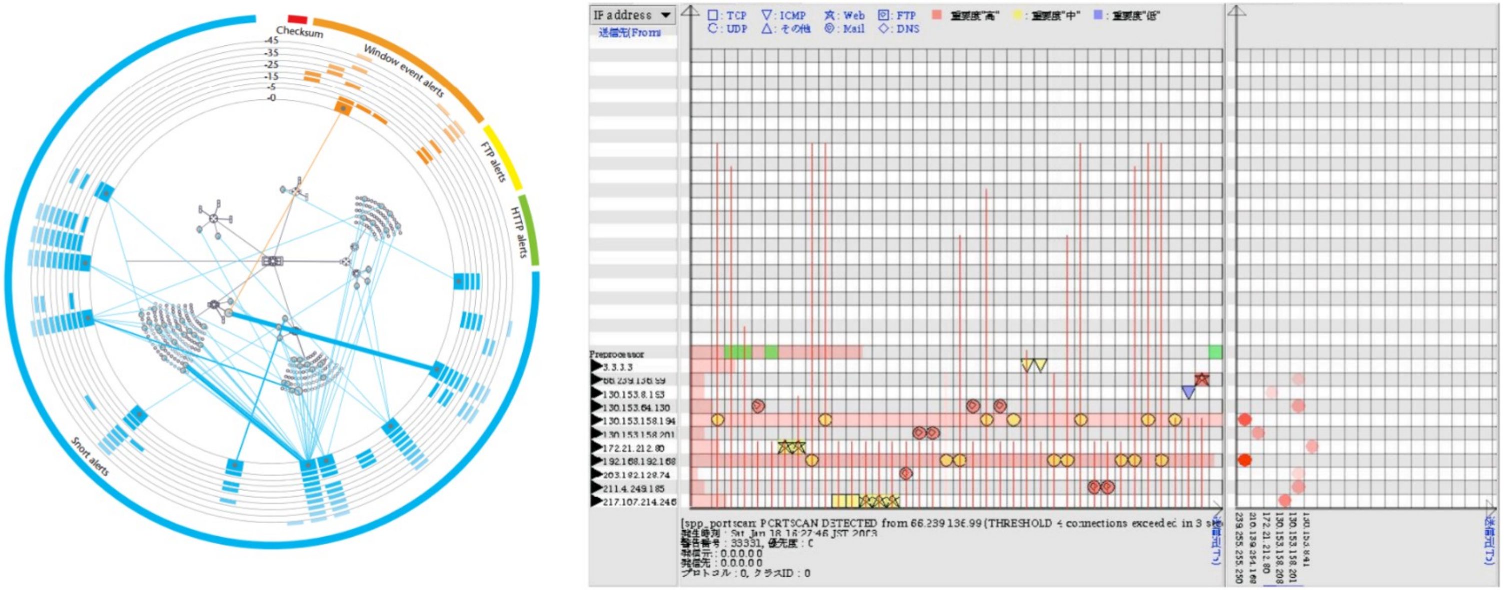
FACULTY
OF INFORMATICS
Masaryk University

Visual Analytics for Cybersecurity
(research preview)

Radek Ošlejšek

Motivation – what is and what is not visual analysis

- Goal: To provide insight into complex data via smart interactive visualizations
- Common design rules, design methodologies concepts, evaluation methodologies, …
- Different application domain (different data) => tight cooperation with domain experts



[spp_portscan: PORTSCAN DETECTED from 66.239.136.99 (THRESHOLD 4 connections exceeded in 3 se
発生時刻 : Sat Jan 18 16:27:46 JST 2003
警告番号 : 33331, 優先度 : 0
発信元 : 0.0.0.0
発信先 : 0.0.0.0
プロトコル : 0, クラスID : 0

Example of alert-based network security visualization.
[Livnat et al. „A Visualization Paradigm for Network Intrusion Detection“, IAW 2005]

Cybersecurity domain

“Applied” cybersecurity

- Detection and mitigation of cyber threats
- Huge domain, intensive research addressing the usage of VA for network analysis, system logs analysis, anomaly detection, etc.

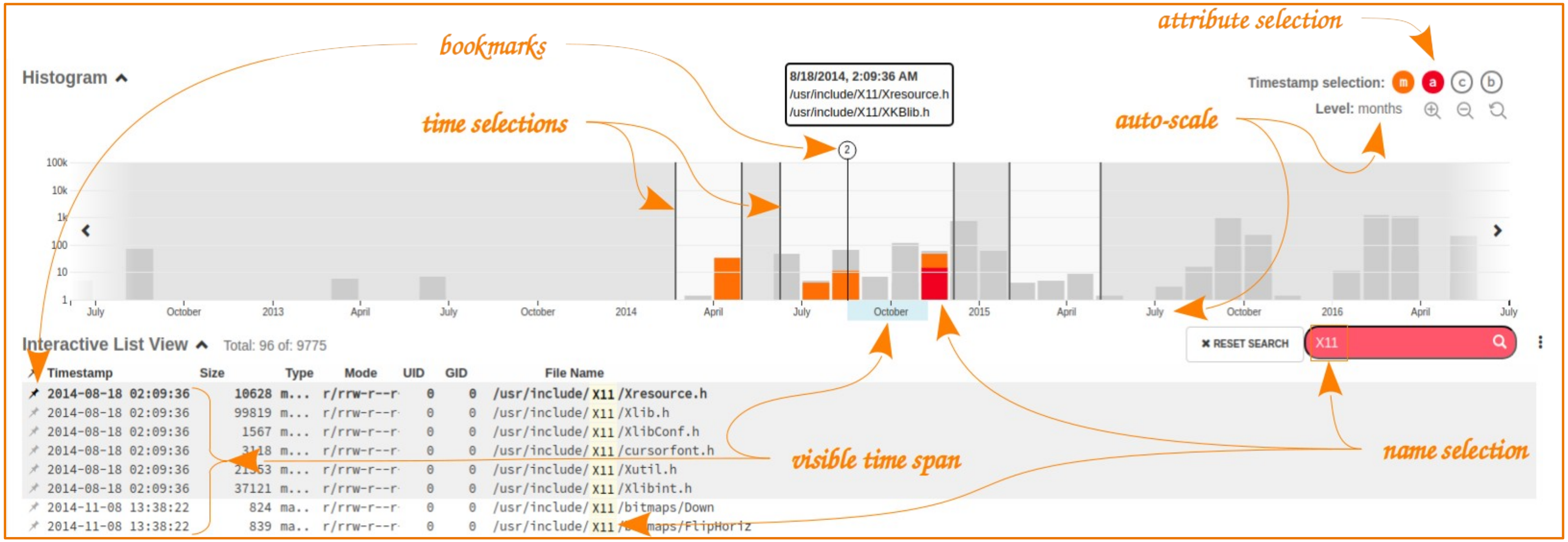
Cybersecurity education and training

- Overlaps with learning analytics
- New domain as it was difficult to organize hands-on training so far.

Applied cybersecurrity – FIMETIS

- Forensic investigation of disks
- Significantly improves the investigation
- Easy to use even for less experienced analysts

video



8/18/2014, 2:09:36 AM
/usr/include/X11/Xresource.h
/usr/include/X11/XKBlib.h

Timestamp selection: m a c b

Level: months

Interactive List View Total: 96 of: 9775

X11

Timestamp	Size	Type	Mode	UID	GID	File Name
2014-08-18 02:09:36	10628	m...	r/rrw-r--r	0	0	/usr/include/X11/Xresource.h
2014-08-18 02:09:36	99819	m...	r/rrw-r--r	0	0	/usr/include/X11/Xlib.h
2014-08-18 02:09:36	1567	m...	r/rrw-r--r	0	0	/usr/include/X11/XlibConf.h
2014-08-18 02:09:36	3118	m...	r/rrw-r--r	0	0	/usr/include/X11/cursorfont.h
2014-08-18 02:09:36	21[illegible]53	m...	r/rrw-r--r	0	0	/usr/include/X11/Xutil.h
2014-08-18 02:09:36	37121	m...	r/rrw-r--r	0	0	/usr/include/X11/Xlibint.h
2014-11-08 13:38:22	824	ma..	r/rrw-r--r	0	0	/usr/include/X11/bitmaps/Down
2014-11-08 13:38:22	839	ma..	r/rrw-r--r	0	0	/usr/include/X11/[illegible]maps/FlipHoriz

BERAN, Martin, František HRDINA, Dan KOUŘIL, Radek OŠLEJŠEK, Kristína Zákopčanová. **Exploratory Analysis of File System Metadata for Rapid Investigation of Security Incidents.** In *IEEE Symposium on Visualization for Cyber Security (VizSec'20).*

Hands-on Cybersecurity Training

Solving practical cybersecurity tasks in computer networks

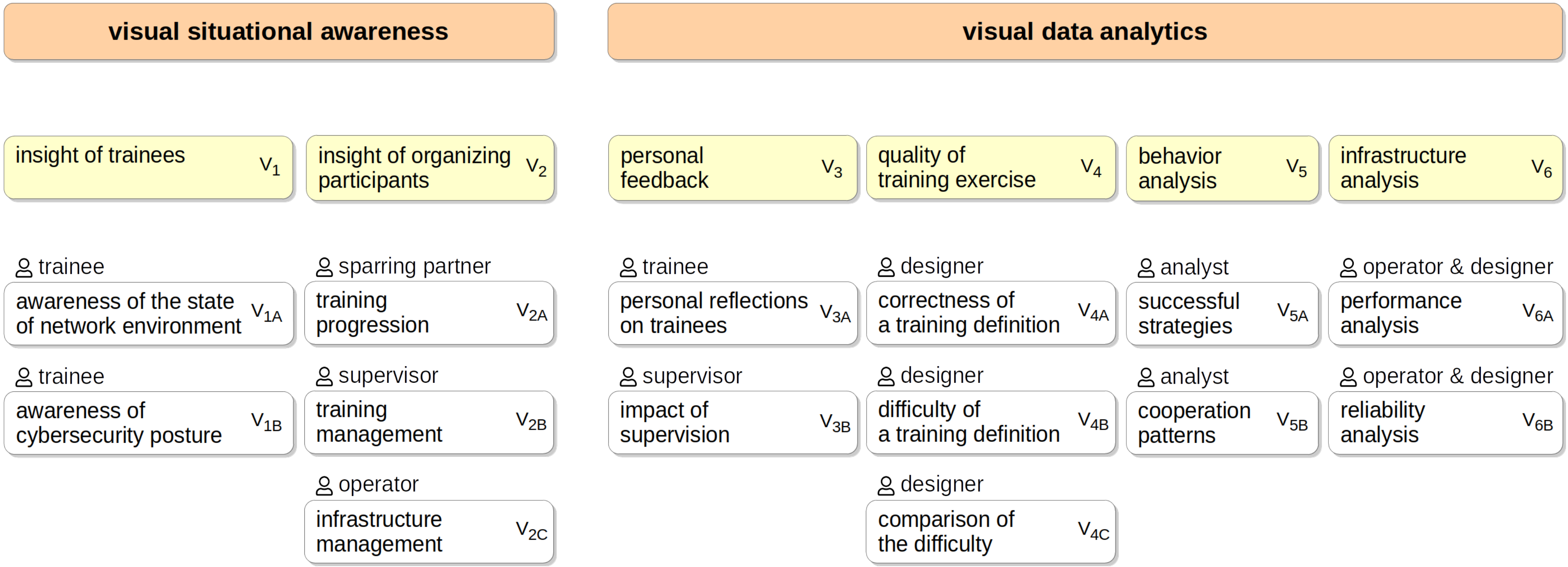
- E.g., scan the network and find vulnerable server, exploit vulnerability, ...
- Focused on higher-order thinking and problem-solving.
- Similar to programming, for instance.

Cybersecurity training is process-oriented and then abstract

- No tangible output like code to be assessed or compared.
- Difficult to check the progress of trainees, troubles during training, etc.

=> **good domain for (visual) analytics**

VA for Hands-on Cybersecurity Training



visual situational awareness

insight of trainees V_1

- trainee: awareness of the state of network environment V_{1A}
- trainee: awareness of cybersecurity posture V_{1B}

insight of organizing participants V_2

- sparring partner: training progression V_{2A}
- supervisor: training management V_{2B}
- operator: infrastructure management V_{2C}

visual data analytics

personal feedback V_3

- trainee: personal reflections on trainees V_{3A}
- supervisor: impact of supervision V_{3B}

quality of training exercise V_4

- designer: correctness of a training definition V_{4A}
- designer: difficulty of a training definition V_{4B}
- designer: comparison of the difficulty V_{4C}

behavior analysis V_5

- analyst: successful strategies V_{5A}
- analyst: cooperation patterns V_{5B}

infrastructure analysis V_6

- operator & designer: performance analysis V_{6A}
- operator & designer: reliability analysis V_{6B}

OŠLEJŠEK, Radek, Vít RUSŇÁK, Karolína DOČKALOVÁ BURSKÁ, Valdemar ŠVÁBENSKÝ, Jan VYKOPAL and Jakub ČEGAN. **Conceptual Model of Visual Analytics for Hands-on Cybersecurity Training.** In *IEEE Transactions on Visualization and Computer Graphics*, 2020.

Insight of trainees

insight of trainees V_1

insight of organizing participants V_2

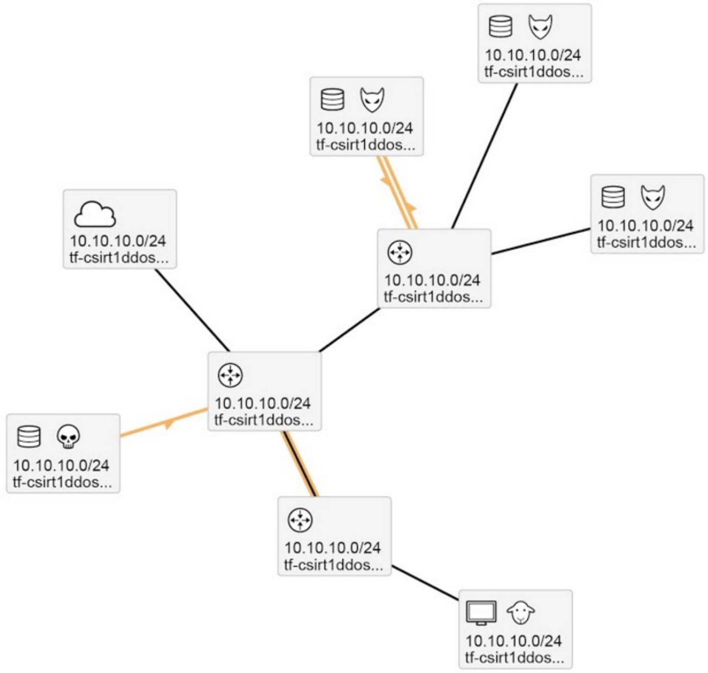
personal feedback V_3

quality of training exercise V_4

behavior analysis V_5

infrastructure analysis V_6

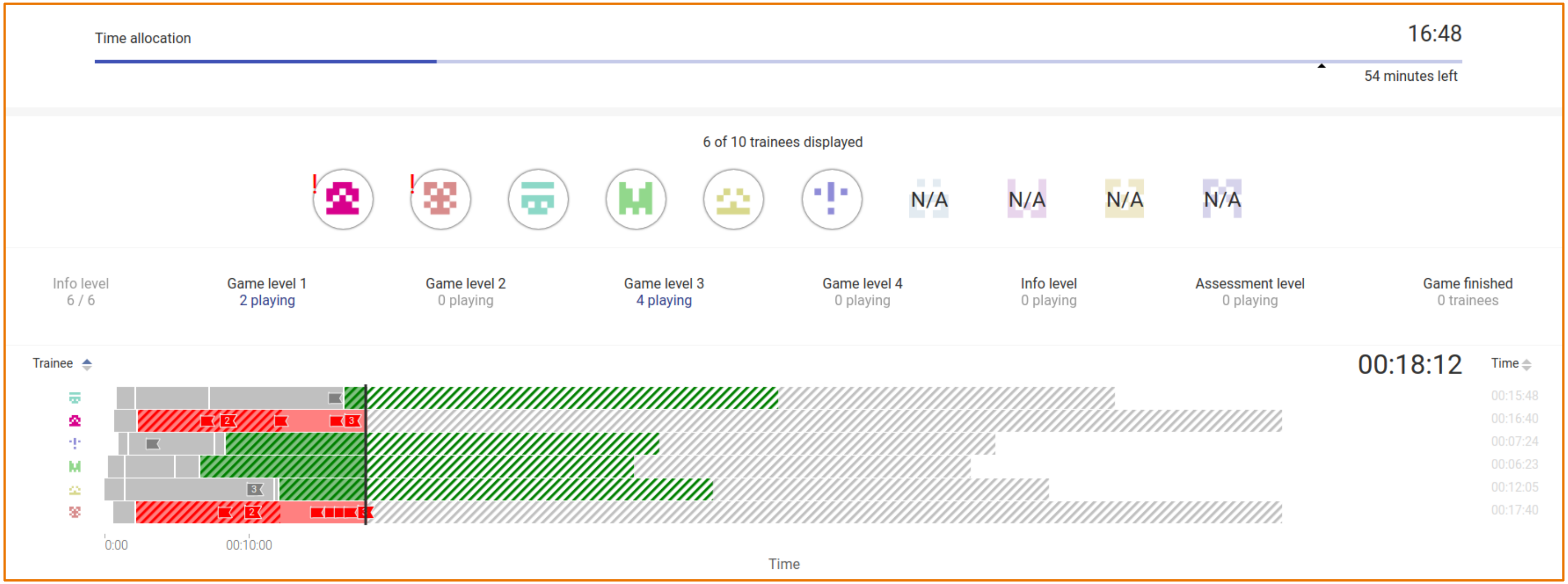
- Is server X under attack?
- Is the host X accessible via SSH?
- What stage of training em I in?
- ...



Insight of organizing participants

insight of trainees V_1 | **insight of organizing participants V_2** | personal feedback V_3 | quality of training exercise V_4 | behavior analysis V_5 | infrastructure analysis V_6

- Which trainees are in troubles?
- Is the training session on schedule or it there some delay?
- Is the underlying infrastructure working properly?

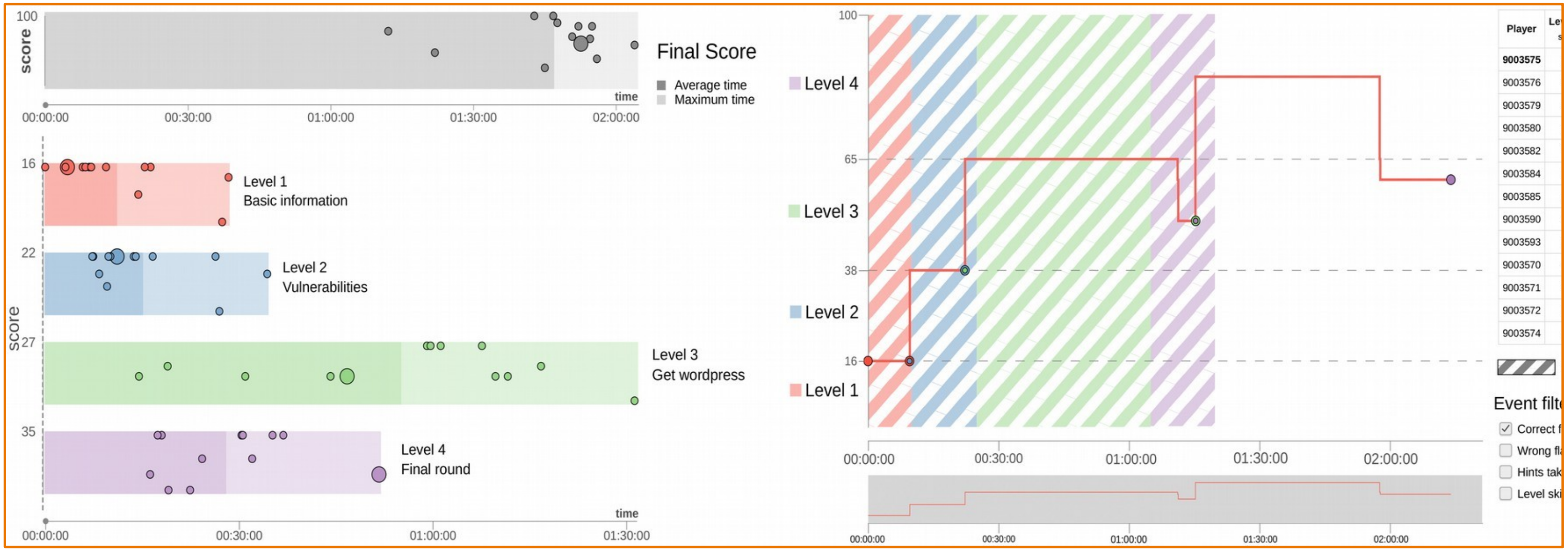


[Burská et al. **Data-driven Insight Into the Puzzle-based Cybersecurity Training**, CHI’21, to be submitted]

Personal feedback

insight of trainees V_1 | insight of organizing participants V_2 | **personal feedback V_3** | quality of training exercise V_4 | behavior analysis V_5 | infrastructure analysis V_6

- [trainee] What did I do wrong in the task X?
- [trainee] Where I lost most points and why?
- [supervisor] Did I intervene in time?



[Ošlejšek et al. **Visual Feedback for Players of Multi-Level Capture the Flag Games: Field Usability Study**, VizSec'20]

Quality of exercise

- Were the teams of trainees well balanced?
- What is the most difficult task in the training?

Quality of exercise & Behavior analysis

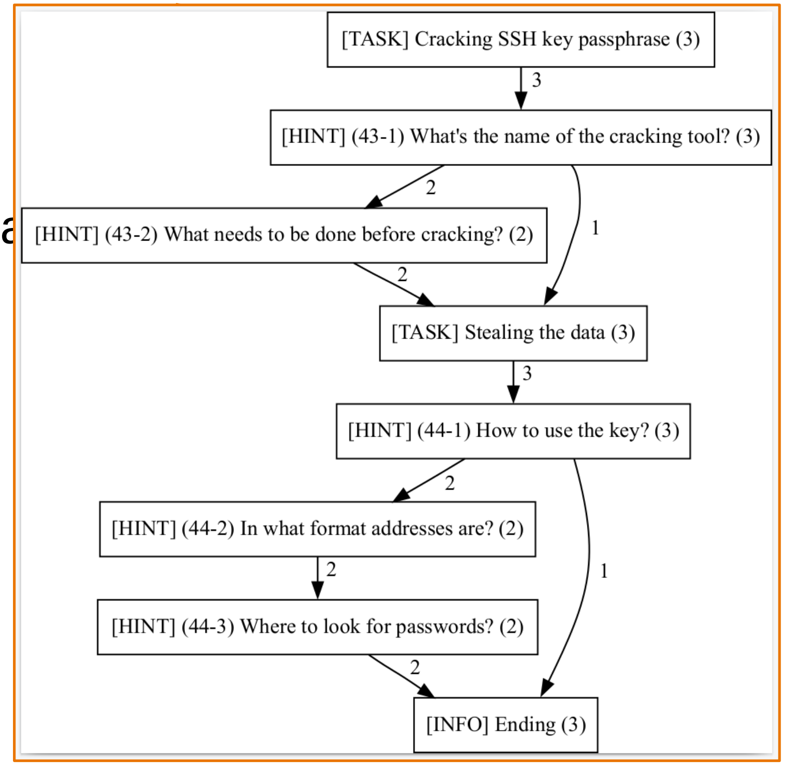
insight of trainees V_1 | insight of organizing participants V_2 | personal feedback V_3 | **quality of training exercise V_4** | **behavior analysis V_5** | infrastructure analysis V_6

- Were the teams of trainees well balanced?
- What is the most difficult task in the training?
- What is the most sufficient strategy of solving tasks?
- Was there some exceptional trainee?

} Process analysis

Quality of exercise & Behavior analysis

- Were the teams of trainees well balanced?
- What is the most difficult task in the training?
- What is the most sufficient strategy of solving ta
- Is there some exceptional trainee?


[TASK] Cracking SSH key passphrase (3)
3
[HINT] (43-1) What's the name of the cracking tool? (3)
2
1
[HINT] (43-2) What needs to be done before cracking? (2)
2
[TASK] Stealing the data (3)
3
[HINT] (44-1) How to use the key? (3)
2
1
[HINT] (44-2) In what format addresses are? (2)
2
[HINT] (44-3) Where to look for passwords? (2)
2
[INFO] Ending (3)

Ongoing research with Martin Macák

Infrastructure analysis

insight of trainees V_1 | insight of organizing participants V_2 | personal feedback V_3 | quality of training exercise V_4 | behavior analysis V_5 | **infrastructure analysis V_6**

- Analytical tasks of operators and maintainer of cyber ranges.

Thank you for your attention!