Timely Feedback in Unstructured Cybersecurity Exercises

Jan Vykopal, Radek Ošlejšek, **Karolína Burská**, Kristína Zákopčanová
vykopal@ics.muni.cz, oslejsek@fi.muni.cz, {**burska|zakopcanova**}**@mail.muni.cz**

February 22, 2018

KYPO

Outline

MASARYK
UNIVERSITY

Introduction

Global shortage of cybersecurity workers with the skills to prevent or respond to cyber
security attacks ->

- **Cyber defence exercises** (CDX)
    - unstructured, step-by-step hands-on trainings
    - enable participants to experience cyber attacks first-hand with real-life limitations
    - intensive, short-term events lasting several days
- ... feedback from these exercises?

Introduction

	Cyber Exercise Score					
Team Name	Services	Attacks	Injects	Users	VNC	Total Score
Blue Team 1	91,843	-8,500	9,000	-1,100	0	**91,243**
Blue Team 5	92,230	-5,000	3,600	-400	0	**90,430**
Blue Team 2	81,280	-10,750	6,425	-4,000	0	**72,955**
Blue Team 4	74,518	-11,000	6,650	0	-4,000	**66,168**
Blue Team 3	85,756	-12,000	2,475	-1,700	-9,500	**65,031**

Figure: A scoring table, the only feedback for the learners

MASARYK
UNIVERSITY

Green Team
- maintain
- repair
- fix

White Team
- rules
- score
- guide

Blue Team
- secure
- monitor
- defense

Red Team
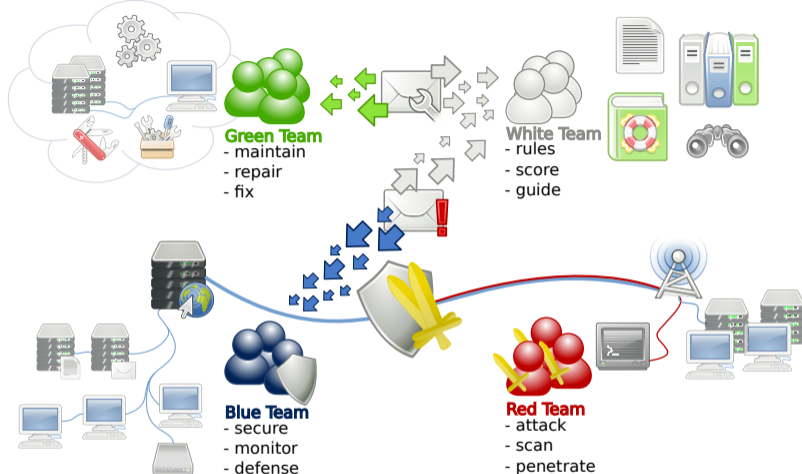- attack
- scan
- penetrate

Figure: Exercise participants, their interactions and tasks.

Exercise Phases

Table: Phases of the exercise with time allocation

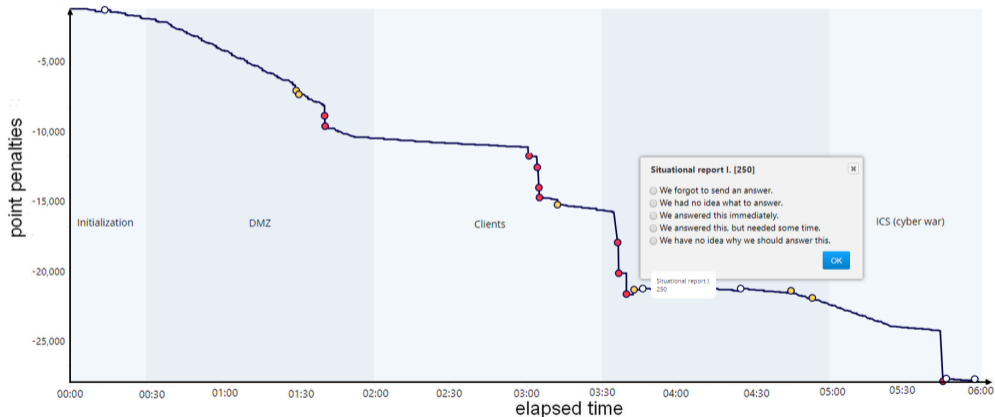| Order	Phase	Duration	Day
1	Exercise familirization	3 hrs	1
2	Actual exercise	6 hrs	2
3	Post-exercise survey	5 mins	2
4	Break	25 mins	2
5	**Scoring timeline interaction**	**10 mins**	**2**
6	**Scoring timeline survey**	**5 mins**	**2**
7	Quick exercise debriefing	15 mins	2

Scoring Timeline

Figure: Scoring timeline providing personalized feedback for each team.

Post-exercise & Scoring Timeline Survey

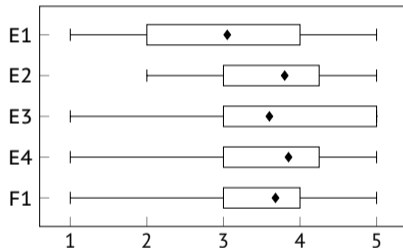|	
E1	My knowledge and skills were sufficient.
E2	I found exercise difficult for me.
E3	Exercise was well organized and structured.
E4	Exercise was beneficial and useful to me.
F1	The scoring timeline of my team displayed after the end of the exercise provided useful feedback.
F2	Do you have any comments on the scoring timeline?

Figure: Answers distribution E1 – E4 and F1.

1 = strongly disagree, 5 = completely agree

MASARYK
UNIVERSITY

Discussion

- **Teams sought out feedback** regardless of their achieved score
- **A need for more detail** according to survey question F2 ("Do you have any comments on the scoring timeline?")
- **Benefits for instructors** which lie in reflection from the learners
- Two **limitations of the study** – small group of participants, simplicity of the timeline evaluation survey

MASARYK
UNIVERSITY

Conclusion

- Motivation – very limited and/or delayed feedback in CDX
    - -> limited opportunity to learn from the mistakes
- Our experiment: an analysis of a simple survey and an interaction with a new tool
- Feedback gathering was automatized; only limited level of detail
- The new feature was valued by learners
- Future work
    - Learners would welcome more detailed feedback
    - Not only show the point gain/loss, but also a comment from the instructor

MASARYK
UNIVERSITY

Any questions?
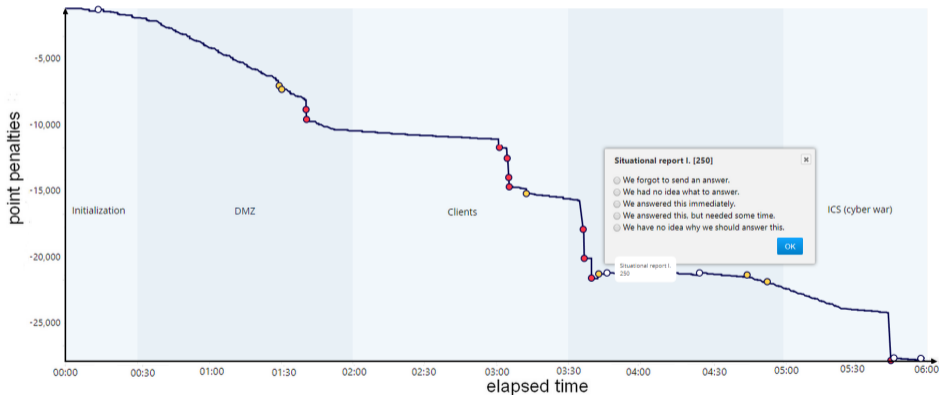
Contact e-mail: **vykopal@ics.muni.cz**, oslejsek@fi.muni.cz, {burska|zakopcanova}@mail.muni.cz