Finding the Balance Between Guidance and Independence

Richard Weiss
*The Evergreen State College*

Franklyn Turbak
*Wellesley College*

Jens Mache, Erik Nilsen
*Lewis & Clark College*

Michael E. Locasto
*SRI International*
The Challenge of Cybersecurity Education

- Our goal: develop exercises that teach analysis skills/abilities and the security mindset.
- Having good exercises is half of the battle.
- The other half is providing the context/guidance.
- Clear learning goals are important.
- Prerequisite background: know the audience.
- Formative assessment – any tool that helps to give students timely and helpful feedback (guidance).
- Summative assessment – need to verify that they met the learning goals.
Formative Assessment: Challenges

- Having the right tools: Complete/Accurate
- Large class size
- No TA support
- Limited time
- * Equitable distribution of attention *
An example from network security: suppose these were the goals

- Analyze a large address space
- Explain how ping works and use it
- Use efficient options in nmap
- Understand CIDR addresses
What is wrong with this picture?

1. Click Start in the Search Programs box, type cmd and press ENTER.
2. At the command line type nmap and press ENTER.
   a. observe the output
   b. What version of nmap are you running?
3. At the command line type nmap -sn 192.168.100.0/24 and press ENTER
   a. observe the output
   b. how many hosts did nmap find?

... 

- Analyze a large address space
- Explain how ping works and use it
- Use efficient options in nmap
- Understand CIDR addresses
Rubrics

- Students can not do the exercise without meeting the goals.
- If a student is stuck, you can give a hint without giving the answer.
- The exercise structure does not preclude reasonable ways to meet the learning goals.
Strace: essential facts

- Students may not know about Linux: syscalls, child processes, file permissions, etc
- The output can be voluminous.
- The student must be able to recognize what is important and what is not
Start with the empty program, then
strace -o empty1 ./empty
strace -o empty2 ./empty
diff empty1 empty

- copy a file.
- > mystery foo abc
  writes abc to file foo
- trace a known script that forks a process
- Use the -e option for strace to filter output
Trojan cat

> cat secret
Dynamic Analysis Example: strace

- Goals: students will be able to analyze a process to discover if it is reading/writing files that it should not.
- Trojan cat writes the contents of the file to a new file and appends all of the new filenames to a separate file.
- The permissions are set, so that they cannot list the directory, but they can read the files.
- The task is to read other students' files.
How do we provide formative assessment?
A Tool for assessing student work

bash history

visualization
Possible Uses for this Information

- Instructor can see visually if student is on the right track
- Student can use it after the exercise to reflect on what they did/did not do.
- Instructor can use it in a debrief after the exercise.
- Note: it gives more information than whether the student was successful or not
Students working on EDURange
EDURange Project

What it is: a cloud-based (AWS) framework for designing and instantiating interactive cybersecurity exercises

What it aims to teach: ethical hacking and cybersecurity analysis skills

Variety of scenarios: networking, reverse engineering, etc
Conclusions

- We need engaging exercises with clear learning goals and tools for timely, precise feedback.
- Backwards design can help by starting with the learning goals.
- Identifying rubrics and level of guidance can help with design.
- Some parts of our strace exercise are too prescriptive – they do not conform to our rubrics.
Future work

- How to teach students how to choose the right tools for a problem, including ones we haven't taught them.
- Shifting from tool-based exercises to problem-based exercises.
- Improving our tools to give better feedback to students and instructors.
- Collaboration with DETER, and we want your help.
Our website

For general information:
http://www.edurange.org

to sign up
cloud.edurange.org