In this chapter you can find answers to some of the most frequently asked questions. The latest FAQ is always available at http://www.tamos.com/en_faq.htm.

NBScan

Q. I try to use NBScan to check my own IP address but I can't see my computer's name table.
A. It most probably means that your computer either doesn't offer resource sharing or it has Winsock version 1 originally shipped with Windows 95. In the latter case consider using nbtstat -A xxx.xxx.xxx.xxx instead, or upgrading to Winsock version 2. This limitation neither applies to viewing other computers' name tables (Winsock 1 works just as good as Winsock 2), nor to NATShell (you can audit your own computer with it).

Q. I check the address xxx.xxx.xxx.xxx by NBScan and get no results, but nbtstat gives me the name table.
A. Two possible reasons. You either set a very short timeout and the response to the query couldn't reach your computer in time, or you are not using the Advanced Mode. In that mode the program lists 100% of the computers nbtstat can potentially list. Please read the **Advanced Mode** paragraph in the NBScan chapter.

Q. I check the address xxx.xxx.xxx.xxx by both NBScan and nbtstat and get no results. The person to whose computer this address is assigned checks the same address (his own) and gets his own computer's name table. Why can he see it and can't I?
A. There is a firewall or some other packet-filtering device between his computer and your computer. Certain packets may be rejected due to the firewall settings. Also some Internet Service Providers filter packets without informing their customers about it. If that's the case you may want to audit the network form a different account**.**

NATShell

Q. What is that magic *SMBSERVER name in the NATShell log?
A. This name is equivalent to the computer name you are connecting to. Here is the quotation from the Microsoft knowledge base article:

"There are currently two ways of finding a valid NetBIOS name to connect to on the target computer:

- *Trying a NetBIOS session setup to the new "*SMBSERVER" name that recent implementations support.*
- *Issuing a NetBIOS adapter status request to the destination IP address, and then parsing the returned name table for the name registered by the server service (<computername>[0x20]). "*

If you see the *SMBSERVER name then NAT is using the first method.

Q. Why can't I see any results for some time after I start NATShell?
A. The program displays new data as soon as they are received from the NAT buffer. Since several lines of text are required to fill up the buffer, NATShell usually starts displaying the first results after a minute or so. It doesn't influence the actual speed of the auditing process, this is just a short delay in displaying results.

Q. Can I use NATShell to audit my own computer?
A. Yes you can. Just enter your own IP address in the Starting IP and Ending IP fields. Remember that NATShell can be used only for auditing computers with user-level access control, i.e. Windows NT and

Windows 2000. Windows 95/98 computers normally have share-level access control.

Shares

Q. When I try to mount a share I receive the “The network is not present or not started” error, but I’m connected!
A. You are probably using Dial-Up Networking and you forgot to check “Log on to network” box in the connection properties.

Q. When I try to mount a share I receive the “Shared Resource Not Found” error, but I know I typed the correct path to the remote share.
A. Make sure that the computer name is present in the lmhosts file and that it’s a unique name in the file. There should not be 2 or more computers with the same name in the lmhosts file. You can check whether your computer is capable of “understanding” the name by typing ping computername in the DOS prompt. If the computer is successfully pinged it means that you can use Essential NetTools to connect to it.

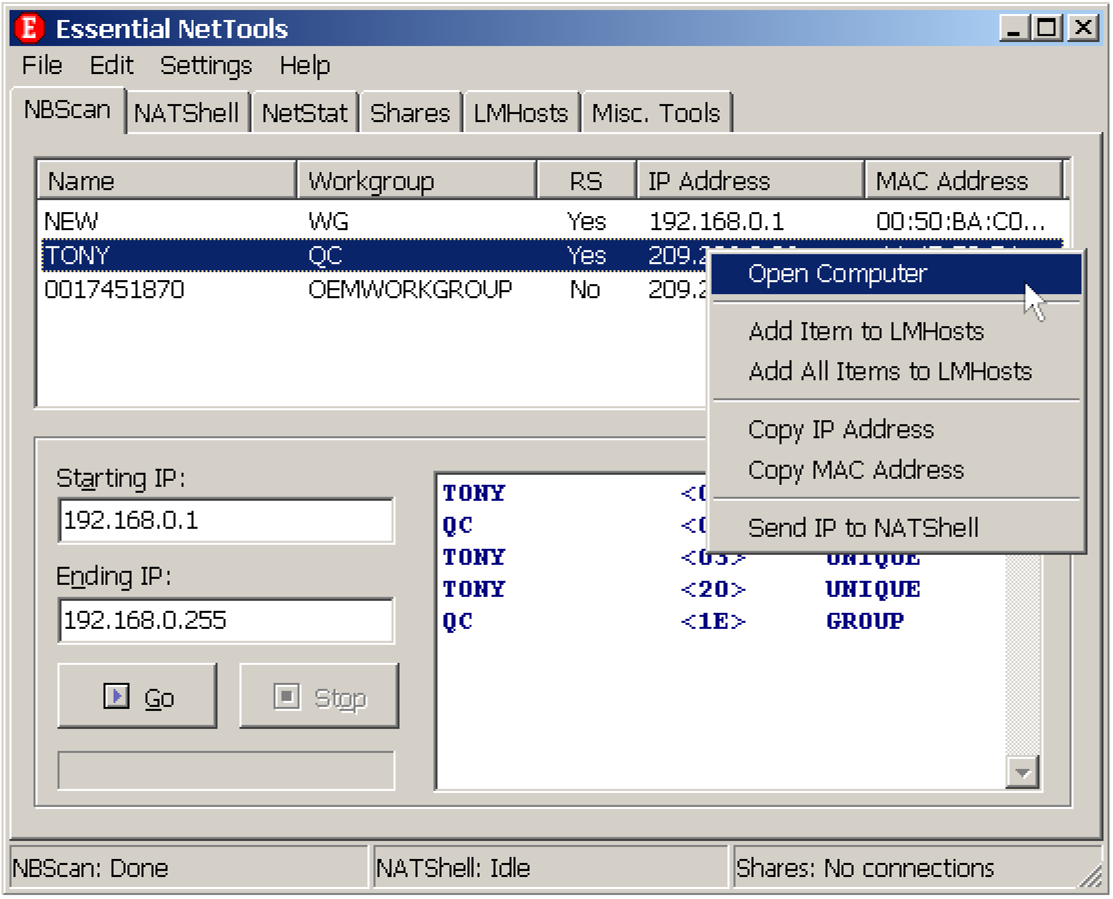
Q. When I select the Open Computer command or try to mount a share the program displays an hourglass and nothing happens for some time.
A. Well, be patient :-) Usually it takes several seconds to establish a connection.

General

Q. Will there be a German (French, Italian, Dutch, etc.) version of Essential NetTools?

A. Currently we don’t plan to release any versions with localized interface, but we do plan to provide users with manuals in foreign languages. Want to help? Translate the manual (this help file) shipped with the program into one of these languages and get a license for free. But contact us first please.

NBScan is a NetBIOS Scanner, a powerful and fast tool for exploring networks. NBScan can scan a network within a given range of IP addresses and list computers offering NetBIOS resource sharing service as well as their name tables. Unlike nbtstat utility supplied with Windows 95/98 and Windows NT, this tool provides a friendly graphical user interface, easy management of the lmhosts file and features parallel scanning which allows to check a class C network in less then 1 minute. Both Class C and B networks can be scanned. NBScan can facilitate routine tasks often carried out by system integrators, administrators and analysts.



Name	Workgroup	RS	IP Address	MAC Address
NEW	WG	Yes	192.168.0.1	00:50:BA:C0...
TONY	QC	Yes	209.2	
0017451870	OEMWORKGROUP	No	209.2	

Starting IP: 192.168.0.1

Ending IP: 192.168.0.255

```
TONY          <0
QC            <0
TONY          <03>     UNIQUE
TONY          <20>     UNIQUE
QC            <1E>     GROUP
```

NBScan: Done | NATShell: Idle | Shares: No connections

Before you start scanning you should enter the starting and ending IP addresses in the **Starting IP** and **Ending IP** fields as shown above. When the range is set click on the **Go** button to start scanning. You can stop scanning at any moment by clicking on the **Stop** button.

The scanning speed can be modified by selecting **Settings** => **Options** in the program menu (see Setting Options for details).

When NBScan detects a computer that offers NetBIOS resource sharing within the set range, the information about the computer is added to the list. The **Name**, **Workgroup, IP Address,** and **MAC address** columns are self-explanatory. **RS,** or **Resource Sharing** column is used to asses whether the computer offers resource sharing: some computers may not be configured to share resources, however they respond to NetBIOS queries and are listed.

Left-clicking on a listed computer displays its name table in the lower window. If you have a problem interpreting name tables you can take a look at the NetBIOS Table reference included in this help file.

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

Open Computer – attempts to open the selected computer. If the computer is accessible, a new Windows Explorer window with remote resources will appear.
Add Item to LMHosts - adds a record associated with the selected computer to the lmhosts file in the appropriate format. Check the #PRE flag on the LMHosts tab before adding if you want the name to be preloaded into the name cache.
Add All Items to LMHosts - adds records associated with the listed computers to the lmhosts file in the appropriate format (computers which have no shared resources are not added). Check the #PRE flag on the LMHosts tab before adding if you want the names to be preloaded into the name cache.
Copy IP Address – copies the selected computer's IP address to the clipboard.
Copy MAC Address – copies the selected computer's MAC address to the clipboard.
Send IP to NATShell - automatically fills the Starting and Ending IP fields of the NATShell tab, which allows you to start auditing the selected computer without manually typing the IP address.

To save the NBScan report in HTML or CSV (comma delimited) format, click on the program menu and select **File** => **Save NBScan Report As …** Select the file format from the **Save as type** drop-down list.

Advanced Mode

Due to some peculiarities in handling NetBIOS connections a small percentage of computers can send replies to queries only to port 137, no matter from which port the query was sent. The advanced mode allows you to choose whether you want the program to receive replies sent to port 137. To switch to the advanced mode click on the program menu and select **Settings** => **Advanced NBScan Mode**. When this mode is on a bullet is displayed next to the menu item. The advanced mode is only available if the computer has not logged on to the network. If the computer has already logged on, this menu item is disabled. If you want to use this mode you should turn it on BEFORE logging on to the network. For example, if you use a dial-up connection to the Internet you should first launch the program, check **Advanced NBScan Mode** and then dial-up.

Important: Using the advanced mode can influence the operation of some of the Windows network services bound to port 137, e.g. you might not be able to use nbtstat or connect to remote computers. In order to restore the normal operation of such services you should turn off the advanced mode, log off the network and log on again.

The reason for these limitations is simple: there is only one port 137 on any system and it is "owned" by the process that claimed the port first. If the Essential NetTools was the first to bind to this port, the program can operate in the advanced mode, but the OS is unable to use it. If the OS binds to it first, then the Essential NetTools cannot use the same port.

Please remember that this mode is just an advanced feature and you may not need to use it. In fact it's quite probable that you will not notice any difference between the results obtained with the advanced mode turned on and off.

Essential NetTools is a set of network tools useful in diagnosing networks and monitoring your computer’s network connections. It includes:

- NBScan - a fast multithreaded NetBIOS scanner for locating computers offering resource sharing on the network.
- NATShell - a user-friendly interface for the popular NetBIOS Auditing Tool (NAT), one of the best network auditing utilities.
- NetStat utility that displays all the computer’s network connections.
- A monitor of external connections to your computer’s shared resources.
- A handy tool for quick connection to remote resources that gives Windows 95/98 users NT user-level connectivity features.
- A convenient LMHosts editor.
- Other useful tools.

Essential NetTools is an easy-to-use and powerful replacement for such Windows utilities as nbtstat, netstat, NetWatcher and has many advanced features that standard Windows utilities can’t offer.

This program is a 30-day evaluation version. A single user license costs $19.

As a registered user you will receive:

- Fully functional unrestricted copy of the software.
- Free updates that will be released within 1 year from the date of purchase.
- Information on updates and new products.
- Free technical support.

We accept credit card orders, orders by phone and fax, checks, and wire transfers. Prices, terms, and conditions are subject to change without notice: please check our web site for the latest product offerings and prices.

http://www.tamos.com/order.htm

If you want to place a credit card order online you can go directly to the secure (SSL) server:

Order Now!

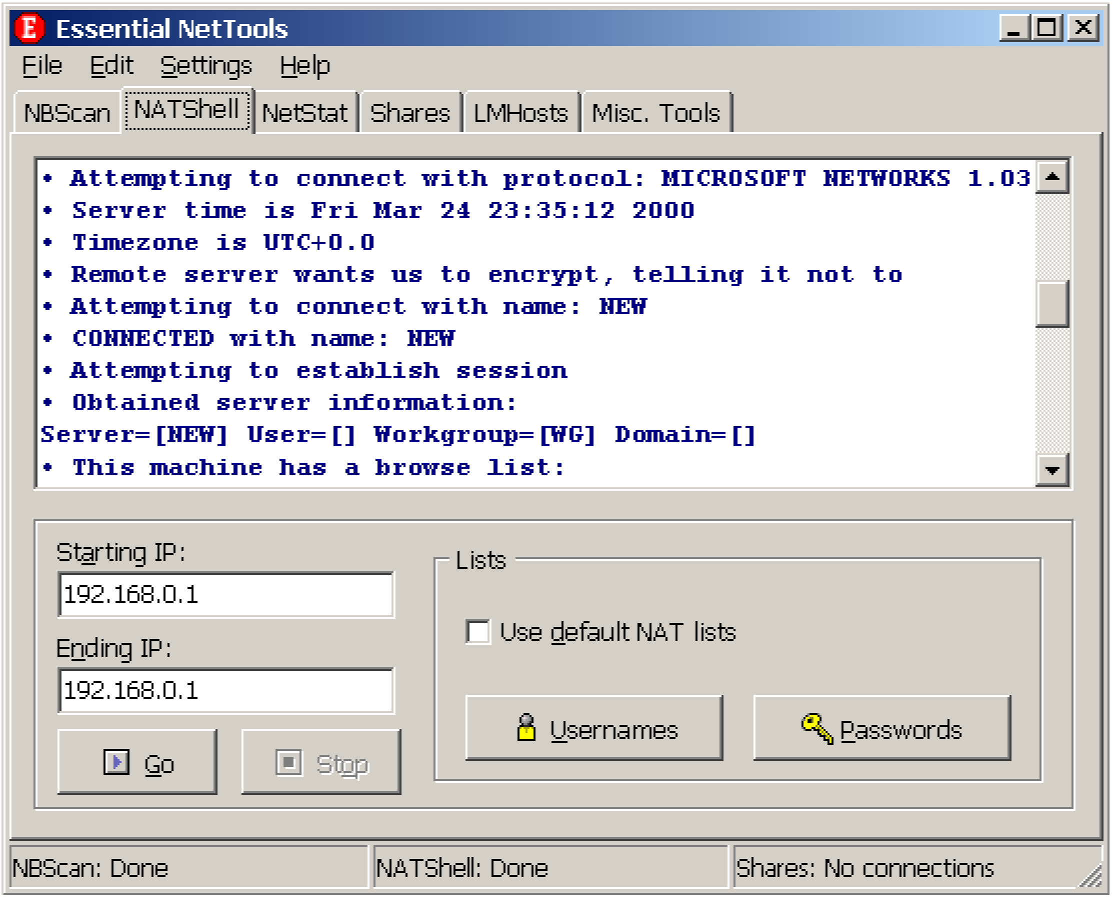
Questions? Comments? Suggestions? Bug reports? Don’t hesitate to contact us.

http://www.tamos.com/

If you have a question that is not answered in this manual please take a minute to check our Frequently Asked Questions page before contacting the technical support. There is a good chance that you will find the answer there. When describing your problem please be as specific as possible. Detailed description of the problem will help us solve it much faster. Please don’t forget to mention the OS version, the program version and build (Help => About), and all other details that you think may be relevant.

NATShell provides a friendly and easy-to-use graphical interface for the NetBIOS Auditing Tool (NAT), a popular free command-line program for auditing networks and individual computers running NetBIOS file sharing service (distributed under GNU General Public License).

Despite the fact that very powerful and expensive solutions exist to check hundreds of potential loopholes in a network, most of security problems stem from incorrect configuration of NetBIOS resource sharing. With NATShell you can easily audit your network and/or individual computers. If you are not familiar with NAT you can read a brief NAT Reference included in this manual.



```
• Attempting to connect with protocol: MICROSOFT NETWORKS 1.03
• Server time is Fri Mar 24 23:35:12 2000
• Timezone is UTC+0.0
• Remote server wants us to encrypt, telling it not to
• Attempting to connect with name: NEW
• CONNECTED with name: NEW
• Attempting to establish session
• Obtained server information:
Server=[NEW] User=[] Workgroup=[WG] Domain=[]
• This machine has a browse list:
```

Starting IP: 192.168.0.1

Ending IP: 192.168.0.1

Lists

☐ Use default NAT lists

NBScan: Done | NATShell: Done | Shares: No connections

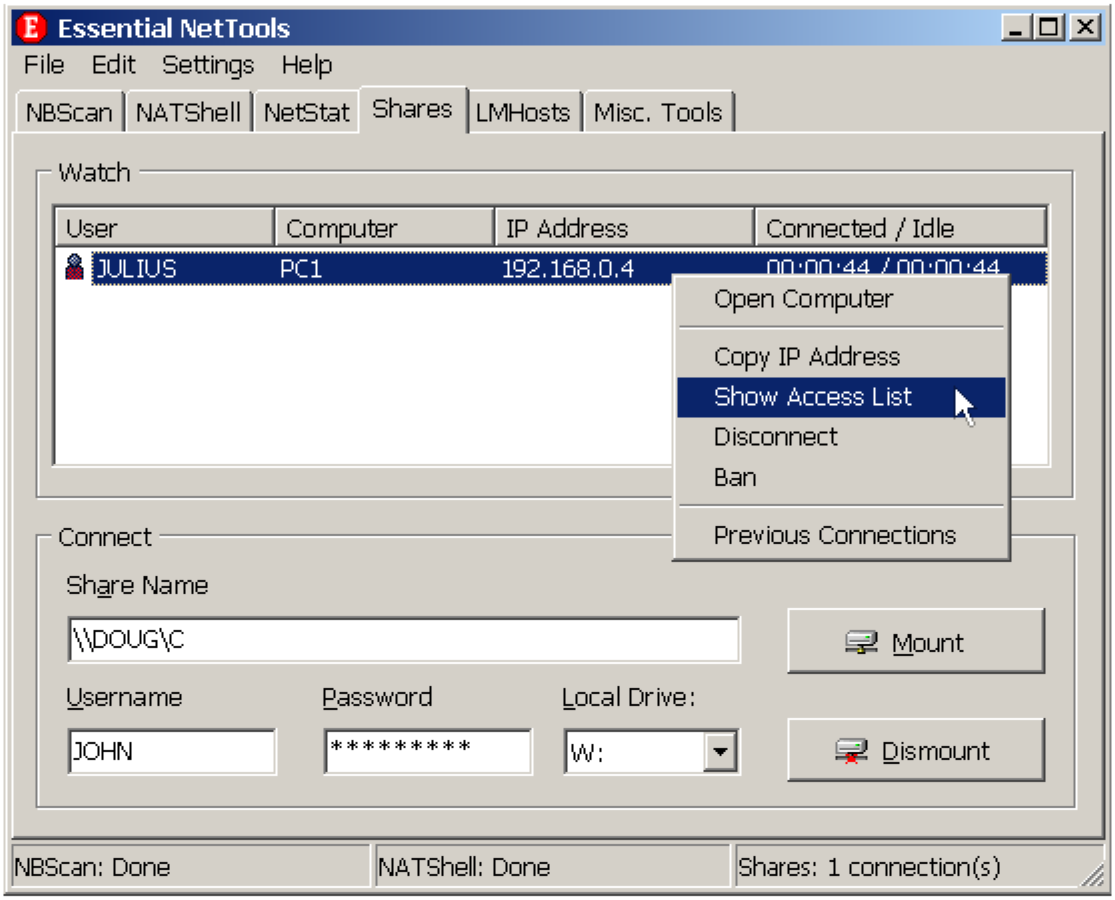
Before you start auditing you should enter the starting and ending IP addresses in the **Starting IP** and **Ending IP** fields as shown above. Please mind that the first 3 octets of the starting and ending IP addresses should be the same.

You can customize the username and password lists by clicking on the **Usernames** and **Passwords** buttons correspondingly. These lists are used to check the possibility of potential intrusion and you can customize them based on the name table obtained by NBScan or any other considerations. A null password is always added to the end of the password list automatically because it is non-printable, however often a good password to try. If you have previously modified the lists, you can restore the default values by clicking on the **Restore Defaults** button. If you want the program to use built-in NAT lists you can do so by checking the **Use default NAT lists** box.

To start auditing click on the **Go** button. You can stop the process at any moment by clicking on the **Stop** button. Remember that auditing a computer is a lengthy process that depends on many factors and you should be prepared to wait for a long time, especially if you set a wide range of IP addresses. When NATShell detects a security flaw in the computer being audited an alert sound is played and the tray icon starts blinking.

To save the NATShell report in HTML format, click on the program menu and select **File** => **Save NATShell Report As …**

The Shares tab allows you to perform two tasks: watching connections to your resources and connecting to remote resources over the network.



User	Computer	IP Address	Connected / Idle
JULIUS	PC1	192.168.0.4	00:00:44 / 00:00:44

Share Name: \\DOUG\C

Username: JOHN

Password: *********

Local Drive: W:

NBScan: Done | NATShell: Done | Shares: 1 connection(s)

Watch

When the program detects an external connection to your computer it displays the information about the user as shown above. A new connection is also indicated by a sound alert and the tray icon color: the icon turns red. Right-clicking on the window brings up a menu with the following commands:

Open Computer – attempts to open the selected computer. If the computer is accessible, a new Windows Explorer window listing remote resources will appear.
Copy IP Address – copies the selected computer's IP address to the clipboard.
Show Access List – brings up a window listing the local files accessed by the selected user.
Disconnect – disconnects the selected computer.
Ban – adds the selected computer's name to the ban list. When a banned user tries to connect to your computer, he or she will be automatically disconnected. To edit the ban list click on the program menu and select **Edit** => **Ban List**.
Previous Connections – shows the log of previous connections.

Important: disconnecting or even banning users cannot be considered as a serious security measure. By disconnecting a user you instruct the operating system to terminate the current connection, but the user can still re-connect in a few second. This can only slow down such connections. If you notice an unauthorized connection it is recommended that you change the access policy by setting passwords for shared resources.

Connect

You can use this tool for connecting to remote resources over the network. It is convenient for Windows NT users and indispensable for Windows 95/98 users. Unlike Windows NT, Windows 95/98 has no user-level connectivity after the boot: you can only specify a password, but not a username. This tool gives Windows 95/98 machines NT user-level connectivity features: you can set both a username and a password. Windows NT users can also use this tool for connecting to remote resources.

To map a remote resource to your local free drive you should enter a valid share name in the **Share Name** field. A valid share name is a computer name preceded with 2 backslashes and followed by 1 backslash, and a resource name. For example, in order to map the folder “COMMON” on the computer “STATION1” you should type:

\\STATION1\COMMON

You should also enter a username and a password in the corresponding fields and select a free drive letter from the **Local Drive** drop-down list.   Note that your computer should be able to resolve the remote computer name you specified to the corresponding IP address. It usually means that the IP address - computer name pair should be present in your lmhosts file (you can do that with the LMHosts tool).

Finally, click on the **Mount** button to map a share to a local drive. You can unmap a resource by clicking on the **Dismount** button. Please note that the **Dismount** command will attempt to disconnect the drive specified in the **Local Drive** field, so if multiple resources have been connected you should select a corresponding drive letter.

You can also use this tool for mapping remote resources of Windows 95/98 computers.

You the **Options** dialog to configure the program's advanced options.

NBScan

Query timeout -sets the timeout for NBScan queries in seconds. This is the time NBScan waits for responses to queries. The default value is 5 seconds, which is normally long enough to receive replies from most of computers being scanned. However the response time may vary from network to network and from connection to connection and is influenced by many factors, so you can decrease this value if you feel that the connection is fast enough.

Number of sockets - sets the number of simultaneous queries sent by NBScan in one cycle. For example, if the query timeout is set to 5 seconds and the number of sockets is set to 25, NBScan sends 25 queries, then waits for 5 seconds, then sends another 25 queries and waits for another 5 seconds, and so on. With such settings a Class C network can be scanned within approximately 50 seconds. The maximum number of sockets is 100 for the registered version and 3 for the evaluation version.

Exclude subnet boundaries – check this box if you want the program to skip IP addresses ending with .0 and .255.

Cleat the list on new query – check this box if you want the program to clear the NBScan list every time you start scanning a new range of IP addresses. If this box is not checked, the program will preserve the results of all previous scans and auto-sort new items by IP address.

NetStat

Show UDP statistics – check this box if you want to have UDP connections listed in the NetStat window.
Show TCP statistics - check this box if you want to have TCP connections listed in the NetStat window.
Show established only - check this box if you want the NetStat window to list established connections only. All other connections (listening, closing, etc) will not be listed.

Sound Alerts

NATShell security flaw detection, **External connection detection** - check these boxes to accompany some of the program events by sound alerts. To change the default sound files click on the Browse button next to the event description and locate a new sound file in the .WAV format. To test the file, click on the button with a speaker icon.

Miscellaneous

Disable mouse tracking - when this box is checked, there is no visual feedback when the mouse passes over list items and users can't select items by pausing the mouse.

Below is the interpretation of NetBIOS name tables used by computers running Windows NT/2000 and Windows 95/98.

Name	Hex Suffix	Type	Description
<computername>	00	U	Workstation Service
<computername>	01	U	Messenger Service
<.._MSBROWSE_>	01	G	Master Browser
<computername>	03	U	Messenger Service
<computername>	06	U	RAS Server Service
<computername>	1F	U	NetDDE Service
<computername>	20	U	File Server Service
<computername>	21	U	RAS Client Service
<computername>	22	U	Exchange Interchange
<computername>	23	U	Exchange Store
<computername>	24	U	Exchange Directory
<computername>	30	U	Modem Sharing Server Service
<computername>	31	U	Modem Sharing Client Service
<computername>	43	U	SMS Client Remote Control
<computername>	44	U	SMS Admin Remote Control Tool
<computername>	45	U	SMS Client Remote Chat
<computername>	46	U	SMS Client Remote Transfer
<computername>	4C	U	DEC Pathworks TCP/IP Service
<computername>	52	U	DEC Pathworks TCP/IP Service
<computername>	87	U	Exchange MTA
<computername>	6A	U	Exchange IMC
<computername>	BE	U	Network Monitor Agent
<computername>	BF	U	Network Monitor Application
<username>	03	U	Messenger Service
<domain>	00	G	Domain Name
<domain>	1B	U	Domain Master Browser
<domain>	1C	G	Domain Controllers
<domain>	1D	U	Master Browser
<domain>	1E	G	Browser Service Elections
<INet~Services>	1C	G	Internet Information Server
<IS~computername>	00	U	Internet Information Server

NAT is a tool written to perform various security checks on systems offering the NetBIOS file sharing service. NAT will attempt to retrieve all the information available from the remote server and to access all listed and some potentially unlisted shares.

If the server requires passwords for the shares, password guessing is carried out. All supplied passwords are tried for all usernames.

Below is a sample NATShell output:

```
• Checking host: ***.***.***.***
• Obtaining list of remote NetBIOS names

• Attempting to connect with name: *
• Unable to connect

• Attempting to connect with name: *SMBSERVER
• CONNECTED with name: *SMBSERVER
• Attempting to connect with protocol: MICROSOFT NETWORKS 1.03
• Server time is Thu Jul 02 16:31:06 1998
• Timezone is UTC-5.0
• Remote server wants us to encrypt, telling it not to
• Attempting to connect with name: *SMBSERVER
• CONNECTED with name: *SMBSERVER
• Attempting to establish session
• Was not able to establish session with no password
• Trying  Username: `' Password: `ADMINISTRATOR'
• Trying Username: `' Password: `GUEST'
• Trying  Username: `' Password: `ROOT'
• Trying Username: `' Password: `ADMIN'
• Trying  Username: `' Password: `PASSWORD'
• Trying  Username: `' Password: `TEMP'
• Trying Username: `' Password: `SHARE'
• Trying  Username: `ADMINISTRATOR' Password: `'
• Trying  Username: `ADMINISTRATOR' Password: `ADMINISTRATOR'
• Trying  Username: `ADMINISTRATOR' Password: `GUEST'
• Trying  Username: `ADMINISTRATOR' Password: `ROOT'
• Trying  Username: `ADMINISTRATOR' Password: `ADMIN'
• CONNECTED: Username: `ADMINISTRATOR' Password: `ADMIN'
• Obtained server information:
Server=[SKY] User=[] Workgroup=[SKYGROUP] Domain=[]
• Obtained listing of shares:
      Sharename         Type        Comment
      ---------            ----        -------
      ADMIN$               Disk:       Remote Admin
      ARCserve$            Disk:       ARCserve System Directory
      C                    Disk:
      C$                   Disk:       Default share
      IPC$                 IPC:        Remote IPC
      mspclnt              Disk:
      NETLOGON             Disk:       Logon server share

• This machine has a browse list:
      Server                 Comment
```

```
    ---------           -------
    JACK
    SKY
• Attempting to access share: \\*SMBSERVER\
• Unable to access
• Attempting to access share: \\*SMBSERVER\ADMIN$
• Unable to access
• Attempting to access share: \\*SMBSERVER\ARCserve$
• WARNING: Able to access share: \\*SMBSERVER\ARCserve$
• Checking write access in: \\*SMBSERVER\ARCserve$
• Attempting to exercise .. bug on: \\*SMBSERVER\ARCserve$
• Attempting to access share: \\*SMBSERVER\C
• WARNING: Able to access share: \\*SMBSERVER\C
• Checking write access in: \\*SMBSERVER\C
• WARNING: Directory is writeable: \\*SMBSERVER\C
• Attempting to exercise .. bug on: \\*SMBSERVER\C
• Attempting to access share: \\*SMBSERVER\C$
• Unable to access
• Attempting to access share: \\*SMBSERVER\mspclnt
• WARNING: Able to access share: \\*SMBSERVER\mspclnt
• Checking write access in: \\*SMBSERVER\mspclnt
• Attempting to exercise .. bug on: \\*SMBSERVER\mspclnt
• Attempting to access share: \\*SMBSERVER\NETLOGON
• WARNING: Able to access share: \\*SMBSERVER\NETLOGON
• Checking write access in: \\*SMBSERVER\NETLOGON
• Attempting to exercise .. bug on: \\*SMBSERVER\NETLOGON
• Attempting to access share: \\*SMBSERVER\D$
• Unable to access
• Attempting to access share: \\*SMBSERVER\ROOT
• Unable to access
• Attempting to access share: \\*SMBSERVER\WINNT$
• Unable to access
```

Version 2.2

- You can now scan Class B networks with NBScan (registered version only).

Version 2.1

- NBScan now lists MAC addresses.
- With NBScan you can scan multiple LAN segments preserving the previous scans' results.
- CSV (comma-delimited) format is available when saving NBScan reports.
- LMHosts allows you to specify a #DOM tag.
- A new TCP Raw Connect tool has been added.
- The interface font can be customized.
- A few bugs fixed in NBScan.

Version 2.02

- You can now add the whole NBScan list to the lmhosts file with one mouse click.
- When you use the DNS tool to resolve a hostname, you can send the obtained IP address to NBScan or NATShell using the context menu.
- Computer names containing spaces and special characters are now added to the lmhosts file in the correct format.
- Multiple record selection is allowed when working with the lmhosts file.

Version 2.01

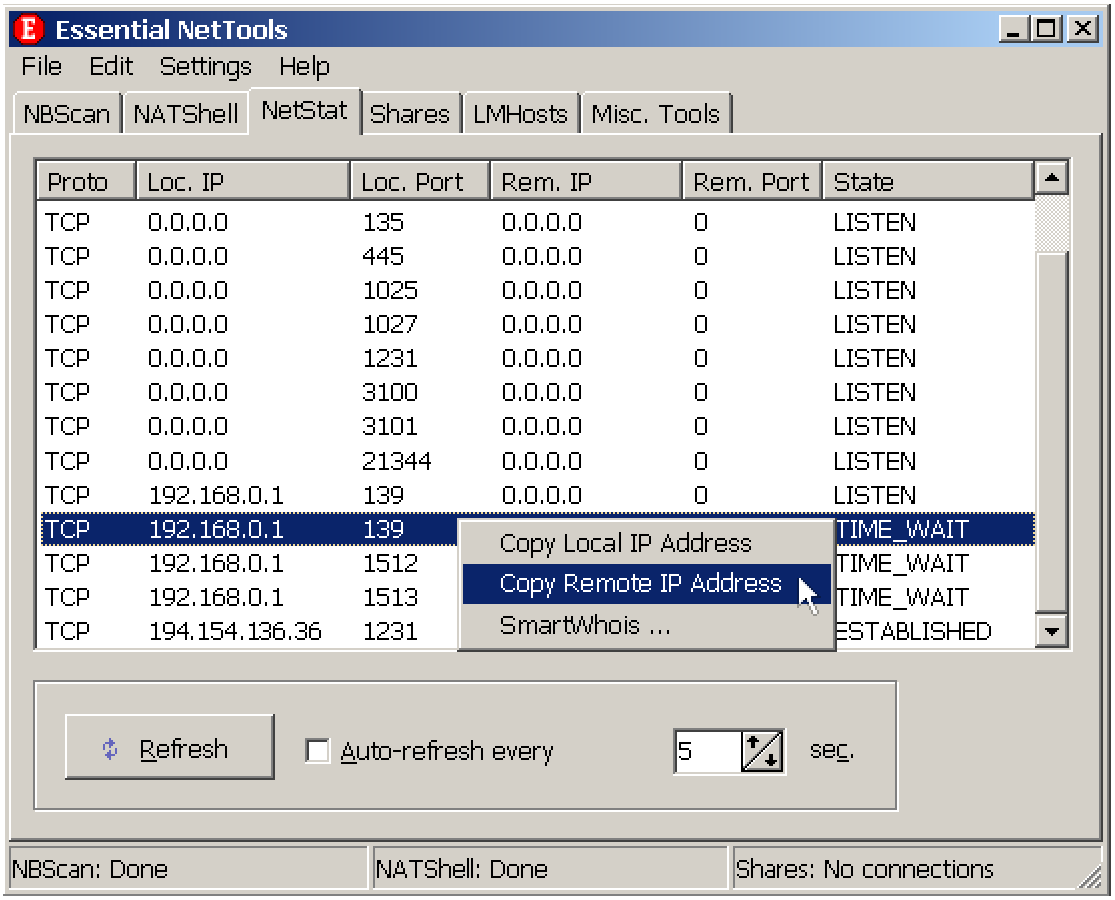
This version fixes a few bugs in HTML report generation found in the previous version of the program.

Version 2.0

Essential NetTools version 2.0 has undergone a major re-design and introduces the following new features and enhancements:

- The source code was re-written from scratch. The new version is much more compact and works faster.
- New NetStat tool that displays TCP and UDP connection information.
- New Watch tool that monitors external connections to your computer.
- New convenient LMHosts editor.
- Now opens remote computers with one mouse click.
- HTML report generation for NATShell.
- Many other new nice features.

This tool is a replacement of the standard Windows netstat command-line utility. It displays all the inbound and outbound connections to your computer.



Proto	Loc. IP	Loc. Port	Rem. IP	Rem. Port	State
TCP	0.0.0.0	135	0.0.0.0	0	LISTEN
TCP	0.0.0.0	445	0.0.0.0	0	LISTEN
TCP	0.0.0.0	1025	0.0.0.0	0	LISTEN
TCP	0.0.0.0	1027	0.0.0.0	0	LISTEN
TCP	0.0.0.0	1231	0.0.0.0	0	LISTEN
TCP	0.0.0.0	3100	0.0.0.0	0	LISTEN
TCP	0.0.0.0	3101	0.0.0.0	0	LISTEN
TCP	0.0.0.0	21344	0.0.0.0	0	LISTEN
TCP	192.168.0.1	139	0.0.0.0	0	LISTEN
TCP	192.168.0.1	139			TIME_WAIT
TCP	192.168.0.1	1512			TIME_WAIT
TCP	192.168.0.1	1513			TIME_WAIT
TCP	194.154.136.36	1231			ESTABLISHED

☐ Auto-refresh every 5 sec.

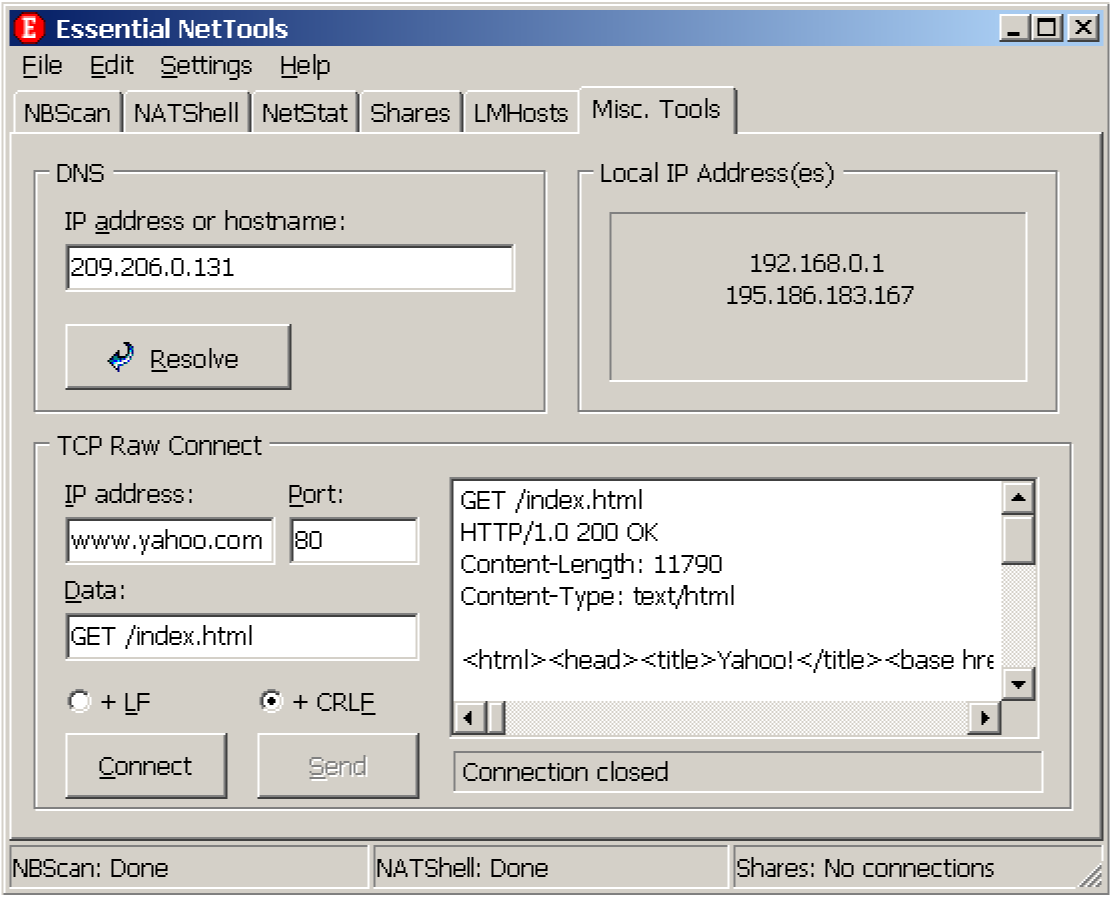
NBScan: Done NATShell: Done Shares: No connections

Check the Auto-refresh box to have the list automatically refreshed. You can also manually refresh the list by clicking on the **Refresh** button. The program can be configured not to display all the connections, see Setting Options for more information. Right-clicking on the window brings up a menu with the following commands:

Copy Local IP Address – copies the local IP address to the clipboard.
Copy Remote IP Address – copies the remote IP address to the clipboard.
SmartWhois – sends the selected remote IP address to SmartWhois, if it is installed on your system. SmartWhois is a stand-alone application developed by our company capable of obtaining information about any IP address or hostname in the world. It automatically provides information associated with an IP address, such as domain, network name, country, state or province, city. The program can be downloaded from our site.

To save the NetStat report in HTML format click on the program menu and select **File** => **Save NetStat Report As …**

This tab provides you with a DNS tool capable of resolving IP addresses to hostanames and vice versa, a list of local IP addresses (if your system has several IP addresses, all of them are listed), and a TCP raw connect tool that allows you to connect to an IP address and send/receive raw data.



IP address or hostname: 209.206.0.131

192.168.0.1
195.186.183.167

IP address: www.yahoo.com

Port: 80

Data: GET /index.html

○ + LF ● + CRLF

```
GET /index.html
HTTP/1.0 200 OK
Content-Length: 11790
Content-Type: text/html

<html><head><title>Yahoo!</title><base hre
```

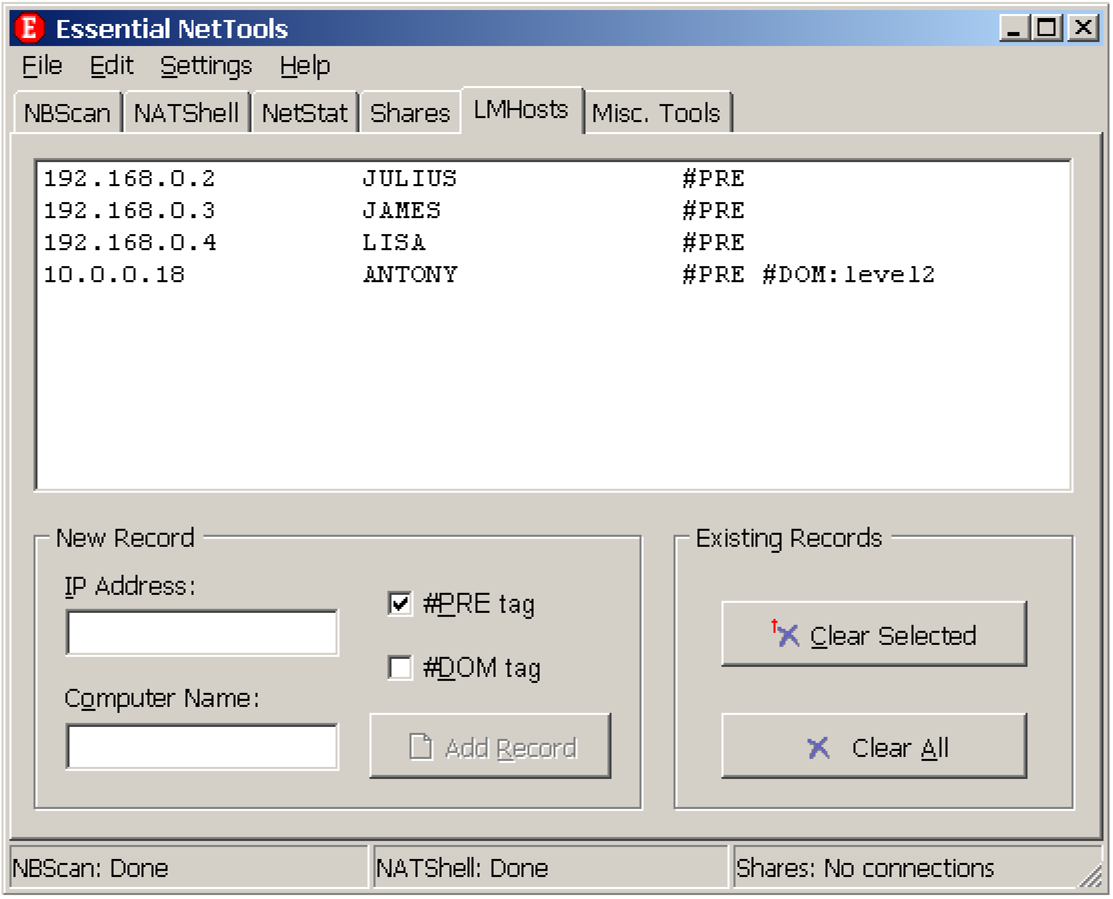
Connection closed

NBScan: Done | NATShell: Done | Shares: No connections

If you use the DNS tool to resolve a hostname, you can send the obtained IP address to NBScan or NATShell using the context menu.

When sending data using the raw connect tool, you can toggle the characters used as a string delimiter: LineFeed (0x0A) or CarriageReturn + LineFeed (0x0D0A).

Use this tab for managing your lmhosts file. All the valid lmhosts records are listed as shown below:



```
192.168.0.2         JULIUS              #PRE
192.168.0.3         JAMES               #PRE
192.168.0.4         LISA                #PRE
10.0.0.18           ANTONY              #PRE #DOM:level2
```

NBScan: Done | NATShell: Done | Shares: No connections

Use the **Add Record** button to add new records to the lmhosts file. If the file does not exist, it will be automatically created. By checking the **#PRE tag** box you can make sure that the computer name is preloaded into the name cache. By checking the **#DOM tag** box you can associate the entry with a domain (you'll be prompted for the domain name). Adding a record also automatically reloads the name cache (corresponds to the nbtstat –R command).

To remove one or all the existing records use the **Clear Selected** or **Clear All** buttons. Removing records automatically reloads the name cache.

Our special thanks to François Piette and Gleb Yourchenko.

Please read the following terms and conditions carefully before using this software. Your use of this software indicates your acceptance of this license agreement. If you do not agree with the terms of this license you must remove this software from your storage devices and cease to use the product.

Copyright

This software is copyright 1998-2000, TamoSoft, Inc. Essential NetTools is a trademark of TamoSoft, Inc The use and copyright of this software is governed by international copyright treaties. TamoSoft, Inc. retains full title and rights to this software and documentation and in no way does the license granted in any way diminish the intellectual property rights of TamoSoft, Inc. You must not redistribute the registration codes provided, either on paper, electronically, or in any other form.

Evaluation Version

This is not free software. You are hereby licensed to use this software for evaluation purposes without charge for a period of 30 days. Using this software after the evaluation period is in violation of copyright laws and may result in severe civil and criminal penalties.

Registered Version

One registered copy of this software may either be used by a single person who uses the software personally on one or more computers, or installed on a single workstation used non simultaneously by multiple people, but not both.

Disclaimer

THIS SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT WILL TAMOSOFT, INC. BE LIABLE TO YOU FOR ANY DAMAGES, INCLUDING INCIDENTAL OR CONSEQUENTIAL DAMAGES, ARISING OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE, UNDERSTAND IT, AND AGREE TO BE BOUND BY ITS TERMS.

Distribution

This software may be distributed freely in its original unmodified and unregistered form. The distribution has to include all files of its original distribution. Distributors may not charge any money for it. Anyone distributing this software for any kind of remuneration must first contact us for authorization.

Other Restrictions

You may not modify, reverse engineer, decompile or disassemble this software in any way, including changing or removing any messages or windows.

Windows is a registered trademark of Microsoft Corporation. All other trademarks and service marks are the property of their respective owners.

NAT GNU GPL License

For users' convenience the program distribution includes the NetBIOS Auditing Tool (NAT) binary files: NAT.EXE and CYGWIN. NAT is a free tool distributed under GNU General Public License. This license is included in the distribution of Essential NetTools for you reference and gives you the right to use and further redistribute NAT. Please read the natgpl.txt file located in the application folder for details. Please note that the GNU General Public License applies ONLY to NAT.

This error message is generated when the program detects a wrong version of Snmpapi.dll on your system. If you have multiple copies Snmpapi.dll in different directories, leave the one that has the latest version and delete all others. If it doesn’t help, please contact technical support. Don’t forget to include information about your OS version and Snmpapi.dll version.

CommView

CommView is a program for monitoring network activity capable of capturing and analyzing packets on any Ethernet network. It gathers information about data flowing on a LAN and decodes the analyzed data. With CommView you can see the list of network connections, vital IP statistics, and examine individual packets. IP packets are decoded down to the lowest layer with full analysis of the main IP protocols: TCP, UDP, and ICMP. Full access to raw data is also provided in real time. CommView is a helpful tool for LAN administrators, security professionals, network programmers, or anyone who wants to have a full picture of the traffic going through one's PC or LAN segment.

More information

SmartWhois

A handy utility for obtaining information about any IP address or hostname in the world. Unlike standard Whois utilities, SmartWhois automatically provides information associated with an IP address no matter where it is registered geographically. In just a few seconds you can learn all you want to know about a user: domain, network name, country, state or province, city. Even if the IP address cannot be resolved to a hostname, SmartWhois won't fail.

More information