



## A S4 Bonus Training Opportunity Tuesday, 19 January 2010

### Using and Customizing SCADA Security Tools

Digital Bond's Control System Security Research Team is offering a special 6-hour, hands-on advanced security class to S4 attendees the day prior to S4. Class size is limited to 24 students, and there will be 4 instructors in the class. Spend an extra day in beautiful Miami Beach and learn how to use and customize security tools specifically built for control systems.

1. Use and customize Bandolier Security Audit Files for Nessus and other vulnerability scanners.

Bandolier is a Department of Energy funded project that allows an asset owner or vendor to audit the hundreds of security settings in a workstation or server component. Over twenty Bandolier Security Audit Files are available today. The first part of this module will show how to use the Nessus compliance plugin and Bandolier security audit files to perform low impact security testing, as well as how to analyze the results.

The class will then move quickly to modifying the Bandolier Security Audit Files. Students will learn how to customize the individual audit tests for their specific environment, how to delete non-applicable audit tests, and even how to write new audit tests.

2. Use and customize SCADA preprocessors, plugins and signatures for network IDS

Students will learn how to use the SCADA protocol preprocessors, plugins and signatures developed in the DHS funded Quickdraw project. The first step will be to write and trigger new SCADA IDS signatures that use the SCADA preprocessors and plugins. Then students will learn how to write a plugin to create new keywords that pull decoded SCADA protocol fields as well as some preprocessor internals.

#### Extra Credit

Students that master the course content will have the opportunity to learn how to access the Portledge detected cyber security events and corresponding event chains in a PI server.

Digital Bond will also open up its lab to students during the class. The lab contains many different brands of controllers, HMI and control system applications. Students can try to identify each of the systems and then run whatever attacks or tests they desire.

#### Prerequisites, Cost and Registration

- Understanding of networking and some programming experience is recommended. Digital Bond will provide preparatory materials in advance of the course for students who are less experienced. Multiple instructors will be available to help with varying skill levels.
- A laptop with CD drive and a wireless LAN card.
- Cost: \$600
- Registration: <https://www.digitalbond.com/event.php>

