WORKSHOP SERIES 1
Thursday • 2:00 pm - 4:00 pm

Cyber Fire: Puzzle-Based Training
Neale Pickett and Grace Herrera, Los Alamos National Laboratory

Cyber Fire is a computer security incident investigation training program within the U.S. Department of Energy. In this puzzles-only sampler of the event, you will use your laptop or mobile device to step through puzzles that teach investigation techniques. Cyber Fire establis es an environment where participants are encouraged to take risks and make mistakes with access to veteran responders to help explain approaches to puzzles and how they relate to real investigations. This hands-on event is heavy in practical application of cybersecurity skills such as mathematics, manual/automated packet inspection, static/dynamic analysis and disk/memory image inspection.

ATT&CK and Threat Actors
Kat Seymour, Heather Linn, Ken Smith and James Thomas, Bank of America

This workshop introduces you to some basic techniques used to replicate threat actor behavior. You will work hands-on in putting a threat model to the test and trying various techniques like command injection and using the penetration testing framework Metasploit to accomplish an objective from the perspective of a threat actor. You should come away from the workshop with an increased understanding of how threat actors follow a chain of events to accomplish an objective, as well as a better understanding of how to protect yourself personally and professionally from a variety of threat actor techniques. You will be provided some pre-reading/pre-work to help make the most of this hands-on workshop.

Red Team Your Resume: Insiders Share Secrets
Kaitlin O’Neil, Kate Broussard, Kelly Albrink, Bishop Fox, Troy Steece, McAfee and Linda Martinez, Protiviti

Are you applying for jobs in cybersecurity, and do you want recruiters to actually look at your resume? If you answered ‘yes,’ then maybe it’s time to consider having your resume “red teamed.” Each panelist will share their personal stories surrounding their starts in the industry. The path to success is rarely linear, and a well-rounded security resume should reflect that reality. Insights will include: certifications you’ll want to earn, career highlights you may be ignoring and traditional versus non-traditional security backgrounds. The InfoSec job of your dreams is within your reach; it may require tearing apart your resume to land it. This panel will provide you with enough perspectives to feel like you have the knowledge to position yourself as a competitive candidate.

Join us for a Blue Team CTF — Solve security puzzles using network and host-based forensics in a Jeopardy-style CTF. Get a taste for what working on the Blue Team is like with real-world data and examples pulled from our actual jobs. No experience necessary! Bring a laptop with wifi and software to run a VM (e.g. VMware or VirtualBox); we’ll provide you with the other tools needed to solve the puzzles. Puzzles will range in difficulty and subject, so everyone will find something they can work on, and forming teams will be encouraged. We’ll play with PCAPs to dissect network traffic, emails to diagnose phishing, and Windows Event Logs to track down the malware.

Blue Team Capture the Flag (CTF)
Elizabeth Schwinsberg and Bridget Pelletier-Ross, Facebook

Join us for a Blue Team CTF — Solve security puzzles using network and host-based forensics in a Jeopardy-style CTF. Get a taste for what working on the Blue Team is like with real-world data and examples pulled from our actual jobs. No experience necessary! Bring a laptop with wifi and software to run a VM (e.g. VMware or VirtualBox); we’ll provide you with the other tools needed to solve the puzzles. Puzzles will range in difficulty and subject, so everyone will find something they can work on, and forming teams will be encouraged. We’ll play with PCAPs to dissect network traffic, emails to diagnose phishing, and Windows Event Logs to track down the malware.

SFS MEETUP
SCHOLARSHIP FOR SERVICE
Thursday, 7:00-8:00 pm - Kings Terrace

Come and meet SFS (CyberCorps) students, faculty and agencies participating in the program. Learn how to get into the program. Network with fellow students currently in the program.

1:1 FUNDING MEETUP
EDUCATORS & FUNDING AGENCIES
Thursday, 8:00-9:00 pm - Kings Terrace

For Educators, this sessions provides one-to-one conversations with program directors/managers at various funding agencies such as NSF and NSA.
**WORKSHOP SERIES 2**

**Thursday • 4:30 pm - 6:30 pm**

**Distributed Forensics Across Time and Space**
Elena Kovakina and Jesus Aguilar, Google

Welcome to Cyber Forensic Affordances (CFA). For the length of this workshop, you are a part of the CFA investigative team trying to solve the mysterious Greendale case. This interactive workshop will introduce timeline building and analysis with open source digital forensics tools. We will use the processing depth of Plaso and the analytic and collaborative capabilities of Timesketch to achieve our goals and solve the case. You will learn how to build timelines, analyze logs data from multiple machines and tell exciting stories with your insights.

**Gaining Initial Access in a Penetration Test**
Krysta Coble, Kelly Thiele, Laura Puterbaugh and Petya Lopez, Department of Homeland Security

Have you ever wondered what it would be like to hack into a government agency? We can tell you all about that—legally, of course! At the Department of Homeland Security (DHS), the National Cybersecurity Assessments and Technical Services (NCATS) team works to help federal and state governments enhance their cybersecurity posture through a variety of free services. As phishing campaigns are the most successful attack vector from real-world threats, our workshop will cover how we use phishing as a method to gain initial access into our customer networks.

This workshop provides a high-level explanation of the hacker methodology with hands-on experience in the Exploitation/Initial Access phase. We are operating under the assumption that all legal agreements and scopeing has already been conducted to start the assessment and considered completion of the Reconnaissance phase. To start, we’ll discuss infrastructure setup and assessment prerequisites. Next, we’ll craft phishing emails and attach “malicious” payloads that report back to our attack platform when clicked. Finally, we’ll achieve situational awareness of our current access and strategize our next steps in the assessment.

**WiCyS Social CTF Village and Competition**
Dr. Dan Manson, Cal Poly Pomona, Kaitlyn Bestenheider, Tevora, Franz Payer, Cyber Skyline, Jeana Cosenza and Vicente Gomez, Pace University

The National Cyber League (NCL) offers engaging, entertaining, measurable and scalable methods of learning to enlist a new generation of cybersecurity professionals. Following up on our highly successful NCL workshop at WiCyS 2018, we will host an immersive social NCL Capture the Flag (CTF) to take place during the entire WiCyS 2019 conference.

Activities will occur in an NCL village. This will be a multi-station space with something for everyone. There will be dedicated spots for fellow NCL student champions, who will help run challenge category-specific work groups training students and coaches alike in categories such as Cryptography, Log Analysis, Network Traffic Analysis, Web Access Exploitation, Password Cracking and more.

Students can talk with NCL Chief Player ambassador Kaitlyn “CryptoKait” Bestenheider to learn how NCL jump-started her education and career. Educators and coaches can learn about incorporating NCL into their classroom curriculum from Chief Coach ambassador Steven Miller. Recruiters and talent scouts can meet with NCL commissioner Dr. Dan Manson to learn how they can use NCL’s Scouting Report to find top talent in their area! Challenges for this entire conference-long CTF will be tailored for the WiCyS community in an effort to drive students to learn more about WiCyS as part of their research to solve challenges. Competition winners will receive prizes and a free game code for the next NCL season, and all students will receive NCL swag.

**Advanced APT Hunting with Splunk**
Lily Lee and John Stoner, Splunk Inc.

You wanna learn how to hunt the APTs? This is the workshop for you. Using a real-world type dataset, this workshop will teach you how to hunt the fictional APT group Taedonggang. We will discuss the Diamond model, hypothesis building, LM Kill Chain and MITRE ATT&CK framework and how these concepts can frame your hunting. Then we will look deep in the data using Splunk and OSINT to find the APT activity riddling a small startup’s network. We will walk you through detecting lateral movement, the P of APT and even PowerShell Empire. At the end, we will give you a similar dataset and tools to take home to try newly learned techniques yourself.
WORKSHOP SERIES 3
Friday • 3:30 pm - 5:30 pm

National Cybersecurity Curriculum Program: Labs and Resources for Your Classroom or Student Club
Dr. Blair Taylor, National Security Agency Contractor and Maureen Turney, National Security Agency

Faculty, are you looking for cybersecurity curriculum and resources? Cybersecurity clubs, are you looking for enrichment activities and exercises that help students enhance their cybersecurity knowledge and skills?

In this workshop, you will access, use and download cybersecurity curricula, labs and resources freely available through the National Security Agency's National Cybersecurity Curriculum Program (NCCP). Over 50 schools and universities have developed effective and engaging cyber curriculum modules in needed topic areas including networking, risk management, cybersecurity laws and policies, cybersecurity principles, secure coding, ethics and cyber threats and vulnerabilities. This workshop will provide an overview of NCCP and allow faculty and students time to access and download curriculum from www.clarkcenter.org. By the end of this workshop, you will leave with your own library of curriculum resources for your classroom or clubs.

Apprenticeships Powered by Industry - Build Your Talent Pipeline

Think apprenticeships can't work in cybersecurity? Think again. Across the world, companies are struggling to find skilled talent. We must rethink the way we approach education, especially in innovative industries where technology rapidly outpaces traditional education and training. It is time to innovate talent development, and no one is better situated to do that than the industry innovators themselves.

This workshop will dig deep into two successful cybersecurity apprenticeship programs that are building their cybersecurity talent pipeline. Integrated Systems Group (ISG), a small technology company, and IBM are two very different companies addressing the challenge of finding, training and retaining talent through apprenticeships. Maher & Maher and the U.S. Department of Labor and Employment are partnering with companies like ISG, IBM and national trade associations to create and deliver tools and support to help companies of all sizes as well as explore and implement apprenticeships as a modern talent development solution.

This workshop will provide access to those tools and resources to help you customize a program that will work for you and the women you seek to fill the talent pipeline. You will learn the key elements of high-quality programs and how to partner with educators and other public and industry partners to access existing tools while building a program that will work for you.

Acquiring & Retaining Cybersecurity Talent: A Proven Model
Deidre Diamond, CyberSN and Brainbabe

Workforce development is reliant on the combination of a subject-matter common language framework of projects and tasks. Job descriptions are then derived from this same framework definition. A career development plan based on standardized projects and tasks, along with a culture that allows for psychological safety, will allow you to acquire and retain talent. When we combine daily processes of business operations derived from a subject-matter common language, in which all teammates know their role and the roles of others on the team (along with a culture that allows humans to think, feel and perceive without negative consequences), we can truly experience workforce development in any subject-matter profession. Come hear how to achieve this success in cybersecurity. Between our technology and our theories, we are showing that organizations can obtain cybersecurity talent in less than 60 days and retain them.

GROW WITH WICYS
Saturday, 10:45 am-11:30 am - Commonwealth 1

Interested in joining or starting a WiCyS Student Chapter at your institution? Come to the Student Chapter Meetup! 49 WiCyS Student Chapters have launched over the last 6 months. You will hear about successes as well as challenges from Chapter leaders, learn how to overcome those challenges, share your story, and find peer support. You will also learn how Student Chapters can secure funding for their activities, as well as use the WiCyS Online Community Forum and Social Media outlets.

Join us and get inspired to bring cybersecurity awareness and cyber-engagement activities to your campus.

#WiCyS2019
WORKSHOP SERIES 4
Saturday • 2:30 pm - 4:30 pm

Listening to Internet Background Radiation
Luna Frank-Fischer and Pamela Toman, Expanse, Inc.

Beneath the surface of the internet, there is a huge amount of “noisy” packets that are illegitimate attempts to connect to services. This noise is persistent, consistent and loud. The majority comes from bots and worms like Mirai and WannaCry, which blindly attempt to infect their internet neighbors and spread their reach. The existence of background radiation is an emergent property of the networked internet, and trends in background radiation give defenders insight into the relative attention of attackers.

Blockchain Technology and the Future
Dr. Cynthia Irvine and Dr. Britta Hale, Naval Postgraduate School

Blockchain technology (BT) supports distributed ledgers and has been identified as a mechanism that can support applications ranging from crypto currencies and event logs to supply chain security and as a cause of and mitigation for climate change. This two-hour, interactive workshop will introduce you to the basic concepts associated with BT and prepare you to ask critical questions regarding blockchain proposals, applicability and implementations. You will learn how to set up a simple blockchain lab and be guided through a simple exercise.

In this workshop, we’ll support you in standing up software to observe internet background radiation, and we’ll enable you to perform basic analyses on what you see and report on those findings. You will establish AWS machines in varied locations, log the connections received and work together to identify the ports that garner substantial interest. You will walk away with an understanding of how internet scanning fits into the landscape of cybersecurity as both an omnipresent source of attacks and a powerful defensive tool. You will be empowered to independently build on what you learn during this workshop and engage in larger conversations about internet security with new context and skills.

Pittsburgh CTF: Steal the Steel
Dr. Vitaly Ford, Arcadia University, Amela Gjishti, Bank of America and Daniel Tyler, Optum

Capture the Flag competitions (CTFs) have become a de facto standard for cybersecurity training. As a result, CTFs are a great way to showcase your cybersecurity skills and build your resume. There are many CTFs available (like https://ctftime.org/) that cover such topics as cryptography, steganography, forensics, exploitation and web attacks. However, very few are focused on the secure coding aspects of software engineering. In this workshop, we plan to teach secure coding through a team-based, Pittsburgh-themed “Steal the Steel” CTF (steel will represent the flag points for each challenge as Pittsburgh is known for steel production and having the most bridges than any other city in the world).

CTF4 Noobz: Tools and Tips for Cybersecurity Competitions
Marcelle Lee, WiCyS Mid-Atlantic Affiliate, Lisa Jiggetts and Mari Galloway, Women’s Society of Cyberjutsu

Interested in cybersecurity competitions but don’t know where to start? Or have you tried one or two or 10 and want more practice? In this hands-on keys workshop, we will explore different types of competitions from Capture the Flag to offense/defense and everything in between. In addition, we will review various tools of the cyber trade. These will become part of your toolkit to solve cybersecurity competition challenges! You will be provided with a virtualized environment that will be used to explore techniques associated with reconnaissance, scanning and enumeration, and exploitation. Also featured will be forensic challenges, hash-cracking, binary analysis, crypto decoding, etc. The challenges are related to topics covered in the EC Council Certified Ethical Hacker (CEH) certification.