IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELOUISE PEPION COBELL, et al.,

Plaintiffs,

v.

GALE A. NORTON, Secretary of the Interior, et al.,

Defendants.

Case No. 1:96CV01285
(Judge Lamberth)

INTERIOR DEFENDANTS' SUBMISSION PURSUANT TO THE JULY 28, 2003 PRELIMINARY INJUNCTION REGARDING RECONNECTION OF COMPUTER SYSTEMS

On July 28, 2003, the Court issued a Preliminary Injunction that required the Department of the Interior ("Interior") to immediately disconnect from the Internet all information technology ("IT") systems that house or access individual Indian trust data, subject to exceptions for systems that are essential for protection against fires or other threats to life or property, systems that do not house or access individual Indian trust data, and systems that are secure from Internet access by unauthorized users.[1] Preliminary Injunction at 3-4. The Court further required Interior Defendants to submit a proposed method for reconnection of disconnected computer systems and of determining whether reconnected systems remain secure:

[1] The Preliminary Injunction required Interior Defendants to submit certifications regarding systems that were subject to these exceptions. Those certifications were filed on August 11, 2003.

> Within thirty (30) days of the date of entry of this Order, the Interior defendants shall file with the Court a proposal setting forth a method of approving individual reconnections of disconnected Interior computer systems, and of determining whether the Reconnected Systems should stay reconnected. The proposal should demonstrate a method of providing to the Court adequate evidence that the Reconnected Systems and the Information Technology Systems disconnected pursuant to this Order are secure against Internet access by unauthorized users, and provide a means to verify the representation that the Reconnected Systems and the Information Technology Systems disconnected pursuant to this Order are secure against Internet access by unauthorized users.

Preliminary Injunction at ¶ B.3.[2] In compliance with the foregoing provision, Interior Defendants respectfully submit their method for approving individual reconnections of disconnected bureau or office IT systems and ascertaining whether reconnected systems should stay connected.

Interior Defendants reiterate that this and other submissions they make in connection with the Preliminary Injunction and any related orders the Court may issue should not be construed as a waiver of objections they have asserted or may assert, their right to pursue an appeal, or their right to seek modification or vacatur with respect to the Preliminary Injunction and any related orders.

[2] Paragraph B.3 of the Court's Order, relating to the submission of reconnection and monitoring plans, does not explicitly exclude systems that do not house or access individual Indian trust data. However, because Interior Defendants understand those systems to be beyond the intended scope of the Preliminary Injunction (see Paragraph B.1), the reconnection and monitoring plans set forth herein do not encompass such systems.

I. **Procedures for Reconnection of Disconnected Systems**

The Preliminary Injunction requires that the method for determining whether disconnected bureau or office IT systems[3] should be reconnected include two basic elements. First, the Order provides that the submission should demonstrate a method of providing the Court with "adequate evidence" that the bureau or office IT system is secure against Internet access by unauthorized users. Preliminary Injunction at ¶ B.3; Memorandum Opinion at 33 (July 28, 2003). Second, the Order states that the submission should provide the Court with the "means to verify the representation" that the bureau or office IT system is secure against unauthorized Internet access.[4] Preliminary Injunction at ¶ B.3; Memorandum Opinion at 33-34. The Department of the Interior proposal set forth herein satisfies those two requirements.

Under the procedures provided herein, the Department of the Interior will provide reconnection submissions to the Court describing the analysis undertaken by the bureau or office and the basis for the

[3] Interior believes that four bureaus or offices hosting fiduciary trust IT systems fall into this category: the Office of the Special Trustee ("OST"); the Office of Hearing and Appeals ("OHA"); the trust portion of the Bureau of Indian Affairs ("BIA"); and the Office of the Solicitor ("SOL"). Proposals for the reconnection of OHA and OST were submitted to the Special Master under the terms of the December 17, 2001 Consent Order, and the Special Master's IT experts tested those systems on a number of occasions. In reports dated April 23, 2003, the Special Master's experts recommended that OHA be allowed to reconnect to the Internet, but the Special Master failed to act on this report. OST corrected certain minor personnel-related objections raised by the Special Master's experts and provided this information to the Special Master on May 16, 2003, thereby resolving all outstanding objections. However, no final action was taken by the Special Master in response to the May 16, 2003 communication.

[4] The Court explained in its Memorandum Opinion that "[t]he nature of such independent tests may either be borrowed from an existing set of testing standards, such as that developed by the National Institute of Standards and Technology, or determined by either an independent contractor with whom the Court is satisfied or a separate government agency, such as computer experts from the Department of the Treasury." Memorandum Opinion at 34.

conclusion that the subject IT system is secure from Internet access by unauthorized users. In addition to the analysis, the submission will summarize the security testing undertaken by the bureau or office to verify the representation that the individual Indian trust data housed by the IT system is secure from Internet access by unauthorized users. Interior intends to utilize a testing program that will include relevant testing procedures sufficient to support and verify its representation that the systems are secure from unauthorized Internet access.[5] A bureau or office that makes a reconnection submission would be entitled to reconnect to the Internet, absent an order to the contrary, 14 days after the filing of the submission. Any judicial review would take place on a highly expedited basis, in view of the harm to the government and the public interest that result from disconnection of Interior's IT systems.

A. Adequate Evidence that the Information Technology System Is Secure from Internet Access by Unauthorized Users

There is no fixed test or set of standards, guidelines, or technologies that distinguish between a secure IT system and one that is deemed not secure, nor is there a uniformly accepted minimum

[5] The detailed results of the testing (i.e., the "raw data") will not be included in Interior's Court submission because of the extremely sensitive nature of some of this material. The "raw data" and detailed results of the testing would be maintained by the agency and be available for inspection *in camera* or pursuant to an appropriate protective order. As the Court is aware, on August 4, 2003, Interior Defendants filed a motion for a protective order as to IT security materials required to be submitted in connection with the Preliminary Injunction. Interior Defendants' Motion For A Protective Order With Regard To Information Technology Security Materials To Be Submitted Pursuant To July 28, 2003 Preliminary Injunction (Aug. 4, 2003).

standard within the federal government for IT system information security.[6] Instead, various standards and policies identify mechanisms and types of technology that can be utilized to increase the security of IT system information. As is explained below, the decision whether to connect government IT systems to the Internet is committed by federal law to the respective agencies, to be made after considering appropriate factors.

The Federal Information Security Management Act of 2002 ("FISMA") vests in the heads of federal agencies the responsibility to provide information security protections. 44 U.S.C. § 3544 (2003). FISMA provides for agencies to develop programs under which the agency conducts periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency. 44 U.S.C. § 3544(b)(1). Accordingly, Interior's bureau and office heads and Chief Information Officers, when determining whether an IT system is "secure" for purposes of deciding whether or not to connect to the Internet, consider the significant benefits and advantages to the agency or office and to the public in being connected to the Internet, as well as the risk of harm that could result from unauthorized access.

[6] The Office of Management and Budget has issued Circular A-130, which establishes policy for the management of federal information resources, including procedural and analytical guidelines for implementing specific aspects of the policy. The National Institute of Standards and Technology ("NIST") provides guidance for information security that is used by federal agencies to assess and improve IT security. Although neither Circular A-130 nor NIST guidance establishes a single defined standard for determining if a government IT system is secure for purposes of connecting to the Internet, Interior considers both sets of guidelines in assessing the security status of its IT systems.

Each submission for reconnection of a disconnected bureau or office IT system to the Internet will contain a summary of information relied upon by the bureau or office head in making the determination that such IT system is adequately secure from unauthorized access to permit connection to the Internet. IT security will be considered by the bureau or office head in the context of its mission, the role that Internet access plays in the accomplishment of the mission, and the nature of the sensitive information in the possession of the bureau or office. Recognizing that no IT system connected to the Internet can be made impregnable from every potential risk of unauthorized access, the head of the bureau or office will balance the need for the access against the security features built into the IT system before making a determination that the system is adequately secure to permit Internet connection. The bureau or office submission for reconnection to the Internet will include a discussion of these factors.[7] The submissions generally would include information regarding (1) the bureau or office's mission and its need for Internet access; (2) the nature of the individual Indian trust data it possesses; and (3) the bureau or office's current security status, including the use of firewalls and other defenses, identification

[7] The procedure proposed by the Department of the Interior is similar to that employed in the certifications submitted to the Court on August 11, 2003 concerning the secure status of the IT systems housing or accessing individual Indian trust data (Minerals Management Service ("MMS"), Bureau of Land Management ("BLM"), National Business Center ("NBC"), and the Office of the Inspector General ("OIG")). The submissions to the Court for reconnection will contain the same general type of information; more detailed information will be maintained by Interior for inspection if required by the Court, as public disclosure of this sensitive information would seriously endanger the security of the IT systems. Under the Consent Order, this information was not publicly disclosed, and was provided to the Special Master's experts under various protective orders, culminating in the Special Master's May 2, 2002 Revised Order.

and authentication, filtering, personnel security, vulnerability assessments and remediation, response plans, and testing done to the IT systems.[8]

B. Means to Verify Representation that System is Secure from Internet Access by Unauthorized Users

Each bureau or office for which reconnection is intended will take steps to verify its representation that the IT system is secure from Internet access by unauthorized users. The documentation will incorporate the data necessary to support a risk-based decision on Internet reconnection. The assessment may include, as appropriate: (1) network mapping and enumeration; (2) SANS/FBI Top 20 Vulnerability List Comparison; (3) vulnerability assessment; and (4) penetration testing.[9] Alternative comparable methods may also be utilized in the assessment, depending on the characteristics of the particular system being tested. A report which provides a detailed summary of the procedures and the results of the system tests will be provided.[10]

[8] Determinations of whether IT systems are adequately secure are, by their nature, system-specific. Accordingly, the foregoing is intended to provide an illustration of the factors that may be considered by the agency in making such determinations, rather than an exhaustive or mandatory list to be followed by the bureau or office in every situation.

[9] In performing the assessment, Interior or its contractor will draw from a variety of tools, including some of those identified by NIST in its security testing guidelines. See, e.g., National Institute of Standards and Technology, Sp. Pub. No. 800-42, Draft Guideline on Network Security Testing § 4.C ("Common Testing Tools"). A copy of the relevant excerpt is attached hereto as Exhibit 1. The entire publication is presently available through the Internet at http//csrc.nist.gov/publications/drafts/security - testing.pdf.

[10] The raw data gathered as a result of the testing programs will not be attached to the submission because of the sensitive nature of this information.

1. Network Mapping and Enumeration

These tests are designed to accurately map all active devices and systems connected to the target network. Interior or its contractor[11] will use various tools to discover active network devices to create an accurate baseline of the target network. Target networks are network segments that are or will be accessible to the Internet. Such segments will include network "Demilitarized Zones" or "DMZs." The baseline created from these tests will be utilized to identify target systems for ensuing assessment phases.

2. SANS/FBI Top 20 Vulnerability List Comparison

These tests are designed to identify vulnerabilities listed in the SANS/FBI Top 20 Vulnerability List. This is a list of the most common exploitable and critical vulnerabilities prioritized by the security experts of the SANS Institute and the FBI.[12] Assessment tools that are specifically configured to identify any vulnerability found on the list may be employed.

3. Vulnerability Assessment

Vulnerability testing is designed to determine vulnerabilities on all external facing hosts or hosts made accessible to the Internet. Interior or its contractor will make use of open-source tools and various techniques to accurately determine and verify the security status for such hosts. The vulnerability testing program will assist the IT staff at each site to analyze tool output, to prioritize vulnerabilities, and to eliminate both real and false positives.

[11] Interior's current contractor is Science Applications International Corporation ("SAIC").

[12] The SANS Institute refers to the System Administration, Network and Security Institute. Attached hereto as Exhibit 2 is a description of the SANS/FBI Top 20 List extracted from a document available at http://www.sans.org/top20/.

4. Penetration Testing

Penetration testing involves the attempt to identify, exploit, or expose high risk, configuration-specific vulnerabilities that are found. The purpose of such testing is to evaluate further the security controls implemented at the target site by allowing the penetration test engineer to use techniques and tools utilized by real-world malicious intruders to launch attacks. To simulate such attacks, Interior or its contractor will use proprietary and publicly available tools to attempt to gain access to systems that may be vulnerable to attack. Tools will be selected based upon their applicability to the IT system and/or the threat circumstance being emulated. Evidence of exploited vulnerabilities will be collected and documented. This will include objects such as screenshots, log files, and file notations.

5. Reporting

Interior or its contractor will assess all data gathered, including information collected from IT staff, tool output, observations, and any other notes collected during the overall assessment. At the conclusion of the analysis, a detailed report regarding the security posture of the system will be provided to the system owner. This summary will describe the effectiveness of the security controls, processes, and procedures in place. The summary, along with the other data, forms the basis for a decision by Interior regarding the system's security posture.

II. Procedures for Monitoring the Security of Reconnected Systems

In its Memorandum Opinion, the Court stated that Interior's proposal must provide for continued monitoring of systems that have been reconnected to the Internet to ascertain whether such systems remain secure. Memorandum Opinion at 34. Consistent with this instruction, bureaus and offices with reconnected systems that house or access individual Indian trust data will file a status report with the Court on an annual basis with approximately one quarter of the agencies reporting each quarter.[13] Each status report filed with the Court will consist of a report from the bureau or office, and may also include supplemental information from the Department. The bureau or office report will include the steps taken in the previous twelve-month period to monitor and improve the security of the IT system. Specifically, it may include a discussion of the security measures in place; any tests that were performed and the results of those tests (e.g., NESSUS scans, password cracking, vulnerability testing); and any improvements to IT security, including new hardware or software and training developments. Supplemental information from the Department may include a description of IT security oversight activities and any testing conducted by the Department on the bureau or office's IT system including, for example, the SANS/FBI Top 20 vulnerabilities testing. In addition, the Inspector General has informed the Office of the Chief Information Officer that it intends to pursue independent testing or auditing of various IT systems, and of its willingness to make available the results of such testing to further inform the Court.

Dated: August 27, 2003

[13] The bureaus or agencies that will be on this reporting schedule are MMS, BLM, NBC and OIG. Once approval for reconnection is obtained for OST, OHA, SOL and the trust portion of BIA, those agencies will be integrated into the reporting schedule. The first report would be filed approximately six months after the Court rules on the monitoring plan, and may be filed as part of Interior's Quarterly Reports to the Court. Thus, for example, if the monitoring plan were implemented next month, BLM and MMS would report in the first quarterly filing in 2004, followed by BIA and OST in the second quarter, OHA and NBC in the third quarter, and SOL and OIG in the fourth quarter.

If the Court wishes to verify the present security status of the Reconnected Systems, it can review the SANS/FBI Top 20 vulnerability scans performed on these systems since January 2003. Additionally, the Special Master and his experts have the results of other testing done on these systems.

Respectfully submitted,

ROBERT D. McCALLUM, JR.
Associate Attorney General
PETER D. KEISLER
Assistant Attorney General
STUART E. SCHIFFER
Deputy Assistant Attorney General
J. CHRISTOPHER KOHN
Director

SANDRA P. SPOONER
D.C. Bar No. 261495
Deputy Director
JOHN T. STEMPLEWICZ
Senior Trial Counsel
GLENN D. GILLETT
JOHN WARSHAWSKY
D.C. Bar No. 417170
GINO D. VISSICCHIO
Trial Attorneys
Commercial Litigation Branch
Civil Division
P.O. Box 875
Ben Franklin Station
Washington, D.C. 20044-0875
Telephone: (202) 514-7194
Facsimile: (202) 514-9163

C. Common Testing Tools

C.1. File Integrity Checkers

Tool	Capabilities	Website	Linux	Win32	Cost
Aide	Unix and Linux	http://www.cs.tut.fi/~rammer/aide.html	✓		Free
Description	*AIDE (Advanced Intrusion Detection Environment) is a free replacement for Tripwire. It does file integrity checking and supports a number a large number of Unix and Linux platforms.*				
LANGuard	Windows 2000/NT	http://www.gfi.com/languard/		✓	Free
Description	*LANguard File Integrity Checker is a utility that provides intrusion detection by checking whether files have been changed, added or deleted on a Windows 2000/NT system.*				
Tripwire	Windows, Unix, Linux, and Routers	http://www.tripwiresecurity.com/	✓	✓	Free
Description	*Tripwire monitors file changes, verifies integrity, and notifies the administrator of any violations of data on network hosts.*				

C.2. Network Sniffers

Tool	Capabilities	Website	Linux	Win32	Cost
Dsniff	Unix sniffer	http://www.monkey.org/~dugsong/dsniff/	✓		Free
Description	*Dsniff is a collection of tools for network auditing and penetration testing. Dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, and webspy passively monitor a network for interesting data (passwords, e-mail, files, etc.). Arpspoof, dnsspoof, and macof facilitate the interception of network traffic normally unavailable to an attacker (e.g, due to layer-2 switching). Sshmitm and webmitm implement active monkey-in-the-middle attacks against redirected SSH and HTTPS sessions by exploiting weak bindings in ad-hoc PKIs.*				
Ethereal	Unix/Windows sniffer with GUI	http://www.ethereal.com/	✓	✓	Free
Description	*Ethereal is a free network protocol analyzer for Unix and Windows. It allows users to examine data from a live network or from a capture file on disk. It can interactively browse the capture data, viewing summary and detail information for each packet. Ethereal has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session.*				
Sniffit	Unix sniffer	http://reptile.rug.ac.be/~coder/sniffit/sniffit.html http://www.symbolic.it/Prodotti/sniffit.html (Windows)	✓	✓	Free
Description	*A freeware general-purpose sniffer for various versions of Linux, Unix, and Windows.*				
Snort	Unix sniffer/IDS	http://www.snort.org	✓	✓	Free
Description	*A freeware lightweight IDS and general-purpose sniffer for various versions of Linux, Unix and Windows.*				
TCPDump	Unix sniffer	http://www-nrg.ee.lbl.gov/	✓		Free
Description	*A freeware general-purpose sniffer for various versions of Linux and Unix.*				

EXHIBIT 1
Defs' Submissions Regarding
Reconnection of Computer Systems

C.3. Password Crackers

Tool	Capabilities	Website	Linux	Win32	Cost
Crack 5	Unix password cracker	http://www.sun.rhbnc.ac.uk/~phac107/	✓		Free
Description	*Crack is a password guessing program that is designed to quickly locate insecurities in Unix (or other) password files by scanning the contents of a password file, looking for users who have misguidedly chosen a weak login password.*				
IMP 2.0	Novell Netware password cracker	http://www.wastelands.gen.nz		✓	Free
Description	Imp is a NetWare password cracking utility with a GUI (Win95/NT). It loads account information directly from NDS or Bindery files and allows the user to attempt to compromise the account passwords with various attack methods.				
John the Ripper	Windows and Unix password cracker	http://www.openwall.com/john/	✓	✓	Free
Description	*John the Ripper is a fast password cracker, currently available for many flavors of Unix, DOS, Win32, and BeOS. Its primary purpose is to detect weak Unix passwords, but a number of other hash types are supported as well.*				
L0pht	Windows password cracker	http://www.securitysoftwaretech.com/		✓	$
Description	*A password cracking utility for Windows NT, 2000 and XP.*				
Nwpcrack	Novell Netware password cracker	http://www.nmrc.org/files/		✓	Free
Description	*A password cracking utility for Novell Netware.*				

C.4. Privilege Escalation and Back Door Tools

Tool	Capabilities	Website	Linux	Win32	Cost
Elitewrap	Trojan delivery	http://www.megasecurity.org/		✓	Free
Description	*EliteWrap is an EXE wrapper, used to pack files into an archive executable that can extract and execute them in specified ways when the packfile is run.*				
Getadmin	Windows NT privilege escalation	http://www.nmrc.org/files/		✓	Free
Description	*Allows a local user to escalate their privileges on an unpatched NT host to Administrator.*				
Hunt	TCP session hijacking	http://lin.fsid.cvut.cz/~kra/index.html	✓		Free
Description	*HUNT is a tool for exploiting well-known weaknesses in the TCP/IP protocol suite.*				
Invisible Keystroke Logger	Keystroke logger	http://www.amecisco.com/iksnt.htm		✓	$

Tool	Capabilities	Website	Linux	Win32	Cost
Description	*A stealth keyboard logger that can capture even NT's "trusted path" (e.g. the alt-ctrl-del logon).*				
Netcat	Back door Port redirector	http://www.atstake.com/research/tools	✓	✓	Free
Description	*A simple utility which reads and writes data across network connections, using TCP or UDP protocols. It is designed to be a reliable "back-end" tool that can be used directly or easily driven by other programs and scripts.*				
Pwdump2	Windows NT/2000 password collector	http://www.webspan.net/~tas/pwdump2		✓	Free
Description	*Pwdump2 dumps the password hashes from the NT/2K/XP SAM database, whether or not SYSKEY is enabled on the system.*				
Virtual Network Computing (VNC)	Remote control tool	http://www.uk.research.att.com/vnc/	✓	✓	Free
Description	*VNC allows remote access to most types of hosts including most flavors of Linux, Unix and Windows.*				

C.5. Scanning and Enumeration Tools

Tool	Capabilities	Website	Linux	Win32	Cost
DUMPSec	Windows enumeration tool	http://www.systemtools.com		✓	Free
Description	*DumpSec is a security auditing program for Microsoft Windows. It dumps the permissions (DACLs) and audit settings (SACLs) for the file system, registry, printers and shares in a concise, readable listbox format, so that holes in system security are readily apparent. DumpSec also dumps user, group, and replication information.*				
Firewalk	Firewall filter rule mapper	http://www.packetfactory.net/firewalk/	✓		Free
Description	*Firewalking is a technique that employs traceroute-like techniques to analyze IP packet responses to determine gateway ACL filters and map networks. Firewalk the tool employs the technique to determine the filter rules in place on a packet forwarding device.*				
Nmap	Port scanner OS detection	http://www.insecure.org/nmap/	✓	✓	Free
Description	*Nmap ("Network Mapper") is an open source utility for network exploration or security auditing. It was designed to rapidly scan large networks, although it also works against single hosts. Nmap uses raw IP packets to determine what hosts are available on the network, what services (ports) they are offering, what operating system (and version) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.*				
Solarwinds	Network enumeration	http://www.solarwinds.net/		✓	$
Description	*A collection of network and management and discovery tools.*				

SuperScan	Port scanner, OS detection, and Banner enumeration	http://www.foundstone.com/		✓	Free
Description	*A GUI network mapper. It will rapidly scan large networks to determine what hosts are available on the network, was services they are offering, the version of these services and the type and version of the operating system. Will also perform reverse DNS lookup.*				

C.6. Vulnerability Scanning Tools

Tool	Capabilities	Website	Linux	Win32	Cost
CyberCop Scanner	Vulnerability scanner	http://www.pgp.com/products/	✓	✓	$
Description	*CyberCop Scanner is a network-based vulnerability-scanning tool that identifies security holes on network hosts.*				
ISS Internet Scanner	Vulnerability scanner	http://www.iss.net/		✓	$
Description	*ISS Internet Scanner is a network-based vulnerability-scanning tool that identifies security holes on network hosts.*				
Nessus	Vulnerability scanner	http://www.nessus.org/	✓	✓ (client only)	Free
Description	*A freeware network-based vulnerability-scanning tool that identifies security holes on network hosts.*				
SAINT	Vulnerability scanner	http://www.wwdsi.com/saint/	✓		$
Description	*SAINT is an updated and enhanced version of SATAN, is designed to assess the security of computer networks.*				
SARA	Vulnerability scanner	http://www-arc.com/sara/	✓		Free
Description	*Sara is a freeware network-based vulnerability-scanning tool that identifies security holes on network hosts.*				
SATAN	Vulnerability scanner	http://www.fish.com/satan/	✓		Free
Description	SATAN is a tool to help system administrators. It recognizes several common networking-related security problems, and reports the problems without actually exploiting them.				

C.7. War Dialing Tools

Tool	Capabilities	Website	Linux	Win32	Cost
PhoneSweep	War Dialer	http://www.sandstorm.net/		✓	$
Description	A commercial war-dialing program that supports multiple modems and attempts automated penetration.				
Telesweep	War Dialer	http://www.securelogix.com/telesweepsecure/		✓	$
Description	A commercial war dialing application that supports multiple modems and attempts to automated penetration.				
THC	War Dialer	http://packetstorm.decepticons.org/wardialers/		✓	Free
Description	Freeware DOS based war dialing program.				
ToneLoc	War Dialer	http://www.hackersclub.com/km/files/		✓	Free
Description	Freeware DOS based war dialing program.				

SANS INSTITUTE SANS//FBI TOP 20 LIST

The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts' Consensus

Version 3.23 May 29, 2003 Copyright © 2001-2003, The SANS Institute
Questions / comments may be directed to top20@sans.org.
www.fbi.gov www.nipc.gov www.sans.org

-----Jump To Index of Top 20 Threats -----

Introduction

The majority of the successful attacks on operating systems come from only a few software vulnerabilities. This can be attributed to the fact that attackers are opportunistic, take the easiest and most convenient route, and exploit the best-known flaws with the most effective and widely available attack tools. They count on organizations not fixing the problems, and they often attack indiscriminately, scanning the Internet for any vulnerable systems. System compromises in the Solar Sunrise Pentagon hacking incident, for example, and the easy and rapid spread of the Code Red and NIMDA worms can be traced to exploitation of unpatched vulnerabilities.

Two years ago, the SANS Institute and the National Infrastructure Protection Center (NIPC) released a document summarizing the Ten Most Critical Internet Security Vulnerabilities. Thousands of organizations used that list, and the expanded Top Twenty, which followed a year later, to prioritize their efforts so they could close the most dangerous holes first. The vulnerabilities that led to all three examples above - the Solar Sunrise Pentagon incident, and the Code Red and NIMDA worms - are on that list.

This updated SANS/FBI Top Twenty is actually two Top Ten lists: the ten most commonly exploited vulnerable services in Windows, and the ten most commonly exploited vulnerable services in Unix. Although there are thousands of security incidents each year affecting these operating systems, the overwhelming majority of successful attacks target one or more of these twenty services.

While experienced security administrators will find the Top Twenty to be a valuable resource in their arsenal, the list is especially intended for those organizations that lack the resources to train, or those without technically-advanced security administrators. The individuals with responsibility networks in those organizations often report that they have not corrected many of these flaws because they simply do not know which vulnerabilities are most dangerous, they are too busy to correct them all, or they do not know how to correct them safely. Traditionally, auditors and security managers have used vulnerability scanners to search for five hundred or a thousand or even two thousand very specific vulnerabilities, blunting the

Printer Friendly Version (PDF) >>

Related Resources

- US/UK/CA Top 20 Press Release
- Tools that Test for the Top Twenty (Updated June 18, 03)
- Testing for the Top 20
- Staying Current: Critical New Vulnerabilities (e-mail every Monday, free)
- Monitoring All New Vulnerabilities (e-mail every Thursday, free)
- GISRA Scanning Requirements and NASA Case Study
- Top 20 List 10/01 | Top 10 List 7/00
- Air Force CIO John Gilligan's remarks at 2001 Top 20 Announcement

Learn how to improve your system security

- London, U.K. 2003-06-23
- Dallas, TX 2003-06-26
- Washington, DC 2003-07-14
- Washington, DC 2003-07-21
- Tysons Corner, VA 2003-07-24
- Austin, TX 2003-07-26
- Melbourne, AUS 2003-07-28
- Ottawa, ON 2003-08-11
- Denver, CO 2003-08-14
- Virginia Beach, VA 2003-08-24
- Madrid, ES 2003-09-08
- Boston, MA 2003-09-15
- Los Angeles, CA 2003-09-29
- New York, NY 2003-10-09
- Raleigh, NC 2003-10-13
- Amsterdam, NL 2003-10-27
- Online Training
- Instructor Led Online Training
- Local Mentor Program

Checklists

- SQL Server 2000 Security Guidelines
- SCORE: Web Applications

Top 20 List Version 3 Update Log

v3.23 - 5/29/03
- Complete Update To Section W.3

v3.22 - 3/3/03
- Sections U8.1 & U8.3

v3.21 - 10/29/02
- Sections W9.1 & W9.3 added Windows ME
- Section U4.1/U4.5 - General Edits

EXHIBIT 2
Defs' Submissions Regarding
Reconnection of Computer Systems

focus administrators need to ensure that all systems are protected against the most common attacks. When a system administrator receives a report showing thousands of vulnerabilities across hundreds of machines, he is often paralyzed.

The Top Twenty is a prioritized list of vulnerabilities that require immediate remediation. The list is sorted by service because in many cases a single remedy -- disabling the service, upgrading to the most recent version, applying a cumulative patch -- can quickly solve dozens of specific software flaws, which might show up on a scanner. This list is designed to help alleviate that problem by combining the knowledge of dozens of leading security experts. They come from the most security-conscious federal agencies, the leading security software vendors and consulting firms, the top university-based security programs, and CERT/CC and the SANS Institute. A list of participants may be found at the end of this document.

v3.2 - 10/17/02
- Section W3 - Cumulative patch for SQL Server
- Sections WS, U1, U2, U4, U5, U8, U9 - CVE/CAN listings
- Section U9.5 - General Edits
- Section U4.1/U4.5 - General Edits

v3.1 - 10/07/02
- Section W3 - Cumulative patch for SQL Server

v.3.0 - 10/01/02
- New Version Posted

Translations

- Italian

The SANS/FBI Top Twenty is a living document. It includes step-by-step instructions and pointers to additional information useful for correcting the security flaws. We will update the list and the instructions as more critical threats and more current or convenient methods are identified, and we welcome your input along the way. This is a community consensus document -- your experience in fighting attackers and in eliminating the vulnerabilities can help others who come after you. Please send suggestions via e-mail to info@sans.org with the subject "Top Twenty Comments."

Notes For Readers:

CVE Numbers

You'll find references to CVE (Common Vulnerabilities and Exposures) numbers accompanying each vulnerability. You may also see CAN numbers. CAN numbers are candidates for CVE entries that have not yet been fully verified. For more data on the award-winning CVE project, see http://cve.mitre.org.

The CVE and CAN numbers reflect the top priority vulnerabilities that should be checked for each item. Each CVE vulnerability reference is linked to the associated vulnerability entry in the National Institute of Standards and Technology's ICAT vulnerability indexing service (http://icat.nist.gov). ICAT provides a short description of each vulnerability, a list of the characteristics of each vulnerability (e.g. associated attack range and damage potential), a list of the vulnerable software names and version numbers, and links to vulnerability advisory and patch information.

Ports to Block at the Firewall

At the end of the document, you'll find an extra section offering a list of the ports used by commonly probed and attacked services. By blocking traffic to these ports at the firewall or other network perimeter protection devices, you add an extra layer of defense that helps protect you from configuration mistakes. Note, however, that using a firewall to block network traffic directed to a port does not protect the port from disgruntled co-workers who are already inside your perimeter, or from hackers who may have penetrated your perimeter using other means.

Back to Top ^

Top Vulnerabilities to Windows Systems

- W1 Internet Information Services (IIS)
- W2 Microsoft Data Access Components (MDAC) -- Remote Data Services
- W3 Microsoft SQL Server
- W4 NETBIOS -- Unprotected Windows Networking Shares
- W5 Anonymous Logon -- Null Sessions
- W6 LAN Manager Authentication -- Weak LM Hashing
- W7 General Windows Authentication -- Accounts with No Passwords or Weak Passwords

- W8 Internet Explorer
- W9 Remote Registry Access
- W10 Windows Scripting Host

Top Vulnerabilities to Unix Systems

- U1 Remote Procedure Calls (RPC)
- U2 Apache Web Server
- U3 Secure Shell (SSH)
- U4 Simple Network Management Protocol (SNMP)
- U5 File Transfer Protocol (FTP)
- U6 R-Services -- Trust Relationships
- U7 Line Printer Daemon (LPD)
- U8 Sendmail
- U9 BIND/DNS
- U10 General Unix Authentication -- Accounts with No Passwords or Weak Passwords

Back to Top ^

Top Vulnerabilities to Windows Systems (W)

W1 Internet Information Services (IIS)

W1.1 Description

IIS is prone to vulnerabilities in three major classes: failure to handle unanticipated requests, buffer overflows, and sample applications. Each will be addressed briefly here.

1. *Failure to Handle Unanticipated Requests.* Many IIS vulnerabilities involve a failure to handle improperly (or just deviously) formed HTTP requests. A well-known example is the Unicode directory traversal vulnerability, which was exploited by the Code Blue worm. By crafting a request to exploit one of these vulnerabilities, a remote attacker may:

    - View the source code of scripted applications.
    - View files outside of the Web document root.
    - View files the Web server has been instructed not to serve.
    - Execute arbitrary commands on the server (resulting in, for example, deletion of critical files or installation of a backdoor).

2. *Buffer Overflows.* Many ISAPI extensions (including the ASP, HTR, IDQ, PRINTER, and SSI extensions) are vulnerable to buffer overflows. A well-known example is the .idq ISAPI extension vulnerability, which was exploited by the Code Red and Code Red II worms. A carefully crafted request from a remote attacker may result in:

    - Denial of service.
    - Execution of arbitrary code and/or commands in the Web server's user context (e.g., as the IUSR_servername or IWAM_servername user).

3. *Sample Applications.* Sample applications are generally designed to demonstrate the functionality of a server environment, not to withstand attacks, and are not intended to serve as production applications. Combined with the facts that their default location is readily known and their source code is readily available for scrutiny, this makes them prime exploit targets. The consequences of such exploits can be severe; for example:

    - A sample application, newdsn.exe, allowed the remote attacker to create or overwrite arbitrary files on the server.
    - A number of such applications allow remote viewing of arbitrary files, which may be used to gather information such as database userids and passwords.
    - An iisadmin application, ism.dll, allows remote access to sensitive server information including the Administrator's password.

W1.2 Operating Systems Affected

CERTIFICATE OF SERVICE

I declare under penalty of perjury that, on August 27, 2003 I served the foregoing *Interior Defendants' Submission Pursuant to the July 28, 2003 Preliminary Injunction Regarding Reconnection of Computer Systems* by facsimile in accordance with their written request of October 31, 2001 upon:

Keith Harper, Esq.
Native American Rights Fund
1712 N Street, N.W.
Washington, D.C. 20036-2976
(202) 822-0068

Dennis M Gingold, Esq.
Mark Kester Brown, Esq.
607 - 14th Street, NW, Box 6
Washington, D.C. 20005
(202) 318-2372

Per the Court's Order of April 17, 2003,
by facsimile and by U.S. Mail upon:

Earl Old Person *(Pro se)*
Blackfeet Tribe
P.O. Box 850
Browning, MT 59417
(406) 338-7530

By U.S. Mail upon:

Elliott Levitas, Esq
1100 Peachtree Street, Suite 2800
Atlanta, GA 30309-4530

K.P. Kingston
Kevin P. Kingston