April 2000

Inside Oversight

Office of Independent Oversight OA Performance Assurance
U.S. Department of Energy

Inside this Edition

Front Page

Cyber Security Network Performance Testing

About Independent Oversight

Tabletop Walkthroughs Provide Big Benefit at Low Cost

Classified Materials Storage Problems

Page 2: Distributed Denial of Service

Page 4: Upcoming Oversight Activities

Page 4: Solicitation of Comments

For More Information: Visit Our Website at: http://tis.eh.doe.gov/iopa

Cyber Security Network Performance Testing

Most assessment activities in the Office of Cyber Security and Special Reviews (OA-20) involve performance testing. Performance testing is used to identify deficiencies in the technical implementation of computer network security at DOE sites that might allow penetration by an outside threat. However, the purpose of performance testing is not merely to attempt penetration of a site's network, but to fully evaluate the ability of the computer network system at a DOE site to protect computer resources and data from both external and internal threats. Therefore, OA-20 also reviews firewall parameters, or "rules," to analyze all potential pathways into the network and the likelihood that the pathways could be exploited without access to the rules.

Complete security evaluation of a computer network system at a DOE site typically involves external testing to evaluate the strength of barriers that protect against external threats (e.g., hackers, foreign intelligence), and internal testing to evaluate the barriers that protect against internal threats (e.g., disgruntled employees, visitors).

(Continued on Page 2)

About Independent Oversight

In response to concerns over security, the Secretary of Energy announced his Security Reform Package on May 11, 1999, a significant feature of which was the creation of the Office of Independent Oversight and Performance Assurance (OA), reporting directly to the Secretary of Energy.

(Continued on Page 4)

Tabletop Walkthroughs Provide Big Benefit at Low Cost

Tabletop walkthroughs are a method of performance testing and one of the most valuable data collection methods available to OA-30 appraisal team members. Tabletop walkthroughs are designed to determine whether personnel and organizations have the tools, skills, and abilities to perform their duties, and also whether procedures will work as written. Virtually any skill, duty, or procedure can be performance tested by tabletop walkthroughs.

OA-30 uses tabletop walkthroughs to assess the performance of selected emergency response personnel, typically incident commanders or other personnel responsible for initial decision-making, in response to a postulated event that requires an immediate site action.

(Continued on Page 3)

Classified Materials Storage Problems

DOE has established requirements for storing classified materials under both standard and non-standard storage methods. Under standard storage methods, classified materials through Top Secret are typically stored within Limited Areas in vaults, in vault-type rooms, or in Government Services Administration (GSA)-approved repositories.

(Continued on Page 3)

Distributed Denial of Service

The recent attacks on several popular, commercial Internet sites have sparked public interest in a "new" technique for attacking a network system from several locations concurrently. In fact, these distributed denial of service (DDoS) capabilities have been available as part of certain commercial software products for some time. However, toward the end of 1999, several open-source DDoS tools were released into the public domain on the Internet. The wide-spread availability of these tools led, eventually, to the attacks that have since been the source of much debate and reporting.

The DDoS tools that fostered the recent spate of attacks against commercial Internet sites are user/server applications that use bandwidth-based attacks from several servers and cause targeted systems to become unresponsive. The server applications are controlled remotely by a user/attacker using a single user control program. The results of the attacks can be devastating, as multiple networks saturate the targeted system's available bandwidth and cause system failure and, eventually, network collapse.

The current generation of DDoS tools is capable of "spoofing" source address information by using random source addresses and ports. Thus, discovering the origins of the attacks can be very difficult. Attacks are usually traced by back stepping through the network stream to each network component where an inordinate amount of traffic occurs. Most anti-virus software programs as well as commercial intrusion detection systems can detect the presence of these attack tools. However, the best defense against DDoS tools or any other Internet Control Message Protocol (ICMP)-based tools is to block all ICMP traffic at the firewall or border router.

Readily available hacker tools can cause network collapse.

Unfortunately, a new generation of DDoS tools, which may result in far more problems for Internet servers, is on the horizon. One new type of tool uses network stream vulnerabilities in the Transmission Control Protocol/Internet Protocol (TCP/IP). Attacks by this type of DDoS tool require less network traffic to "jam" target systems and cause them to become unresponsive.

A second type of tool involves multicasting. Multicasting was first used in the widely publicized "smurf" attacks. Multicasting attacks use systems that multiply packets of network output across one or more network segments. Newer multicasting tools could use these systems to amplify the saturation process. Thus, they, too, would require fewer servers to crash a targeted system.

DOE and DOE sites are, daily, increasing their reliance on the Internet for both communications and research activities. DDoS attacks highlight the need for strong firewalls at DOE sites and continued diligence by computer network administrators to stay abreast of the latest trends for attacking Internet sites, so that communications and research activities can proceed, secure and uninterrupted. Again, the best defense against even the new generation of DDoS tools is to block all ICMP traffic at the firewall. ■

Cyber Security (continued)

Most systems are tested in two phases: offsite and onsite. OA-20 conducts the offsite phase of performance testing from its testing facility. This phase consists of scanning telephone numbers at a site to identify which, if any, are used for computer modems in "auto-answer" mode. The site's Internet addresses are also scanned for vulnerabilities or configuration anomalies that could allow unauthorized access to the site's computer network system.

OA-20 uses the same scanning tools during the onsite phase of testing to evaluate systems located behind a site's firewalls. During this phase, OA-20 evaluates both the effectiveness of barriers that protect against external threats and the host-level security features that protect against internal threats. Using information derived through network mapping and automated scanning, evaluators attempt to access systems protected by the site's firewalls. Vulnerabilities that may be exploited during testing include buffer overflows, application or system misconfiguration problems, routing problems, Domain Name Server (DNS) attacks, cracking of captured passwords, address "spoofing," share access, and inherent system trust relationships. If a user account is compromised, that account is tested for access permissions, and attempts are made to subvert systems into granting super user, root, or administrator access to internal devices. Any additional information discovered may also be used to gain access to other systems. Finally, other attack tools or information gathering tools may be installed to further penetration, depending on need and applicable protocols.

During announced performance testing at a DOE site, all activities are coordinated with the site's cyber security point-of-contact through the DOE operations office. Every attempt is made to prevent damage to computers and other network devices during testing. However, some penetration scenarios may cause temporary service interruption. If services are interrupted, OA-20 works with site personnel to restore the system to its desired state of operation. ■

Classified Materials Storage (continued)

Schedules for patrols by protective forces and response times for alarms are also established for all standard storage methods.

Under non-standard storage, classified materials may be stored within Limited Areas without vaults, vault-type rooms, or repositories, i.e., in open storage, provided that the requirements of the *DOE Classified Matter Protection and Control Manual* (the Control Manual) are met. The requirements in the Control Manual rely primarily on effective alternative protection measures in lieu of standard storage. Typically, these protection measures include more frequent patrols by protective forces. The schedule of patrols for non-standard storage locations is determined through vulnerability analyses and on the basis of reasonable risk.

Over the past year, the Office of Independent Oversight and Performance Assurance (OA) has observed a number of problems involving the storage of classified materials, e.g., weapons components, at several sites within the DOE weapons complex. Most problems have been associated with storage of classified materials in non-standard open storage. The problems included:

- Storage of small, classified material items in unapproved security containers, such as steel file cabinets, older repositories, and "space savers."
- Storage of classified materials in open storage locations that site Security was unaware of.
- Storage of classified materials within Limited Areas in storage buildings with no interior alarm sensors. Both perimeter and interior alarm sensor arrays are required to meet vault or vault-type room requirements.
- Storage of classified materials in unalarmed, open storage buildings where patrols by protective forces were ineffective, e.g., no building walk-downs, or walkdowns were too infrequent or lacked a reasonable analysis for determining their frequency.

DOE is currently drafting guidance directing DOE field elements to provide information to Headquarters on the alternative protection measures being used for non-standard storage of classified materials at their sites. DOE Headquarters will evaluate these measures for effectiveness and reasonability considering the materials involved, and, as appropriate, will approve the non-standard storage.

Even before this guidance is final, however, DOE sites can act to address problems with non-standard storage of classified materials. Corrective measures may include:

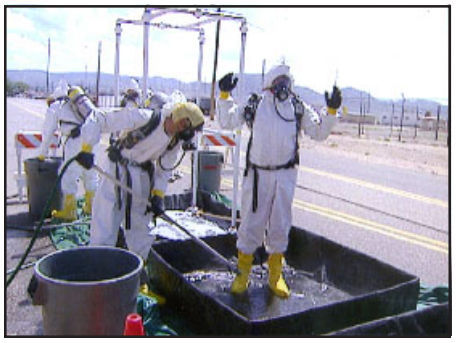
- Replacing older, non-GSA-approved repositories with approved containers
- Relocating and consolidating classified materials in older, unapproved repositories into vaults or vault-type rooms
- Decreasing the need for storage of classified materials by increasing the rate of destruction of unneeded materials
- Consolidating classified materials into fewer or centralized, standard (approved) storage locations
- Increasing the frequency with which non-standard storage locations are patrolled
- Establishing protective force posts at non-standard storage locations. ■

Tabletop Walkthroughs (continued)

These walkthroughs are particularly useful when an onsite assessment visit does not coincide with a scheduled site exercise or drill. The OA-30 evaluator develops an emergency scenario to test the proficiency of the emergency responder in selected functions, such as event categorization and classification. A subject matter expert is designated by the site to be the "trusted agent." This individual reviews the emergency scenario to ensure that it is consistent with site plans, procedures, and terminology and to validate the appropriate response. To begin the walkthrough, the individual being evaluated is briefed on its purpose and on the guidelines that will be followed for conducting the tabletop walkthrough. The examinee is then provided the initial conditions and assumptions, as well as all information and response tools he/she would normally have available during the postulated event. The evaluator observes the actions taken by the examinee and notes the documentation used to support his/her actions. Several walkthroughs are conducted (a sample of incident commanders), using the same scenario, to ensure that any conclusions regarding emergency responder readiness and proficiency are valid.

OA-30 believes that an important near-term step that DOE sites can take to improve emergency management is the establishment of their own program of challenging tabletop walkthroughs. Such a program would have several benefits, including:

- Verifying that individuals and organizations can perform their duties that involve time-urgent decisions



- Validating that procedures will work as written
- Minimal cost and resources to set up and conduct
- Identifying weaknesses in reference information, tools, and decision aids.

OA-30 encourages all Headquarters and field elements with emergency management responsibilities to incorporate tabletop exercises as a component of their training program. Efforts are now being coordinated to provide feedback to SO-40 in their development of a training class focusing on performance based tabletop walkthroughs. ■

About Independent Oversight (continued)

OA is responsible for conducting independent oversight – inspections, evaluations, and reviews – of how DOE policies and operations are being carried out at DOE sites in the areas of nuclear safeguards, security, cyber security, emergency management, and other critical functions. To perform its mission, OA has a dedicated team of managers and professional staff with extensive experience in independent oversight. The key managers are:

- Glenn Podonsky, Director for OA
- Michael Kilpatrick, Deputy Director for OA
- Barbara Stone, Director, Office of Safeguards and Security Evaluations
- John Hyndman, Deputy Director, Office of Safeguards and Security Evaluations
- Brad Peterson, Director, Office of Cyber Security and Special Reviews
- Chuck Lewis, Director, Office of Emergency Management Oversight
- Ali Ghovanlou, Information Management and Tracking Group.

The OA independent oversight function has been formally defined in DOE Order 470.1A, Security and Emergency Management Independent Oversight and Performance Assurance Program, March 2000. OA has also established an Appraisal Process Guide that delineates the processes and protocols that govern the conduct of OA appraisals. Both the order and Appraisal Process Guide incorporate the direction from the Deputy Secretary related to time frames for developing corrective action plans in response to OA findings. The order and Appraisal Process Guide can be found under the *Guidance Documents* portion of the *Reports* section on the OA Web site (http://tis.eh.doe.gov/iopa/reports/reports.html).

Although DOE has had an independent oversight program for over 15 years, the establishment of OA has provided an opportunity to reevaluate and improve previous processes. As one example, OA has established a separate office within OA that focuses primarily on cyber security, which is an area of immense importance to DOE. Cyber security is a significant challenge for DOE to address for many reasons, including the ever-increasing availability of hacker tools and techniques. For example, one of the articles in this edition describes how readily-available hacker tools can be used to "crash" DOE computer networks, and the importance of a firewall in deterring and mitigating such attacks.

As another area of emphasis, OA is taking a much more active role in working with cognizant secretarial offices and the Office of Security and Emergency Operations (SO) with the goal of working collegially to ensure that identified weaknesses are resolved in a timely manner. For example, OA is working with SO to ensure that the results of a recently-completed OA emergency management follow-up review are coordinated with SO initiatives related to emergency management, particularly in the area of training and tabletop exercises.

Communication with the field has always been, and will continue to be, a high priority for OA. OA plans to issue this newsletter from time to time. This first issue provides four articles related to the results of recent independent oversight activities. In future newsletters, OA will provide similar information about its program and the results of oversight reviews, with a major focus on summarizing lessons learned and sharing results that DOE sites may find interesting and useful in improving their safeguards and security, cyber security, or emergency management programs. As always, OA is interested in your feedback on this newsletter, as well as suggestions for future articles.

Upcoming Oversight Activities

Review of Headquarters Cyber Security
Purpose: Scanning and penetration testing and onsite review of cyber security at Headquarters.
Dates: March 30-April 28, 2000
Contact: Brad Peterson, 301-903-5781

Review of Nevada Operations Office
Purpose: Programmatic review of selected aspects of safeguards and security at the Nevada Operations Office and Nevada Test Site.
Dates: April 10-21, 2000
Contact: Barbara Stone, 301-903-5895

Review of Waste Isolation Pilot Project
Purpose: Review of emergency management with emphasis on transportation of hazardous materials.
Dates: May 1-11, 2000
Contact: Chuck Lewis, 301-903-1554

Composite Adversary Team Training
Purpose: Annual training for the Composite Adversary Team on tactics, equipment, and security systems.
Location: Nevada Test Site, Las Vegas, Nevada
Dates: April 17-21, 2000
Contact: Ricky Honaker, 301-903-9123

Presentation at the 22nd Annual DOE Computer Security Conference
Purpose: The presentation will describe the OA-20 methodology used to evaluate cyber security programs through the use of performance testing and management reviews.
Date: May 2, 2000
Contact: Brad Peterson, 301-903-5781

Solicitation of Comments, Questions, and Suggestions

OA welcomes your thoughts about our newsletter. Please send or phone comments, questions, or suggestions to:

Glenn S. Podonsky, Director
Office of Independent Oversight and Performance Assurance
U.S. Department of Energy
19901 Germantown Road
Germantown, MD 20874
301-903-3777

e-mail: Glenn.Podonsky@eh.doe.gov

This newsletter can be found on the OA web site at **http://tis.eh.doe.gov/iopa**.