Cybersecurity Tournament

for students in information/cyber security

Introduction

The Cybersecurity Tournament is a group of arenas where participants are challenged by the arena's organizer (such as a cybersecurity or telecommunication company) in the field of cybersecurity. It is an opportunity to allow students, practitioners and companies active in cybersecurity to meet and learn about one another by challenging each other. It is an opportunity for a company to display their expertise, what challenges could await students if they were to join the company, etc. and vice versa.

General structure

Arenas

- The tournament is made out of several "arenas" which are organized by partners.
    - Each arena is managed by a partner.
    - The partner prepares challenges, makes them available during the tournament, keeps the scores and publishes the score for their arena at the end of the tournament.
    - Based on these scores, a winner is decided for the arena. The winners of an arena are getting prizes.
    - The first places in each arena provide points to each participants that produce an overall winner of the Tournament. The winners of the tournament are getting prizes.
- An arena is therefore a collection of challenges created, setup and maintained by a partner and made available to the participants over a period of time (1 day, several weeks, ...).
- The bundle of these arenas is called the Tournament. It is therefore a sort of "Cybersecurity Olympic's game" where each game allows participants to earn medals and the winner of the Olympics is the participants with the largest amount of medals.

Types of arenas

Topics

We are interested in arena aiming at all the topics pertaining to cybersecurity practices including but not limited to penetration testing, forensics, cryptography, reverse engineering, social engineering, ... (see also topics in: https://masterincybersecurity.ulb.ac.be/).

Examples of types

The tournament is not a "CTF" ("Capture The Flag") only event. Different arenas will have different forms such as, but not limited to:

- **Capture The Flag (CTF)** where typically students are offered a series puzzle(s) or a target and must recover a piece of information,
    -

    - "Keep it real": The "puzzles" we are most interested in are "puzzles"/"enigmas" that could really be part of a professional cybersecurity practitioner's day to day life.
- **Protect The Flag (PTF)** where students are offered a piece of information and a requested to design, setup and deploy a system that delivers certain services while protecting that information,
- **Analyze The Attack/Infrastructure/Problem (ATAIP)** where students
    - are offered some information (architecture design, a puzzle, a piece of software, etc.),
    - are to evaluate that information
    - and will be evaluated by a jury based on the presentation of their analysis.

An arena can be a collection of challenges such as a suite of 20 challenges in order of increasing difficulty but others types are welcome as well. Some partners did organize in the past complete one day tournaments as their arena and other could consider building a single large challenge such as a real infrastructure to penetrate or secure. In such cases, we are welcoming partners that try to design their challenge while including checkpoints that can be measured in order to attribute points to prevent an "all or nothing situation". However, priority is given to realistic aspects of challenges, and such "all or nothing" situations are also part of the day to day life of a cybersecurity practitioner. Therefore, these are also acceptable.

Management of an arena

- An arena can be team based, individual or mixed as decided by the partner managing that arena.
- CTFs are often more easy to organize as they can be managed and evaluated with a classical "submit the flag" website.
- PTFs can be evaluated with the same "submit the flag website" (except each team should host his own regarding their infrastructure) but usually require more ressources to host the infrastructure that is defended by each team.
    - Example:
        - A partner could set-up a server with a barebone hypervisor (called "physical hypervisor");
        - The master hypervisor could host several virtual hypervisors;
        - The arena could start with:
            - These virtual hypervisors hosting a predefined IT infrastructure;
            - The virtual hypervisors not being connected one to another;
        - The arena could be in 2 phases:
            - Phase 1: hardening, preparing the defences. During this phase, participants are not allowed to attack each other nor to be attacked by the partner. They are using their time to set-up controls and defense mechanisms.
            - Phase 2: the infrastructure hosted on virtual hypervisors are made available from one another or from any participants through a VPN and can be attacked.
- ATAIPs are usually evaluated by a jury. They often do:
    - not require much of a physical IT infrastructure (description of the arena can be sent by mail).
    - require to be evaluated in person by a jury.
    - require to find a time and place to gather the jury and the participants.
    - allow for more flexibility as to what is evaluated to choose the winner (such as originality or best demonstration of the understanding of the underlying principles of the solution).

Registration

Partners & Sponsors

By email, see section "Person of contact" below.

Participants

Via online form. The purpose is to count and help participants identification. This helps selecting the appropriate rooms and times for the different events as well as keep score and distribute prizes.

Target audience

This tournament is organized firstly to challenge our first and second year students in cybersecurity. We have not made participation mandatory for any of the students below.

1st year MA/SB cybersecurity students

These students include student that are in the "first year" ("Bloc 1" or "Bridge year") in the master in cybersecurity organized by ERM/RMA, HE2B/ESI, HELB, UCL, ULB, University Namur (alphabetical order) as well as the students in information security at HE2B/ESI. All of these students already have a bachelor (most of the time, either in engineering or ICT). Lots of those students

- have courses on the various campuses throughout the week;
- might have a job during the day, in particular in the specialization in infosec at HE2B/ESI;
- started studying cybersecurity in a academic environment in September. The number of participants from this category should typically not exceed 60 students.

2nd year MA cybersecurity students

These students include student that are in the "second year" ("Bloc 2") in the master in cybersecurity organized by ERM/RMA, HE2B/ESI, HELB, UCL, ULB, University Namur (alphabetical order). Lots of those students:

- have courses on the various campuses throughout the week;
- have studied cybersecurity for at least one year;
- have already performed an internship in cybersecurity of 10 weeks. The number of participants from this category should typically not exceed 30 students.

Dedicated arenas for 2nd year students

We are most interested in arenas dedicated to these students where participants have to adopt a defensive, preventive, ... stance.

Other students

Students from the 6 institutions ERM/RMA, HE2B/ESI, HELB, UCL, ULB and University Namur (alphabetical order) will be invited to participate to the tournament. We are also considering inviting students from other institutions such as VUB since their students expressed such a desire in 2016-2017. Lots of those students:

- have courses on the various campuses throughout the week;

This would be the first year during which these participants will be invited. Therefore, the number of participants from this category is completely unknown. A not really well-informed guess could be: "at most 30 participants".

Type of arenas

We are inviting partners to provide different types of arenas to challenge participants on various topics, various skills and experiences. For instance, we are welcoming more attacks/find the weakness types of challenge for students in first year and to require more of a defensive/real-world/white hat/cybersecurity officer for second year students arenas. Combination of both are also welcome.

How to combine?

A possible approach to combine both approach could be to design an arena that serves both as a CTF and PTF respectively for first and second year students. To further the example, one could consider offering 2nd year students access to an infrastructure as described in section "Types of arenas" (with physical and virtual hypervisors) for two weeks, in order to give them the opportunity to setup defence for their IT services and then allow first year students to try and penetrate those infrastructure during the two following and remaining weeks of the Tournament.

Restricted audience

An arena can be labelled as targeted towards 1st year, 2nd year or any year students. Such a label simply means that these students will have a higher priority for that arena. For example, if only 50 students can participate to an arena, students from the targeted audience will have priority to these spots. Same goes in case of scheduling conflicts.

Partnerships: What are we looking for?

Partners to organize an arena

We are welcoming companies that are willing to organize, deploy and manage an arena as described in this document.

Partners to provide resources

We are welcoming companies that have resources to give or share to help organizing such an event. Such resources could be, but are not limited to:

- "time and skills", if the company wishes to provide coaches for the different teams as long as all the teams are provided with equal support and do provide that support in due time and that coaches are limiting their participation to coaching (and not solving challenges).
- "hardware/software", of any type. Firewalls, VPN boxes, switches, servers with large amount of RAM, licences for software, etc. as long as the partner understands that this is an academic cybersecurity tournament. Therefore, we do not have dedicated resources to manage and protect these elements. Hence, we are feeling more comfortable receiving hardware that holds "no value" anymore to the partner. That way, we will not be afraid that they might get damaged or worse during the event.
- "rooms". It could happen that we have a shortage of rooms with enough Internet bandwidth and electricity during the challenge. In particular if participation rate for a single day arena reaches 50 people. A partner offering such a resources, if guaranteed and stable, could help remove "first come first served" restriction upon certain events.

Partners to provide puzzles

We are currently working on the deployment of a platform that should host an arena consisting of challenges/puzzles that are not managed by a partner. This would allow us to accept submission of puzzles by researchers, freelance cybersecurity practitioners, etc. that do not have the capacity to host their own arena.

Sponsors to provide prizes

The point of the tournament is not to provide prizes. Which is why we are mainly looking for partners. Nonetheless, these are quite good incentive and since participation is not mandatory, we feel they are more than relevant to give the little nutch required to boost motivation and have a large participation. Therefore, if your company would like to support the Tournament but does not have the resources to organize an arena, you are more than welcome to sponsor it with prizes for participants or gifts that can help organizing the event (such as giving away network equipment, servers, etc.).

Duration, Time, Date, Schedule

Preparation

- To ensure the correct launch of the tournament on the first of February, we will have to require that everything is to be ready at the latest on the **first of January**.
    - This include full description of every arena, availability of any required material, website and prizes. We need to be able to announce the full content of the Tournament (every arena, prize, rules of engagement, etc.) before it starts. This is the reason why we are also asking for the prizes to be delivered to the person of contact before that date. This ensure that we can guarantee availability of the prize on the celebration ceremony.
- Announcements will be made before January and right before tournament's launch. We will try not to contact the participants during the first weeks of January as most of them are in exams.

The Tournament

- The Tournament will be held during the month of February. No arena shall be opened before the first of February and all the results will be provided before the end of February.
- The Tournament is not a single day event. However, an arena within the Tournament could be.
    - These are harder to organize because they require to solicit participants during a specific time frame.
    - These are often also harder to organize because they might require to regroup all participants in the same location.
    - Therefore, as a start, organizing the arena in such a matter makes it harder to prevent conflicts with the courses schedule.
- If an arena is only open during 24 or 48 hours, please consider opening the arena during the week-ends.
- If an arena requires to regroup all the participants in a single place at the same time, then we strongly invite arenas to be organized and organizable from 18:00 PM to 22:00 PM.

The celebration ceremony

At the end of the Tournament, we will host a ceremony to thank all the partners and the participant for their contribution to this event as well as distribute the prizes. The exact time, date and location are not known yet as it will depend on course schedule, number of participants, etc. Nonetheless, we expect to host this event in the week that includes the first days of March.

Location

The Tournament

- In the past, most of the arenas were made available online. These are the easiest to setup and provide 24/7 participants access to. Therefore, it is the form we recommend for most arenas.
- Nonetheless, some arenas can be organized around a particular geographical spot or in a single room if required. Please, make sure to discuss this with the person of contact to ensure students availability or room availability if you are unable to provide one.

The Ceremony

In 2016-2017, the ceremony was held at ESI in Brussels: 67 Rue royale, 1000 Brussels, Belgium. We expect to do the same for future iteration of the Tournament.

Scoring system

- Participants earn points in arenas ("Arena points"). These "Arena points" allow to produce an "Arena Ranking" and thus to declare an "Arena Winner".
- Based on the "Arena Ranking", participants collect "Tournament points". These "Tournament points" allow to produce a "Tournament Ranking" and thus to declare a "Tournament Winner".
- Making a distinction between "Arena points" and "Tournament points" allows the partners to distribute points and decide on a scale for their "scoring system" as they see fit. One arena can provide 1 point per challenge and have 20 of them, another can have 40 challenges for 100 points each and another can have a single very big "all or nothing" challenge with not arena points. As long as all these arenas are producing an "Arena Ranking", it is fine.

Per challenge

- The organizer of an arena will be the one deciding when and if a challenge is solved by a participant or team.
- Since the partner is deciding upon the scoring system in their arena, they are responsible for providing the same prizes to all participants in case of equal score.

NOT Time-based

- We are less interested in arenas where the winner is decided based on how fast the arena's challenge(s) was solved.
- From an academic point of view, we want students to:
    - keep investing themselves in their other learning activities,
    - manage their time and effort throughout the month,
    - take their time and try to understand why a solution was effective versus a particular problem presented in an arena.
- Also, time should not be an important factor in particular seeing that they will be several arenas open at the same time. Winning points in an arena should not be equivalent to losing point in another because of time.

- Therefore, one should design an arena with this objective in mind. We are less interested in arenas made of "20 easy puzzles" where the winner is simply the fastest participant. We are more interested in 20-30 puzzles where most participants will be able to solve 50% of them during the tournament's duration, only a few will solve 75% of them and maybe none will solve the rest as they are deemed
    - to be realistic and valid for a cybersecurity practitioner
    - but maybe too hard for a non-experienced participants to solve.
- Cases such as a one-day arena based on Incident Response simulating the real world importance of time as a decisive factor could obviously be an exception.

Per arena (Arena Points/Ranking)

- The organizer decides how many points each challenge/enigma/puzzle provides.
- The organizer produces a ranking based on those points.
- Participants with equal ranking in a challenge will receive equal points added to their score in an arena.
- The participant to the arena that obtained the most "Arena points" is declared the winner of the arena.

For the whole tournament (Tournament Points/Ranking)

- If an arena is team-based, each member of the first, second and third ranking team will respectively receive three, two and one point.
- If an arena is solo, the five first participants will receive five, four, three, two and one point respectively starting from the first to the fifth.
- Participants with equal ranking in an arena will receive equal points added to their score in the Tournament.

Prizes

We are asking partners to provide prizes for their "Arena winner(s)" as well as for the "Tournament winner(s)".

Arena prizes

- Since there is an "Arena Ranking", we would like the partner managing that arena to provide prizes for the winners of that arena.
- Examples:
    - partner X decides to offer the following book(s) to all 5 first ranked participants to the its arena.
- If a partner decides his arena to be team based, that partner should be prepared to distribute prizes suitable for a team (where all team members receive the same prize).

Tournament prizes

- Examples:
    - partner X decides to offer the following book(s) to all 5 first ranked participants to the Tournament.
    - partner Y decides to offer the the "Tournament Winner" for him to join his company for their participation to the Chaos Computer Congress.
    - partner Z decides to offer Raspberry Pis to the all 3 first ranked participants to the Tournament.
- Please make sure you can provide those prizes and, in case of large prizes that you cannot afford to duplicate, explicitly detail what should happen in case of equal score between participants.
- Academic staff will deliver a certificate of accomplishment to the winner of the Tournament.

Organisation gifts

- We welcome any gifts that you think might be useful for the organization of future Tournament or Courses that students participate to. These are most welcomed, help our motivation but are absolutely not mandatory.

Suggestions

Books

- There are quite a lot of interesting books published by No Starch Press https://www.nostarch.com/ see: https://www.nostarch.com/catalog/security
- Another source of inspiration could be: http://dfir.org/?q=node/8
- Mc Graw Hill publishes quite a few books in computer security certification https://www.mhprofessional.com/
- See also suggestion by the GIAC advisory https://www.sans.edu/cyber-research/book-reviews/article/security-books-best
- Subscription to infosec/cybersecurity magazines such as MISC. https://www.miscmag.com/

Entrance tickets

- To conferences and events such as, but not limited to: BruCon, NuitDuHack, HackInTheBox, hack.lu, SHA2018, Computer Chaos Congress, Black Hat, Defcon, ...
- Please consider supporting the travel expenses too when these events are abroad. Otherwise, offering a ticket might be a gift that no students or even academics could enjoy.

Cybersecurity tools: hardware, software, ...

- Licence, software, online services
  - Licence to security tools, VPNs, webservices, operating systems, hypervisors, IDS/Firewall subscription (Snort, PFSense Gold, ...), Antivirus solutions, etc.
- Harware
  - Any IT hardware (since lots of the work is made using regular machine, hard drives etc.)
  - Alternative computing platforms
    - Utilite
    - TrimSlice
    - Chromebooks
    - SolidRun - CuBox
    - Raspberry Pi
    - HardKernel - ODROID
    - Beaglebone Black
    - USBArmory by InversePath
    - FriendlyARM
    - BananaPi
    - Nexus / OnePlus device for NetHunter
    - ...
  - Small tools/devices
    - Cheap Logic analyzer (aliexpress)
    - Alpha Antenna
    - Lockpicking set
    - SDR receiver
    -

    - RFID reader
    - Hardware write blocker
    - ZM-VE400
    - Verbatim Store 'n' Go® Secure Pro
    - USB-G https://globotron.nz/
    - Network devices (switches, access points, etc.)
    - Firewall/Network security platforms (such as APU2C4, APU3A4 https://www.pcengines.ch/apu2.htm)
    - YubiKey
    - OpenCL/Cuda compatible graphic cards for cryptographic computations (Nvidia, AMD)
    - TL-WN722N
    - TL WR710N
    - Micro SD cards and accessories for RPi
    - ...
  - Target platforms
    - Mobile devices (android phone/tablet, ...) to train on at home
    - Small hypervisors to use as mini-labs Intel NUC Kit NUC6i7KYK
    - ...

Publicity

In 2017, during the first Tournament, we made the following announcements mentioning partners, their contribution, logos, etc.:

- the Tournament was publicly announced on: https://masterincybersecurity.ulb.ac.be/tournament.html; (the page is currently still up. In a few days, I'll archive it to prepare for the 2017-2018 Tournament)
- Press releases were sent to the PR department of both ULB and HE2B for public release;
- students were regularly kept informed of the progress of partners on their arenas;
- partners were invited to the ceremony were logos of their companies were displayed.

If you would like to be mentioned associated to this event, we will require of you to send us a written document asking us (and thus allowing us) to do so and to provide us with the material (logos, etc.) that you would like us to try to make us of (such as on the webpage etc.). That way, the material that is being displayed is the one you chose. However, we will ask of you to send us only vectorial (SVG files) or high definition logos/picture to ensure a clean layout of the communication.

Person of contact

If you are interested and/or have any question regarding the Tournament, feel free to contact by email the person below. Please mention "Cybersecurity Tournament 2017-2018" as well as your question in your email title.

Dr. Jérôme Dossogne
http://esi-bru.be - http://qualsec.ulb.ac.be
Haute École Bruxelles-Brabant École Supérieure D'Informatique - Université Libre de Bruxelles
jdossogne@he2b.be - jdossogn@ulb.ac.be