Nsauditor
White Paper

NSASOFT LLC.
http://www.nsauditor.com
E-mail: info@nsauditor.com

Version 2.1 – Last updated 09/08/2005

Abstract

This paper outlines the functionality of Nsauditor software. You can also find the key features and advantages of this software product. Note that this white paper is for informational purposes only.

Contents

Introduction

Installation and Removing

Ordering

Introduction

Introduction

Nsauditor is a network security audit system designed to audit network and detect available security vulnerabilities in the network. It also provides a set of tools performing a real-time traffic and protocol analysis, showing detailed listings of all TCP and UDP endpoints on your system, including the owning process name, loaded modules, kernel objects, memory details, remote address and state of TCP connections, host dns name, country where from, network class type, service associated with connection, possible trojans associated with port and service description for monitoring. The Auditor module of Nsauditor can audit network and automatically detect security vulnerabilities, it can also identify possible security holes in your network, detect potential Trojans installed on users' workstations as well as make a variety of attack probes, such as stealth port scans, CGI attacks, SMB probes. The NetBios Auditor module is discovering network information, including NetBIOS Names, LANA, Shares, Security Policy and Information, Groups/Users. Tcp / Udp scanner is a tool which scans using all TCP header flags (syn, fin, ack, null, xmas, bogus). It also allows protocol scanning and remote OS fingerprint creation.

This document covers features that will help you:

- Become acquaint with the key features of Nsauditor
- Understand using Nsauditor.
- Understand how Nsauditor works

The key features of Nsauditor

Here are the key features of Nsauditor:

- Network monitor
- Auditor(Network Security Auditor)
- NetBIOS Auditor
- Web Proxy CGI Scanner
- MS SQL Server Auditor
- SNMP auditor
- Ms RPC Auditor

- Sun RPC Auditor
- Packet Filter
- LM/NTLM Spider (support NTLMv1 and recovering LM passwords, NTLM password recovering and NTLMv2 support will be added in the next releases)
- Intrusion Detection System based on security Event log analyzer
- Ping (ICMP, TCP, UDP)
- Trace Route
- Finger
- Whois
- DNS Lookup
- Email Validate
- Tcp, Udp tools (Client / Server, Port redirector)
- Local IP, TCP, UDP and ICMP statistics
- Local Addressing information table
- Local Net to media information table
- Process details discoverer
- Alerts when IP Address Table or Routing Table changed.
- Security event log monitor
- Abuse Address finder
- RBL (spammers realtime black list) check
- Packet Editor (IP, ICMP, TCP, UDP, NETBIOS-SSN packet decoding)
- Security Events Alerter
- Port Scanner
- Remote System OS detector and OS Fingerprint database creator
- Services Probe
- Audit Reports viewer.
- IP Address / ASN Country lookup
- IP Routing, Net Table
- Http traffic generator
- Traffic Emulator
- MAC/Vendor Lookup

The description of Nsauditor features

All tools are located in four different sections: **utils, statistics, tools, sessions**.

<u>The Sessions tab contains:</u>

Network Monitoring - Network Monitoring shows detailed listings of all TCP and UDP endpoints, including the owning process name and details, remote address and state of TCP connections, as well as the host dns name, country ,network class, appropriate service name and service description.
Auditor - Auditor is a tool for discovering network services and well known service vulnerabilities. This tool creates an audit report. The auditor consists in two main parts: TCP and UDP . To audit Ftp vulnerabilities, smtp vulnerabilities, telnet vulnerabilities, pop3 vulnerabilities, tcp services, http vulnerabilities, Net bios options, Udp services enable appropriate settings. You can use the default profile, or a user defined profile, which can be saved in the file.
Netbios Auditor - NetBios Auditor is a tool for discovering NetBios names. NetBios names are the names of the Services and Machines. NetBIOS Scanner is a powerful and a fast tool for exploring networks , scanning a network within a given range of IP addresses and listing computers which offer NetBIOS resource sharing service as well as their name tables and netbios connections.
Network Scanner - Network Scanner is a tool for scanning large networks or a single host. This tool uses raw IP packets to determine available hosts, what ports they are offering , what operating systems they are running and other important characteristics.
Web Proxy Scanner - Web proxy scanner is a tool that let you check the vulnerabilities of web servers. It is evident that CGI probes are sent against web servers. This tool provides an ability to configure the scanner to run CGI probes through that proxy or without proxy.
MsSql Auditor - This tool allows you perform an audit on a machine running MS SQL server.
SNMP Auditor - SNMP auditor is a tool that allows walk through all SNMP MIBs of your nodes and to audit SNMP community names using values stored in xml database.
MsRpc Auditor - Audit MSRPC, is a Microsoft implementation of DCE RPC. The auditor dump is a list of named pipes that are used by Windows RPC services as endpoints. The interface identifier associated with each named pipe represents the service typically accessed when a given named pipe is used.

SunRpc Auditor - Audit Sun RPC uses ONCRPC (Sun RPC) protocols to access the Portmapper daemon/service that typically runs on port 111 of UNIX or Linux machines. This tool includes a portmapper to dump where a list of all running registered daemons are shown.

Packet Filter - Packet Filter provides a real-time network packet filtering and analyzing. It filters the packet by all IP, ICMP, TCP, UDP, NETBIOS-SSN packet header fields.
LM/NTLM Spider - LM/NTLM Spider is a password audit and recovery tool. Passwords are sources of vulnerabilities in different machines. This tool allows identifying and accessing password vulnerabilities. Auditing user password is one of the most important problems for network administrator. This is to know the strength of password the users are using. Week passwords represent vulnerability points for any organization.

The Tools tab contains:

Ping - Ping is a tool that allows you verify that the specified IP address exists. This tool is used to ensure that a host you are trying to reach is accessible. Ping also can be used with the reachable host to see how long it takes to get the response back. Also you can get information about the operating system of remote host.
Trace Route - TraceRoute is a tool that traces the route (the specific gateway computers at each hop) from a client machine to the remote host by reporting all the router IP addresses between them. It also calculates and displays the duration that each hop takes. TraceRoute is a handy tool for both understanding where problems exist in the Internet network and for getting a detailed sense of the Internet itself.
Dns Lookup - DNS lookup converts IP addresses to hostnames and vice versa and obtains aliases. DNS lookup performs advanced DNS queries, such as MX or CNAME. Full list of queries are A, NS, MD, MF, CNAME, SOA, MB, MG, MR, NULL, WKS, PTR, HINFO, MINFO,MX,TXT,AXFR,MAILB,MAILA,*.
DNS Lookup supports checking if the host is in a Real-time Black list for spammers "RBL ".
Whois - This tool will lookup information on a domain, IP address, or a name. You can select a specific WhoIs Server, or you can use the 'Default' option for the default server.
Finger - Finger is a tool for discovering user information by using well known finger service. Using Finger tool makes possible to get "Abuse Address" of remote host.
For example to get the abuse address of prontomail.com you should type prontomail.com@abuse.net in the finger input section. As a result you will receive
abuse@mailcentro.com (for prontomail.com) in the finger response section.
Email Validate - The Email Validate Tool is a client utility for checking the validity of an email account. The tool supports two modes:
VRFY - checks the validity of an account using SMTP VRFY command,
EXPN - is used to find the delivery address of mail aliases also full name of the recipients.
Enumerate Computers - Enumerate computers is a tool to enumerate computers in a domain. Depends on enumeration parameters the tool can work in different ways. It can enumerate all computers, all SQL servers only, all primary domain controllers only , backup domain controllers only , primary domains only ,etc.
TCP Client Server - The Tcp Client / Sever is a useful tool for testing some services, firewalls and intrusion detection systems. This tool also can be used for debugging the program and configuring other network tools.

TCP Port Redirector - The Tcp Port Redirector is a useful tool to redirect TCP traffic from one port on the same or another machine to another. This tool is used for testing some services, firewall and intrusion detection systems. This tool also can be used for debugging programs and configuring other network tools.

UDP Client Server - The Udp Client / Sever is a useful tool for testing some udp services, as well as the firewalls and intrusion detection systems. This tool also can be used for debugging the program and configuring other network tools.

Traffic Emulator - Network TrafficEmulator generates IP/ICMP/TCP/UDP traffic to stress test servers, routers and firewalls. It is a very simple and fast program which can simulate client activity.

HTTP Traffic Generator - Http TrafficGen is a tool that generates an http traffic to the specified URL **.**

The Statistic tab contains:

IP Statistics, ICMP Statistics, TCP Statistics, UDP Statistics - This tools shows the **IP, TCP, UDP and ICMP** statistics. Analyzing this statistics allows the detection of different kinds of network treatments as well as port scanning probes and network attacks.

IP Tables - IP Tables provides a tool to retrieve an information related to the interface–to–IP address mapping table, IP routing table, IP-to-physical address mapping table. This tool shows the details about each IP address in the table. Each part of the table contains information about IP address including address, interface index, subnet mask, broadcast address, reasm size.

The Utils tab contains:

Interfaces - Interfaces is a tool for getting available network interface parameters, such as, network mask, broadcast address, broadcast enabled/disabled state, running enabled/disabled state, PPP enabled/disabled state, loopback enabled/disabled state, multicast enabled/disabled state.

Net Configuration - Net Configuration is a tool that lets you get information about the local host and network. Host information, such as, host name, domain name, DNS servers list, node type, scope ID, routing enabled/disabled state, proxy enabled/disabled state, DNS enabled/disabled state and adapter information, such as, interface name, adapter type, IP address, subnet mask, mac address, adapter name, autoconfig enabled/disabled state, wins enabled/ disabled state, etc. are available.

Process Monitoring - Process Monitoring is a tool that displays the list of processes currently running on computer and shows the program name, the unique process ID, the full path of program's executable file, the name of the file manufacturer, and the name of modules and kernel objects used by the selected process.

Report - Report contains remote host security audit information generated by "Auditor" - network security auditor module with HTML and XML output. The RTF and PDF report generation will be available in the next releases. You can convert the report to PDF format. If you have installed Adobe acrobat just right click on the report, select “Print” menu item and in the opened Printer dialog select “Adobe PDF” as a printer and set path to save the document. The report will be automatically converted to PDF format.

Ports - This tool gives the port specific information including service name, port number, protocol type, trojan name, service description.

IP/ASN Country - IP/ISN Country is a tool that lets you determine which country an IP address or autonomous system number is assigned to . This tool supports two ways of find the country; searching by IP address or autonomous system number.

MAC/Vendor Lookup - This tool allows you get information about adapter manufacturer. The only thing you need is to fill the full MAC address (ex. 00:80:48:2A:83:41) or only the first part of MAC address (ex. 00:80:48).

Program advantages

Nsauditor has all features that needs a network security auditing program. Besides these features Nsauditor has advantages that other programs have not. These advantages are:
Automatic creation of XML based format Operating System fingerprint.
Creation of Operating System fingerprint with different user specified Tcp options .

Program perspective

In perspective the product will also include the Expert Firewall Controls, Wireless networks leak detector, Parasite and Trojans or backdoor software detector, Patch Manager, Traffic Generator and Network Scene designer with scripting language for writing security audit checks. It will include an editor with syntax highlighting capabilities and a debugger. The expert firewall control will give a precise control of firewall settings.

Installation and Removing

System requirements

- Windows 2000/2003 or Windows XP.
- Internet Explorer 5.1 or higher.
- Installation of Microsoft Network Client on the local computer.
- Stopping Personal Firewall software or the Windows Internet Connection Firewall during scan. Such software can block functionality of Nsauditor.
- Administrator privileges on local computer.
- 128 MB memory.
- 30 MB of free disk space.

Installing Nsauditor

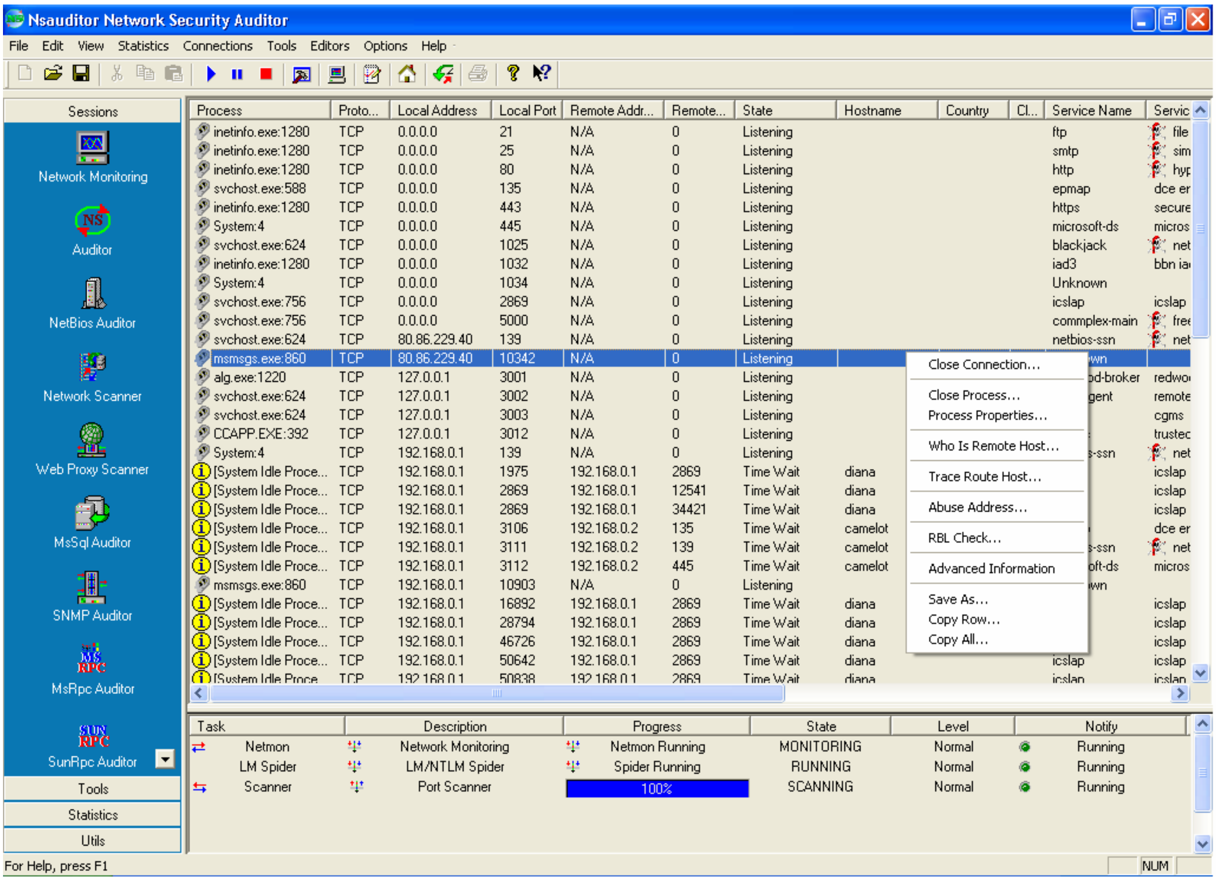
To install Nsauditor double click on Setup.exe and follow the instructions on the screen. You can also install Nsauditor from the Run dialog. Open the Run command prompt by clicking on the Windows Start button, then select Run. Browse and find “setup.exe” downloaded from http://www.nsauditor.com/downloads/setup.exe and press Ok. Afer, follow the instructions on the screen.

Uninstalling Nsauditor

To uninstall Nsauditor , click on the Windows Start button , go to Programs then go to Nsauditor and click on Uninstall Nsauditor . Follow the instructions on the screen to uninstall Nsauditor from you system.

Starting Nsauditor

Click on the Windows Start button. Then from Programs select Nsauditor and click on Nsauditor. The program will start and the following interface will appear on the screen.



Process	Proto...	Local Address	Local Port	Remote Addr...	Remote...	State	Hostname	Country	Cl...	Service Name	Servic
inetinfo.exe:1280	TCP	0.0.0.0	21	N/A	0	Listening				ftp	file
inetinfo.exe:1280	TCP	0.0.0.0	25	N/A	0	Listening				smtp	sim
inetinfo.exe:1280	TCP	0.0.0.0	80	N/A	0	Listening				http	hyp
svchost.exe:588	TCP	0.0.0.0	135	N/A	0	Listening				epmap	dce er
inetinfo.exe:1280	TCP	0.0.0.0	443	N/A	0	Listening				https	secure
System:4	TCP	0.0.0.0	445	N/A	0	Listening				microsoft-ds	micros
svchost.exe:624	TCP	0.0.0.0	1025	N/A	0	Listening				blackjack	net
inetinfo.exe:1280	TCP	0.0.0.0	1032	N/A	0	Listening				iad3	bbn ia
System:4	TCP	0.0.0.0	1034	N/A	0	Listening				Unknown	
svchost.exe:756	TCP	0.0.0.0	2869	N/A	0	Listening				icslap	icslap
svchost.exe:756	TCP	0.0.0.0	5000	N/A	0	Listening				commplex-main	free
svchost.exe:624	TCP	80.86.229.40	139	N/A	0	Listening				netbios-ssn	net
msmsgs.exe:860	TCP	80.86.229.40	10342	N/A	0	Listening				wn	
alg.exe:1220	TCP	127.0.0.1	3001	N/A	0	Listening				d-broker	redwo
svchost.exe:624	TCP	127.0.0.1	3002	N/A	0	Listening				gent	remote
svchost.exe:624	TCP	127.0.0.1	3003	N/A	0	Listening					cgms
CCAPP.EXE:392	TCP	127.0.0.1	3012	N/A	0	Listening					trustec
System:4	TCP	192.168.0.1	139	N/A	0	Listening				s-ssn	net
[System Idle Proce...	TCP	192.168.0.1	1975	192.168.0.1	2869	Time Wait	diana				icslap
[System Idle Proce...	TCP	192.168.0.1	2869	192.168.0.1	12541	Time Wait	diana				icslap
[System Idle Proce...	TCP	192.168.0.1	2869	192.168.0.1	34421	Time Wait	diana				icslap
[System Idle Proce...	TCP	192.168.0.1	3106	192.168.0.2	135	Time Wait	camelot				dce er
[System Idle Proce...	TCP	192.168.0.1	3111	192.168.0.2	139	Time Wait	camelot			s-ssn	net
[System Idle Proce...	TCP	192.168.0.1	3112	192.168.0.2	445	Time Wait	camelot			oft-ds	micros
msmsgs.exe:860	TCP	192.168.0.1	10903	N/A	0	Listening				wn	
[System Idle Proce...	TCP	192.168.0.1	16892	192.168.0.1	2869	Time Wait	diana				icslap
[System Idle Proce...	TCP	192.168.0.1	28794	192.168.0.1	2869	Time Wait	diana				icslap
[System Idle Proce...	TCP	192.168.0.1	46726	192.168.0.1	2869	Time Wait	diana				icslap
[System Idle Proce...	TCP	192.168.0.1	50642	192.168.0.1	2869	Time Wait	diana			icslap	icslap
[System Idle Proce	TCP	192.168.0.1	50838	192.168.0.1	2869	Time Wait	diana			icslap	icslap

Task	Description	Progress	State	Level	Notify
Netmon	Network Monitoring	Netmon Running	MONITORING	Normal	● Running
LM Spider	LM/NTLM Spider	Spider Running	RUNNING	Normal	● Running
Scanner	Port Scanner	100%	SCANNING	Normal	● Running

In the left side of the dialog you can find all the features. The same features can also be used from menus. The detailed description of each feature you can find in www.nsauditor.com. This document only outlines the description of each feature.

Despite the various types of tools included in Nsauditor, the system is designed for easy use. The program has a user friendly interface. It has an ability to remember the preferences of previous sessions so you do not have each time to configure the tool you are using.

Before using each tool find the appropriate help topic, by pressing F1 or selecting Help Topics from Help menu. These topics will provide the detailed description of each tool.

Ordering

Ordering Nsauditor and entering License key after installation

The downloaded version is a 15 day trial version. If you then decide to purchase Nsauditor you can just enter the License key without having to reinstall it.
You can order Nsauditor here: **http://www.nsauditor.com/order.html**
And you will receive the registration information by an e-mail during 12 hours.
After entering license key you will be entitled to

- the fully functional unrestricted version of the program
- free updates and subversions that will be available up to version 2.0.

You must license Nsauditor for the number of machines that you wish to run it on.

Prices

Here is the price list for one user and multi-user licensing:

Nsauditor Licenses	**Price**
1 User License	$37.00
5 User License	$148.00
10 User License	$259.00
25 User License	$549.00
50 User License	$925.00
100 User License	$1479.00
250 User License	$2775.00

Conclusion

Nsauditor is designed to protect your system against unauthorized access. It also provides a set of network tools useful in auditing networks and monitoring your computer’s network connections. It has two great advantages that other such kinds of programs have not including automatic creation of XML based format operating system fingerprint and creation of operating system fingerprint with different user specified tcp options. The system is designed for easy use and has a user friendly interface.

Thus Nsauditor is an important tool for everyone interested in a set of powerful and useful network tools.

Glossary of Terms

A

Application Layer: The top layer of TCP/IP stacks.

B

Broacast: A broadcast packet is always acceptable by any node of the network.

C

Client: A system that requests a service of another system.

D

DNS: DNS is a system that provides the data query service. The general purpose of DNS is the look up of IP addresses based on host names.

E

Email: A system that provides an ability to exchange messages between different computer users using network.

F

Finger: A standard service for gaining access to user information.

G

Gateway: The system that chooses the route of traffic . It uses different algorithms to find the best route.

H

Header: Header is the part of packet, which is preceding the data. Header contains source and destination addresses, etc.

Hop: This term usually is used in routing. A series of hops describes a path to a specified destination which passes through routers .

Host: A computer on the network which initiates and accepts different types of connections.

Hostname: The name that is given to a specified computer.

Host Address: A 32 bits internet address assigned to hosts using TCP/IP protocol family.

I

IP: Internet Protocol. This protocol is a network layer of TCP/IP protocol family.

M

MAC Address : A physical address of device connected to the network.

MIB: The set of parameters that SNMP management station can query and set in the SNMP agent .

N

NetBios: Network Basic Input Output System. The standard interface to networks on IBM PC .

P

Packet: A data unit sent across a network. Generally used to describe data units. of application layer.

Protocol: The description of rules that allows message exchange between different computers. The mentioned message format is described by the specified protocol.

R

RPC: Remote Procedure Call. To execute the procedure using this mechanism you should send a request to the remote system. The result will be returned to the caller. There are different implementations of RPC protocols.

Routing: The process of selecting correct hop for a packet dedicated to the specific destination address.

S

Server: A system that provides other systems with resources.

SMTP : Simple Mail Transfer Protocol. This protocol is used to transfer mails between computers.

SNMP: Simple Network Management Protocol. This protocol is used to manage nodes on an IP network.

SQL: Structured Query Language. The standard language for accessing relational databases.

Subnet mask: An IP address that shows which part of the address is the subnet number.

T

TCP: Transmission Control Protocol. Connection oriented transport layer protocol.

Trojan Hourse: A computer program which allows the creator access to the system which uses it.

U

UDP: User Datagram Protocol. Connectionless transport layer protocol.

Unauthorized access : External access to the system without any permission.

UNIX: multi-user operating system.

V

Viruses: A program which is incorporated into other programs that are shared among computer systems (i.e. a virus can be incorporated into *.exe file that is attached to an e-mail) and can damage any part of computer system.