REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

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

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 summer '98 issue continues the focus on current information assurance initiatives underway within the Department of Defense. An overview of the IA Tools Database is provided that highlights the current collection of Vulnerability Analysis tools. In addition, two new sections have been added: Industry Initiatives and R&D Perspective.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Information Security, Information Assurance, Information Warfare	11
	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

IA newsletter

Vol. 2, No. 1
Summer 1998

IATAC
is a DoD-Sponsored Information Analysis Center Administered by the Defense Technical Information Center (DTIC).

Incorporating IA into GLOBAL GUARDIAN

by Mr. Ward Parker
United States Strategic Command

For the last few years, United States Strategic Command has incorporated computer network attack (CNA) scenarios into its annual major exercise known as GLOBAL GUARDIAN. The primary purpose of including CNA is to test the processes we have in place in case of a real attack against our information infrastructure.

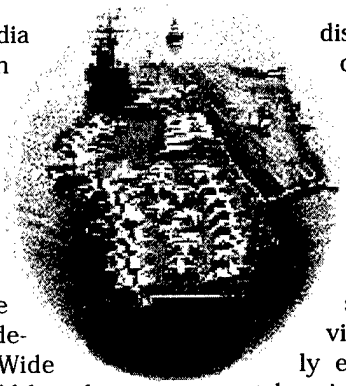
During the first couple of exercises we kept the attacks simple. They were designed solely to raise the awareness of Command members. Although we continue to employ scenarios to educate users, we now use sophisticated, on-line attacks to test the security posture of the Command's systems and key personnel.

The attack scenarios for our most recent exercise, GLOBAL GUARDIAN, were developed months prior to the actual start date of the exercise. The attacks we developed focused on affecting the decision makers in the Command—the purpose of information operations. We accomplished this by concentrating our efforts on how we could realistically affect the confidentiality, integrity, and availability of data; however, one of the rules of engagement was not to modify or change any data.

We worked closely with our intelligence personnel to ensure our attacks were consistent with the overall scope of the exercise. To carry out the attacks, we employed Command "red team" members and other organizations to act as enemy agents. Our goal was to make the attacks seamless, in the sense that they were all related and graduated in severity. The attacks ranged from attempting to penetrate the Command from the Internet to a "bad" insider with access to a key command and control system. The attackers also "war dialed" our phones to tie up the phones and sent faxes to numerous fax machines throughout the Command. Attackers also claimed they had the ability to shut down our systems.

Security Tools for Network Centric Warfare

by LT Reese Zomar, USN
Navy INFOSEC Program Office



The news media are replete with reports of attacks via the Internet on networks and computer systems around the world, often specifically through the increasingly widespread World Wide Web (WWW). Although many of these attacks take advantage of well-known security flaws and vulnerabilities in complex operating systems such as UNIX and Windows NT, some systems continue to be infected with computer viruses, which can seriously disrupt a company's business, and also disrupt warfighting operations and exercises. Although the exact origin of many viruses is often not known, the reason for the spread of the viruses can be easily explained. All it takes is one individual, with one corrupt disk, or one corrupt program downloaded from the Internet, and the virus is inside the network. Once inside, if the virus signatures in the network antivirus software are not up to date, or virus scans are not performed when programs are opened, the virus can propagate undetected and uncontrolled.

A number of tactical systems on-board naval vessels were originally designed to operate in a closed environment; however, with the end-to-end worldwide network connectivity that comes with network centric warfare, the environment is no longer closed. Many of the best-known and most common attacks that occur on the Internet are those that target information integrity by corrupting or destroying it, usually by using agents such as viruses. Another common class of attack, commonly called denial of service attacks, seeks to deny

INSIDE

Security Tools

continued from cover

use of the system, using techniques such as message flooding. Still other attacks, such as Internet Protocol (IP) address spoofing, focus on allowing the attacker to masquerade as a valid user who can then plant bogus information or deny access. It is well known that opening a "hostile" Webpage (i.e., with imbedded code operating in the background that may be malicious), can lead the innocent user into a scenario where he/she may be unknowingly infecting a ship's warfighting networks and computer systems with potentially dangerous software agents.

As the Navy embraces the concept of network centric warfare, security is being emphasized and implemented as an integral part of the network infrastructure. Using secure protocols, turning off unused services, and designing applications that periodically incorporate operating system patches has recently become standard practice. The Navy Information Systems Security Program Office at the Space and Naval Warfare Systems Command (SPAWAR), has developed a Network Information Assurance Team (NIAT) that has been integrated into an existing Battle Group Systems Integration Test (BGSIT) process. Using a variety of commercially available security tools, the NIAT examines the afloat security posture of the various integrated shipboard networks and provides ships with the means to combat threats to their information systems.

The first phase of a typical NIAT visit includes a meeting with the ship's systems administrators and a tour of the computer spaces, both classified and unclassified. During the meeting, the team explains that its primary job is security, but that it is also willing to provide network technical and also administrative support where needed.

The second phase is a network scan and mapping using tools such as Strobe, Ballista and SATAN. These tools provide a network overview and probe for known vulnerabilities. More and more security tools are available to today's network administrators, and the NIAT team is always willing to try any commercially available tools that are user friendly and not overly complex. The NIAT has begun providing copies of the security tools (with training) to shipboard personnel who are responsible for operating and maintaining networks.

Phase 3 concentrates on network policy, including file structure, system security policy, and password policy. The NIAT currently uses the Kane Security Analyzer to scan file structure and system security policy. The main tools used to test password policy are Pass Crack and L0phtcrack.

The final phase of the visit is a recommendation and education phase. During this period, the team provides its security recommendations, reviews findings of the scans, discusses best known practices, outlines industry solutions and holds classes on topics such as Windows NT administration, Transmission Control Protocol/Internet Protocol (TCP/IP), Domain Naming System (DNS), and router access control lists. The most recent versions of antiviral software are always provided. One of the most important benefits of the NIAT is that the team provides formal feedback to system developers, integrators, and implementers, helping to ensure that future releases of the warfighting application software have the security problems fixed.

Over the past 5 months, the NIAT has provided systems support to the USS LINCOLN (CVN-72) and USS EISENHOWER (CVN-69) Battle Groups (BG), and the USS ESSEX (LHD-2), USS WASP (LHD-1), and USS SAIPAN (LHA-2) Amphibious Readiness Groups (ARG). Additionally, the team has provided valuable training, antivirus, and configuration support in the network security arena to units and commands located at various shore sites. Because of the high quality of assistance, the number of requests for shipboard (and ashore), NIAT assistance is growing. Captain Dan Galik, Program Manager for Navy Information Security (INFOSEC) notes that "with the rapid advances being made in information technology, it is very difficult to provide our sailors and other Navy personnel with the required technical training to keep pace with these technical advances, particularly in the area of network security. Our sailors need hands-on expert technical help, and that's one of the key benefits that NIAT is providing." In its relatively short existence, the NIAT program has been recognized throughout the fleet for security excellence.

Lieutenant Zomar has a B.S. in Aerospace Engineering and a B.S. in Applied Mathematics from University of Colorado. He received his M.S in Electrical Engineering from Rensselaer Polytechnic Institute. LT Zomar reported aboard SPAWAR in August of 1997 after serving in the S-3 Viking community. He may be reached at 619-524-7340 or via email: zomarr@spawar.navy.mil.

Vol. 2 No. 2

The ***IANewsletter*** is published quarterly by the Information Assurance Technology Analysis Center (IATAC). The Summer '98 issue continues the focus on current information assurance initiatives underway within the Department of Defense. An overview of the IA Tools Database is provided that highlights the current collection of Vulnerability Analysis Tools. In addition, two new sections have been added: Industry Initiatives and R&D Perspective.

Writing for *IANewsletter:*
We welcome your input and comments on related articles, photos, notices, feature programs or ideas for future issues. If you're interested in writing for the *IA Newsletter,* contact Christina Wright at the address below.

Accessing IATAC
8283 Greensboro Drive
Allen Bldg. 663
McLean, VA 22102

Phone 703-902-3177
Fax 703-902-3425
STU-III 703-902-5869
STU-III Fax 902-3991
Email: iatac@dtic.mil
URL: www.iatac.dtic.mil
Intelink-S:
http://204.36.65.5/index.html
Intelink:
http://www.web1.rome.ic.gov/iatac

Director and Editor
Robert Thompson
Collection &Analysis
Alethia Tucker
Art &Production Manager
Christina Wright
Webmaster
Steve Gunther

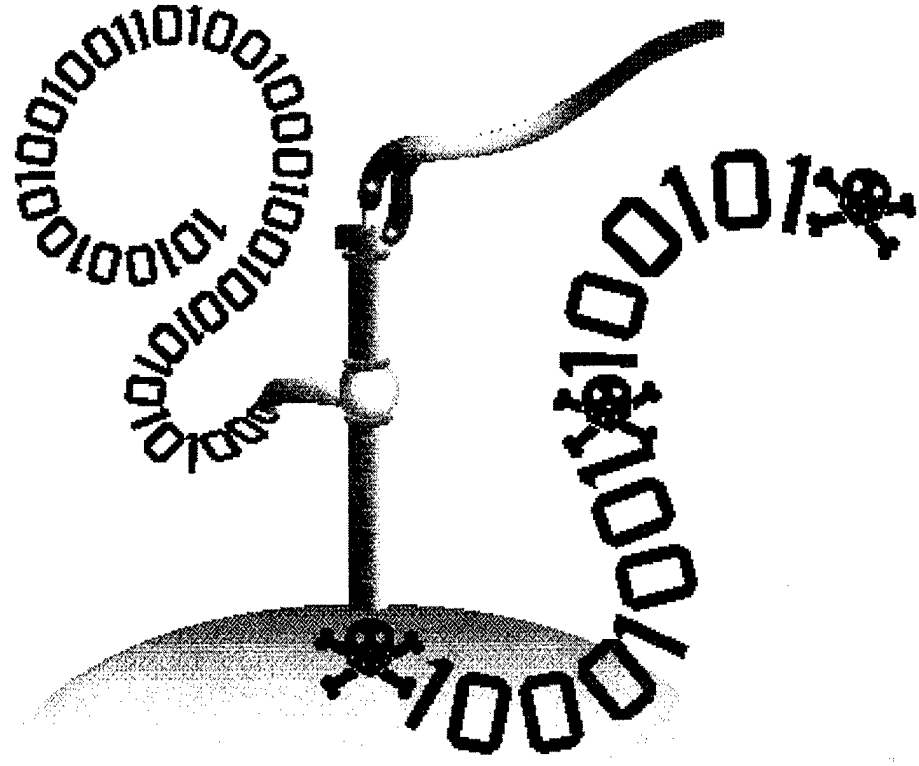
ARL Primes Army Information Assurance Capability

by LTC Paul Walczak
Army Research Laboratory

The Army Research Lab (ARL) seeks ways to reduce the risks associated with future digitized land warfare by executing fundamental research and analysis leading to development of new information assurance (IA) technology. ARL pursues this objective by analyzing the Army Warfighter Experiments (AWE), a series of coordinated events that will determine the right blend of technology for the first digitized division and corps); by gaining practical experience in computer incident response; and by executing its research programs that help to develop the operational concepts of the Army After Next, (AAN) the overarching vision for the future Army.

Achieving AAN vision places unprecedented reliance on information and the technology that supports its processing and distribution. The Army's concern for IA stems from its understanding of the potential consequences of failed or corrupted access to information (i.e., ultimately the loss of lives). ARL has been involved with the development of information technology since the earliest days of modern computing machines. ARL's predecessor laboratories pioneered digital computing, creating ENIAC, one of the first functional digital computers. ARL currently operates the DoD's Major Shared Resource Center (MSRC) for classified information, as well as the Army's High-Performance Computing Research Center. This experience and resources uniquely qualify ARL to conduct basic and applied IA research at the forefront of the era of digitized warfare, an era that places new value on information and its assured distribution.

The AWE series reveals significant challenges for battlefield information assurance. In collaboration with the Army Digitization Office (ADO), ARL provides analysis to identify and characterize vulnerabilities in command and control (C2) systems for the First Digitized Division/Corps (FDD/C). The fundamental technical capability that distinguishes the FDD/C is the Tactical Internet (TI). The TI is a complex adaptation of the protocols used on the public Internet, shared across new families of automated battlefield information processing systems. ARL investigates



and military interest in the public Internet (MILNET). These potential problems can be examined using a coordinated approach that produces dual-use solutions. One of ARL's unique capabilities lies in having an analytic element within its organization focused on the survivability of the TI (as described above), and another operating to protect ARL's own MILNET-based computer network operations. ARL has gained practical knowledge in MILNET incident detection and response through its computer security incident response lab, operated by the Computer Security Incident Response Team (CSIRT). Led by Angelo Bencivenga, the CSIRT oversees 6,000 nodes that comprise common commercial hardware and software components located at several sites in the continental United States. Through its monitoring, intrusion detection, and analytic activities, CSIRT pumps fresh data into ARL's corporate repository. and filtered network traffic data, which is made available to ARL-directed research projects. The CSIRT has been recognized for success in developing organizational procedure and in refining off-the-shelf assurance tools, extending their functionality and performance while reducing the number of false alarms.

Analyses of both the digital tactical network and the MILNET provide a well-grounded basis for ARL's IA research program.

DIA Information Warfare Course

by Ms. Joan Putman
Program Analyst, DoD IAC Programs

The Introduction to Information Operations course taught at the Defense Intelligence Agency (DIA) offers intelligence professionals a current picture of what is happening in the Department of Defense (DoD) in Information Operations (IO) A ticket to this course is a must for the well-rounded, well-educated information specialist in DoD.

Mr. Douglas Dearth, who teaches and facilitates the class at the Joint Military Intelligence Training Center (JMITC), draws a very diverse cross-section of civilian government and military personnel into the classroom, which offers the attendees a chance to network with their peers in other government organizations. The real "missing piece" of information that the attendee gains from attending this course is the intelligence slant of IO today and especially, a chance to talk with some of our allies in a special briefing and open exchange session. This course helps the student think from the current global perspective.

This course provides a nonattributional forum where briefings and discussions are held at various levels of classification. Students are required to have a Top Secret level clearance to attend, which allows for specific and timely information to be presented, candid discussions, observations and an open exchange of ideas from the diverse audience. Students have time during the week to reflect on what they are being taught and plan how to apply that information to aid their own organizations. This course, along with the Information Operations, Warfare, and Strategy course offered by NDU, is needed for the whole DoD overview of Information Operations. A great amount of valuable printed material from some of the briefers supplements the continual flow of seminar-like briefings that the students attend. Supplemental reading is recommended and additional materials are generously provided.

This enlightening 5-day course is offered only threetimes a year, and is generally open to Infowarriors, at the GS-11 and above, civilian level; and captains through colonels, military level. The course usually accommodates a group of about 35 for each class offering.

Mr. Dearth is the point of contact. If you want to attend, call (202) 231-3290 /DSN 428-3290 or email dhdearth@aol.com. If accepted, you may be placed on a waiting list, but this course is worth waiting for.

continued from cover

GLOBAL GUARDIAN provided us the opportunity to test our newly-developed Information Operations Conditions, more commonly known as INFOCONs. Our INFO-CONs serve as a notification mechanism to warn the Com-mand of possible increasing threats to our information infrastructure. Once the attack was identified, we wanted to assess how fast the Command could respond by changing the INFOCON. As the exercise progressed, INFOCON levels changed several times, giving us the opportunity to assess the effectiveness of the INFOCON concept.

We were extremely pleased with how rapidly the Command raised INFOCON levels. Proper procedures and training allowed the Command to quickly raise the INFOCON levels to the appropriate level of threat. The Command is now in the process of disseminating the INFOCON system to our task forces for implementation.

We were also impressed with the response of our "front-line" defenders—our system administrators, who were extremely vigilant in monitoring computer audit logs and other anomalies that might signify an ongoing attack. Our computer emergency response team was also instrumental in identifying the attacks, reporting them up the chain of command, and making recommendations to limit the "damage" of the attack. Senior-level leadership was also very supportive of our activities, understanding that timely, accurate information is vital to accomplishing the mission.

GLOBAL GUARDIAN has provided us with a venue for measuring the effectiveness of the Command's information assurance posture during times of heightened danger, allowing us to emphasize the threat of computer network attack to the warfighter. We plan to increase the level of CNA in future GLOBAL GUARDIAN exercises to imitate as closely as possible the technical capabilities of a hostile source.

Ward Parker

Is Your Network Under Attack?

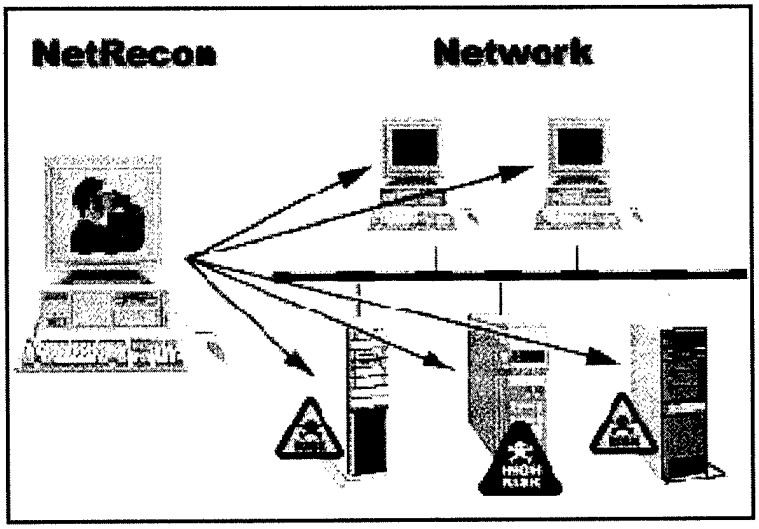
by Steve Jackson
AXENT Technologies, Inc.

Your data is vulnerable, but how vulnerable? What is the risk to your data from internal or external attacks? You need to think like the enemy to truly understand the security issues associated with your data. Your network is extremely complex—data exists on the wire and on every node. In a system with vulnerabilities, prying eyes can capture data easily. Understanding the vulnerabilities within your network is the first step to securing your data.

AXENT Technologies, Inc., recently introduced a new security tool to help address these issues. This tool, NetRecon, is a third-generation vulnerability scanner. It uses a technology called UltraScan to find vulnerabilities in an entire network. Unlike all other scanners that locate vulnerabilities on each system in isolation, NetRecon uses vulnerabilities from one or more systems to find additional vulnerabilities on the rest of the systems. With this technology, NetRecon can prove that your network is "only as secure as the weakest system in the network."

Working as a "Tiger Team," NetRecon starts by scanning in parallel for vulnerabilities on all systems. As data from the systems are retrieved, other scans are initiated by coupling the data retrieved and using that as input to the systems found. A "Tiger Team" takes the information gathered, couples it, and uses the resulting data to attack all systems discovered. As shown in the figure below, NetRecon finds login vulnerabilities on one system, password files on a second system, and File Transfer Protocol (FTP) services from yet another. Those vulnerabilities are duly noted and then NetRecon scans at the next level. Using UltraScan, NetRecon couples these three separate vulnerabilities, builds a new set of objectives, and attacks all systems discovered. With this technology NetRecon can find vulnerabilities on systems previously thought to be highly secure. UltraScan builds and rebuilds the attack objectives every time data from multiple systems can analytically be coupled for future attacks.

NetRecon provides immediate feedback to the user interface on vulnerabilities found. Within seconds of starting a scan, results are displayed graphically as well as in text format for immediate viewing and manipulation. Hypertext Markup Language (HTML) page entries are built for each vulnerability found, with hot links to locations providing solutions for those vulnerabilities. These solutions provide a point and click method to correct the vulnerabilities within the network. Unlike other scanners that operate only on the Internet Protocol (IP), NetRecon scans multiple protocols (IP, IPX, SPX, and Windows Networking).



NetRecon makes it possible to determine nodes, names, cracking passwords; find services (such as telnet, login, http, NIS, and smtp) running on UNIX, NT and other platforms; exploit and attack those services; and get through the barriers currently in place. This process informs management of the potential threats and provides solutions to those threats.

NetRecon not only provides UltraScan results across multiple protocols in an easy-to-read HTML report, but those results are displayed immediately for quick feedback when running NetRecon. NetRecon offers security solutions to secure your data and to assist your organization by providing a better understanding of how a hacker could break through security barriers currently in place.

For more information, contact AXENT Technologies, Inc., at 1-888-44-AXENT or on-line at http://www.axent.com.

Steve Jackson received his B.S. in Computer Science from Brigham Young University in 1982. He is the OmniGuard/Enterprise Security Manager (ESM) Product Manager for AXENT Technologies, Inc.

The IATAC Information Assurance Tools Database hosts information on intrustion detection, vulnerability analysis, firewalls and antivirus appliations. A brief summary of Vulnerabilility Analysis Tools is provided on these two pages. For more information, see the IATAC Product Order Form on page 11.

Title	Attributes	Description
Ballista	comprehensive vulnerability analysis	Network security auditing tool used to discover weaknesses in networked environments.
CheckXusers	simple vulnerability analysis	Identifies users logged onto the current machine from insecure X servers.
Chkacct	simple vulnerability analysis	Designed to check the settings and security of the current user's account.
CONNECT	simple vulnerability analysis	This /bin/sh shell script scans a range of Internet Protocol (IP) addresses for machines that offer the Trivial File Transfer Protocol (TFTP) service.
COPS *(Computer Oracle and Password System)*	comprehensive vulnerability analysis	COPS is a security toolkit that examines a system for a number of known weaknesses and alerts the system administrator to them.
CPM *(Check Promiscuous Mode)*	simple vulnerability analysis	CPM checks whether any network interface on a host is in promiscuous mode.
Crack	password cracker	Password-cracking program with a configuration language that allows the user to program the types of guesses attempted.
DOC *(Domain Obscenity Control)*	simple vulnerability analysis	DOC diagnoses misconfigured domains by sending queries to the appropriate domain name system (DNS) nameservers and performing simple analysis on the responses.
DumpAcl	simple vulnerability analysis	DumpAcl dumps the permissions and audit settings for the Windows NT files system, registry, user/group information, and printers in a concise, readable, listbox format so the user can identify readily apparent security vulnerabilities.
ESPRIT *(Expert System for Progressive Risk Identification Techniques)*	risk analysis	Risk analysis and risk management tool that provides a detailed analysis of an information system in terms of assets, threats to assets, vulnerabilities, and countermeasure recommendations.
ICE-PICK	comprehensive vulnerability analysis	Automated security tool used to evaluate the vulnerabilities of network-based systems that use TCP/IP.
IdentTCPscan	simple vulnerability analysis	Scans remote hosts for active Transmission Control Protocol (TCP) services.
Internet Scanner	comprehensive vulnerability analysis	Performs scheduled and selective probes of network communication services, operating systems, key applications, and routers in search of common vulnerabilities that open the network to attack.
KSA *(Kane Security Analyst)*	misuse detection, system monitoring, comprehensive vulnerability analysis	KSA assesses the security status of a Novell and Windows NT network and generates reports in six areas: password strength, access control, user account restrictions, system monitoring, data integrity, and data confidentiality.
L0PHTCrack	password cracker	Comprehensive password cracker for Windows NT system and local area network (LAN) manager passwords.
Netective	simple vulnerability analysis	Identifies security vulnerabilities at both the operating system level and the network level. Netective validates the system using MD5 checksums and other security checks on system files, operating system patches, file permissions, and system passwords.
NetRecon	comprehensive vulnerability analysis	Runs on a Windows NT workstation and probes networks and network resources. NetRecon's UltraScan technique allows it to immediately dis play vulnerabilities as they're detected & quickly perform deeper probes.

Title	Attributes	Description
NetSonar	comprehensive vulnerability analysis	Using NetSonar from a central console, the user can assess the security state of an enterprise's entire network, track historical vulnerability trends, and create reports of potential security risks.
NSS (Network Security Scanner)	comprehensive vulnerability analysis	Scan individual remote hosts and entire subnets of hosts for various simple network security problems. The majority of the tests can be performed by any nonprivileged user on a typical UNIX machine.
Nfsbug	simple vulnerability analysis	Nfsbug checks for a variety of configuration errors in NFS, mountd, and portmapper daemons.
Omniguard/ ESM	comprehensive vulnerability analysis	Platform-independent security management tool that enables the user to manage and evaluate diverse systems according to unique, customizable security policies.
Perl Cops	comprehensive vulnerability analysis	Security toolkit that examines a system for a number of known weaknesses & alerts system administrator to them.
PINGWARE	comprehensive vulnerability analysis	PINGWARE systematically scans and tests all the systems on a TCP/IP based network from a single workstation.
RiskWatch v7.1	risk analysis	Conducts automated risk analysis and vulnerability assessments of information systems, including data centers, application programs, facilities, networks, and field offices.
SATAN *(Security Analysis Tool for Auditing Networks)*	comprehensive vulnerability analysis	SATAN scans systems connected to the network noting the existence of well-known, often-exploited vulnerabilities.
Secure Sun	simple vulnerability analysis	This program checks for 14 common SunOS configuration security vulnerabilities.
Snoopy Tools	comprehensive vulnerability analysis	A suite of programs that determine what network services are running under TCP/IP and attempt to exploit bugs in those services.
SPI-NET	comprehensive vulnerability analysis	Supports multihost system security inspections managed from a designated "command host." These inspections include access control testing, system file authentication, file system change detection, pass word testing, and common system vulnerability checks.
Strobe	vulnerability anlaysis	Network security tool that locates and describes all listening tcp ports on a (remote) host or on many hosts.
System Security Scanner	comprehensive vulnerability analysis	Assesses operating system configuration, file permissions and ownership, network devices, account setups, program authenticity, and common user-related security issues such as guessable passwords.
Tiger	comprehensive vulnerability analysis	Used to check for security problems on a UNIX system; it scans system configuration files, file systems, and user configuration files for possible security problems and reports them.
ToneLoc	war dialers	Scans a block of telephone numbers for active dial-up services.
Trident Information Protection Toolbox	risk analysis	Trident's Toolbox is a set of three complementary tools that assist in protecting critical information assets.
VISART *(Value of Information Structured Analysis Risk Tool)*	risk analysis	(Under development) This tool allows the user to analyze systems, their vulnerabilities, and possible threats, and quantify what types of counter-measures are justifiable in terms of cost.
Xscan	simple vulnerability analysis	This utility scans a host, or a range of hosts, for unprotected X displays.

Support for User Inquiries

by Mr. Robert P. Thompson
Director, IATAC

IATAC offers the DoD a quick response capability for IA technical inquir-ies. User inquiries vary in nature, from "I'd like to receive a copy of the Vulnerability Analysis Report" to more complex requests such as "how do you develop secure code for web pages". Inquiries are received via the IATAC home page, e-mail, telephone, verbally at meetings, and/or tasking from the IAC Program Manage-ment Office (IAC PMO). For IATAC to process the inquiry, the requestor must be a registered DTIC user (ref http://www.dtic.mil/dtic/regprocess.html). Inquiries fall into 4 categories.

Basic: requests for information requiring 8 technical hours or less to complete. Funded through existing IATAC operations.

Extended: requests for information requiring 8–24 technical hours to complete. Funded on a cost recovery basis.

Search & Summary: consists of, but not limited to, a literature search and printout of relevant abstracts to include reviewing the abstracts and identifying the most pertinent information and requiring 24– 40 technical hours to complete.

Review & Analysis: additional to extended and search & summary efforts, support consists of direct consultation with staff and/or consulting subject-matter experts, a brief paper synthesizing the results of the technical review, complete copies of references and the requisite materials for access to databases, if necessary and requiring 40–80 technical hours to complete. Inquiries exceeding 80 hours of support are accomplished through a technical area task.

Results of technical inquiries are provided back to the requestor and are entered into the IATAC IA scientific and technical information (STI) collection, which functions as a primary resource for the processing of future technical inquiries. The collection, coupled with the broad range of technical expertise available, allows IATAC to quickly respond to both routine and high priority technical inquiries.

continued from page 3

Another basic component is up-to-date knowledge of research conducted in academia, other government agencies, and commercial activities (especially DARPA, the other service basic research labs, and ARL's collaborating partners). ARL strives to leverage progress made elsewhere and eliminate duplication of effort by identifying common areas of interest and opportunities for collaboration. Its objective is to identify IA research needs bearing on land warfare or the institutional Army that are not being met through external programs. These land warfare digitization challenges are generally related to assured information services for highly mobile ground combat in theaters of operation that are likely to be composed of coalition forces.

ARL's approach to IA orients the lab's traditional areas of expertise to address relevant IA problems. This approach directs ARL's scientific capabilities (i.e., information technology, human factors, and electromagnetic effects) to IA needs that are defined not only by the technical environment but equally by operational doctrine and future warfighting concepts. The problem domain consists of challenges that impede fulfillment of the Army's near-term (i.e., to 2010) digitization objectives as well as those for the AAN. End-users, testers and evaluators, ARL analysts, industry consultants, and developers of future doctrine and force structure identify these "challenges," which ARL assimilates as input to its program of IA research. Major ARL thrusts bearing on IA problems include:

- Developing advanced tactical telecommunications protocols
- Applying intelligent software agents to assure information systems
- Researching human factors to understand how Army organizations value, consume, and protect information
- Investigating "survivable systems" principles to create new high-level architectures and elevate the practice of hardware and software engineering.

Analysis supporting the AWE, coupled with CSIRT experience, gives ARL insight into tactical and sustaining-base IA issues facing the digitized land force of the future. This insight produces an approach, tempered both in practice and theory, that focuses ARL's scientific expertise on IA problems. To assist in solving these problems, ARL is building an IA knowledge base that will lead to improvements in Army IA capability, reducing the risks to land operations while contributing to progress in national information infrastructure protection.

LTC Walczak is Program Manager for Information Assurance Research at the Army Research Lab. He is a member of the Army Acquisition Corps and is a certified computing professional (CCP).

calendar

JUL 21-23

IET[21] — Leveraging Intelligent and Emerging Technology to Support 21st Century Leaders
Fort McNair, Washington, DC
Sponsored by the National Defense University and The Army CIO Strategic & Advanced Computer Center
extranet.ndu.edu/keg/register.htm

AUG 17–21

WebSec '98: The Conference on Web, Internet and Intranet Security
San Francisco, CA
call 508.879.7999
www.misti.com
WebSec '98 offers up-to-date solutions for ensuring information integrity, privacy and security on the 'Net. The conference expo will be August 18 and 19.

SEP 9–10

InfowarCon '98: The 8th Annual Conference on Information Assurance and Information Operations for the Enterprise and the Infrastructure
Produced by Winn Schwartau and MIS Training Institute
Washington, DC
call 509.879.7999
www.misti.com/regform.html
Email: mis@misti.com
This conference zeros in on military operations, infrastructure protection, and the growing threat of high-tech terrorism and espionage in today's information-dependent world.

SEP 22–24

Achieving Information Dominance & Assurance
Sponsored by AFCEA Fort Monmouth Chapter
Long Branch, NJ
call Diane Carnes 732.758.9009

OCT 6–7

Information Systems Security Exposition (ISSE)
Exposition sponsored by AFCEA International
Conference sponsored by the National Institute of Standards and Technology and National Computer Security Center
Crystal City, VA
call J. Spargo & Associates, Inc., 703.631.6200

OCT 7–8

Command, Control, Communications and Intelligence Systems Technology (C⁴IST)
Sponsored by the AFCEA Southern Arizona Chapter
Fort Huachuca, AZ
call Bill Reich 520.378.2045

OCT 18–21

Milcom '98 (Unclassified and Secret Sessions)
Sponsored by the Institute of Electrical and Electronics Engineers Communications Society, Raytheon Company and AFCEA International
Bedford, MA
call Dr. Fred Unkauf
508.490.1126

OCT 20-22

Infotech '98 Conference and Exposition
Sponsored by the AFCEA Dayton-Wright Chapter
Dayton, OH
call J. Spargo & Associates, Inc.
703.631.6250

OCT 28–29

Fall Intelligence Symposium (Top Secret SI/TK)
Sponsored by AFCEA International
Washington, D.C.
call AFCEA Intelligence Department 703.631.6250

what's new

IA Tools Report: Vulnerability Analysis

New Products

The latest IATAC Information Assurance (IA) Tools report, Vulnerability Analysis is now available. This report provides an index of vulnerability analysis tool descriptions contained in the IATAC IA Tools Database, one of IATAC's knowledge bases. It summarizes pertinent information, providing users with a brief description of available tools and contact information. As a living document, this report will be updated periodically as additional information is entered into the database.

Currently the IA Tools database contains descriptions of 35 tools that can be used to support vulnerability and risk assessment. The information type and level of detail provided among tools varies greatly. Although some can identify only a minimal set of vulnerabilities, others can perform a greater degree of analysis and provide detailed recommended countermeasures The database includes commercial products, individually developed tools, government-owned tools, and research tools. The database was built by gathering as much open-source data, analyzing that data, and summarizing information regarding the basic description, requirements, availability and contact information for each vulnerability analysis tool collected. For instructions on obtaining this report, refer to IATAC Product Order Form.

New Holdings

Report on the NS/EP Implications of Intrusion Detection Technology Research and Development

Originator: National Security Telecommunications Advisory Committee (NSTAC) Network Group, Intrusion Detection Subgroup, December 1997

Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection

Originator: Thomas H. Ptacek and Timothy N. Newsham, Secure Networks, Inc., January 1998

Conference Proceedings, The Tenth Annual Software Technology Conference, "Knowledge Sharing — Global Information Networks"

Originator: Utah State University, April 19–23, 1998

White Paper, The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63

Originator: THE WHITE HOUSE, May 22, 1998

White Paper - Intrusion Detection Methodologies

Source: Robert A. Clyde, AXENT Technologies, Inc.

IATAC Product Order Form

IMPORTANT NOTE: *All IATAC Products are distributed through the Defense Technical Information Center (DTIC). If you are NOT a registered DTIC user, you must do so PRIOR to ordering any IATAC products. To register with DTIC go to http://www.dtic.mil/dtic/regprocess.html.*

Name _____

Organization_____Ofc. Symbol _____

Address_____ Phone _____

_____ E-mail _____

_____ Fax _____

_____

DoD Organization? ❑ YES ❑ NO If NO, complete **LIMITED DISTRIBUTION** section below.

LIMITED DISTRIBUTION	QTY.	PRICE EA.	EXTD. PRICE
In order for NON-DoD organizations to obtain LIMITED DISTRIBUTION products, a formal written request must be sent to IAC Program Office, ATTN: Sherry Davis, 8725 John Kingman Road, Suite 0944, Ft. Belvoir, VA 22060-6218			
Contract No. _____ *For contractors to obtain reports, request must support a program & be verified with COTR*			
COTR _____ Phone _____			
❑ **Modeling & Simulation Technical Report**		No Cost	
❑ **IA Tools Report — Intrusion Detection**		No Cost	
❑ **IA Tools Report — Vulnerability Analysis**		No Cost	
❑ **Malicious Code Detection SOAR** ❑ TOP SECRET ❑ SECRET		No Cost	

Security POC_____ Security Phone _____

UNLIMITED DISTRIBUTION	QTY.	PRICE EA.	EXTD. PRICE
❑ **Newsletters** *(Limited number of back issues available)*			
❑ Vol. 1, No. 1 ❑ Vol. 1 No. 2 ❑ Vol. 1 No. 3 ❑ Vol. 2, No. 1		No Cost	
		ORDER TOTAL	

Please list the Government Program(s)/Project(s) that the product(s) will be used to support:_____

_____

_____

Once completed, Fax to IATAC at 703.902.3425

ARE sharing your IAnewsletter

For Additions, Deletions and Changes

— U.S. Distribution Only —
Copy this page, complete the form and fax to IATAC at 703-902-3425

❑ Change ❑ Add ❑ Delete

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