```
gifsicle consente di inserire commenti (quindi codice php sotto forma di commento o shell) in una gif
gifsicle --comment "`tr '\n' ' ' < shell.php`" < mappainquinamentoeuropaqo1.gif >
mappainquinamentoeuropaqo1_offuscato_1.gif

===

Tamper Data
add-on firefox per caricare un php invece di jpeg intercettando la chiamata al server e modificando il
POST

si cambia l'estensione del file, ad es., shell.php in gif,jpeg; poi si fa partire Tamper Data e si
prova a fare un upload dell'immagine. La chiamata viene intercettata da Tamper Data e con questo si
cambia di nuovo l'estensione da jpeg in php

===

semanage: aggiunge la porta 13123 (per utilizzo/test reverse shell) al protocollo http
semanage port -a -t http_port_t -p tcp 13123

===

sealert comando per analizzare il log di SELinux (avvisi di tipo AVC):
sealert -a /var/log/audit/audit.log

===

ad es. di default la variabile bool httpd_can_network_connect_db e' settata su no e se provo a far
partire una web app che si connette ad un db, questa non parte;

 getsebool -a | grep http | grep db
 setsebool httpd_can_network_connect_db off/on
   off => http://catenaccio.cnaf.infn.it/DVWA-1.9/setup.php
   on => http://catenaccio.cnaf.infn.it/DVWA-1.9/login.php

Il comando setsebool dato cosi' modifica il valore solo per la sessione corrente; se si vuole rendere
la modifica persistente al boot, bisogna usare l'opzione "-P"

===

le regole SELinux vengono mostrate con l'opzione "-Z" ad es.:
ls -Z, ps -Z etc.

 ls -Z /etc/group -rw-r--r--. root root system_u:object_r:passwd_file_t:s0 /etc/group

 cp /etc/group /tmp/
 ls -Z /tmp/group -rw-r--r--. root root unconfined_u:object_r:user_tmp_t:s0 /tmp/group

 cp -p /etc/group /tmp/
 ls -Z /tmp/group -rw-r--r--. root root unconfined_u:object_r:user_tmp_t:s0 /tmp/group

 touch /etc/test
 ls -Z /etc/test -rw-r--r--. root root unconfined_u:object_r:etc_t:s0   /etc/test
 cp /etc/test /tmp/
 ls -Z /tmp/test -rw-r--r--. root root unconfined_u:object_r:user_tmp_t:s0 /tmp/test
 mv /tmp/test /etc/
 ls -Z /etc/test -rw-r--r--. root root unconfined_u:object_r:user_tmp_t:s0 /etc/test

 the copy (cp) command will typically adopt the destination directory's or file's security context,
move (mv) will maintain the source's security context.

 restorecon -v /etc/test (ripristina i contesti del file)
 restorecon reset /etc/test context unconfined_u:object_r:user_tmp_t:s0->unconfined_u:object_r:etc_t:s0
 ls -Z /etc/test
-rw-r--r--. root root unconfined_u:object_r:etc_t:s0   /etc/test

if we simply wanted to examine the security contexts of the /var/www/html directory to see if any
files needed their security contexts restored, we can use restorecon with the -n switch to prevent any
relabelling occurring:

# restorecon -Rv -n /var/www/html

===
```

2 comandi utili per capire, dai log, cosa non va e come risolvere sono "audit2why" ed "audit2allow"

===

anche il man: `man -k selinux` da' le pagine del man installate
man httpd_selinux (nel caso di "No manual entry for httpd_selinux" installare, CentOS, selinux-policy-devel);

===

audit2allow -w equivale ad audit2why

```
echo "type=AVC msg=audit(1446128957.821:4764): avc:  denied  { getattr } for  pid=24329 comm="httpd"
path="/etc/shadow" dev="dm-1" ino=402989571 scontext=system_u:system_r:httpd_t:s0
tcontext=system_u:object_r:shadow_t:s0 tclass=file" | audit2allow -M test_selinux_mod
```

genera i due file per il modulo richiesto e spiega come installarli:
semodule -i test_selinux_mod.pp

si puo' verificare con
semanage module -l | grep test_selinux
prima = niente
e
dopo = test_selinux_mod   1.0

===

mappatura utenti Linux - SELinux

```
# semanage login -l
Login Name           SELinux User         MLS/MCS Range        Service

__default__          unconfined_u         s0-s0:c0.c1023       *
root                 unconfined_u         s0-s0:c0.c1023       *
system_u             system_u             s0-s0:c0.c1023       *

# semanage user -l
                Labeling   MLS/       MLS/
SELinux User    Prefix     MCS Level  MCS Range                     SELinux Roles

guest_u         user       s0         s0                            guest_r
root            user       s0         s0-s0:c0.c1023                staff_r sysadm_r system_r
unconfined_r
staff_u         user       s0         s0-s0:c0.c1023                staff_r sysadm_r system_r
unconfined_r
sysadm_u        user       s0         s0-s0:c0.c1023                sysadm_r
system_u        user       s0         s0-s0:c0.c1023                system_r unconfined_r
unconfined_u    user       s0         s0-s0:c0.c1023                system_r unconfined_r
user_u          user       s0         s0                            user_r
xguest_u        user       s0         s0                            xguest_r
```