THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

New Zealand Cyber Security Challenge

Rules and Eligibility

Eligibility

New Zealand Cyber Security Challenge is the annual event for people who are interested in cyber security. To be consistent and to keep Cyber Security Challenge challenging for participants, three categories of contestants are proposed:

1. Secondary School Students (Year 9-13) (NB: students younger than Year 9 are most welcome)
2. Tertiary Education Students (Universities, Institutes of Technology, Polytechnics, Colleges and etc).
3. Open Category (Professionals, anonymous participants and etc).

Registration

Every person should be registered individually and indicate the name of the team where he/she would like to compete.

Rounds

The Challenge consists of 4 Rounds: Round 0, Round 1, Round 2 and Round 3.

Round 0 is the qualifying round open to NZ and regional contestants (e.g. Tonga), and the top 150 participants (i.e. the Master Class) will be invited to participate in Round 1, 2 and 3 on the Hamilton campus of the University of Waikato.

The qualifying round consists of 5-6 Capture-The-Flag (CTF) challenges at easy and medium levels. Contestants will be scored based on successful flags captured, and the time taken to capture them. The contestant's main goal at Round 0 is to qualify further

into the Challenge and be invited for further competition rounds. Round 0 will be opened to registered contestants for 12 days. The main criteria of passing is to solve as much as possible and as fast as possible. Contestants will need to attempt Round 0 individually. The top 150 qualified contestants can either compete individually or form teams of up to 3 qualified contestants.

Round 1, 2 and 3 are organized at the University of Waikato's Hamilton campus and computers will be provided to all participants. Participants are not allowed to use their own laptops for Rounds 1, 2 and 3.

Round 1 is a 2-hour competition designed with easy, medium and hard Capture-The-Flag challenges. Round 1 is worth 90% of your cumulative final score for both Round 1 and Round 2. There are typically more than 10 challenges in Round 1 each year.

Round 2 is the Policy Round and is worth 10% of your cumulative final score for Rounds 1 and 2. In this Round the teams will be provided a few fictitious scenarios and should be able to answer several questions in a pub-quiz style. The goal of Round 2 is to allow contestants to appreciate the national and corporate policy aspects of cyber security.

After Round 1 and Round 2 are finished the organizers will tabulate final points for each team and the Top 5 teams will be announced for final Round 3. In Round 3, each of the team will take the role of Blue Teams defending fictitious enterprise infrastructure, in the face of attacks from a single Red Team consisting of actual experienced cyber security professionals. The team scoring will be based on the resiliency of the assigned systems to attacks from the Red Team, and the maintaining of "up-time" for the infrastructure. After Round 3 the Grand Winner is announced.

Teams

Participant is either an Individual person or a Team of up to a maximum of 3 contestants. The teams can be formed on any stage before Round 1. However, it is important to note that only qualified contestants (i.e. Top 150 individuals) can take part in Round 1 and 2. As such, teams need to make their own judgement and decisions in team formation. We also suggest to interested contestants that they should form teams only AFTER the results of Round 0.

Challenges

Challenges for the competition are from different areas of cybersecurity related with Web Application Security Risks, Applied Cryptography, Cryptanalysis, Reverse Engineering, Digital Forensics, Steganography, and Network Dump Analysis.

Trainings

On 13th July, organizers provide free-of-charge training for Master Class (Top 150) participants. Training sessions will be recorded as online video tutorials and provide relevant information for the preparation of the NZ Cyber Security Challenge.

Tutorials will be available from the Day1 of the Challenge and can be studied ay any convenient location and time.

Workshops

In 2018, the Women in Cyber Security Workshop (WICSW) will be organized on Day 1 of the Challenge. Everyone registered for this Workshop will be invited on campus regardless Round 0 qualification. Note that the Women in Cyber Security Workshop is separate career-focused event open only to women (of all ages). If a woman registered for the WICSW would like to participate in the main NZ Cyber Security Challenge, she should still need to register for the main challenge and get qualified through Round 0 as part of the Master Class (Top 150).

Grants

Thanks to our kind sponsors, we have 10 individual grants for people who travel to the competition from further NZ locations. The Grants will be at the value of NZ$250 as a reimbursement for their travelling expenses (after verification of receipts). All other costs above $250 will be be paid by the grant awardee.

Sponsorship

The NZ Cyber Security Challenge is a fully not-for-profit event. All costs are covered by sponsors introduced on the home page of our web site cybersecuritychallenge.org.nz

All received sponsorship are distributed among NZCSC expenses such as t-shirts, prizes, travelling grants, food, and the promotion of challenge.

Prizes

All the prizes are indicated in New Zealand Dollars.

Grand Winner (Winner of the competition after Round 3) - $2550

Rounds 1 and 2(Winner for Round 1 and 2 in every category: Secondary, Tertiary, Open) - $2100

Runners-Up(Winner for Round 1 and 2 in every category: Secondary, Tertiary, Open) - $810

Challenges Rewards

Easy and medium complexity challenges

$20 per challenge in cash

Hard challenges

$50 per challenge in cash

Women in Cyber Security Workshop Technical Competition

Winner in in every category: Secondary, Tertiary, Open

$700

Runners-Up in every category: Secondary, Tertiary, Open

$270

Drone challenge

The prize either the physical real drone or 3D model of the drone.

Behaviour

Behaviour is regulated by the Ethics Agreement and Code of Conduct. These documents are published on the web site and all participants must agree to these documents before they are allowed to take part. The Ethics Agreement will be signed on campus by every participant during the registration process prior to Round 1.