Implications of Security and Accreditation for 4DWX (Information Assurance)

By
Scott Halvorson
Forecasters Training
26 February 2009
If I [user] am doing my job, then they [DOIM] are not doing theirs!

If they [DOIM] are doing their job than I [user] am not doing mine!*

*Van Pool Rider
DOIM

- **USB Virus (2008)**
  - Affected Windows
  - Several million dollars in damages and eradication
  - Loss privileges to use USB storage devices

- **Suckit Root Kit (2004)**
  - Affected Linux
  - Breached DoD, National Labs, etc.
  - Shutdown 4DWX ~3 months
Information Assurance Trend

- Best Business Practice
- Army
- RDT&E Met

EXPENSIVE

TIME ➔ DIACAP (Current)
1/1000 Rule

Mitigating known vulnerabilities costs only one unit!

An exploit on an unmitigated vulnerability can cost 1000(s) units!
DIACAP (DPG)  
DoD Information Assurance Certification and Accreditation Process  
(DoD Instruction 8510.01)
"Between all the day-to-day security concerns and the compliance requirements, I forget what my real job used to be."
4DWX Accreditation (Mitigation Process)

- Migrate 4DWX to the DMZ
  - Allow remote access
  - Allow single method of authentication
- Loss of administrative rights
  - NCAR
  - Local Users
  - Need to be level II certified
- Harden Linux/Windows systems
  - DoD approved security assessment tools
  - Manual mitigate “Findings”
  - CAT I, II, III vulnerabilities must be ALL mitigated
  - Mitigation process broke many applications
4DWX Accreditation
(Mitigation Process)

- Incorporate additional applications (DoD approved)
  - Antivirus
  - Host base intrusion detection
  - Auditing

- Paperwork
  - Summary of backup/recovery procedures
  - Summary of software applications
  - Sign acceptable usage policy (everyone)

- Physical security walk through
Mitigating the Stress

- Understanding the documentation and regulations (not easy)
  - Knowing your rights
  - Mitigating issues (planning)
  - New or changed policies

- Working and mitigating issues through DoD approved vulnerability assessment tools (derived from the STIGs)
DoD Approved Vulnerability Assessment Tools

- **Security Readiness Reviews**
  - Unix/Linux
  - Web Servers (Apache)
  - DISA Gold Disk (Windows XP)

- **CSA Tool Scan**
  - Developed by “Ware On Earth” for HPCMP

- **OVAL**
  - Open Vulnerability Assessment Language
  - [http://oval.mitre.org/](http://oval.mitre.org/)

¹DoD CAC required to download tools
Level II – System level privileges (root access)

DoD Manual 8570.01-M (15 May 2008)
  - Baseline for Level II
    - Security+
    - Commercial certification in computing environment of administration

AR 25-2 Section 4-3 training requirements
  - Must complete Level I certification
    - IASO course ([https://ia.gordon.army.mil](https://ia.gordon.army.mil)) – estimated time: 2-3 working days
    - IA Technical Level I course (SkillPort>CIO G-6/NETCOM Information Assurance> Technical Level I Certification – 11 modules) – estimated time: 5-7 working days.
Documentation

DoD Directives and Instructions

DISA Security Technical Information Guides (STIG)

Army Regulations 25-1, 25-2, 380-5

DIACAP Guidance
http://iase.disa.mil/ditscap/ditscap-to-diacap.html#diacap

NSA Secure Guidance on RedHat Enterprise 5
Recommendations

- Assign a POC for each met team that can:
  1. Periodically review documentation
  2. Work on POA&M (Plan of Action and Milestones) to mitigate security issues

- During accreditation processing have an NCAR or Level II certified admin on site during assessment/mitigation period

- Be Proactive!
Lessons Learned from DPG DIACAP Process

– Used the following documents to harden the OS
  • DISA STIGS
  • NSA Guide on Red Hat Enterprise 5
– Configuration Vulnerability Assessment
  • DISA Security Readiness Review
  • HPCMP CSA (Comprehensive Security Assessments)
– IAVA Vulnerability Assessment
  • Harrisstat or Retina Eye
  • Need to be done by certified range staff
– Documentation (Ongoing)
ARMADA, NPORT & (New) Metbox Accreditation

- External threat mitigation
  - Tools
    - IP tables (Firewall)
    - TCP wrappers
    - Audit reviews
  - Access control list
    - Implicit deny (deny all)
    - Explicit allow (define host, user, etc.)
    - No remote root access!
  - Strong Passwords
    - 15 characters
    - 2 upper, 2 lower, 2 numbers, 2 special characters
    - Changed every 60 days
ARMADA, NPORT & (New) Metbox Accreditation

- **Internal threat mitigation**
  - **Tools**
    - Host based Intrusion Detection
      - AIDE (Advanced Intrusion Detection Environment)
    - Antivirus (McAfee)
    - SELinux (Security Enhanced Linux) – target
  - **Vulnerability Assessments**
    - IAVA (Information Assurance Vulnerability Alert) compliance
      - Remote vulnerability assessment tool
      - Applying security patches
    - DoD STIG compliance
      - CSA
      - Security Readiness Review (SRR)
    - Mitigate “Findings”
  - Monthly OS upgrades
Physical security

- Locked case (?)
- Bios password
- Grub password (single user mode)
- Only bootable from system disk
- Only root or user defined in sudo can reboot or shutdown
  - CTRL-ALT-DEL disabled

ARMADA, NPORT & (New) Metbox Accreditation
Crystal Ball

- Networthiness – software approval*
- SELinux (Security Enhanced Linux)
- 2 Methods of authentication (Linux/Test Networks)
  - Something you know (Pin/Password)
  - Something you have (CAC/SecureID)
- Linux will be required to use LDAP and/or Kerberos (Active Directory?)
- Internet Protocol Version 6 (IPV6)
  \(2^{128}\) or \(3.4 \times 10^{38}\) Addresses

*Now
Summary

- DIACAP
  - Plan on a lot of work!
  - Plan on changes in data processes!
  - Know your rights!

- ARMADA/NPORT/Metbox
  - Mitigate threats based on STIGS
    - External
    - Internal
    - Physical
  - Mostly DIACAP compliant
Questions?