Network Vulnerability Assessment and Penetration Testing

Sir/Madam,

Greetings!

BitShield Security Consulting, Inc. invites you to an essential workshop, **NETWORK VULNERABILITY ASSESSMENT AND PENETRATION TESTING.** Please find below the details including the fee for your information and guidance.

Course Title:

NETWORK VULNERABILITY ASSESSMENT AND PENETRATION TESTING

DESCRIPTION

The training will take students into the realm of real-world hacking. Discover how hackers really work and execute - from this perspective, students will be able to understand hackers' styles and techniques - enabling them to strategize how to defend their corporate networks.

Fully understand the importance and business value of Penetration Testing, determine assets that requires security assessment, conduct Vulnerability Assessments, develop and execute Penetration Testing work plans, utilize security tools, manage security changes in a corporate setting and generate and analyze technical and managerial reports.

WORKSHOP OUTLINE

Module 1: Network Security Testing Overview

- Network Security Testing Methodologies
  - The Open Source Security Testing Methodology (OSSTMM)
  - The Information Systems Security Assessment Framework (ISSAF)
  - The NIST Guideline on Network Security Testing (SP 800-115)
- Information Security Testing Techniques
  - Passive and Active
  - DEMO: Passive and Active Gathering/Scanning
  - White-Box and Black-Box Approach
  - Blue Team and Red Team

- Phases in Network Security Testing
- Legal Perspective

Module 2: Footprinting and Information Gathering

- How information about a target may be gathered discreetly
- Acquiring target information (Passive Reconnaissance)
- Scanning and enumerating resources (Active Reconnaissance)
  - Network Mapping
  - Operating System and Services banner grabbing
  - Operating System and Services Fingerprinting

Module 3: Vulnerability Assessments (VA) Concept

- Definition of Risk, Vulnerability and Threat
- Risk Assessment
- Vulnerability Assessment Methodology
- Common Vulnerabilities and Exposure (CVE) list
- Vulnerability Assessment tools
- LAB: Vulnerability Scanner

Module 4: Windows Enumeration and Hacking

- Microsoft NetBIOS Names
- NetBIOS Name Service Enumeration
- LAB: NetBIOS Enumeration
- Microsoft RPC Services
- LAB: RPC Enumeration
- Microsoft SMB
- Enumerating Shares
- Enumerating Users, Group, SID (Security Principals)
- Automated SMB Enumeration Tools
- LAB: SMB Enumeration (via Null Session)
- SNMP Protocol
- LAB: SNMP Enumeration
- Windows DNS Enumeration
- Directory Service Enumeration
- LAB: Automated Windows Enumeration Tools

Module 5: Firewall & IDS Evasion

- How attacks may traverse a firewall
- The role of intrusion detection & how it may be evaded using advanced techniques
- LAB: Evasion Tools

Module 6: Exploits

- Memory Organization
- Buffer and Heap Overflows
- Attacking with Metasploit
- Pilfering target information
- Metasploit Framework
- LAB: Metasploit Framework

Training Investment Fee:

P20, 000 +VAT

Training Package:

Training Materials
Certificate of Completion
Meals (Lunch and AM/PM Snacks)

Duration: 3 days
Tentative Schedule: January 20-22, 2016
Time: 8:00 am to 4:00 pm
Venue: TBA

REGISTER NOW

Limited Seats Only!!

For reservation / inquiry please call us
Tel. (02) 661.9118

Ask for Grace

Or text / call **0946.2374453**

Email: **training@bitshieldsecurity.com**

If you have other concerns, please do not hesitate to contact us and we will be glad to assist you. Thank you very much and we are looking forward to have you as one of our attendees in the future.

Very truly yours,

Mary Grace Ibarreta
InfoSec Account Consultant