ECC Advanced Network Defense (CAST 614) – Hardening Your Enterprise

Course Outline:

Module 1: Firewalls

- Firewalls
- Firewall Types: Stateless Packet Filters
- Improving Device Remote-Access Security
- Locking Down the Console Port
- Protecting Terminal Lines
- Establishing Encrypted Communications
- Configuring HTTPS
- Configuring SSH

LAB: Securing the Perimeter

Module 2: Advanced Filtering

- Advanced Filtering Techniques
- Ingress Filtering
- Egress Filtering
- Source Address Verification (SAV)
- uRPF
- Additional Filtering Considerations
- Time-Based ACLs
- Reflexive ACLs
- Reflexive ACL vs. Static ACL

- Context-Based Access Control (CBAC)
- Essential Steps to Harden Routers
- LAB: Advanced Filtering

Module 3: Firewall Configuration

- Firewall Types: Stateful Packet Filters
- Application Proxies
- Application Proxies vs. Stateful Packet filters
- Web Application Firewalls
- Web Application Firewall Types
- Web Application Firewall Products
- Firewall Architecture
- Screened Subnet Firewall
- The Classic Firewall Architecture
- Belt and Braces Firewall
- Separate Services Subnet
- Fortress Mentality
- De-parameterization
- Perimeter Configuration

Lab: Selecting a Firewall Architecture

Module 4: Hardening: Establishing a Secure Baseline

- Windows NT/2000/2003 and XP
- Windows 2000/2003/XP
- Windows 2003
- Windows Vista
- Server 2003 Architecture
- Broken Kernel
- Modes of the OS
- UNIX/Linux
- Secure Server Guidelines
- Hardening Systems
- Security Compliance Manager
- Device Security
- Essential Steps to Harden Switches

LAB: Hardening

Windows Server 2008/2012 Security (Part I)

- Server 2008 Components
- Server 2012 Components
- Enterprise Protection
- AD RMS
- AD RMS Components
- EFS
- EFS Enhancements in Server 2008/2012
- EFS Best Practices

LAB: Server 2008 Lab

Windows Server 2008/2012 Security (Part II)

- IPsec Rules
- Firewall Scripting
- netsh
- Isolating a Server
- Group Policy Object
- Server Isolation Steps
- Domain Isolation
- Domain Isolation Issues
- Best Practices
- Trusted Platform Module
- Wave Systems
- TPM Architecture
- Crypto API
- Example
- Embassy Server Software
- Embassy Client Software
- Self-Encrypting Drives

LAB: TPM

Module 5: Intrusion Detection and Prevention Why Intrusion Detection?

- Windows 2003, 2008, 2012 & 7 & 8
- Fortress Mentality
- Intrusion Detection 101
- What is Intrusion Detection?
- False positives!
- Topology concerns
- Recommended in most circles
- Realistic
- Intrusion Prevention
- Types of IPS
- Host-Based Intrusion Prevention Systems

LAB: Intrusion Detection

Module 6: Protecting Web Applications

- Windows 2003, 2008 & 2012
- Top 10 www.owasp.org
- Injection Flaws
- Cross Site Scripting
- Broken Authentication
- Insecure Cryptographic Storage
- Reverse Engineering Web Apps
- Tools
- Hackbar
- Tamper Data
- The Two Main Attacks for Web
- XSS
- SQL Injection
- xp_ cmdshell
- There is More
- More Tools
- SQL Inject Me
- XSS ME
- Choose The Right Database
- Practice, Practice, Practice
- Tutorials

- Mutillidae
- Web Application Firewalls
- Components of Web Application Firewall

LAB: Protecting Web Apps

Module 7: Memory Analysis

- Data Types Revisited
- Volatile
- System date and time
- Current network connections and Open ports
- Processes that opened ports
- Cached NetBIOS Names
- Users Currently Logged On
- Internal routing
- Running Processes
- Pslist
- Trivia
- Pslist –t
- Tasklist
- Tlist
- Running Services
- Open Files
- Process Memory Dumps

LAB: Memory Analysis

Module 8: Endpoint protection

- Introduction to NAC
- NAC Defined
- NAC General Architecture
- NAC General Architecture Illustrated
- NAC Concepts
- Inline NAC
- Out-of-Band
- Identifying NAC Requirements
- Implementing User-Based Identity Access Control

- Network Access Protection (NAP)
- NAP Components
- NAP Enforcement
- NAP Best Practices
- 802.1x
- EAP Explained

LAB 1: Network Access Protection with DHCP

- EMET
- Micro-VM

LAB 2: Endpoint Protection

Module 9: Securing Wireless

- Wireless Tools
- Wireless Vulnerabilities Summary
- MAC Filtering
- Hiding Access Points
- Hijacking
- Jamming
- Identifying Targets
- Wardriving
- Sniffing on Wireless
- Attacking Encrypted Networks
- Wep Data
- The other case
- Reality
- WPA Tools
- WPA
- LEAP
- Asleap
- Comparison

LAB: Securing Wireless