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 goaldevelop 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?

…

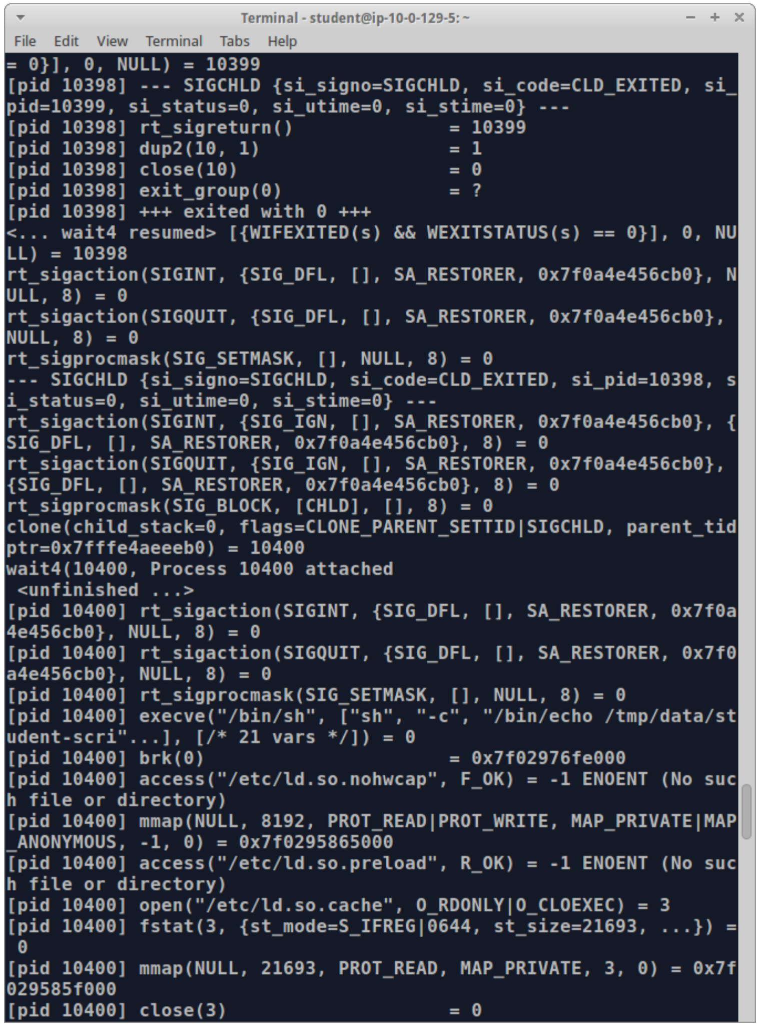
- Analyze a large address space
- Explain how ping works and use it
- Use efficient options in nmap
- Understand CIDR addresses

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



```
= 0}], 0, NULL) = 10399
[pid 10398] --- SIGCHLD {si_signo=SIGCHLD, si_code=CLD_EXITED, si_
pid=10399, si_status=0, si_utime=0, si_stime=0} ---
[pid 10398] rt_sigreturn()              = 10399
[pid 10398] dup2(10, 1)                 = 1
[pid 10398] close(10)                   = 0
[pid 10398] exit_group(0)               = ?
[pid 10398] +++ exited with 0 +++
<... wait4 resumed> [{WIFEXITED(s) && WEXITSTATUS(s) == 0}], 0, NU
LL) = 10398
rt_sigaction(SIGINT, {SIG_DFL, [], SA_RESTORER, 0x7f0a4e456cb0}, N
ULL, 8) = 0
rt_sigaction(SIGQUIT, {SIG_DFL, [], SA_RESTORER, 0x7f0a4e456cb0},
NULL, 8) = 0
rt_sigprocmask(SIG_SETMASK, [], NULL, 8) = 0
--- SIGCHLD {si_signo=SIGCHLD, si_code=CLD_EXITED, si_pid=10398, s
i_status=0, si_utime=0, si_stime=0} ---
rt_sigaction(SIGINT, {SIG_IGN, [], SA_RESTORER, 0x7f0a4e456cb0}, {
SIG_DFL, [], SA_RESTORER, 0x7f0a4e456cb0}, 8) = 0
rt_sigaction(SIGQUIT, {SIG_IGN, [], SA_RESTORER, 0x7f0a4e456cb0},
{SIG_DFL, [], SA_RESTORER, 0x7f0a4e456cb0}, 8) = 0
rt_sigprocmask(SIG_BLOCK, [CHLD], [], 8) = 0
clone(child_stack=0, flags=CLONE_PARENT_SETTID|SIGCHLD, parent_tid
ptr=0x7fffe4aeeeb0) = 10400
wait4(10400, Process 10400 attached
 <unfinished ...>
[pid 10400] rt_sigaction(SIGINT, {SIG_DFL, [], SA_RESTORER, 0x7f0a
4e456cb0}, NULL, 8) = 0
[pid 10400] rt_sigaction(SIGQUIT, {SIG_DFL, [], SA_RESTORER, 0x7f0
a4e456cb0}, NULL, 8) = 0
[pid 10400] rt_sigprocmask(SIG_SETMASK, [], NULL, 8) = 0
[pid 10400] execve("/bin/sh", ["sh", "-c", "/bin/echo /tmp/data/st
udent-scri"...], [/* 21 vars */]) = 0
[pid 10400] brk(0)                      = 0x7f02976fe000
[pid 10400] access("/etc/ld.so.nohwcap", F_OK) = -1 ENOENT (No suc
h file or directory)
[pid 10400] mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP
_ANONYMOUS, -1, 0) = 0x7f0295865000
[pid 10400] access("/etc/ld.so.preload", R_OK) = -1 ENOENT (No suc
h file or directory)
[pid 10400] open("/etc/ld.so.cache", O_RDONLY|O_CLOEXEC) = 3
[pid 10400] fstat(3, {st_mode=S_IFREG|0644, st_size=21693, ...}) =
 0
[pid 10400] mmap(NULL, 21693, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7f
029585f000
[pid 10400] close(3)                    = 0
```

Scaffolding of strace

- Start with the empty program, then

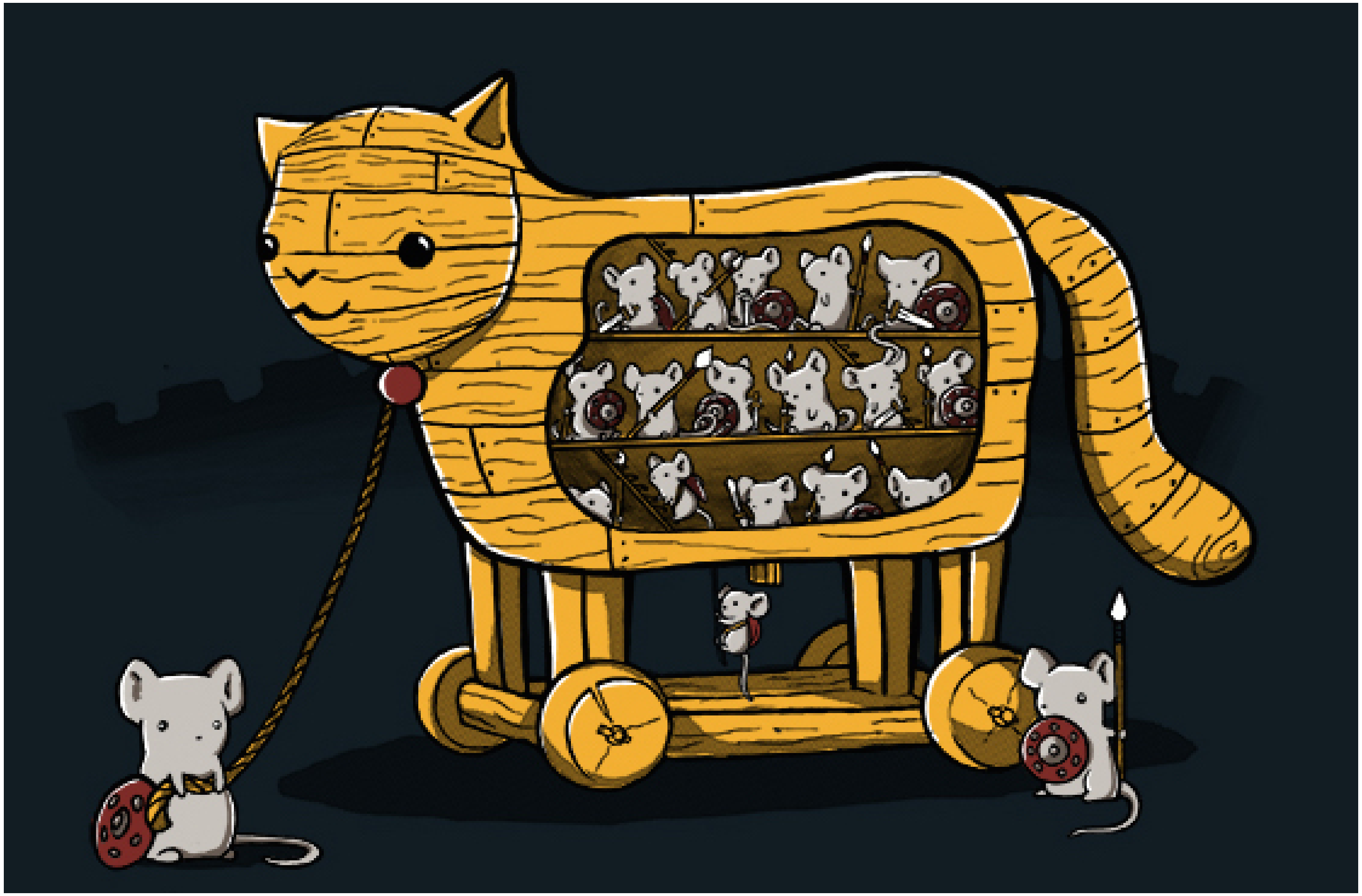
  ```
  strace -o empty1 ./empty
  strace -o empty2 ./empty

  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

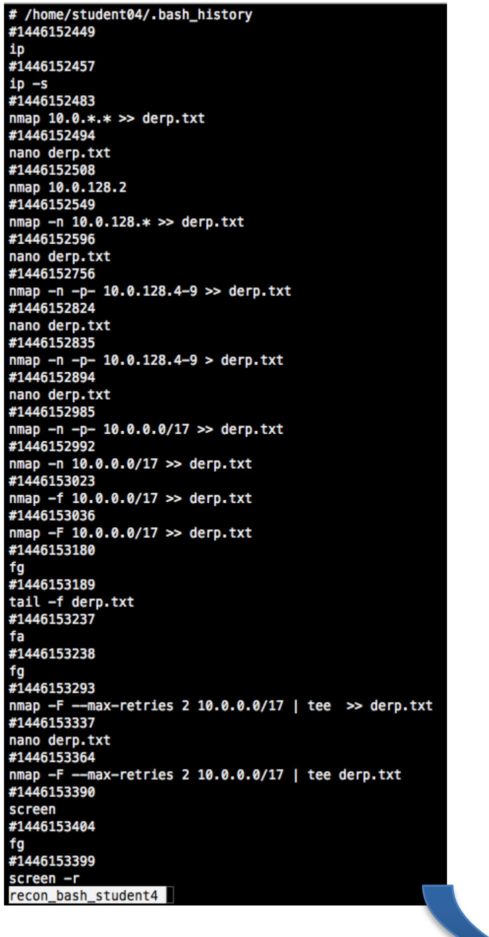
- Goals: students will be able to analyze a process to discover if it is reading/writing files that it should not.
- Trojan cat writes the contents of the file to a new file and appends all of the new filenames to a separate file.
- The permissions are set, so that they cannot list the directory, but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

How do we provide formative assessment?

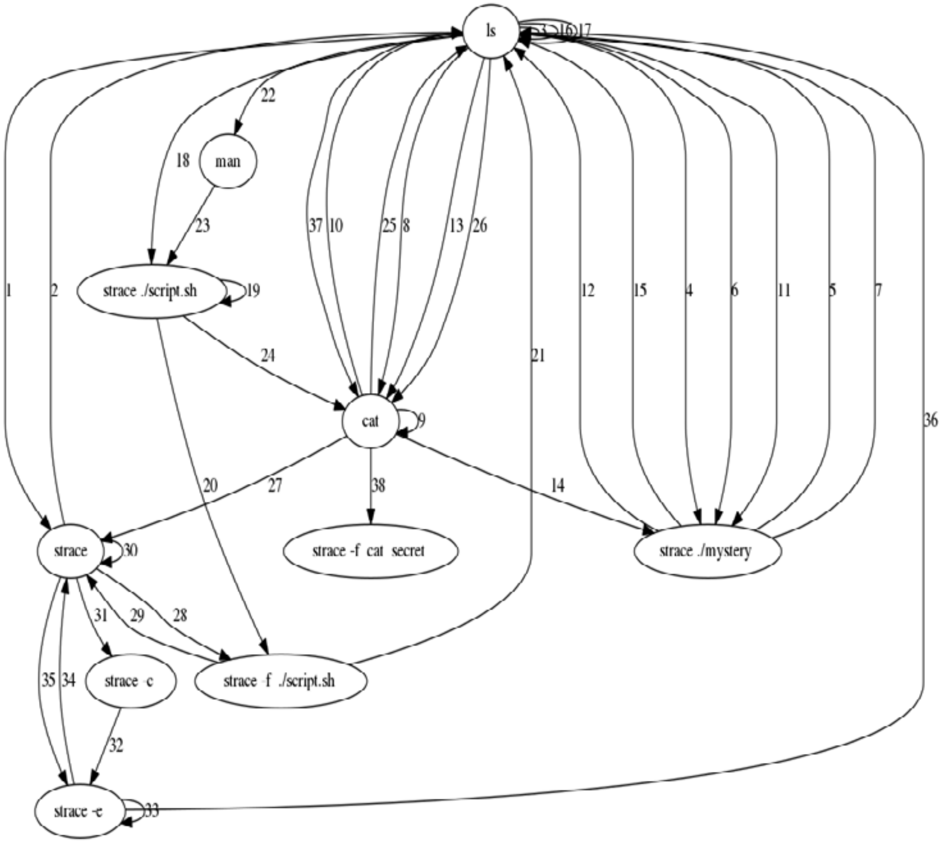
A Tool for assessing student work

bash history

visualization



```
# /home/student04/.bash_history
#1446152449
ip
#1446152457
ip -s
#1446152483
nmap 10.0.*.* >> derp.txt
#1446152494
nano derp.txt
#1446152508
nmap 10.0.128.2
#1446152549
nmap -n 10.0.128.* >> derp.txt
#1446152596
nano derp.txt
#1446152756
nmap -n -p- 10.0.128.4-9 >> derp.txt
#1446152824
nano derp.txt
#1446152835
nmap -n -p- 10.0.128.4-9 > derp.txt
#1446152894
nano derp.txt
#1446152985
nmap -n -p- 10.0.0.0/17 >> derp.txt
#1446152992
nmap -n 10.0.0.0/17 >> derp.txt
#1446153023
nmap -f 10.0.0.0/17 >> derp.txt
#1446153036
nmap -F 10.0.0.0/17 >> derp.txt
#1446153180
fg
#1446153189
tail -f derp.txt
#1446153237
fa
#1446153238
fg
#1446153293
nmap -F --max-retries 2 10.0.0.0/17 | tee  >> derp.txt
#1446153337
nano derp.txt
#1446153364
nmap -F --max-retries 2 10.0.0.0/17 | tee derp.txt
#1446153390
screen
#1446153404
fg
#1446153399
screen -r
recon_bash_student4
```



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

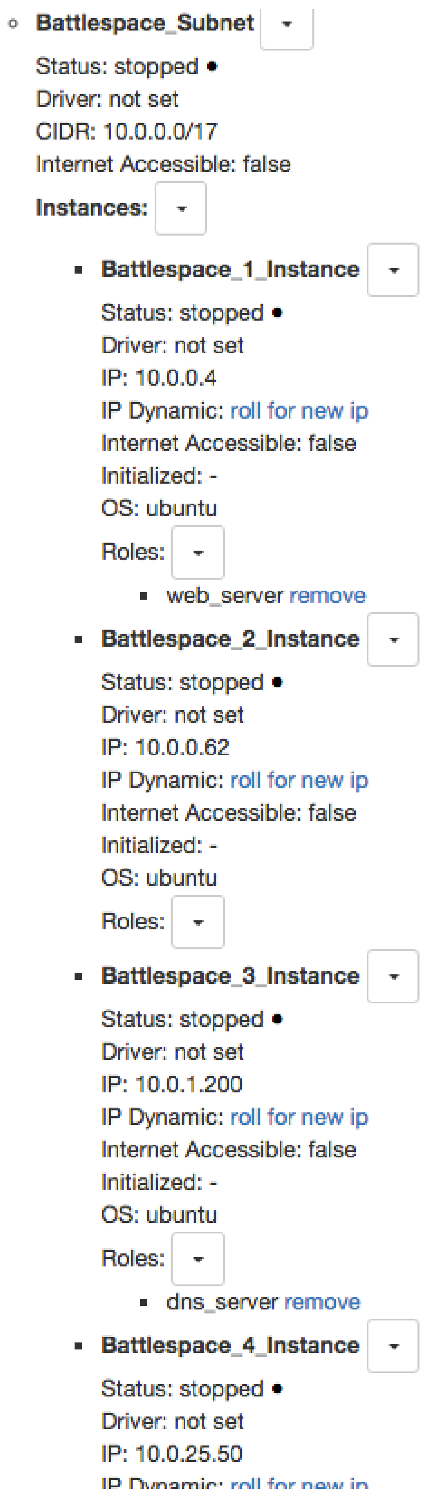
If you are the last one out, please close the door.
Parallelizing Tompa's Exact Algorithm for Finding Short Motifs in DNA

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



- **Battlespace_Subnet**

  Status: stopped ●
  Driver: not set
  CIDR: 10.0.0.0/17
  Internet Accessible: false
  Instances:

  - **Battlespace_1_Instance**

    Status: stopped ●
    Driver: not set
    IP: 10.0.0.4
    IP Dynamic: roll for new ip
    Internet Accessible: false
    Initialized: -
    OS: ubuntu
    Roles:

    - web_server remove
  - **Battlespace_2_Instance**

    Status: stopped ●
    Driver: not set
    IP: 10.0.0.62
    IP Dynamic: roll for new ip
    Internet Accessible: false
    Initialized: -
    OS: ubuntu
    Roles:
  - **Battlespace_3_Instance**

    Status: stopped ●
    Driver: not set
    IP: 10.0.1.200
    IP Dynamic: roll for new ip
    Internet Accessible: false
    Initialized: -
    OS: ubuntu
    Roles:

    - dns_server remove
  - **Battlespace_4_Instance**

    Status: stopped ●
    Driver: not set
    IP: 10.0.25.50
    IP Dynamic: roll for new ip

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