Kali Linux's Experience

By Raphaël Hertzog
<hertzog@debian.org>
<buxy@kali.org>

DebConf 16
2016-07-05
Cape Town
Plan

- Presentation of Kali Linux
  - My role in Kali Linux
- Hardware and software infrastructure
- Structure of the distribution
  - Relationship with Debian Testing
- Packaging related workflows
- Quality assurance
- Problems and wishlist
Presentation of Kali Linux

- Debian derivative focused on penetration testing: https://www.kali.org
  - Successor of BackTrack since 2013
- Developed by Offensive Security
  - Penetration tests and security trainings
  - https://www.offensive-security.com
A popular distribution in its field

- >= 100K ISO downloads for each release
  - Dozens of mirrors worldwide
- Very active forums and IRC channel
- Reference distribution for many upstream developers of penetration testing/security software

→ a large base of Debian Testing users!
My role in Kali Linux

- Debian developer since 1998 working as consultant since 2004 (Freexian)
- Working with Offensive Security since 2012, doing:
  - Setup and maintenance of the packaging infrastructure
  - Packaging of many software
  - Training of other persons involved in packaging
  - Monitoring and fixes to keep the distribution in a working state
Hardware infrastructure

- Many rented servers and VM
  - Internal repository
  - Public archive: archive.kali.org
  - Mirror redirector (http.kali.org, cdimage.kali.org)
  - 6 Kali-managed mirrors (archive-X.kali.org)
  - 4 build servers
    - amd64/i386, armel, armhf, arm64
  - Quality assurance server
  - Management server
Management server

- Most services are managed with SaltStack
  - Easy to redeploy or to switch servers when needed
- SaltStack events coordinate some operations
  - Ex: central repository downloads daily ISO images from each build daemon upon reception of a “build-completed” notification.
- We created some useful “Salt formulas”
  - debootstrap, schroot, sbuild
- We contributed fixes to other formulas we use
Internal repository server

- Repositories managed by reprepro
- Accepts uploads by SSH
  - Source uploads from developers
  - Binary uploads from build daemons
- Enqueues build jobs on build daemons via SSH
- Centralizes ISO images built
- Imports packages from Debian, runs britney, pushes the public archive
Public archive : archive.kali.org

- Nginx to serve files over HTTP
- Rsync daemon with access restricted to official mirrors
- Debian's "archvsync" mirroring script
  - SSH triggered by internal repository every 6 hours
  - Also used to trigger downstream mirrors
- Firewall and archvsync managed by salt
  - List of official mirrors is managed as "salt pillar data" and shared with the mirror redirector
Mirror redirector: http.kali.org, cdimage.kali.org

- Managed by Mirrorbrain (apache module):
  - http://www.mirrorbrain.org
- Redirects users to a working mirror close to them (using GeoIP and optionally routing data)
  - Monitors mirrors for HTTP availability
  - For Kali, we also disable mirrors which are outdated
- Mirrorbrain is not yet in Debian but upstream provides .deb, help is welcome to package it
- Some rough sides but is working reliably
  - Returns 404 for files still existing on some of the mirrors
Build servers
amd64/i386, armel, armhf, arm64

• Package builds managed by “rebuilddd” with custom build scripts relying on sbuild:
  • Hacked in binNMU support in build scripts
  • Build chroots setup with salt's sbuild-formula
  • Packages uploaded back with SSH
• ISO image builds managed by “live-build”
  • Official releases
  • Daily builds
Quality assurance

- Private jenkins server with many jobs
  - All tests are restricted to amd64/i386 though.
  - Initially setup by Holger Levsen.
- Public bug tracker: https://bugs.kali.org
  - Mantis setup
Structure of the distribution

- Repositories layout
- Meta-packages
- Kali specific packages
Repositories layout

- **kali-dev-only**: 400 kali packages (and only that)
  - Where Kali developers upload packages
- **debian-testing**: plain mirror of Debian Testing
- **kali-dev**: debian-testing + kali-dev-only
  - In case of conflict, kali-dev-only takes precedence
- **kali-rolling**: britney-managed version of kali-dev
  - No delay, no RC bugs
  - Dependency/installability checks
  - Availability on all architectures
Metapackages

- Simple way to install a set of related packages
- Default Kali Linux system: kali-linux-full
- Topic based (kali-linux prefixed):
  - sdr, gpu, wireless, web, forensic, voip, pwtools, rfid, nethunter
- Desktop oriented (kali-desktop prefixed)
  - gnome, kde, lxde, xfce
- Special
  - all → all metapackages
  - top10 → most popular packages
Kali specific packages (1/2)

- **New packages:**
  - kali-defaults, kali-menu, kali-root-login, kali-meta, kali-archive-keyring

- **Forked packages:**
  - For branding / identification as a derivative:
    - base-files, desktop-base, rootskel-gtk
  - Desktop features:
    - gnome-shell-extensions: application menu with support of nested menus
    - gnome-terminal: bring back transparency
Kali specific packages (2/2)

- Forked packages
  - linux: adding wifi injection patch
  - init-systemHelpers: update-rc.d fork
  - debian-installer:
    - customized through preseed in initrd
    - netcfg (udeb): change default hostname #719101
    - net-retriever (udeb): use of kali-archive-keyring
- For support of kali codenames
  - debootstrap
  - debian-cd
- Live-build: EFI boot support
Packaging related workflows

- All packages in git.kali.org
- `git-buildpackage`, `pristine-tar`, 3.0 (quilt), `dh`, ...
- Synchronizing a forked package with Debian
  - `gbp import-dsc --debian-branch=debian foo.dsc`
  - `git checkout kali/master`
  - `git merge debian`
    - `dpkg-mergechangelogs configured`
- Deal with (britney) migration problems
Quality assurance

- Many jenkins jobs
  - Installing meta-packages in minimal chroots
  - Upgrading kali-rolling with all Kali packages from last snapshotted release to current
  - Building ISO images
  - Installing Kali from daily ISO image
- We would like to go further with autopkgtest
  - Running DEP-8 tests
  - Hooking results into britney
Problems affecting Kali

- Bugs filed: [http://deb.li/kalibugs](http://deb.li/kalibugs)
  - 64 bugs filed, 26 still open
- Missing features in reprepro:
  - Integration with britney
  - Keeping files of deleted packages for X days
  - Dealing with conflicting `.orig.tar.gz` during import
- Out-of-date Debian packages
  - MIA maintainers → pkg-security team to take over
Problems caused by Debian Testing usage (1/2)

- Packages being removed below us due to
  -Unhandled RC bugs
    - MIA maintainers
    - Maintainers not caring about testing
      → our plan: monitor how-can-i-help
  - QA team requesting removal for low popcon, etc.
    - Debian is not aware of usage of packages by derivatives → new tracker.debian.org feature?
- Release team kicking packages out to finish a transition
Problems caused by Debian Testing usage (2/2)

- Broken packages
  - Partial transitions
    - Allowed by incomplete dependencies
    - Untested combination that ends up not working
  - Upstream not caring about backwards compatibility
    - Debian tends to mitigate that but only later in the release cycle
- Bugs filed too late or at a non-RC severity
- Regressions with newer kernel releases
Our wishlist (1/2)

- Britney ↔ autopkgtest integration
- Missing reprepro features
- Debian caring more about Testing
  - Individual developers
  - Release team acknowledging that it's more than a tool to build stable and being more open to accept quick and temporary fixes
  - Real CUT team (Constantly Usable Testing)
- Improve reportbug behaviour on derivatives, see #703678
Our wishlist (2/2)

- More data about transitions
  - Automatically check if Kali is affected
  - Be aware when it has been completed
- Some application bundling support
  - ruby-on-rails web app with gazillions of gems
  - containerization for applications doing nasty/unclean operations as root
- Proper mirrorbrain package in Debian
- More volunteers in pkg-security
Questions?
Credits & License

- Content by Raphaël Hertzog
  https://raphaelhertzog.com
  License: GPL-2+

- Cliparts from https://openclipart.org
  License: Public domain

- OpenOffice.org template by Raphaël Hertzog
  http://raphaelhertzog.com/go/ooo-template
  License: GPL-2+

- Background image by Alexis Younes “ayo”
  http://www.73lab.com
  License: GPL-2+