

<http://www.nsauditor.com> Nsasoft
llc.

Auditor

Network Auditor is a tool to discover the network services and to check them for discovering well known vulnerabilities. This tool creates an audit report. The auditor consists in two main parts: TCP and UDP. To enable an option (options) select appropriate checkbox(es).

The enabled **Extended Tcp Ports (Extended Udp Ports)** feature contains the number of ports, used to audit the network. You can add ports by clicking on the **Add Ports** button and selecting port from Ports Dialog.

The screenshot shows the 'Network Audit Dialog' window. It is divided into two main sections: TCP and UDP.

TCP Section:

- TCP
 - Extended Tcp Ports
 - Ports (Example: 13,17,21-23,25,42,43,53,79-80,109-111,113,118-119,135,137-139,143)
 - 13,17,21-23,25,42,43,53,79-80,109-111,113,118-119,135,137-139,143,156,179,389,443,445,512-515, [Add Ports]
 - Ftp Vulnerabilities (Port 21)
 - Check Ftp Vulnerabilities
 - Check Weak Passwords
 - SmtP Vulnerabilities (Port 25)
 - SMTP Vulnerabilities
 - SMTP Relaying
 - Net Bios
 - NetBios Names, Common Info
 - Retrieve Users Logs
 - Enumerate Users
 - Enumerate Machines
 - Enumerate Groups
 - Enumerate Shares
 - Enumerate Hidden Shares
 - Enumerate Connections
 - Enumerate Network Devices
 - Enumerate Services
 - Enumerate Processes
 - Retrieve Policies Information
 - Retrieve Registry Information
 - Retrieve Time of Day
 - Telnet Vulnerabilities (Port 23)
 - Check Telnet Vulnerabilities
 - Check Weak Passwords
 - Pop3 Vulnerabilities (Port 110)
 - Check Pop Vulnerabilities
 - Check Weak Passwords
 - Tcp Services
 - Who Is (Port 43)
 - Finger (Port 79)
 - Sun Rpc (Port 111)
 - IMAP4 (Port 143)
 - Remote EXEC (Port 512)
 - Ms SQL (Port 1433)
 - My SQL (Port 3306)
 - Http Vulnerabilities (Port 80,8080)
 - Common
 - Apache
 - Netscape
 - ColdFusion
 - Frontpage
 - IIS
 - DoS

UDP Section:

- Udp
 - Extended Udp Ports
 - Ports (Example: 42,43,53,67-69,88,111,135-138,143,161,445,514,520,1900)
 - 42,43,53,67-69,88,111,135-138,143,161,445,514,520,1433-1434,1512,1900 [Add Ports]
 - Udp Services
 - Dns Vulnerabilities (Port 53)
 - Snmp Vulnerabilities (Port 161)
 - MsSql Monitor (Port 1434)
 - Sun Rpc (Port 111)
 - Plug and Play Vulnerabilities (Port 1900)

Profile Name: Default Audit Profile

Target Host / Local Interface:

- Local Interface: 192 . 168 . 0 . 226 [Icon]
- Target Host: 0 . 0 . 0 . 0 [Icon]

Comand Buttons: Load Default, Load Profile, Save Profile, Start Audit, Cancel, Save As

To audit ftp vulnerabilities enable **Ftp Vulnerabilities** option. This option allows you to check **Ftp Vulnerabilities** and **Weak Passords** . To audit smtp vulnerabilities enable **SmtP Vulnerabilities** option.

This option allows you to check **SMTP Vulnerabilities** and **SMTP Relaying**. To audit telnet vulnerabilities enable **Telnet Vulnerabilities** option. This option allows you to check **Telnet Vulnerabilities** and **Weak Passwords** . To audit pop3 vulnerabilities enable **Pop3 Vulnerabilities** option. This option allows you to check **Pop Vulnerabilities** and **Weak Passwords**.

To audit different Net Bios settings you can enable some or all **Net Bios** options including **NetBios Names**, **User Logs**, **Users**, etc.

To audit different Tcp services you can enable some or all **Tcp Services** including **Who Is**, **Finger**, etc.

To audit http vulnerabilities enable **Http Vulnerabilities** option.

To audit different Udp services you can enable some or all **Udp Services** including **Dns Vulnerabilities**, **Sun Rpc**, **Sntp Vulnerabilities** , **Plug and Play Vulnerabilities**, **MsSql Monitor**.

The field **Profile Name** contains the profile name. The profile can be loaded by clicking on the **Load Profile** button and selecting the file name (The profile file is stored in XML format).

Clicking on the **Load Default** button loads the default profile. Clicking on the **Save Profile** button will save the profile in the selected file. You can save the profile in another file by clicking on the **Save As** button.

To start auditing clicking on the **Start Audit** button .

To close the dialog click on the **Cancel** button.

To load an interface click on the **Local Interface** button. Clicking on this button opens the Available Network Interfaces dialog.

Clicking on the button Target Host opens the Host Range and Credentials Selection Dialog.

After the auditing process is started the Network Audit Dialog will be closed and the view that shows the audit process will appear in the screen.

The left part of the view contains all selected TCP and UDP ports. The top of the right part contains the remote host settings including Remote Address, Remote Port , Info, Banner, Trojan, Service Name, Service Description. The bottom of the right part contains information about the current auditing process.

Nsauditor Network Security Auditor

File Edit View Statistics Connections Tools Editors Options Help

Sessions

- Network Monitoring
- Auditor
- NetBios Auditor
- Network Scanner
- Web Proxy Scanner
- MsSql Auditor
- SNMP Auditor
- MsRpc Auditor
- SunRpc Auditor

Tools

Statistics

Utils

Host 192.168.0.2

Remote Address	Remote Port	Info	Banner	Trojan
192.168.0.2	21	Open	Windows	
192.168.0.2	25	Open		Back Cc
192.168.0.2	80	Open		Ajan, An
192.168.0.2	110	Open		711 troje
192.168.0.2	135	Open		ProMail I
192.168.0.2	139	Open		
192.168.0.2	143	Open		Chode, (
192.168.0.2	443	Open		
192.168.0.2	445	Open		
192.168.0.2	1025	Open		Remote
192.168.0.2	1433	Open		
192.168.0.2	Host Scan Done!	Host Scan Done!		
192.168.0.2	OS Detected	OS Detected	Windows 2000 SP4,	
192.168.0.2	Scan Completed!	Scan Completed!		
192.168.0.2	111	Open		
192.168.0.2	135	Open		

192.168.0.2 Scan Completed! Scan Completed!

192.168.0.2 Auditing Services

- Auditing FTP
- Auditing SMTP
- Auditing HTTP
- Auditing POP3
- Auditing MSRPC
- Auditing NetBios
- Auditing IMAP4
- Auditing HTTP
- Auditing MSRPC
- Auditing Ms SQL
- Auditing Sun Rpc
- Auditing MSRPC
- Auditing MSRPC
- NetBios Names
- Auditing SNMP
- Auditing SNMP
- Auditing Ms Sql
- Auditing Ms Sql

SECURITY AUDIT COMPLETED TIME:09/07/2004 20:37:45
CLICK THE AUDIT REPORT TOOLBAR ITEM TO VIEW RESULTS!

For Help, press F1

NUM