

Monitoring Your Network

Chris Bamber, IT Systems Manager
Somerville College

Confidentiality: The contents of this presentation and workshop discussion are to be held in strictest confidence.

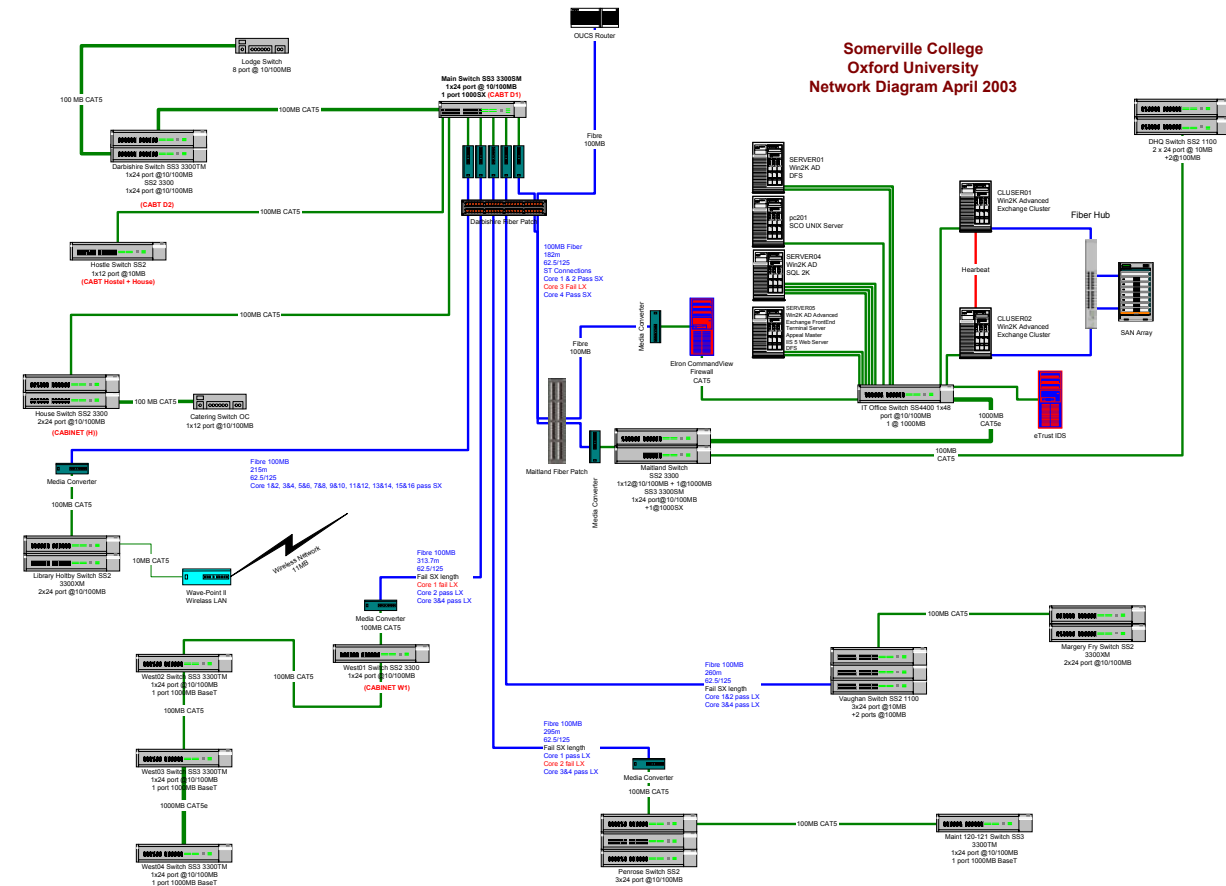
What We Can Use the Tools for

- Identifying unofficial services or servers
- Monitoring usage and traffic statistics
- Protecting your network from the world
- Troubleshooting your network
- Investigating a security incident
- Keeping logs of users activities for accountability

Who? What? Where? How? When?

- Who is accessing your network?
 - students, academics, staff, visitors or others
- What are they accessing your network for?
 - academic study, social use, business use, illegal use
- Where are they accessing your network from?
 - internal, external
- How are they accessing your network?
 - remote user, local Ethernet, WAN, dial-up, Wi-Fi, VPN
- When did they access your network?
 - today, yesterday, last week, last month...

A College Network



Software Tools

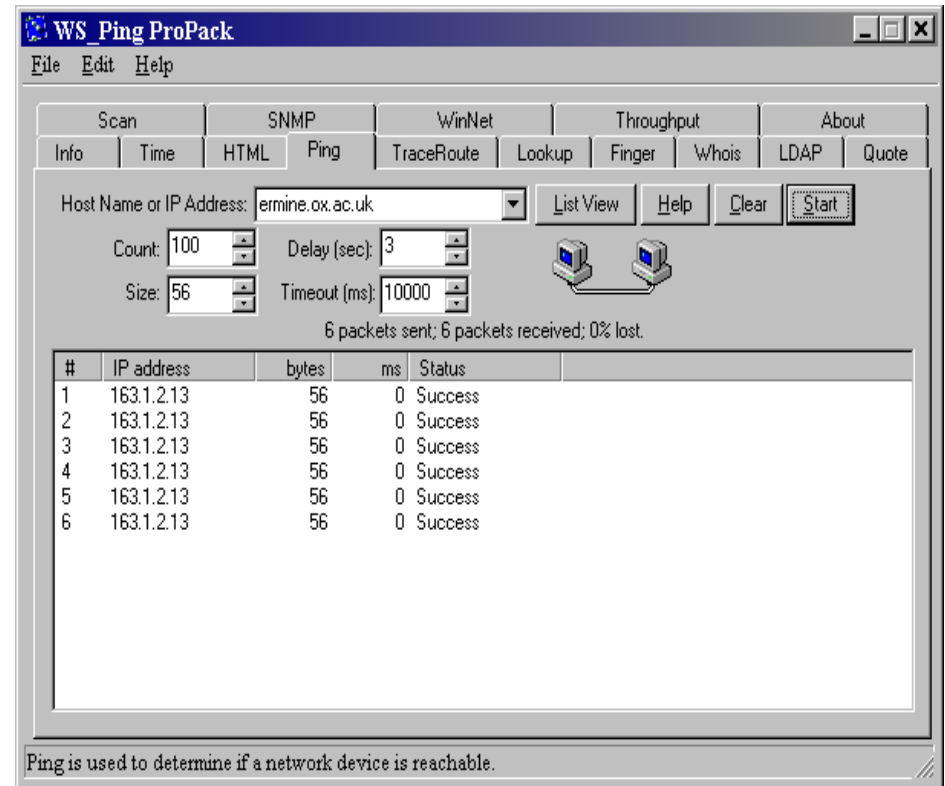
- WS_Ping_ProPack
- XploiterStat Lite
- Windows Event Viewer
- Sophos Anti-Virus for NT
- Sophos Anti-Virus ADMIN Tool
- Software Firewalls
- eTrust Intrusion Detection (Sessionwall)
- 3Com Network Supervisor
- GFI LANguard Network Security Scanner
- Network Probe

A Linux Solution

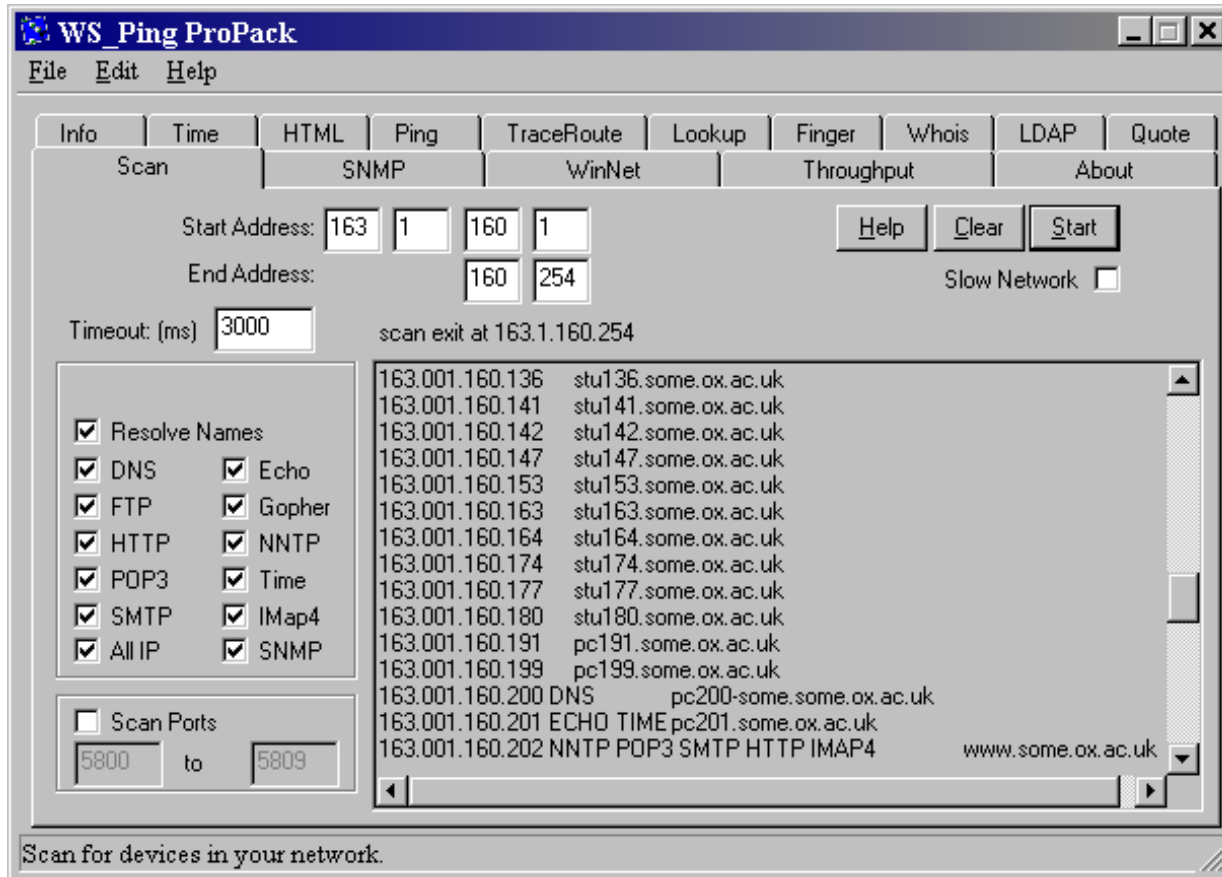


Ws_Ping_ProPack

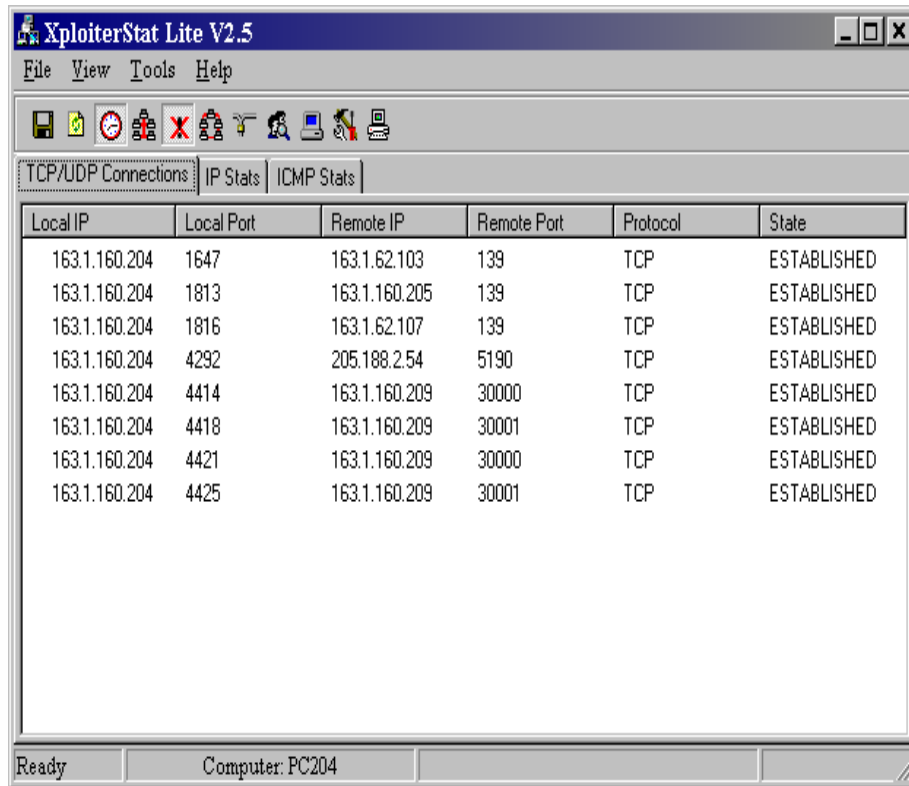
- This tool gives you basic windows interface into a few very handy utils:- Ping, Scan, TraceRoute, Whois, Lookup etc
- Doing regular scans of common ports on your network will help to discover unauthorised services or servers
- Very quick and simple, also cheap £30.00 for a licence



A Port Scan



XploiterStat Lite



The screenshot shows the XploiterStat Lite V2.5 application window. The title bar reads 'XploiterStat Lite V2.5'. The menu bar includes 'File', 'View', 'Tools', and 'Help'. Below the menu bar is a toolbar with various icons. The main window has three tabs: 'TCP/UDP Connections', 'IP Stats', and 'ICMP Stats'. The 'TCP/UDP Connections' tab is active, displaying a table with the following data:

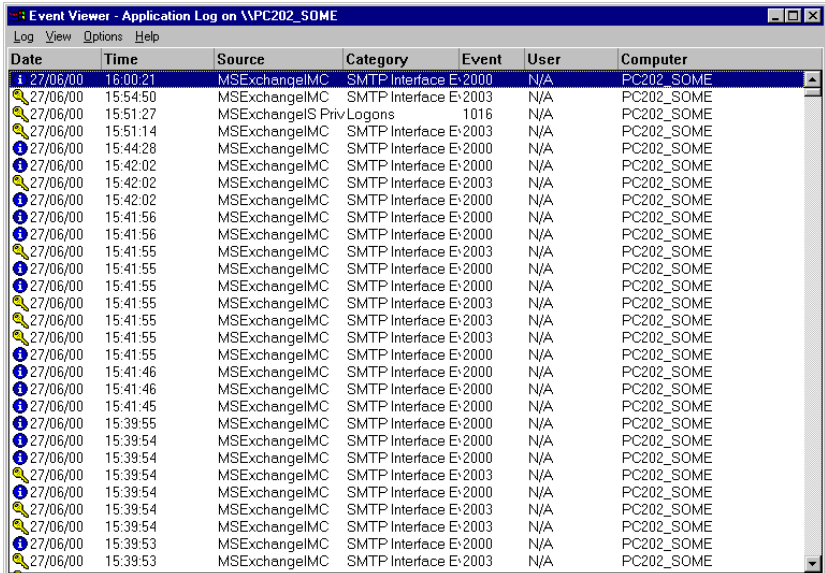
Local IP	Local Port	Remote IP	Remote Port	Protocol	State
163.1.160.204	1647	163.1.62.103	139	TCP	ESTABLISHED
163.1.160.204	1813	163.1.160.205	139	TCP	ESTABLISHED
163.1.160.204	1816	163.1.62.107	139	TCP	ESTABLISHED
163.1.160.204	4292	205.188.2.54	5190	TCP	ESTABLISHED
163.1.160.204	4414	163.1.160.209	30000	TCP	ESTABLISHED
163.1.160.204	4418	163.1.160.209	30001	TCP	ESTABLISHED
163.1.160.204	4421	163.1.160.209	30000	TCP	ESTABLISHED
163.1.160.204	4425	163.1.160.209	30001	TCP	ESTABLISHED

The status bar at the bottom of the window shows 'Ready' and 'Computer: PC204'.

- Port monitoring software, TCP and UDP
- Free, upgrade available at approx. £30.00
- Produce text logs of active connections to your machine or servers
- Handy for putting a trace on a machine your concerned about

Windows Event Viewer

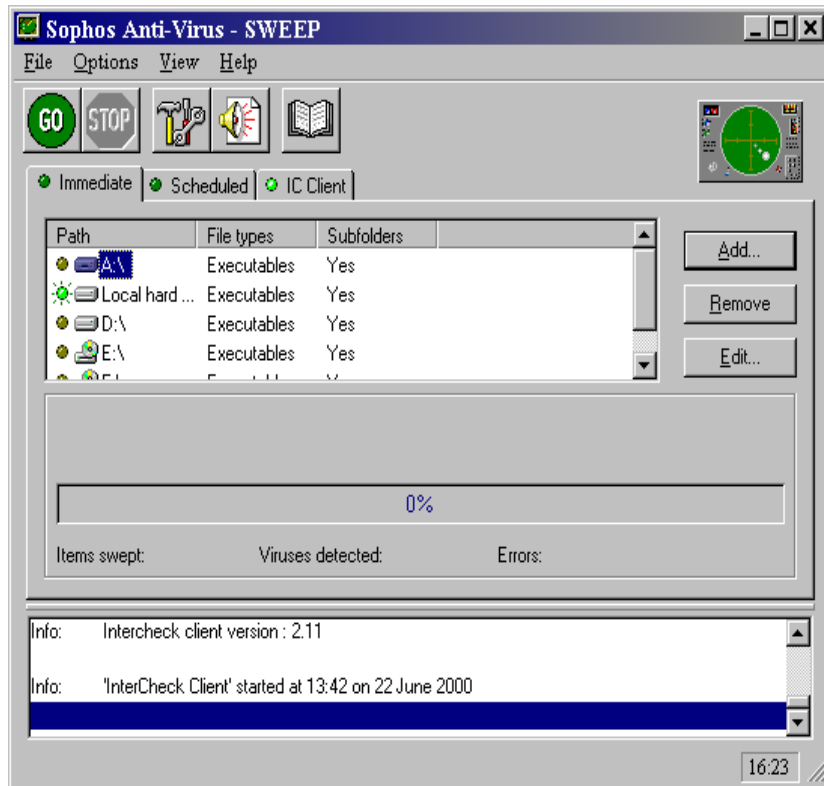
- Comes with MS Servers, Windows 2000 and XP, it's FREE!
- Use it to look at your logs
- Make sure you have some logs
- Export your logs to examine them in Excel, it's quicker



The screenshot shows the Windows Event Viewer window titled "Event Viewer - Application Log on \\PC202_SOME". The window contains a table of event logs with the following columns: Date, Time, Source, Category, Event, User, and Computer. The logs are filtered to show events from the source "MExchangeLMC".

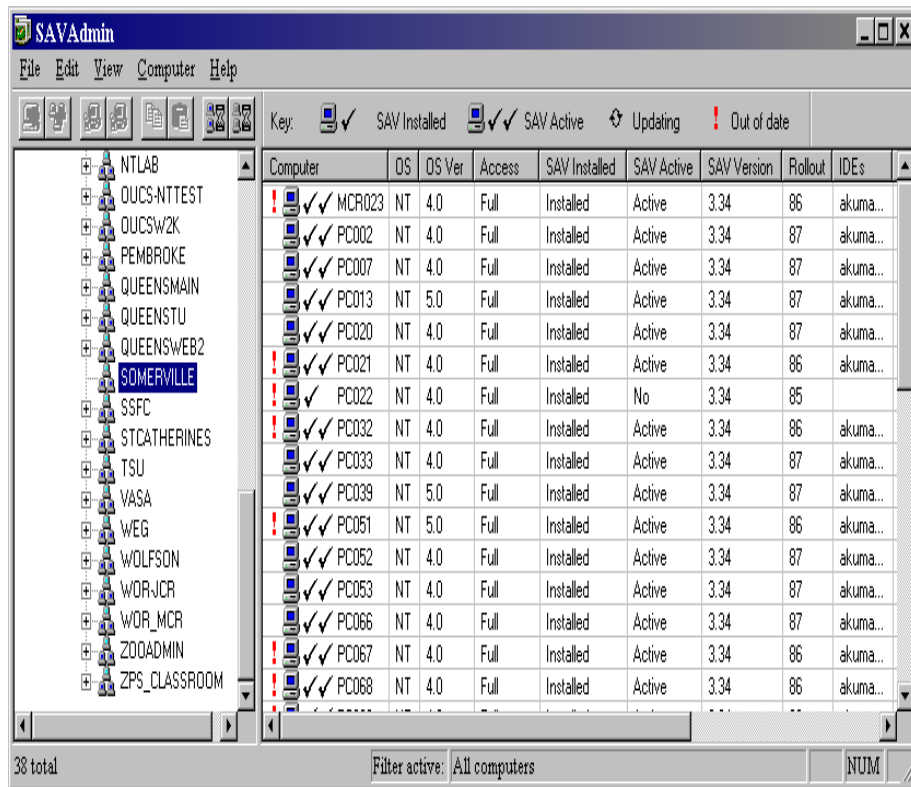
Date	Time	Source	Category	Event	User	Computer
27/06/00	16:00:21	MExchangeLMC	SMTP Interface E:2000		N/A	PC202_SOME
27/06/00	15:54:50	MExchangeLMC	SMTP Interface E:2003		N/A	PC202_SOME
27/06/00	15:51:27	MExchangeLMC	SMTP Interface E:2003		N/A	PC202_SOME
27/06/00	15:51:14	MExchangeLMC	SMTP Interface E:2003		N/A	PC202_SOME
27/06/00	15:44:28	MExchangeLMC	SMTP Interface E:2000		N/A	PC202_SOME
27/06/00	15:42:02	MExchangeLMC	SMTP Interface E:2000		N/A	PC202_SOME
27/06/00	15:42:02	MExchangeLMC	SMTP Interface E:2003		N/A	PC202_SOME
27/06/00	15:42:02	MExchangeLMC	SMTP Interface E:2000		N/A	PC202_SOME
27/06/00	15:41:56	MExchangeLMC	SMTP Interface E:2000		N/A	PC202_SOME
27/06/00	15:41:56	MExchangeLMC	SMTP Interface E:2000		N/A	PC202_SOME
27/06/00	15:41:55	MExchangeLMC	SMTP Interface E:2003		N/A	PC202_SOME
27/06/00	15:41:55	MExchangeLMC	SMTP Interface E:2000		N/A	PC202_SOME
27/06/00	15:41:55	MExchangeLMC	SMTP Interface E:2000		N/A	PC202_SOME
27/06/00	15:41:55	MExchangeLMC	SMTP Interface E:2003		N/A	PC202_SOME
27/06/00	15:41:55	MExchangeLMC	SMTP Interface E:2003		N/A	PC202_SOME
27/06/00	15:41:55	MExchangeLMC	SMTP Interface E:2003		N/A	PC202_SOME
27/06/00	15:41:55	MExchangeLMC	SMTP Interface E:2000		N/A	PC202_SOME
27/06/00	15:41:46	MExchangeLMC	SMTP Interface E:2000		N/A	PC202_SOME
27/06/00	15:41:46	MExchangeLMC	SMTP Interface E:2000		N/A	PC202_SOME
27/06/00	15:41:45	MExchangeLMC	SMTP Interface E:2000		N/A	PC202_SOME
27/06/00	15:39:55	MExchangeLMC	SMTP Interface E:2000		N/A	PC202_SOME
27/06/00	15:39:54	MExchangeLMC	SMTP Interface E:2000		N/A	PC202_SOME
27/06/00	15:39:54	MExchangeLMC	SMTP Interface E:2000		N/A	PC202_SOME
27/06/00	15:39:54	MExchangeLMC	SMTP Interface E:2003		N/A	PC202_SOME
27/06/00	15:39:54	MExchangeLMC	SMTP Interface E:2000		N/A	PC202_SOME
27/06/00	15:39:54	MExchangeLMC	SMTP Interface E:2003		N/A	PC202_SOME
27/06/00	15:39:54	MExchangeLMC	SMTP Interface E:2000		N/A	PC202_SOME
27/06/00	15:39:53	MExchangeLMC	SMTP Interface E:2000		N/A	PC202_SOME
27/06/00	15:39:53	MExchangeLMC	SMTP Interface E:2003		N/A	PC202_SOME

Sophos Anti-virus for NT



- It's FREE!, site licensed to Oxford University
- Protect your workstations from viruses
- Use a protected install so users can't remove it
- Make it mandatory for all computers connected to your network
- Keep it updated...

Sophos Anti-Virus ADMIN Tool



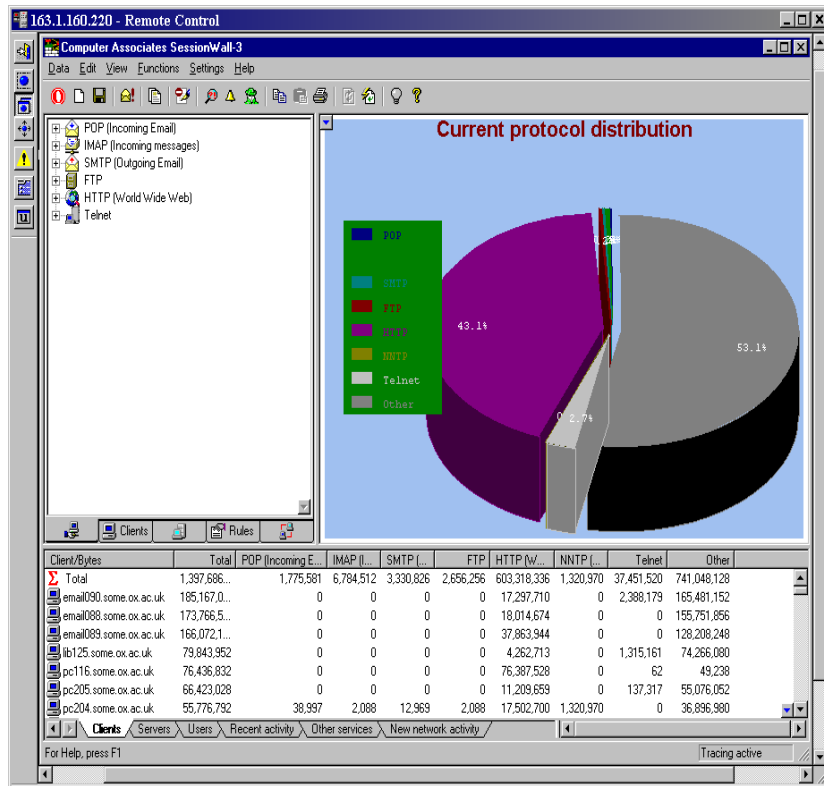
- It's FREE!
- Allows you to install SAV onto your NT workstations remotely
- You need to have their admin shares(C\$) available for the initial install
- Allows you to update and change the configuration of SAV
- Monitors the status and current rollout of the IDE files
- Allows you to force an update to the user workstation
- Quick and simple

Software Firewalls



- Some free, some not
- Elron Command View Firewall for NT
- SmoothWall – Free and Commercial versions
- FreeBSD Firewalls...

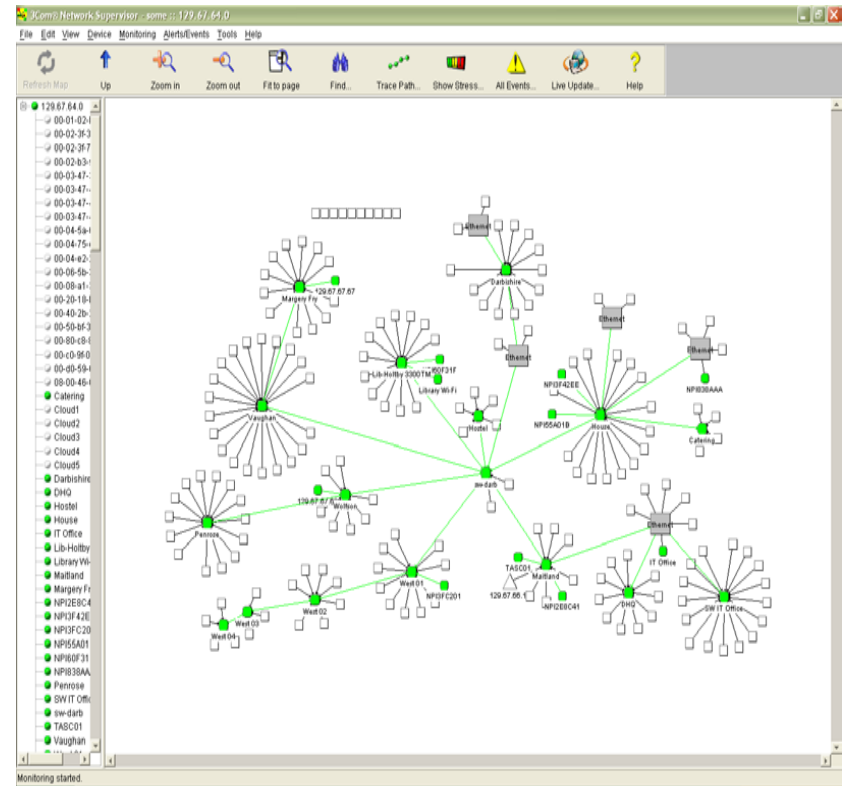
eTrust Intrusion Detection



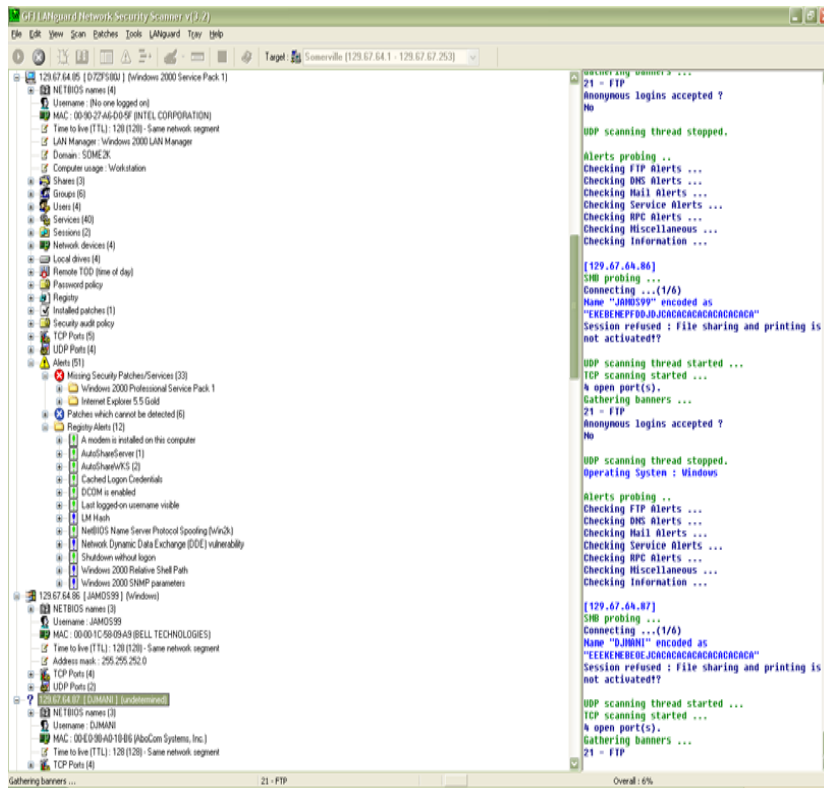
- Providing real-time, non-intrusive detection, policy-based alerts, and automatic prevention
- Integrated anti-virus engine with automatic signature updates
- Dynamic URL blocking and logging
- Predefined policies for a wide range of attacks
- Comprehensive built-in reports

3Com Network Supervisor

- Network management utility for managing 3com hubs and switches
- It's free, unless you want the advanced functions
- Auto Detects network structure, well almost



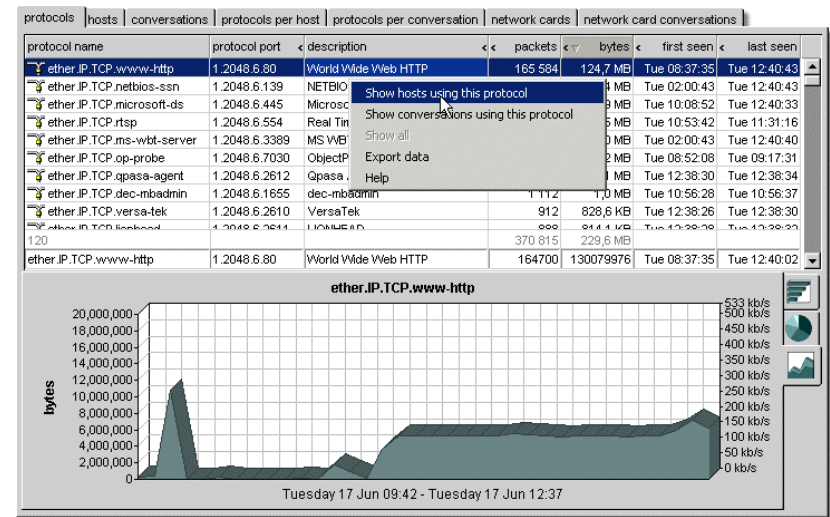
GFI LANguard Network Scanner



- Free version available
- Purchase for extra functions including patching capability
- Will scan a subnet at timed intervals
- Produces html reports: [demo report](#)

Network Probe

- Free software probe
- Needs to be placed where it can sniff the network traffic
- Works on windows using a web interface



Hardware Tools

- Fibre & Copper Taps
- Network Analysers
- IDS Appliances
- Firewall Appliances

Software Sites

- WS_Ping_ProPack - http://www.ipswitch.com/Products/WS_Ping/index.html
- XploiterStat Lite - <http://www.xploiter.com/tambu/totostat.shtml>
- Sophos Anti-Virus – <http://www.sophos.com/>
- MAILsweeper - <http://www.mimesweeper.com/>
- Elron Firewall - <http://www.elronsoftware.com/enterprise/cvfirewall.htm>
- eTrust - http://www.cai.com/solutions/enterprise/etrust/intrusion_detection/
- Transcend - http://www.3com.com/prod/en_UK_EMEA/prodlist.jsp?tab=cat&cat=65
- Network Probe - <http://www.objectplanet.com/Probe/>

Documents to Read

Oxford University's Computer Usage Rules and Etiquette

<http://www.ox.ac.uk/it/rules/>

Somerville Rules for Computer Use

http://www.some.ox.ac.uk/it/cp_rules.html

Contact Information

Christopher Bamber
IT Systems Manager
Somerville College, OX2 6HD
E-mail: chris.bamber@some.ox.ac.uk
Tel: 01865 2 70661