

Security Precautions at La Trobe University, Bendigo Campus

How we track/locate infected machines

Presented by **Russell Bovaird**

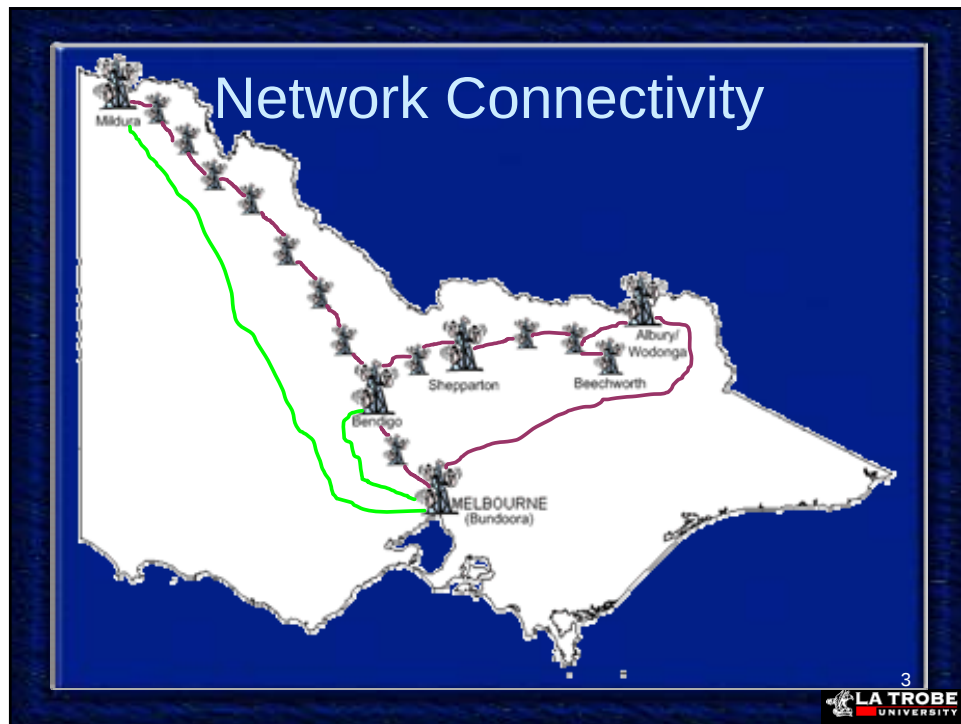


Brief History

- 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 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



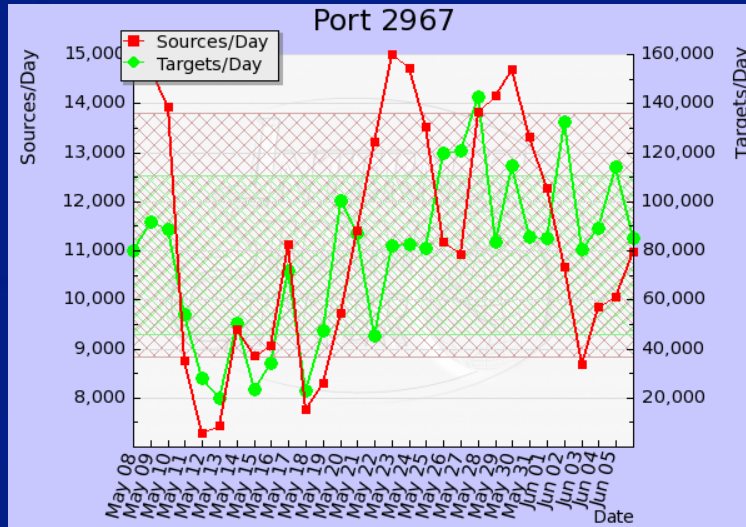
The screenshot displays the ZoneAlarm Pro interface with the 'Alerts & Logs' window open. The window shows a list of network events with columns for Rating, Date/Time, Type, Protocol, Program, Source IP, Destination IP, Direction, Action, Count, Source DNS, and Dest. The interface includes a sidebar with navigation options like Overview, Firewall, Program Control, Antivirus, Monitoring, E-mail Protection, Privacy, and Bit Lock. At the bottom, there is an 'Entry Detail' section showing a specific log entry: 'Packet sent from 61.145.116.151 (TCP Port 6000) to 145.144.4.51 (TCP Port 2967) was blocked'.

Rating	Date/Time	Type	Protocol	Program	Source IP	Destination IP	Direction	Action	Count	Source DNS	Dest
Medium	2007/06/01 14:10:08+10	Firewall	TCP (Flags S)		216.117.126.101.3407	145.144.4.51.106	Incoming	Blocked	2	nameservices.net	BEN.VMS
Medium	2007/06/01 14:50:42+10	Firewall	KMP (type 3) (type 3)		145.144.4.51.119	145.144.4.51	Incoming	Blocked	1		BEN.VMS
Medium	2007/06/01 14:50:42+10	Firewall	KMP (type 3) (type 3)		145.144.4.51.121	145.144.4.51	Incoming	Blocked	3		BEN.VMS
Medium	2007/06/01 14:50:42+10	Firewall	KMP (type 3) (type 3)		145.144.4.51.122	145.144.4.51	Incoming	Blocked	3		BEN.VMS
Medium	2007/06/01 09:40:50+10	Firewall	TCP (Flags S)		222.73.29.13.56348	145.144.4.51.22	Incoming	Blocked	1		BEN.VMS
Medium	2007/06/01 16:50:26+10	Firewall	TCP (Flags S)		213.195.77.192.40244	145.144.4.51.10000	Incoming	Blocked	1	192.77.196.213.bercom.com	BEN.VMS
Medium	2007/06/01 17:00:22+10	Firewall	TCP (Flags S)		213.195.77.192.38976	145.144.4.51.20000	Incoming	Blocked	1	192.77.196.213.bercom.com	BEN.VMS
Medium	2007/06/01 12:34:30+10	Firewall	TCP (Flags S)		74.222.3.40.2945	145.144.4.51.25	Incoming	Blocked	1		BEN.VMS
Medium	2007/06/01 14:54:26+10	Firewall	TCP (Flags S)		65.214.69.42	145.144.4.51.6000	Incoming	Blocked	1	10204902.scrv.net.computel.net	BEN.VMS
Medium	2007/06/01 14:14:45+10	Firewall	TCP (Flags S)		222.74.126.14.6000	145.144.4.51.2967	Incoming	Blocked	1	14.126.74.222.broad.en.nm.dyns	BEN.VMS
Medium	2007/06/01 14:14:45+10	Firewall	TCP (Flags S)		222.74.126.14.6000	145.144.4.51.2967	Incoming	Blocked	1	14.126.74.222.broad.en.nm.dyns	BEN.VMS
High	2007/06/02 12:21:45+10	Firewall	TCP (Flags S)		192.114.166.149.4025	145.144.4.51.80	Incoming	Blocked	1		BEN.VMS
Medium	2007/06/02 20:12:44+10	Firewall	TCP (Flags S)		61.187.249.167.6000	145.144.4.51.2967	Incoming	Blocked	1		BEN.VMS
Medium	2007/06/02 08:49:34+10	Firewall	TCP (Flags S)		202.92.92.714.6000	145.144.4.51.22	Incoming	Blocked	1		BEN.VMS
Medium	2007/06/04 05:52:32+10	Firewall	TCP (Flags S)		64.40.101.119.2080	145.144.4.51.10000	Incoming	Blocked	1	actent.com	BEN.VMS
Medium	2007/06/05 00:52:02+10	Firewall	TCP (Flags S)		205.177.186.89.1604	145.144.4.51.3372	Incoming	Blocked	1	205.177.186.89.1604.com	BEN.VMS
Medium	2007/06/05 08:41:54+10	Firewall	TCP (Flags S)		211.3.149.105.5920	145.144.4.51.1026	Incoming	Blocked	1	CF5th-12q-188.ppt11.cdn.ad.jp	BEN.VMS
Medium	2007/06/05 08:41:58+10	Firewall	TCP (Flags S)		211.3.149.105.5920	145.144.4.51.1026	Incoming	Blocked	1	CF5th-12q-188.ppt11.cdn.ad.jp	BEN.VMS
Medium	2007/06/05 12:43:54+10	Firewall	TCP (Flags S)		217.172.51.114.6296	145.144.4.51.3389	Incoming	Blocked	1	rdi.acsgrind.rakuten.co.jp	BEN.VMS
Medium	2007/06/06 02:02:32+10	Firewall	TCP (Flags S)		64.41.73.96.20467	145.144.4.51.20000	Incoming	Blocked	1		BEN.VMS
Medium	2007/06/06 04:10:14+10	Firewall	TCP (Flags S)		70.87.36.2.51851	145.144.4.51.10000	Incoming	Blocked	1	2.24.5746.static.thepire.com	BEN.VMS
Medium	2007/06/06 05:04:34+10	Firewall	TCP (Flags S)		124.57.92.51.10370	145.144.4.51.1089	Incoming	Blocked	1		BEN.VMS
Medium	2007/06/06 07:10:32+10	Firewall	TCP (Flags S)		61.145.116.151.6000	145.144.4.51.2967	Incoming	Blocked	1		BEN.VMS
Medium	2007/06/06 14:02:24+10	Firewall	TCP (Flags S)		145.144.4.51.6000	145.144.4.51.2967	Incoming	Blocked	2	145.135.45.15.dsl.adsls.com.au	BEN.VMS
Medium	2007/06/06 14:24:20+10	Firewall	KMP (type 3) (type 3)		83.31.262.40	145.144.4.51	Incoming	Blocked	1	caq00.nepplus.adsl.tnet.pl	BEN.VMS
Medium	2007/06/06 14:24:20+10	Firewall	KMP (type 3) (type 3)		83.31.262.89	145.144.4.51	Incoming	Blocked	1	caq00.nepplus.adsl.tnet.pl	BEN.VMS
Medium	2007/06/06 14:24:20+10	Firewall	KMP (type 3) (type 3)		83.31.262.109	145.144.4.51	Incoming	Blocked	1	caq00.nepplus.adsl.tnet.pl	BEN.VMS
Medium	2007/06/06 14:24:20+10	Firewall	KMP (type 3) (type 3)		83.31.262.89	145.144.4.51	Incoming	Blocked	1	caq00.nepplus.adsl.tnet.pl	BEN.VMS
Medium	2007/06/06 14:24:20+10	Firewall	KMP (type 3) (type 3)		83.31.262.119	145.144.4.51	Incoming	Blocked	1	caq00.nepplus.adsl.tnet.pl	BEN.VMS
Medium	2007/06/06 14:24:20+10	Firewall	KMP (type 3) (type 3)		83.31.262.85	145.144.4.51	Incoming	Blocked	1	caq00.nepplus.adsl.tnet.pl	BEN.VMS
Medium	2007/06/06 14:24:20+10	Firewall	KMP (type 3) (type 3)		83.31.262.32	145.144.4.51	Incoming	Blocked	1	caq00.nepplus.adsl.tnet.pl	BEN.VMS
High	2007/06/06 16:41:18+10	Firewall	TCP (Flags S)		85.116.64.27.3034	145.144.4.51.53	Incoming	Blocked	1	hars.euro.it	BEN.VMS
Medium	2007/06/06 17:45:52+10	Firewall	TCP (Flags S)		85.25.135.203.2825	145.144.4.51.5188	Incoming	Blocked	1	brav000.server.kyoudo	BEN.VMS
Medium	2007/06/07 02:05:02+10	Firewall	TCP (Flags S)		211.3.160.199.48454	145.144.4.51.1027	Incoming	Blocked	1	CF5th-12q-188.ppt11.cdn.ad.jp	BEN.VMS
Medium	2007/06/07 02:05:02+10	Firewall	TCP (Flags S)		211.3.160.199.49535	145.144.4.51.1027	Incoming	Blocked	1	CF5th-12q-188.ppt11.cdn.ad.jp	BEN.VMS

Entry Detail
 Description: Packet sent from 61.145.116.151 (TCP Port 6000) to 145.144.4.51 (TCP Port 2967) was blocked
 Rating: Medium
 Date / Time: 2007/06/06 07:10:32+10:00 GMT
 Type: Firewall



World Wide Port Details

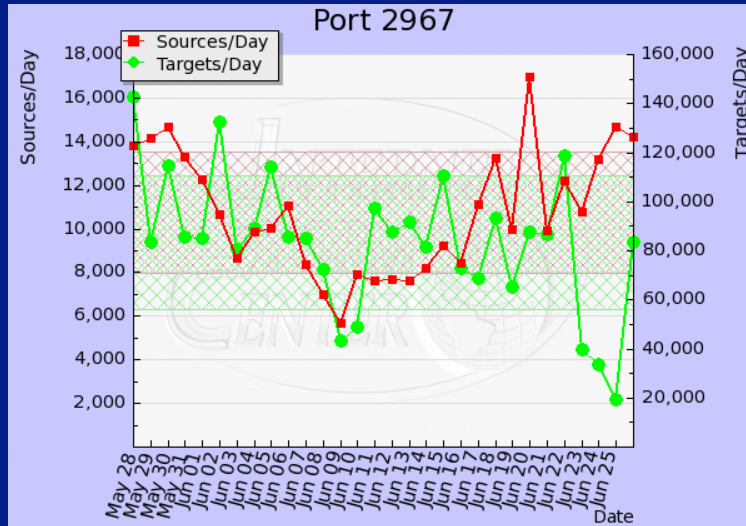


Source: <http://isc.sans.org/port.html?port=2967>

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



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



Utilities

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



StatSeer Monitor

File Edit View Options Database Script Tools Help

StatSeer Monitor

Row	Src IP Address	Dest IP Address	TotalPkts	TotalBytes	Pkts/sec	Bytes/sec
437068	192.168.0.110	75.66.152.212	5	250	0	0
437069	192.168.0.110	75.66.152.212	1	140	0	0
437070	192.168.0.110	75.177.72.103	1	70	0	0
437071	192.168.0.110	76.18.37.37	4	250	0	0
437072	192.168.0.110	76.17.121.25	8	500	0	0
437073	192.168.0.110	76.27.13.108	216	15120	0	0
437074	192.168.0.110	76.50.21.196	3	180	0	0
437075	192.168.0.110	76.200.238.95	3	180	0	0
437076	192.168.0.110	81.103.70.75	2	140	0	0
437077	192.168.0.110	81.156.82.213	64	4480	0	0
437078	192.168.0.110	81.156.87.99	1	70	0	0
437079	192.168.0.110	81.207.152.117	22	1510	0	0
437080	192.168.0.110	82.144.39.32	1	70	0	0
437081	192.168.0.110	82.54.197.11	2537	152020	0	0
437082	192.168.0.110	82.169.111.82	1	70	0	0
437083	192.168.0.110	83.81.193.219	4	280	0	0
437084	192.168.0.110	84.56.155.114	310	20760	0	0
437085	192.168.0.110	86.147.208.207	1	70	0	0
437086	192.168.0.110	87.4.17.139	1	70	0	0
437087	192.168.0.110	88.142.13.232	1	70	0	0
437088	192.168.0.110	88.106.18.108	8	560	0	0
437089	192.168.0.110	88.156.29.170	1	70	0	0
437090	192.168.0.110	88.106.38.15	1	70	0	0
437091	192.168.0.110	88.106.43.139	1	70	0	0
437092	192.168.0.110	88.106.49.166	2	140	0	0
437093	192.168.0.110	88.106.52.175	1	70	0	0
437094	192.168.0.110	88.106.59.217	1	70	0	0
437095	192.168.0.110	88.106.65.246	1	70	0	0
437096	192.168.0.110	88.106.65.221	1	70	0	0
437097	192.168.0.110	88.106.67.134	1	70	0	0
437098	192.168.0.110	88.106.68.186	1	70	0	0
437099	192.168.0.110	88.106.69.107	1	70	0	0
437100	192.168.0.110	88.106.69.206	4	280	0	0
437101	192.168.0.110	88.106.97.18	1	70	0	0
437102	192.168.0.110	88.106.101.105	1	70	0	0
437103	192.168.0.110	88.106.112.103	1	220	0	0
437104	192.168.0.110	89.245.10.7	25	1500	0	0
437105	192.168.0.110	89.247.83.5	1	70	0	0
437106	192.168.0.110	124.27.42.51	1	60	0	0
437107	192.168.0.110	124.82.70.124	3	180	0	0
437108	192.168.0.110	124.176.96.152	1	70	0	0
437109	192.168.0.110	124.183.86.211	19	1330	0	0
437110	192.168.0.110	135.156.25.209	12	780	0	0
437111	192.168.0.110	131.172.2.2	491	43105	0	0
437112	192.168.0.110	131.172.2.22	380	32366	0	0
437113	192.168.0.110	131.172.4.11	242	22264	0	0
437114	192.168.0.110	131.172.4.48	17	1766	0	0
437115	192.168.0.110	131.172.4.66	171	139281	0	0
437116	192.168.0.110	131.172.4.103	18	1630	0	0
437117	192.168.0.110	131.172.7.10	477	105221	0	0
437118	192.168.0.110	131.172.7.11	6790	1633936	0	0
437119	192.168.0.110	131.172.7.20	576	148278	0	0
437120	192.168.0.110	131.172.7.21	6082	1403500	0	0
437121	192.168.0.110	131.172.7.28	5901	1546354	0	0
437122	192.168.0.110	149.138.49.15	3	180	0	0
437123	192.168.0.110	149.144.187.2	2142	301866	0	0
437124	192.168.0.110	149.144.187.66	4751	541142	0	0
437125	192.168.0.110	154.20.185.45	31	2030	0	0
437126	192.168.0.110	172.131.232.196	5	320	0	0
437127	192.168.0.110	172.161.96.258	1	70	0	0
437128	192.168.0.110	172.201.174.73	1	70	0	0
437129	192.168.0.110	196.243.163.108	1008	62846	0	0
437130	192.168.0.110	199.243.163.114	348	21976	0	0
437131	192.168.0.110	201.152.152.103	1	70	0	0

Ready

13

LA TROBE UNIVERSITY

Bendigo IP Admin DB

Bendigo IP Admin - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites

Address

La Trobe IP Database
IP / Subnet / DHCP / System

IP Search Criteria

IP Number (e.g. 149.244.2.2) 192 168 . .

IP Name (* to show all)

Subnet (e.g. 149.244.32) 192 168 .

Owner's Name

Owner's Active Directory Username

Cost Centre

MAC (e.g. 0000A7665544)

Building

Search Report Create

Copyright © La Trobe University 2003. All rights reserved.

14

LA TROBE UNIVERSITY

Bendigo IP Admin DB

La Trobe IP Database
IP | Subnet | DHCP | System
Create IP Entry

IP	192.168	Active	☐
IP Name		DHCP Enabled (for this ip number)	☐
Owner's Name		MAC	
Owner's AD Username		Cost Centre	
Building			
Room		Wall Plug	
Comments			
CName 1			
CName 2			
CName 3			
CName 4			
CName 5			

Confirm Create

15



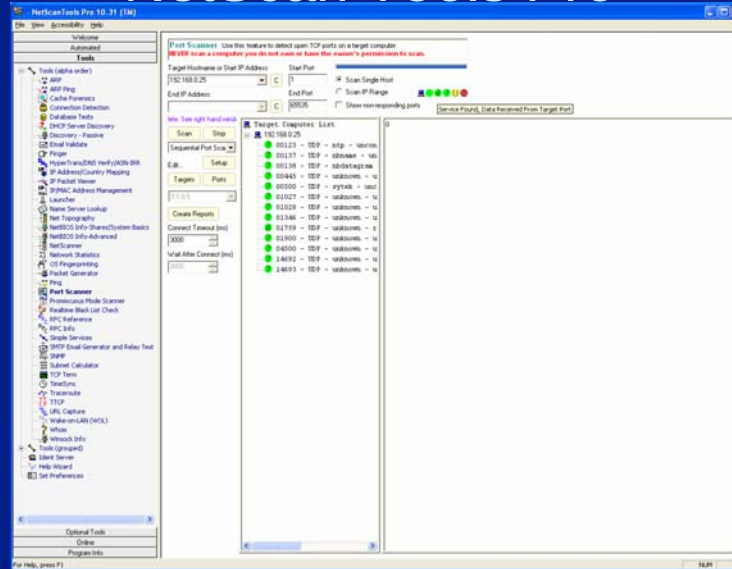
Login Script

- 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



NetScan Tools Pro



Precautionary Resources

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

19



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



Other Resources Used

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

21



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



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