Toward Guidelines for Designing Cybersecurity Serious Games

Miriam Gáliková, Valdemar Švábenský, Jan Vykopal
Faculty of Informatics, Masaryk University, Czech Republic

Motivation

Hands-on practical training enables deep understanding

No standardized methodology for creating cybersecurity serious games

Creative and engaging learning approach

Goals of the Guidelines

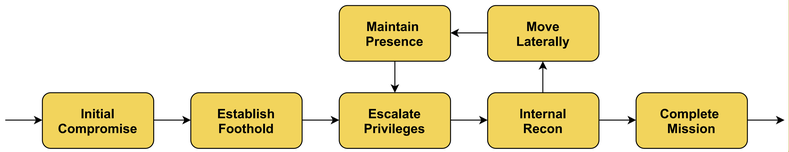
Learning by solving realistic tasks in a game-like structure

Based on proven teaching methods

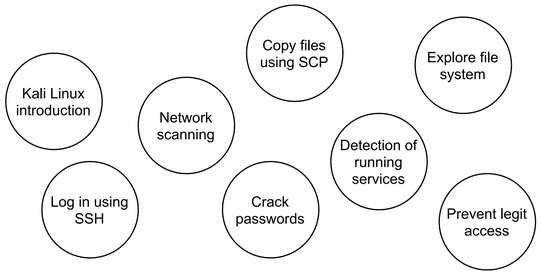
Practical guide for game creators that is easy to follow

Challenge Design

Using the methods, we create games in which the players proceed in steps of the Mandiant's attack lifecycle [1].



Learning Objectives



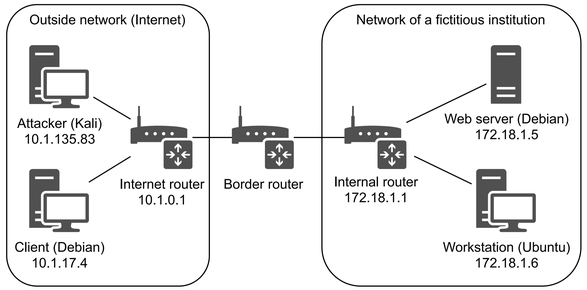
Game Example Task

Level: Looking for the server's IP address

You managed to guess the password on a Wi-Fi router, so you have already accessed the local network of one institution. You also saw the other machines' IP addresses in the router's web UI. There are two machines with IP addresses `172.18.1.5` and `172.18.1.6`. Now, your your goal is to gain access to the server. Since there are two machines in the network, scan the hosts and recognize the server's IP address. You can recognize the server by its running services.

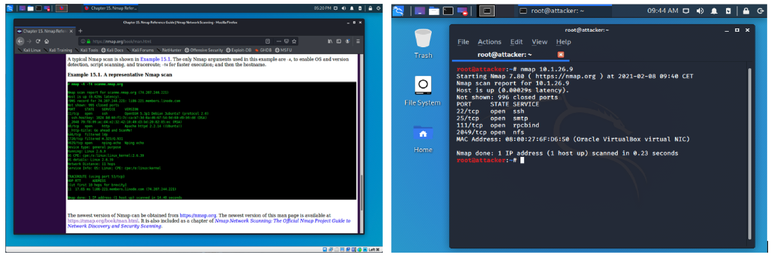
The answer is the port number on which the file sharing service is running on the server's machine.

Game Example Topology



Game Example Environment

Players can interact with the machines in the game network using GUI or terminal.



State of the Art

- Cybersecurity serious games combine proven teaching methods and creative means of cybersecurity education [2].
- Games aim to effectively reproduce real-world security situations that require strategic and adversarial thinking [3].
- While playing the game, players can acquire knowledge from various areas, such as penetration testing, network forensics, or secure coding [4].

Guidelines Aspects

- Learning objectives
- Design of challenges/tasks and their solutions
- Hints and suitable scaffolding
- Gamification elements, such as narrative, players' game identity, injects, special rewards
- Technical environment, testing, and troubleshooting
- Data gathering, privacy, and ethical considerations
- Evaluation and final documentation
- Copyright and game licences
- Rules and anti-cheating policies

References

[1] Mandiant Intelligence Center. "APT1: Exposing one of China's cyber espionage units". In: *Mandian. com* (2013). url: `https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf`.

[2] V. Aleven et al. "Toward a Framework for the Analysis and Design of Educational Games". In: *2010 Third IEEE International Conference on Digital Game and Intelligent Toy Enhanced Learning*. 2010, pp. 69–76.

[3] N. M. Katsantonis et al. "Conceptual Framework for Developing Cyber Security Serious Games". In: *2019 IEEE Global Engineering Education Conference (EDUCON)*. 2019, pp. 872–881.

[4] L. A. Annetta. "The "I's" Have It: A Framework for Serious Educational Game Design". In: *Review of General Psychology* 14.2 (2010), pp. 105–113. doi: `10.1037/a0018985`. url: `https://doi.org/10.1037/a0018985`.

Contact

If you are interested in playing the example cybersecurity game, please contact the author at **galikova@mail.muni.cz**. We would also love to hear your feedback and comments!