Faculty Professional Development Trainings – 2019
Sponsored by the CAE – CDE grant funding

TWO Great Locations:

1) Springtime on the Mississippi

a. Trainings to be held at Metro State University in St Paul, MN
b. Lodging reserved at the Hyatt Place, St Paul – Downtown
c. May 30 and 31, 2019
d. Travel date is May 29, 2019

2) Summertime in Sin City

a. Trainings to be held at the Park MGM in Las Vegas, NV
b. Lodging reserved at the Park MGM
c. August 6 and 7, 2019
d. Travel date is August 5, 2019

FOUR Great Topics: (descriptions found later in this document)

1) SCADA
2) Intrusion Detection and Prevention
3) Penetration Testing
4) Software Exploitation

Registration:

Sign up for one or both, depending on your travel abilities. **Registration link on page 4**. The CAE – CDE grant is paying for:

a. 12 hours of instruction over two days
b. Two faculty trainers per class
c. Exercises, presentations, and resources to use in your classes
d. Hotel rooms during your stay (2* nights in St Paul, and 3 nights in Las Vegas)
e. Breakfasts
f. Morning Breaks
g. Lunches
h. Afternoon Breaks
i. Networking Reception

* You can get one additional night if you attend the North Central Region Meeting being held on Wednesday, May 29, 2019 in St Paul – a different registration for that (also included)

**You and/or your institution will have to pay travel and evening meals. Airfare to MSP and LAS is quite reasonable and, in most cases, a direct flight.

Each training is limited to 25 participants. Rosters will fill up quickly, first come first served. Feel free to list 1st choice, 2nd choice, etc. for each training location. If you wish to attend both training locations, you will need to register for each. When the classes are full, we will start a waiting list.

Topic Descriptions:

SCADA

This workshop will introduce attendees to open source open access Supervisory Control and Data Acquisition (SCADA) and Industrial Control System (ICS) cybersecurity curriculum published on https://clark.center. The curriculum and corresponding lab components are divided based upon content and complexity. Modules are designed to use virtual SCADA testbeds in Docker, a program which runs on both Windows and Linux. The curriculum also includes lecture materials, homework, exam problems, and lab exercises. This curriculum has both two-year college and four-year college application. Attendees will also learn how to use OpenPLC (http://www.openplcproject.com/) to build hands on SCADA systems.
Topics:

- Introduction to SCADA Control Systems
- SCADA Control System Networking
- SCADA Control System Network Enumeration, Interruption, Injection, and Alteration
- SCADA Control System Network Intrusion Detection
- SCADA Control System Network Confidentiality and Authentication
- OpenPLC Ladder Logic Programming
- OpenPLC Human Machine Interface Programming
- Building Reference SCADA Control Systems with OpenPLC and UniPi

---

Intrusion Detection and Prevention

This workshop will cover intrusion detection and prevention systems with commonly used tools, techniques, and procedures that are readily available to faculty at no cost. These industry standard tools and concepts will be leveraged in a hands-on environment giving students practical experience. This course will conclude with a scavenger hunt exercise guiding students through conducting network forensics on a realistic intrusion.

- Wireless Intrusion Monitoring
- Network Traffic Analysis
- Intrusion Detection Systems
- Signature Detection
- Anomaly Detection
- File Carving

Penetration Testing

This workshop will cover the theoretical and practical aspects of penetration testing. The course will follow current penetration testing methodologies including commonly used tools, techniques, and procedures. Hands-on labs will accompany an experiential-based approach, and the course will conclude with a capture the flag style event for participants to exercise their newly acquired skills in a simulated environment.

Topics:

- Penetration Testing Methodology
- Planning Penetration testing events
- Active and Passive Reconnaissance
- Alternative Attacks and Threat Modeling
- Exploitation
- Internal Reconnaissance
- Pivoting, Privilege Escalation, Persistence
- Command and Control
- Reporting

Software Exploitation

This course will provide an introduction to binary exploitation as well as a look at various exploitation mitigations and methods for defeating them. Hands-on exercises will be provided for each topic. Both Windows and Linux platforms will be covered. Time permitting, other topics may include: fuzzing, static analysis, and/or heap exploitation. Students will be expected to have moderate-to-strong knowledge of C and x86 assembly language as well as a computer capable of running a virtual machine.

Topics:

- C / ASM
- VM Setup
- GDB / Windbg
- What is “Software Exploitation”
- Stack overflows
- Shellcode
- DEP/NX
- ROP
- ret2libc
- ASLR / PIE
- Brute force
- non-ASLR modules
- Partial overwrites
- Leaking pointers
- And more!

Please join us:

Your peers that attended the trainings in 2018 really enjoyed the event and had some excellent takeaways that could go right into their curriculum. That is what this is all about, trying to help each other in our journey to educate the wave of cyber employees. The 2019 topics came from the results of a survey sent out in the CAE Community newsletter. Thank you for the great topics.

Lodging:

We will be handling all reservations for all events. We will provide your name and email address to the hotels, then when you check in, you provide a credit card for incidentals. The room charges are direct billed to us at the CRRC. A pain free way to get your room. In St Paul you will be 2 blocks from the Mississippi River, and in Las Vegas you will be right on the Strip. Great locations! Participants get 2 nights lodging in St Paul (or 3 if they register for the North Central CRRC meeting being held on May 29th) and 3 nights in Las Vegas.

Food:

Participants will be provided breakfast, morning breaks, lunch, and afternoon breaks during the workshops. You will also be provided transportation in St Paul from the Hotel to the University.

Questions:

Questions can be sent to Dr Wayne E Pauli at CRRC@dsu.edu. Please place "Prof Dev Training" in the subject line.

Link for Workshop or use the URL

https://tinyurl.com/y82e7n74

Prior to the Workshop in St Paul the North Central Region will be having a regional meeting. If you would like to join for this meeting, it is open, just register below. Please note that your travel date is 1 day earlier, and you get another night lodging. NSA representatives will be there. Metro State University is hosting this meeting also.

Link for North Central CRRC Meeting or use this URL

https://tinyurl.com/ycuh9ljl

being held May 29, 2019 at same location (travel date is May 28, 2019)