http://www.nsauditor.com

Nsasoft llc.

Product Features

- **Intrusion Detection System based on security Events analyzer**
  Nsauditor have incrusted intrusion detection system based on Security Event Log analyzing.

- **Alerts**
  Alerts when IP Address Table or Routing Table are changed by using E-mail,Net Send,Speech Recognation method or by playing user selected voice file.

- **Expert Firewall Controls (will be available in** the **next** releases**)**
  Personal firewall provides home users and small-business owners with the highest level of protection. It stops known and unknown Internet threats and blocks annoying ads.

- **Security Event Log Monitor**
  Security Event Log Monitor monitors the security event logs of Windows NT/2000/XP servers or workstations and notifies of the possible intrusions/attacks by using E-mail,Net Send,Speech Recognation method or by playing user selected voice file.

- **Network monitor**
  Network Monitor 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.

- **NetBIOS Auditor**
  NetBios Auditor is a tool to discover NetBios names. NetBios names are the names of the Services and Machines. NetBIOS Scanner is a powerful and fast tool for exploring networks , scanning a network within a given range of IP addresses and for listing computers which offer NetBIOS resource sharing service as well as their name tables and netbios connections.

- **MS SQL Server Auditor**
  This tool allows to perform an audit on a machine running MS SQL server.

- **SNMP auditor**
  SNMP auditor is a tool that allows to walk through all SNMP MIBs of your nodes and to audit SNMP community names using values stored in xml database.

- **Packet Filter (the protocols count will be enhanced in** the **next** releases **)**
  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.

- **Packet Editor (the protocols count will be enhanced in** the **next** releases **)**
  Packet Editor is a tool to decode IP, ICMP, TCP, UDP, NETBIOS-SSN packets.

- **Sun RPC 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.

- **MS RPC 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.

- **Port Scanner**
  Port Scanner is a TCP/UDP scanner, a tool that detects if certain TCP/UDP ports are open and accepts connections. TCP scanners are usually used to check if the remote computer runs services (e.g. Telnet or FTP). The main function of the port scanner consists in sending messages to the user-defined port list .The type of received response indicates whether the ports are opened. Port Scanner has the following scan modes: connect scan, SYN stealth, FIN stealth, Ping sweep, UDP scan, NULL scan, XMAS tree, IP protocol scan, ACK scan.

- **Trojan horses or backdoor software Detector (will be available in** the **next releases)**
  Port scanner will list all open ports. If the port is a well-known Trojan port, it will be displayed in RED.

- **CGI Scanner**
  CGI probes are sent against web servers. This tool provides an ability to turn them off and if the user is running an audit from a proxy server, he/she can configure the scanner to run CGI probes through that proxy.

- **Remote System OS detector**
  Remote OS detector uses well known TCP, UDP, ICMP packet probes and available OS fingerprints.

- **Auditor**
  Network Auditor is a tool to discover network services and to check them for discovering well known vulnerabilities.This tool creates an audit report.

- **Ping**
  Ping is a tool that provides an opportunity to 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 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.
- **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.
- **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.

- **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. The full query list contains 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 ".

- **TCP/UDP Client/Server/Port Redirector**
  This is a useful tool for testing some services, firewall and intrusion detection systems. This tool also can be used for debugging the program and configuring other network tools.

- **Local IP, TCP, UDP and ICMP 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 Routing, Net Table**

  IP Tables provides the tool to retrieve an information releated to 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.The each part of the table contains information about IP address including address, interface index, subnet mask, broadcast address, reasm size.

- **Local Addressing information table**
  This tool shows the available network interfaces and their IP addresses, Network Mask, Broadcast addresses, PPP, Multicast and Loopback modes.

- **Local Net to media information table**
  This tool shows the available network adapters and their MAC address, Subnet mask, Gateways, DNS servers, WINS servers, DHSPs, interface names ,etc.

- **Process Monitor**
  Process Monitor is a tool to display the list of the processes currently running on computer and to show the program name, the unique process ID, the full path of

program executable file, the name of the file manufacturer, and the name of modules and kernel objects used by the selected process.

- **MAC/Vendor Lookup**
  This tool allows you to 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).