SAND2012-6012C

The Center for Cyber Defenders

Expanding Computer Security Knowledge

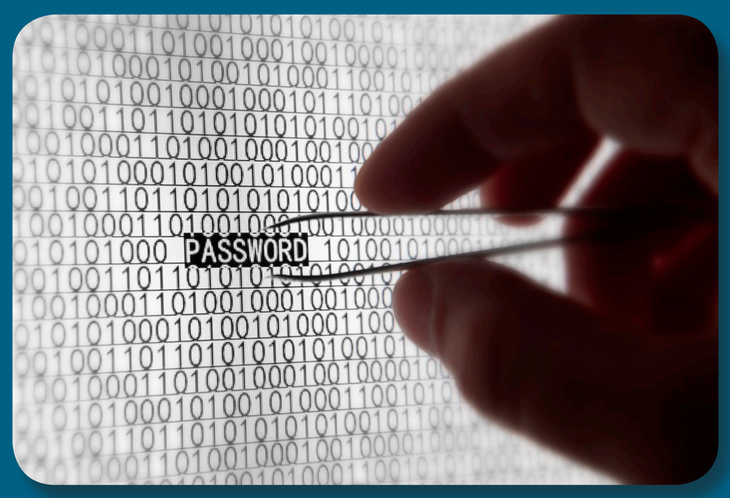
Cyber Training Using Large Scale Testbeds

Steven Elliot, North Carolina State University; Evan Jensen, Polytechnic Institute of NYU;
Omar Soliman, New Mexico Institute of Mining and Technology; Tyler Morris, La Cueva HS

Project Mentors: Theodore Reed and Christopher Davis, 5623

Problem Statement:

- The immediate and long term future of the nation's national security will depend heavily on cyber security.
- There is a deficit of cyber security experts and a lack of a cyber skilled workforce available to replenish them.
- This is partly due to a deficiency of hands-on, self-guided, cyber training for high school and early college students.



- In addition, resources and equipment necessary to train in cyber security are often too costly for pre-university students to gain access to.

Objective:

- Investigate the applicability of large-scale network testbeds and cloud Infrastructure As A Service (IAAS) technologies for creating training simulations.
- Create cyber training exercises that require no hardware, infrastructure, or cost to the student.

By using IAAS, the complexity of providing cyber simulations is abstracted away from the participants.

Approach:

- Develop training modules of varying skill level and domain, including the following:
  - Cloud-hosted virtual machines and networks containing cyber exercises and demonstrations for use in Internet equipped settings.
  - Mobile platform-based app for use with pre-existing Android and iPhone infrastructure.
  - Card game for use in no-cost/equipment sites.

Results:

- To achieve the objectives, the approach was realized through the implementation of training modules packaged into an open source Linux distribution.

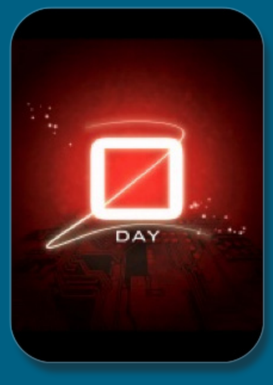
Backtrack Linux was used as a base for the training modules, as well as for its own built-in cyber tools. This provided both a host OS for the simulations and the necessary means for solving the training exercises.

The modules include:

- Offensive security (including vulnerability scanning, remote exploits, and password cracking). Students will learn techniques hackers use so that they can defend against them.
- Low-level hardware vulnerability techniques, including stack-based buffer overflows.
- Cryptography, the evolution of its defenses and failures, and encryption schemes.

A mobile education application which utilizes the prevalence of smartphones among students to teach good cyber practices was also developed.

A popular card game was also modified to implement cyber terminology and themes, and provides a no-infrastructure-necessary introduction.



Left: Cover art for the cyber security card game ZeroDay.

Right: Screenshots of the cyber security application.

Impact and Benefits:

Via our exercises, a wide range of students are able to receive cyber security training that was previously inaccessible.

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2012-XXXXP.