Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Distributed Scan Model for Enterprise-Wide Network Vulnerability Assessment

Conducting an Enterprise-wide Vulnerability Assessment (VA) on a regular basis, as required risk management, is an extremely time-consuming task for security professionals. Enterprise networks are usually widely distributed, located in different places, towns and even counties. A structure of the network is very complex and is separated into different types of zones, sometimes with highly restricted physical access. The average number of hosts in a network is sometimes estimated at thousands or tens of thousands. Secur...

Copyright SANS Institute
Author Retains Full Rights

AD

Distributed scan model for Enterprise-Wide Network Vulnerability Assessment.

Introduction.

Conducting an Enterprise-wide Vulnerability Assessment (VA) on a regular basis, as required risk management, is extremely time-consuming task for security professionals. Enterprise networks are usually widely distributed, located in different places, towns and even counties. A structure of the network is very complex and is separated to different type of zone, sometimes with highly restricted physical access. Average amount of hosts in network is estimated as thousands or tens thousands. Security administrators cannot accommodate a growing amount of requests for network assessment. They are looking for new ideas, news approaches and news tools for Enterprise Vulnerability Assessment.

Vulnerability assessment technology.

To the time of this writing some vendors have separated a network-based vulnerability assessment scanners in to a three generations. ([3], [4])

First generation scanners.

First generation vulnerability assessment scanners were created as set of hacker's tools with ability to create simple plain-text report. Set of scripts or c-code exploits were converted in to a program that collected results of each testing step to a final report. These scripts or programs were executed of a single machine and could scan either local machine or a numbers of remote hosts. However, updates were infrequent and required manual intervention. Generated reports were text or html based, contained extensive amount of information about each host and found vulnerability, and suggested ways how to fix a problem.

Second-generation scanners.

Second-generation vulnerability assessment scanners are characterized by modular structure that makes possible more frequent automated updates, improved Graphical User Interface (GUI) or web-enabled management and reporting console. Based on the assessment task, scanners have subdivided to network scanners, host-based scanners, database scanners, web-scanners and wardialers. ([1], [2], [6], [7]) Wide range of predefined reporting templates allows create and customize final report to highlight specific aspects of tested network. Integrated knowledge base adds into report significant amount of step-by-step instruction how to eliminate findings. Results of each testing session are collected in a database or in a similar structure that gives ability to accumulate information on a period of time, determine a way of improvement and answer the immemorial question: "are we getting better or worst". Nonetheless second-generation vulnerability assessment scanners still cannot accommodate requirements of enterprise systems management and perform even semi-real-time information gathering.
Great work by was done by 'Talisker' to collect, assort and characterize most of second-generation of scanners into the table [8]:

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Network Vulnerability Scanners	Host Vulnerability Scanners	Wardialers	Database Vulnerability Scanners	On Line Vulnerability Scanners
Bullet	Appscan	ModemScan	Braintree Database	ActiveX Check
bv-control for Internet Security	bv-Control for Windows 2000	PhoneSweep	Cerberus' Internet Scanner	Critical Watch
Cisco Secure Scanner	bv-control for Microsoft Exchange	PocketDial	Cyrano	CyberCop ASaP
CyberCop CASL	bv-Control for NetWare	TBA	CyberCop Scanner	Desktop Audit
CyberCop Scanner	bv-Control for NDS	TeleSweep	DbDetective	Elephant Toolbox
CyberTrace CT Probe	bv-control for Microsoft Exchange	Telephony Scanner	ISS Database Scanner	E-Soft
VIGILANTe SecureScan NX	Centrax	THC-PBX	ESM for Oracle	Hacker Whacker
Gabriel SATAN Detector	Cerberus Internet Scanner	THC-Scan	E-Trust Policy Compliance	ISS Online Scanner
Hackershield	CyberCop Scanner	Toneloc	SQLdict	Marcs Online
Hailstorm	Cybersight	Xiscan		OnLine Trojan
ISS Internet Scanner	Enterprise Security Manager			Pro CheckNet
Nessus	eTrust Policy Compliance			Privacy Analysis
NetRecon	ForixNT			QualysGuard
Net Sonar	ISS System Scanner			QUICKinspector
Nmap	Kane Security Analyst			Secure Design
NmapNT	NetPulse 2000			SecureMe
Retina	NOSadmin			SecureScan
Retriever & Expert	Security CeNTer			Shields Up
SAINT	Security Expressions			Sygate Scan
SARA	STAT			Symantec Security Check
ShadowScan	TARA			Thresher
Solarwinds	VigilEnt			
Swarm	WebTrends			
twwwscan				
Whisker				

Third generation distributed network scanners.

Third generation distributed network scanners are most approached to the purposes and tasks of Enterprise Vulnerability Assessment. A distributed architecture by locating remote scanning agents in a distant networks meet the needs of security administrators to conduct a vulnerability assessment of multiple geographically dispersed networks from one single location. Automated

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

process of delivery updated for scanning agents' policies allows simultaneously modify settings of all scanning engine over enterprise. Centralized management provides ability to schedule any testing activity out of working hours and minimize a network performance impact. The collecting of all scanning results from all locations at the central database dramatically reduces reporting time and creates a real-time snapshot of network security posture.

Advantages of distributed scanner model ([3]):

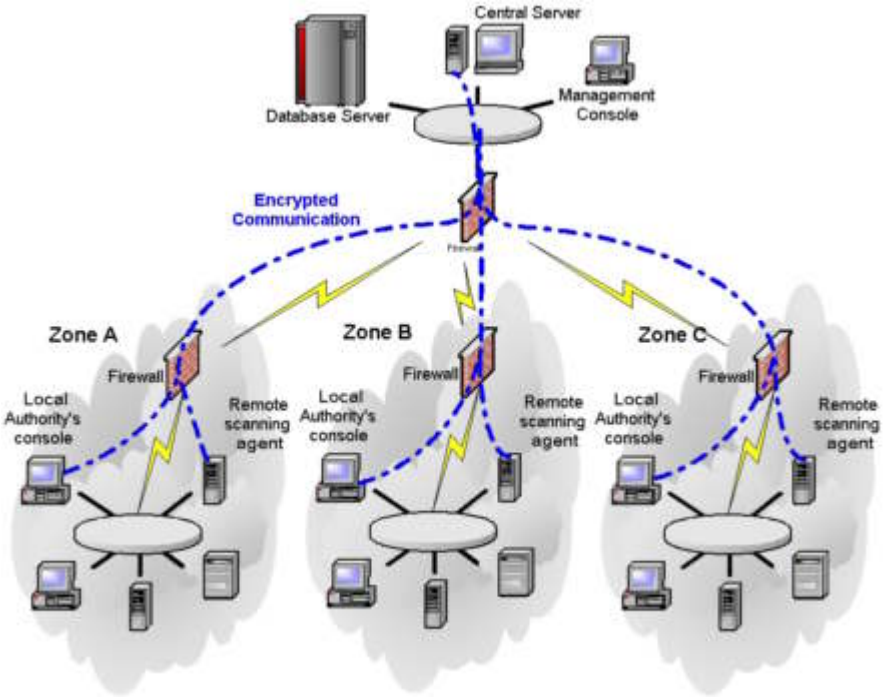
Centralized management	All activities on multiply networks are conducted and managed from a single console or from multiply consoles in case of dividing a network to localized 'zones of authority'.
Concurrent Multi-network testing	Scanning of remote subnets, subnets behind NAT, behind a firewall, a complete evaluation of firewall filtering rules.
Performance	Multiple remote networks can be tested concurrently. Performance of the low bandwidth network segment never affect remote scanning agent's efficiency.
Non-intrusiveness	All scans occur on local segments. Distributed scanning overcomes network topology specific bandwidth restrictions. Scanning traffic does not alert IDS sensors, located between separated zones. Scanning traffic does not affect scan-sensitive equipment.
Reporting	Central ODBC compliant database provides an ability to gather information from multiply networks in one location. Database approach to scans analysis allows to accumulate testing result from thousands hosts over time, track and detect any changes in network topology, improve hosts hardening process, and follow up with a fixing vulnerability. Comprehensive reporting mechanism in conjunction with flexibility of database data mining technology allows reflecting a various aspects of the network security status. Using a Common Vulnerabilities and Exposures (CVE) naming agreement for reporting. ([12])
Automation	Any process at distributed remote scanning agent can be automated, scheduled and controlled from central administration console. The scheduled processes are • Scan start/stop time, • Security policy update to execute predefined set of modules, • Add/Upgrade testing module to keep engine up-to-date, • Automatic report generation and publishing

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Confidentiality	All auxiliary communication between management console and remote agent is encrypted. (3DES – Distributed CyberCop 2.0, SSLv3 - SecureScan NX)

Architecture of Distributed Network Scanners.

The following picture illustrates a presumable architecture for enterprise-wide distributed network scanners deployment.



Enterprise network is separated to local zones. Each zone has remote scanning agent and local console. Zones are isolated from enterprise network by a firewall, probably also by screening router. Some of them may connect to enterprise backbone via low bandwidth WAN link. Central management server, management console and database server are separated from enterprise network and composed into a security management zone with restricted access. Central management server conduct all control operations, schedule scanning tasks, maintain security policy, provide access restriction, update scanning modules and deliver it to remote agent on demand or by schedule. Management console is a front-end of system and provide management functionality for central server. It also creates vulnerability assessment reports and makes available for end user. Part of this reporting functionality is delegated to Local Authority's Console to generate self-report about local zone. Enterprise VA report access policy should be carefully designed to grant necessary access to results according to level of authority. Database server provides data-redundancy and backup. It also accomplishes a task for access restrictions. All communications between elements of distributed scanning model are encrypted and signed.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Distributed scanners.

To the time of this writing information about only two commercial distributed network scanners is available. These network scanners are utilized benefits of distributed architecture

- PGP security, Distributed CyberCop Scanner 2.0
- VIGILANTe, SecureScan NX (former CYRANO, NV e-secure)

Open-source **NESSUS** scanner employs elements of distributed architecture. It consists of two parts: Nessus-server and client. All scanning tasks are initiated from console and executed on server. One console can control multiply scanning servers and form a final assessment report from server's 'knowledge base'. ([9], [10]). Nessus 'knowledge base' represents a text file which contents a scan results in proprietary format. Nessus client and server for communication use **twofish/ripemd160:3** encryption.
So, this architecture is close to a model presented below, however it is not so flexible and convenient for the task of enterprise vulnerability assessment.

Some other ideas of distributed port scanning were realized in **Remote Nmap** (**Rnmap**). ([11]). This tool allows executing *nmap* scan on remote agent and return results to 'rnmap' server. Rnmap uses RSA encryption with 1024 bit key length and Blowfish algorithm with 128 bit session keys from amkCrypto python cryptography package.

Distributed CyberCop Scanner 2.0

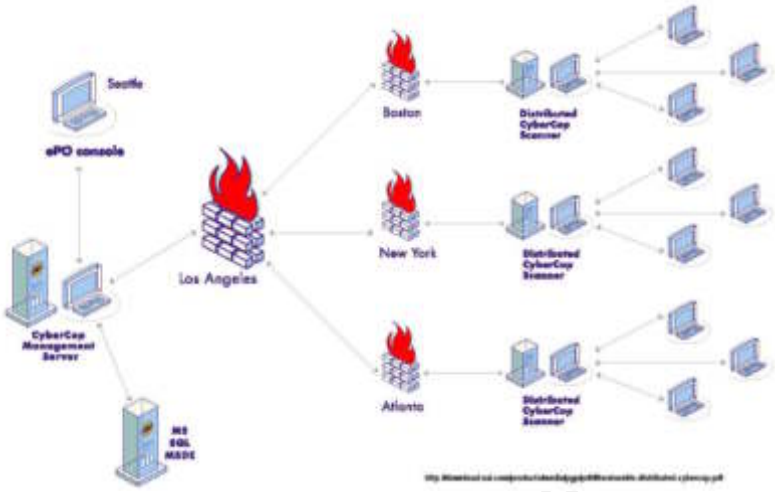
PGP security extends the use of e-Policy Orchestrator (ePO) technology from distributed antivirus protection to distributed network vulnerability assessment. Redesigned CyberCop 5.5 leverages ePO model for distributed networks and firewall scanning to meet the needs of enterprise risk management. It consists of following elements: CyberCop Management Server, ePO Management Console, Scan Repository Database server and Remote CyberCop Agent.

The key features of Distributed CyberCop Scanner 2.0 are ([4]):

- Remote Scan Management with CyberCop Agents controls multiple scans of multiple networks from one central location
- Central Scan Repository stores results and policies in a MSDE or MSSQL database.
- Reporting tool generates reports using standard database queries and Crystal Report engine.
- Multiple account administration levels allow managing access control to the scan repository.
- Scheduled Scans defines the frequency and timing to perform scans
- AutoUpdate delivers regular, automated updates to keep scanning engine current.
- The use of Common Vulnerabilities and Exposures (CVE) in reports allows search the vulnerability database for specific CVE numbers
- Custom Audit Scripting Language (CASL) Scripting Tool helps create custom scan tests for any IP device or protocol

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

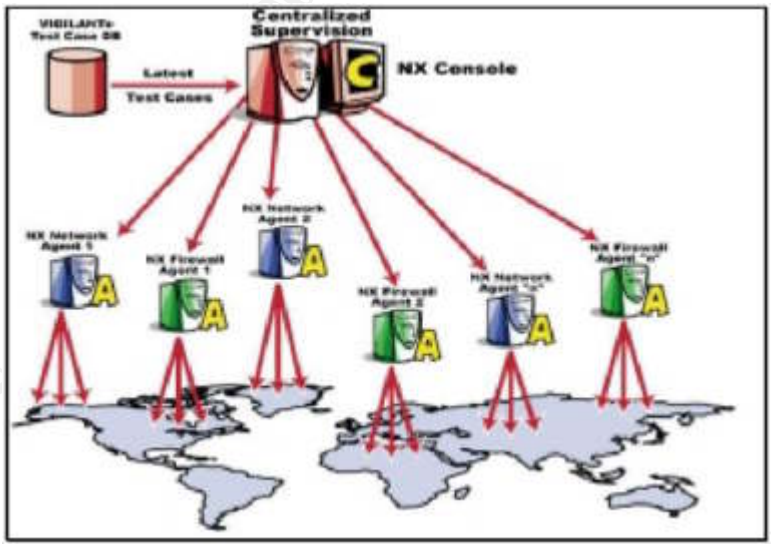
Architecture of Distributed CyberCop Scanner 2.0 ([4])



EPO Architecture uses certificate-based authentication. All trusted communication between Remote agent, Management Server and ePO console employs X.509 digital certificates ("ceptograms") with 1024-bit key length via TLS (Transport Layer Security). Certificate are issued and managed by the Net Tool PKI Server. [5]

VIGILANTe, SecureScan NX

Architecture of SecureScan NX ([3])



The Central Console is the management center for main task of vulnerability assessment: security testing and reporting. Security administrator initiates vulnerability assessment using the central console to define and submit scanning task or set of "Test Case" to the Remote Agent. Single Central Console can control any number of Remote Agents. After Remote Agent finishes

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

the task it returns the scanning results back to Central Console. Central Console stores the results in ODBC complaint database (MSDE or MSSQL) for further report generating. SecureScan NX provides wire range of predefined reporting templates and leverages CVE search for multi-vendor compatibility.
All communication between Console and Remote agent is conducted via port 9999/TCP and encrypted using SSLv3.
Based of the scanning task, submitted to Remote Host, it can perform three types of testing: Network, System and Firewall. Network scan provides the capability to make an auto-discovery of IP range and then conduct a vulnerability assessment of all hosts on a discovered network regarding the type of OS. System scan mode allows to conduct server vulnerability assessment to detect server's security problem, current OS patch level and recommend the way how to eliminate a found vulnerability. Firewall mode provides end-to-end testing of the filtering rules existing between Remote agent and Probe. Probe is a specially configured remote Agent located after firewall or router. Control communication between Console and Probe is also secured using SSLv3.
Auto-update feature of SecureScan runs automatically every time the Console is started and reminds the security administrator to check vendor's online database for new "Task case". These can be downloaded, verified and distributed to Remote Agent.

Conclusion.

Traditional approaches are not allowed anymore to perform real-time network assessment and real-time statistical risk analysis of security posture of an enterprise. New 3rd generation scanning tools implements client/server solution with a centralized console to manage remote scanning agents, making it easy to conduct scans on regular basis and quickly report vulnerabilities. Single management console coordinates all remote scanning agents to perform testing of multiply networks concurrently, collects results into ODBC-compliant database for post analysis, and creates a comprehensive reports. Database approach to vulnerability assessment allows applying a power of data mining technology for enterprise risk management and helps quickly find correlation between current network status and current threat to mitigate risk.

References:

1. SANS Institute Publications. "Roadmap to Security Tools and Services Online".
URL: http://www.sans.org/tools/tools1.htm
2. Jeff Forristal and Greg Shipley (Network Computing) [Jan 6, 2001]. Network Computing. "Feature Security Vulnerability Assessment Scanners Page 1" [January 8, 2001].
URL: http://www.nwc.com/1201/1201f1b1.html
3. VIGILANTe SecureScan NX, "Commercial Whitepaper" [September 2001]
URL: http://www.vigilante.com/securescan/nx/nx-whitepaper-10-2001.pdf
4. PGP Security, "Distributed CyberCop Scanner 2.0" [August 2001]
URL: http://download.nai.com/products/media/pgp/pdf/literature/ds-distributed-cybercop.pdf
5.. NAI web site, "Event Orchestrator". [2001]
URL: http://www.nai.com/international/uk/asp_set/solutions/activesecurity/eventorchestrator.asp
6. Internet Security Systems, Inc. "Network and Host-based Vulnerability Assessment."
URL: http://documents.iss.net/whitepapers/nva.pdf

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

7. CERN, “Computer security tools and documentation”, [April 20, 2000]
URL: http://wwwinfo.cern.ch/dis/security/general/tools/index.html
8. “Talisker”, “Network Security Tools, Vulnerability scanner”, [2000, 2001]
URL: http://www.networkintrusion.co.uk/scanners.htm
9. Nessus official web site. “Documentation”
URL: http://www.nessus.org/documentation.html
10. Sam Costello, IDG News Service, NetworkWorldFusion News,. “Developer previews next version of Nessus security tool.” [August 11, 2001]
URL: http://www.nwfusion.com/news/2001/0711nessus.html
11. Rnmap documentation., Rnmap home page
URL: http://rnmap.sourceforge.net/
12. Common Vulnerabilities and Exposures (CVE). Web site. “The Key to Information Sharing”
URL: http://cve.mitre.org/docs/docs2000/key_to_info_shar.pdf

© SANS Institute 2002, Author retains full rights.

Last Updated: May 23rd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced