Surviving the Zombie Apocalypse

Security in the Cloud − Containers, KVM and Xen

Ian Jackson <ian.jackson@eu.citrix.com>

FOSDEM 2015

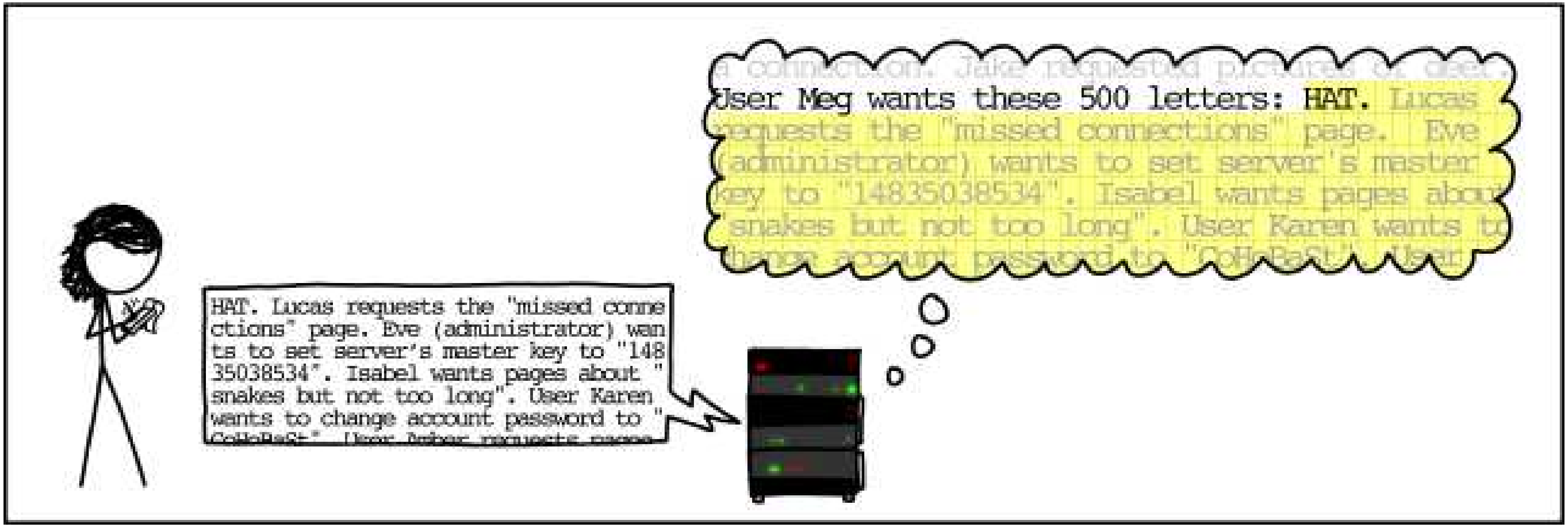
originally based on a talk and research by George Dunlap

"Some people make the mistake of thinking of containers as a better and faster way of running virtual machines. From a security point of view, containers are much weaker." - Dan Walsh, SELinux architect(?)

"There’s contentions all over the place that containers are not actually as secure as hypervisors. This is not really true. Parallels and Virtuozo, we’ve been running secure containers for at least 10 years." -James Bottomley, Linux Maintainer and Parallels CTO

"Virtual Machines might be more secure today, but containers are definitely catching up." -- Jerome Petazzoni, Senior Software Enginner at Docker

"You are absolutely deluded, if not stupid, if you think that a worldwide collection of software engineers who can’t write operating systems or applications without security holes, can then turn around and suddenly write virtualization layers without security holes."
-Theo de Raadt, OpenBSD project lead



a connection. Jake requested pictures of deer. User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about snakes but not too long". User Karen wants to change account password to "CoHoBaSt". User
HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about " snakes but not too long". User Karen wants to change account password to " CoHoBaSt". User Amber requests pages

From **http://xkcd.com/1354/** by Randall Munroe

Zombies only come out at night

Zombies are strong enough to break down a door or smash through a window, easily

But, zombies are usually too stupid to recognise a door or a window for what it is.

Some Free Software VM hosting technologies
Vulnerabilities published in 2014

	Xen PV	KVM+ QEMU	Linux as general container
Privilege escalation (guest−to−host)	0	3−5	7−9
Denial of service (by guest of host)	3	5−7	12
Information leak (from host to guest)	1	0	1

Some Free Software VM hosting technologies
Vulnerabilities published in 2014

	Xen PV	KVM+ QEMU	Linux as general container	Linux app container (non−root)
Privilege escalation (guest−to−host)	0	3−5	7−9	4
Denial of service (by guest of host)	3	5−7	12	3
Information leak (from host to guest)	1	0	1	1

Hosts only application, not guest OS