Linux Secure Server Distribution

Martin Poole
Quatermass Research

UKUUG Winter Conference 1999

Contents of this talk

- What is LSSD?
- Why produce LSSD?
- What does it consist of?
- Where has it been used?
- What had to change?
- What comes next?
What is LSSD?

- Basic operating system and utilities.
- Secure platform for network services.
- Selection of installable network applications.
- Framework for further secure development.

Why produce LSSD?

- To avoid traditional overheads.
- An alternative to traditional securing methodologies.
- To provide a basic platform for further experimentation and research.
Why produce LSSD?

- To avoid traditional overheads.
  - Most OSs are geared for traditional users.
  - Traditional installs include excess user tools

Why produce LSSD?

- An alternative to traditional securing methodologies.
  - Securing most OSs requires previous knowledge.
  - Securing most OSs is a subtractive operation.
  - Default configurations tend to be insecure.
  - Forget one service and you're dead.
Why produce LSSD?

- To provide a base platform for further experimentation and research.
- A minimalist base reduces the chances of adverse interaction.
- Application architecture has changed with internet growth.
- Security architecture has not received the same attention.

What does it consist of?

- Base operating system and maintenance utilities.
- Selection of optional network applications.
What does it consist of?

- Base operating system and maintenance utilities.
  - Originally based on Slackware 3.4
  - Kernel (currently 2.0.36/38)
  - libc 5.4.46
  - ssh v1.2.26
  - perl 5.005_02 with ssl, libwww and a few others.
  - optionally, Webmin.

What does it consist of?

- Selection of optional network applications.
  - sendmail 8.9.3, procmail, qpopper.
  - Apache 1.3.4, Apache 1.3.4 with mod_ssl.
  - squid, squidguard.
  - bind 8.2.2p5.
  - proftpd.
  - samba.
  - xinetd.
Where has it been used?

- Personal gateway.
- Co-Located Bastion Host.
- ISP Infrastructure.
- Corporate Infrastructure and DMZ.

Where has it been used?

- Personal gateway.
  - standard kernel firewall rules.
  - sendmail for SMTP mail delivery.
  - diald for connectivity.
Where has it been used?

- Co-Located Bastion Host.
- Web server.
- Sendmail
- Web-based reading.

Where has it been used?

- ISP Infrastructure.
- DNS servers.
- Mail servers.
- Web servers.
- Systems monitoring.
Where has it been used?

- Corporate infrastructure and DMZ.
  - DNS
  - Mail routing.
  - Monitoring.
  - Web Servers and Caches.
  - Firewalls.
What had to change?

- Full virtual hosts on all services - postponed.
- Read-Only primary filesystems.

What comes next?

- Upgrade to V2.2 kernel / Wait for V2.4 ?
- Upgrade to glibc2
- Change to RedHat base ?
- Change to Slackware 7.0 base ?
- Further virtualisation.
- World Domination or at least another beer.
The End - for now.

- Web Site
  - http://quatermass.co.uk/
  - ftp://quatermass.co.uk/
- Martin Poole
  - mpoole@quatermass.co.uk