



HACKFEST
NINE LIVES

HACKFEST 2017

9 LIVES EDITION

PLAN DE LA PRÉSENTATION

- ▶ Qu'est-ce que le Hackfest?
- ▶ Résumé de la 9^{ème} édition
- ▶ Conclusion

HACKFEST?

QU'EST-CE QUE LE HACKFEST?

- ▶ Le plus gros événement sur le piratage et la sécurité informatique au Canada(~900 participants)
 - ▶ **Quand?** En novembre
 - ▶ **Où?** À Québec
 - ▶ **Combien?** 90\$ en prévente, 120\$ à la porte
 - ▶ **Quoi?** Conférences, Ateliers, CTF, Crochetage, Ingénierie sociale
 - ▶ Bilingue, *mais surtout anglophone*

CTF?

- ▶ *Capture the Flag*
- ▶ Jeu d'habileté qui simule un environnement présentant des vulnérabilités pouvant être exploitées par les participants
- ▶ Il existe différents types d'épreuves demandant des aptitudes différentes
 - ▶ Rétro-ingénierie
 - ▶ Analyse du trafic réseau
 - ▶ Programmation
 - ▶ Encryption
 - ▶ Attaque/Défense
 - ▶ Électronique
- ▶ Un fois un défi résolu, un **flag** est remis et peut être validé pour obtenir des points

CTF-EXEMPLE D'INJECTION SQL

- Trouver une requête acceptant les entrées de l'utilisateur

[←](#) [→](#) [↻](#) [testphp.vulnweb.com/artists.php?artist=1](#)

 acunetix  acu art

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

[Browse categories](#)
[Browse artists](#)
[Your cart](#)
[Signup](#)
[Your profile](#)

artist: r4w8173

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent

CTF-EXEMPLE D'INJECTION SQL

- ▶ Essayer de modifier les paramètres de la requête

The screenshot shows a web browser with the address bar containing the URL: `testphp.vulnweb.com/artists.php?artist=-1 UNION SELECT 1, 2, 3`. The numbers 2 and 3 are highlighted in orange. The page header features the Acunetix logo and the text "acuart". Below the header, a navigation bar includes links: [home](#), [categories](#), [artists](#), [disclaimer](#), [your cart](#), [guestbook](#), and [AJAX Demo](#). On the left side, there is a sidebar with a search bar labeled "search art" and a "go" button. Below the search bar are links: [Browse categories](#), [Browse artists](#), [Your cart](#), [Signup](#), and [Your profile](#). The main content area displays "artist: 2" with the number 2 highlighted in orange. Below this, there is a link [3](#) (highlighted in orange) and two links: [view pictures of the artist](#) and [comment on this artist](#).

CTF-EXEMPLE D'INJECTION SQL

- ▶ Abuser la requête pour récupérer des données

The screenshot shows a web browser window with the address bar containing the URL: `testphp.vulnweb.com/artists.php?artist=-1 UNION SELECT 1,pass,cc FROM users`. The page displays the Acunetix logo and the text "TEST and Demonstration site for Acunetix Web Vulnerability Scanner". A navigation menu includes links for home, categories, artists, disclaimer, your cart, guestbook, and AJAX Demo. On the left, there is a search bar labeled "search art" with a "go" button and a list of links: "Browse categories", "Browse artists", "Your cart", "Signup", and "Your profile". The main content area shows "artist: test" followed by a highlighted phone number "1234-5678-2300-9000" and two links: "view pictures of the artist" and "comment on this artist".

← → ↻ `testphp.vulnweb.com/artists.php?artist=-1 UNION SELECT 1,pass,cc FROM users`

acunetix **acu art**

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

[Browse categories](#)
[Browse artists](#)
[Your cart](#)
[Signup](#)
[Your profile](#)

artist: test

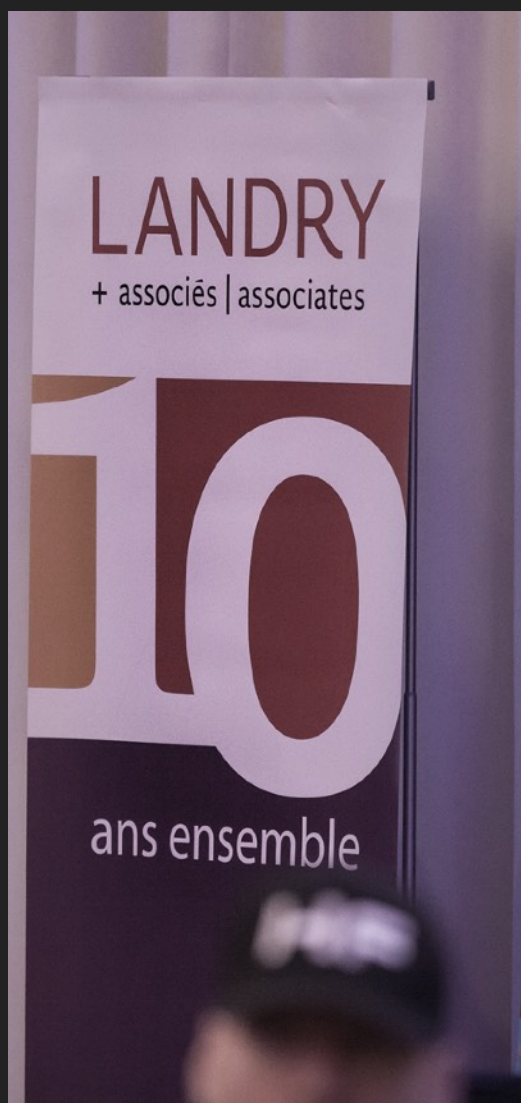
1234-5678-2300-9000

[view pictures of the artist](#)
[comment on this artist](#)

RÉSUMÉ DE LA 9ÈME EDITION

POUR LA PREMIÈRE FOIS, DES ÉTUDIANTS DU COLLÈGE PARTICIPENT!





FORMATIONS





JOUR 1

SUPERHÉROS TOUS! COMMENT L'EMPATHIE PEUT AIDER L'INCLUSION DU PERSONNEL AVEC ASD/ADHD



FINGERPRINTING ANDROID MALWARE PACKAGING PROCESS THROUGH STATIC ANALYSIS TO IDENTIFY THEIR CREATOR

Fingerprinting Android malware packaging
process through static analysis to identify
their creator



François Gagnon
francois.gagnon@ccirc-ccirc.ca
www.cegep-ste-foy.qc.ca/cybersecurite



Frédéric Massicotte
Canadian Cyber Incident Response Centre (CCIRC)
Public Safety Canada

Hackfest 2017

CREATING A PROFESSIONAL-QUALITY EMBEDDED DEVICE ON A BUDGET



MAKE A THING – CREATING A PROFESSIONAL- QUALITY EMBEDDED DEVICE ON A BUDGET

Michael Vieau, CISSP, CEH

Kevin Bong, GSE, PMP, QSA,
CISSP, GCIH, GCFA

November 3, 2017



HOW TO PWN AN ENTERPRISE IN 2017 (OR 2016, OR 2015...)



BEATING THE DISINFORMATION DRIFT: FACTS ABOUT THE ALPHABAY MARKET

Beating the Disinformation Drift Facts about the AlphaBay Market

Masarah Paquet-Clouston
GoSecure Research

GOSECURE



PRACTICAL ANALYSIS OF AWARENESS



BANKING ON INSECURITY: WHY ATTACKERS CAN TAKE THE MONEY AND RUN





CTF

HACKFEST

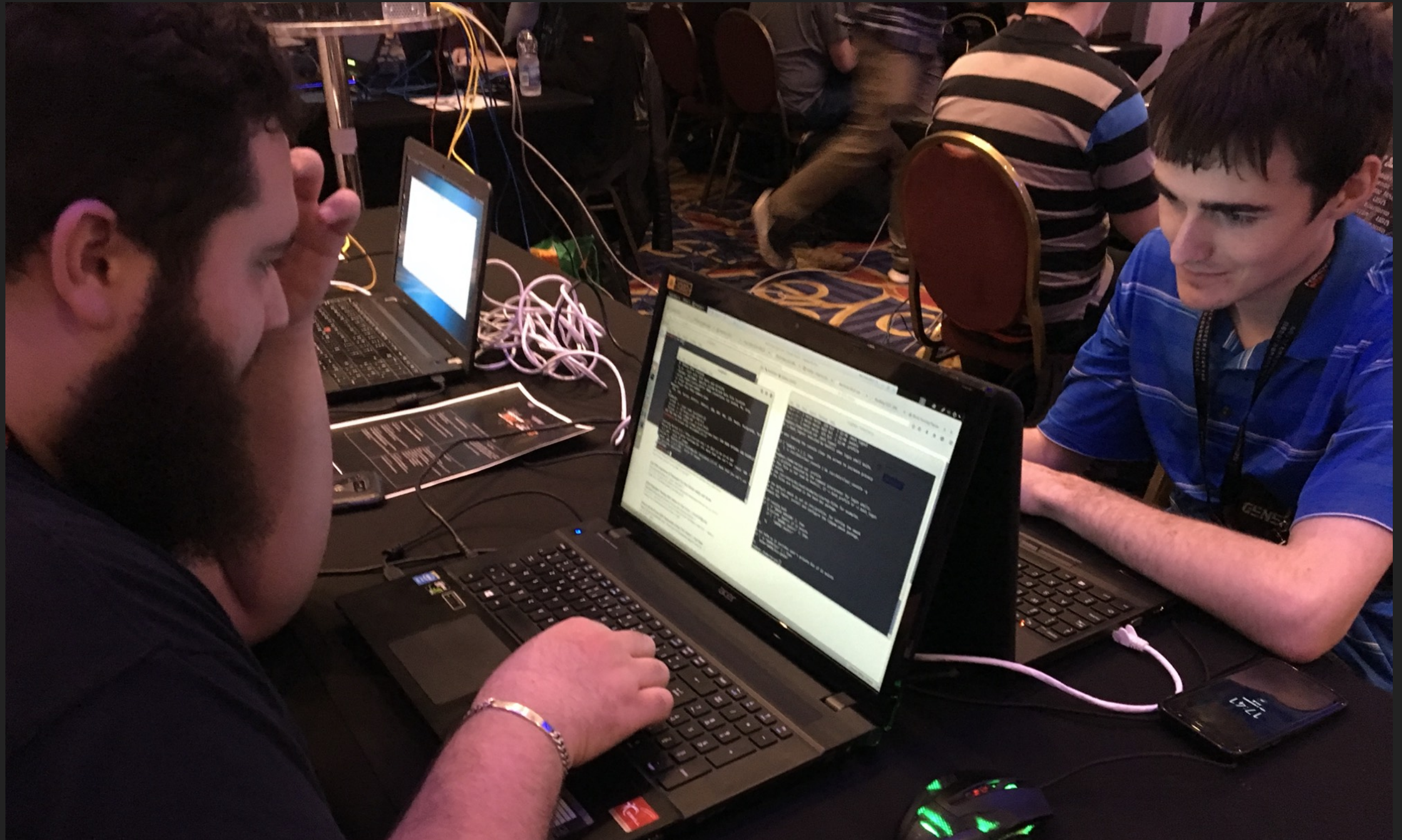
CTF



CTF



CTF



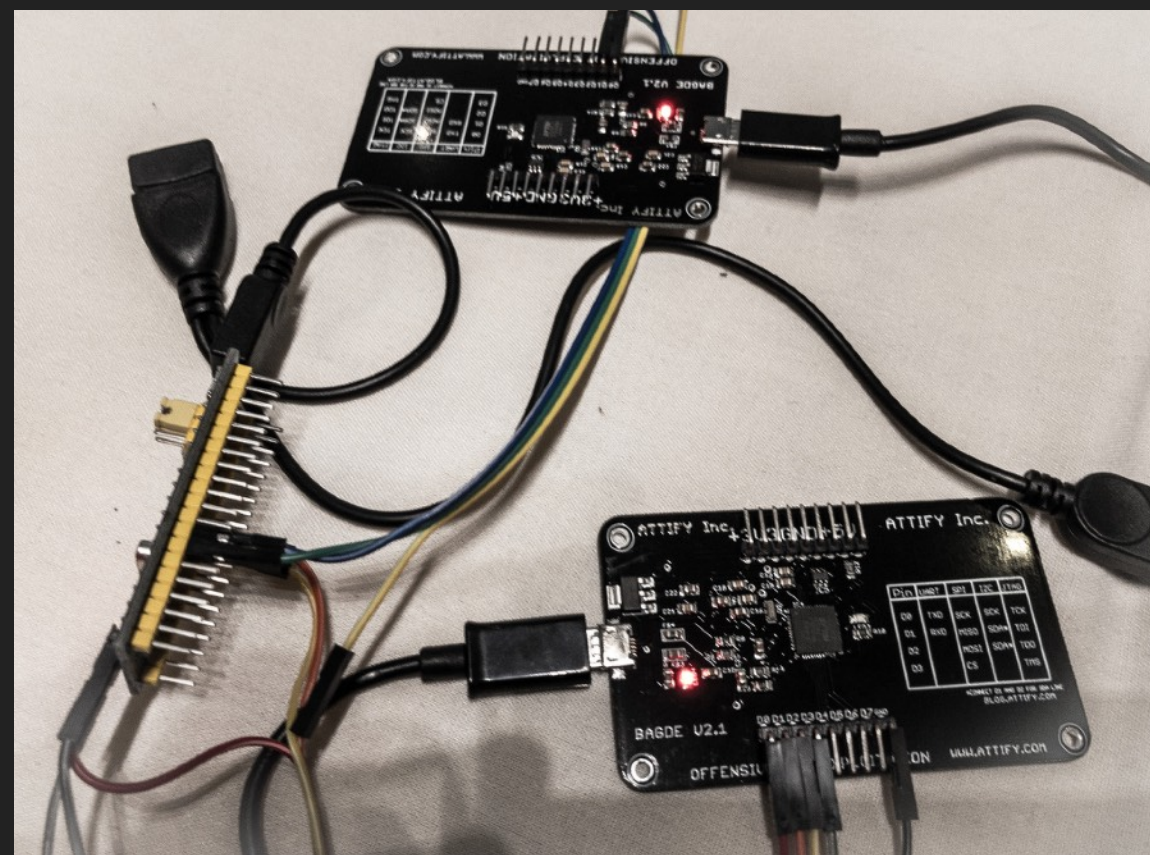
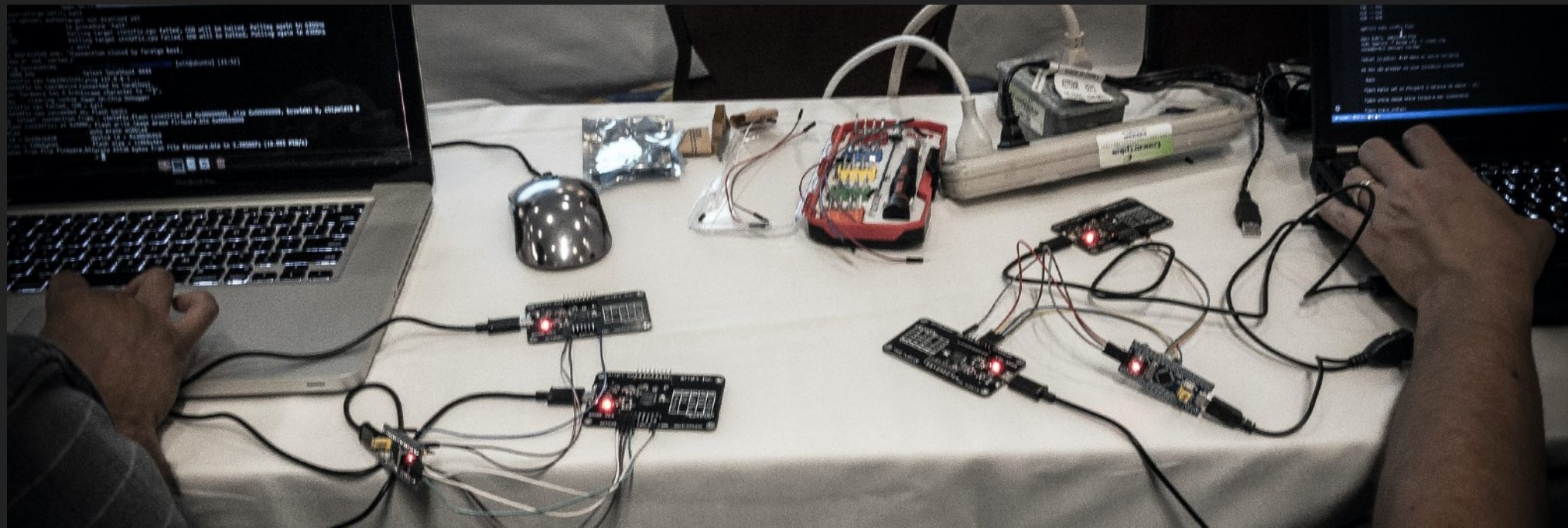
CTF – 270 PARTICIPANTS



CTF - CROCHETAGE



CTF - ÉLECTRONIQUE



CTF – INGÉNIERIE SOCIALE





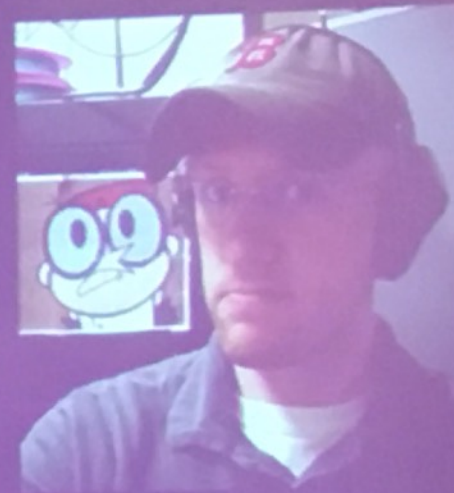
JOUR 2

ATTACK DRIVEN DEVELOPMENT: GETTING STARTED IN APPLICATION SECURITY

hackfest.ca

Attack Driven Development

Getting Started in Application Security



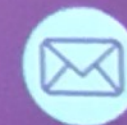
Presented by:
Keith Hoodlet



@andMYhacks



<https://github.com/andMYhacks>



keith@attackdriven.io

Nov. 3rd & 4th, 2017

GENETIC ALGORITHMS FOR BRUTE FORCING



DISSECTING A METAMORPHIC FILE-INFECTING RANSOMWARE



STATIC-ANALYSIS TOOLS: NOW YOU'RE PLAYING WITH POWER!



HADOOP SAFARI : HUNTING FOR VULNERABILITIES

WAVESTONE

HACKFEST
2017

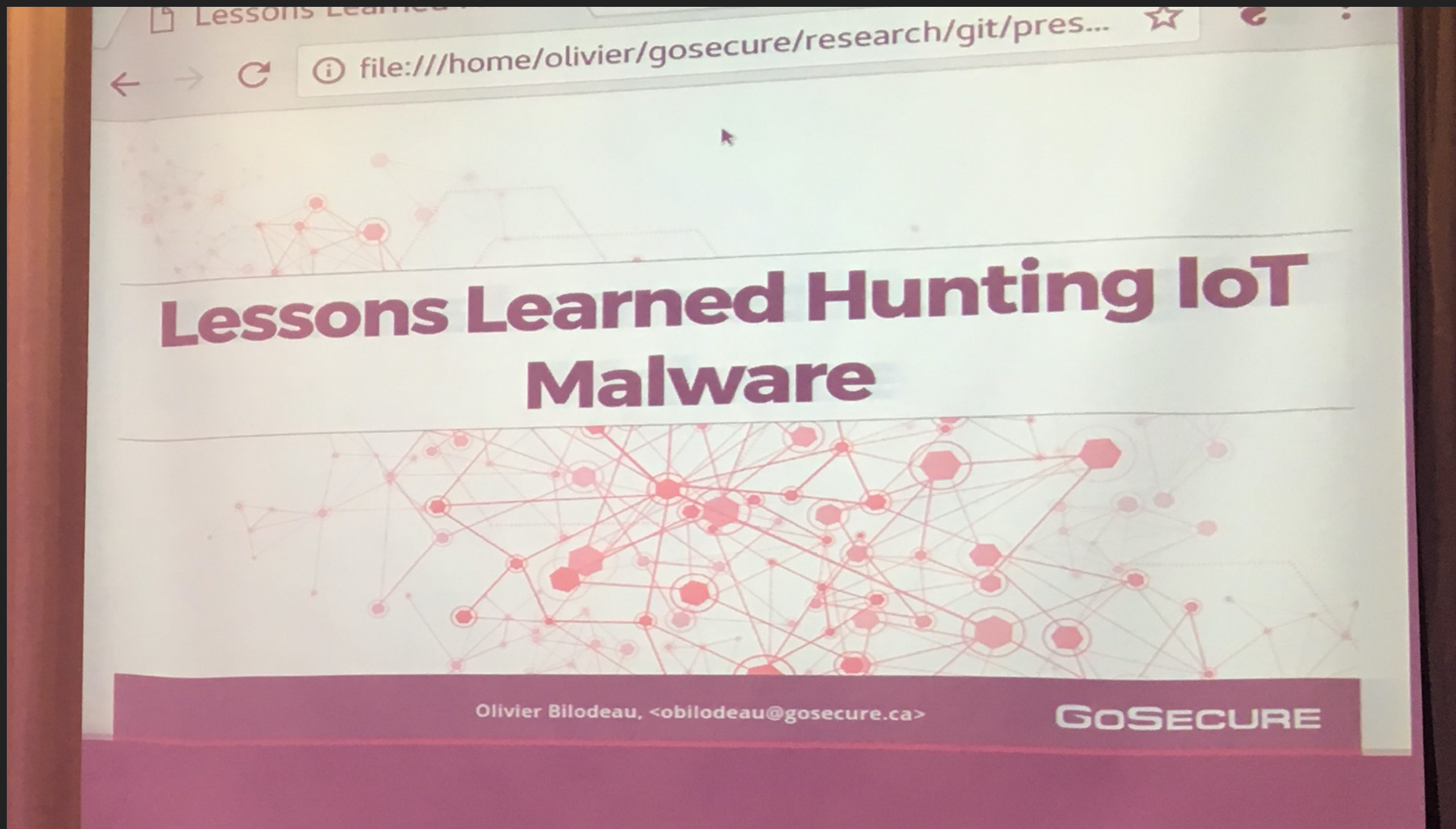
TRAININGS 31-1-2ND
CONFERENCES 3-4TH
NOVEMBER 2017
QUEBEC CITY, QC, CANADA

Hadoop safari: Hunting for vulnerabilities

Hackfest 2017 – November, 4th

Thomas DEBIZE
thomas.debize@wavestone.com

LESSONS LEARNED HUNTING IOT MALWARE



LES VÉHICULES AUTONOMES, LEUR TÉLÉMÉTRIE ET L'IMPACT SUR LA SÉCURITÉ

Les véhicules autonomes, leur télémétrie
et l'impact sur la sécurité

Marc-André Bélanger, CFE, CEPT, CISSP, CPO ►
Hackfest 2017

BUGCROWD PARTY ET MINI-CTF OWASP



<DUALCORE>

► <http://dualcoremusic.com/nerdcore/>



PODCAST – LA FRENCH CONNECTION

► <http://securite.fm/>



MINI-CTF OWASP



MINI-CTF OWASP : 12ÈME / 57

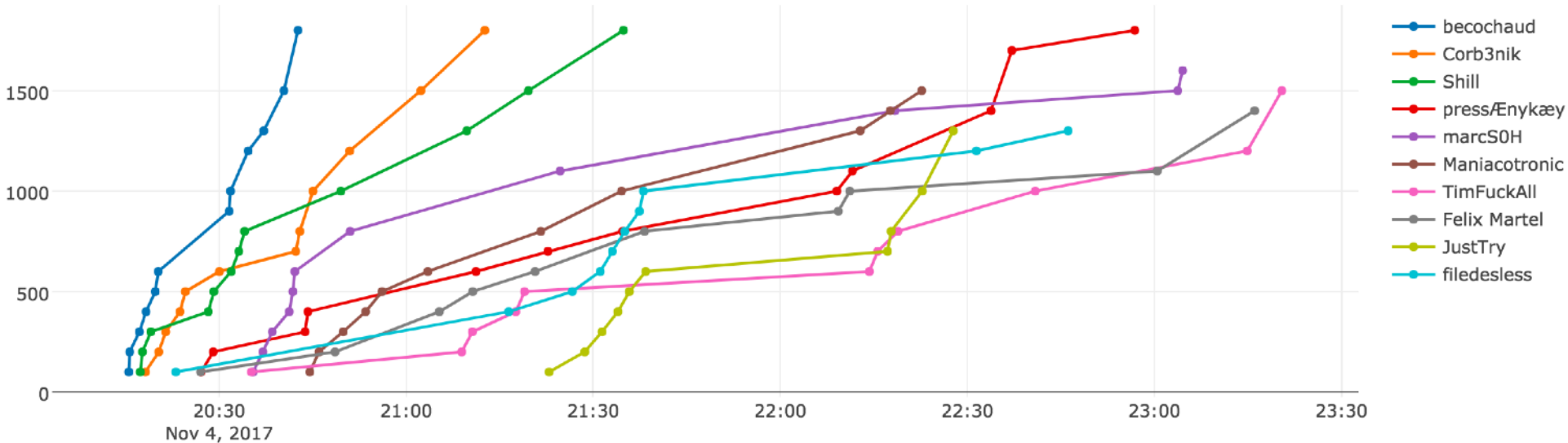
Challenges

Qualification

Privilege Escalation 2 100	Upload 1 100	Privilege Escalation 1 100	SQL Injection 1 100	Encoding 1 100	RCE 1 100
Local File Inclusion 1 100	Direct Object Reference 1 100	XXE 1 200	Exploit 1 200	Upload 2 300	SQL Injection 2 300

Scoreboard

Top 10 Teams



CONCLUSION

CONCLUSION

- ▶ Le Hackfest est un événement unique au Canada
- ▶ La communauté *infosec* est très ouverte et accueillante
- ▶ Sans être un expert en sécurité, il est important d'être sensibilisé à ces enjeux
- ▶ C'est un événement très accessible pour en apprendre plus sur tout ce qui touche la sécurité informatique!

HACKFEST SUR LE WEB



<http://www.hackfest.ca/>



[@hackfest_ca](https://twitter.com/hackfest_ca)



[hackfestca](https://www.youtube.com/hackfestca)



<https://www.flickr.com/photos/hackfest2k9>

RESSOURCES POUR DÉMARRER

- ▶ <https://www.hackerone.com/start-hacking>
- ▶ <https://www.offensive-security.com/metasploit-unleashed/>
- ▶ https://www.owasp.org/index.php/Main_Page
- ▶ <https://leanpub.com/web-hacking-101>
- ▶ <https://leanpub.com/ltr101-breaking-into-infosec>
- ▶ <https://www.amazon.ca/Web-Application-Hackers-Handbook-Exploiting/dp/1118026470>

IMPACT DU HACKFEST AU COLLÈGE SHAWINIGAN

- ▶ Site du département

<https://shawinigan.info/le-departement-participe-au-hackfest-2017-a-quebec/>

- ▶ Journal du réseau collégial du Québec

http://lescegeps.com/pedagogie/approches_pedagogiques/des_conferences_formatrices_en_securite_informatique_a_u_college_shawinigan_

- ▶ Mise en place d'un club de sécurité informatique au département à l'hiver **2018**

QUESTIONS? 😊