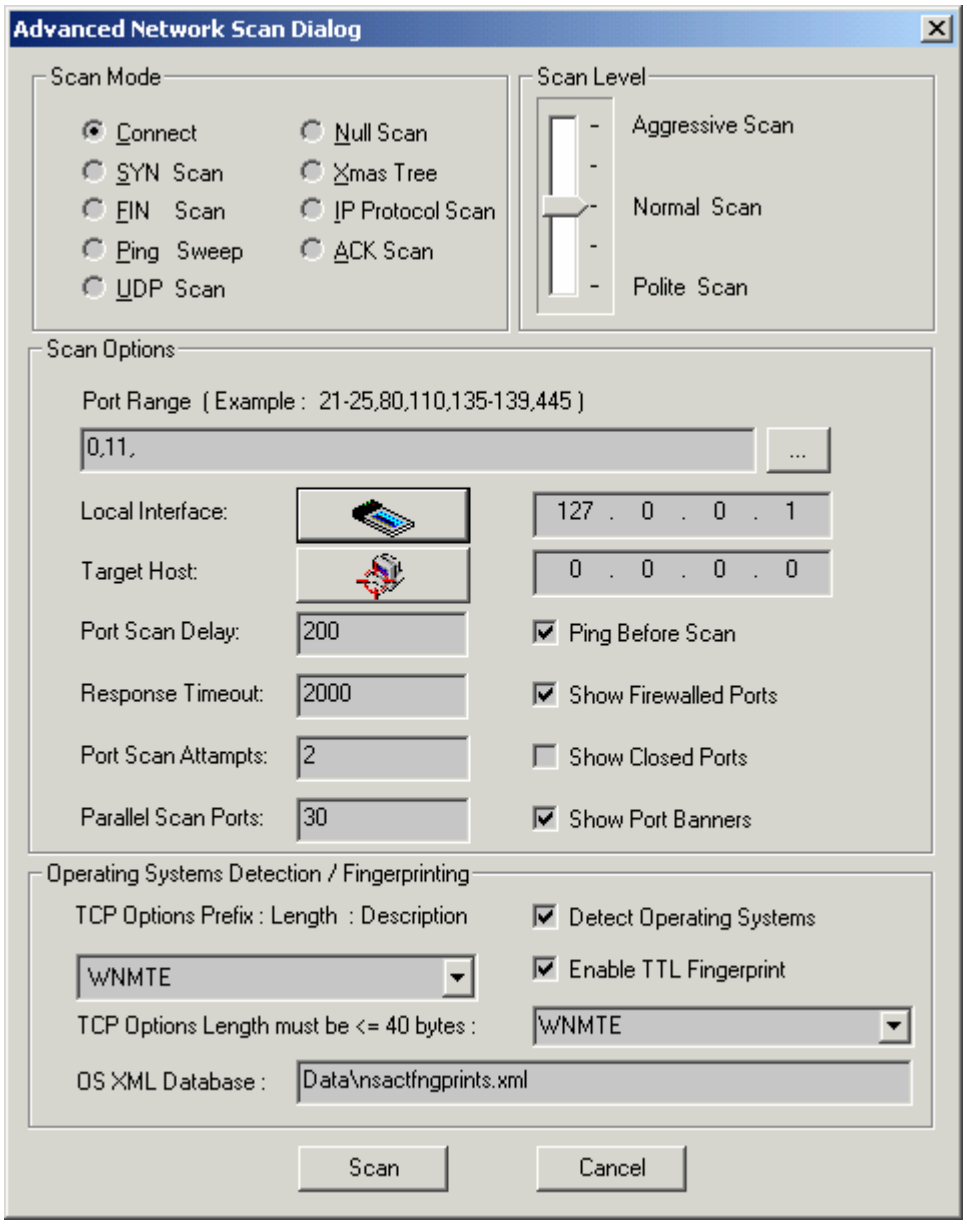
http://www.nsauditor.com

Nsasoft llc.

Network Scanner

Network Scanner is a tool to scan large networks or a single host. This tool uses raw IP packets to determine available hosts, what ports they are offering , what operating systems they are running and other important characteristics.
You can specify the scan mode by selecting the appropriate mode.
Here are the supported scan mode types :



Connect – this is the basic mode of scanning. The connect() system call is used to open a connection to every listening port on the host . If the port is not listening the call of connect() will fail.
This scan type is easily detectable because of target host logs .

SYN Scan – this scan type doesn't open a full TCP connection. Instead of opening a real connection you can send a SYN packet and wait for a response. An indicative of listening port is SYN/ACK and RST is an indicative of non-listener. In case of receiving SYN/ACK, RST is send to close the connection. Not all privileges you have allow you to build this packet. Note that fewer sites will log this scanning mode.
FIN Scan – in some cases SYN scan isn't stealthy enough because some programs can detect this scans. The FIN scan uses an RST packet for the closed ports to reply to your probe(for the probe is used a FIN packet.). This scan type doesn't work against systems running Windows95/NT.
Ping Sweep – ping is used to know which hosts on the network are accessible. One of the ways to check the host availability is sending ICMP echo request packet to every specified IP address. Hosts that respond are available. This method will work only for sites that haven't blocked the echo requests. In such cases TCP ACK packet is used.
UDP Scan – UDP scan is used to determine the opened UDP ports.To each port is sent a zero byte UDP packet . For the closed ports ICMP port unreachable message is received. Otherwise the port is marked as an open. Note that sometimes UDP scanning is slow, because the ICMP error message rate is limited. .
Null Scan – this type of scanning turns off all flags.
Xmas Tree – this scan type turns on only FIN, URG and PUSH flags. This types of packets can be used for a probe while the closed ports should reply with en RST.
IP Protocol Scan - this scan type is used to determine which IP protocols are supported on a specific host. To each specified protocol on the target host is send an IP packet. If the protocol is not in use the ICMP protocol unreachable message will be send as a reply. Note that some hosts may not send protocol unreachable message. So all the protocols will be assumed as "open".
ACK Scan – this scan type sends an ACK packet to specified ports. The port is assumed as "unfiltered " if an RST message is returned. If there is no reply than the port is assumed as "filtered".

Here are the supported scan level types :
Aggressive Scan – aggressive mode adds a five minute timeout for each host and for each probe response waits not more than 1.25 seconds.
Normal Scan - this is the default scan type. It tries to run quickly without overloading the network and scanning all hosts.
Polite Scan – this scan type reduces the chances of crashing machine. It waits at least 0.4 seconds between the probes.

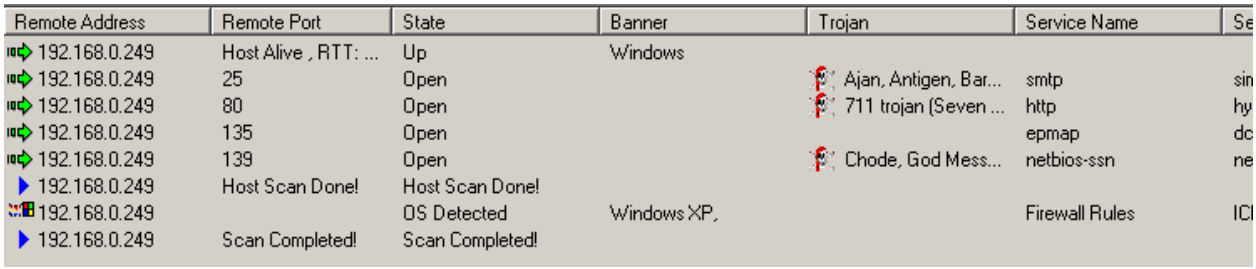
You can click on the browse button and select the **Port Range** in the scan options part.
Clicking on the **Local Interface** button the Available Network Interfaces dialog.

Clicking on the **Target Host** button opens the **Host Range and Credentals Selection** dialog.
You can set **Port Scan Delay**, **Response Timeout**, **Port Scan Attempts**, **Parallel Scan Ports** manually.The values of these fields depend on scan level . The scan results will be shown depending on the enabled/disabled state of each option (**Show Firewalled Ports , Show Closed Ports, Show Port Banners**).
If the option **Ping Before Scan** is enabled appropriate packets (see **Ping Sweep**)will be sent before scanning .
Operating System Detection/ Fingerprinting part contains:
TCP Options (prefix:length: description):

W:3:Window Scale Option,
N:1:No Operation,
M:4:Maximum Segment Size,
T:10:Timestamps Option,
E:1:Endoptions List,
O:2:Selective ACK Permitted,
S:10:Selective ACK Option,
C:6:Tcp Echo Option,
A:6:Tcp Echo ACK Option,
K:2:POC Permitted Option,
P:3:POC Service Option,
X:6:TCP CC Options,
Y:6:TCP CC New Options,
Z:6:TCP CC Echo Options,
U:3:TCP Alternate CheckSum.

You can select the options you want .The default option that is used by the program is WNMTE.
Detect Operating Systems - enabling this option allows to create a fingerprint and to compare it with its own database of known OS fingerprints and thus to decide what type of system you are scanning.The fingerprint is created automatically.
Enable TTL Fingerprint - To add a TTL field in the fingerprint you should enable the TTL fingerprint. In this case it uses TTL during OS detection.

Note that if the scanner can not find the appropriate OS fingerprint in the XML database (the program will create new XML OS fingerprint entry in XML database and will set the system name , OS family and IP address. For the example bellow “Windows 192.168.0.2” will be set in case of operating system Windows or “Unknown 192.168.0.2” in case of uknown OS family).
User can find the OS fingerprint in the XML Database and can set the valid OS name. Later during scanning similar operating systems the tool can find the OS family using the fingerprint (if for ex. the OS that is scanning is “WindowsXP” and in XML database there isn’t such name ,then the name “Windows 192.168.0.2” will be used instead of “WindowsXP”. This means that the OS of scanning host is similar to OS of the host 192.168.0.2).



Remote Address	Remote Port	State	Banner	Trojan	Service Name	Se
192.168.0.249	Host Alive , RTT: ...	Up	Windows			
192.168.0.249	25	Open		Ajan, Antigen, Bar...	smtp	sin
192.168.0.249	80	Open		711 trojan (Seven ...	http	hy
192.168.0.249	135	Open			epmap	dc
192.168.0.249	139	Open		Chode, God Mess...	netbios-ssn	ne
192.168.0.249	Host Scan Done!	Host Scan Done!				
192.168.0.249		OS Detected	Windows XP,		Firewall Rules	ICI
192.168.0.249	Scan Completed!	Scan Completed!				

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

Save As – saves the data to the text file.
Copy All - copies all rows.
Close - closes the selected connection.

The most important privileges of Nsauditor are:
Automatic creation of OS fingerprint.
The XML based format of OS fingerprint.
The user interface that allows TCP options creation.