REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	Spring 1998	Newsletter Vol. 1 No. 3

4. TITLE AND SUBTITLE
Information Assurance Technology
IA Newsletter

5. FUNDING NUMBERS

6. AUTHOR(S)
Information Assurance Technology Analysis Center

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

A

13. ABSTRACT ***(Maximum 200 Words)***

The Information Assurance Technology Newsletter is published quarterly by the Information Assurance Technology Analysis Center (IATAC). The third issue continues the focus on current information assurance initiatives underway within the Department of Defense. In addition, an overview of the IA Tools Database is provided that highlights the current collection of Intrusion Detection tools.

14. SUBJECT TERMS
Information Security, Information Assurance, Intrusion Detection

15. NUMBER OF PAGES
7

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	None

INFORMATION ASSURANCE TECHNOLOGY

Newsletter

IATAC is a DoD Sponsored
Information Analysis Center

Spring 1998

DEFENDING AGAINST C2W AND IW ATTACK

Editor's Note: This article is part of a continuing series that highlights current Information Assurance (IA) initiatives within the Department of Defense. The Joint Command and Control Warfare Center (JC2WC) is located at Kelly Air Force Base (AFB) in San Antonio, Texas.

by Colonel Charles C. South, USAF
Deputy Director for Protect/
Defense, Joint Command and
Control Warfare Center

The mission of the Joint Command and Control Warfare Center (JC2WC) is to "provide direct Command and Control Warfare support to operational commanders"[1] and serve as the principal field agency within the Department of Defense (DoD) for non-Service-specific C2W support. The JC2WC executes its mission through its directorates of Operations (OP), Protect / Defense (PD), Operations Support and Technical Integration (OT), Systems Integration (SI), the Office of Plans and Programs (XR), and the Special Technical Operations (STO) Division. The focus of the Protect/Defense Directorate is to assist the combatant commanders in the development of strategies to defend against C2W and Information Warfare (IW) attacks.

The Directorate's original concept was that of "Red Teaming" or exploiting information operations and related information technologies to raise the awareness of CINCs and OSD program managers to information related vulnerabilities. However, as concepts and doctrine for IW and Information Operations (IO) developed, we realized that

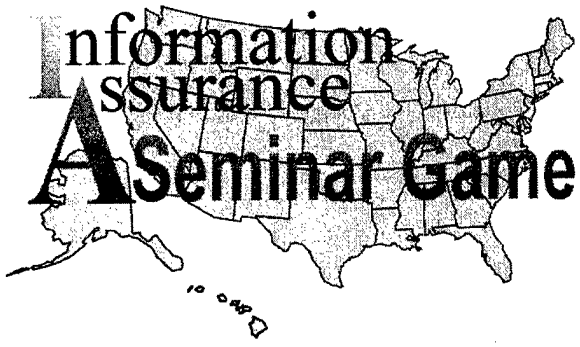
Continued on page 2.

INSIDE

INFORMATION ASSURANCE SEMINAR GAME

The U.S. Army War College, Center for Strategic Leadership, hosted an Information Assurance Seminar Game that examined the emerging roles of the public and private sectors in protecting our critical information infrastructures from Information Warfare attacks. The Seminar Game was held 3-5 February 1998 at the Center for Strategic Leadership (CSL) Carlisle Barracks, Pennsylvania and was jointly sponsored by the CSL, Booz·Allen & Hamilton, and the National Computer Security Association. Seminar Game participants were composed of industry and government experts whose views influence national information assurance policy and direction. The Seminar Game provided participants with a unique opportunity to interact on matters of increasing concern to all, and resulted in a more balanced view of information warfare and its threat to our nation's critical infrastructure, private and public.

Presentations by recognized national security experts were provided to help participants define the threat, assess vulnerabilities and consider ways to estimate damages in the wake of an information infrastructure attack. Participants investigated ways to detect and disclose infrastructure attacks while addressing an appropriate process for response and recovery. The seminar also considered the national response to a strategic information attack.



Results of the game will be distributed to participants, key government offices, and selected agencies for publication. Further details can be obtained by contacting one of the following:

U.S. Army War College
Mr. Robert F. Minehart, Jr. (717) 245-4472

International Computer Security Association
Mr. Fred Tompkins (717) 241-3241

Booz•Allen & Hamilton, Inc.
Mr. Albert J. Ross (410) 684-6635

VOL. 1 NO. 3

The Information Assurance Technology Newsletter is published quarterly by the Information Assurance Technology Analysis Center (IATAC). The third issue continues the focus on current information assurance initiatives underway within the Department of Defense. In addition, an overview of the IA Tools Database is provided that highlights the current collection of Intrusion Detection Tools.

IATAC, a DoD-Sponsored Information Analysis Center (IAC), is administratively managed by the Defense Technical Information Center (DTIC) under the DoD IAC Program. Inquiries about IATAC capabilities, products and services may be addressed to:
Robert Thompson
Assoc. Director, IATAC

We welcome your input. To submit your related articles, photos, notices, feature programs or ideas for future issues, please contact:
IATAC
ATTN: C. Wright
8283 Greensboro Dr.
Allen 663-D
McLean, VA 22102
Phone 703-902-3177
Fax 703-902-3425
STU-III 703-902-5869
STU-III Fax 902-3991
E-mail: iatac@dtic.mil
Internet: www.iatac.dtic.mil
Intelink-S:
http://204.36.65.5/index.html
Intelink:
http://www.web1.rome.ic.gov/iatac

DEFENDING

Continued from page 1.

IO vulnerabilities should be addressed in the larger context of IW and IO. That is, since command and control (C2) is a subset of IW, we need to protect information with C2 application and value, regardless of whether or not it resides in a C2 system. In addition, we need to address those IO objectives and tasks associated with peacetime defense.

Accordingly, the Protect/Defense Directorate's mission is evolving from (C2) Protect and (IW) Defense to Defensive IO. In this context, we are orienting our mission to the new definitions prescribed by DODD S-3600. *(Information Operations)*, CJCSI 3210.1 *(Joint Information Warfare Policy)*, CJCSI 651001A *(Defensive IW Implementation)*, and Draft Joint Pub 3-13 *(Joint Doctrine for Information Operations)*. DODD S-3600 provides that "DoD information systems critical to the transmission and use of minimum-essential information for command and control of forces shall be designed, employed, and exercised in a manner that minimizes or prevents exploitation, degradation, or denial of service from a multiple variety of attacks to include computer network attack." Draft Joint Pub 3-13 refers to the following related defensive IO areas: information assurance, physical security, OPSEC, counter-deception, counter-PSYOP, counter intelligence (CI), electronic protect, and special information operations. The Defense IO mission also involves responses to IW attacks that may be either defensive or offensive in nature and may involve interface with law enforcement agencies.

As you can see, Defensive IO is a relatively broad mission. It is also a dynamic one — as IW and IO concepts and doctrine evolve, so does our mission, and we continue to examine processes that best support the combatant commanders in the areas listed above. Since this is a new mission area for the JC2WC, we continue to seek out the best training available in these areas to enable us to provide the requisite expertise as a "center of excellence." To accomplish this mission, the Directorate has established three functional area teams (see Figure 1 below) to respond to our evolving defensive IO mission. These

Continued on page 7.

Figure 1. Protect/Defense Functional Areas

Penetration Testing Course

Course Objective:

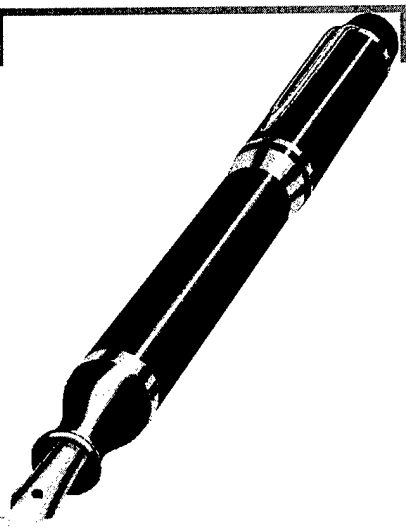
The purpose of this full-day tutorial is provide attendees an accurate depiction of the role penetration testing plays in analyzing a system's overall security posture. The tutorial is designed to provide a thorough understanding of penetration testing concepts, terminology, approaches and techniques that can be applied to all system and network configurations.

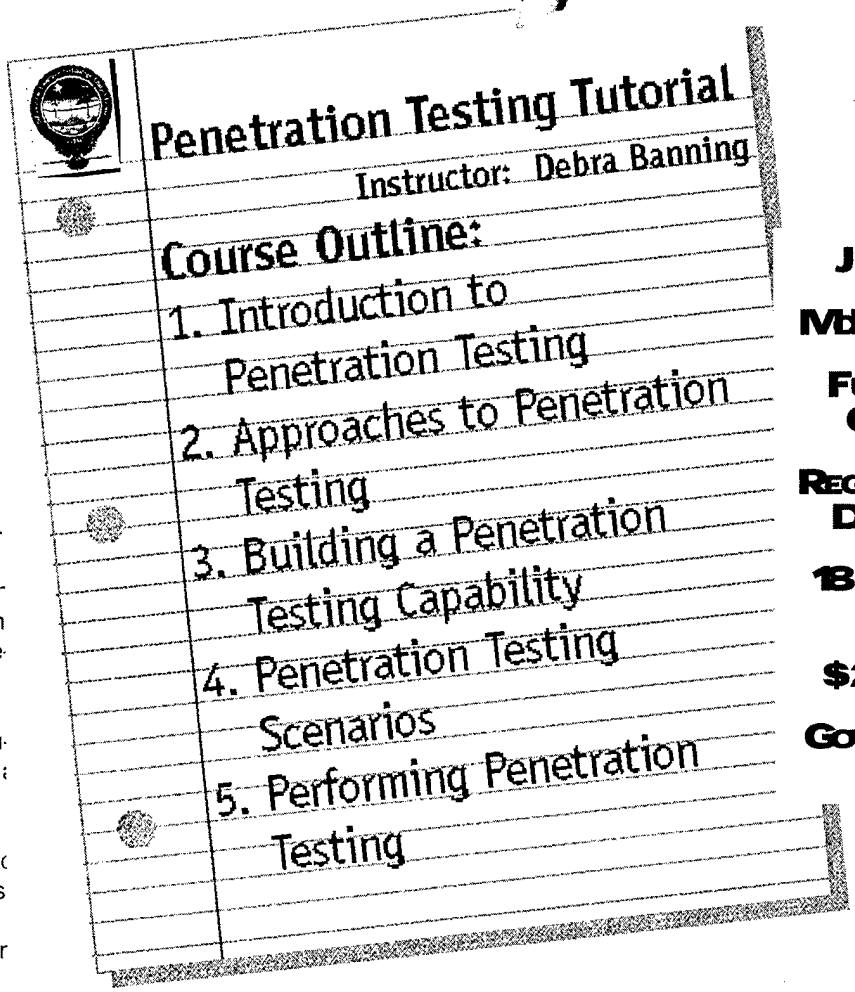
This course is NOT intended to teach specific system vulnerabilities or how to exploit them, but will provide information on publicly available sources and tools that are commonly used by hackers. During this course attendees will learn how penetration testing fits into life-cycle system/network security and how it can complement other commonly performed security activities such as risk analysis and security test and evaluation. Attendees will also learn the limitations to penetration testing and that it is not a comprehensive analysis of a system's security.

At the completion of this tutorial, attendees should have a better understanding of what penetration testing is and is not, how it can be beneficial to organizations, and restrictions imposed when performed by professional consultants within legal boundaries. Attendees will have obtained the basic foundation necessary for building a penetration testing capability and performing penetration tests.

The tutorial will be held as Government-Only (see registration form on page 8) at the Booz·Allen & Hamilton McLean Campus — 8283 Greensboro Drive. A registration fee of $225.00 is required and due by May 18, 1998. A $50.00 late fee will be applied for all registrations received after May 18, 1998 and for payment at the door.

For more information concerning the tutorial, please contact Christina Wright at 703-902-3176/3177 or via e-mail at iatac@dtic.mil.





JUNE 4

McLEAN, VA

FULL DAY COURSE

REGISTRATION DEADLINE

18 MAY 98

COST $225.00

GOVERNMENT ONLY

ABOUT THE INSTRUCTOR

Debra Banning is a Senior Associate at Booz·Allen & Hamilton specializing in security/risk assessments and penetration testing. Ms. Banning has been planning, performing and leading penetration exercises for government and commercial clients for 13 years. She recently presented the Penetration Tutorial on which this workshop is based at the 13th Annual Computer Security Applications Conference sponsored by the IEEE Computer Society.

Information Assurance Tools Database: Intrusion

The **IATAC Information Assurance Tools Database** hosts information on intrusion detection, vulnerability analysis, firewalls, and anti-virus applications. A brief summary of Intrusion Detection Tools is provided on these two pages. For more information, see **IATAC Products** on page 6.

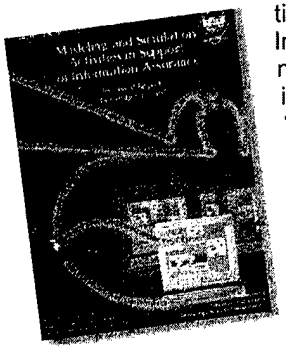
Title	Attributes	Description
ADS	attack detection	Attack detection system for secure computer systems
AID	audit-based, misuse detection	Distributed intrusion detection system that consists of agents on the monitored hosts and a central monitoring station with an expert system
ALVA	anomaly detection, audit-based	Real-time tool for detecting potential security violations in UNIX audit logs. The system gains some level of platform independence by analyzing command logs that are pre-computed from the system audit logs.
Argus	audit-based, system monitoring	Generic IP network transaction auditing tool for UNIX
ARPMon	system monitoring	Maps IP addresses to physical network or hardware addresses to monitor the usage of IP addresses on a network
ARPWATCH	system monitoring	Aims to protect against address spoofing by monitoring Ethernet activity and maintaining a database of Ethernet/IP address pairings
ASAX	audit-based, misuse detection	Distributed audit trail analysis system that also has incorporated configuration analysis
ASIM	anomaly detection	Air Force project designed to measure the level of unauthorized activity against its systems
CMDS	anomaly detection, audit-based, expert system, misuse detection	Real-time audit reduction and analysis to detect and deter computer misuse
Courtney	system monitoring	Monitors the network and identifies the source machines of SATAN probes/attacks
CyberCop	anomaly detection, misuse detection, system monitoring	Real-time security solution that issues alarms when attacks are identified, recognizes networked elements under attack, logs the activity, and captures evidence of the intrusion
EMERALD	anomaly detection, system monitoring	Distributed scalable tool suite for tracking malicious activity through and across large networks and introduces a highly distributed, building-block approach to network surveillance, attack isolation, and automated response
Gabriel	system monitoring	SATAN detector available for Sun platforms, written entirely in C and comes pre-built
GrIDS	anomaly detection	Uses graph-based language for analyzing network connection activity in a LAN-MAN sized system to detect large-scale automated attacks on networked systems
IDES	anomaly detection, expert system, misuse detection, system monitoring	Real-time intrusion-detection expert system that observes user behavior on a monitored computer system and adaptively learns what is normal for individual users, groups, remote hosts, and the overall system behavior
IDIOT	misuse detection	Based on complexity of matching and temporal characteristics
Ifstatus	anomaly detection	Checks network interfaces for promiscuous or debug mode in an attempt to determine if a sniffer is being run
Internet Scanner Toolset	anomaly detection	Perform scheduled and selective probes of a network's communication services, operating systems, key applications, and routers in search of those vulnerabilities most often used by individuals to probe, investigate, and attack
INTOUCH INSA	anomaly detection, keystroke surveillance, misuse detection	Scans all network-based user activity, regardless of the computer manufacturer or operating system being used, utilizing keystroke-level surveillance
ITA	anomaly detection, audit-based, misuse detection	Detect intruders or abuse by analyzing audit data from the operating systems it supports utilizing a rules engine
Kane Security Monitor	misuse detection, system monitoring	Provides network security monitoring using artificial intelligence, and identifies internal and external violations
md5check	file integrity	Compares the MD5 checksums of several critical SunOS 4.x system files to a database
NADIR	anomaly detection	Rules-based expert system to automatically detect intrusion attempts and other network security anomalies

Detection Tools

Title	Attributes	Description
NETMAN	system monitoring	Package of network monitoring and visualization tools for monitoring and displaying network communications
NetRanger	anomaly detection, misuse detection, system monitoring	Analyzes the data traffic for content and context while searching for signatures indicative of hacking attacks or other security violations
NID	anomaly detection, misuse detection	Detects, analyzes, and gathers evidence of intrusive behavior on Ethernet and FDDI networks using the Internet protocol
NIDES	anomaly detection, expert system, misuse detection, system monitoring	Real-time monitoring of user activity on multiple target systems connected via Ethernet. rule-base employs expert rules to characterize known intrusive activity represented in activity logs, and raises alarms.
NOCOL	system monitoring	Monitors network and system variables, such as ICMP or RPC reachability, RMON variables, nameservers, Ethernet load, port reachability, host performance, SNMPtraps, modem line usage, Appletalk and Novell routes/services, BGP peers
Noshell	system monitoring	Provides the system administrator with additional information about who is logging into disabled accounts
NSM	system monitoring	Network-based network traffic monitor
POLYCENTER	misuse detection, system monitoring	Knowledge-based analysis of audit data to recognize and respond to simple security-relevant events
RealSecure	system monitoring	Real-time, automated attack recognition and response system that rests on the network, monitoring the network traffic stream looking for attacks and unauthorized access attempts
SecureNet Pro	keyword-level surveillance, system monitoring	Combines several key technologies, including session monitoring, firewalling, hijacking, and keyword-based intrusion detection
Stake Out	anomaly detection, misuse detection, system monitoring	Monitors network traffic and detects intrusive or suspicious activity as it occurs
Stalker	misuse detection	Identifies intruders and internal misuse by analyzing audit trail data and reporting on suspicious user and system activities
Swatch	misuse detection, system monitoring	Monitors events on a large number of systems and modifies certain programs to enhance their logging capabilities and software to then monitor the system logs
Tripwire	file integrity	Compares a designated set of files and directories to information stored in a previously generated database
T-sight	system monitoring	Visualizes traffic and data transiting a network, evaluates risks of certain transactions, and displays connection/transaction data that can either be logged or viewed during real-time monitoring
UNICORN	audit-based	Accepts audit logs from Unicos (Cray UNIX), Kerberos, and a common file system, then analyze them and attempts to detect intruders in real time
USTAT	misuse detection, state transition analysis	Makes use of the audit trails that are collected by the C2 Basic Security Module of SunOS and keeps track of only those critical actions that must occur for the successful completion of the penetration
WatchDog	system monitoring	Monitors and manages the SunOS audit trail produced by the system's C2 security features and responds in real time to events that appear, and stores the audit trail
WebStalker Pro	misuse detection	Controls access to Web content files, and can watch all Web and non-Web accesses, all processes, and all changes to Web and other files; notifies in realtime through SNMP, pager, or e-mail when anything suspicious occurs
X Connection Monitor	system monitoring	Monitors X connections by using RFC931 to display user names, when the client host supports RFC931, and allows the user to freeze and unfreeze connections, or kill them, independent of the client and independent of the server

IATAC PRODUCTS

For more information on IATAC products & reports, contact Alethia Tucker at 703-902-3177.

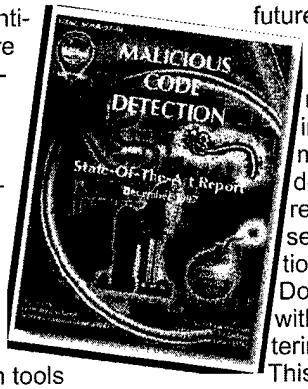


Modeling & Simulation Technical Report

This unclassified report describes the models, simulations and tools being used or developed by selected organizations that are chartered with the Information Assurance mission. Data collection efforts focused on the current definitions of Information Operations, Information Warfare, and Information Assurance as described in DoD Directives S-3600.1, *"Information Operations,"* and Chairman, Joint Chiefs of Staff Instruction 6510.1A, *"Defensive Information War - fare Policy."* In addition, the definitions prescribed by DMSO for model and simulation were used to determine what entities should be included in this IA models, simulations and tools report.

Intrusion Detection Report

This Information Assurance Tools Report provides an index of intrusion detection tool descriptions contained in the IATAC Information Assurance (IA) Tools Database. The IA Tools Database hosts information on intrusion detection, vulnerability analysis, firewalls, and antivirus software applications. Information was obtained via open source methods, including direct interface with various agencies, organizations, and vendors. Research for this report identified 43 intrusion detection tools currently employed and available. Tool information includes title, author, source, contact information and tool abstract.



Malicious Code Detection SOAR

This IATAC State-Of-The-A Report (SOAR) addresses Ma licious Software Detection. Included within the report is a taxonomy for malicious software to provide the audience with a better understanding of commercial malicious software An overview of the current state-of-the-art commercial ma licious software detection prod ucts and initiatives, as well as future trends is present· ed. The same is then done for current state-of-the-ar in regards to DoD malicious software detection. Lastly, the report presents observations and asser tions to support the DoD as it grapples with this problem entering the 21st century This report is classifiec and has a limited release.

Secure STINET's Customization

The Dynamic Secure STINET Service now has added the following:

Secure STINET's Customization provides the power to create and modify your own personalized web page. See what has changed in STINET by filtering out what is old and concentrating on what is new...set up a personal profile based on subject fields and groups and automatically receive citations via e-mail to the latest accessions in DTIC's Technical Report collection twice a month...save search queries for both the Technical Report and Work Unit Information System collections for reuse.

Abstracts are now included with citations to unclassified/ limited documents in the Technical Reports Bibliographic Database. Viewing abstracts is based on individual user profile access restrictions. If your profile does not permit you to view a particular citation's abstract, you will be allowed to view the rest of the citation, minus the abstract.

Over 3,000 full-text technical reports are now available for viewing and downloading. Special Collections highlights reports found in DTIC's Technical Reports collection based on the source, topic, or targeted group. In addition to setting up your own search parameters, you can search using preestablished profiles developed by retrieval experts.

The Partnership for Peace Information Management System (PIMS) is designed to enhance the education of U.S. Service school students. Topic searches developed by DTIC for the PIMS community provide information ranging from air traffic control management to public affairs. PIMS also offers students the capability to construct custom searches for information not covered in the topic searches.

The subscription for the Secure STINET Service access via a web client is $50 per year/per subscriber To subscribe to Secure STINET Service, contact DTIC's Registration Branch:

Telephone: (703) 767-8272
DSN 427-8272
Toll Free: 800-225-3842
(menu selection 2, option 2, sub-option 2)
Fax: (703) 767-8228
DSN 427-8228
E-mail: reghelp@dtic.mil

Questions concerning this product may be directed to the Product Management Branch, DTIC-BCP, 800-225-3842 (menu selection 2, option 3), 703-767-8267, or DSN 427-8267.

DEFENDING....

Continued from page 2.

unctional teams are entitled Combat Support, Advanced Technology, and Field Support. Since the directorate is relatively small, with only 17 people, we leverage IO "opposition force" and analytical capabilities of other national agencies, service IW activities, and contractors.

The Protect/Defense Directorate supports six to eight CINC-sponsored exercises each year. The Combat Support Team provides direct defensive IO support to the combatant commander and serves as the joint coordination focal point for vulnerability assessment (i.e., exercise CONOP), IW Red Team scenario development, external agency coordination, defensive IO awareness training (as requested), Red Team scenario execution, and After-Action-Reporting.

The JC2WC has been asked by OSD to perform vulnerability assessments in support of the Advanced Concept Technology Demonstration (ACTD) program. During FY97, the Advanced Technology Team provided vulnerability assessment support for the following ACTDs: Rapid Terrain Visualization, Counter Proliferation, Air Base/Port Bio Detection, Combat ID, Battlefield Awareness and Data Dissemination, Joint Countermine, Rapid Force Projection Initiative, and Precision SIGINT Targeting System. ACTDs tentatively planned for evaluation in FY98 include Navigation Warfare, Joint Logistics, Military Ops in Urban Terrain, Extended Littoral Battlespace, Chemical Add-on (to Air Base/Port Bio Detection), and Unattended Ground Sensor. Vulnerability assessment support provides critical insight into system design and allows OSD and the Services to correct deficiencies before production and fielding of a system. As such, CINC users are made aware of the limitations associated with a system before depending on the information in an operational environment. Other FY98 approved ACTDs are still under review for assessment.

The Field Support Team functions as a self-sustaining, deployable "IW Red Team" that supports the Combat Support and Advanced Technology teams. Field Support Team deployable capabilities include HF/VHF/UHF/ EHF, Signal Intercept and DF, Radar/IR Detection, and RF Jamming. Instrumentation assets include GPS, oscilloscopes, pulse analyzer, and spectrum analyzer. In addition, Field Support Team assets include shelters, generators, and cargo trucks.

As the IO environment becomes more complex, and the Defense Information Infrastructure more integrated with the National and Global Information Infrastructures, defensive IO measures also become more important and more difficult to assure. In any case, we will continue to leverage heavily off of the resources and capabilities of National agencies such as National Security Agency (NSA) and the Services' IW Centers/ Activities in providing defensive IO support to the combatant commanders. The JC2WC will continue to strive to be the acknowledged IO leader, responsive to the CINCs, for integrating information operations into the overall military campaign plan.

[1] CJCSI 5118.01. Charter for the Joint Command and Control Warfare Center, 15 September 1994.

CONFERENCES & SYMPOSIA

Fiesta Informacion '98
Convention Center • San Antonio, TX
"The Virtual Enterprise in the 21st Century"
For information call 800-564-4220
14—16 Apr 98

10th Ann. Software Technology Conference
Salt Palace Convention Ctr, Salt Lake City, UT
"Knowledge-Sharing — Global Information Networks."
http://www.stc98.org
19—24 Apr 98

USPACOM
Information Assurance Conference
Honolulu, HI
POC: SFC Huff 808-477-1046
e-mail: huffsd00@hq.pacom.mil
28—30 Apr 98

Introduction to Information Operations
TS/SCI clearance, O-3 through O-6 and equivalents,Bolling AFB, DC.
POC: Mr. Doug Dearth
703-780-2584
e-mail: dhdearth@aol.com
4—8 May 98

Penetration Testing Course
This course is Government Only. Booz•Allen & Hamilton McLean Campus. See page 3 for complete description. http://www.iatac.dtic.mil
4 Jun 98
Fee: $225.00
Registration form on back of newsletter.

IIBW9xxx: Intermediate Information Operations/Warfare (IBW)
5 days, SECRET clearance required, O-4 through O-6 and equivalents, School of Information Warfare and Strategy, National Defense University, Fort McNair, DC
POC: Dr. Fred Giessler, 202-685-2209
IBW9804 13—17 Jul 98
IBW9901 12—23 Oct 98

Penetration Testing Course Registration

June 4, McLean VA

(Government Only)

Title _____

Attendee Name _____

Organization (Govt. or Military)

_____

Organization Address

_____

_____

_____

Phone _____ Fax _____

E-mail_____

Fee $225.00 (Add $50.00 after 18 May 1998)

❑ Check enclosed for $_____

Attach payment and mail by 18 May 98 to:

IATAC, 8283 Greensboro Drive, Allen 663-D
McLean, VA 22102-3838

Distribution & Information

U.S. Distribution Only

❑ Change ❑ Add

❑ Send IATAC Technical Area Task Info (Govt Only)

Name _____

Title _____

Company/Org. _____

Address _____

_____

City/State/Zip _____

Phone _____

Fax_____

DSN _____

E-mail_____

Organization (check one):

❑ USA ❑ USN ❑ USAF ❑ USMC ❑ OSD

❑ Contractor

Information Assurance
Technology Analysis Center
8283 Greensboro Drive, Allen 663
McLean, VA 22102-3838