

# Linux Hardening

Compass Security Network  
Computing AG  
Werkstrasse 20  
Postfach 2038  
CH-8645 Jona

Tel +41 55 214 41 60  
Fax +41 55 214 41 61

[team@csnc.ch](mailto:team@csnc.ch)  
[www.csnc.ch](http://www.csnc.ch)

## Enable **DEP**:

- ✦ **Default** since like forever
- ✦ (for old cpus: kernel.exec-shield = 1)
- ✦ To disable for a binary: gcc -z noexecstack

## Enable **ASLR**:

- ✦ **Default** since like forever
- ✦ /proc/sys/kernel/randomize\_va\_space = 2

## Enable **Stack protector**:

- ✦ -fstack-protector (**Default**)
- ✦ -fstack-protector-all (ALL Functions)
- ✦ -fstack-protector-strong (Better)

## More Compiler options:

- ✦ **-D\_FORTIFY\_SOURCE=2**
  - ✦ FORTIFY\_SOURCE provides (lightweight) buffer overflow checks for the following functions:
    - ✦ memcpy, mempcpy, memmove, memset, strcpy, stpcpy, strncpy, strcat, strncat, sprintf, vsprintf, snprintf, vsnprintf, gets.
  - ✦ Compile time warnings
  - ✦ **Default** in Ubuntu
- ✦ **Formatstring**
  - ✦ **Default** in Ubuntu
  - ✦ -Wformat -Wformat-security
- ✦ **Full Static Relocation:**
  - ✦ **Default** in Ubuntu
  - ✦ -Wl,-z-,relro -Wl,-z,now
- ✦ **Position independent code**
  - ✦ **NOT Default** in Ubuntu (*performance penalty*)
  - ✦ -pie -fPIE

# Ubuntu Packages Compiled as PIE



Source package	8.04 LTS	9.04	9.10	10.04 LTS	10.10	11.04	11.10
openssh (native)	yes	yes	yes	yes	yes	yes	yes
apache2	--	yes	yes	yes	yes	yes	yes
bind9	--	yes	yes	yes	yes	yes	yes
openldap	--	yes	yes	yes	yes	yes	yes
postfix	--	yes	yes	yes	yes	yes	yes
cups	--	yes	yes	yes	yes	yes	yes
postgresql-8.3	--	yes	yes	yes	yes	yes	yes
samba (native)	--	yes	yes	yes	yes	yes	yes
dovecot	--	yes	yes	yes	yes	yes	yes
dhcp3	--	yes	yes	yes	yes	yes	yes
ntp	--	--	yes	yes	yes	yes	yes
amavisd-new	--	--	yes	yes	yes	yes	yes
squid	--	--	yes	yes	yes	yes	yes
cyrus-sasl2	--	--	yes	yes	yes	yes	yes
exim4	--	--	yes	yes	yes	yes	yes
nagios3	--	--	yes	yes	yes	yes	yes
nagios-plugins	--	--	yes	yes	yes	yes	yes
xinetd	--	--	yes	yes	yes	yes	yes

## Ubuntu 16.10: PIE everywhere ?!

### Built as PIE

All programs built as Position Independent Executables (PIE) with "-fPIE -pie" can take advantage of the exec ASLR. This protects against "return-to-text" and generally frustrates memory corruption attacks. This requires centralized changes to the compiler options when building the entire archive. PIE has a large (5-10%) performance penalty on architectures with small numbers of general registers (e.g. x86), so it should only be used for a **select number of security-critical packages** (some upstreams natively support building with PIE, other require the use of "hardening-wrapper" to force on the correct compiler and linker flags). PIE on 64-bit architectures do not have the same penalties, and will eventually be made the default (as of 16.10, it is the default on amd64, ppc64el and s390x).



# Ubuntu Packages compiled as PIE - 18.04



COMMAND	PID	RELRO	STACK	CANARY	SECCOMP	NX/PaX	PIE	FORTIFY
systemd	1	Full RELRO	Canary	found	Seccomp-bpf	NX enabled	PIE enabled	Yes
sshd	129631	Full RELRO	Canary	found	Seccomp-bpf	NX enabled	PIE enabled	Yes
bash	129672	Full RELRO	Canary	found	Seccomp-bpf	NX enabled	PIE enabled	Yes
tmux: client	129702	Full RELRO	Canary	found	Seccomp-bpf	NX enabled	PIE enabled	Yes
login	1299	Full RELRO	Canary	found	Seccomp-bpf	NX enabled	PIE enabled	Yes
rsyslogd	129948	Full RELRO	Canary	found	Seccomp-bpf	NX enabled	PIE enabled	Yes
systemd-network	130214	Full RELRO	Canary	found	Seccomp-bpf	NX enabled	PIE enabled	Yes
systemd-resolve	130220	Full RELRO	Canary	found	Seccomp-bpf	NX enabled	PIE enabled	Yes
systemd-journal	130225	Full RELRO	Canary	found	Seccomp-bpf	NX enabled	PIE enabled	Yes
systemd	1339	Full RELRO	Canary	found	Seccomp-bpf	NX enabled	PIE enabled	Yes
(sd-pam)	1340	Full RELRO	Canary	found	Seccomp-bpf	NX enabled	PIE enabled	Yes
bash	1350	Full RELRO	Canary	found	Seccomp-bpf	NX enabled	PIE enabled	Yes
accounts-daemon	149	Full RELRO	Canary	found	Seccomp-bpf	NX enabled	PIE enabled	Yes
systemd-logind	150	Full RELRO	Canary	found	Seccomp-bpf	NX enabled	PIE enabled	Yes
cron	153	Full RELRO	Canary	found	Seccomp-bpf	NX enabled	PIE enabled	Yes
networkd-dispat	159	Partial RELRO	Canary	found	Seccomp-bpf	NX enabled	No PIE	Yes
dbus-daemon	163	Full RELRO	Canary	found	Seccomp-bpf	NX enabled	PIE enabled	Yes
agetty	179	Full RELRO	Canary	found	Seccomp-bpf	NX enabled	PIE enabled	Yes
sshd	187	Full RELRO	Canary	found	Seccomp-bpf	NX enabled	PIE enabled	Yes
tmux: server	24721	Full RELRO	Canary	found	Seccomp-bpf	NX enabled	PIE enabled	Yes
bash	24722	Full RELRO	Canary	found	Seccomp-bpf	NX enabled	PIE enabled	Yes
bash	24746	Full RELRO	Canary	found	Seccomp-bpf	NX enabled	PIE enabled	Yes
bash	27486	Full RELRO	Canary	found	Seccomp-bpf	NX enabled	PIE enabled	Yes
pickup	44165	Full RELRO	Canary	found	Seccomp-bpf	NX enabled	PIE enabled	Yes
sshd	44169	Full RELRO	Canary	found	Seccomp-bpf	NX enabled	PIE enabled	Yes
bash	44209	Full RELRO	Canary	found	Seccomp-bpf	NX enabled	PIE enabled	Yes
mc	5437	Full RELRO	Canary	found	Seccomp-bpf	NX enabled	PIE enabled	Yes
bash	5439	Full RELRO	Canary	found	Seccomp-bpf	NX enabled	PIE enabled	Yes
master	583	Full RELRO	Canary	found	Seccomp-bpf	NX enabled	PIE enabled	Yes
qmgr	591	Full RELRO	Canary	found	Seccomp-bpf	NX enabled	PIE enabled	Yes
bash	86454	Full RELRO	Canary	found	Seccomp-bpf	NX enabled	PIE enabled	Yes
bash	86481	Full RELRO	Canary	found	Seccomp-bpf	NX enabled	PIE enabled	Yes

```
root@ubuntu-1804:~/cfi/checksec.sh#
```



# Check: Checksec

init	1235	Full RELRO	Canary found	NX enabled	PIE enabled
dbus-launch	1436	Partial RELRO	Canary found	NX enabled	No PIE
dbus-daemon	1453	Partial RELRO	Canary found	NX enabled	No PIE
dbus-daemon	1454	Partial RELRO	Canary found	NX enabled	No PIE
upstart-event-b	1465	Full RELRO	No canary found	NX enabled	PIE enabled
window-stack-br	1471	Partial RELRO	No canary found	NX enabled	No PIE
upstart-dbus-br	1486	Full RELRO	No canary found	NX enabled	PIE enabled
upstart-dbus-br	1488	Full RELRO	No canary found	NX enabled	PIE enabled
upstart-file-br	1497	Full RELRO	Canary found	NX enabled	PIE enabled
ibus-daemon	1503	Partial RELRO	Canary found	NX enabled	No PIE
unity-settings-	1517	Partial RELRO	No canary found	NX enabled	No PIE
bamfdamon	1519	Partial RELRO	Canary found	NX enabled	No PIE
at-spi-bus-laun	1523	Full RELRO	Canary found	NX enabled	PIE enabled
gnome-session	1524	Partial RELRO	Canary found	NX enabled	No PIE
dbus-daemon	1529	Partial RELRO	Canary found	NX enabled	No PIE
gvfsd	1533	Partial RELRO	No canary found	NX enabled	No PIE
ibus-dconf	1538	Partial RELRO	No canary found	NX enabled	No PIE
ibus-ui-gtk3	1539	Partial RELRO	No canary found	NX enabled	No PIE
ibus-x11	1542	Partial RELRO	Canary found	NX enabled	No PIE
gvfsd-fuse	1545	Partial RELRO	No canary found	NX enabled	No PIE
at-spi2-registr	1555	Full RELRO	Canary found	NX enabled	PIE enabled
pulseaudio	1645	Full RELRO	Canary found	NX enabled	No PIE
ibus-engine-sim	1692	Partial RELRO	No canary found	NX enabled	No PIE
metacity	1775	Partial RELRO	Canary found	NX enabled	No PIE
dconf-service	1781	Partial RELRO	Canary found	NX enabled	No PIE
gnome-panel	1819	Partial RELRO	Canary found	NX enabled	No PIE
indicator-appli	1835	Partial RELRO	No canary found	NX enabled	No PIE
unity-fallback-	1836	Partial RELRO	No canary found	NX enabled	No PIE
indicator-bluet	1837	Partial RELRO	No canary found	NX enabled	No PIE
vmtoolsd	1839	Partial RELRO	Canary found	NX enabled	No PIE
polkit-gnome-au	1841	Partial RELRO	No canary found	NX enabled	No PIE
nautilus	1848	Partial RELRO	Canary found	NX enabled	No PIE
nm-applet	1852	Partial RELRO	Canary found	NX enabled	No PIE
initctl	1853	Full RELRO	No canary found	NX enabled	PIE enabled
indicator-messa	1858	Partial RELRO	No canary found	NX enabled	No PIE
indicator-power	1863	Partial RELRO	No canary found	NX enabled	No PIE

## Check: Paxtest



Anonymous mapping randomization test	: 28 quality bits (guessed)
Heap randomization test (ET_EXEC)	: 13 quality bits (guessed)
Heap randomization test (PIE)	: 28 quality bits (guessed)
Main executable randomization (ET_EXEC)	: 28 quality bits (guessed)
Main executable randomization (PIE)	: 28 quality bits (guessed)
Shared library randomization test	: 28 quality bits (guessed)
VDSO randomization test	: 11 quality bits (guessed)
Stack randomization test (SEGMEXEC)	: 28 quality bits (guessed)
Stack randomization test (PAGEEXEC)	: 28 quality bits (guessed)
Arg/env randomization test (SEGMEXEC)	: 20 quality bits (guessed)
Arg/env randomization test (PAGEEXEC)	: 20 quality bits (guessed)
Randomization under memory exhaustion @~0	: 28 bits (guessed)
Randomization under memory exhaustion @0	: 28 bits (guessed)
Return to function (strcpy)	: return addr has NULL byte
Return to function (memcpy)	: Vulnerable
Return to function (strcpy, PIE)	: return addr has NULL byte
Return to function (memcpy, PIE)	: Vulnerable



What is the fundamental difference between attack and defense?

You know when an attack does not work...

# Advanced Linux hardening

The non-standard stuff

Compass Security Network  
Computing AG  
Werkstrasse 20  
Postfach 2038  
CH-8645 Jona

Tel +41 55 214 41 60  
Fax +41 55 214 41 61

[team@csnc.ch](mailto:team@csnc.ch)  
[www.csnc.ch](http://www.csnc.ch)

## Grsecurity

### Uses PaX

- ✦ Kernel patch
- ✦ Improved DEP and ASLR
- ✦ For userspace
- ✦ And kernelspace protection (e.g. SMAP emulation)
- ✦ Better randomness, more randomness

### Also provides:

- ✦ Chroot hardening
- ✦ Hide /proc stuff
- ✦ Ptrace restrictions
- ✦ Kernel module loading restrictions
- ✦ RBAC (Role Based Access Control)

# Container

## Linux Container

Compass Security Network  
Computing AG  
Werkstrasse 20  
Postfach 2038  
CH-8645 Jona

Tel +41 55 214 41 60  
Fax +41 55 214 41 61

[team@csnc.ch](mailto:team@csnc.ch)  
[www.csnc.ch](http://www.csnc.ch)

## Relevant?

- ✦ TEH CLOUD

## Container: All container share the same kernel

- ✦ LXC
- ✦ Docker
- ✦ FreeBSD Jails (since March 2000)
- ✦ Solaris Zones
- ✦ Obsolete: Vserver, openvz

## Virtualization: Each guest has his very own kernel

- ✦ Vmware, virtualbox, kvm, ...
- ✦ Not covered here

## RBAC's

- ✦ SELinux (redhat), Apparmor (Suse), ...
- ✦ Not covered here

- Chroot is not a container
  - **Path** restriction only
  - But: Can access other processes, the kernel, IPC, etc.

```
compass@ubuntu:~$ sudo chroot /var/chroot
```

```
root@ubuntu:/# cd root/
```

```
root@ubuntu:/root# ./w00t -0 --dir /nonexisting  
classic
```

```
[+] creating /nonexisting directory
```

```
[+] chrooting to /nonexisting
```

```
[+] change working directory to real root
```

```
[+] chrooting to real root
```

```
root@ubuntu:/# ls /
```

```
bin    cdrom  etc    initrd.img  lib64    media  
boot  dev    home   lib          lost+found  mnt
```

```
root@ubuntu:/# █
```



# LXC/Docker: Use namespaces for containerization

- ✦ Restrict view/access of certain processes

Linux provides the following namespaces:

Namespace	Constant	Isolates
IPC	<code>CLONE_NEWIPC</code>	System V IPC, POSIX message queues
Network	<code>CLONE_NEWNET</code>	Network devices, stacks, ports, etc.
Mount	<code>CLONE_NEWNS</code>	Mount points
PID	<code>CLONE_NEWPID</code>	Process IDs
User	<code>CLONE_NEWUSER</code>	User and group IDs
UTS	<code>CLONE_NEWUTS</code>	Hostname and NIS domain name

## Lxc container cannot:

- Interact with host processes
- Access root file system
- Access special devices (block, network, ...)
- Mount filesystems
- Execute special ioctl's

## Lxc container can access:

- /proc: certain files
- /sys: certain files
- Do a lot of other stuff

## Seccomp-bpf

- ✦ Seccomp: Since Kernel 2.6.12 (2005)
- ✦ Seccomp-bpf: Since Kernel 3.5 (2012)
- ✦ Whitelist (blacklist) system calls
  - ✦ E.g. `exit()`, `read()`, `write()`, ...
- ✦ Who cares?
  - ✦ Chrome-Flash, Chrome-Renderer, vsftpd, OpenSSH, Firefox, Tor, ...

## FS hardening, only provide:

- ✦ /proc
- ✦ /sys
- ✦ /dev/[zero, null, urandom]
- ✦ Nothing else

## AppArmour

- ✦ “additional restrictions on mounts, socket, ptrace and file access. Specifically restricting cross-container communication.”

