Security Precautions at La Trobe University, Bendigo Campus

How we track/locate infected machines

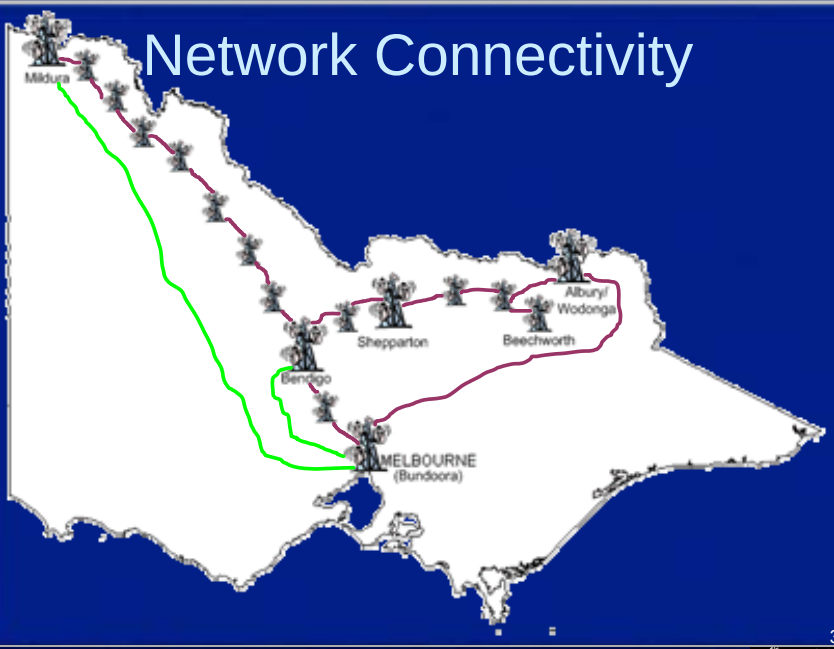
Presented by **Russell Bovaird**

Brief History

- School of Mines - 1873
- Teacher's College and Bendigo Institute of Technology amalgamated to form
  - Bendigo College of Advanced Education - 1976
- University College of Northern Victoria - 1991
- La Trobe University - 1994
- For more information see: http://www.latrobe.edu.au/bg/ben-his.html

2

Network Connectivity



3

LA TROBE UNIVERSITY

Network Equipment

- Total Cisco Environment
- Core Network
  - 6500 routers
  - 4510 switches
- Mainly 3750s at floor levels

4

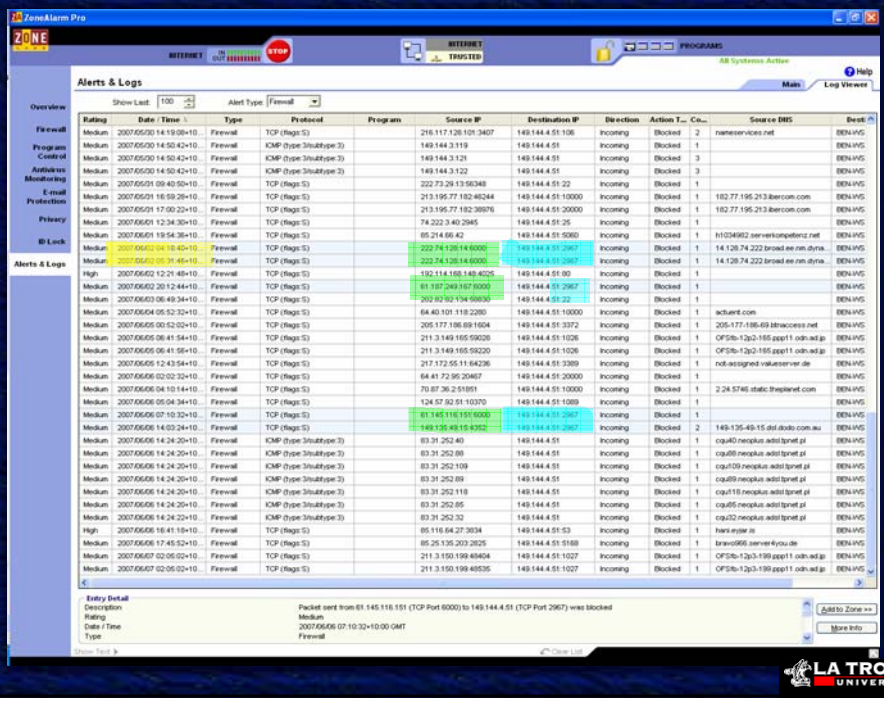
LA TROBE UNIVERSITY

Utilities

- Zone Alarm
  - Good logging facility
  - Easy viewing of logs
  - Commercial

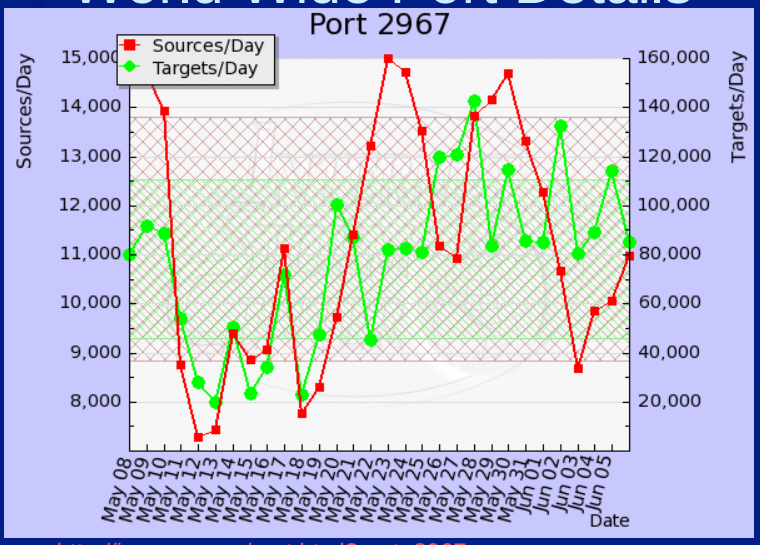
5

LA TROBE UNIVERSITY



LA TROBE UNIVERSITY

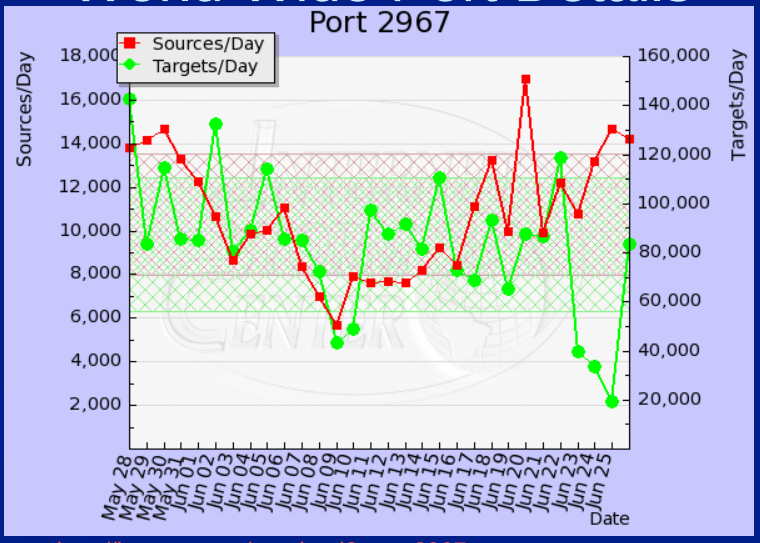
World Wide Port Details



Source: http://isc.sans.org/port.html?port=2967

7

World Wide Port Details



Source: http://isc.sans.org/port.html?port=2967

8

Utilities

- NBTSTAT
  - Windows only - Displays protocol statistics and current TCP/IP connections using NBT (NetBIOS over TCP/IP) – changed in XP SP2 and does not list user
  - Built into Windows operating system

9

LA TROBE UNIVERSITY

Nbtstat Output

Windows XP SP2

C:\>nbtstat -A 192.168.0.25

Local Area Connection:
Node IpAddress: [192.168.0.51] Scope Id: [ ]

NetBIOS Remote Machine Name Table

Name	Type	Status
BEN-LAB25	<00> UNIQUE	Registered
STUDENTS	<00> GROUP	Registered
BEN-LAB25	<20> UNIQUE	Registered
STUDENTS	<1E> GROUP	Registered

MAC Address = 00-12-3F-C0-99-F9

Windows 2000/XP SP1

C:\>nbtstat -A 192.168.0.153

Local Area Connection:
Node IpAddress: [192.168.0.51] Scope Id: [ ]

NetBIOS Remote Machine Name Table

Name	Type	Status
BEN-WS199700	<00> UNIQUE	Registered
LTU Domain	<00> GROUP	Registered
BEN-WS199700	<03> UNIQUE	Registered
BEN-WS199700	<20> UNIQUE	Registered
BEN-WS199700$	<03> UNIQUE	Registered
LTU Domain	<1E> GROUP	Registered
BRUBBLE	<03> UNIQUE	Registered

MAC Address = 00-D4-23-0D-C8-55

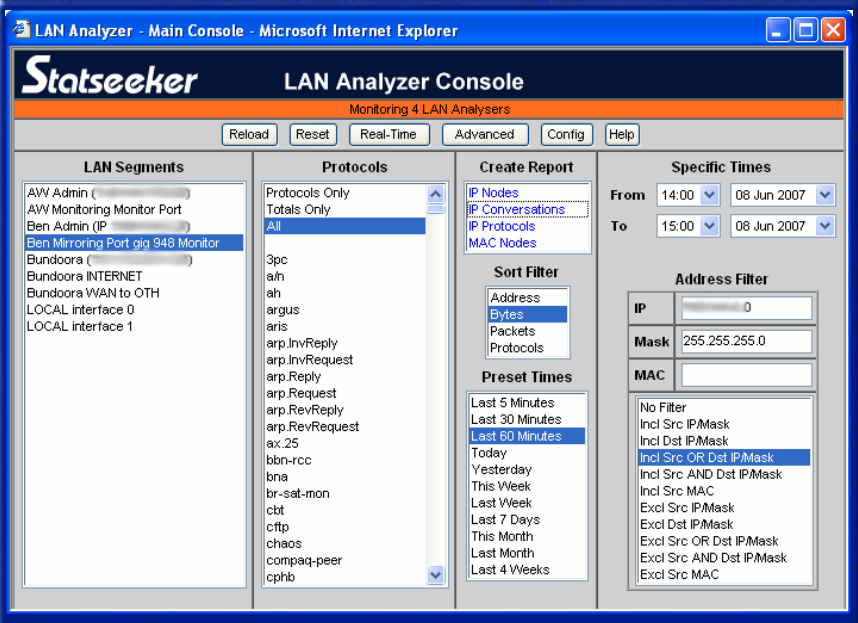
10

LA TROBE UNIVERSITY

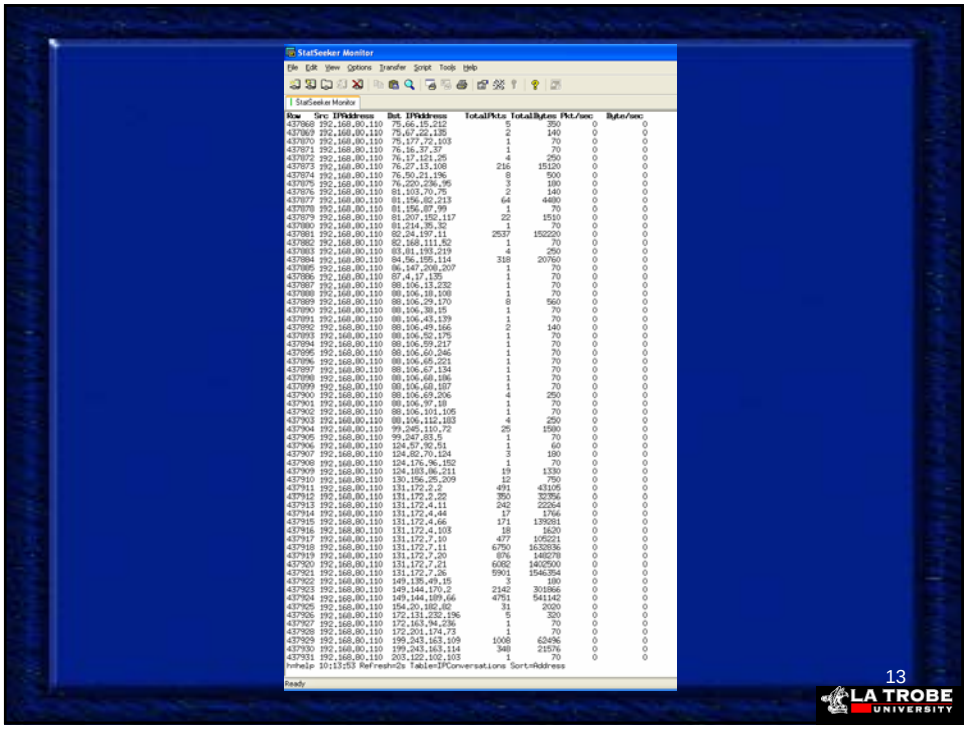
Utilities

- StatSeeker
  - Shows traffic on the monitored port
  - Ingress and egress to the Bendigo Campus
  - Commercial

11



12

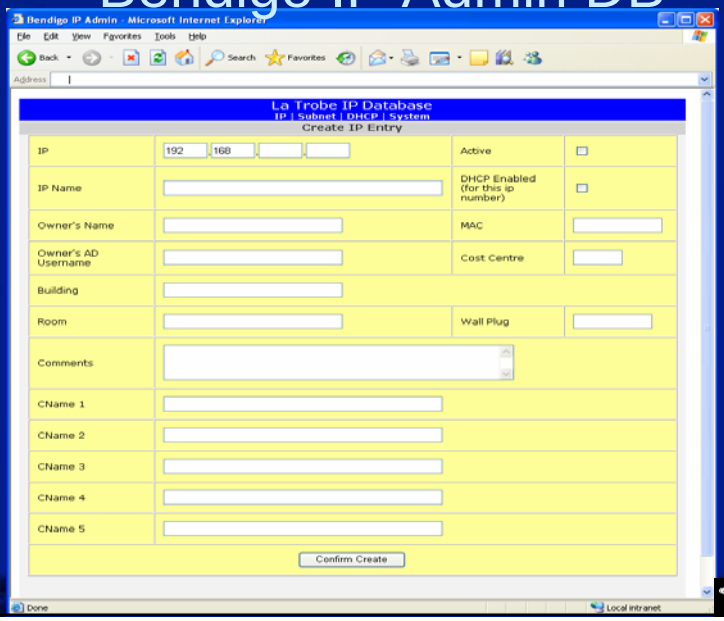


LA TROBE UNIVERSITY

Bendigo IP Admin DB

LA TROBE UNIVERSITY

Bendigo IP Admin DB



15

LA TROBE UNIVERSITY

Login Script

- Date
- Time
- AD username
- Name
- IP Number
- AD Computer Name
- Operating System
- Administrator of Machine?
- Service Pack details
- Free HD Space
- Speed of Processor
- Memory on Machine
- MAC Address

2007/05/17,15:23:51,jstone,John Stone,192.168. 0. 26,BEN-WS781824,OS='Windows XP Professional',Admin=No,SP=2,MbFree=10824,Mhz=2793,Mem=503,Mac=000D7EA4D477

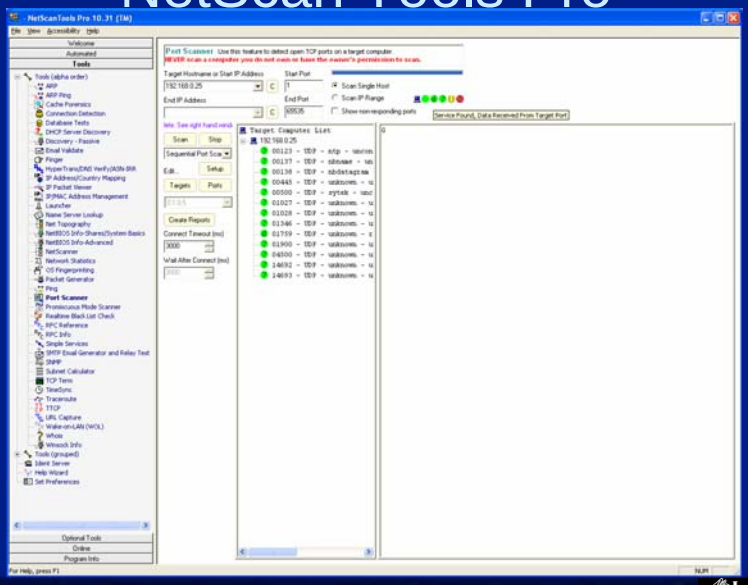
2007/05/17,15:25:50,fflintstone,Fredrick Flintstone,192.168. 0.132,BEN-WS688753,OS='Windows XP Professional',Admin=No,SP=2,MbFree=8112,Mhz=1494,Mem=511,Mac=00A6235DBE58

2007/05/17,15:26:47,erubble,Elizabeth Rubble,192.168. 0.105,BEN-WS902359,OS='Windows XP Professional',Admin=Yes,SP=2,MbFree=99160,Mhz=2990,Mem=2045,Mac=001E8BADFAFC

16

LA TROBE UNIVERSITY

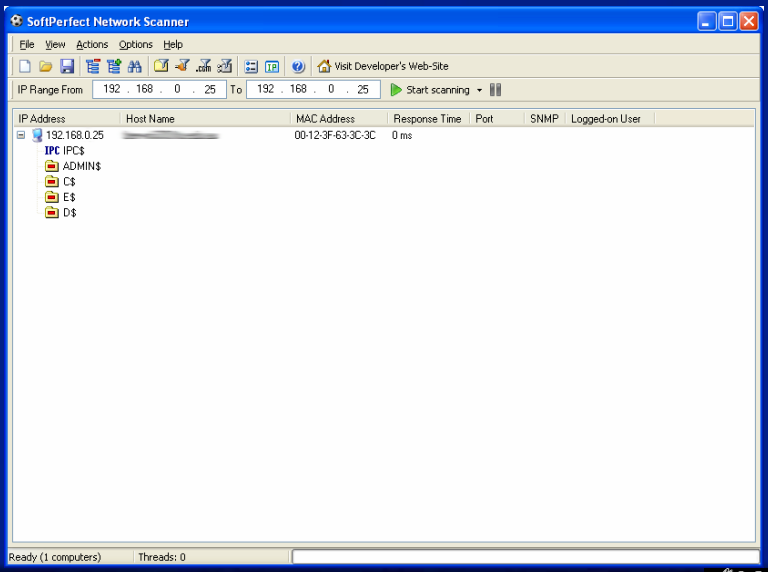
NetScan Tools Pro



17

LA TROBE UNIVERSITY

SoftPerfect Network Scanner



18

LA TROBE UNIVERSITY

Precautionary Resources

- SUS Updater
  - Automatically dispenses MS updates
- Anti Virus Software – Sophos
- Sophos PureMessage – Email
  - Spam & Virus Filtering

19

LA TROBE UNIVERSITY

Sophos PureMessage Statistics

	March	April
Legit email	905,863	406,267
Spam	4,390,340	1,991,935
Virus	25,657	8,515

	May	June
Legit email	381,359	749,554
Spam	1,175,697	2,248,184
Virus	3,025	5,540

20

LA TROBE UNIVERSITY

Other Resources Used

- Cisco PIX firewall
- Monitoring Analysis Response System (MARS)
  - Alerts and rules for suspicious activity

21

LA TROBE UNIVERSITY

Takedown Policy

- 24 hours to remove from Network
- If not done within 72 hours port disabled
- Immediate removal if a threat to ICT environment
- Analysis of device to be undertaken
- Device should be rebuilt **NOT** repaired
- Needs approval to be reconnected to network

22

LA TROBE UNIVERSITY

Contact Details

Russell Bovaird

r.bovaird@latrobe.edu.au


(03) 5444 7247


(03) 5444 7612


ICT – Computer Services Centre
La Trobe University
PO Box 199
Bendigo 3552
Victoria Australia