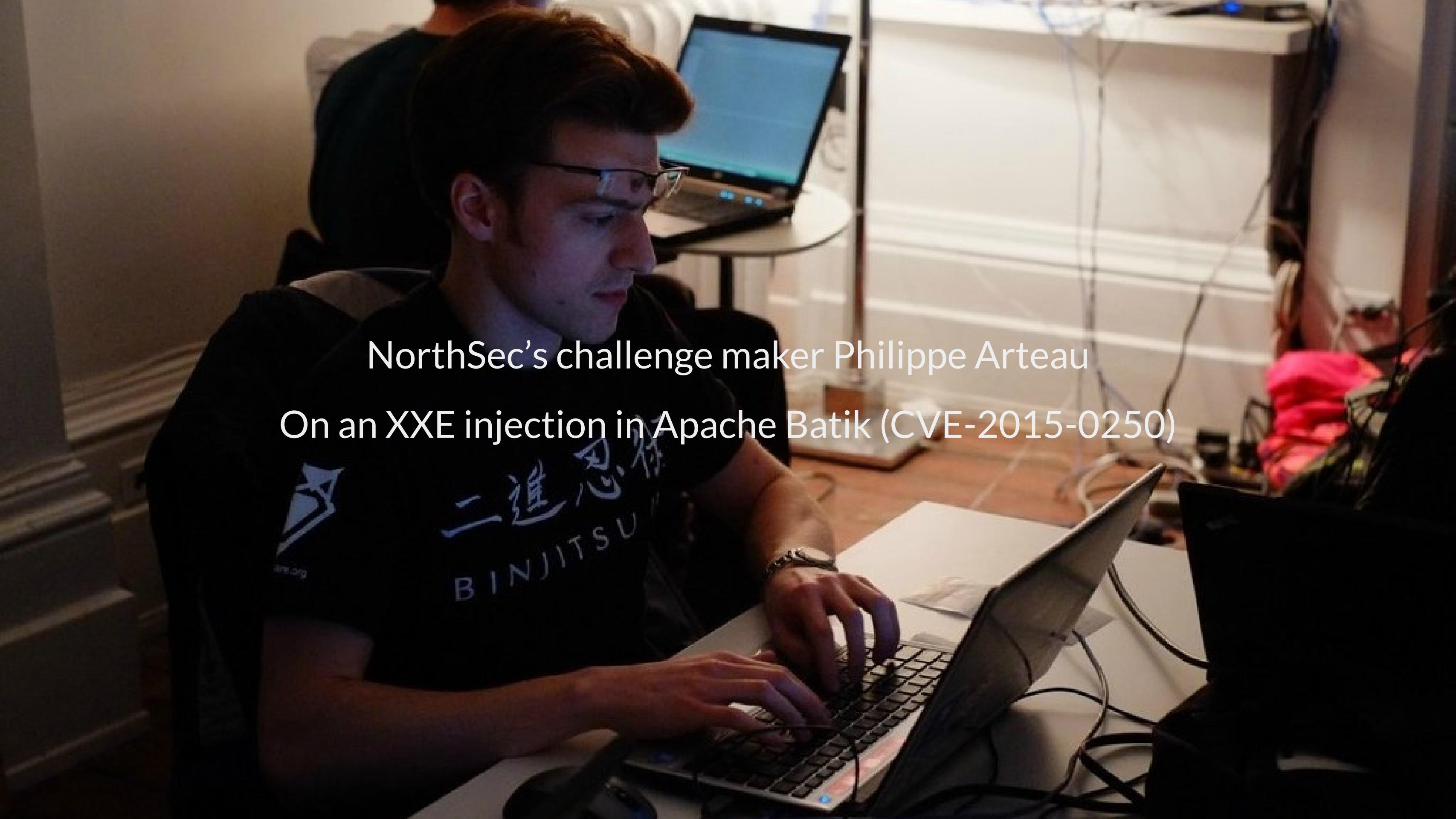
Going 3x over allocated timeslot



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

A photograph of a man with dark hair and glasses, wearing a black t-shirt with a white graphic that includes the text "B IN JITSU" and some stylized characters. He is sitting at a desk, looking down at a laptop screen. In the background, there is another computer monitor on a stand. The setting appears to be a workshop or laboratory.

NorthSec's challenge maker Philippe Arteau

On an XXE injection in Apache Batik (CVE-2015-0250)

LESSONS

LESSON #0

Co-maintainership doesn't work

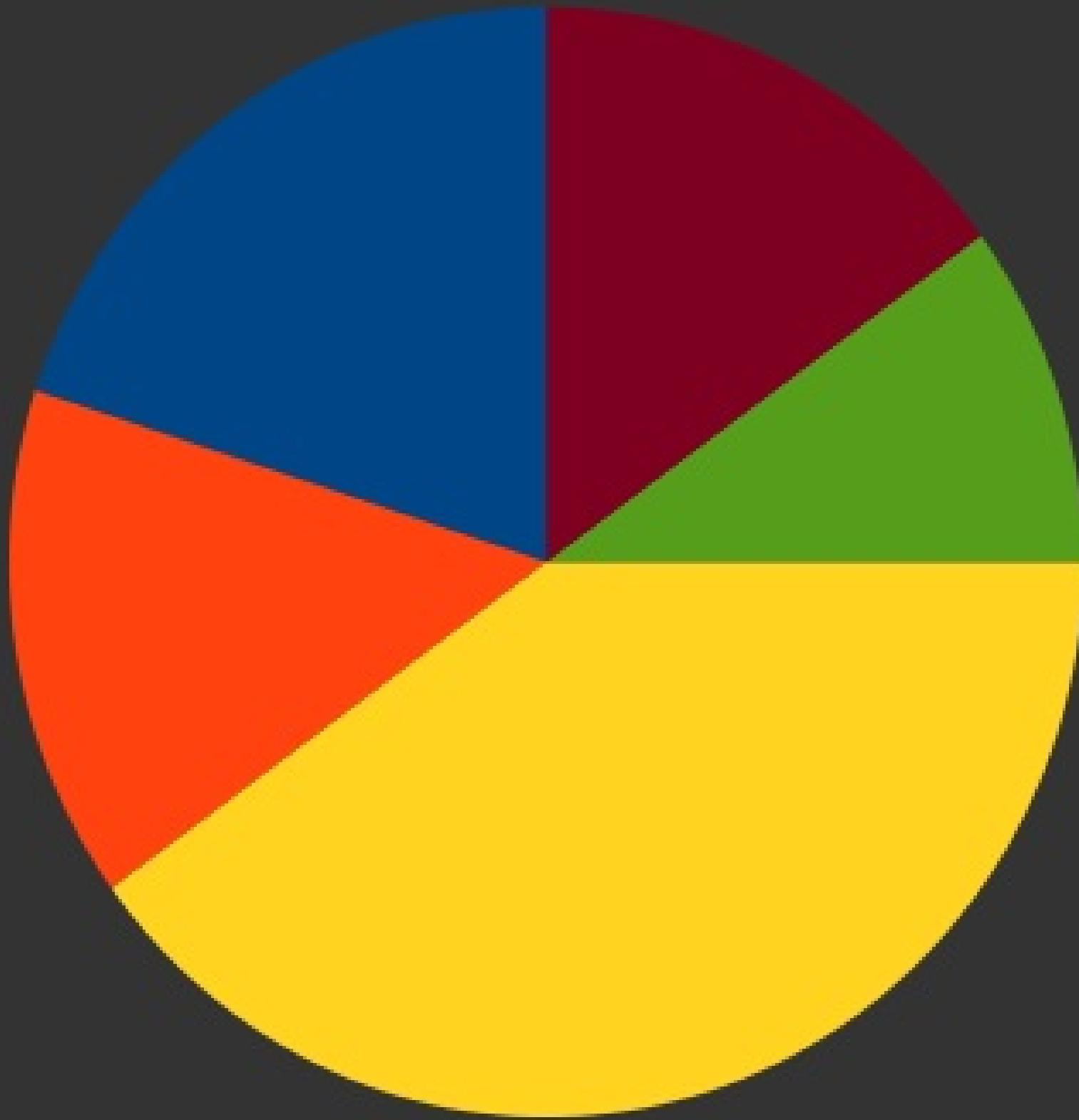
LESSON #1

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



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

A photograph of a man with dark hair and glasses, wearing a black zip-up hoodie. A white rectangular protest banner is pinned to his chest with four black pushpins. The banner has the text "NO LOGS = NO CRIME" printed on it in bold, black, sans-serif capital letters.

QUESTIONS?

Thanks for your time!

@montrehack, @obilodeau