San Diego Regional Cyber Lab

Wanted: Newsletter Contributors!

The San Diego Regional Cyber Lab (SDRCL) is nothing without our regional partners. If you are reading this, you are still at the ground floor of the lab's regional rollout. In the coming months and years, regional organizations will be given opportunities to participate in a variety of activities hosted at our downtown lab location. From partnerships with local universities (free PenTests, anyone?) to hands-on forensics equipment training sessions, the Cyber Lab is bound to have something to benefit your organization.

Many of these resources are due to our regional relationships with organizations just like yours. In future issues, we hope that many of you will see this newsletter as an opportunity to spread the news on your own organization's offerings and contribute an article of your own. Does your organization provide services that you feel would benefit other regional groups? We can host your agency in the lab for other attendees to join and connect. Is your organization struggling with a challenge that would benefit from a larger collaborative effort? Get it posted here and perhaps one of our partners will have a potential solution for you.

As you will see in the following issue, our lab will have a plethora of virtual and physical resources for your organization to test out. If your teams have professional experience with any of our forensics hardware, for example, we would love for your team to provide a hands-on demo to show our partners how you currently utilize this equipment in your own daily operations. We would love for your teams to host sessions in our lab and advertise them here in the newsletter.

We look forward to your future contributions!

Helpful Hackers

Several local universities have reached out to the SDRCL in an effort to obtain new capstone projects for their soon-to-graduate senior cybersecurity students. If you believe your organization could benefit from the services of a team of local students, please reach out to us for more details. These universities have previously provided organizations with free penetration testing, risk analyses, cybersecurity consulting services, Internet of Things (IoT) landscape reviews, gap analyses, and more.

For smaller organizations that may not have the financial resources to hire a full cyber support team, this could be a great opportunity to have a review of your current environment with no cost obligations. Please reach out to Ian Brazill at ibrazill@sandiego.gov for additional details.

Upcoming SDRCL Events:

- *Final Physical Lab Equipment Deliveries*
- *Website Launch*
- *Physical Lab Debut & Walkthrough*

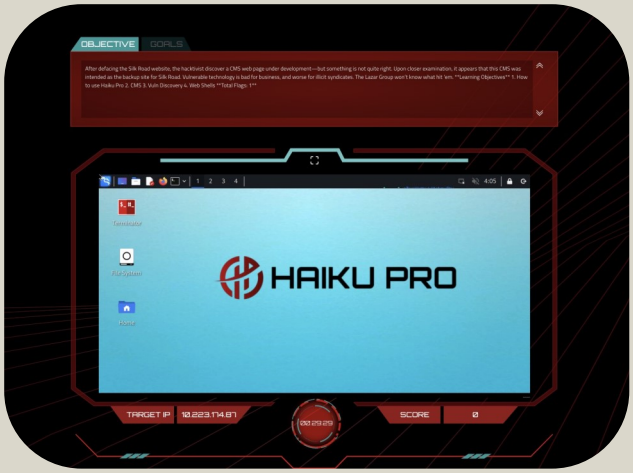
In This Issue

Hacking 101

The SDRCL has partnered with a great team over at the Cyber Center of Excellence (CCOE) to provide a large number of licenses for our partners to experience the benefits of Haiku — a new interactive hacking experience that trains users on the basics of offensive and defensive cybersecurity strategies.

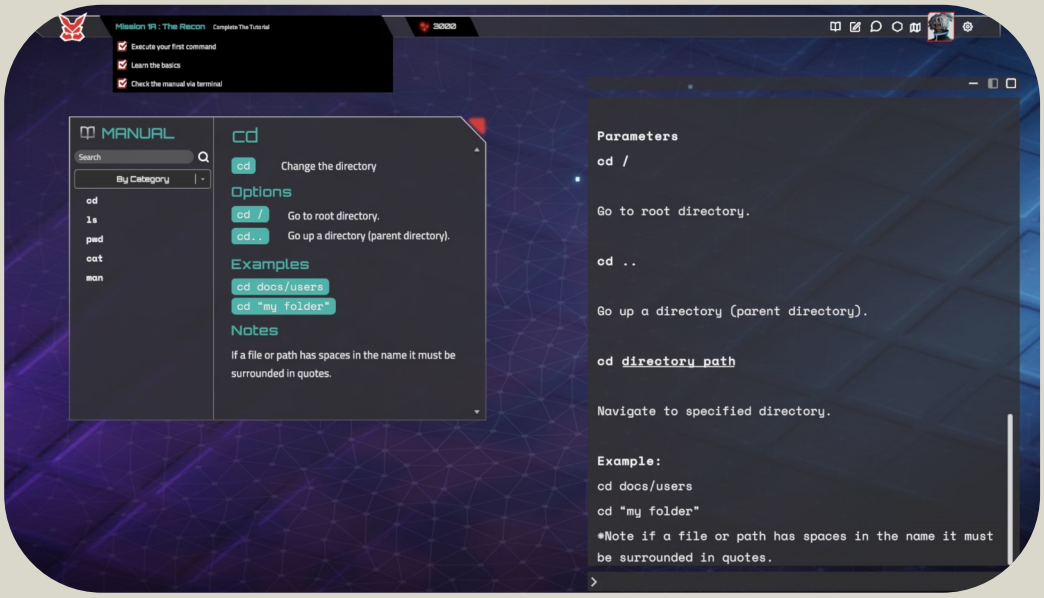
Here's a short preview from Haiku that should help describe the benefits that our regional partners will enjoy with a license:

"The Haiku product suite is designed to train students and professionals in hands-on cybersecurity skills, either in conjunction with a certification or degree or solely as a hands-on training tool. The 'World of Haiku' is a downloadable game that takes a player from zero cybersecurity training to, by game's end, a solid understanding (with hours of experience) of working from a Linux command prompt as well as an understanding of offensive and defensive cybersecurity methods and tools.



The Haiku Pro tool is designed for more advanced users (including those who completed 'World of Haiku') and provides a browser-based series of cyber range challenges to further test the player and develop their hands-on cybersecurity skills. Haiku Pro includes the Vulcan Forge tool which allows a user to use a drag and drop interface to build their own ranges to support a training curriculum or cyber challenge.

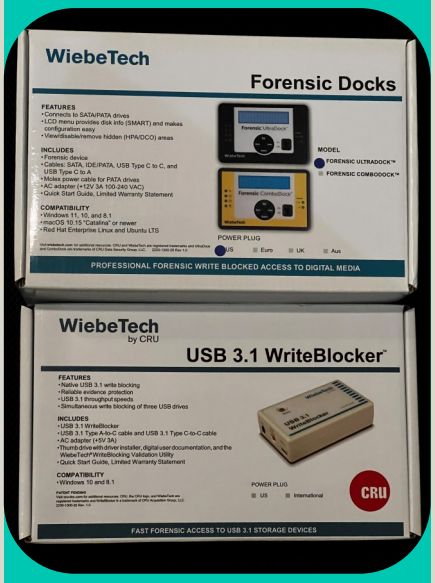
To connect the player's training to jobs, the Haiku Job Connect provides jobs that directly require the skills that the players have developed in their profile, and the Haiku Skillz Resume allows the player to demonstrate the proof of their skills (in terms of hours spent and an assessment of their level) on a resume they can provide to potential or current employers or educational providers."



Flirting with Forensics

Do you work in law enforcement? Would your organization benefit from hands-on training experiences with industry-leading forensics hardware? The Cyber Lab recently procured a suite of devices that could benefit any organization that works in forensically sensitive environments. A few examples of our offerings:

- Tableau TD2U Forensic Duplicator Kit
- Tableau TX1 Forensic Imager Kit
- Wiebetech Forensic Ultradocks and USB 3.1 Writeblockers
- Cellebrite UFED Touch2 Ultimate Standard
- Cellebrite UFED 4PC Ultimate Kit
- EnCase Forensic v21.1 and SMS license



Stakeholder Volunteers Wanted

Every partner of the SDRCL has their own strengths and weaknesses when it comes to cybersecurity. The benefit of the SDRCL is that one organization's weakness may be another's strength.

We hope your organization will consider utilizing our downtown space for some of the following suggested activities:

- Roundtable discussions about problem areas (What tools are being used, resource problems, etc.)
- Gatherings to solve organization-specific challenges
- Hackathons
- Collaboration to solve larger regional security problems
- Data collection for pattern identification among SDRCL partners

Surfing the Web(site)

In the coming weeks, we will announce the launch date for our brand-new SDRCL website and we can't wait to show it off. In the meantime, we'd like to highlight a few of the site's features.

Information Library

The Information Library will contain a wide range of resources and reference materials for you to review while bolstering your own cybersecurity environments. Examples include:

- Links to various threat intelligence feeds
- Information on the Homeland Security Information Network (HSIN)
- Security policy templates from SANS
- Information on the National Institute of Standards and Technology (NIST) Framework
- Links to various cyber podcasts, newsletters, and more

Cyber Simulation Tools

- Access to our free virtual cyber range where you can hone your skills in a collaborative, controlled, cloud-hosted environment
- Access to the Haiku cyber range
- Access to Cyber Catch, a quick and useful evaluation tool for small- and medium-sized businesses to assess their organization's current cyber readiness

Last but certainly not least, the website will be your one-stop shop to find details on our physical lab space. You will be able to schedule an appointment for the lab space through an online webform and gather all of the details you might need prior to your arrival. We sincerely hope you enjoy browsing the website when it is released!

Big Costs, Big Ambitions

By the time our Cyber Lab is fully stood up, we will have spent nearly $1 million to create a lab worthy of the San Diego region — and we're just getting started. So far,we have acquired all of our furniture, workstations, and roughly half of our forensics equipment. Given the global shipping delays, we are still waiting for the rest of our forensics devices as well as our large server rack.

The photo below is a small preview of the lab's current state. Once we acquire the rest of our equipment, as well as some much-needed decorations, we'll be ready to go! We are anticipating a kickoff in September and will reach out to everyone when that is finalized.

Top Exploited Vulnerabilities of 2021

1. Log4Shell (CVE-2021-44228)
2. Zoho ManageEngine ADSelfService Plus (CVE-2021-40539)
3. ProxyShell (CVE-2021-31207, CVE-2021-34473, CVE-2021-34523)
4. ProxyLogon (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065)
5. Atlassian Confluence Server & Data Center (CVE-2021-26084)
6. VMware vSphere Client (CVE-2021-21972)
7. ZeroLogon (CVE-2020-1472)
8. Microsoft Exchange Server (CVE-2020-0688)
9. Pulse Secure Pulse Connect Secure (CVE-2019-11510
10. Fortinet FortiOS and FortiProxy (CVE-2018-13379)

Click here for additional details.

San Diego Regional Cyber Lab
1200 Third Avenue, Ste. 1800
San Diego, CA 92101

Join the SDRCL LinkedIn Group

A LinkedIn group allows organizations to maintain open dialogues in a social media-style format. We believe this will encourage more collaborative conversations in a private group inaccessible to the larger LinkedIn community.

If you have a question for the region but don't feel like it is appropriate or formal enough for an email, consider posting your question on the group's timeline. Click **here** to locate the group, as you will not be able to locate it simply by searching on LinkedIn.

Contact Us

SDRCL Program Lead
Ian Brazill
IBrazill@sandiego.gov

SDRCL Cyber Lead
Brendan Daly
BMDaly@sandiego.gov

Chief Information Security Officer, CoSD
Darren Bennett
DBennett@sandiego.gov

SDRCL Project Manager
Megan Hartung
MHartung@sandiego.gov

Cyber Center of Excellence (CCOE), Community Partner
Lisa Easterly
Lisa.easterly@sdccoe.org