Secure Linux Integrated Configuration Tool

Dale Reilley, Aleah Delgado, Shani Melbourne | Kevin Burk, Mike Cloud

Project Objective and Interns Contribution:
Our aim was to provide an easy-to-use tool that automates the process of securing a Raspberry Pi.

The method we used to accomplish this was:

1. Refer to the General OS STIG as well as recommendations from our Navy sponsor to determine what security features would apply and be achievable on a Raspberry Pi.
2. Find a way to talk to Ansible through Python with the python package ansible-runner.
3. Create a web server to host an intuitive graphical user interface that enables selecting and running Ansible scripts.
4. Create Ansible scripts to automate the desired configurations gathered from the General OS STIG.

Our contributions were:

- A web server to run Ansible scripts and report the results after all scripts have completed.
- Ansible scripts that:
  - Configure custom firewall utilizing iptables to block all incoming packets by default.
  - Set up an admin user.
  - Implement password and login policies.
  - Enable address space randomization to randomize the locations of different parts of programs in memory.
  - Configures ssh.
  - Disable and blacklist wireless connections to prevent loading at boot.
  - Disable unused services if present.
  - Upgrade all packages and remove all unused packages.
- Documentation for future users and developers.

Results / Accomplishments / Next Steps:
We demonstrated an accessible way to secure a Raspberry Pi that is within the Department of Defense’s guidelines.

The impact for the Navy is for them to have an easy-to-use tool at their disposal that enables a more secure, wide deployment of Raspberry Pi’s into various applications.

What’s most important is that users will be able to make many security configurations to their Raspberry Pi’s without needing to have in-depth, technical knowledge.

In the future, this work will be able to be expanded in its functionality through scaling it to include more Debian systems and including more security options with our documentation as a starting point to enable a wider utilization of Raspberry Pis with less risk of compromising military assets.

1. What are you most proud of this summer [with respect to your experience/project]?
   
   **Dale:** I’m proud of learning how to properly collaborate and work alongside team members in programming a shippable product.
   
   **Shani:** I’m most proud of becoming familiar and comfortable with new tools that I can envision using outside of this project.
   
   **Aleah:** I am proud that we were able to complete a fully functioning tool given the time constraints.

2. Why was the internship valuable?

   **Dale:** It gave me a chance to see what it was like to work in the real world with hard deadlines and necessary problem-solving when there’s sometimes not just a simple answer.
   
   **Shani:** It showed me that I was more capable at doing new things than I initially thought, as well as showing me how valuable a compatible team is to successfully complete a big project within short amount of time.
   
   **Aleah:** I learned a lot this internship. I became familiar with different tools and was able to collaborate with others in a remote setting, which are skills that will aid me in future scholarly and professional opportunities.

3. Advice for future cohorts?

   **Dale:** Create a defined schedule early on to follow and stick to it to build discipline. It will give you better structure around your work life and day-to-day life.
   
   **Shani:** Don’t be afraid to ask questions, even if it seems as if the answer would be obvious.
   
   **Aleah:** Ask lots of questions, and pay attention to information, even if it doesn’t pertain to your specific tasks.