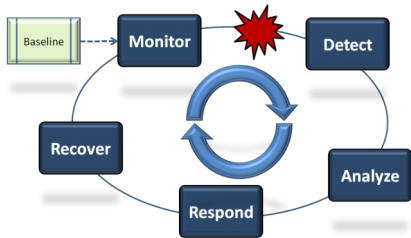


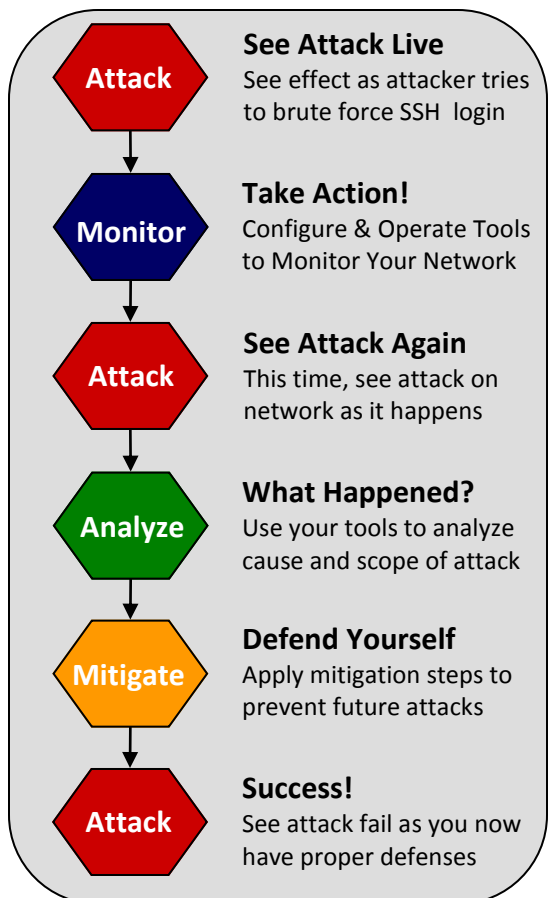
Registry Operations Curriculum: Secure Registry Operations Course



This three day workshop introduces ccTLD technical and operations staff to the security aspects of operating a registry. Students learn principles of proactively securing their registries in addition to monitoring and response. A structured approach guides students through creating a baseline, monitoring ongoing operations, detecting and analyzing cyber attacks, incident response, and recovery and mitigation strategies. Using hands-on exercises



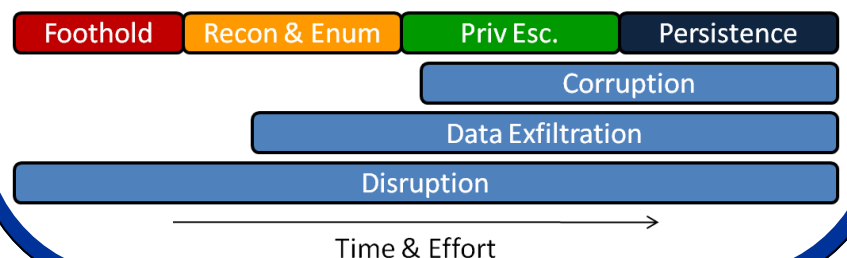
as the primary method of instruction, students see attacks, use monitoring and detection tools to analyze those attacks, and implement protective measures, all **LIVE** on the in-class network. The class architecture provides one “registry” network for every two students, allowing each small group to get hands-on experience in base lining, monitoring, detection, analysis and response. This course is made for students who want to evolve their skills and capacity to deal with the ever changing threats present on today’s Internet.



ATTACK CATEGORIES

Learn from a variety of attacks in each category

- Δ **Foothold** - Zero day, spear phishing, SQL injection
- Δ **Reconnaissance** - Port scanning, zone transfers
- Δ **Privilege Escalation** - Brute force, password cracks
- Δ **Persistence** - Root kits, stealth methods, awareness
- Δ **Corruption** - Web defacement, cache poisoning
- Δ **Disruption** - DDoS, reconfiguration, redirection
- Δ **Data Exfiltration** - Encrypted tunnels, obfuscation



Attack
Awareness

Monitoring &
Detection

Response &
Recovery

Mitigation
Strategies

This course is the last of a three part ccTLD capacity building program. The Registry Operations Curriculum (ROC) is a set of three hands-on courses which cover topics ranging from basic technical foundations of a ccTLD to security implementation. The first course in the series teaches network and registry operation basics, including operating systems and name servers. The second course in the series teaches network management and advanced registry functions, including architecture and management tools.

For more information on these courses, contact your regional TLD or ICANN representative