SiteHost

Hardened Hosting

Quintin Russ

OWASP New Zealand Chapter 2011
6th December 2011

About Me

- Quintin Russ
  - Technical Director, SiteHost
    - http://www.sitehost.co.nz
    - quintin@sitehost.co.nz
  - Web Developer in previous life
  - Focused on web infrastructure for last 5 years

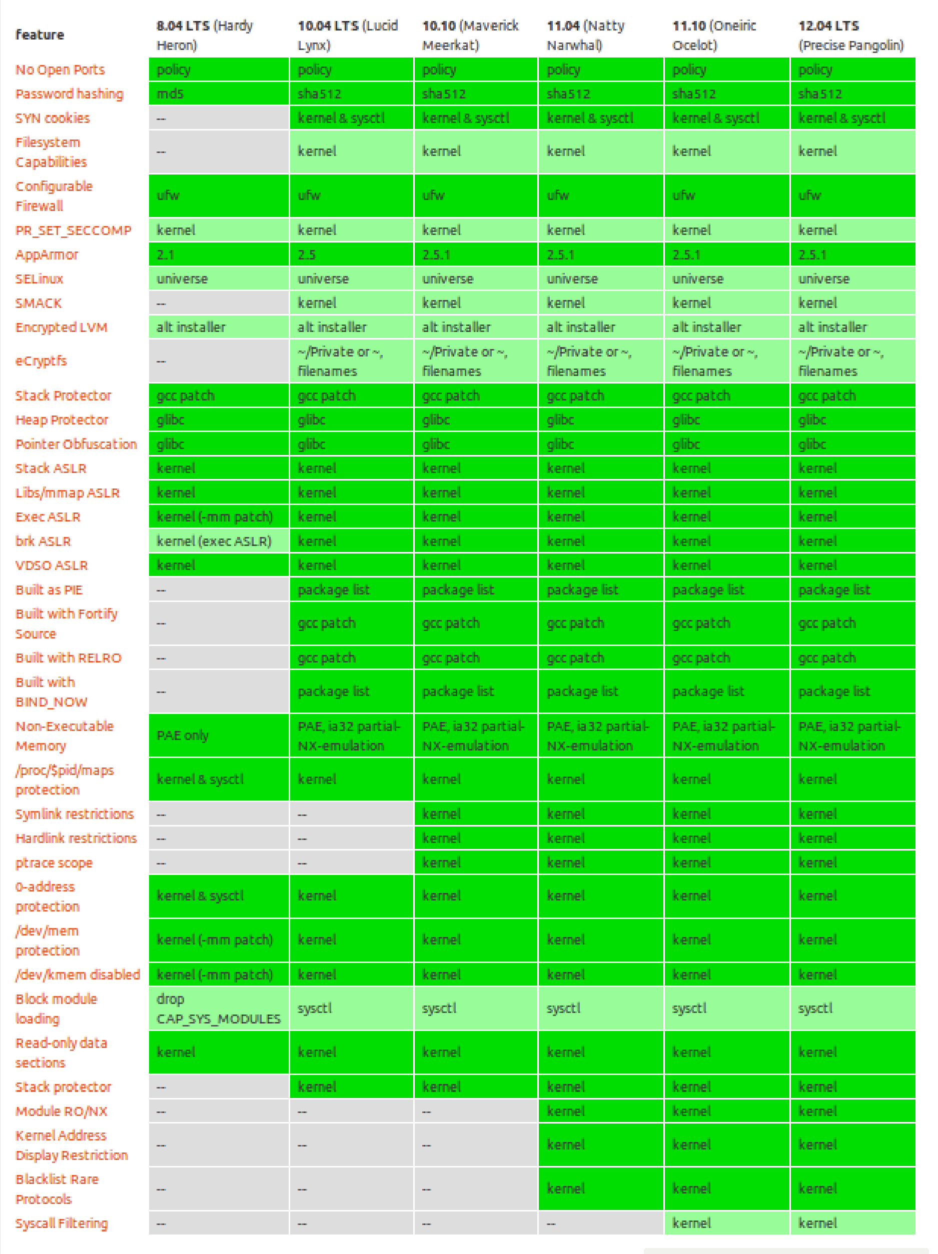
Disclaimer

- There is no substitute for bug-free code

Hardening

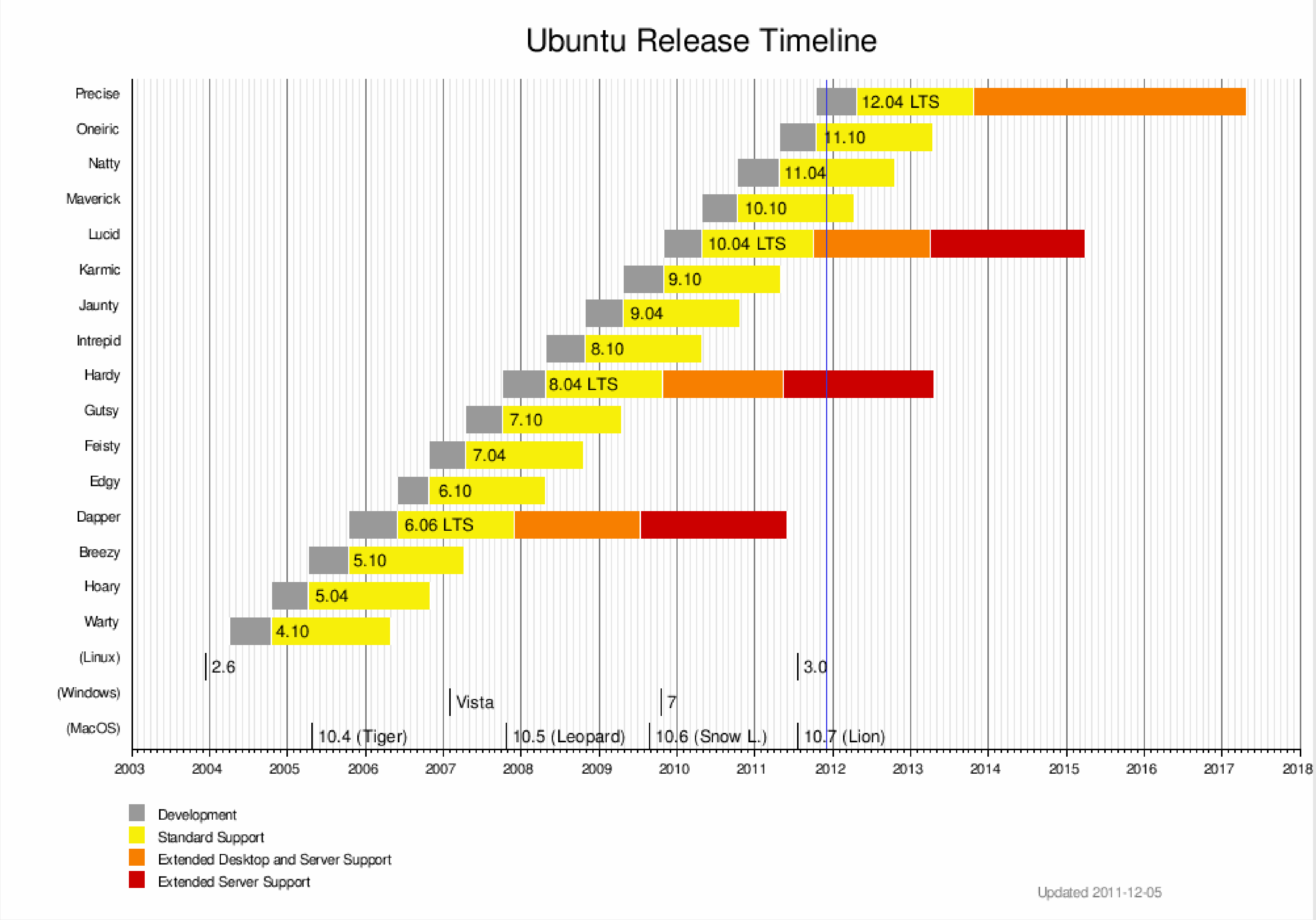
- Hardening a Linux web server
  - Searching returns a lot of information on this topic
    - Not very useful, focused on Linux less on Web
  - Start by picking the right distribution – Ubuntu
    - Their security features are continually getting better
    - Their LTS releases are supported for longer periods
  - https://wiki.ubuntu.com/Security/Features
  - http://en.wikipedia.org/wiki/List_of_Ubuntu_releases#Version_timeline

Ubuntu Security Features

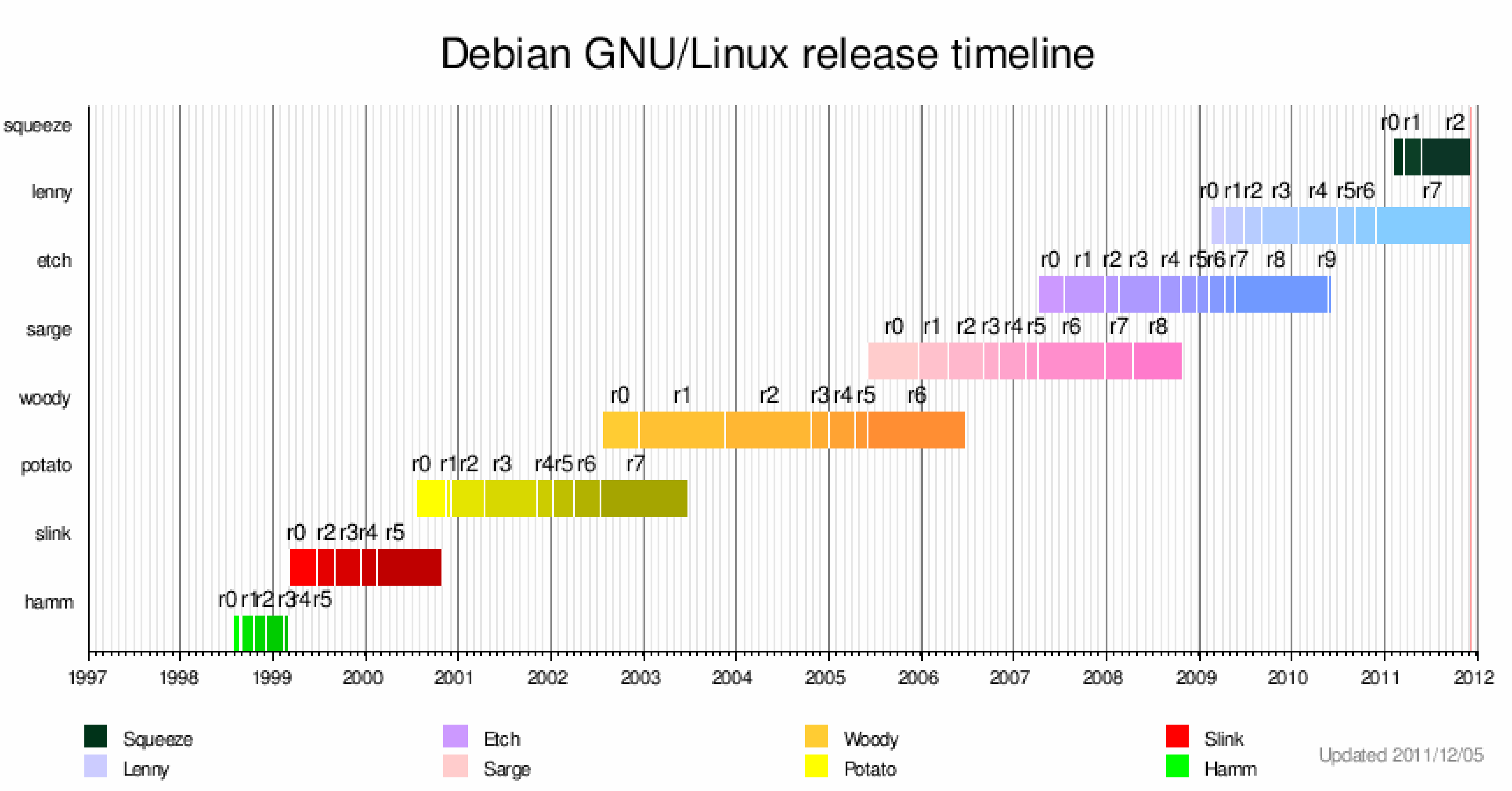


feature	**8.04 LTS** (Hardy Heron)	**10.04 LTS** (Lucid Lynx)	**10.10** (Maverick Meerkat)	**11.04** (Natty Narwhal)	**11.10** (Oneiric Ocelot)	**12.04 LTS** (Precise Pangolin)
No Open Ports	policy	policy	policy	policy	policy	policy
Password hashing	md5	sha512	sha512	sha512	sha512	sha512
SYN cookies	--	kernel & sysctl	kernel & sysctl	kernel & sysctl	kernel & sysctl	kernel & sysctl
Filesystem Capabilities	--	kernel	kernel	kernel	kernel	kernel
Configurable Firewall	ufw	ufw	ufw	ufw	ufw	ufw
PR_SET_SECCOMP	kernel	kernel	kernel	kernel	kernel	kernel
AppArmor	2.1	2.5	2.5.1	2.5.1	2.5.1	2.5.1
SELinux	universe	universe	universe	universe	universe	universe
SMACK	--	kernel	kernel	kernel	kernel	kernel
Encrypted LVM	alt installer	alt installer	alt installer	alt installer	alt installer	alt installer
eCryptfs	--	~/Private or ~, filenames	~/Private or ~, filenames	~/Private or ~, filenames	~/Private or ~, filenames	~/Private or ~, filenames
Stack Protector	gcc patch	gcc patch	gcc patch	gcc patch	gcc patch	gcc patch
Heap Protector	glibc	glibc	glibc	glibc	glibc	glibc
Pointer Obfuscation	glibc	glibc	glibc	glibc	glibc	glibc
Stack ASLR	kernel	kernel	kernel	kernel	kernel	kernel
Libs/mmap ASLR	kernel	kernel	kernel	kernel	kernel	kernel
Exec ASLR	kernel (-mm patch)	kernel	kernel	kernel	kernel	kernel
brk ASLR	kernel (exec ASLR)	kernel	kernel	kernel	kernel	kernel
VDSO ASLR	kernel	kernel	kernel	kernel	kernel	kernel
Built as PIE	--	package list	package list	package list	package list	package list
Built with Fortify Source	--	gcc patch	gcc patch	gcc patch	gcc patch	gcc patch
Built with RELRO	--	gcc patch	gcc patch	gcc patch	gcc patch	gcc patch
Built with BIND_NOW	--	package list	package list	package list	package list	package list
Non-Executable Memory	PAE only	PAE, ia32 partial-NX-emulation	PAE, ia32 partial-NX-emulation	PAE, ia32 partial-NX-emulation	PAE, ia32 partial-NX-emulation	PAE, ia32 partial-NX-emulation
/proc/$pid/maps protection	kernel & sysctl	kernel	kernel	kernel	kernel	kernel
Symlink restrictions	--	--	kernel	kernel	kernel	kernel
Hardlink restrictions	--	--	kernel	kernel	kernel	kernel
ptrace scope	--	--	kernel	kernel	kernel	kernel
0-address protection	kernel & sysctl	kernel	kernel	kernel	kernel	kernel
/dev/mem protection	kernel (-mm patch)	kernel	kernel	kernel	kernel	kernel
/dev/kmem disabled	kernel (-mm patch)	kernel	kernel	kernel	kernel	kernel
Block module loading	drop CAP_SYS_MODULES	sysctl	sysctl	sysctl	sysctl	sysctl
Read-only data sections	kernel	kernel	kernel	kernel	kernel	kernel
Stack protector	--	kernel	kernel	kernel	kernel	kernel
Module RO/NX	--	--	--	kernel	kernel	kernel
Kernel Address Display Restriction	--	--	--	kernel	kernel	kernel
Blacklist Rare Protocols	--	--	--	kernel	kernel	kernel
Syscall Filtering	--	--	--	--	kernel	kernel

Ubuntu Release Timeline



Debian Release Timeline



Basic Hardening

- Your (web?) server is soft by default
  - No Firewalling
  - Soft SSH config – remote root enabled / pw auth
  - Weak directory permissions
  - Web Server runs as a single user
    - Apache has /icons/ alias
  - Numerous other weak defaults often found
    - Weak passwords on MySQL (Percona builds)
    - Poor PHP defaults (magic quotes?)
    - Trace enabled in Apache (fixed in modern distros)

File Uploads

- File Uploads
  - Completely disabled is the best option
  - If you cannot disable then filter the uploads
  - Mod_Security - SecUploadApproveScript
  - Suhosin – suhosin.upload.verification_script
  - PHP – auto-prepend-file
    - Easy to customize behaviour on a global basis

File Uploads

- File Uploads – LFI to Remote Code Execution
  - PHP local file inclusion to arbitrary code execution
  - PHP uploads file to /tmp before running script
  - Just need to guess the filename to execute
  - Protect against with open_basedir restrictions
  - or... by completely disabling uploads
  - http://www.insomniasec.com/releases/whitepapers-presentations

Firewalling

- Firewalling
  - Outbound is very important on web servers
  - Whitelist if you can, blocking all other services, irc etc
  - Test first
    - iptables -I OUTPUT -m tcp -p tcp --dport 443 -j ACCEPT
    - then check counters: iptables -L -v

Firewalling

- Mod Security
  - Very good when configured correctly
    - I personally found the CRS to be too prohibative
    - WHM / cPanel distributed rules much less painful
      - Based on AtomicCorp.com rules
  - Can be configured to block known bad behaviour
  - Handy for blocking known vulnerabilities (timthumb.php)
  - Also have seen it identify other bad behaviour
  - I will go into this aspect in more detail in the future
  - https://www.owasp.org/index.php/Category:OWASP_ModSecurity_Core_Rule_Set_Project

Firewalling

- Example of good firewalling
  - Proftpd vulnerability exploited late 2010
  - Used reverse shell connect back on port 45295
  - More work to change this value to port 80 or 443
  - Harder to automate however
  - Ubuntu's stack protection helped mitigate exploitation

Firewalling

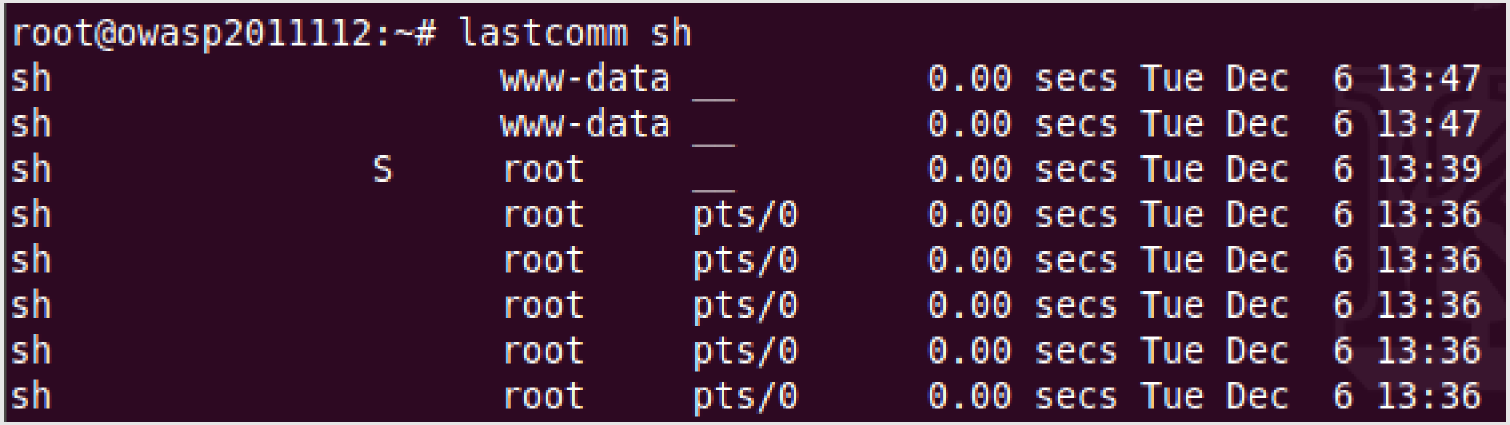
- Example of good firewalling
  - timthumb.php – included in thousands of WP Templates
  - Remote code execution bug – massively exploited
  - Customers asked us to loosen Mod_Security rules
  - Can also protect your network from outbound DoS
    - Is UDP outbound valid for your application?
  - Need to monitor number of dropped packets

Auditing + Automation

- Auditing
  - Lsat
    - Runs a number of host checks
    - Lists SUID binaries
    - Produces and Diffs MD5's of system / important files
  - Backups
    - Handy for should you get compromised
    - Not optional, make sure you manage them directly

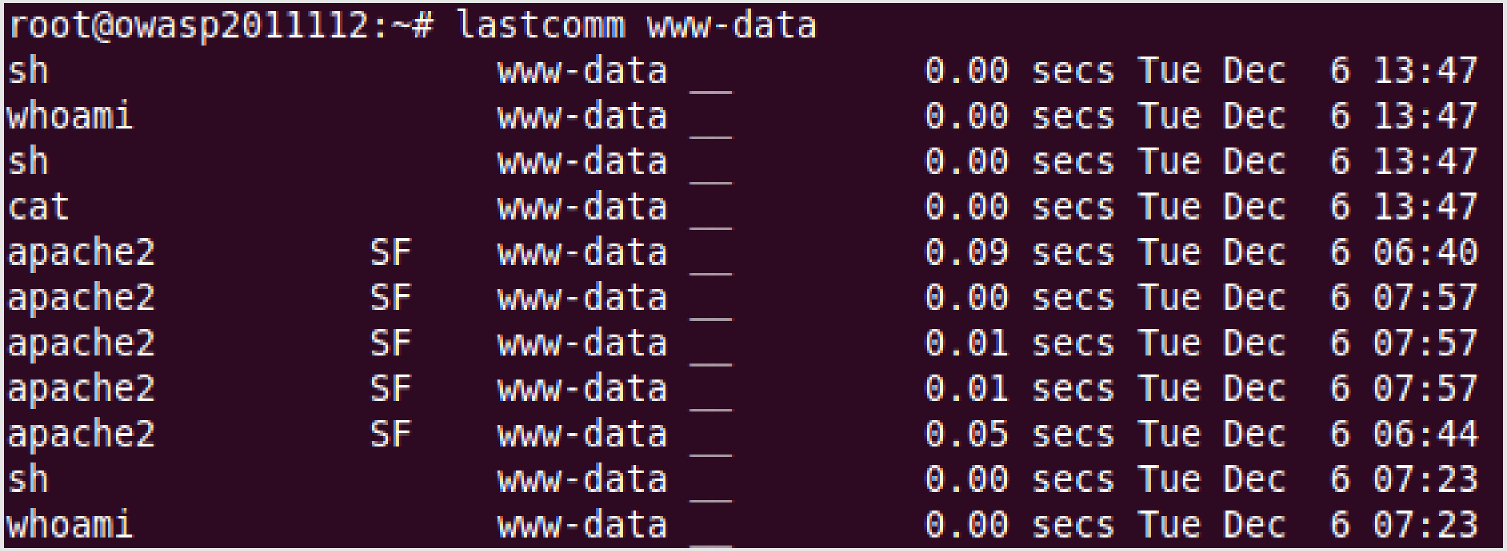
Auditing + Automation

- Process Accounting
  - apt-get install acct
  - No configuration “it just works”
  - Can filter by binary / command



```
root@owasp2011112:~# lastcomm sh
sh                     www-data __         0.00 secs Tue Dec  6 13:47
sh                     www-data __         0.00 secs Tue Dec  6 13:47
sh               S     root     __         0.00 secs Tue Dec  6 13:39
sh                     root     pts/0      0.00 secs Tue Dec  6 13:36
sh                     root     pts/0      0.00 secs Tue Dec  6 13:36
sh                     root     pts/0      0.00 secs Tue Dec  6 13:36
sh                     root     pts/0      0.00 secs Tue Dec  6 13:36
sh                     root     pts/0      0.00 secs Tue Dec  6 13:36
```

- Process Accounting
  - Can filter by user



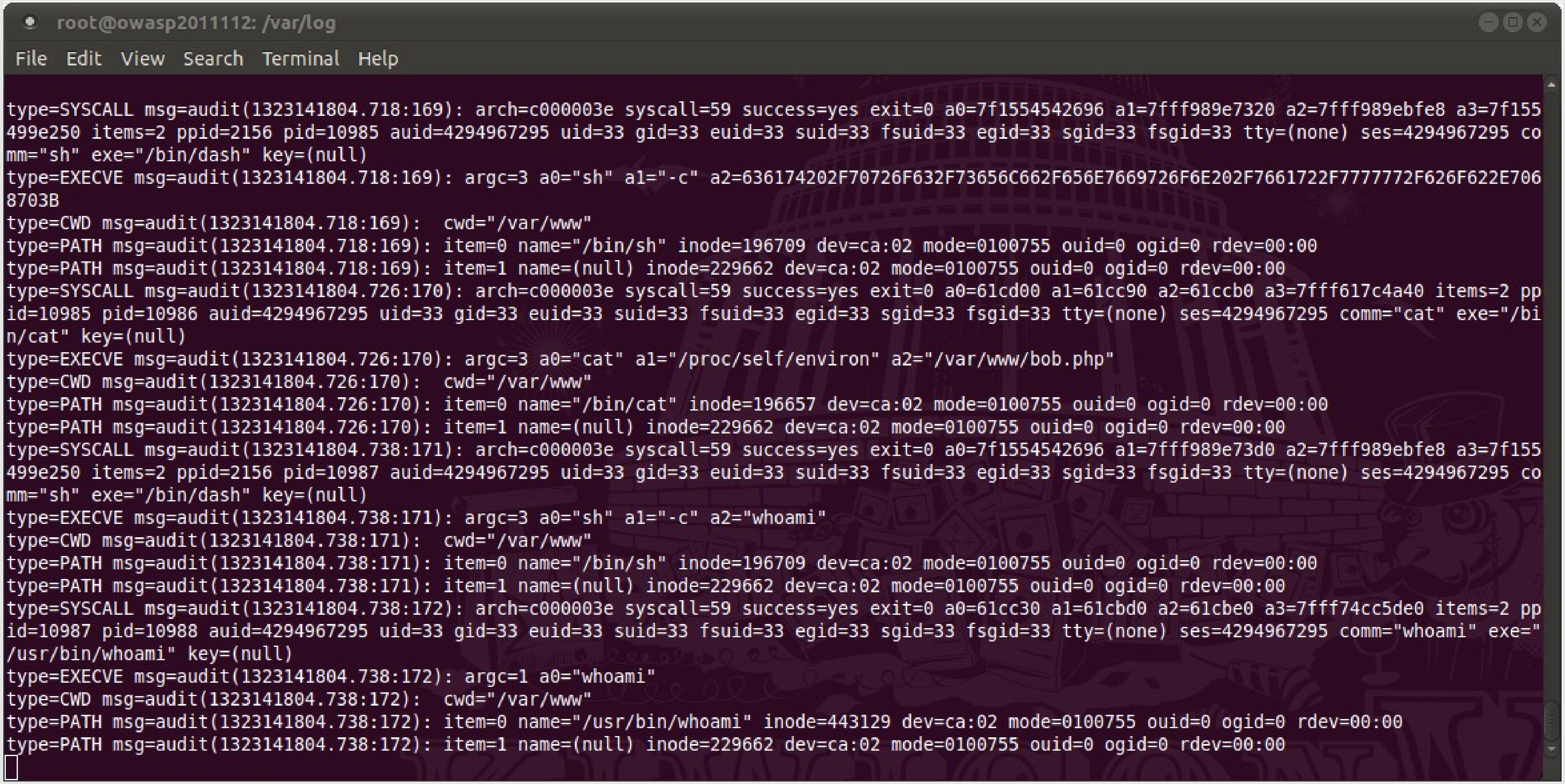
```
root@owasp2011112:~# lastcomm www-data
sh                      www-data __          0.00 secs Tue Dec  6 13:47
whoami                  www-data __          0.00 secs Tue Dec  6 13:47
sh                      www-data __          0.00 secs Tue Dec  6 13:47
cat                     www-data __          0.00 secs Tue Dec  6 13:47
apache2           SF    www-data __          0.09 secs Tue Dec  6 06:40
apache2           SF    www-data __          0.00 secs Tue Dec  6 07:57
apache2           SF    www-data __          0.01 secs Tue Dec  6 07:57
apache2           SF    www-data __          0.01 secs Tue Dec  6 07:57
apache2           SF    www-data __          0.05 secs Tue Dec  6 06:44
sh                      www-data __          0.00 secs Tue Dec  6 07:23
whoami                  www-data __          0.00 secs Tue Dec  6 07:23
```

  - Unfortunately it does not display arguments :(
  - It can also report CPU usage, using sa

Auditing + Automation

- AuditD – monitoring file and syscall events
    - Really easy to install - apt-get install auditd
    - Does need configuring however.
- Monitor read, write, attributes to /etc/passwd
    - auditctl -w /etc/passwd -p war -k password-file
- Monitor execution of /bin/dash binary
    - auditctl -w /bin/dash -k dash -p x
- Monitor EXECVE syscall from web server user
    - auditctl -S execve -A exit,always -F uid=33 -F gid=33
- Use an external syslog server if you can

- AuditD – monitoring file and syscall events


root@owasp2011112: /var/log
File Edit View Search Terminal Help

```
type=SYSCALL msg=audit(1323141804.718:169): arch=c000003e syscall=59 success=yes exit=0 a0=7f1554542696 a1=7fff989e7320 a2=7fff989ebfe8 a3=7f155
499e250 items=2 ppid=2156 pid=10985 auid=4294967295 uid=33 gid=33 euid=33 suid=33 fsuid=33 egid=33 sgid=33 fsgid=33 tty=(none) ses=4294967295 co
mm="sh" exe="/bin/dash" key=(null)
type=EXECVE msg=audit(1323141804.718:169): argc=3 a0="sh" a1="-c" a2=636174202F70726F632F73656C662F656E7669726F6E202F7661722F7777772F626F622E706
8703B
type=CWD msg=audit(1323141804.718:169):  cwd="/var/www"
type=PATH msg=audit(1323141804.718:169): item=0 name="/bin/sh" inode=196709 dev=ca:02 mode=0100755 ouid=0 ogid=0 rdev=00:00
type=PATH msg=audit(1323141804.718:169): item=1 name=(null) inode=229662 dev=ca:02 mode=0100755 ouid=0 ogid=0 rdev=00:00
type=SYSCALL msg=audit(1323141804.726:170): arch=c000003e syscall=59 success=yes exit=0 a0=61cd00 a1=61cc90 a2=61ccb0 a3=7fff617c4a40 items=2 pp
id=10985 pid=10986 auid=4294967295 uid=33 gid=33 euid=33 suid=33 fsuid=33 egid=33 sgid=33 fsgid=33 tty=(none) ses=4294967295 comm="cat" exe="/bi
n/cat" key=(null)
type=EXECVE msg=audit(1323141804.726:170): argc=3 a0="cat" a1="/proc/self/environ" a2="/var/www/bob.php"
type=CWD msg=audit(1323141804.726:170):  cwd="/var/www"
type=PATH msg=audit(1323141804.726:170): item=0 name="/bin/cat" inode=196657 dev=ca:02 mode=0100755 ouid=0 ogid=0 rdev=00:00
type=PATH msg=audit(1323141804.726:170): item=1 name=(null) inode=229662 dev=ca:02 mode=0100755 ouid=0 ogid=0 rdev=00:00
type=SYSCALL msg=audit(1323141804.738:171): arch=c000003e syscall=59 success=yes exit=0 a0=7f1554542696 a1=7fff989e73d0 a2=7fff989ebfe8 a3=7f155
499e250 items=2 ppid=2156 pid=10987 auid=4294967295 uid=33 gid=33 euid=33 suid=33 fsuid=33 egid=33 sgid=33 fsgid=33 tty=(none) ses=4294967295 co
mm="sh" exe="/bin/dash" key=(null)
type=EXECVE msg=audit(1323141804.738:171): argc=3 a0="sh" a1="-c" a2="whoami"
type=CWD msg=audit(1323141804.738:171):  cwd="/var/www"
type=PATH msg=audit(1323141804.738:171): item=0 name="/bin/sh" inode=196709 dev=ca:02 mode=0100755 ouid=0 ogid=0 rdev=00:00
type=PATH msg=audit(1323141804.738:171): item=1 name=(null) inode=229662 dev=ca:02 mode=0100755 ouid=0 ogid=0 rdev=00:00
type=SYSCALL msg=audit(1323141804.738:172): arch=c000003e syscall=59 success=yes exit=0 a0=61cc30 a1=61cbd0 a2=61cbe0 a3=7fff74cc5de0 items=2 pp
id=10987 pid=10988 auid=4294967295 uid=33 gid=33 euid=33 suid=33 fsuid=33 egid=33 sgid=33 fsgid=33 tty=(none) ses=4294967295 comm="whoami" exe="
/usr/bin/whoami" key=(null)
type=EXECVE msg=audit(1323141804.738:172): argc=1 a0="whoami"
type=CWD msg=audit(1323141804.738:172):  cwd="/var/www"
type=PATH msg=audit(1323141804.738:172): item=0 name="/usr/bin/whoami" inode=443129 dev=ca:02 mode=0100755 ouid=0 ogid=0 rdev=00:00
type=PATH msg=audit(1323141804.738:172): item=1 name=(null) inode=229662 dev=ca:02 mode=0100755 ouid=0 ogid=0 rdev=00:00
```

More Hardening

- Apparmor / SELinux
  - Are a sysadmins worst enemy
  - A lot of documentation tells you to turn these off
  - Can be very helpful depending on your environment
  - Will go into these technologies in a future talk

Thank you for listening, questions?

We're Hiring!

Hardened Hosting

Quintin Russ
quintin@sitehost.co.nz