HARDENING WINDOWS NETWORKS TRAINING PROGRAM

Based on more than 15 years of security assessment and penetration testing experience, our Hardening Windows Networks Training Program goes beyond theory and best practices to deliver proven, field-tested solutions for mitigating, monitoring, and protecting Microsoft Windows based networks.

Students will learn effective countermeasures to defend against common attacks and exploit techniques in a hands-on virtual environment that resembles a real-world network. Upon completion of the course, students will be able to apply operating system and active directory hardening techniques, mitigate legacy software risks, and design tolerant networks that are resistant to present and future threats.

FEATURES

Students will harden a network consisting of:

- Microsoft Exchange
- Outlook Web Access
- Proxy Server
- Microsoft IIS
- Microsoft Windows 7/10
- MS Windows Server 2012
- Microsoft Windows SQL Server
- Microsoft Software Update Services
- Firewall

HIGHLIGHTS

- Common Exploitation Techniques
- Active Directory Group Policies
- Authentication Mechanisms
- Windows Auditing
- Log Monitoring and Alerting
- Oracle Java Deployment Ruleset
- Windows AppLocker/Software Restriction
- Host Firewall Configuration
- Network Traffic Analysis
- Proxy Server
- File System Security
- Microsoft LAPS
- Microsoft EMET
- SNORT intrusion detection

FINAL LAB

- Students will deploy host and network intrusion detection in a virtual windows network (SNORT, syslog, Windows events)
- Run automated attacks and identify the source, destination, and type of attack
- Harden a virtual Windows network
- Run automated attacks to test windows hardening

Course Dates and Locations

September 17th to 20th, 2019	London, Ontario
October 29th to November 1st, 2019	London, Ontario
November 26th to 29th, 2019	London, Ontario

For further information and please visit: www.digitalboundary.net
Or contact us: training@digitalboundary.net