

Mobile Computing in Libraries

Mark Round



Agenda

- What is it?
- Brief History
- The Problem
- The current solution
- The Future

What is “mobile computing”

- The ability for a library reader to sit at a desk in a library, connect their laptop and access catalogues, electronic resources and the internet.

Brief History

- Started out in the Law Library in 1996.
- Originally named “Open Access Ethernet”
- Users were not allowed to use their own ethernet card
- Users were issued with a bootable floppy which contained IP address etc.

History Continued

- Eventually user network cards were allowed and DHCP was used.
- With this came registering MAC addresses
- Eventually registration was scrapped and open DHCP was used
- 2002 – 2004 saw a massive increase of virus', worms, and questionable downloads. Restrictions were needed.

Other attempts at restriction

- All machines allowed and use “network black holes”.
- All machines denied and scanning took place on separate scanning station before being allowed to use networks. This is basically where the current system was derived from.

The Problem we faced in designing the current system

- Security issues
- University members able to use the libraries: circa 22,000
- non-University members able to use the libraries: circa 22,000
- Data points available to readers: 2,000ish

The Problem we faced in designing the current system

- No of technical staff to support readers = 0 (zero)
- Many locations
- Ideally no change to networks
- Small network cabinets
- Limited cable Infrastructure
- Very little money

The Solution – must be:

- Simple
- Updateable
- Manageable
- Scalable
- Able to restrict users
- No major change to network infrastructure

What would you do?



What we do

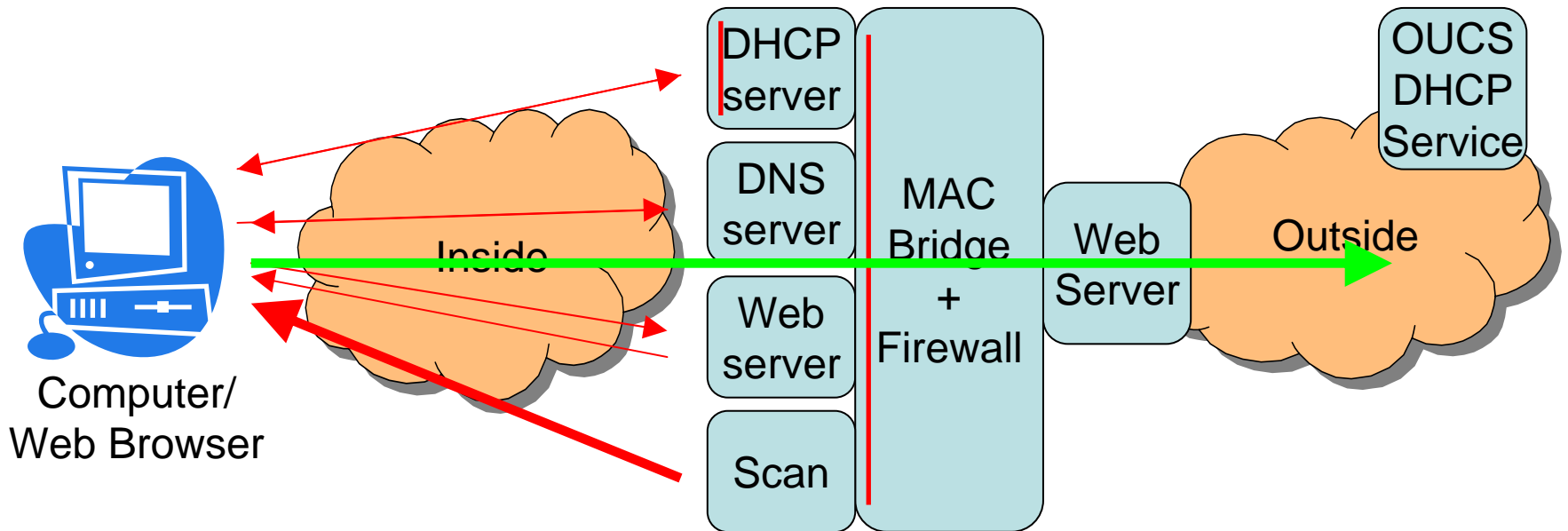
- Deny Everyone
- Scan each laptop
- If scan passes allow use of network
- If scan fails deny use of network and advise the user of the reason(s)
- Rescan everyone, every 7 days

User Requirements

- Computer
- Ethernet port
- Ethernet cable
- IP and DNS set to DHCP assigned

How it Works

~~How it works: user receives a page from an internal web server going through a proxy page~~



Technology Used

- OpenBSD (nice and simple for creating a MAC bridge)
- Apache for Web servers
- Nessus for scanning
- Perl
- OUCS DHCP for public addresses

User Interface

- Simple
- Informative



Oxford University Library Services

Your computer needs to be scanned

Before we connect your computer to the network, we need to scan it for vulnerabilities.

This scan will not access any of the files on your computer.

If your computer is running Windows XP and you have not installed Service Pack 2, it will most likely fail our scan. You can download SP2 from [here](#).

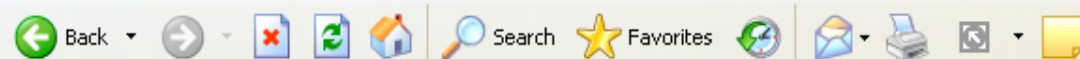
If you have a Mac running OS X and you don't have version 10.4.3, it may fail our scan. You can download a combo update from [here](#) that will update version 10.4 or later.

[Click here to begin the scan](#)





Your IP address: 10.0.0.120

Your hardware address: 00:b0:d0:f4:60:3b

Version: \$Id: scan-status.pl,v 1.16 2005/11/28 15:01:37 chardi Exp \$



Address  http://scanner/scan-status.pl?start=1

  Go  Links 

Oxford University Library Services

Beginning the scan...

Your IP address: 10.0.0.120

Your hardware address: 00:b0:d0:f4:60:3b

Version: \$Id: scan-status.pl,v 1.16 2005/11/28 15:01:37 chardi Exp \$

Address <http://scanner/scan-status.pl?start=1>

Go

Links >>

Oxford University Library Services

Your computer is being scanned -- please wait

In order to protect both our systems and those of other readers, your computer is being scanned for vulnerabilities that could permit malicious activity. This should take around five minutes.

If nothing untoward is found, access will be granted automatically.

This page will refresh automatically every 15 seconds.

Your IP address: 10.0.0.120

Your hardware address: 00:b0:d0:f4:60:3b

Version: \$Id: scan-status.pl,v 1.16 2005/11/28 15:01:37 chardi Exp \$



Oxford University Library Services

Your computer has been barred from the network

A scan of your computer has revealed weaknesses that leave your machine vulnerable to malicious activity. It may already have been compromised.

To protect both our systems and those of other readers, we have blocked access to the network from your computer.

You can [view the results of the scan](#) which may help you fix the problems. Some technical knowledge is required to interpret the results.

If you have fixed the problems, you can [restart the scan now](#).

If your computer is running Windows XP and you have not installed Service Pack 2, it will most likely fail our scan. You can download SP2 from [here](#).

If you have a Mac running OS X and you don't have version 10.4.3, it may fail our scan. You can download a combo update from [here](#) that will update version 10.4 or later.

Your IP address: 10.0.0.120

Your hardware address: 00:b0:d0:f4:60:3b

IT Services, Oxford University Library Services, 11/03/2005 11:01:37 AM

Done

Local intranet

start

Oxford University Lib...

Microsoft PowerPoint ...

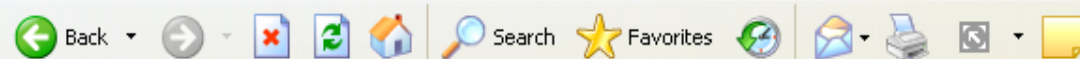
12:42

Oxford University Library Services

Scan failure results for 00:b0:d0:f4:60:3b

Only the problems highlighted in red need to be fixed in order to pass the scan. Any other issues listed are acceptable to us, but you may want to address them anyway.

00.b0.d0.f4.60.3b	general/tcp	19506	NOTE	Information about this scan : ;Nessus version : 2.2.7;Plugin feed version : 200606202215;Type of plugin feed : B delay);Scanner IP : 10.0.0.254;Port scanner(s) : nessus_tcp_scanner ;Port range : default;Thorough tests : no;Exp level : 1;Report Verbosity : 1;Safe checks : yes;Max hosts : 20;Max checks : 20;Scan Start Date : 2006/6/21 12
00.b0.d0.f4.60.3b	blackjack (1025/tcp)	13852	REPORT	;Synopsis ;;Arbitrary code can be executed on the remote host;;Description ;;There is a flaw in the Task Sched allow a;remote attacker to execute code remotely. There are many attack vectors;for this flaw. An attacker, expl either ;have the ability to connect to the target machine or be able to coerce a;local user to either install a .job file website;;Solution ;;Microsoft has released a set of patches for Windows 2000, XP and 2003 ;;http://www.microsoft.com/technet/security/bulletin/ms04-022.mspx;;Risk factor ;;Critical / CVSS Base S (AV:R/AC:L/Au:NR/C:C/A:C/I:C/B:N);CVE : CVE-2004-0212;BID : 10708;
00.b0.d0.f4.60.3b	microsoft-ds (445/tcp)	18028	REPORT	;Synopsis ;;Arbitrary code can be executed on the remote host due to a flaw in the ;TCP/IP stack;;Description : version of Windows which has a flaw in its TCP/IP;stack;;The flaw may allow an attacker to execute arbitrary co on the remote host, or to perform a denial of service attack;against the remote host;;Proof of concept code is av Service against;a vulnerable system;;Solution ;;Microsoft has released a set of patches for Windows 2000, XP 2003 ;;http://www.microsoft.com/technet/security/bulletin/ms05-019.mspx;;Risk factor : ;High / CVSS Base Sec (AV:R/AC:L/Au:NR/C:P/A:C/I:P/B:A);CVE : CVE-2005-0048, CVE-2004-0790, CVE-2004-1060, CVE-20 0688;BID : 13124, 13116;
00.b0.d0.f4.60.3b	microsoft-ds	18500	REPORT	;Synopsis ;;Arbitrary code can be executed on the remote host due to a flaw in the ;SMB implementation;;Desc of Windows contains a flaw in the Server Message;Block (SMB) implementation which may allow an attacker to



Address  http://scanner/scan-status.pl?start=1



Links >>

Oxford University Library Services

Scan complete -- no vulnerabilities found.

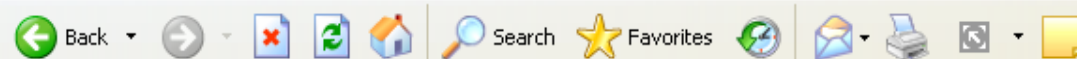
Your computer has passed our tests and will shortly have access to the network.


You will be redirected to the Oxford University home page in 60 seconds.



Your IP address: 10.0.0.120

Your hardware address: 00:b0:d0:f4:60:3b

Version: \$Id: scan-status.pl,v 1.16 2005/11/28 15:01:37 chardi Exp \$



Address  http://scanner/scan-status.pl

 Go  Links >>

Oxford University Library Services

Scan complete -- please restart your browser.

We were unable to redirect you automatically. Please restart your browser to gain network access.

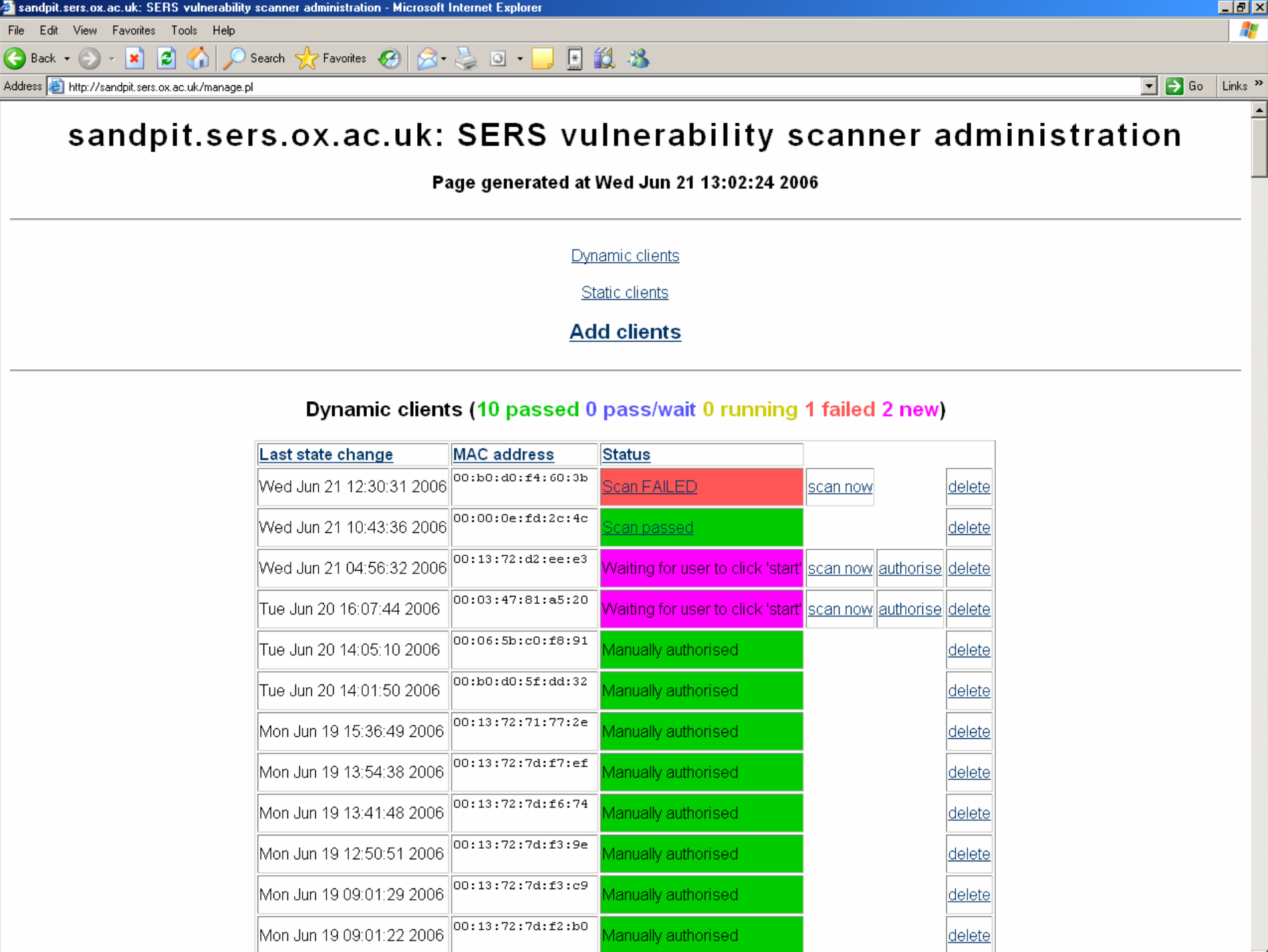
Your IP address: 10.0.0.120

Your hardware address: 00:b0:d0:f4:60:3b

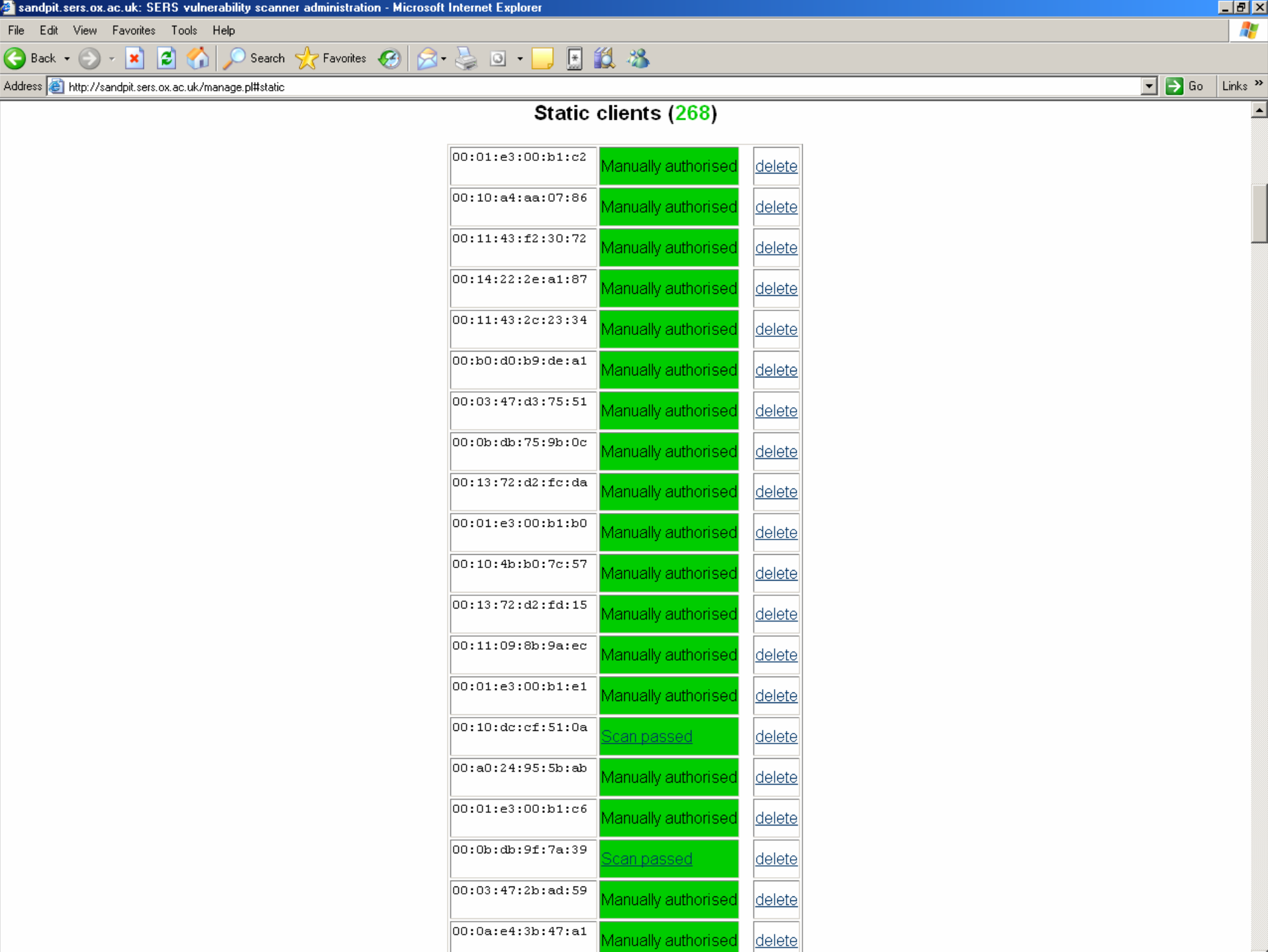
Version: \$Id: scan-status.pl,v 1.16 2005/11/28 15:01:37 chardi Exp \$

The management interface

- Add
- Remove
- Monitor



sandpit.sers.ox.ac.uk: SERS vulnerability scanner administration					
Page generated at Wed Jun 21 13:02:24 2006					
Dynamic clients					
Static clients					
Add clients					
Dynamic clients (10 passed 0 pass/wait 0 running 1 failed 2 new)					
Last state change	MAC address	Status			
Wed Jun 21 12:30:31 2006	00:b0:d0:f4:60:3b	Scan FAILED	scan now	delete	
Wed Jun 21 10:43:36 2006	00:00:0e:fd:2c:4c	Scan passed			delete
Wed Jun 21 04:56:32 2006	00:13:72:d2:ee:e3	Waiting for user to click 'start'	scan now	authorise	delete
Tue Jun 20 16:07:44 2006	00:03:47:81:a5:20	Waiting for user to click 'start'	scan now	authorise	delete
Tue Jun 20 14:05:10 2006	00:06:5b:c0:f8:91	Manually authorised			delete
Tue Jun 20 14:01:50 2006	00:b0:d0:5f:dd:32	Manually authorised			delete
Mon Jun 19 15:36:49 2006	00:13:72:71:77:2e	Manually authorised			delete
Mon Jun 19 13:54:38 2006	00:13:72:7d:f7:ef	Manually authorised			delete
Mon Jun 19 13:41:48 2006	00:13:72:7d:f6:74	Manually authorised			delete
Mon Jun 19 12:50:51 2006	00:13:72:7d:f3:9e	Manually authorised			delete
Mon Jun 19 09:01:29 2006	00:13:72:7d:f3:c9	Manually authorised			delete
Mon Jun 19 09:01:22 2006	00:13:72:7d:f2:b0	Manually authorised			delete



Static clients (268)		
00:01:e3:00:b1:c2	Manually authorised	delete
00:10:a4:aa:07:86	Manually authorised	delete
00:11:43:f2:30:72	Manually authorised	delete
00:14:22:2e:a1:87	Manually authorised	delete
00:11:43:2c:23:34	Manually authorised	delete
00:b0:d0:b9:de:a1	Manually authorised	delete
00:03:47:d3:75:51	Manually authorised	delete
00:0b:db:75:9b:0c	Manually authorised	delete
00:13:72:d2:fc:da	Manually authorised	delete
00:01:e3:00:b1:b0	Manually authorised	delete
00:10:4b:b0:7c:57	Manually authorised	delete
00:13:72:d2:fd:15	Manually authorised	delete
00:11:09:8b:9a:ec	Manually authorised	delete
00:01:e3:00:b1:e1	Manually authorised	delete
00:10:dc:cf:51:0a	Scan passed	delete
00:a0:24:95:5b:ab	Manually authorised	delete
00:01:e3:00:b1:c6	Manually authorised	delete
00:0b:db:9f:7a:39	Scan passed	delete
00:03:47:2b:ad:59	Manually authorised	delete
00:0a:e4:3b:47:a1	Manually authorised	delete

The Future

- Nessus version – issue with OpenBSD
- Central Database so users scan in one library and have access to all for 1 week
- Small libraries – Use of FroDo to deliver the same service across many small locations

Additional benefits

- Rarely appearing staff laptops are unable to compromise the network
- Stopping rogue machines is very simple

Questions for you?

- Do you do something similar?
- Do you do something completely different?
- Is 7 days for rescan too soon?
- Does such an approach change the culture of users and security?

Further Information

- <http://www.bodley.ox.ac.uk/mobile/>