HANDS-ON CYBERSECURITY EXERCISES

Jens Mache
Lewis & Clark College, Portland, OR
jmache@lclark.edu

Richard Weiss
The Evergreen State College, Olympia, WA
weissr@evergreen.edu

ABSTRACT

In order to address the cybersecurity education and workforce challenges, we need a greater number of prepared faculty. In this workshop, we will introduce the EDURange framework, present one or two hands-on exercises that faculty can try, and discuss how they can be taught in classes.

OVERVIEW

Student exposure to practical, hands-on exercises is critical for cybersecurity curricula. It helps students internalize concepts taught in class, learn to use cybersecurity tools, and learn critical and adversarial thinking.

EDURange [1, 2, 3, 4] is a cloud-based framework for cybersecurity exercises designed with the following goals: 1) ease-of-use for students and instructors. Scenarios run on VMs that are created automatically in the Cloud. Students don't need special software and can work anywhere with Internet service. Instructors can register their classes, and they can work in groups. It can collect data to make assessment easier. 2) engaging for students and faculty. Students from a variety of backgrounds can learn practical security concepts, tools, and skills in scenarios that gamify realistic challenges. 3) flexibility to use simple scripts to specify exercises at a high level and create variations. This enables instructors to tailor exercises to their specific classes and student backgrounds and continue to modify them in order to minimize risk of students finding the answers online.

In cybersecurity exercises, there is often a delicate balance between guidance and independence [5]. Students following prescriptive "cookbook" instructions are often not learning the analysis skills they need to solve real-world problems, but students given no guidance can flail and learn very little. The scaffolding exercises of EDURange promote a middle ground in which students can receive guidance while they learn essential concepts and skills before they attempt more challenging aspects of the scenario in a more independent fashion. Instructors have the flexibility to use (or not use) the scaffolding in different ways depending on the background of the class. We will present both an introductory exercise that teaches about the command line and a more advanced exercises that introduces malware analysis.

One goal of EDURange is to provide instructors with assessment tools to see in real time how their students are doing and help them identify students who are missing

pieces of the required background. EDURange supports assessment by providing the instructor with the bash histories of each of the students, so that it is possible to identify misconceptions early on in the exercise. EDURange has been instrumented to track user activities in such a way that they're more easily analyzable. This information, including timestamps and exit status for all commands, can be accessed by the instructor at any time. We are experimenting with visualizations of the bash history data that allow an instructor to quickly determine how far students have gotten in a scenario and whether they might need guidance.

ACKNOWLEDGEMENTS

This work was partially supported by National Science Foundation grants 1723705, 1723714, 1516100 and 1516730.

REFERENCES

[1] Weiss, R., Boesen, S., Sullivan, J., Locasto, M.E., Mache, J., Nilsen, E., Teaching cybersecurity analysis skills in the cloud", *Proc. of the 46th ACM Technical Symposium on Computing Science Education (SIGCSE'15*), 2015. http://dx.doi.org/10.1145/2676723.2677290

[2] Weiss, R., Locasto, M.E., Mache, J., A reflective approach to assessing student performance in cybersecurity exercises, *Proc. of the 47th ACM Technical Symposium on Computing Science Education (SIGCSE '16)*, 597-602, 2016. http://dx.doi.org/10.1145/2839509.2844646

[3] Weiss, R., Mache, J., Locasto, M.E., The EDURange framework and a movie-themed exercise in network reconnaissance, *Proceedings of USENIX Security: Advances in Security Education Workshop (ASE),* 2017.

[4] Weiss, R., Turbak, F., Mache, J., Locasto, M. E., Cybersecurity education and assessment in EDURange, in *IEEE Security & Privacy*, 15 (3), 90-95, 2017. http://doi.ieeecomputersociety.org/10.1109/MSP.2017.54

[5] Weiss, R., Turbak, F., Mache, J., Nilsen, E., Locasto, M.E., Finding the balance between guidance and independence in cybersecurity exercises, *USENIX Workshop on Advances in Security Education*, 2016.