Karlsruher Institut für Technologie

apt-dater:

Semi-automatisches Patchen von Linux-Rechnern

ATIS - Abteilung Technische Infrastruktur, Fakultät für Informatik

Problemstellung

- Software aktuell halten (Patches, vom Hersteller unterstützte Versionen, . . .),
- Systeme härten, bevor sie in Produktion gehen,
- Patchen,
- geeignete Konfiguration sicherstellen,
- Patches einspielen,
- gelegentlich Penetrationstests gegen die eigenen(!) Systeme fahren,
- Patches installieren,
- Nutzer sensibilisieren,
- nicht vergessen zu patchen!

Quelle: IT-Sicherheitsschulung – Tobias Dussa

Problemstellung

- N Rechner
- Mit 2 verschiedene Distributionen
- In jeweils 2 verschiedenen Major-Releases
- Pro Woche ~70 Mails über die DFN-Cert-Security-Mailingliste
- Pro Woche ~10 Security Announcements von RedHat
- Applikation XYZ hat einen Bug
- Welcher meiner Rechner ist betroffen ?
- Distri **A** hat eine Fix für Release **X**, Distri **B** einen für Release **Y**
- Distri **B** hat einen neuen Kernel, ist der schon gebootet ?

- **Wer blickt da noch durch ?**

Problemstellung

- Patchen jede Nacht per cron-Job im Blindflug?
  - No risk, no fun ….
  - Was ist mit meinen Applikation?
    - Werden die neu gestartet?
    - Was passiert, wenn die auf den Bauch fallen?
    - Was passiert, wenn nur die Libraries getauscht werden?

- Gar nichts machen ?
  - Never touch a running system…..

apt-dater

- Nicht nur für apt / Debian Pakete
- Sondern auch für yum / rpm – Systeme
- Minimal invasiv -> KISS
- Macht nichts von alleine
- Kein Daemon
- Man hat immer völlige Kontrolle darüber, was gemacht wird
- https://www-old.ibh.de/apt-dater/
- https://github.com/DE-IBH/apt-dater
- Voraussetzungen:
  - screen, ncurses, tcl/tk, ssh, sudo, perl

apt-dater

- Management-Host
  - **`/usr/bin/apt-dater`**
  - hosts.conf:
    ```
    [GruppeA]
    Hosts=hostA;hostB;
    [GruppeB]
    Hosts=hostX;hostY;
    ```
  - **`ssh-keygen …`**
  - **`ssh-copy-id …`**

- rpm-Clients
  - **`/usr/bin/apt-dater-host`** (für rpm)
  - **`useradd apt-dater …`**
  - /etc/sudoers:
    `apt-dater ALL=NOPASSWD: /usr/bin/yum`
  - **`~apt-dater/.ssh/authorized-keys`**

- dpkg-Clients
  - **`/usr/bin/apt-dater-host`** (für dpkg)
  - **`useradd apt-dater`**
  - /etc/sudoers:
    `apt-dater ALL=NOPASSWD: /usr/bin/apt-get, /usr/bin/aptitude`
  - **`~apt-dater/.ssh/authorized-keys`**

Exkurs: patchen mit yum

- yum check-update <=> apt-get update && apt list –upgradable

```
# yum check-update
openssl.x86_64                          1:1.0.1e-51.el7_2.7                     updates
openssl-libs.x86_64                     1:1.0.1e-51.el7_2.7                     updates
```

- yum update <=> apt-get upgrade

```
# yum update tzdata
[...]
================================================================================
 Package              Arch                 Version                  Repository             Size
================================================================================
Updating:
 tzdata               noarch               2016g-2.el7              updates               440 k
Transaction Summary
================================================================================
Upgrade  1 Package
Total download size: 440 k
Is this ok [y/d/N]: y
Downloading packages:
tzdata-2016g-2.el7.noarch.rpm                                | 440 kB  00:00:00
[...]
Running transaction
  Updating   : tzdata-2016g-2.el7.noarch                                    1/2
  Cleanup    : tzdata-2016f-1.el7.noarch                                    2/2
  Verifying  : tzdata-2016g-2.el7.noarch                                    1/2
  Verifying  : tzdata-2016f-1.el7.noarch                                    2/2
Updated:
  tzdata.noarch 0:2016g-2.el7
Complete!
```