

# Compliance Assessment Team (CAT ) Full Scope Security Assessments



**Connect. Integrate. Collaborate.**

31 August 2009

**Gene Bransfield and Tim Watt**

IC CIO / ICIA / Compliance Assessment Team Security Engineers



CREATE DECISION ADVANTAGE

Accurate as of  
11 March 2009

UNCLASSIFIED

*Intelligence Community Chief Information Officer*

# Background

- **Purpose and Scope of Briefing**
  - Provide an overview of the IC CIO Compliance Assessment Team (CAT) approach to Full Scope Security Assessments
  
- **Who We Are**
  - Team of Defensive Security Engineers supporting the IC Senior Information Security Officer (SISO)
    - Expertise in IC IA Policy
    - Expertise in Information Security Engineering
    - Expertise in Vulnerability Assessments and Full-Scope Security Assessments
    - Expertise in Cross-Domain Security Engineering



## CAT – What we do?

- **Advise the IC SISO:**
  - Technical aspects of policy decisions
  - Appropriate mitigations for potential risks
- **Support programs of IC & DoD interest**
- **Services Provided**
  - Advice and Assistance throughout the System Development Lifecycle (SDLC)
  - Verification and Validation Testing
    - Lab Testing
    - Site Testing
  - Full-Scope Security Assessments
  - Penetration Testing (White-Box or Black-Box)



# Additional CAT Services

- **Architecture Analysis during evaluation**
- **Keep aware of trends, and apply trend analysis to systems**
  - Just cause it wasn't a threat 2 years ago doesn't mean it isn't now
- **Translate security requirements into English and vice versa**
- **Translate systems jargon into English and vice versa**
- **Recognize and attempt to remediate over-engineering**



# We are not Omnipotent

- **No one team member is an expert in all systems**
  - Leverage each other's experience and insight
  - Leverage the experience of the developer
- **Not 1337 H@xz0rs**
  - We cannot successfully pull off every hack known to man
  - Just because we can't leverage a vulnerability doesn't mean that that vulnerability cannot be leveraged
- **Not an Approval Authority**
  - We report findings to the relevant Decision Makers
  - Decision Makers say "yes" or "no"
- **Not trying to make your system fail accreditation**
  - We want the systems to pass – and will help as much as we can



# Full Scope Security Assessment

- **Assessment of System and/in its Environment:**
  - Documentation
    - System
    - Procedures (aka Certification Test Procedures)
  - System and its Surrounding Support Structure
    - Secured properly; formal test procedures, malicious user testing, penetration testing
    - Offer proper protection
  - Personnel
    - Qualified Personnel
    - Properly trained
  - Risks and Threats offered by all of the above



# Security Assessments: Standardization

- **CAT DCID 6/3 How-To Guide**
  - Endorsed by IC CIO
  - Free to both Developer and C&A Communities
    - Some OS-specific versions available
  - Basis used for CAT evaluation process
  - Will be working on 800-53 version
- **Eliminates Subjectivity**
  - Black & White descriptions
  - Written description controls subjectivity
- **Eliminates Misinterpretation**
  - Plain-English description of expectations
- **Provides Consistency**
  - Each requirement is addressed
  - Written description controls evaluation



## Security Evaluations:Docs:SSP

- **Does the SSP Describe the Security Features of the System?**
- **Is the SSP a Work of Fiction?**
  - System profile and capabilities accurately depicted
- **Shared with the Community**
  - Senior Decision Makers should not be surprised
- **Reciprocity**
  - System does what the SSP says, then there's a lot less to complain about from our end.



# Security Evaluations:Docs:User Guide

- **Privileged/Administrator User guide**
  - Readability
  - Accuracy
  - Proper Methodology (root is wrong)
  - In use
  
- **General User's Guide (End User)**
  - Readability
  - Accuracy
  - Functionality



## Security Evaluations:Docs:CTP

- **Developer Prepares Certification Test Procedures (CTPs)**
  - Procedures fully address requirement?
  
- ***Vehicle Test Drive***
  - *You are buying the car*
  - *Dealer dictates test drive methodology*
    - *Generally Insufficient*
      1. *Pull out of parking spot*
      2. *Pull back into parking spot*
      3. *Test drive complete*
  - *Some people would buy it anyway*
  - *Dealer said this was standard test*



# Security Evaluations: Docs:Supplemental Testing

- **Supplemental testing**
  - Ensures requirements are fully addressed
  - Fills any “gaps” in the submitted and executed CTPs
  - Each test tied to a requirement
  
- **Test Drive**
  - *In addition to parking, we will*
    - *Take it around the block*
    - *Take it out on the highway*
    - *Take it on a curvy road*
    - *Test lights, tires, turn signals, etc...*
    - *Other, depending on requirements...*



# Security Evaluations: Surrounding Support Structure

- **Firewalls**
  - Firewall part of the deployed solution?
  - Proper Firewall rules
  
- **ACLs**
  - On the switch, router, or host
  - Part of the deployed solution
  - Properly applied
  
- **Interactive Systems**
  - Part of the deployed solution
  - Properly hardened



## Security Evaluations: Personnel

- **Properly Trained Personnel**
  - Windows geek should not be expected to administer a Solaris 10tx machine
  - Solaris 10 geek should not be expected to administer a Cisco Firewall
  
- **Competent Personnel**
  - Can the Administrator do their job?
  
- **Findings for Personnel issues have been reported.**



# Penetration Testing

- ***Penetration testing is performed to identify weaknesses and vulnerabilities of a system within its operational environment***
- **Traditionally performed from the perspective of an outsider with no privileged access**
- **CAT normally includes additional malicious user testing to evaluate susceptibility to the insider threat**
- **Limitations defined by Rules of Engagement:**
  - Network Mapping
  - Social Engineering?
  - Vulnerability Exploitation?
  - Temporary Modification or Creation of Files?
  - Installation and Use of Executable Files?



# Penetration Testing Process

- **Document Acceptance**
  - Constitutes approval to conduct penetration testing against the system in accordance with the procedures and restrictions contained within the Rules of Engagement (ROE)
    - Determines test perspective
    - Determine target network
    - Identify appropriate site personnel to contact to alert of potential network attacks and/or successful intrusions
    - Establish test hours and impact coordination
  
- **Tests conducted in four phases**
  - Phase One – Planning and Enumeration
  - Phase Two – Vulnerability Analysis
  - Phase Three – Execute Attacks
  - Phase Four – Reporting and Follow-up



# CAT PenTest Tools

- **Backtrack CD, as customized by the CAT**
  - Includes large number of specialized and general-purpose attack tools (*e.g., Metasploit*) and custom Cisco exploit tools
  - Contains useful network reconnaissance and sniffing tools (*e.g., wireshark, p0f, hping, fping, other Unix-like network management tools*)
  
- **User-accessible programming and scripting languages**
  - E.g., (x)sh, Perl, Python, Windows Powershell, and others which are commonly found on systems under evaluation
  
- **User-accessible application scripting languages**
  - E.g., StarBasic/OpenOffice Basic, GIMP Script-fu, and Microsoft Visual Basic for Applications



# Malicious User Testing

- **Extremely relevant for cross-domain systems**
  
- **Trust of Single Admin Presents Greater Risk**
  - Can create full-duplex circuit between security domains
  - Greater attention to detail
    - Least Privilege
    - Role Separation
  
- **Privileged User elevation of privilege**
  - Very relevant vulnerability
  - System Admin
  - Security Admin



# Security Assessments: Common Problems

- **Subjectivity**
  - Evaluations tainted by an evaluator's personal bias
  - Evaluator deeply involved in development
    - Evaluator already “knows” the answers
  
- **Misinterpretation of Requirements**
  - Lack of thorough understanding of security concepts
  
- **Lack of Consistency**
  - Evaluation Standards change for no valid environmental reason



# Most Common Flaws Found

- **DOCUMENTATION**
  - Should show actual state of system
  - Administrators should have a source of reference
  
- **System Misconfigurations**
  - Usually results from poor Configuration Management (CM) practices
    - Development artifacts
    - Incomplete configuration
  
- **Lack of proper network isolation**
  
- **Improperly implemented access controls**
  - Role separation
  - Concept of least privilege



# Scenario 1

- **While performing a network scan, you notice every machine is vulnerable due to the same flaw.**
  - Pwn?
- **Developer/Program Office patch the machines against the flaw and ask for a re-scan to validate mitigagions**
- **Adequate mitigation?**



## Scenario 1 cont.

- **FAIL!!!!!!**
- **Problem goes beyond patching one flaw**
- **Patch Management**
  - Addressed in SSP
- **What is the patch management mitigation?**



## Scenario 2

- **During the security evaluation, you notice configuration settings that are not in line with what is described in the SSP (i.e. telnet is enabled).**
- **Developer says that those configuration changes were made during troubleshooting; and “Bob does that all the time.”**
- **Developer mitigates finding by fixing the configuration**
- **Appropriate?**



## Scenario 2 cont.

- **FAIL!!!!**
- **Finding indicates a lack of proper Configuration Management**
- **System at this level in the development cycle should be under the stated Configuration Management Policy**



# Sad Truth

- **At the book store, how many books to you see on:**
  - Effective Patch Management
  - Effective Configuration Management
  - Hacking
  
- **Which provides greater Return on Investment?**
  - Paying for a Penetration Test
  - Investing time and resources on effective patch management and configuration management



## Scenario 3

- **During a system development control gate review, you notice a design flaw**
- **Citing a documented security requirement, you suggest a mitigation to the design flaw**
- **Govt. Program Manager states that the mitigation would drastically affect the schedule; and that the Govt. PM will not fix the flaw and accept the risk.**
- **Appropriate?**



## Scenario 3 cont.

- **FAIL!!!!!!**
- **Govt. PM does not have the purview to accept the risk for the community**
- **Only the DAA may accept the risk**



# CAT & Reciprocity (Success Stories)

- **MDDS 3.1.2**
  - Evaluated by IC; DIA & DNI IC CIO CAT
  - Evaluated against DCID 6/3
  - DoD identified “gaps” in the Body of Evidence
    - Hundreds of RDAC requirements
    - Roughly a dozen “gaps”
  - RDAC Rating issued based on provided information



# CAT & Reciprocity (Success Stories)

- **DTW 4.1**
  - Evaluated by IC; DIA & DNI IC CIO CAT
  - Evaluated against DCID 6/3
  - DoD identified “gaps” in the Body of Evidence
    - Hundreds of RDAC requirements
    - Roughly 17 “gaps”
  - NSA I-173, DIA, DNI IC CIO CAT Engineers held TEM; reduced number of “gaps” from 17 to 8
  - CAT Engineers travelled to AFRL and evaluated “gaps” for NSA I-173
    - NSA I-173 accepted results to fill gaps
      - 3 days, \$5K
    - NSA I-733 reduced Penetration Testing window to 1-month



# War Stories: Favorite Quotes

- **What's the REAL risk?**
  - “The devil finds work for idle hands to do!”
- **Why would anyone ever do that?**
  - “The devil finds work for idle hands to do!”
- **You HAVE to trust SOMEONE**
- **What's ARP spoofing?**
- **We don't secure this system because it's in the DMZ**
- **We are removing extra software to prevent the system from overheating**



# War Stories: Best Ways to Fail

- ✓ CTPs not executed prior to test date
- ✓ Any SOPs require use of 'root'
- ✓ SysAdmin can create and utilize a SecAdmin (or vice versa)
- ✓ Role separation properly configured, but there is one user with all roles
- ✓ MAC enforcement disabled but system still runs with full connectivity
- ✓ GAMES
- ✓ Default label encodings file in use
- ✓ Not using official classifications
- ✓ System Development is not complete
- ✓ Your password list is “securely” stored in a Windows network share on JWICS
- ✓ Documentation states you're running Solaris, but you're actually running Windows.
- ✓ Ostentatiously dropping the DCID in the trash in front of an evaluator
- ✓ “How did that get there?”
- ✓ Giving half the root password to the SysAdmin and the other half to the SecAdmin
- ✓ Development environment is the same one your wife and kids use to surf the Internet
- ✓ If you've got hacking tools on the system



# Conclusion and Questions

- **We're here to help!**
- **We are committed to providing appropriate recommendations to programs to assist in eliminating or mitigating vulnerabilities**
- **Questions?**



# Contact Information

- **Calleen Torch, CAT Chief**
  - torchcr@dni.ic.gov, calleen.r.torch@ugov.gov
- **Timothy Watt, CAT Team Lead**
  - watttim@dni.ic.gov, tim.watt@ugov.gov
- **David Muran, CAT Tech Lead**
  - murande@dni.ic.gov, david.a.muran-deassereto@ugov.gov
- **Corinne Castanza, CAT Security Engineer**
  - castor@dni.ic.gov, corinne.castanza@ugov.gov
- **Gene Bransfield, CAT Security Engineer**
  - bransfe@dni.ic.gov, gene.j.bransfield@ugov.gov
- **Jack Kirk, CAT Security Engineer**
  - kirkjac@dni.ic.gov, jackie.g.kirk@ugov.gov
- **Jerry Tillery, CAT Security Engineer**
  - tilleje@dni.ic.gov, jerald.j.tillery@ugov.gov



# BACKUP SLIDES

- **BACKUP SLIDES**



## Advice and Assistance (A&A)

- **Unrelated to Security Evaluations**
- **Offered during the Design and Development phase of system**
- **Help ensure proper compliance with DCID 6/3 by identifying design flaws early in the SDLC**
- **Provide recommendations vice solutions to projects**



## Verification and Validation (V&V)

- **Process of checking and testing that security controls are:**
  - In place
  - Functional
  - Correctly configured
- **Different test scenarios**
  - Lab testing
  - Site testing
- **Results in a report identifying problems with the system and describing the specific risks associated with the individual problem**



# V&V Test Process Details

- **Lab Testing**
  - This phase of testing is referred to as Certification Test and Evaluation (CT&E)
  - Conducted against a system in a controlled environment
  - Lab system should NOT be mission-critical or in production environment
- **Site Testing**
  - This phase of testing is often referred to as Security Test and Evaluation (ST&E)
  - Conducted against a fully-configured and operational system
  - Objective is to determine the effectiveness of the security controls in place at the site and confirm that no configuration changes have been made which compromise the security of the system
  - May include penetration testing





# Phase One – Planning and Enumeration

- **Identify scope and goals of the exercise**
- **Enumerate**
- **Document penetration plan**



# Phase Two – Vulnerability Analysis

- **Identify targets**
  - Port Scanning and Host Identification
    - Provides more detailed information about network services that are running on accessible hosts
    - Tools employed to analyze TCP/IP "fingerprint" of accessible hosts in order to identify host Operating System (OS) or other software running on a host
      - Perform vulnerability scans
  - Identify potential vulnerabilities
  - Use commercial and freeware automated security scanning tools (e.g., Nessus)
  - Use manual procedures as needed to identify any vulnerabilities or misconfigurations not detected during automated scanning



## Phase Three – Execute Attacks

- **Test potential vulnerabilities identified in phase two by attempting to exploit them**
  - Techniques employed during this phase of testing will vary tremendously based upon identified system types and vulnerabilities discovered
  - Other techniques may be developed on site as needed by the penetration team
  - If the tests indicate that vulnerabilities do exist, safeguards will be identified to mitigate the associated security exposure



## Phase Four – Reporting and Follow-up

- **External testing is complete when one of the following three criteria is met:**
  - Test team has exhausted all reasonable penetration attempts
  - Program calls a halt to the test
  - Scheduled penetration testing period has ended
  
- **Restoration**
  
- **Penetration Test Report**

