

<http://www.nsauditor.com>

Nsasoft llc.

Network Monitoring

Network monitoring is a tool that monitors network connections and processes (applications and services) currently running on the computer. This tool shows you detailed listings of all TCP and UDP endpoints of your system including owner process name, remote address and state of TCP connections.

The **Process** column shows the name of the program, the **Protocol** column shows the protocol type, the **Local Address** column shows the local Ip address, the **Local Port** column shows the local port, used with the specified process in the local computer, the Remote Address column shows the remote Ip address, if the specified process has an established connection with a remote computer and N/A otherwise, the **Remote Port** column shows the remote computer's port used for the process that has a connection with the specified process, and 0 if there is no connection with remote computer, the **State** column shows the connection state, the **Hostname** column shows the remote host name, the **Country** column shows the country, the **Service Name** column shows the service name, the **Service Description** column shows the description of the specified service.

The screenshot displays the Nsauditor Network Security Auditor interface. The main window shows a list of network connections with columns for Process, Protocol, Local Address, Local Port, Remote Address, Remote Port, State, Hostname, Country, Service Name, and Service Description. A context menu is open over the selected row for process 'msmsgs.exe:860', showing options like 'Close Connection...', 'Close Process...', and 'Who Is Remote Host...'. Below the connection list, there is a 'Task' section with columns for Task, Description, Progress, State, Level, and Notify. The tasks listed are 'Netmon' (Network Monitoring), 'LM Spider' (LM/NTLM Spider), and 'Scanner' (Port Scanner), all in a 'Running' state.

Process	Proto...	Local Address	Local Port	Remote Addr...	Remote...	State	Hostname	Country	Cl...	Service Name	Service Description
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				complex-main	fret
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				msn	msn
alg.exe:1220	TCP	127.0.0.1	3001	N/A	0	Listening				td-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					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				net
[System Idle Proce...	TCP	192.168.0.1	3112	192.168.0.2	445	Time Wait	camelot				olt-ds
msmsgs.exe:860	TCP	192.168.0.1	10903	N/A	0	Listening				msn	micros
[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
[System Idle Proce...	TCP	192.168.0.1	50838	192.168.0.1	2869	Time Wait	diana				icslan

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

The bottom of the window contains information about tasks that are currently running. That information includes Task, Description, Progress, State, Level, Notify. You can switch from one task to another by selecting appropriate row.

Right- clicking on the window brings up a menu with the following commands:

Close Connection – closes the connection with selected process.

Close Process - terminates the process .

Process Properties – opens the Process Details dialog.

Who Is Remote Host – for TCP connections opens the **WhoIs resolver** dialog.

Trace Route Host - for TCP connections opens the **Tracert** dialog.

Abuse Address – shows the abuse address of remote host.

RBL Check - checks if the specified host is in a Real-time Black list for spammers “RBL “.

Advanced Information – opens **DataDisplay** dialog.

Save As – saves the data to the text file.

Copy Row – copies the selected row.

Copy All - copies all rows.

The DataDisplay dialog contains the following information: local port information, local port, service, service description.

