ITX8220/8221 - Special Course in Cyber Security I

Last update: 02 Feb 2017 10:00

1. Main Parameters

The main parameters of the course are the following:

- course code: ITX8220/ITX8221
- subject title: Special Course in Digital Forensic I & II
- course volume CP: 2.0
- ECTS credits: 3.00
- assessment form: pass/fail assessment
- topic: Cyber Defence Exercise Locked Shields 2017

2. Limitations

This course is open only for students who have citizenship of a NATO Nation.

3. Schedule

Date	Time	Location	Event
13 Feb 2017	18.00-20.30	ICT-315	**Kick-Off Meeting** LS background. Skills mapping. Roles and assembling the Test Run Blue Team
27 Feb 2017	18.00-19.30	ICT-315	**Teams progress review** Status of preparations. Experience from last year Blue Team leader(s).
TBD by team leads	TBD by team leads	TBD by team leads	**Team Meetings**
15-16 Mar 2017	**FULL DAY**	TBD by team leads	**Preparation day and Test Run**
25-27 Apr 2017	**FULL DAY**	Swisshotel Tallinn	**Execution**

The students are expected to attend all the events.
Preparatory meetings could be excused for a good reason. Non-attendance of Test Run and Execution will be in general not excused.

4. Background

Locked Shields (LS) is an international technical cyber defence exercise organized by NATO Cooperative Cyber Defence Centre of Excellence together with several partners. During the execution, 20 Blue Teams have to defend virtual network infrastructure against the attacks of the Red Team.
Locked Shields 2017 (LS17) will be executed on 25-27 Apr 2017.
There are two main events when the actual gameplay takes place:

1. Preparation Day and Test Run (15-16 Mar 2017)

Test Run is a gameplay with limited scale and objectives. The main goals are to find issues in the technical infrastructure, prepare the Red Team members for the main run, train the students, and test how the reporting channels and scoring system works.
Test Run will last 2 days:

- 1 day for Red Team/Blue Team preparations (**15 Mar 2017**)
- Student teams will get full access to the systems they have to protect next day against Red Team attacks
- 1 day for the game-play (**16 Mar 2017**)

The Blue Team slots are **open to the students**.
Test Run Blue Teams are assembled from the students of Tallinn University of Technology, Hungarian National University of Public Services, Siemens Germany and members from Finnish non-profit Internet Users Association (KAPSI).

2. Execution (25-27 Apr 2017)

This is the full-scale gameplay. The Blue Teams attending the Execution are composed of IT security professionals coming from military units, other governmental elements and private sector of CCDCOE sponsoring nations. Due to limited number of slots it is not possible to provide the students an option to participate as Blue Team members. Course participants are expected to support the White Team. Day 0 (25 Apr) is for preparations, Day1-Day2 (26+27 Apr) for gaming and Day3 (28 Apr) for hot-wash. Participating the Day3 host-wash session is not mandatory for the students.

5. Course Objectives

The objectives of the course are following:

1. Provide the students a practical experience in assembling a defensive team and preparing a defensive campaign according to exercise scenario. This will be accomplished by engaging the students into the Blue Teams of LS16 Test Run.

- The role of the Blue Teams is to act as cyber rapid reaction teams. The students will get preliminary information about the networks they have to defend, and access for one day before the game starts.
- The majority of work has to be done before the Test Run. Participating in briefings and team meetings, familiarizing with the documentation and individual research is required in order to
    - assign the roles inside the team
    - create a plan
    - select, learn, prepare and test technologies (e.g. Blue Teams can prepare their own virtual machines that could be plugged into the exercise environment)
- Note that Test Run exercise networks are not fully completed – some systems will be missing and some provide only limited functionality.

2. Provide the students an experience in responding to full-scale cyber attack campaign by tasking them to protect exercise networks during one day lasting attack campaign
    - The teams will be overloaded with attacks and other tasks to test their ability to handle stressful situation.
    - The exercise will provide the students an opportunity to test their skills in several areas such as:
      a. learning to know their network
      b. system administration, hardening and prevention of attacks
      c. network monitoring, detecting and responding to attacks
      d. handling cyber incidents
      e. teamwork
      f. reporting and crisis communication
      g. information sharing, cooperation and collective defence
    - Feedback will be provided by the means of automatic and manual scoring
    - Blue Teams will be competing with each other. It is a good opportunity to compare your skills with other universities and team of volunteers assembled from professionals (kapsi.fi and Siemens).

3. Use the help of the students to run LS17. Provide the students insight how technical cyber defence exercises are organized. The students will be engaged into the White Team after the Test Run.
    - The role of the White Team is to control the Game, evaluate the progress of the teams, ensure proper communication between participants, simulate management, media, user activities, etc.
    - During the execution the students will be supporting the LS16 organizers in simulating the activities of ordinary users. Students will be part of traffic and user simulation subteam.
    - Student's tasks in White Team include:
    - Accessing Blue Team workstations as the users and closely cooperating with the client-side subteam of the Red Team. Students have to browse on the sites which may include malicious content, open e-mail attachments and executables crafted by the Red Team members, provide feedback of observed actions, report about availability and usability issues (Blue Teams have locked the users out, workstations have been rendered useless by installing many AV programs) and assign negative scores in case the reported issues are not fixed.
    - Conducting functionality checks of Blue Team systems to ensure the applied protection mechanisms are in accordance to the Exercise rules – Blue Teams are no allowed to break the functionality.

6. Course Outline

The students are expected to take part of the following activities:

1. Participating in the kick-off session: 3x45 min (**13 Feb 2017 18:00-21:00 @ ICT-315**)
    a. Providing overview of LS exercises
    b. Introducing the required commitment
    c. Dividing the interested students into the teams
    d. Initial assignment of roles (team leader, deputy leader, administrators of specific systems, incident handlers, etc)
2. Participating in team progress review meeting: Tentatively 27 Feb 2017 18.00 -19:30@ICT-315

3. Participating in team meetings (TBD by team): 2x90 min minimum
    a. It is up to the team leaders to decide how many internal team meetings they will conduct. Remote participation is accepted but not discouraged.
    b. At minimum 2 meetings are recommended.

4. Individual preparation work
    a. Preparing the defence plan
    b. Familiarizing with the exercise documentation (Scenario, Rules, Communication Plan, Descriptions of Blue Team systems, Lightweight and Situation Reporting Instructions)
    c. Sharpening the skills in or learning new technologies based on the role in team

5. Participating in the Preparation Day and Test Run of LS17 (15-16 Mar 2017) as Blue Team member: 2 days
   NB! Participation in full day events is mandatory!

6. Participating in the Execution of LS17 (25 – 27 Apr 2017) as White Team member: 3 days
   Students are expected to take part of the preparation day and two actual gaming days.
   NB! Participation in full day events is mandatory!

7. Providing feedback

7. Assessment Criteria

1. Participation in the planning meetings and the following main events of Locked Shields 2017 (LS17) cyber defence exercise.

For passing the course the following items are mandatory:

    a. Active participation in all LS17 Test Run Blue Team planning meetings. There will be 2-3 meetings altogether. Upon agreement with the team leader it is also acceptable to participate remotely (E.g. over Skype or WebEx)
    b. Assigned specific role in the LS17 Test Run Blue Team
    c. Participation in LS17 Test Run (15-16 Mar 2017) as the member of the Blue Team
    d. Participation in LS17 Execution (25-27 Apr 2017) as the member of the White Team

Absences are accepted only in exceptional cases (e.g. if you are ill a doctor certificate will be required) and must be coordinated with course instructor and Test Run Blue Team leader.

2. Individual preparation work and documentation of the results. For passing the course it is mandatory to make preparations for participation in the Test Run Blue Team based on the role of specific student:

    a. Blue Team leader and the deputy leader are responsible for assigning the roles and tasks to team members, and tracking the progress. In addition, they have to prepare the general strategy for the team.
    b. The technical experts are responsible for analysing the system descriptions assigned to them, conducting research and testing potential vulnerabilities and mitigation methods, and writing down the plan of activities for the Test Run.

3. Written report

For passing the course each student must submit a written summary report of activities by 05 May 2017 to the team leads who will provide a combined report to course instructor. Each student has to provide

a. Description of the role in LS17 Test Run Blue Team
b. Documentation of the preparatory work
c. Evaluation of Blue Team activities during the Test Run
d. Feedback based on the participation in the LS17 White Team during the Execution with suggestions how to improve the work of traffic and user simulation sub team

8. Point of Contact

Course coordinator is Olaf Maennel, olaf.maennel@ttu.ee