

Tools and Services That Find the Top 20 Vulnerabilities (v5) On Your Systems And Networks*

Updated June 10, 2005

Services You Can Use To Scan Your Systems Without Installing New Software

Lockdown Networks:

Lockdown Networks continues to support the SANS Institute with the recent release of Lockdown v3.0. Lockdown Vulnerability Management Solution is updated with the latest SANS Top-20 list. Integrated policy enforcement provides detailed SANS Top-20 reporting on distributed networks. Lockdown is the pioneer in appliance-based vulnerability management and policy enforcement providing the most scalable enterprise solution. For more information and a Free SANS Top-20 Audit, visit www.lockdownnetworks.com

Qualys:

In support of the SANS Institute initiative, Qualys™, Inc., the leader in Managed Vulnerability Assessment, is offering a free network scan designed specifically to help companies detect and eliminate the 20 critical vulnerabilities announced today by SANS, the FBI and FedCIRC. The free, Web-based scan, available immediately at <http://sans20.qualys.com>, will enable companies to identify and remedy these threats on any IP address within their network. The free scan leverages QualysGuard's fully automated Web platform, with its proprietary Inference-Based Scanning Engine, to ensure accuracy and speed of scanning. For more information: Email support@qualys.com / Web <https://sans20.qualys.com>

SAINT Corporation:

SAINT Corporation, a leader in the network security field, includes updated references to the SANS Top 20 Critical Vulnerabilities list in each of its vulnerability assessment products. The SAINT scanning engine includes a SANS Top 20 scan policy, enabling timely detection of the vulnerabilities on the list. The SAINTwriter reporting engine references SANS Top 20 information to assist IT staff in prioritizing remediation efforts. SAINT Corporation also offers the WebSAINT online scanning service and SAINTbox scanning appliance, providing easy-to-use alternatives for detecting the Top 20 vulnerabilities. www.saintcorporation.com

nCircle:

nCircle fully supports the SANS Institute's effort to help organizations eliminate the most common vulnerabilities and exposures. The vulnerability conditions for which IP360 checks are mapped to the SANS Top 20 categories, allowing customers to easily filter results to produce clear visibility into their SANS Top 20 exposure. Each applicable vulnerability condition references the SANS category and provides a link directly to the Top 20 list. nCircle's unique profiling technology produces the most accurate results, facilitating the most effective remediation efforts. For more information, please visit www.ncircle.com or email sales@ncircle.com.

StillSecure VAM™:

StillSecure VAM™ is a vulnerability management platform that identifies, manages, and repairs network security vulnerabilities.

VAM manages the vulnerability remediation process from end-to-end, allowing you to quickly and systematically fix the vulnerabilities that expose you to attack. Updated hourly with the most current vulnerability signatures, VAM scans for vulnerabilities using scheduled and on-demand scans. The vulnerabilities found during scans are managed by VAM's exclusive Vulnerability Repair Workflow™. VAM tracks all scanning and remediation activities and delivers a range of reports for auditors, managers, and IT staff members.

Designed for both large-scale enterprises and mid-size organizations, VAM can be deployed two ways:

- A turnkey vulnerability management system
- An enterprise-integrated vulnerability management platform

www.stillsecure.com

SquareTrade:

"SquareTrade's security scanning and reporting service is extremely valuable to my business. It helped uncover security vulnerabilities I wasn't aware of and that saved me both time and money. I was able to get the detailed reporting I needed to identify and resolve my TCP/IP vulnerability. Thank you SquareTrade!"

Steven Huang, dvdsupply.com

If you would like to contact Steven in regards to his testimonial, you can email him at contact@dvd-supply.com.

As you may know, a few months back we updated our scanner technology to reflect the most recently published SANS top 20 vulnerabilities. Looking to get through the process of getting on the list for "Tools that Test for the Top 20"

The Square Trade Security Seal uncovered CGI vulnerabilities within our site. We were able to quickly address these issues with the helpful solutions Square Trade provided.

"We wanted a secure site that customers could feel confident buying from. With the Square Trade Seal, our site is effective, making us a top contender in our Google and Overture campaigns."

- Timothy Robitaille, www.colorprintdirect.com

www.squaretrade.com

ScanAlert

ScanAlert certifies that web sites pass the SANS Top 20 Internet Security Vulnerabilities test through its HACKER SAFE® web site security trustmark program. Over 65,000 web sites worldwide, including many of the world's largest ecommerce sites, use HACKER SAFE certification to build the trust that builds their business.

ScanAlert also performs accredited security audits meeting the requirements of the Payment Card Industry (PCI) Data Security Standard, as well as Visa' CISP/AIS and MasterCard's SDP security standards. ScanAlert's easy-to-use vulnerability management portal provides in-depth audit reports, complete remediation information and full technical support from CISSP certified security specialists. More information is available by contacting sales@scanalert.com or on the web at www.scanalert.com

Tenable Network Security

Tenable offers many ways to measure and manage SANS Top 20 vulnerabilities. As the operators of the Nessus (<http://www.nessus.org>) project, Tenable offers subscriptions for the latest vulnerability checks, as well as the NeWT vulnerability scanner for Windows platforms. For continuous monitoring, the NeVO vulnerability monitor can sniff network traffic 24x7 and discover new hosts, new vulnerabilities and even compromises. For enterprise networks, Tenable offers the Lightning Console for scheduled scanning, remediation workflow, IDS event correlation and compliance reporting. For more information, please visit <http://www.tenablesecurity.com>

Xentinel Digital Security

Xentinel Digital Security is a leader in remote security assessment and vulnerability scanning software development, offering its HACKER FREE™ Certification to companies worldwide. A large number of institutions benefit from Xentinel to help detect, analyze, resolve, and monitor vulnerabilities and compliance demands.

HACKER FREE™ Certification is a daily remote vulnerability scanning solution which requires no installation, management, or software updates. It tests websites for thousands of vulnerabilities including the SANS/FBI Top 20, and requirements of the Payment Card Industry (PCI) Data Security Standard. Xentinel vulnerability scans are non-invasive and 100% safe for servers. The US Computer Emergency Readiness Team (CERT) certified that websites being remotely scanned for known vulnerabilities, like those who earn the HACKER FREE™ Certification, will prevent 99.9 percent of hacker intrusions. For more information please contact sales@xentinelsecurity.com or visit them on the web at www.xentinelsecurity.com or www.sanstop20.com

* Updated lists of scanners promising to test the SANS/FBI Top 20, and test results demonstrating that they test accurately, will be posted in the "Related Resources" box at www.sans.org/top20/