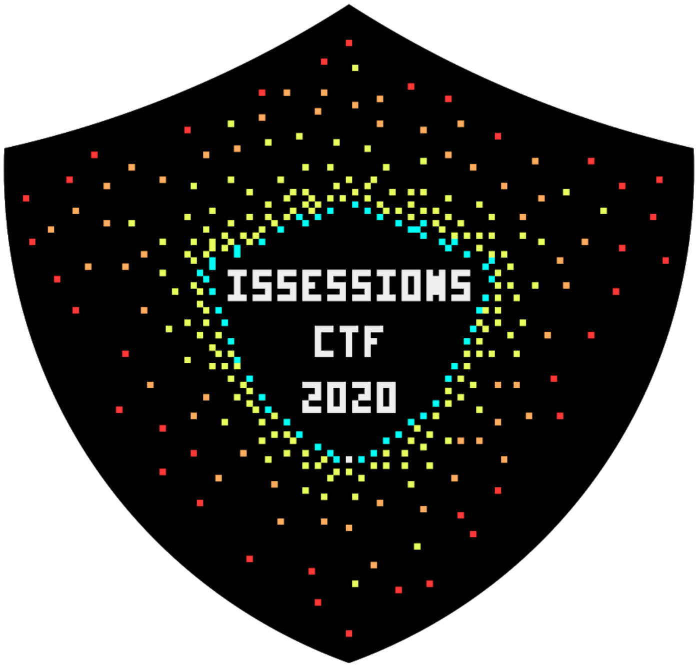
Sheridan | Faculty of Applied Science and Technology

ISSessions

Are You Ready for...



Date: March 14, 2020, 8:00AM

Location: Trend Micro, 1 Snooker Street, Toronto, ON, M6K 1G1

Capture the Flag Competition

ISSessions’s biggest event of the year is the ISSessions Capture the Flag (“ISSessionsCTF”) competition, a wonderful learning and networking opportunity. A CTF is a cybersecurity competition designed to challenge its participants to solve computer security problems and/or capture and defend computer systems. CTFs consist of a series of challenges that vary in their degree of difficulty. Once a challenge is solved, a “flag” is awarded to the players. The flag is then exchanged for points. CTFs are widely used as an educational tool at industry conferences such as DEFCON, RSA, BlackHat, and Bsides.

SSU
sheridan student union

Who We Are

ISSessions is an information security meetup featuring a security news roundup as well as talks by students and industry professionals. In addition, we host a number of technical workshops on various information security topics. Our biggest event of the year is the ISSessions CTF which attracts over a 100 participants from various InfoSec programs across Ontario. Our mission is to develop students into highly-skilled cybersecurity professionals who can defend corporate networks and critical infrastructure against online threats.

ISSessionsCTF2020

ISSessionsCTF2020 is a CTF created for students by students! It will take place on March 14, 2020 at the Trend Micro Office in Toronto (1 Snooker Street, Toronto, ON, M6K 1G1). Students will spend the day solving information security challenges and attending sponsor-provided workshops! This event would not be possible without our industry sponsors this year: Trend Micro, Bell, Deloitte, Security Compass, and Vontel, as well as academic sponsors: Sheridan's Faculty of Applied Computing and Sciences and the Sheridan Student Union!

TREND MICRO™ | research

Bell

Deloitte.

Security Compass

Vontel

Requirements

A laptop and a Kali Linux VM! That's it!

Registration

Registration opens Monday, February 17 @ 11:00AM, on Eventbrite! Follow us on Twitter (@issessions) and Linkedin (ISSessions) for live updates.

CTF Challenges

You must be a student to participate. Students from various schools will compete in teams of 4* to solve 60-70 student-created and sponsored challenges. If you're a beginner to information security, don't fret! This CTF is for you! The challenges will test breadth not depth and will assume an introductory-intermediate level of knowledge. Of course every category will have a few advanced challenges for the CTF fanatics among you! A challenge will earn you somewhere between 10 and 100 points. The challenges fall within the following categories:

- Digital Forensics
- Network Traffic Analysis
- InfoSec Trivia
- Cryptography
- Programming
- Web Application Security
- Linux & SysAdmin
- Lockpicking
- Steganography, and more!

Mini-Workshops

A major element of the competition will be a series of wonderful mini-workshops offered by our Title, Platinum, and Gold sponsors: Trend Micro, Bell, Deloitte, and Security Compass. Each mini-workshop will run for approximately 30mins. Participation in the mini-workshops is optional, however it will help you solve some of the sponsored challenges contributed by the above companies. Furthermore, there is a 100 point reward for attending each workshop*. We are pleased to announce the following workshops:

**An exception to this rule is Deloitte which will be providing 3 workshops at 33 points each.*

TREND MICRO | research

An Introduction to N-Day Vulnerability Research (100 points)

By John Simpson

This workshop will be a light introduction to the world of N-day vulnerability research where researchers analyze patches and craft proof-of-concept exploits in order to better understand how to defend against exploitation attempts. The workshop will touch on the basic toolset necessary for analysis of open source binary applications, Java-based applications, and scripting languages commonly used for web applications such as PHP.

Bell

Threat Hunting Using Mordor (100 points)

By Mangatas Tondang, Sylvain Lu, Avneet Singh, Harmanpreet Gurm

This workshop will help you develop a threat hunting mindset and understand the essence of the profession. We will do both theoretical learning on threat hunting concepts and hands on exercises using ELK and a real attack dataset from Mordor. The Mordor project provides pre-recorded security events generated by simulated adversarial techniques in the form of JavaScript Object Notation (JSON) files for easy consumption. The pre-recorded data is categorized by platforms, adversary groups, tactics and techniques defined by the Mitre ATT&CK Framework.

Deloitte.

Mini-Workshop #1: Threat Intelligence & Vulnerability Management (33 points)

By Ryan Westman

The workshop will discuss how Deloitte's Cyber Intelligence Centre's Threat Intelligence and Vulnerability Management teams work together on a daily basis to support clients maintain secure networks. The workshop will cover:

- How Threat Intelligence works in an operational capacity as opposed to an engagement/project capacity.
- How Vulnerability management works in an operational capacity as opposed to an engagement/project capacity.
- How both teams collaborate to secure our clients networks.

Mini-Workshop #2: Logs and Incident Response (33 points)

By Felipe Mafra

This workshop will provide hands training on to how identify a security risk from logs, how to create a rule and them perform the investigation, covering the following:

- Researching threats
- Developing threat content use cases
- Security operations and investigation steps

Mini-Workshop #3: Penetration Testing Mobile Applications (33 points)

By Guilherme Rother and Tabish Hasan

This workshop will provide an overview on how to approach penetration testing for Android mobile applications, including:

- What tools are available out there to support testing.
- Things to look out for when analyzing apps.
- demonstration of test cases and tools

SecurityCompass

Introduction to IoT Hacking (100 points)

By Adam Greenhill

From your phone to your board-game dice to, quite probably, your fridge as well, outdated and easily exploitable versions of the Bluetooth protocol are equally prevalent. This quick workshop will provide students with a crash course on Bluetooth security, its vulnerabilities, and methods for exploiting them. No prior knowledge of Bluetooth or the leveraged tools (i.e. Wireshark) are required to attend. Hope to see you there!

Crypto Corner

Developed By Joshua Schneider

Yeah you can do encryption using AES, RSA, and Elliptic Curves! But how about a chess board, a card deck, and some dice? Learn cryptography in its simplest form through a series of unique challenges developed by Joshua Schneider, the greatest cryptography professor in the 9 realms!

Lockpicking Table

By Nebo & Dave

Never picked a lock before? Now’s the time to learn! Join Nebo & Dave, alumni, and two of the operators of SECTOR's Lockpicking Village in a variety of locksport challenges. Pick the lock, get the flag. Lessons, picks, and tools will be available for all, but feel free to bring your own. Shoes are mandatory.

Loot (Prizes)

All competition participants will receive an **ISSessionsCTF2020 T-Shirt, ISSessionsCTF2020 stickers,** and **a swag bag** curated by our sponsors! The top 3 teams will have the option of choosing between three equally-valued (read: awesome) bundles. 1st place will get 1st pick, 2nd place, 2nd pick, and so on. Each bundle is valued at approximately $360. The three bundles are:

The "Book Worm" Bundle

4x Blue Team Field Manual (Hard Copy)

4x Red Team Field Manual (Hard Copy)

4x Linux Toolbox Comics (Hard Copy)

4x Black Hat Python, No Starch Press (Hard Copy)

The "Arduinist" Bundle

4 x Arduino Ultimate Starter Kit + 260-Pages of Detailed Tutorials

4 x Arduino Workshop: A Hands-On Introduction with 65 Projects, No Starch Press (Hard Copy)

The "Generalist" Bundle

4 x Sparrows Lockpicking Sets + Practice Cutaway Lock

4 x Backdoors & Breaches Card Game by Black Hills InfoSec

4 x $25 Amazon Gift Cards

Schedule

Time	*CTF Commons*	*Ontario Conference Room*	*Training Room*
8:00AM	*Doors Open: Participant & Sponsor Check-in*		
8:30AM			
9:00AM			
9:30AM	*Kickoff: Louai Abboud, ISSessions President*		
10:00AM	*Trend Micro Keynote: John Simpson,* *N-Day Vulnerability Researcher*		
10:30AM	*CTF-Start*		
11:00AM			
11:30AM		*Deloitte: Threat Intelligence & Vulnerability Management*	*Security Compass: Introduction to IoT Hacking*
12:00PM			
12:30PM		*Bell: Threat Hunting Using Mordor*	*Deloitte: Penetration Testing Android Applications*
1:00PM	*Lunch*		
1:30PM			
2:00PM			
2:30PM		*Trend Micro: Intro to N-Day Vulnerability Research*	*Deloitte: Logs & Incident Response*
3:00PM			

3:30PM		*Trend Micro: Intro to N-Day Vulnerability Research*	*Security Compass: Introduction to IoT Hacking*
4:00PM			
4:30PM		*Bell: Threat Hunting Using Mordor*	*Security Compass: Introduction to IoT Hacking*
5:00PM			
5:30PM		*Trend Micro: Intro to N-Day Vulnerability Research*	*Bell: Threat Hunting Using Mordor*
6:00PM			
6:30PM	*CTF-End*		
7:00PM	*Wrap Up & Prizes*		