The EDURange Framework and a Movie-themed Exercise in Network Reconnaissance

Richard Weiss
The Evergreen State College

Jens Mache
Lewis & Clark College

Michael E. Locasto
SRI International
The Challenge of Cybersecurity Education

• Teaching analysis skills/abilities and the security mindset – not just knowledge.
• Having good exercises (half of the battle)
• Providing the context/guidance (the other half), including clear learning goals.
• Providing prerequisite background
• 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.
What is EDURange?

• A framework for creating cybersecurity exercises.
• A collection of exercises.
• One of those exercises is Total Recon.
Total Recon: An example from network security

• Analyze a large address space
• Understand how ping and TCP work
• Understand CIDR addresses
• Use efficient options in nmap
Demo

• https://cloud.edurange.org
Total Recon: learning nmap

• Why not just use ping?

• nmap will use ping, but if there is no response, it can try TCP.

• Understanding protocols

• Learning the options for nmap: scan all TCP ports? UDP ports?
The Challenge of Formative Assessment

• Having the right tools: Complete/Accurate
• Large class size
• No TA support
• Limited time
• Equitable distribution of attention
Possible Uses for command line history 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
Other EDURange Exercises

- `strace`: teaches about system calls, and dynamic analysis of processes
- `ssh inception`: understanding basics and options
- `Treasure hunt`: command line tools, access control in Linux.
- `scapy hunt`: more advanced network recon
- `elf infection`: static analysis of binaries
- `DaVinci code`: basics of codes and ciphers.
Bash History graph
Conclusions

• We need engaging exercises with clear learning goals and tools for timely, precise feedback.
• We used backwards design and it helped.
• It is possible to use old movies as themes: students and faculty like it.
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, finding open ports that are filtered by a firewall.
• Improving our visualization tools to give better feedback to students and instructors.
Our website

• For general information:
  • [http://www.edurange.org](http://www.edurange.org)
• to sign up
• [cloud.edurange.org](cloud.edurange.org)