Hosts

HARDENING WINDOWS NETWORKS TRAINING
March 14-17, 2017

COURSE OVERVIEW

A hands-on security course that teaches students how to harden, monitor and protect Microsoft Windows-based networks.

A hardening course based on more than 15 years of security assessment and penetration testing experience. This course goes beyond theory and best practices and delivers proven, field-tested solutions for hardening, monitoring and protecting Microsoft Windows-based networks. Students will learn in a hands-on environment that resembles a real world network consisting of Windows 2012 Servers, Windows 7 & 10, Exchange, SQL Server, IIS Server, Linux and more. Students will learn effective countermeasures to defend against common attack tools and techniques. 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.

On the first day, students are given the opportunity to learn, through hands-on exercises, the most common attack techniques. Digital Boundary Group custom, free and open source tools are used to enumerate and exploit Windows hosts found in our virtual network. Days 2 and 3 focus on attack mitigation using field-proven hardening techniques found in Windows, Active Directory Group Policy and implementation of free mitigation tools published by Microsoft and Oracle.

Students will install and configure a host and network intrusion detection system utilizing Syslog, Snort and Windows Events. Students can export the configuration files for easy deployment in their own networks.

On the last day students will take part in a final lab scenario consisting of two phases:

Phase One
Tests the Student's ability to implement a host and network intrusion detection system on a virtual Windows network. Students must identify intrusion attempts by running a set of automated attacks.

Phase Two

Tests the Student's ability to harden a virtual Windows network using the various techniques learned during the class. A set of automated attacks will attempt to break into the network, indicating success or failure of successful hardening.

COURSE DETAILS

Students will harden a network consisting of:

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

Review of Common Exploitation Techniques

- Password Attacks
- SQL Server Attack
- Token Stealing Attack
- Process Injection Attack
- Remote Exploits
- Client-Side Exploits
- Lateral Movement or Pivoting

Information Gathering and Prevention

- Null Session Enumeration
- SID/Name Translation
- NetBIOS Enumeration
- SNMP
- LDAP
- DNS

Active Directory Group Policies

- Time Synchronization
- Local Security Settings
- Top 8 Local Security Settings necessary to secure a Windows network
- Exploiting Windows systems before and after Local Security Settings hardening

Digital Boundary Group

User Account and Password Management

- Windows Password Hashing
- User Rights Assignment
- Least Privileged
- Securing Local Administrator accounts
- Securing Domain Administrator accounts

Authentication Mechanisms

- Securing passwords at rest (LM, NTLM, LSA)
- Securing passwords in motion (LM, NTLM, NTLMv2, Kerberos)

Auditing

- Default Windows auditing configuration
- Configure auditing to capture security events

Event Logs

- Default Windows event log configuration
- Log retention, rotation and archiving
- Event Log Analysis – Identifying security related events

Vulnerability Scanning Tools and Procedures

- Nessus Vulnerability Scanner
- Free and Open Source tools
  - Kali
  - Metasploit Framework

Microsoft Mitigation Tools

- EMET (Enhanced Mitigation Experience Toolkit)
- LAPS (Local Administrator Password Solution)

Oracle Java Mitigation Tools

- Java Deployment Ruleset Policy

Log Monitoring and Alerting

- Converting Windows events to syslog events
- Configure syslog to detect and alert on security events
- Monitoring firewall events

Host Intrusion Detection

- Implement a host intrusion detection system using Windows events and syslog

Network Intrusion Detection

- Implement a network intrusion detection system using firewall events and syslog
- Install Snort intrusion detection software
- Configure Snort as a network sensor and forward events to syslog

Securing Services and Service Accounts

- Locate Service Accounts on a Network
- Reduce or eliminate Domain Administrator privilege for service accounts
- Process injection attack to elevate privileges

Host Firewall Configuration

- Configure Microsoft firewall via GPO
- Strategies to defend against network Worms

Network Traffic Analysis

- Using Wireshark to analyze traffic

Proxy Server

- Configure proxy settings via GPO
- Analyze network attacks before and after proxy deployment

File System Security

- Share security vs. NTFS security
- Distributed File System
- Encrypted File System

Windows AppLocker/Software Restriction Policy

- How a software restriction policy can defeat many malicious attacks
- Implement and test a simple but effective software restriction policy

Software Deployment through Group Policy

- Deploying software in a hardened network
- Deploying software with Windows firewall enabled

Final Lab

- 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

Digital Boundary Group

UPCOMING COURSE DATES AND LOCATIONS:

March 14th to 17th, 2017	Broadview Networks, Winnipeg
May 9th to 12th, 2017	Broadview Networks, Winnipeg

COURSE COST:

- $2,975.00 + applicable taxes (includes refreshments and lunches each day, course materials and course tool-kit)
- 10% discount applied for two or more attending from the same company

CANCELLATION POLICY:

If you must cancel, please provide written notification via email to: training@digitalboundary.net.

- Cancellations must be received at least 15 business days in advance of the course start date in order to avoid a 50% cancellation fee.
- If cancellation notice is received less than 5 business days in advance of the course start date, the cancellation fee will be 100%.
- No refund will be made for non-attendance on the course.

Please Note: Business day means every day of the week except Saturday, Sunday and Statutory Holidays.

IF WE CANCEL YOUR COURSE

Occasionally it may be necessary for Digital Boundary Group to cancel your course (i.e., if registrations do not reach a required level). In this event, we will give you at least 5 business days' notice of the cancellation and will offer an alternative date. If the alternatives given are not convenient, you may cancel your registration at no charge.

Terms and Conditions:

1. Payment of the course registration fee, plus applicable taxes, is required to be received, at the address listed on the registration form, 15 business days in advance of the scheduled start of the course in order to complete the registration process.
2. Course fees must be paid by cheque made payable to Digital Boundary Group.
3. Confirmation of registration will only be made on receipt of full payment of the course fees and applicable taxes.
4. CANCELLATION POLICY: Please refer to above.

Digital Boundary Group

The International Information Systems Security Certification Consortium, Inc. accepts Digital Boundary Group's Security Training Program as credit toward meeting the Continuing Professional Education requirements to maintain the Certified Information Systems Security Professional (CISSP) designation (CISSP Constituents will earn 32 CPE credits)

Hardening Windows Networks Training Registration Form

Broadview Networks

Course Location: **1-1530 Taylor Avenue, Winnipeg, Manitoba R3N 1Y1**

Course Dates: **March 14-17, 2017**

Course Price: **$2,975.00 + 5% GST**

Student Name: _____

Position: _____

Name of Organization: _____

Address of Organization: _____

Telephone: _____

Mobile: _____

Fax: _____

Email: _____

Industry: _____

Fax completed registration to: (204) 984-9899 OR (519) 652-8660

Or mail completed registration and payment to:

Broadview Networks
1 – 1530 Taylor Avenue
Winnipeg, MB R3N 1Y1

OR

Digital Boundary Group
4226 Raney Crescent
London, Ontario N6L 1C3

For more information please call: 1-800-747-3557; Ext. 1 or (519) 652-1000; Ext. 1
Or email us at: info@digitalboundary.net

Digital Boundary Group