

<http://www.nsauditor.com>

Nsasoft llc.

NetBios Auditor

NetBios Auditor is a tool for auditing network. The most security problems appear because of incorrect configuration of NetBios resource sharing.

The screenshot displays the Nsauditor Network Security Auditor application window. The interface includes a menu bar (File, Edit, View, Statistics, Connections, Tools, Editors, Options, Help) and a toolbar with various icons. On the left, a vertical sidebar lists several tools: Network Monitoring, Auditor, NetBios Auditor, Network Scanner, Web Proxy Scanner, MsSql Auditor, SNMP Auditor, MsRpc Auditor, and SunRpc Auditor. The main workspace is divided into several panels:

- Sessions:** A table with columns: IP Address, Machine, Workgroup, Sharing, Ethernet Address, Adapter Producer. It shows one session for IP 192.168.0.2 on machine CAMELOT in the NSAGROUP workgroup.
- Workstation Users, Machines, Groups (Double Click To Get Sid):** A table with columns: Type, Name, Result. It lists users like Administrator and Guest.
- WorkStation Info:** A table with columns: Name, Num..., T..., Usage. It lists system services like Workstation Service, File Server Service, and Messenger Service.
- Account Policies:** A table with columns: Policy, Security Setting. It shows settings for password length, age, and lockout duration.
- Shared Resources (Double Click To Connect):** A table with columns: Resource, Path, Uses. It lists shares like E:\, IPC\$, D:\, ADMIN\$, and C\$.
- IP Address Range:** Fields for Start (192.168.0.2), End (192.168.0.2), and Host.

At the bottom left, it says "For Help, press F1" and at the bottom right, there is a "NUM" label.

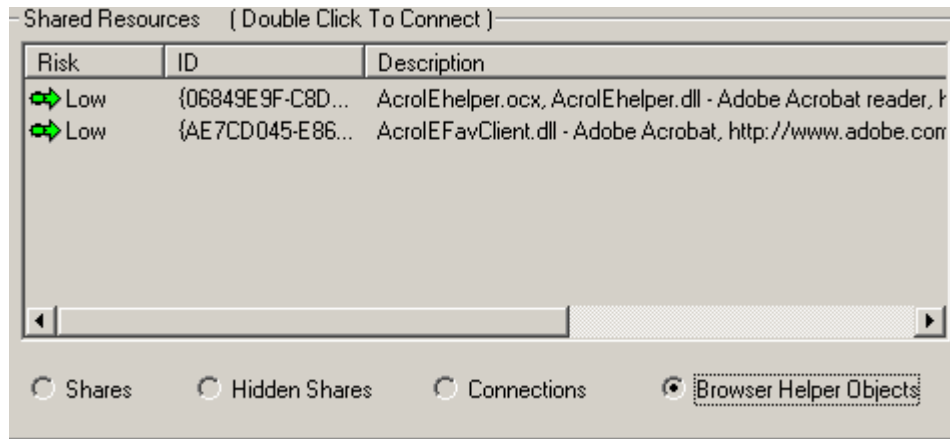
To start auditing click on the toolbar **Start** button. Note that you should fill the **IP Address Range (Start End)** and the first 3 octets of start and end IP addresses should be the same.

After the audit process is over you will get general information about the computer including IP Address, Machine, Workgroup, Sharing, Ethernet Address, Adapter Producer. Also you will get information about workstation users, groups, machines. For each selected option (**Users, Users Log, Machines, Groups**) the appropriate fields will be shown. The workstation info will be available too. For each selected option (**NBNames, Services, Programs, Info, Hotfixes, Run, URLs**) the appropriate fields will be shown. You will also get the information about **Account Policies** (including Policy and Security Setting) and **Shared Resources**. The information about **Shared**

Resources depends on the selected option (**Shares**, **Hidden Shares**, **Connection** , **Browser Helper Objects**).

It is known that the browser helper objects are loaded each time the browser is started up. Such objects run in the same memory context as the browser and can perform any action on the available windows and modules. For ex., a browser helper object can install hooks to monitor messages and actions, etc .

Selecting **Browser Helper Objects** allows you to discover browser helper objects of your computer including parasites and trojans.



You can stop the audit process at any moment by clicking on the toolbar **Stop** button. Note that auditing a computer will take a long time, especially if a wide range of IP addresses is set.