DoD Shared Service Center

for

ISS LOB

Tier I Security Awareness Training a

and

Tier II Role Based Training

UNCLASSIFIED

DoD ISSLOB Annual Awareness Training

- FY11 product in use (DoD, Federal, IC)
- FY12 product funded
- Customer Conference planned for annual update
  - Last week of March
  - Provide feedback on FY11 product
  - Identify new topics, modifications for FY12
- For FY12, two versions only
  - Federal/IC
  - DoD/IC
- Either product will satisfy DoD requirement for annual awareness training
- Currently there is no requirement for more than annual training, but
  - DISA products available to support more frequent awareness training

DoD Annual Awareness Training FY13 and Beyond

- FY 13 product
  - Serious/learning game
  - First increment funded
- One product,
- Three “skins”
  - Federal civilian/IC
  - DoD civilian/IC
  - Military/IC
- Multiple venues: office, home, public site, deployed
- Will be “approved” by DoD Computer-Electronics Accommodations Program (CAP) as being 508 compliant
- Keep content and delivery current

DoD Tier II Training

- **Education, Training and Awareness Catalog (http://iase.disa.mil)**
  - **Free access to full suite of courses**
  - **Web-based, CD ROM and video mediums**
  - **Customization & tailoring not available**
  - **Tracking not available**

- **DoD content being moved to FedVTE**
  - **Over 450 on-line lectures and screencasts**
  - **50 hands-on labs w/ asynchronous instructors**
  - **Learning management system tracking capability**

Tier II Training Alignment

NIST 800-16/800-50

Manage	Acquire	Design and Develop	Implement and Operate	Review and Evaluate

IA for Acquisition Professionals (DAU product)

Representative DISA Products

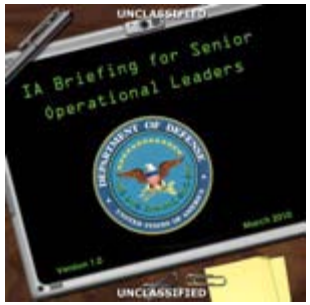
IASE.DISA.mil

IA Awareness Training

- Personal Electronic Devices (PED's)
- Using PKI
- Phishing Awareness
- Personally Identifiable Information (PII)
- Information Operations (IO) Fundamentals
- Information Assurance Awareness Shorts

IA Training for Senior Leaders

- IA Briefing for Senior Operational Leaders



IA Simulations

- CyberProtect

Training for IA Professionals

- Information Assurance Policy and Technology (IAP&T)
- Information Assurance for Professionals Shorts
- IA Hot Subjects
  - Transmission Control Protocol (TCP) reset
  - Distributed Denial of Service (DDoS) Attacks on Routers
  - Spoofing attacks
  - Remote access/remote control
  - Physical security review
  - Simple Network Management Protocol

Advanced CND Analyst Training

- RaD-X (301) delivers hands-on CND scenarios primarily focused on Firewall and IDS analysis and configuration
- Students defend realistic network through simulated network traffic and users (simulation provided by scripts, SAST, and realistic assets)
  - Instructors launch attacks
  - Students defend and respond using:
    - IDS technologies (Sourcefire, Intrushield, etc.)
    - Firewall configuration impact on attack success
    - Server and workstation configuration settings to defend against attacks
- Marriage of RaD-X Curricula with BULWARK DEFENDER exercise results
- Customization & tailoring, train the trainer availability TBD (at cost)
  - Contact DIAP
  - Mobile equipment suite

RaD-X 301: Labs 1-4

Excessive User Rights and Unauthorized software

Policies and technical measures designed to block this activity are often imperfect, and users may find ways to evade controls and engage in these activities.

Client Side Attacks and Detection

Client side attacks are one of the most difficult forms of attack to block. Failure to secure and patch and client on a systems (such as browsers, word processors, spreadsheets, media players, etc) can lead to compromise of the client system.

Server-side Vulnerabilities

Server-side attacks have lead to some of the most devastating attacks in network history, including the widespread 'Blaster' and 'Sasser' worms. In this lab, an actor will successfully attack a windows server via the network. Failure to patch a server for the MS06-040 will lead to direct system compromise.

PHP Attacks and Detection

Web applications are complex, and mis-configuration and lack of patching can lead to server compromise. In this lab, a web server hosts a bulletin board written in the PHP language. The server is missing a critical security patch, and will be compromised by an actor, live over the network.

RaD-X 301: Labs 5-6

The Intrusion Detection / Response Challenge

Students will respond to:

Lab 5

- **Outside attackers' DDoS attack**
- **Attackers' port scans**
- **Attackers' DNS zone transfer**
- **A user who is violating policy by using an internet chat program**
- **A system on our network which has previously been infected with a bot**

Labs 6&7

- **A Windows server that is infected via a server-side attack**
- **A Linux server that is infected via a server-side attack**
- **A database server that is compromised via an SQL injection attack**
- **An internal client that is compromised, and is currently being used by attackers to 'pivot' to attack other internal systems**
- **Attackers' attempting to exfiltrate sensitive data**

RaD-X 101

- Classroom: 4 days with 6 hands-on IA event labs
- Introduction course to prepare students to meet RaD-X 301 requirements
- Learning objectives include:
  - Basic IDS tuning
  - Firewall ports and protocols settings and configuration for the DoD
  - Basic IT and IA technology understanding for implementing networked IA devices and technologies
- Currently developing RaD-X 101 WBT training product (FY 2011-2012)
  - Asynchronous Delivery over DCO (Direct Connect On-Line)
  - FY 2011 will be the last year for platform class

Representative VTE Content

- Hardening Windows Operating Systems
- Information Security for Technical Staff
- Intro to Cisco for Security Professionals
- Introduction to IPv6
- Introduction to Networking
- Managing Enterprise Information Security
- Network Vulnerability Assessment
- Vulnerability Assessment and Remediation
- Wireless Communications and Wireless Network Security
- Forensic Specialist
- Fundamentals of Incident Handling
- IA Managers and IA Technical, Levels 1-3 Courses
- HBSS
- CISSP Prep
- Cisco CCNA Survey
- Cisco Network Security 1 & 2
- CompTIA Network+ Prep
- CompTIA Security+ Prep

DoD Points of Contact

- George Bieber, george.bieber@osd.mil,
- Cathy Fillare, catherine.fillare.ctr@osd.mil, 703-699-0131
- Maryann Dennehy, Director, DISA IA Training Program maryann.dennehy@disa.mil