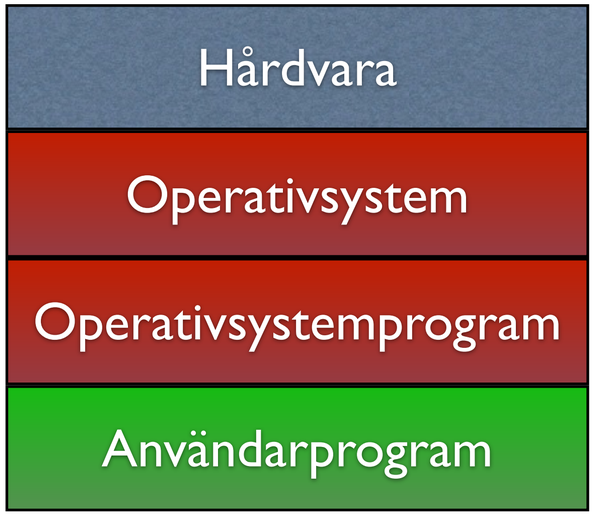
Nätverkssäkerhet
Operativsystemssäkerhet

Marcus Wilhelmsson
marcus.wilhelmsson@lnu.se

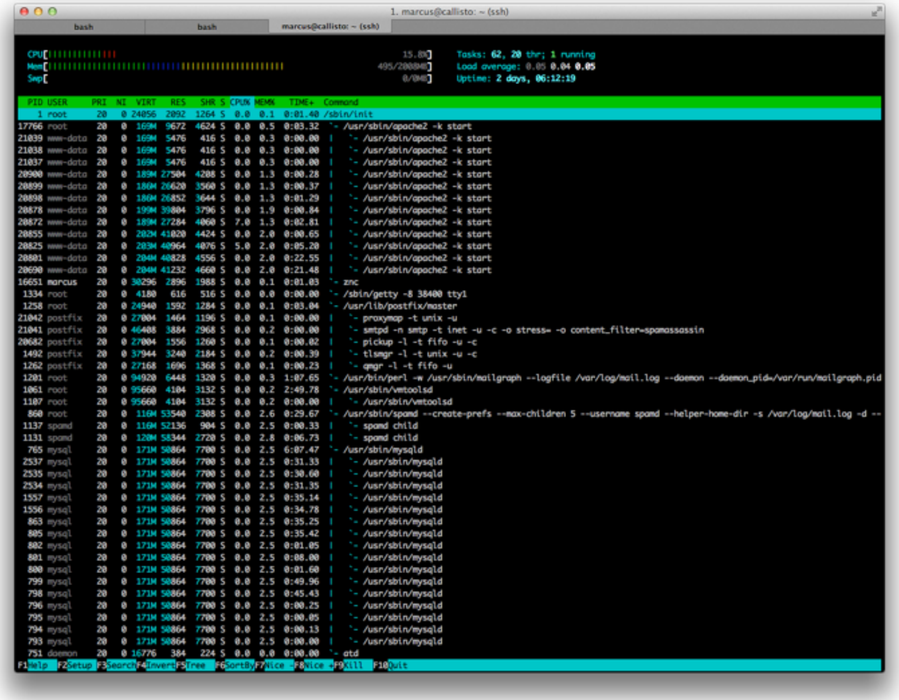
Innehåll

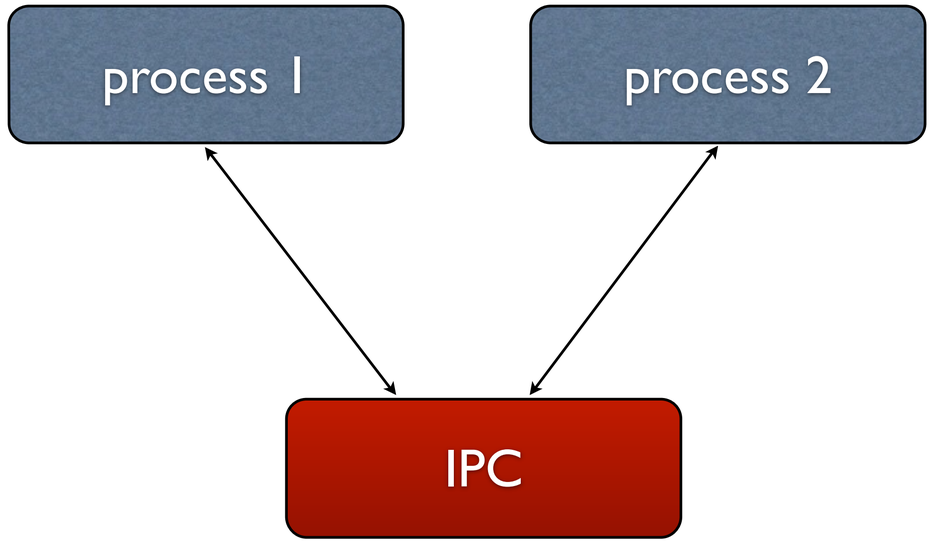
- Operativsystem - övergripande
- Processer och processsäkerhet
- Minne och filsystem
- Programvarusäkerhet

Kärnan och I/O



Processer


1. marcus@callisto: ~ (ssh)
bash
bash
marcus@callisto: ~ (ssh)
CPU[
15.8%]
Mem[
405/2008MB]
Swp[
0/0MB]
Tasks: 62, 20 thr; 1 running
Load average: 0.05 0.04 0.05
Uptime: 2 days, 06:12:19
PID USER PRI NI VIRT RES SHR S CPU% MEM% TIME+ Command
1 root 20 0 24056 2092 1264 S 0.0 0.1 0:01.40 /sbin/init
17766 root 20 0 169M 9672 4624 S 0.0 0.5 0:03.32 `- /usr/sbin/apache2 -k start
21039 www-data 20 0 169M 5476 416 S 0.0 0.3 0:00.00 | `- /usr/sbin/apache2 -k start
21038 www-data 20 0 169M 5476 416 S 0.0 0.3 0:00.00 | `- /usr/sbin/apache2 -k start
21037 www-data 20 0 169M 5476 416 S 0.0 0.3 0:00.00 | `- /usr/sbin/apache2 -k start
20900 www-data 20 0 185M 27504 4208 S 0.0 1.3 0:00.28 | `- /usr/sbin/apache2 -k start
20899 www-data 20 0 186M 26620 3560 S 0.0 1.3 0:00.37 | `- /usr/sbin/apache2 -k start
20898 www-data 20 0 186M 26852 3644 S 0.0 1.3 0:01.29 | `- /usr/sbin/apache2 -k start
20878 www-data 20 0 199M 39804 3796 S 0.0 1.9 0:00.84 | `- /usr/sbin/apache2 -k start
20872 www-data 20 0 189M 27284 4060 S 7.0 1.3 0:02.81 | `- /usr/sbin/apache2 -k start
20855 www-data 20 0 202M 41020 4424 S 0.0 2.0 0:00.65 | `- /usr/sbin/apache2 -k start
20825 www-data 20 0 203M 40964 4876 S 5.0 2.0 0:05.20 | `- /usr/sbin/apache2 -k start
20801 www-data 20 0 204M 40828 4556 S 0.0 2.0 0:22.55 | `- /usr/sbin/apache2 -k start
20690 www-data 20 0 204M 41232 4660 S 0.0 2.0 0:21.48 | `- /usr/sbin/apache2 -k start
16651 marcus 20 0 30296 2896 1988 S 0.0 0.1 0:01.03 `- znc
1334 root 20 0 4180 616 516 S 0.0 0.0 0:00.00 `- /sbin/getty -8 38400 tty1
1258 root 20 0 24940 1592 1284 S 0.0 0.1 0:03.04 `- /usr/lib/postfix/master
21042 postfix 20 0 27004 1464 1196 S 0.0 0.1 0:00.00 | `- proxymap -t unix -u
21041 postfix 20 0 46408 3884 2968 S 0.0 0.2 0:00.00 | `- smtpd -n smtp -t inet -u -c -o stress= -o content_filter=spamassassin
20642 postfix 20 0 27004 1556 1260 S 0.0 0.1 0:00.02 | `- pickup -l -t fifo -u -c
1492 postfix 20 0 37944 3240 2184 S 0.0 0.2 0:00.39 | `- tlsmgr -l -t unix -u -c
1262 postfix 20 0 27168 1696 1368 S 0.0 0.1 0:00.23 | `- qmgr -l -t fifo -u
1201 root 20 0 94920 6448 1320 S 0.0 0.3 1:07.65 `- /usr/bin/perl -w /usr/sbin/mailgraph --logfile /var/log/mail.log --daemon --daemon_pid=/var/run/mailgraph.pid
1061 root 20 0 95660 4104 3132 S 0.0 0.2 2:49.78 `- /usr/sbin/vmtoolsd
1107 root 20 0 95660 4104 3132 S 0.0 0.2 0:00.00 | `- /usr/sbin/vmtoolsd
860 root 20 0 116M 53540 2308 S 0.0 2.6 0:29.67 `- /usr/sbin/spamd --create-prefs --max-children 5 --username spamd --helper-home-dir -s /var/log/mail.log -d --
1137 spamd 20 0 116M 52136 904 S 0.0 2.5 0:00.33 | `- spamd child
1131 spamd 20 0 120M 58344 2720 S 0.0 2.8 0:06.73 | `- spamd child
765 mysql 20 0 171M 50864 7700 S 0.0 2.5 6:07.47 `- /usr/sbin/mysqld
2537 mysql 20 0 171M 50864 7700 S 0.0 2.5 0:31.33 | `- /usr/sbin/mysqld
2535 mysql 20 0 171M 50864 7700 S 0.0 2.5 0:30.60 | `- /usr/sbin/mysqld
2534 mysql 20 0 171M 50864 7700 S 0.0 2.5 0:31.35 | `- /usr/sbin/mysqld
1557 mysql 20 0 171M 50864 7700 S 0.0 2.5 0:35.14 | `- /usr/sbin/mysqld
1556 mysql 20 0 171M 50864 7700 S 0.0 2.5 0:34.78 | `- /usr/sbin/mysqld
863 mysql 20 0 171M 50864 7700 S 0.0 2.5 0:35.25 | `- /usr/sbin/mysqld
805 mysql 20 0 171M 50864 7700 S 0.0 2.5 0:35.42 | `- /usr/sbin/mysqld
802 mysql 20 0 171M 50864 7700 S 0.0 2.5 0:01.05 | `- /usr/sbin/mysqld
801 mysql 20 0 171M 50864 7700 S 0.0 2.5 0:08.00 | `- /usr/sbin/mysqld
800 mysql 20 0 171M 50864 7700 S 0.0 2.5 0:01.60 | `- /usr/sbin/mysqld
799 mysql 20 0 171M 50864 7700 S 0.0 2.5 0:49.96 | `- /usr/sbin/mysqld
798 mysql 20 0 171M 50864 7700 S 0.0 2.5 0:45.43 | `- /usr/sbin/mysqld
796 mysql 20 0 171M 50864 7700 S 0.0 2.5 0:00.25 | `- /usr/sbin/mysqld
795 mysql 20 0 171M 50864 7700 S 0.0 2.5 0:00.05 | `- /usr/sbin/mysqld
794 mysql 20 0 171M 50864 7700 S 0.0 2.5 0:00.13 | `- /usr/sbin/mysqld
793 mysql 20 0 171M 50864 7700 S 0.0 2.5 0:00.00 | `- /usr/sbin/mysqld
751 daemon 20 0 16776 384 224 S 0.0 0.0 0:00.00 `- atd
F1Help F2Setup F3Search F4Invert F5Tree F6SortBy F7Nice - F8Nice + F9Kill F10Quit


process 1
process 2
IPC

Filsystemet

- Filåtkomst
- Filrättigheter
- ACL- och UNIX-rättigheter

Minneshantering

- Minnesåtkomst
- Virtuellt minne
  - Sidfel (page fault)

Processäkerhet

- Trust
- Loggning

Minnes- och filsystemssäkerhet

- Virtuellt minne
- Lösenord
- Setuid

Program och applikationssäkerhet

- Kompilering och länkning
- Buffer overflows

SELinux

- MAC-system för Linux
- Utvecklat av NSA
- Komplext men mycket kraftfullt

Distributioner

- CentOS / RHEL

- Ubuntu
- SUSE
- etc.

Policy

- Targeted
- MLS

SELinux == label(s)

- Allt har en label
  - Processer
  - Filer och kataloger

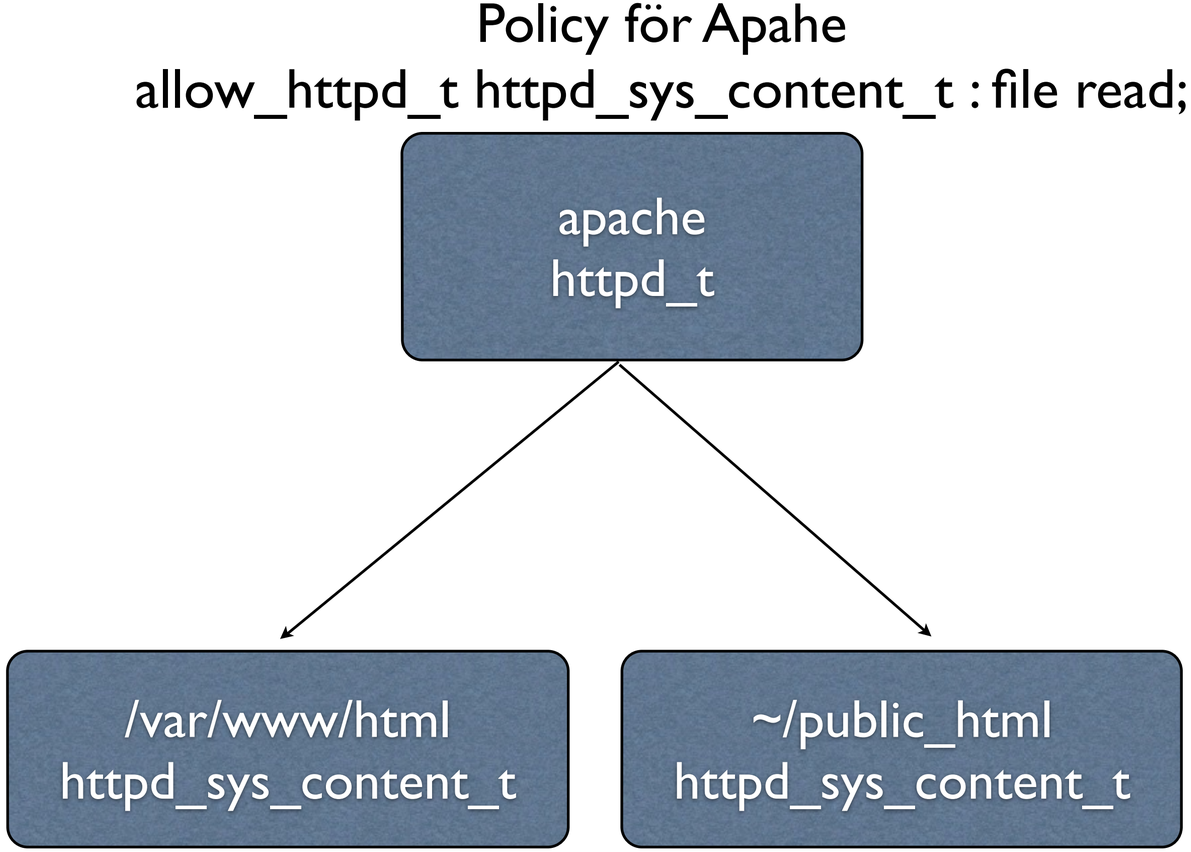
- Allt kontrolleras av kärnan

label exempel

- En label består av fyra delar
  - user (används ej i targeted-policyn)
  - role (används ej i targeted-policyn)
  - type (viktigaste att komma ihåg)
  - MLS (Multi Level Security) /MCS (Multi Category System)

type-exempel

- Apache får läsa vissa kataloger
- Skulle man t.ex. försöka läsa /etc/shadow skulle man få permission denied



Att läsa av labels

- Använd -Z
  - ls
  - id
  - ps
  - etc.

Hur sätts labels?

- Program som är medvetna om SELinux
- Användarskapade filer
- Loginprogram (ger dig din standardlabel)

Övergångar

- Fil
  - Process A_t skapar en fil i katalogen B_t med labeln C_t
  - dhclient_t skapar resolv.conf i katalogen etc_t med labeln net_conf_t
- Process
  - Process A_t exekverar fil B_exec_t, övergår till process B_t
  - user_t exekverar passwd_exec_t som övergår till passwd_t

Vad orsakar fel?

- Något är fel med dina labels
- Minsta möjliga privilegier jämfört med rimliga privilegier
- Buggar
- Du har blivit hackad

Exempel och demo