GridPP
UK Computing for Particle Physics

Security: Best Practice and Monitoring

Romain Wartel

Contents

- Security Best Practice
  - Why it is important
  - How information can be spread
  - Future
- Security monitoring
  - Patching status monitoring with Yumit
  - Monitoring open ports with Scanit
  - Logging system events with syslog-ng

GridPP
UK Computing for Particle Physics

Security Best Practice

Why?

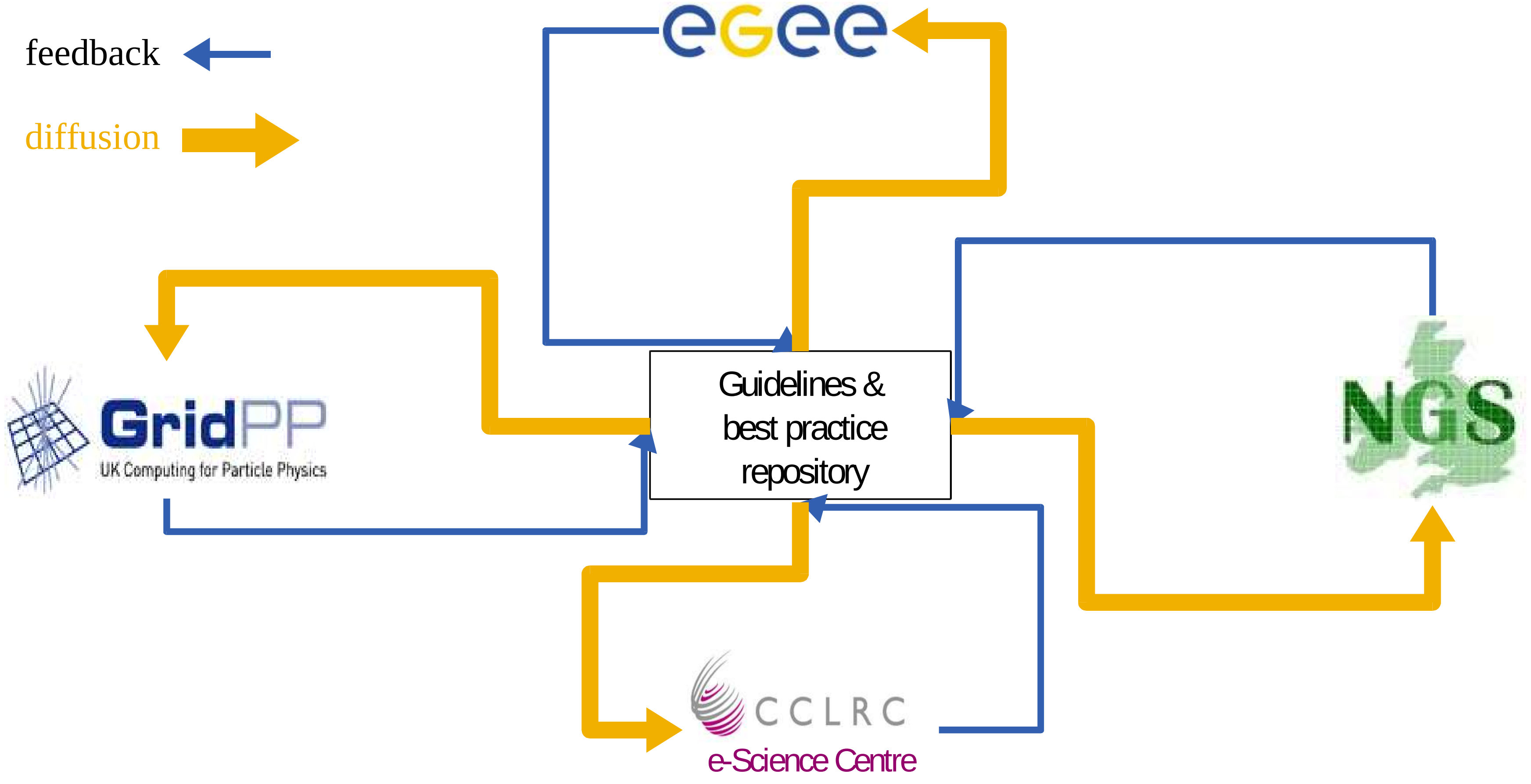
- Most sites have similar security issues
- Heterogeneous groups of systems administrators
- Experience from security incidents is extremely useful
- Good ideas should be spread amongst the community

→ Guidelines & best practice should be advertised

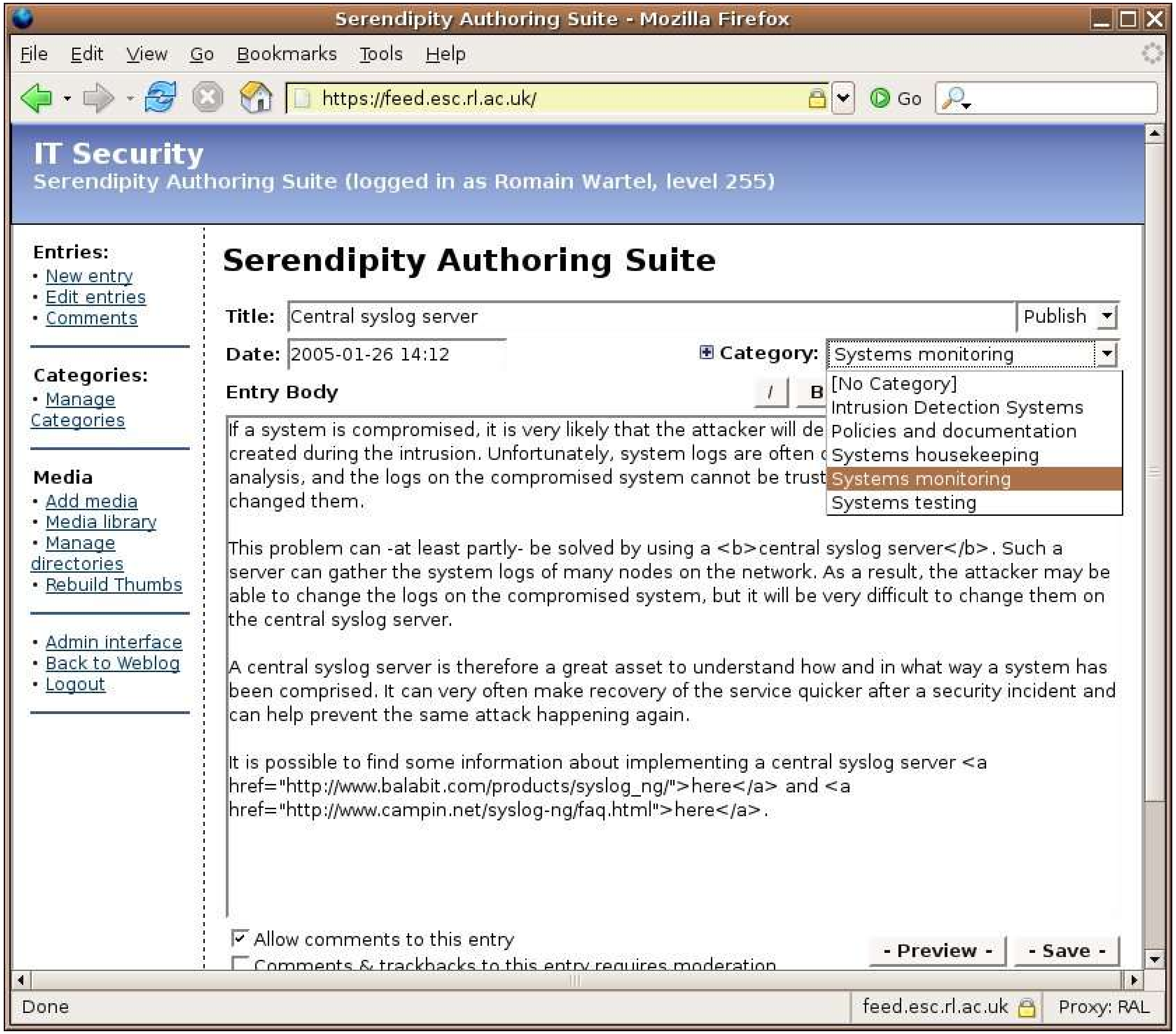
BUT

- Information must be kept up-to-date
- A single source of information is not enough
- Maintaining coherent information amongst many sites is difficult

System architecture



Authoring mechanism


Serendipity Authoring Suite - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://feed.esc.rl.ac.uk/
Go
- Preview -
- Save -
Done
feed.esc.rl.ac.uk
Proxy: RAL

IT Security

Serendipity Authoring Suite (logged in as Romain Wartel, level 255)

Entries:
- New entry
- Edit entries
- Comments

Categories:
- Manage Categories

Media
- Add media
- Media library
- Manage directories
- Rebuild Thumbs

- Admin interface
- Back to Weblog
- Logout

Serendipity Authoring Suite

Title: Central syslog server Publish

Date: 2005-01-26 14:12 **Category:** Systems monitoring

[No Category]
Intrusion Detection Systems
Policies and documentation
Systems housekeeping
Systems monitoring
Systems testing

Entry Body I B

If a system is compromised, it is very likely that the attacker will de
created during the intrusion. Unfortunately, system logs are often
analysis, and the logs on the compromised system cannot be trust
changed them.

This problem can -at least partly- be solved by using a <b>central syslog server</b>. Such a server can gather the system logs of many nodes on the network. As a result, the attacker may be able to change the logs on the compromised system, but it will be very difficult to change them on the central syslog server.

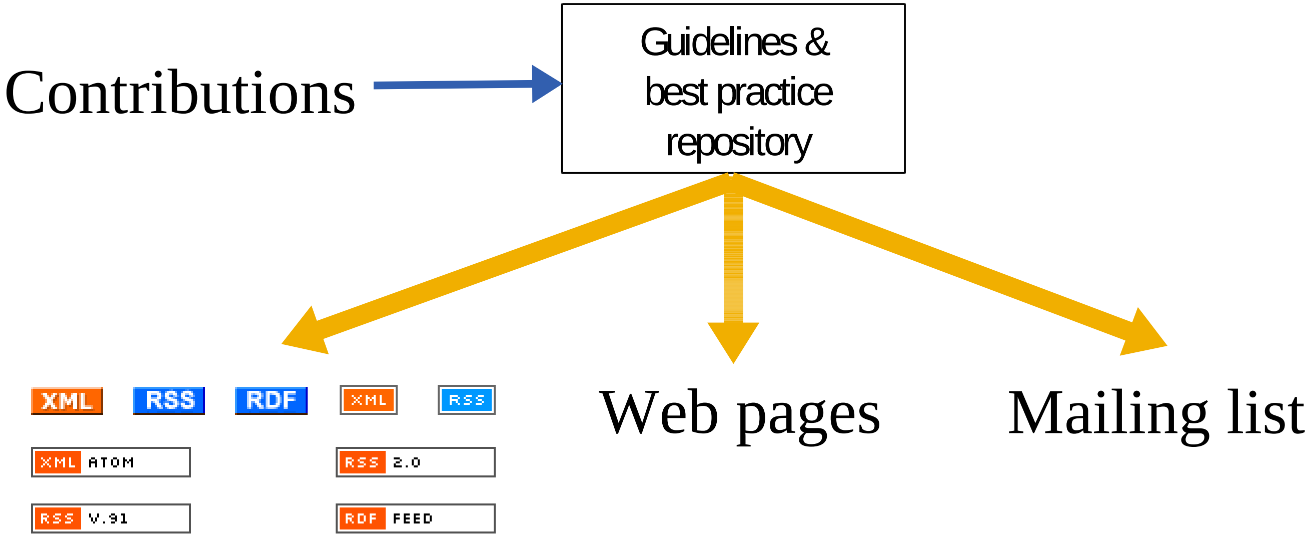
A central syslog server is therefore a great asset to understand how and in what way a system has been comprised. It can very often make recovery of the service quicker after a security incident and can help prevent the same attack happening again.

It is possible to find some information about implementing a central syslog server <a href="http://www.balabit.com/products/syslog_ng/">here</a> and <a href="http://www.campin.net/syslog-ng/faq.html">here</a>.

☑ Allow comments to this entry
□ Comments & trackbacks to this entry requires moderation

- Web interface, currently using Serendipity
- Using Gridsite authentication (x509 certificates)
- Contributions centralized and published by “trusted” people

Publication mechanism


Contributions

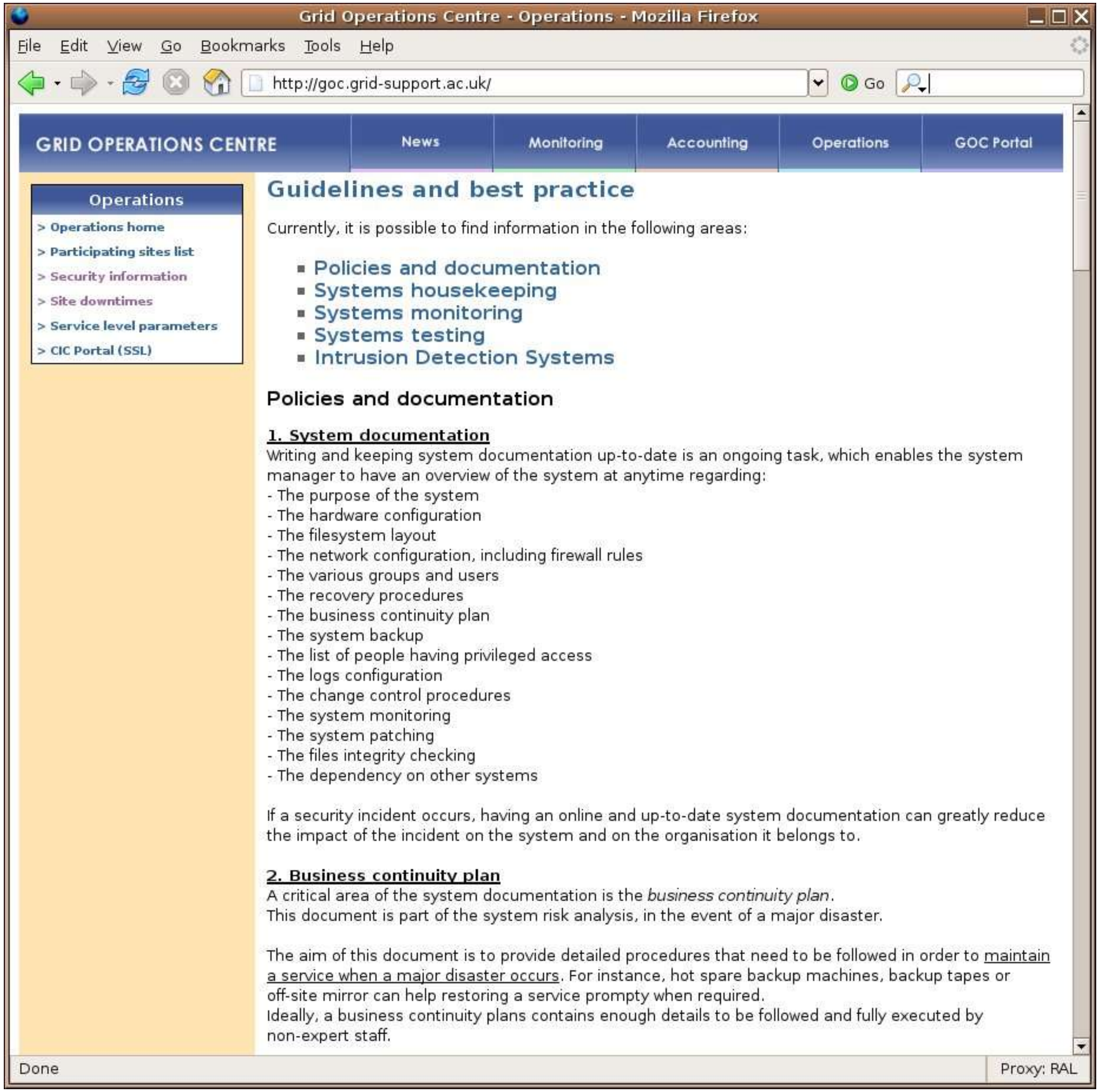
Guidelines & best practice repository

Web pages

Mailing list

- **The information is published via:**
  - Web pages
  - email
  - RSS feed

Getting the information on the Web 1/3


Grid Operations Centre - Operations - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://goc.grid-support.ac.uk/
Go
GRID OPERATIONS CENTRE
News
Monitoring
Accounting
Operations
GOC Portal
Operations
> Operations home
> Participating sites list
> Security information
> Site downtimes
> Service level parameters
> CIC Portal (SSL)
Done
Proxy: RAL

Guidelines and best practice

Currently, it is possible to find information in the following areas:

- Policies and documentation
- Systems housekeeping
- Systems monitoring
- Systems testing
- Intrusion Detection Systems

Policies and documentation

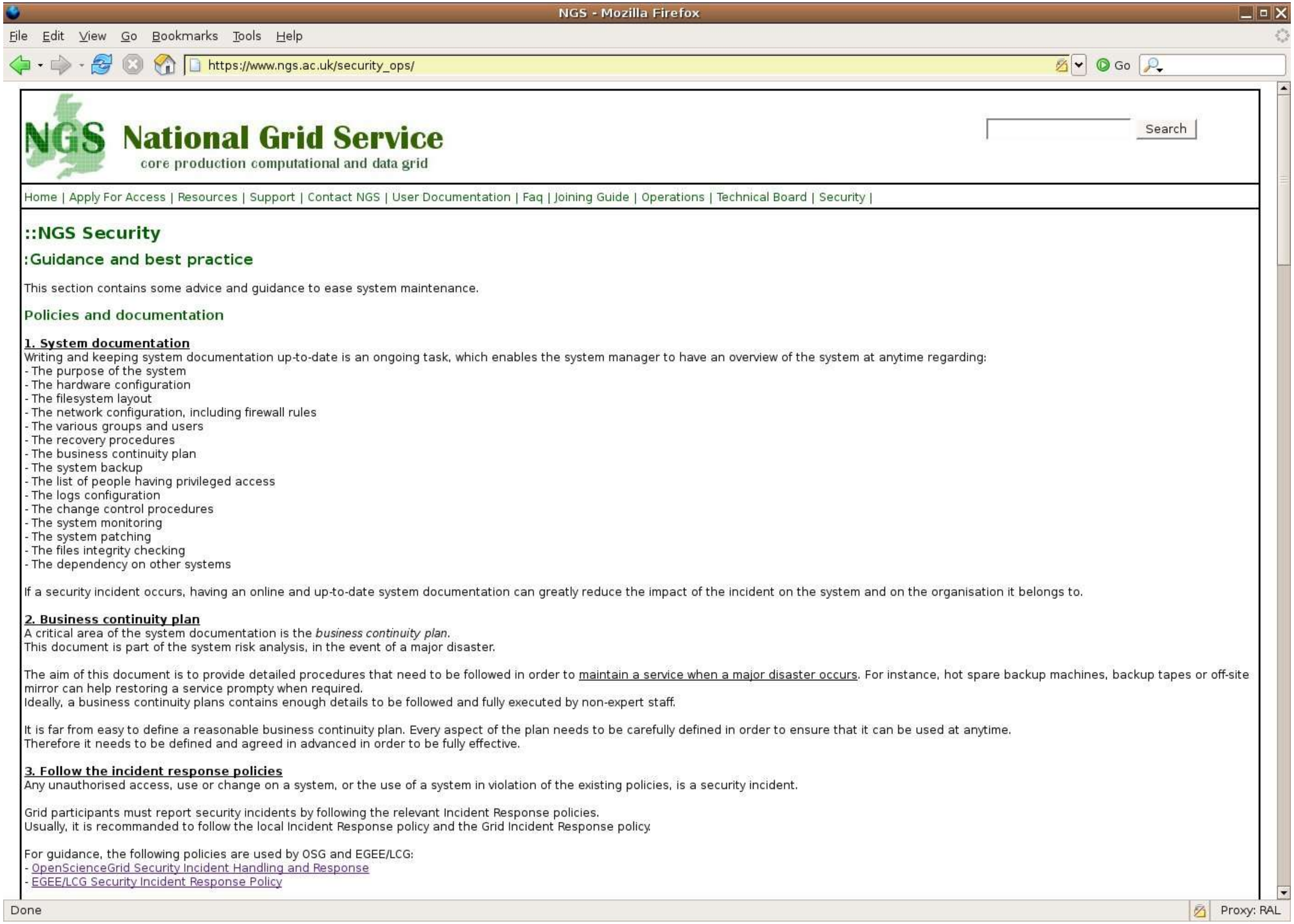
1. System documentation
Writing and keeping system documentation up-to-date is an ongoing task, which enables the system manager to have an overview of the system at anytime regarding:
- The purpose of the system
- The hardware configuration
- The filesystem layout
- The network configuration, including firewall rules
- The various groups and users
- The recovery procedures
- The business continuity plan
- The system backup
- The list of people having privileged access
- The logs configuration
- The change control procedures
- The system monitoring
- The system patching
- The files integrity checking
- The dependency on other systems

If a security incident occurs, having an online and up-to-date system documentation can greatly reduce the impact of the incident on the system and on the organisation it belongs to.

2. Business continuity plan
A critical area of the system documentation is the *business continuity plan*.
This document is part of the system risk analysis, in the event of a major disaster.

The aim of this document is to provide detailed procedures that need to be followed in order to maintain a service when a major disaster occurs. For instance, hot spare backup machines, backup tapes or off-site mirror can help restoring a service prompty when required.
Ideally, a business continuity plans contains enough details to be followed and fully executed by non-expert staff.

Getting the information on the Web 2/3



NGS - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://www.ngs.ac.uk/security_ops/
Go
NGS National Grid Service
core production computational and data grid
Search
Home | Apply For Access | Resources | Support | Contact NGS | User Documentation | Faq | Joining Guide | Operations | Technical Board | Security |
Done
Proxy: RAL

::NGS Security

:Guidance and best practice

This section contains some advice and guidance to ease system maintenance.

Policies and documentation

1. System documentation
Writing and keeping system documentation up-to-date is an ongoing task, which enables the system manager to have an overview of the system at anytime regarding:

- The purpose of the system
- The hardware configuration
- The filesystem layout
- The network configuration, including firewall rules
- The various groups and users
- The recovery procedures
- The business continuity plan
- The system backup
- The list of people having privileged access
- The logs configuration
- The change control procedures
- The system monitoring
- The system patching
- The files integrity checking
- The dependency on other systems

If a security incident occurs, having an online and up-to-date system documentation can greatly reduce the impact of the incident on the system and on the organisation it belongs to.

2. Business continuity plan
A critical area of the system documentation is the *business continuity plan*.
This document is part of the system risk analysis, in the event of a major disaster.

The aim of this document is to provide detailed procedures that need to be followed in order to maintain a service when a major disaster occurs. For instance, hot spare backup machines, backup tapes or off-site mirror can help restoring a service prompty when required.
Ideally, a business continuity plans contains enough details to be followed and fully executed by non-expert staff.

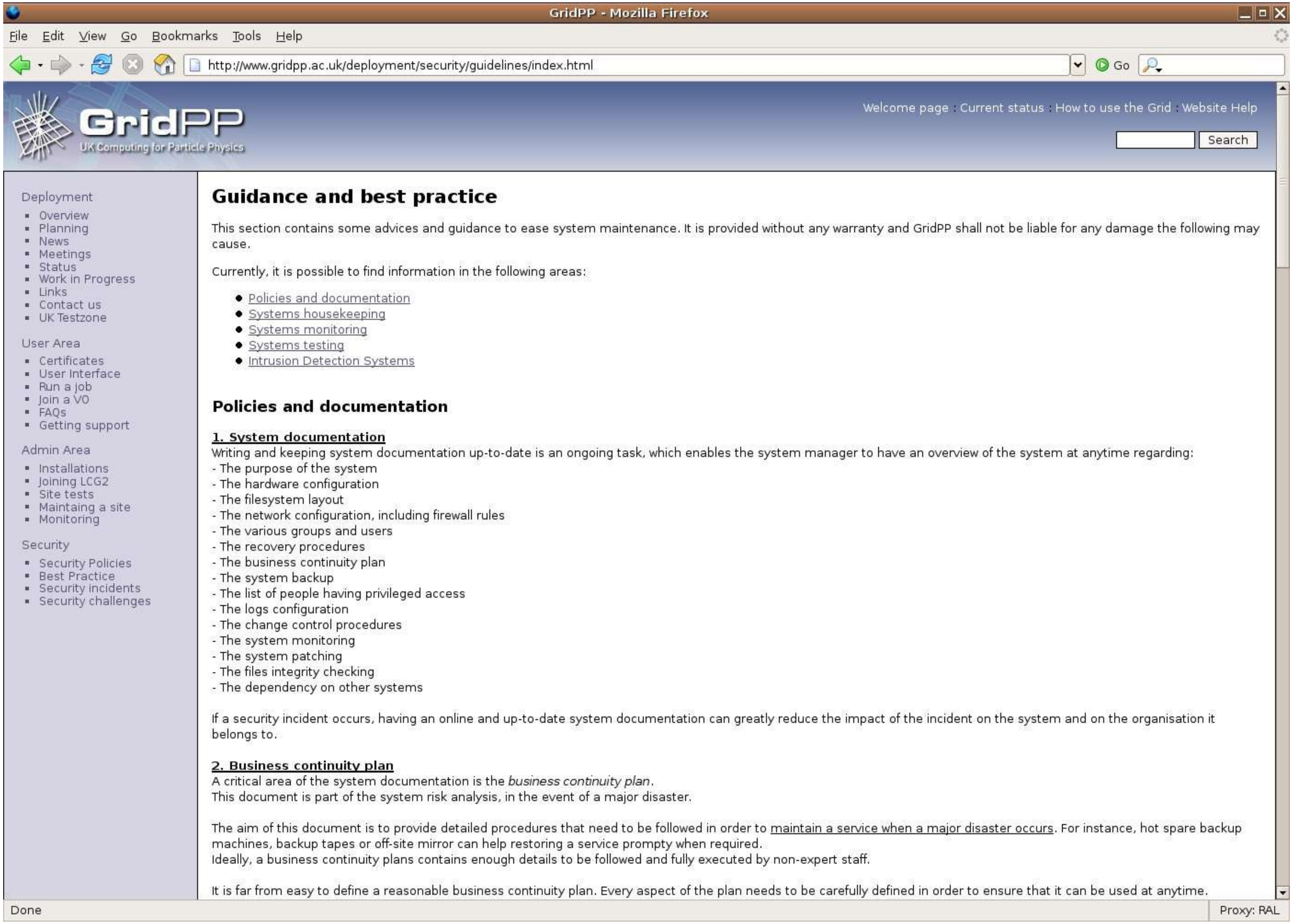
It is far from easy to define a reasonable business continuity plan. Every aspect of the plan needs to be carefully defined in order to ensure that it can be used at anytime.
Therefore it needs to be defined and agreed in advanced in order to be fully effective.

3. Follow the incident response policies
Any unauthorised access, use or change on a system, or the use of a system in violation of the existing policies, is a security incident.

Grid participants must report security incidents by following the relevant Incident Response policies.
Usually, it is recommanded to follow the local Incident Response policy and the Grid Incident Response policy.

For guidance, the following policies are used by OSG and EGEE/LCG:
- OpenScienceGrid Security Incident Handling and Response
- EGEE/LCG Security Incident Response Policy

Getting the information on the Web 3/3



Guidance and best practice

This section contains some advices and guidance to ease system maintenance. It is provided without any warranty and GridPP shall not be liable for any damage the following may cause.

Currently, it is possible to find information in the following areas:

- Policies and documentation
- Systems housekeeping
- Systems monitoring
- Systems testing
- Intrusion Detection Systems

Policies and documentation

1. System documentation
Writing and keeping system documentation up-to-date is an ongoing task, which enables the system manager to have an overview of the system at anytime regarding:
- The purpose of the system
- The hardware configuration
- The filesystem layout
- The network configuration, including firewall rules
- The various groups and users
- The recovery procedures
- The business continuity plan
- The system backup
- The list of people having privileged access
- The logs configuration
- The change control procedures
- The system monitoring
- The system patching
- The files integrity checking
- The dependency on other systems

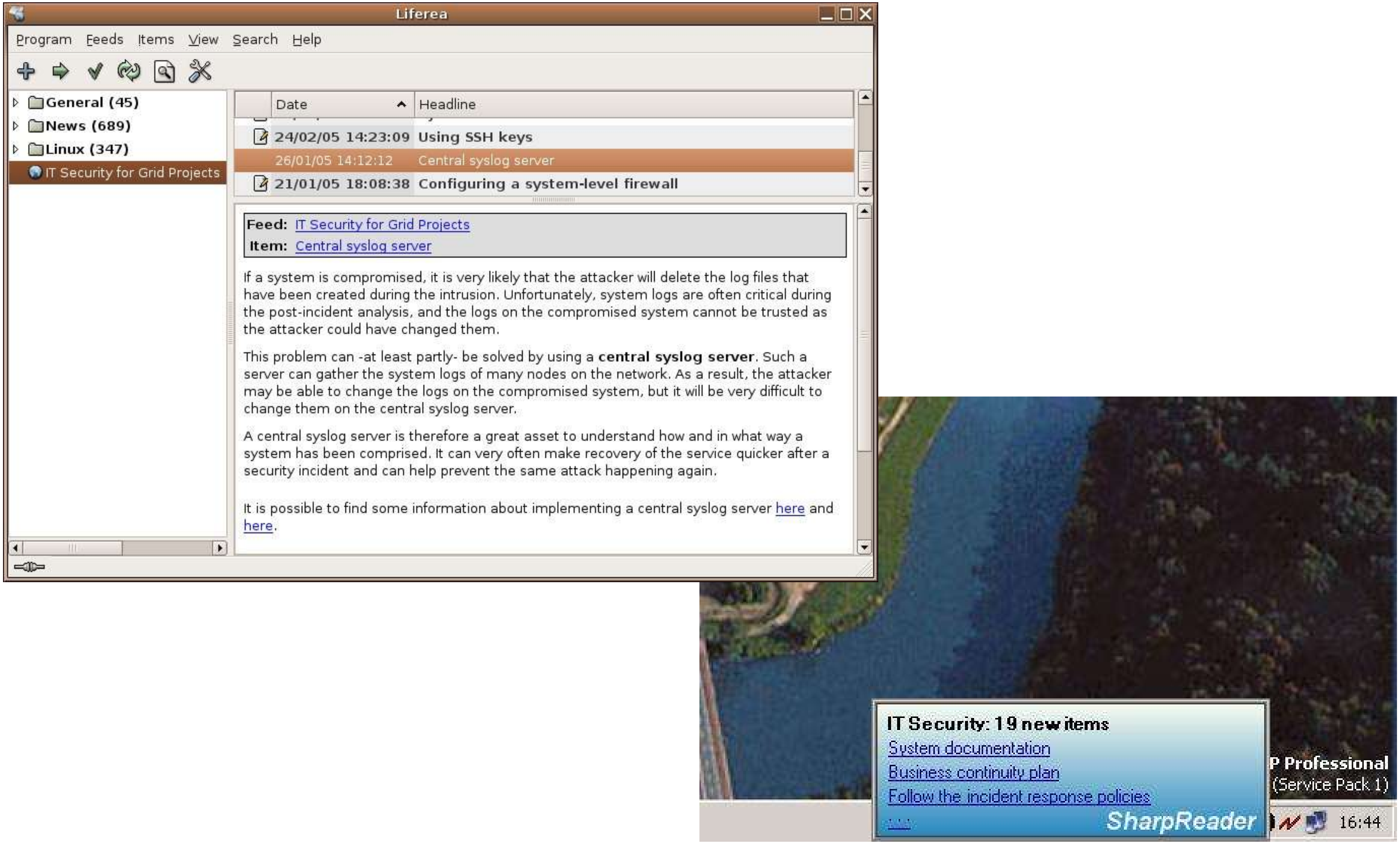
If a security incident occurs, having an online and up-to-date system documentation can greatly reduce the impact of the incident on the system and on the organisation it belongs to.

2. Business continuity plan
A critical area of the system documentation is the *business continuity plan*.
This document is part of the system risk analysis, in the event of a major disaster.

The aim of this document is to provide detailed procedures that need to be followed in order to maintain a service when a major disaster occurs. For instance, hot spare backup machines, backup tapes or off-site mirror can help restoring a service promptly when required.
Ideally, a business continuity plans contains enough details to be followed and fully executed by non-expert staff.

It is far from easy to define a reasonable business continuity plan. Every aspect of the plan needs to be carefully defined in order to ensure that it can be used at anytime.

Getting the information via RSS



Liferea
Program Feeds Items View Search Help
General (45)
News (689)
Linux (347)
IT Security for Grid Projects

Date	Headline
24/02/05 14:23:09	Using SSH keys
26/01/05 14:12:12	Central syslog server
21/01/05 18:08:38	Configuring a system-level firewall

Feed: IT Security for Grid Projects

Item: Central syslog server

If a system is compromised, it is very likely that the attacker will delete the log files that have been created during the intrusion. Unfortunately, system logs are often critical during the post-incident analysis, and the logs on the compromised system cannot be trusted as the attacker could have changed them.

This problem can -at least partly- be solved by using a **central syslog server**. Such a server can gather the system logs of many nodes on the network. As a result, the attacker may be able to change the logs on the compromised system, but it will be very difficult to change them on the central syslog server.

A central syslog server is therefore a great asset to understand how and in what way a system has been comprised. It can very often make recovery of the service quicker after a security incident and can help prevent the same attack happening again.

It is possible to find some information about implementing a central syslog server here and here.

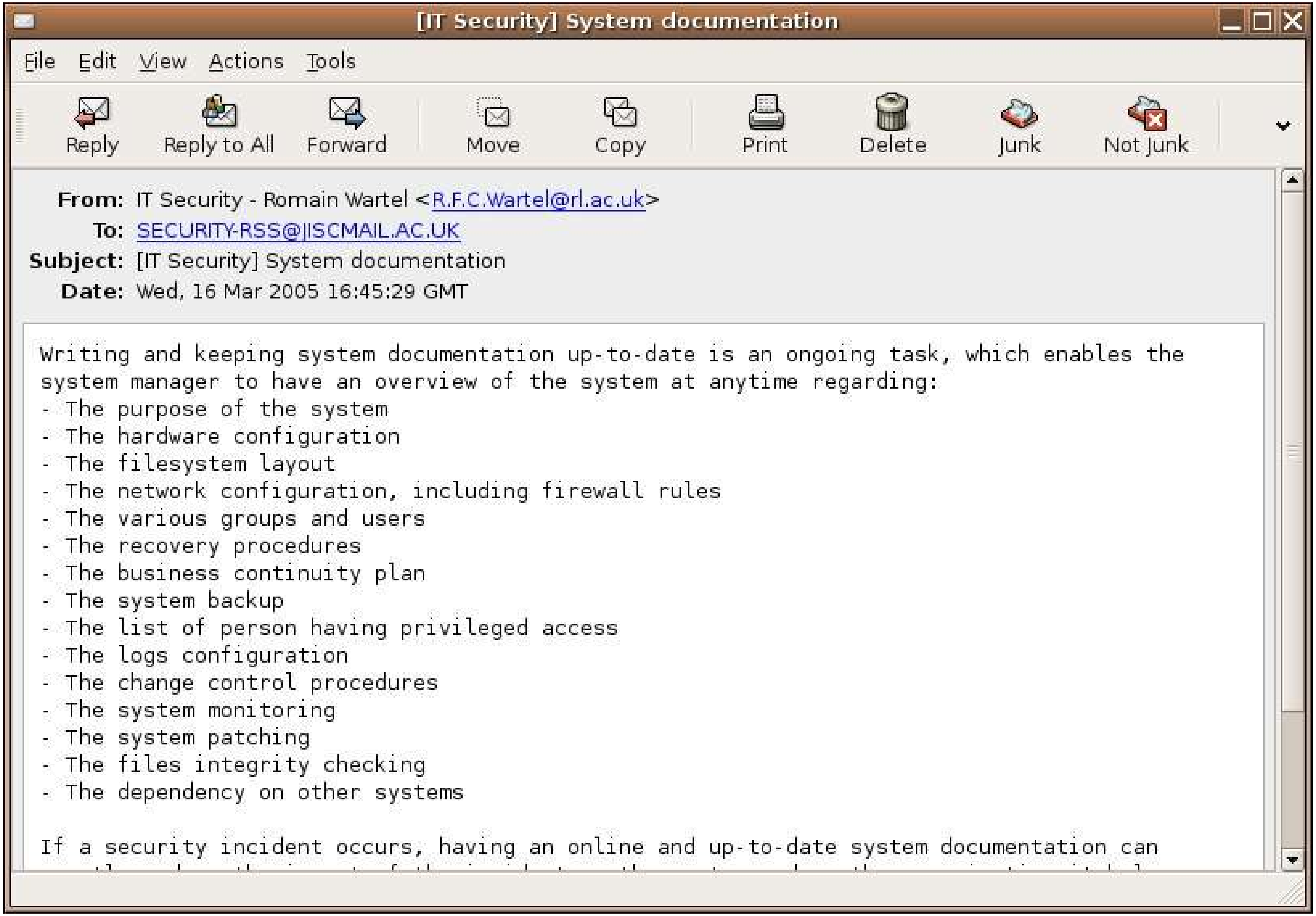
IT Security: 19 new items

System documentation

Business continuity plan

Follow the incident response policies

Getting the information by email



From: IT Security - Romain Wartel <R.F.C.Wartel@rl.ac.uk>
To: SECURITY-RSS@JISCMAIL.AC.UK
Subject: [IT Security] System documentation
Date: Wed, 16 Mar 2005 16:45:29 GMT

```
Writing and keeping system documentation up-to-date is an ongoing task, which enables the
system manager to have an overview of the system at anytime regarding:
- The purpose of the system
- The hardware configuration
- The filesystem layout
- The network configuration, including firewall rules
- The various groups and users
- The recovery procedures
- The business continuity plan
- The system backup
- The list of person having privileged access
- The logs configuration
- The change control procedures
- The system monitoring
- The system patching
- The files integrity checking
- The dependency on other systems

If a security incident occurs, having an online and up-to-date system documentation can
```

Current architecture summary

- XML based, recognized standard
- Widespread technology: many clients and APIs
- Enables injecting security information within existing Websites
- Enables filtering of the information
- Any webmaster can use the feed
- Coherent, up-to-date information is available
- Design up to Webmasters, but some layout can be pushed

However:

- RSS requires a server-side mechanism
- Webmasters need to trust the authors or perform manual updates

Future

We need to:

- Provide better, more targeted content
- Provide a second layer of information, via external Web pages
- Receive contributions from the community
- Deploy the mechanism amongst more sites
- Improve the way the information is sorted

GridPP
UK Computing for Particle Physics

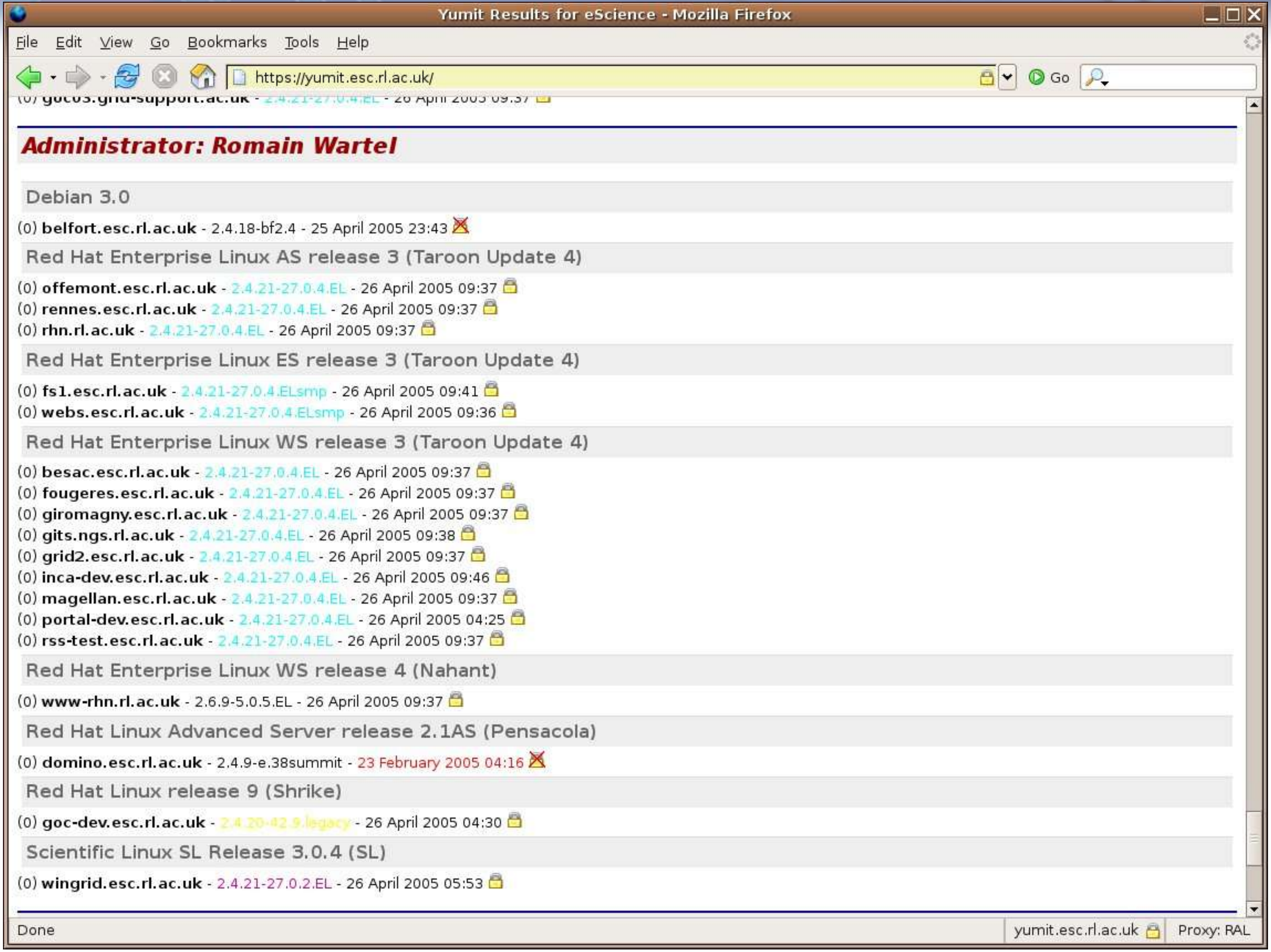
Security Monitoring

Yumit 1/6

- Most attacks are using known software vulnerabilities
- Enables monitoring of patching status for a large farm
- Originally developed by Steve Traylen
- Deployment status
  - RAL eScience has 350+ systems registered
  - RAL Tier1a has 600+ systems registered
  - Deployment started at CERN and within UK NGS
- Packages and documentation available from:

  http://www-staff.esc.rl.ac.uk/Romain/yumit/

Yumit 2/6


Yumit Results for eScience - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://yumit.esc.rl.ac.uk/
Go
Done
yumit.esc.rl.ac.uk
Proxy: RAL

(0) goc03.grid-support.ac.uk - 2.4.21-27.0.4.EL - 26 April 2005 09:37 🔒

Administrator: Romain Wartel

Debian 3.0

(0) **belfort.esc.rl.ac.uk** - 2.4.18-bf2.4 - 25 April 2005 23:43 ☒

Red Hat Enterprise Linux AS release 3 (Taroon Update 4)

(0) **offemont.esc.rl.ac.uk** - 2.4.21-27.0.4.EL - 26 April 2005 09:37 🔒
(0) **rennes.esc.rl.ac.uk** - 2.4.21-27.0.4.EL - 26 April 2005 09:37 🔒
(0) **rhn.rl.ac.uk** - 2.4.21-27.0.4.EL - 26 April 2005 09:37 🔒

Red Hat Enterprise Linux ES release 3 (Taroon Update 4)

(0) **fs1.esc.rl.ac.uk** - 2.4.21-27.0.4.ELsmp - 26 April 2005 09:41 🔒
(0) **webs.esc.rl.ac.uk** - 2.4.21-27.0.4.ELsmp - 26 April 2005 09:36 🔒

Red Hat Enterprise Linux WS release 3 (Taroon Update 4)

(0) **besac.esc.rl.ac.uk** - 2.4.21-27.0.4.EL - 26 April 2005 09:37 🔒
(0) **fougeres.esc.rl.ac.uk** - 2.4.21-27.0.4.EL - 26 April 2005 09:37 🔒
(0) **giromagny.esc.rl.ac.uk** - 2.4.21-27.0.4.EL - 26 April 2005 09:37 🔒
(0) **gits.ngs.rl.ac.uk** - 2.4.21-27.0.4.EL - 26 April 2005 09:38 🔒
(0) **grid2.esc.rl.ac.uk** - 2.4.21-27.0.4.EL - 26 April 2005 09:37 🔒
(0) **inca-dev.esc.rl.ac.uk** - 2.4.21-27.0.4.EL - 26 April 2005 09:46 🔒
(0) **magellan.esc.rl.ac.uk** - 2.4.21-27.0.4.EL - 26 April 2005 09:37 🔒
(0) **portal-dev.esc.rl.ac.uk** - 2.4.21-27.0.4.EL - 26 April 2005 04:25 🔒
(0) **rss-test.esc.rl.ac.uk** - 2.4.21-27.0.4.EL - 26 April 2005 09:37 🔒

Red Hat Enterprise Linux WS release 4 (Nahant)

(0) **www-rhn.rl.ac.uk** - 2.6.9-5.0.5.EL - 26 April 2005 09:37 🔒

Red Hat Linux Advanced Server release 2.1AS (Pensacola)

(0) **domino.esc.rl.ac.uk** - 2.4.9-e.38summit - 23 February 2005 04:16 ☒

Red Hat Linux release 9 (Shrike)

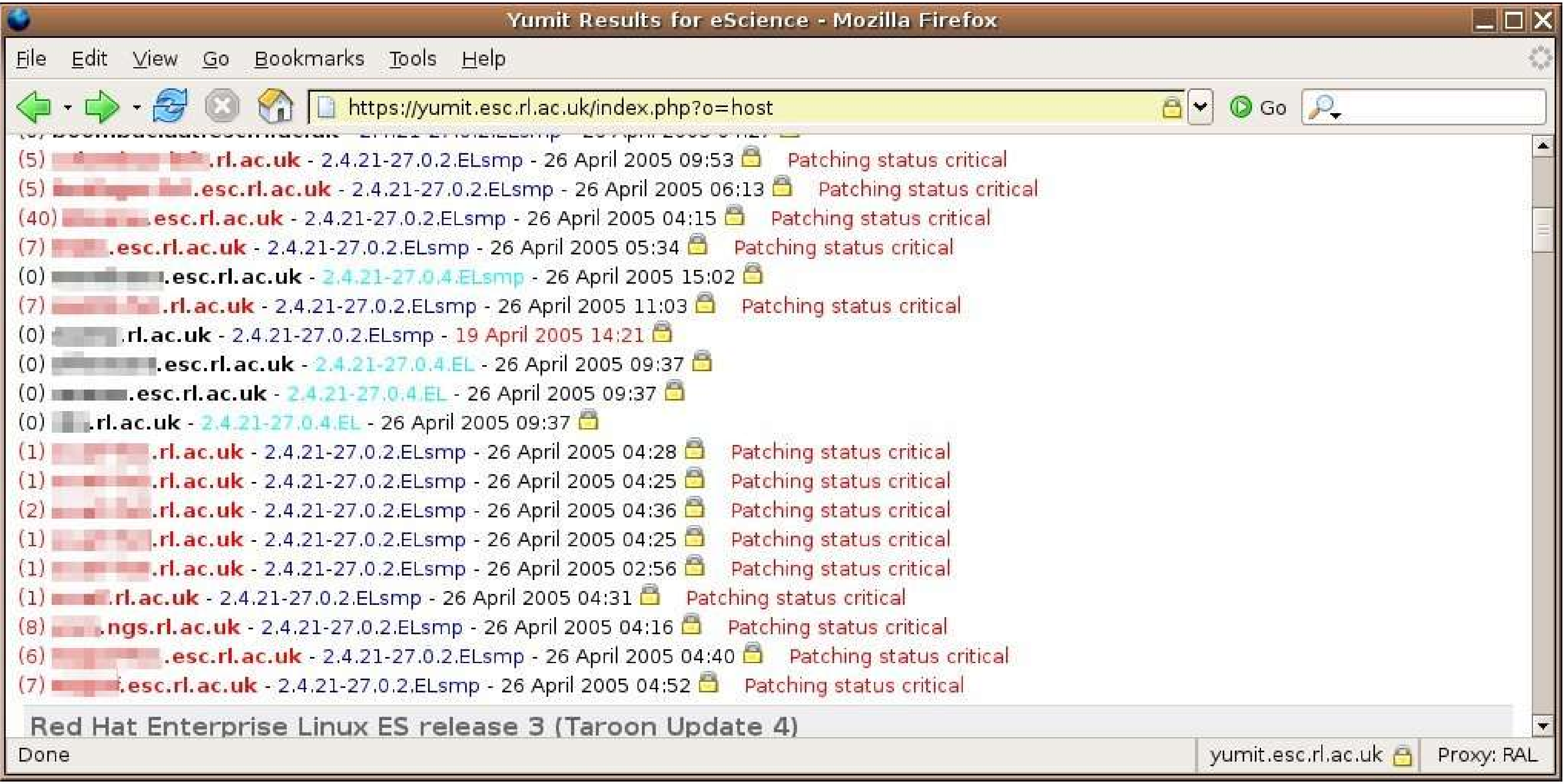
(0) **goc-dev.esc.rl.ac.uk** - 2.4.20-42.9.legacy - 26 April 2005 04:30 🔒

Scientific Linux SL Release 3.0.4 (SL)

(0) **wingrid.esc.rl.ac.uk** - 2.4.21-27.0.2.EL - 26 April 2005 05:53 🔒

GridPP
UK Computing for Particle Physics

Yumit 3/6


Yumit Results for eScience - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
Go
Done
yumit.esc.rl.ac.uk
Proxy: RAL

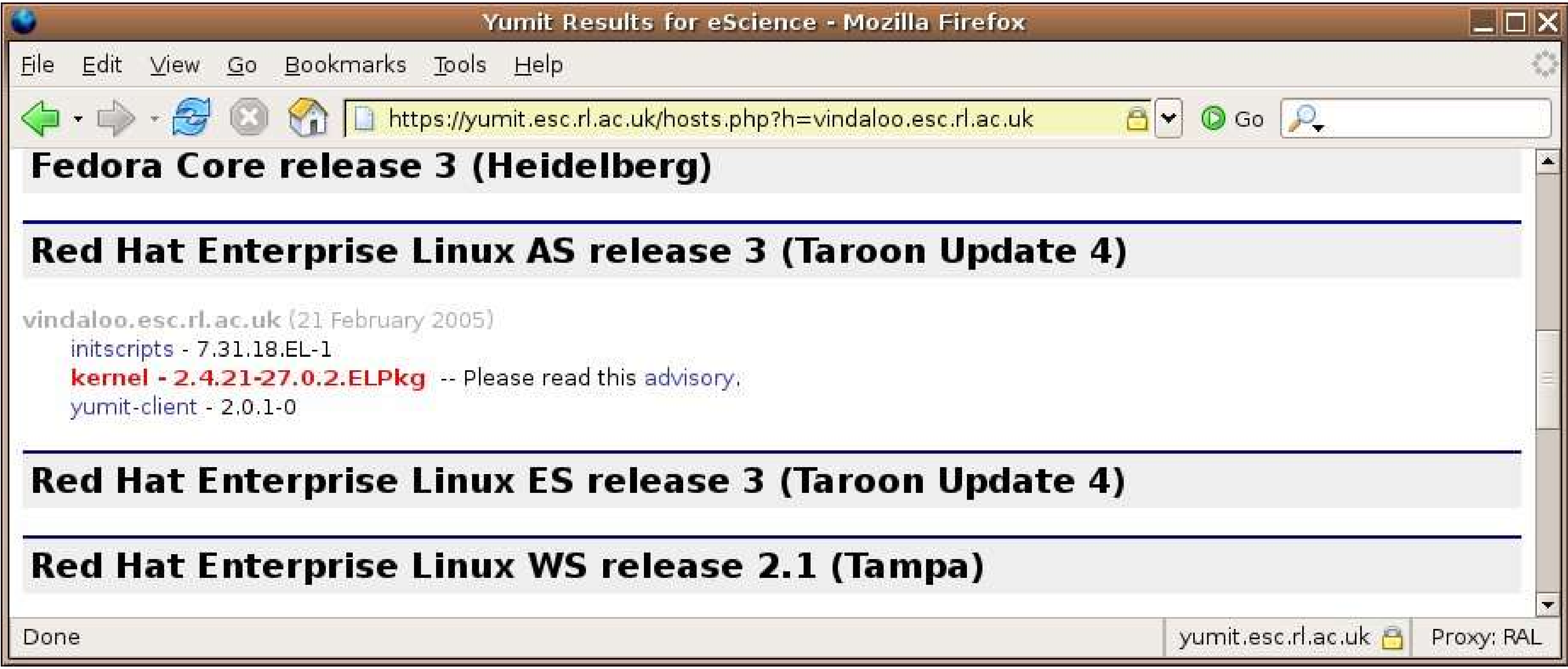
https://yumit.esc.rl.ac.uk/index.php?o=host

```
(5) [redacted].rl.ac.uk - 2.4.21-27.0.2.ELsmp - 26 April 2005 09:53   Patching status critical
(5) [redacted].esc.rl.ac.uk - 2.4.21-27.0.2.ELsmp - 26 April 2005 06:13   Patching status critical
(40) [redacted].esc.rl.ac.uk - 2.4.21-27.0.2.ELsmp - 26 April 2005 04:15   Patching status critical
(7) [redacted].esc.rl.ac.uk - 2.4.21-27.0.2.ELsmp - 26 April 2005 05:34   Patching status critical
(0) [redacted].esc.rl.ac.uk - 2.4.21-27.0.4.ELsmp - 26 April 2005 15:02
(7) [redacted].rl.ac.uk - 2.4.21-27.0.2.ELsmp - 26 April 2005 11:03   Patching status critical
(0) [redacted].rl.ac.uk - 2.4.21-27.0.2.ELsmp - 19 April 2005 14:21
(0) [redacted].esc.rl.ac.uk - 2.4.21-27.0.4.EL - 26 April 2005 09:37
(0) [redacted].esc.rl.ac.uk - 2.4.21-27.0.4.EL - 26 April 2005 09:37
(0) [redacted].rl.ac.uk - 2.4.21-27.0.4.EL - 26 April 2005 09:37
(1) [redacted].rl.ac.uk - 2.4.21-27.0.2.ELsmp - 26 April 2005 04:28   Patching status critical
(1) [redacted].rl.ac.uk - 2.4.21-27.0.2.ELsmp - 26 April 2005 04:25   Patching status critical
(2) [redacted].rl.ac.uk - 2.4.21-27.0.2.ELsmp - 26 April 2005 04:36   Patching status critical
(1) [redacted].rl.ac.uk - 2.4.21-27.0.2.ELsmp - 26 April 2005 04:25   Patching status critical
(1) [redacted].rl.ac.uk - 2.4.21-27.0.2.ELsmp - 26 April 2005 02:56   Patching status critical
(1) [redacted].rl.ac.uk - 2.4.21-27.0.2.ELsmp - 26 April 2005 04:31   Patching status critical
(8) [redacted].ngs.rl.ac.uk - 2.4.21-27.0.2.ELsmp - 26 April 2005 04:16   Patching status critical
(6) [redacted].esc.rl.ac.uk - 2.4.21-27.0.2.ELsmp - 26 April 2005 04:40   Patching status critical
(7) [redacted].esc.rl.ac.uk - 2.4.21-27.0.2.ELsmp - 26 April 2005 04:52   Patching status critical
```

Red Hat Enterprise Linux ES release 3 (Taroon Update 4)

GridPP
UK Computing for Particle Physics

Yumit 4/6


Yumit Results for eScience - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://yumit.esc.rl.ac.uk/hosts.php?h=vindaloo.esc.rl.ac.uk
Go

Fedora Core release 3 (Heidelberg)

Red Hat Enterprise Linux AS release 3 (Taroon Update 4)

vindaloo.esc.rl.ac.uk (21 February 2005)

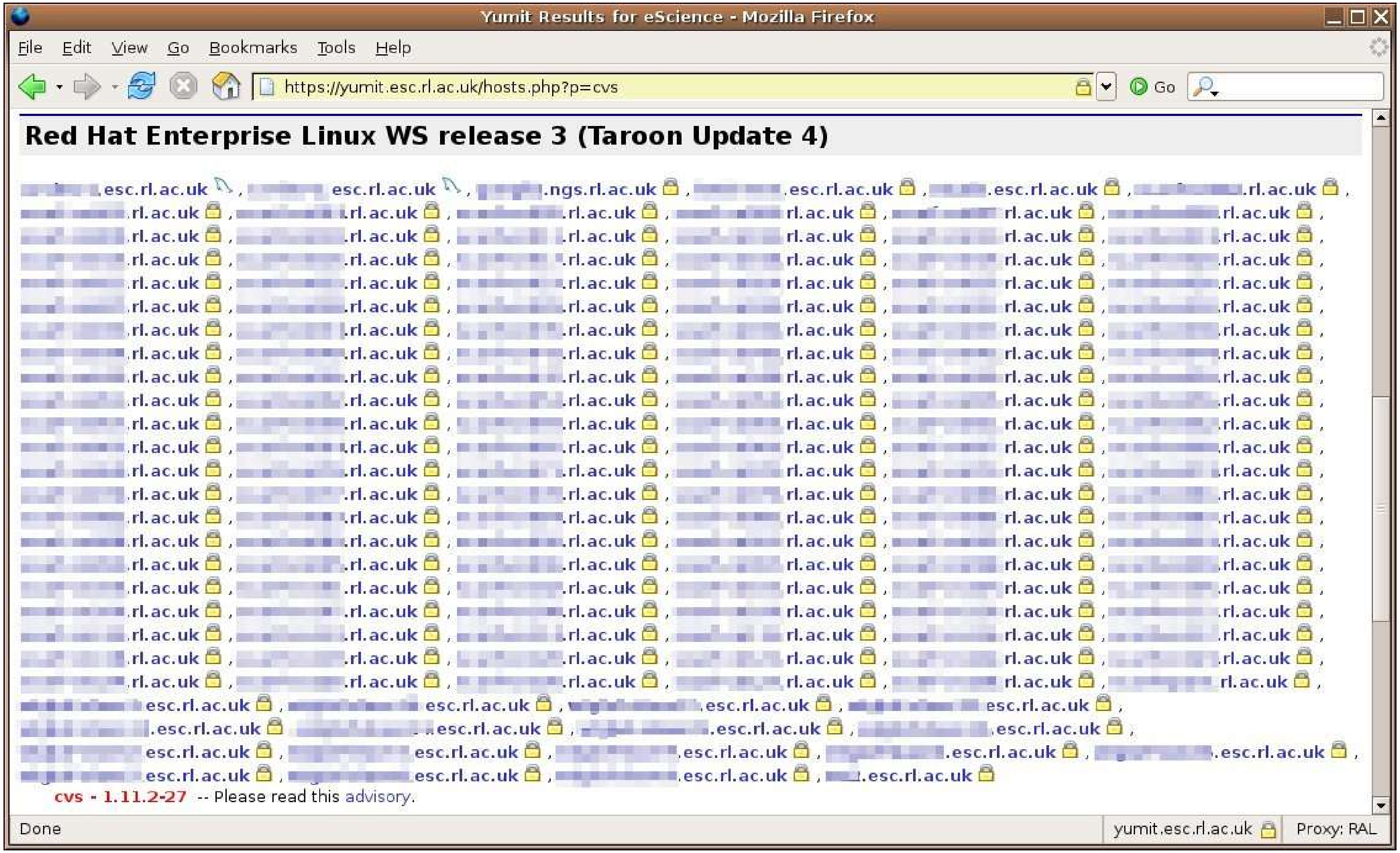
initscripts - 7.31.18.EL-1
kernel - 2.4.21-27.0.2.ELPkg -- Please read this advisory.
yumit-client - 2.0.1-0

Red Hat Enterprise Linux ES release 3 (Taroon Update 4)

Red Hat Enterprise Linux WS release 2.1 (Tampa)

Done
yumit.esc.rl.ac.uk
Proxy: RAL

Yumit 5/6



Yumit Results for eScience - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://yumit.esc.rl.ac.uk/hosts.php?p=cvs
Go

Red Hat Enterprise Linux WS release 3 (Taroon Update 4)

[redacted].esc.rl.ac.uk , [redacted] esc.rl.ac.uk , [redacted].ngs.rl.ac.uk 🔒 , [redacted].esc.rl.ac.uk 🔒 , [redacted].esc.rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 ,
[redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 ,
[redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 ,
[redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 ,
[redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 ,
[redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 ,
[redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 ,
[redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 ,
[redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 ,
[redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 ,
[redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 ,
[redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 ,
[redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 ,
[redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 ,
[redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 ,
[redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 ,
[redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 ,
[redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 ,
[redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 ,
[redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 ,
[redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 ,
[redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted].rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 , [redacted]rl.ac.uk 🔒 ,
[redacted]esc.rl.ac.uk 🔒 , [redacted]esc.rl.ac.uk 🔒 , [redacted].esc.rl.ac.uk 🔒 , [redacted]esc.rl.ac.uk 🔒 ,
[redacted].esc.rl.ac.uk 🔒 , [redacted].esc.rl.ac.uk 🔒 , [redacted].esc.rl.ac.uk 🔒 , [redacted].esc.rl.ac.uk 🔒 ,
[redacted]esc.rl.ac.uk 🔒 , [redacted]esc.rl.ac.uk 🔒 , [redacted].esc.rl.ac.uk 🔒 , [redacted].esc.rl.ac.uk 🔒 , [redacted].esc.rl.ac.uk 🔒 ,
[redacted]esc.rl.ac.uk 🔒 , [redacted]esc.rl.ac.uk 🔒 , [redacted].esc.rl.ac.uk 🔒 , [redacted].esc.rl.ac.uk 🔒

cvs - 1.11.2-27 -- Please read this advisory.

Done | yumit.esc.rl.ac.uk 🔒 | Proxy: RAL

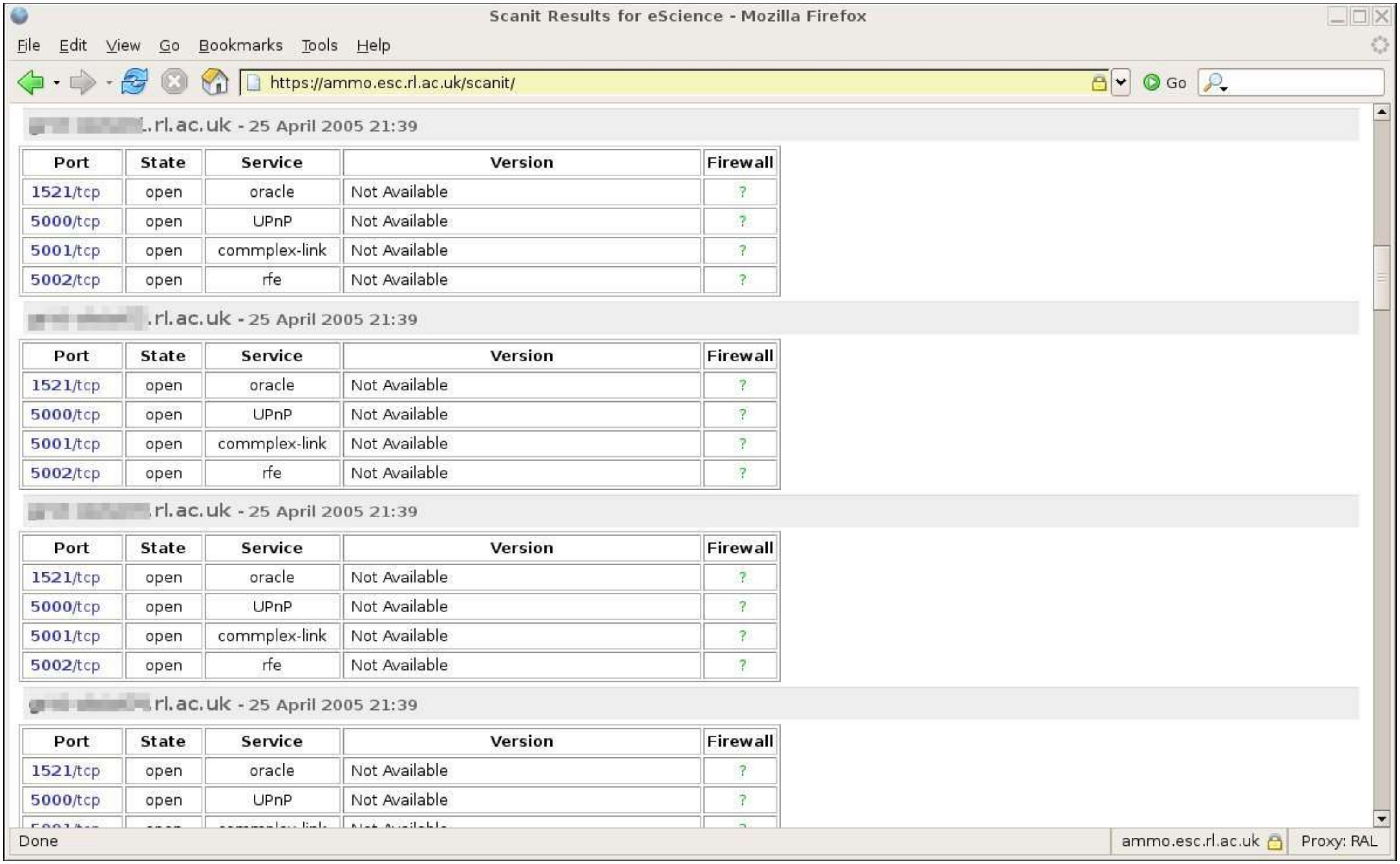
Future work and plans

- The Yumit server needs more documentation
- Deployment mechanisms are needed:
  - To get the latest version
  - To use the "red" security flag
- Perhaps a Grid version through EGEE OSCT?

Scanit 1/6

- Scanit detects changes in the list of open ports
- Useful to detect a system compromise
- Deployment status:
  - Used with RAL-esc
  - Deployment in progress within RAL Tier1a

Scanit 2/6


Scanit Results for eScience - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://ammo.esc.rl.ac.uk/scanit/
Go
Done
ammo.esc.rl.ac.uk
Proxy: RAL

[redacted].rl.ac.uk - 25 April 2005 21:39

Port	State	Service	Version	Firewall
1521/tcp	open	oracle	Not Available	?
5000/tcp	open	UPnP	Not Available	?
5001/tcp	open	commplex-link	Not Available	?
5002/tcp	open	rfe	Not Available	?

[redacted].rl.ac.uk - 25 April 2005 21:39

Port	State	Service	Version	Firewall
1521/tcp	open	oracle	Not Available	?
5000/tcp	open	UPnP	Not Available	?
5001/tcp	open	commplex-link	Not Available	?
5002/tcp	open	rfe	Not Available	?

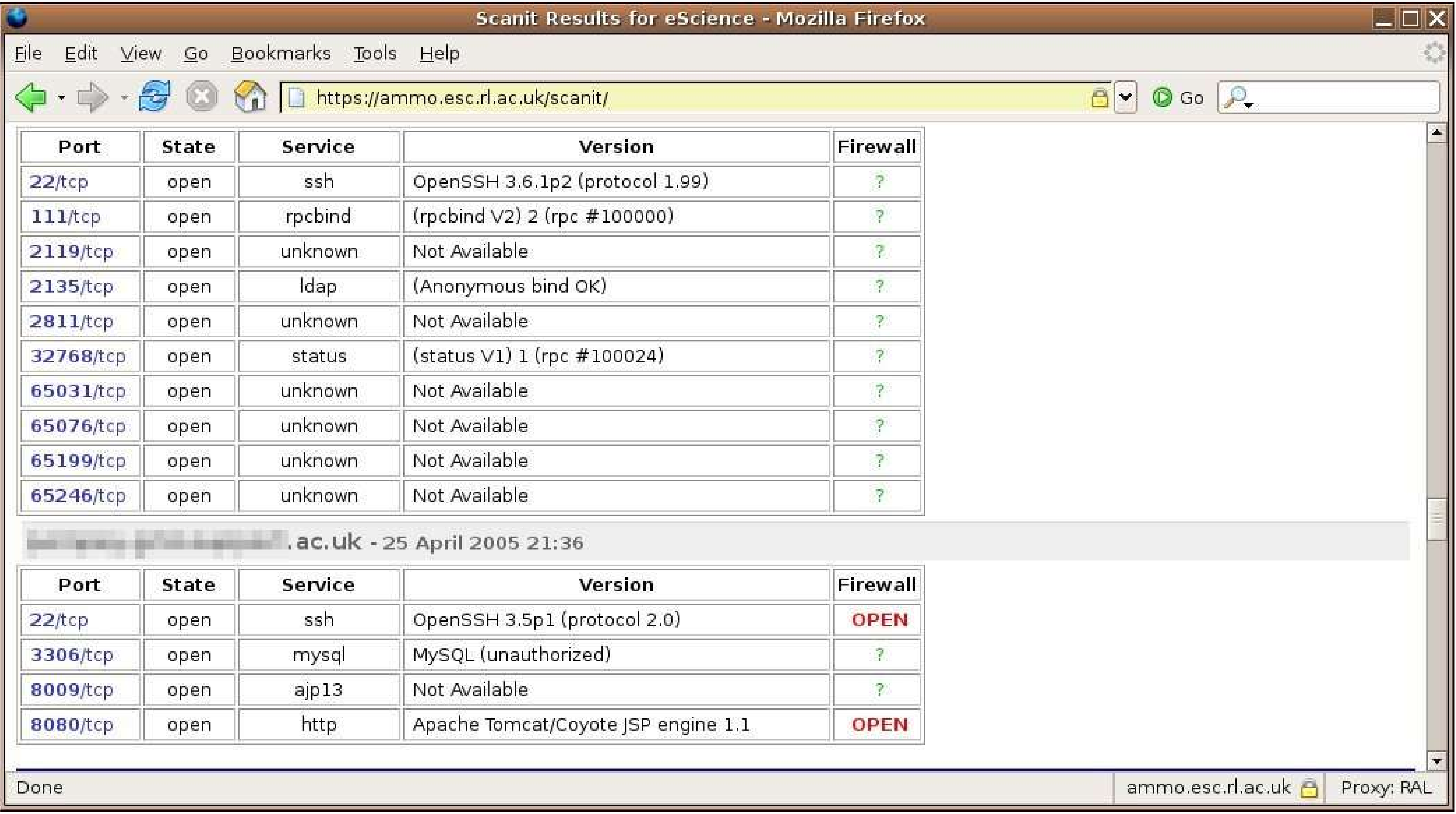
[redacted].rl.ac.uk - 25 April 2005 21:39

Port	State	Service	Version	Firewall
1521/tcp	open	oracle	Not Available	?
5000/tcp	open	UPnP	Not Available	?
5001/tcp	open	commplex-link	Not Available	?
5002/tcp	open	rfe	Not Available	?

[redacted].rl.ac.uk - 25 April 2005 21:39

Port	State	Service	Version	Firewall
1521/tcp	open	oracle	Not Available	?
5000/tcp	open	UPnP	Not Available	?
5001/tcp	open	commplex-link	Not Available	?

Scanit 3/6

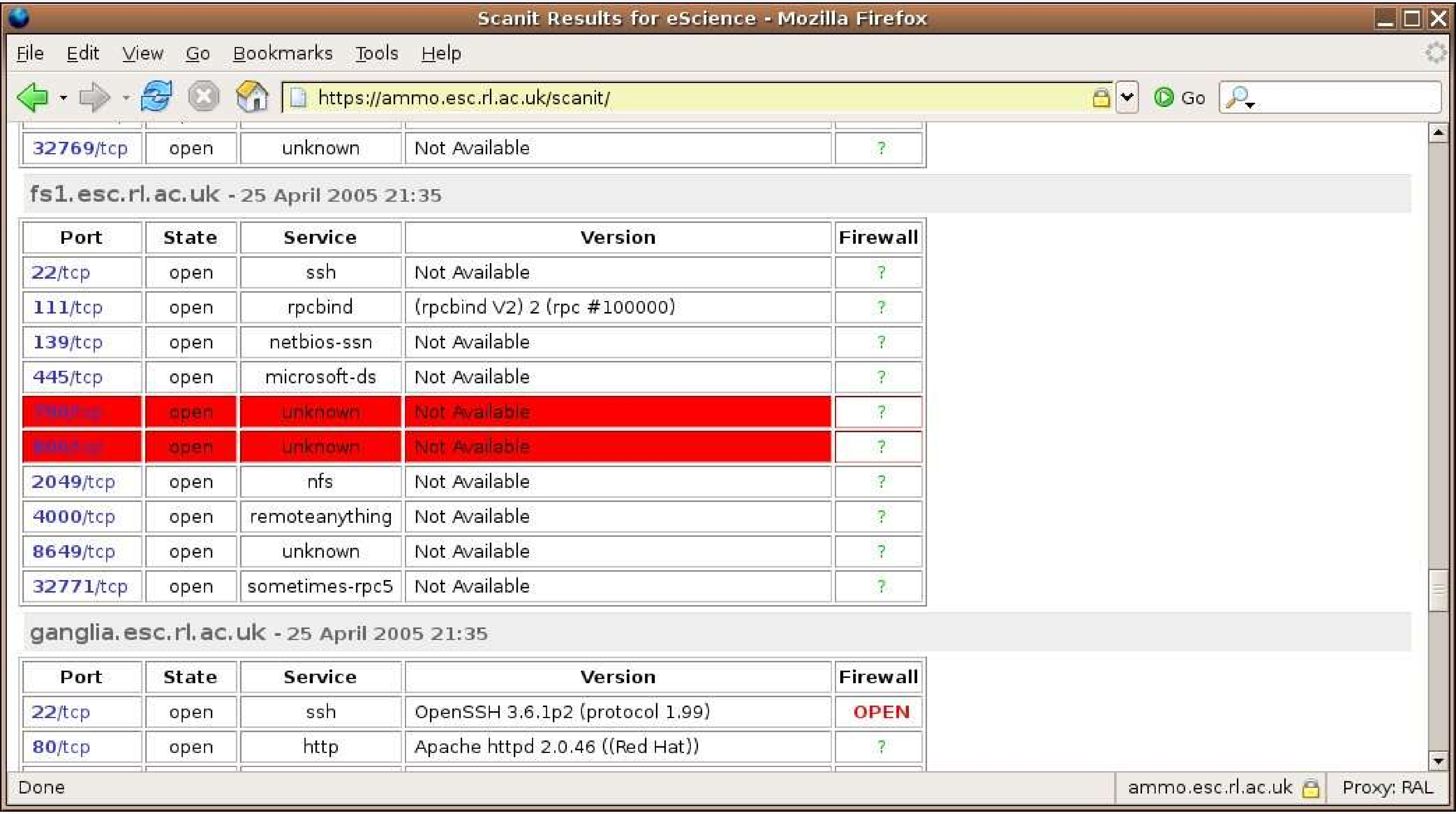

Scanit Results for eScience - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://ammo.esc.rl.ac.uk/scanit/
Go

Port	State	Service	Version	Firewall
22/tcp	open	ssh	OpenSSH 3.6.1p2 (protocol 1.99)	?
111/tcp	open	rpcbind	(rpcbind V2) 2 (rpc #100000)	?
2119/tcp	open	unknown	Not Available	?
2135/tcp	open	ldap	(Anonymous bind OK)	?
2811/tcp	open	unknown	Not Available	?
32768/tcp	open	status	(status V1) 1 (rpc #100024)	?
65031/tcp	open	unknown	Not Available	?
65076/tcp	open	unknown	Not Available	?
65199/tcp	open	unknown	Not Available	?
65246/tcp	open	unknown	Not Available	?

[redacted].ac.uk - 25 April 2005 21:36

Port	State	Service	Version	Firewall
22/tcp	open	ssh	OpenSSH 3.5p1 (protocol 2.0)	OPEN
3306/tcp	open	mysql	MySQL (unauthorized)	?
8009/tcp	open	ajp13	Not Available	?
8080/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1	OPEN

Scanit 4/6


Scanit Results for eScience - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://ammo.esc.rl.ac.uk/scanit/
Go
Done
ammo.esc.rl.ac.uk
Proxy: RAL

32769/tcp	open	unknown	Not Available	?

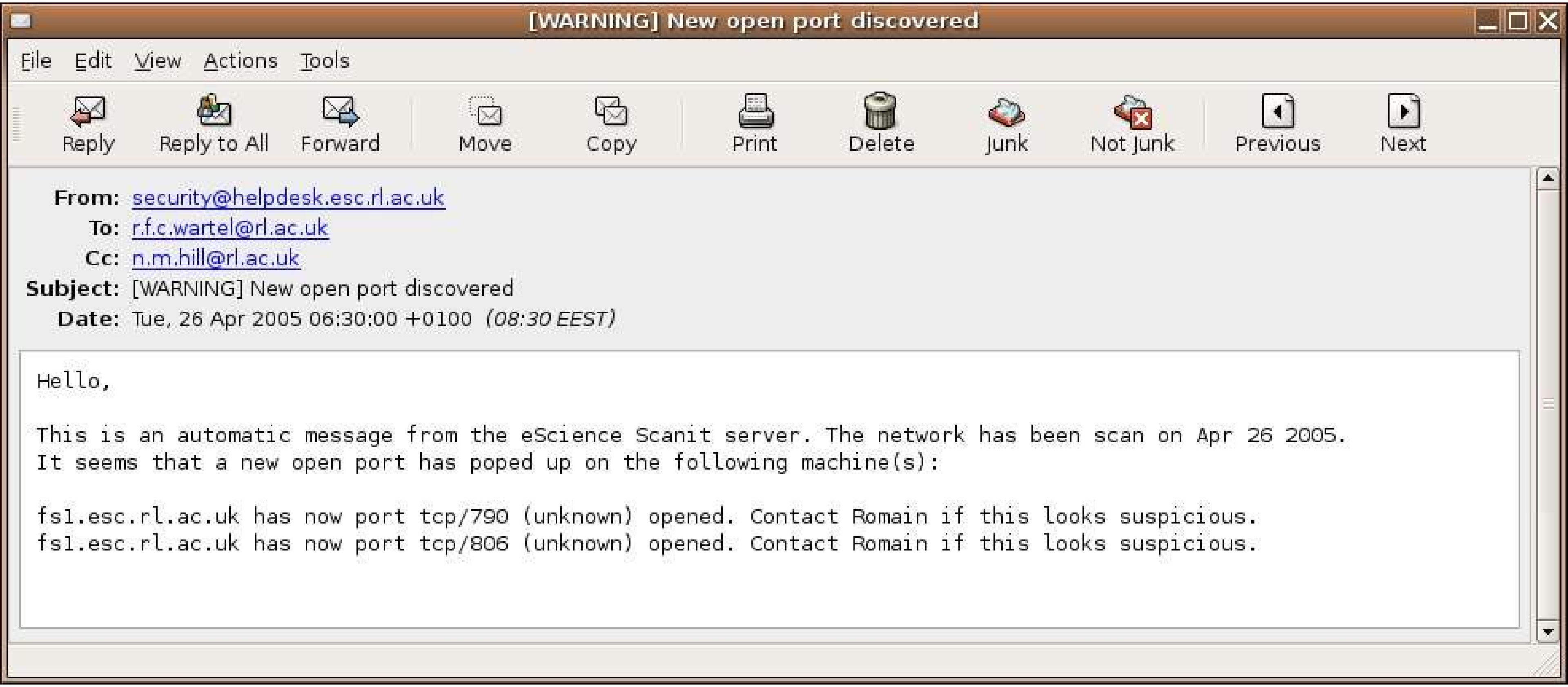
fs1.esc.rl.ac.uk - 25 April 2005 21:35

Port	State	Service	Version	Firewall
22/tcp	open	ssh	Not Available	?
111/tcp	open	rpcbind	(rpcbind V2) 2 (rpc #100000)	?
139/tcp	open	netbios-ssn	Not Available	?
445/tcp	open	microsoft-ds	Not Available	?
[redacted]	open	unknown	Not Available	?
[redacted]	open	unknown	Not Available	?
2049/tcp	open	nfs	Not Available	?
4000/tcp	open	remoteanything	Not Available	?
8649/tcp	open	unknown	Not Available	?
32771/tcp	open	sometimes-rpc5	Not Available	?

ganglia.esc.rl.ac.uk - 25 April 2005 21:35

Port	State	Service	Version	Firewall
22/tcp	open	ssh	OpenSSH 3.6.1p2 (protocol 1.99)	OPEN
80/tcp	open	http	Apache httpd 2.0.46 ((Red Hat))	?

Scanit 5/6



From: security@helpdesk.esc.rl.ac.uk
To: r.f.c.wartel@rl.ac.uk
Cc: n.m.hill@rl.ac.uk
Subject: [WARNING] New open port discovered
Date: Tue, 26 Apr 2005 06:30:00 +0100 *(08:30 EEST)*

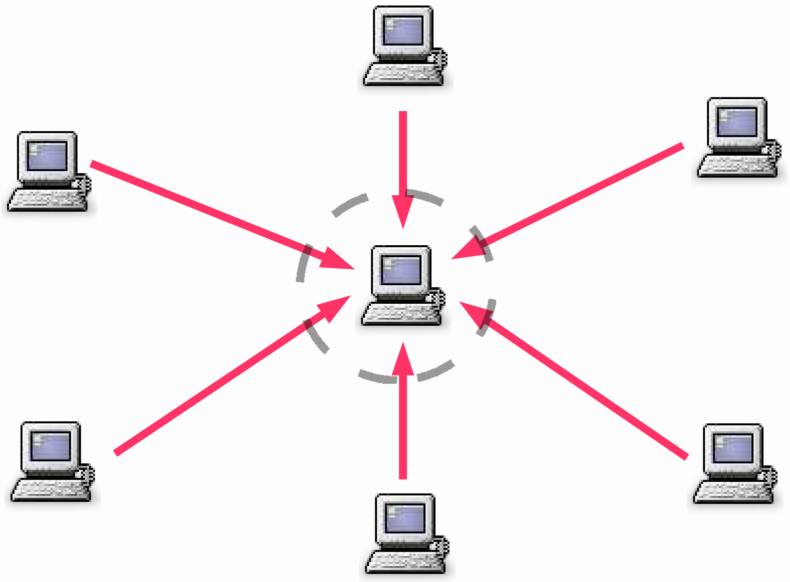
```
Hello,

This is an automatic message from the eScience Scanit server. The network has been scan on Apr 26 2005.
It seems that a new open port has poped up on the following machine(s):

fs1.esc.rl.ac.uk has now port tcp/790 (unknown) opened. Contact Romain if this looks suspicious.
fs1.esc.rl.ac.uk has now port tcp/806 (unknown) opened. Contact Romain if this looks suspicious.
```

Future work and plans

- Used in production at RAL
- Packaging in progress
- A few display bugs need to be fixed
- Documentation and Web page in progress
- Volunteers are more than welcomed

Central syslog server

- Extremely useful, especially during a security incident:
  - Detailed information are needed about system events
  - Information should be as reliable as possible
- The attacker cannot change the logs on the server



Preparing syslog server

- Network services on the server should be limited as much as possible!

- Installation of syslog-ng:

  http://www.balabit.com/products/syslog_ng/

- Good FAQ available from:

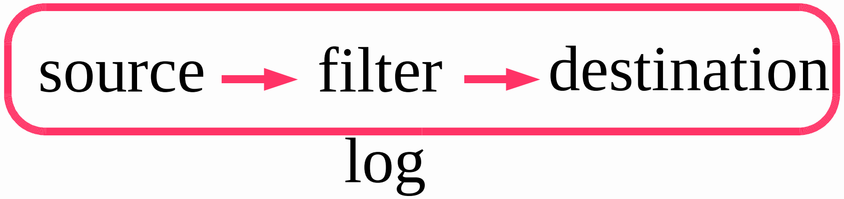
  http://www.campin.net/syslog-ng/faq.html

Syslog-ng configuration

- Main config file is:

  /etc/syslog-ng/syslog-ng.conf

- Syslog-ng uses the following template:



source → filter → destination

log

- Defining several “log” objects can be useful

Logging “all” to files

- All the logs are sent to disc:

```
log {
        source(src);
        destination(std);
};

destination std {
        file("/var/log/HOSTS/$HOST/$YEAR/$MONTH/$DAY/$FACILITY"
                owner(root) group(root) perm(0600) dir_perm(0700) create_dirs(yes)
        );
};
```

SSH entries to a DB

- Several solutions exists

```
log {
        source(src);
        filter(f_ssh_login_attempt);
        destination(d_mysql);
};
filter f_ssh_login_attempt {
        program("sshd.*")
        and match("(Failed|Accepted|authenticated|failed|Password|FAILED|ACCEPTED)")
        ;
};
pipe("/tmp/mysql.pipe"
template("INSERT INTO logs (host, facility, priority, level, tag, date,
time, program, msg) VALUES ( '$HOST', '$FACILITY', '$PRIORITY', '$LEVEL',
'$TAG','$YEAR-$MONTH-$DAY', '$HOUR:$MIN:$SEC', '$PROGRAM', '$MSG' );\n")
template-escape(yes));


};
```

Raising alerts

```
log {
source(src);
filter(f_network_denied);
destination(d_mysql);
destination(contact_sec);
};

filter f_network_denied {
        program("kernel.*")
        and match("DENIED") ;
};

destination contact_sec { file("/var/log/contact_sec"
                   owner(root) group(root) perm(0600) dir_perm(0700) create_dirs(yes)); };
```

- A cron job then simply checks the log file every 10 min
- If the file exists, its content is sent to the security team

Dynamic alerts

- Alerts can be generated for a temporary event

```
log {
        source(src);
        filter(f_suspect);
        destination(mail-alert);
   };
filter f_suspect {
                match("rw45");
};
destination mail-alert { program("/usr/local/bin/syslog-mail-perl"); };
```

suspicious pattern

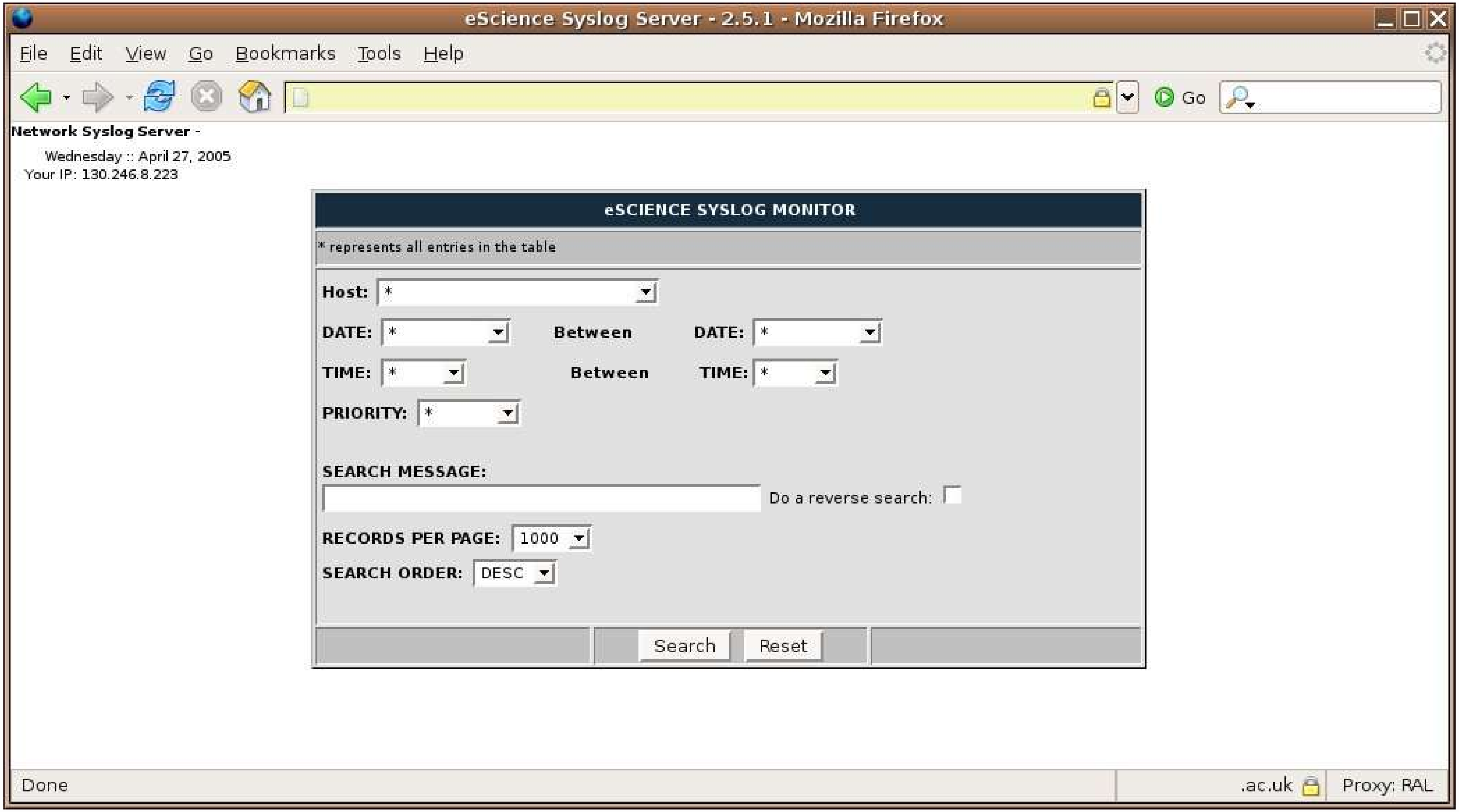
Then the script simply send the entry to the security team

Results

- All logs are archived and stored securely
- Ability to search for user logins, IP addresses, etc.
- Suspicious patterns are escalated
- As a result:
  - Intrusion detection is improved
  - Incident response is more efficient

syslog-ng Web GUI

- The DB is available from the Web to the security team:


eScience Syslog Server - 2.5.1 - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
Go

Network Syslog Server -

Wednesday :: April 27, 2005
Your IP: 130.246.8.223

eSCIENCE SYSLOG MONITOR

* represents all entries in the table

Host: *

DATE: * **Between** **DATE:** *

TIME: * **Between** **TIME:** *

PRIORITY: *

SEARCH MESSAGE:

Do a reverse search: □

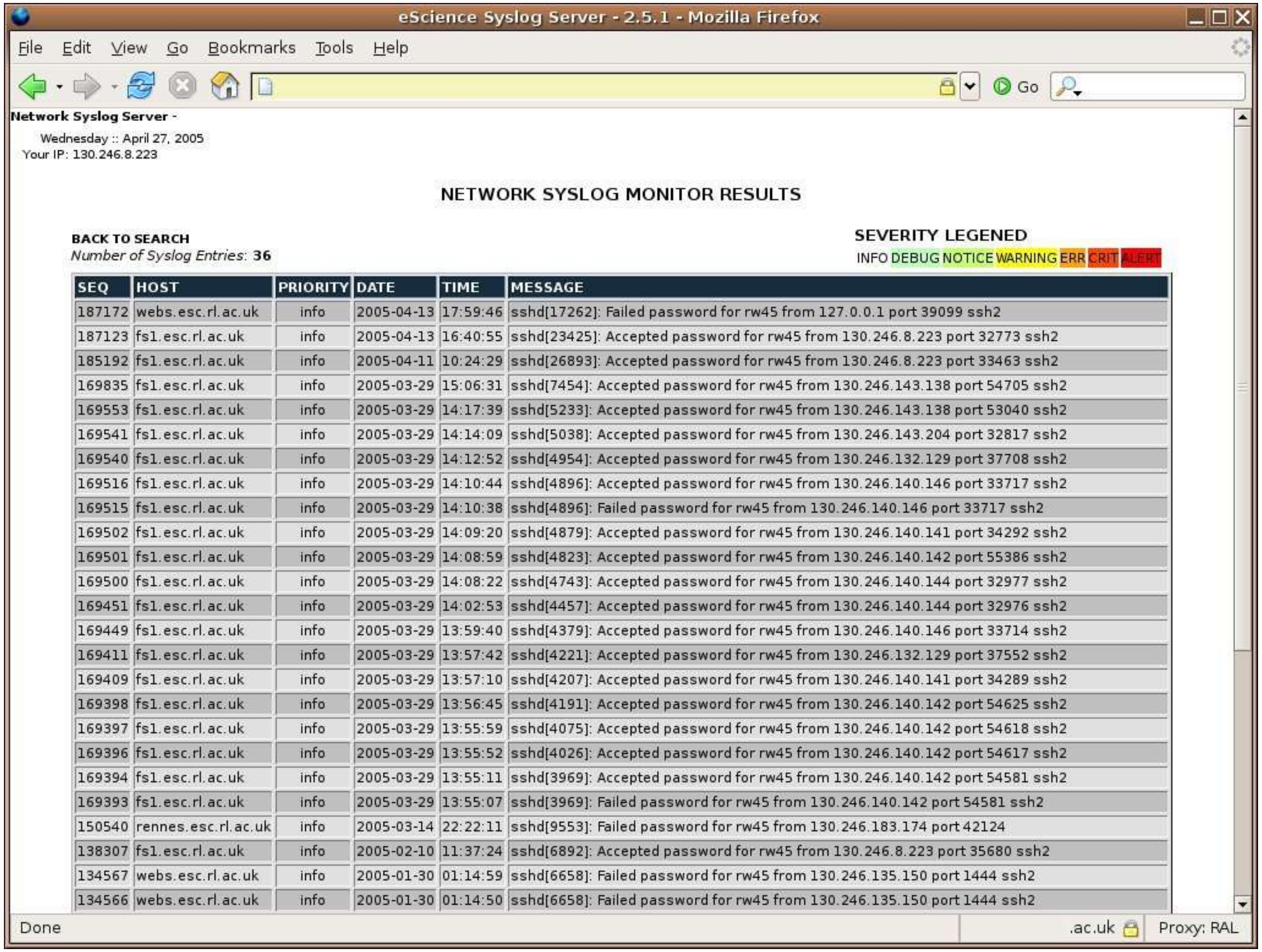
RECORDS PER PAGE: 1000

SEARCH ORDER: DESC

Search
Reset
Done
.ac.uk
Proxy: RAL

Searching for entries

- Searching for any login for “rw45” amongst the farm


eScience Syslog Server - 2.5.1 - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
Go
Done
.ac.uk
Proxy: RAL

Network Syslog Server -

Wednesday :: April 27, 2005
Your IP: 130.246.8.223

NETWORK SYSLOG MONITOR RESULTS

BACK TO SEARCH
Number of Syslog Entries: **36**

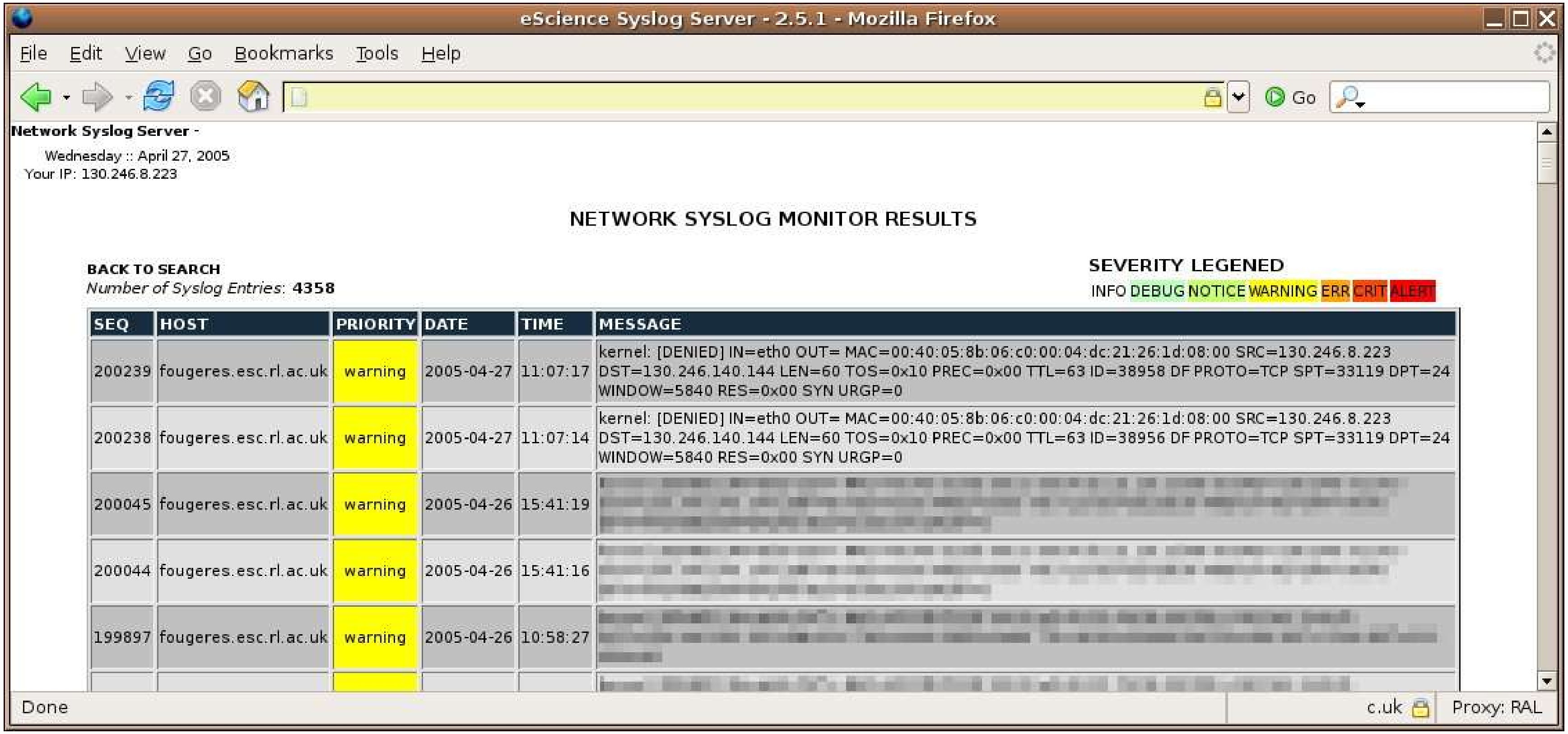
SEVERITY LEGENED
INFO DEBUG NOTICE WARNING ERR CRIT ALERT

SEQ	HOST	PRIORITY	DATE	TIME	MESSAGE
187172	webs.esc.rl.ac.uk	info	2005-04-13	17:59:46	sshd[17262]: Failed password for rw45 from 127.0.0.1 port 39099 ssh2
187123	fs1.esc.rl.ac.uk	info	2005-04-13	16:40:55	sshd[23425]: Accepted password for rw45 from 130.246.8.223 port 32773 ssh2
185192	fs1.esc.rl.ac.uk	info	2005-04-11	10:24:29	sshd[26893]: Accepted password for rw45 from 130.246.8.223 port 33463 ssh2
169835	fs1.esc.rl.ac.uk	info	2005-03-29	15:06:31	sshd[7454]: Accepted password for rw45 from 130.246.143.138 port 54705 ssh2
169553	fs1.esc.rl.ac.uk	info	2005-03-29	14:17:39	sshd[5233]: Accepted password for rw45 from 130.246.143.138 port 53040 ssh2
169541	fs1.esc.rl.ac.uk	info	2005-03-29	14:14:09	sshd[5038]: Accepted password for rw45 from 130.246.143.204 port 32817 ssh2
169540	fs1.esc.rl.ac.uk	info	2005-03-29	14:12:52	sshd[4954]: Accepted password for rw45 from 130.246.132.129 port 37708 ssh2
169516	fs1.esc.rl.ac.uk	info	2005-03-29	14:10:44	sshd[4896]: Accepted password for rw45 from 130.246.140.146 port 33717 ssh2
169515	fs1.esc.rl.ac.uk	info	2005-03-29	14:10:38	sshd[4896]: Failed password for rw45 from 130.246.140.146 port 33717 ssh2
169502	fs1.esc.rl.ac.uk	info	2005-03-29	14:09:20	sshd[4879]: Accepted password for rw45 from 130.246.140.141 port 34292 ssh2
169501	fs1.esc.rl.ac.uk	info	2005-03-29	14:08:59	sshd[4823]: Accepted password for rw45 from 130.246.140.142 port 55386 ssh2
169500	fs1.esc.rl.ac.uk	info	2005-03-29	14:08:22	sshd[4743]: Accepted password for rw45 from 130.246.140.144 port 32977 ssh2
169451	fs1.esc.rl.ac.uk	info	2005-03-29	14:02:53	sshd[4457]: Accepted password for rw45 from 130.246.140.144 port 32976 ssh2
169449	fs1.esc.rl.ac.uk	info	2005-03-29	13:59:40	sshd[4379]: Accepted password for rw45 from 130.246.140.146 port 33714 ssh2
169411	fs1.esc.rl.ac.uk	info	2005-03-29	13:57:42	sshd[4221]: Accepted password for rw45 from 130.246.132.129 port 37552 ssh2
169409	fs1.esc.rl.ac.uk	info	2005-03-29	13:57:10	sshd[4207]: Accepted password for rw45 from 130.246.140.141 port 34289 ssh2
169398	fs1.esc.rl.ac.uk	info	2005-03-29	13:56:45	sshd[4191]: Accepted password for rw45 from 130.246.140.142 port 54625 ssh2
169397	fs1.esc.rl.ac.uk	info	2005-03-29	13:55:59	sshd[4075]: Accepted password for rw45 from 130.246.140.142 port 54618 ssh2
169396	fs1.esc.rl.ac.uk	info	2005-03-29	13:55:52	sshd[4026]: Accepted password for rw45 from 130.246.140.142 port 54617 ssh2
169394	fs1.esc.rl.ac.uk	info	2005-03-29	13:55:11	sshd[3969]: Accepted password for rw45 from 130.246.140.142 port 54581 ssh2
169393	fs1.esc.rl.ac.uk	info	2005-03-29	13:55:07	sshd[3969]: Failed password for rw45 from 130.246.140.142 port 54581 ssh2
150540	rennes.esc.rl.ac.uk	info	2005-03-14	22:22:11	sshd[9553]: Failed password for rw45 from 130.246.183.174 port 42124
138307	fs1.esc.rl.ac.uk	info	2005-02-10	11:37:24	sshd[6892]: Accepted password for rw45 from 130.246.8.223 port 35680 ssh2
134567	webs.esc.rl.ac.uk	info	2005-01-30	01:14:59	sshd[6658]: Failed password for rw45 from 130.246.135.150 port 1444 ssh2
134566	webs.esc.rl.ac.uk	info	2005-01-30	01:14:50	sshd[6658]: Failed password for rw45 from 130.246.135.150 port 1444 ssh2

Tracking network scans

- Tracking network scans

```
romain@romain:~$ telnet fougeres.esc.rl.ac.uk 24
Trying 130.246.140.144...
```


eScience Syslog Server - 2.5.1 - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
Go
Done
c.uk
Proxy: RAL

Network Syslog Server -
Wednesday :: April 27, 2005
Your IP: 130.246.8.223

NETWORK SYSLOG MONITOR RESULTS

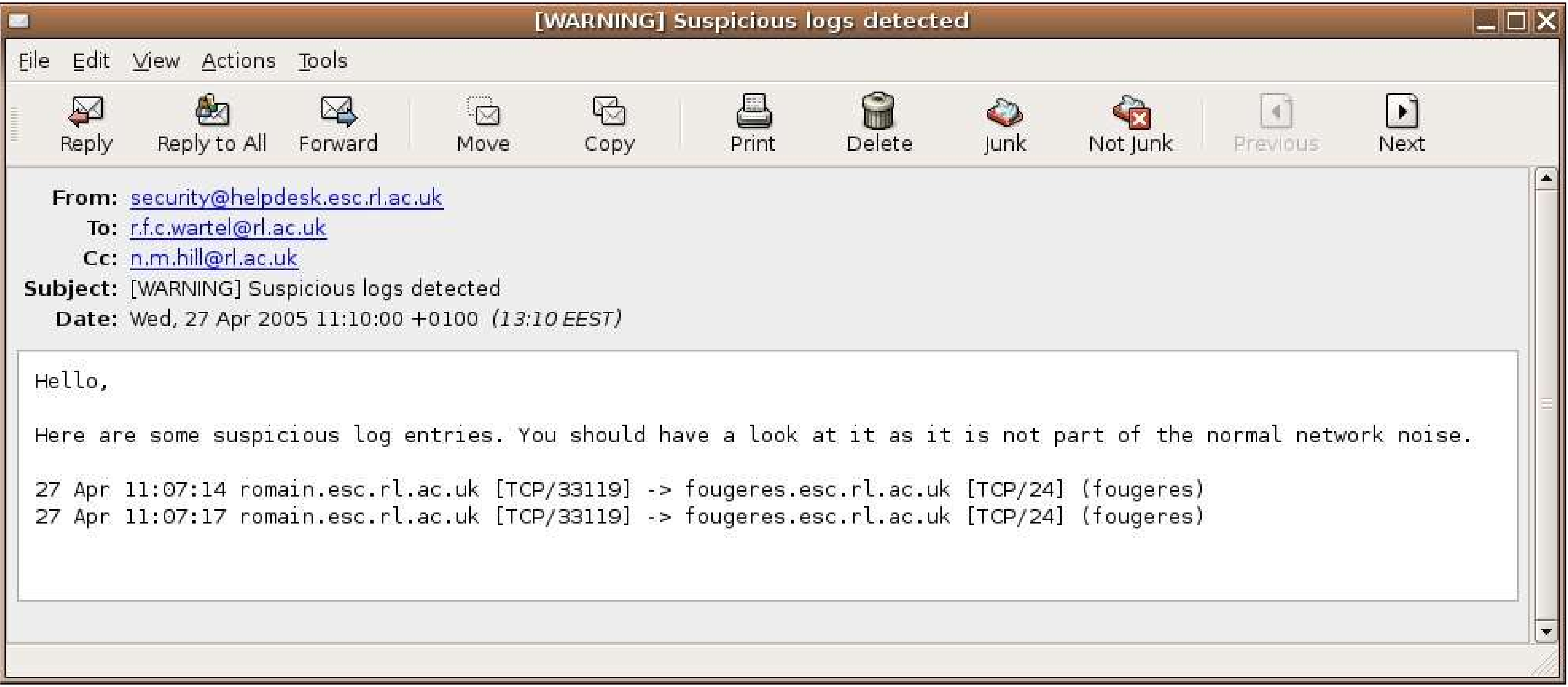
BACK TO SEARCH
Number of Syslog Entries: **4358**

SEVERITY LEGENED
INFO DEBUG NOTICE WARNING ERR CRIT ALERT

SEQ	HOST	PRIORITY	DATE	TIME	MESSAGE
200239	fougeres.esc.rl.ac.uk	warning	2005-04-27	11:07:17	kernel: [DENIED] IN=eth0 OUT= MAC=00:40:05:8b:06:c0:00:04:dc:21:26:1d:08:00 SRC=130.246.8.223 DST=130.246.140.144 LEN=60 TOS=0x10 PREC=0x00 TTL=63 ID=38958 DF PROTO=TCP SPT=33119 DPT=24 WINDOW=5840 RES=0x00 SYN URGP=0
200238	fougeres.esc.rl.ac.uk	warning	2005-04-27	11:07:14	kernel: [DENIED] IN=eth0 OUT= MAC=00:40:05:8b:06:c0:00:04:dc:21:26:1d:08:00 SRC=130.246.8.223 DST=130.246.140.144 LEN=60 TOS=0x10 PREC=0x00 TTL=63 ID=38956 DF PROTO=TCP SPT=33119 DPT=24 WINDOW=5840 RES=0x00 SYN URGP=0
200045	fougeres.esc.rl.ac.uk	warning	2005-04-26	15:41:19	[redacted]
200044	fougeres.esc.rl.ac.uk	warning	2005-04-26	15:41:16	[redacted]
199897	fougeres.esc.rl.ac.uk	warning	2005-04-26	10:58:27	[redacted]
					[redacted]

Tracking network scans

- Network scan alerts



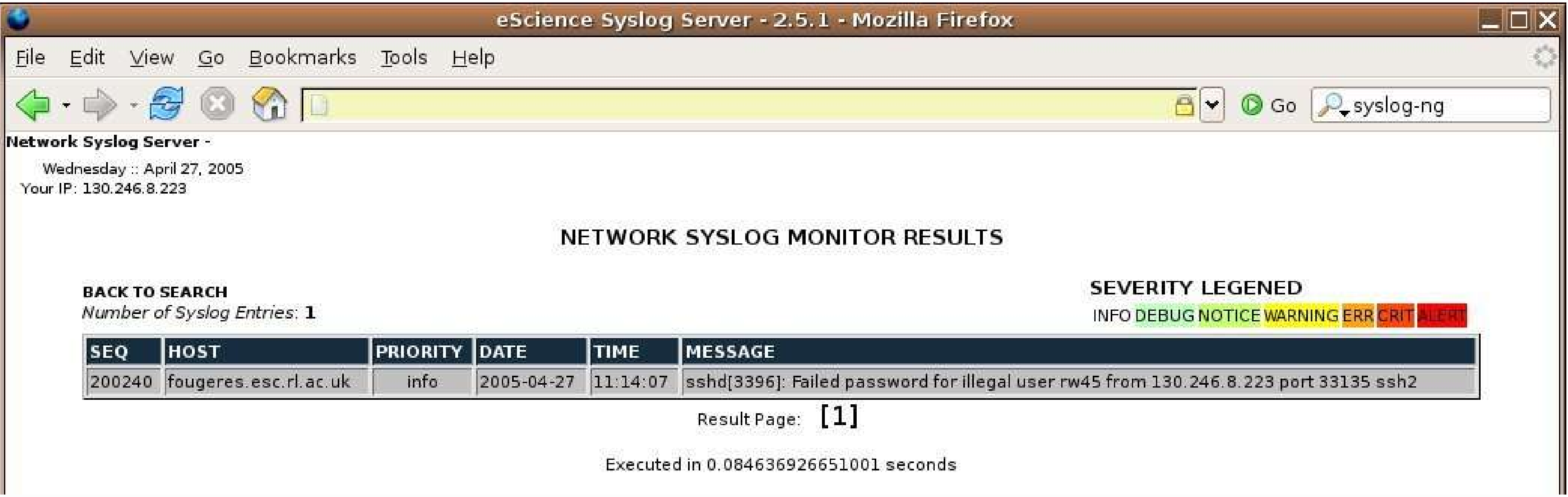
From: security@helpdesk.esc.rl.ac.uk
To: r.f.c.wartel@rl.ac.uk
Cc: n.m.hill@rl.ac.uk
Subject: [WARNING] Suspicious logs detected
Date: Wed, 27 Apr 2005 11:10:00 +0100 *(13:10 EEST)*

```
Hello,

Here are some suspicious log entries. You should have a look at it as it is not part of the normal network noise.

27 Apr 11:07:14 romain.esc.rl.ac.uk [TCP/33119] -> fougeres.esc.rl.ac.uk [TCP/24] (fougeres)
27 Apr 11:07:17 romain.esc.rl.ac.uk [TCP/33119] -> fougeres.esc.rl.ac.uk [TCP/24] (fougeres)
```

Tracking user logins

- Tracking user logins

```
romain@romain:~$ ssh rw45@fougeres.esc.rl.ac.uk
rw45@fougeres.esc.rl.ac.uk's password:
Permission denied, please try again.
```



Network Syslog Server -

Wednesday :: April 27, 2005
Your IP: 130.246.8.223

NETWORK SYSLOG MONITOR RESULTS

BACK TO SEARCH
Number of Syslog Entries: **1**

SEVERITY LEGENED
INFO DEBUG NOTICE WARNING ERR CRIT ALERT

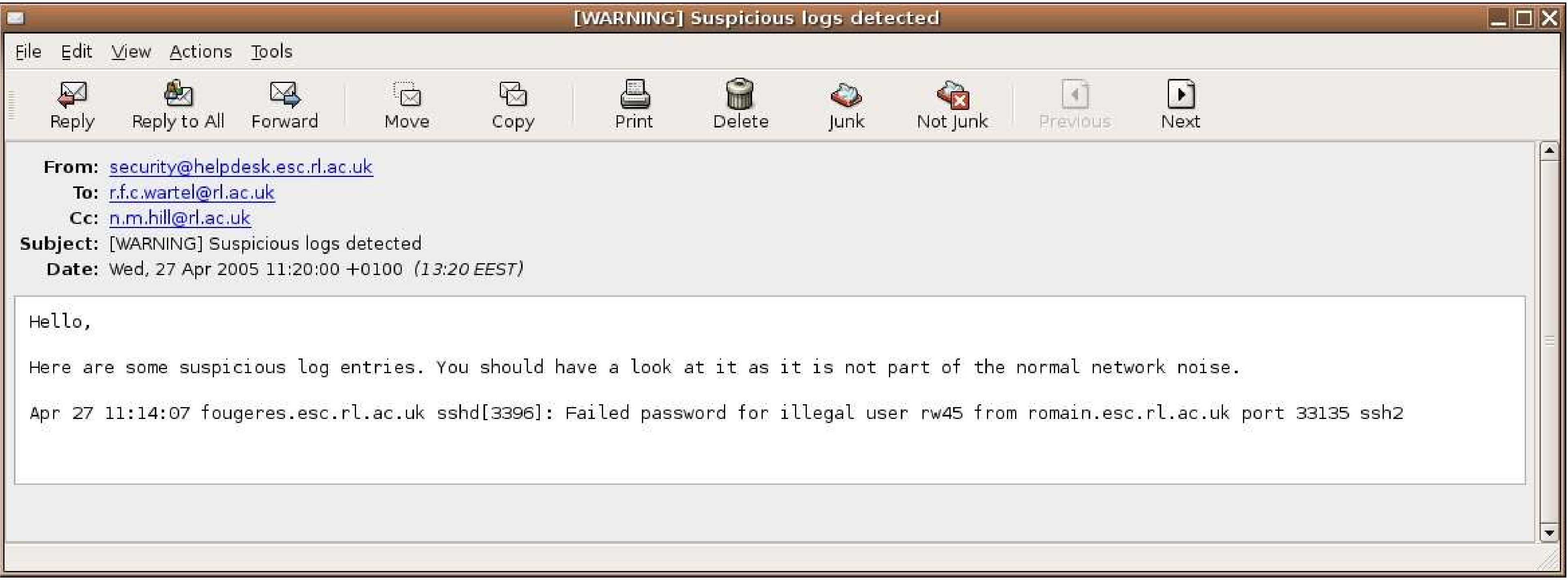
SEQ	HOST	PRIORITY	DATE	TIME	MESSAGE
200240	fougeres.esc.rl.ac.uk	info	2005-04-27	11:14:07	sshd[3396]: Failed password for illegal user rw45 from 130.246.8.223 port 33135 ssh2

Result Page: [1]

Executed in 0.084636926651001 seconds

Tracking user logins

- User logins alert:



From: security@helpdesk.esc.rl.ac.uk
To: r.f.c.wartel@rl.ac.uk
Cc: n.m.hill@rl.ac.uk
Subject: [WARNING] Suspicious logs detected
Date: Wed, 27 Apr 2005 11:20:00 +0100 *(13:20 EEST)*

```
Hello,

Here are some suspicious log entries. You should have a look at it as it is not part of the normal network noise.

Apr 27 11:14:07 fougeres.esc.rl.ac.uk sshd[3396]: Failed password for illegal user rw45 from romain.esc.rl.ac.uk port 33135 ssh2
```

Q&A