

به نام خدا

تمرین سری سوم درس سیستم‌های کامپیوتری امن

سید محمدمهدی احمدپناه ۹۴۱۳۱۰۸۶

پروژه SELinux

این پروژه در محیط سیستم‌عامل فدورا ۱۲ انجام شده است.

برای انجام این پروژه، یک برنامه دارای آسیب‌پذیری Buffer Overflow استفاده شده است که در شکل زیر آمده است. در این برنامه، shellcode همان دستوراتی است که پس از سرریز شدن بافر حافظه، در آدرس بازگشت قرار می‌گیرد و باعث می‌شود تا کاربر غیر root، دسترسی root بگیرد.

```
#include <unistd.h>
#include <stdio.h>
#include <string.h>

char shellcode[] = "\x31\xc0\x89\xc3\xb0\x17\xcd\x80\x31\xd2\x52\x68\x6e\x2f\x73\x68\x68\x2f\x2f\x62\x69\x89\xe3\x52\x53\x89\xe1\x8d\x42\x0b\xcd\x80";

char large_string[128];

int main() {
    char buffer[96];
    int i;
    long *long_ptr = (long *) large_string;

    for (i=0; i<32; i++)
        *(long_ptr + i) = (int) buffer;

    for (i = 0; i < strlen(shellcode); i++)
        large_string[i] = shellcode[i];

    strcpy(buffer, large_string);
    return 0;
}
```

برای کامپایل کردن برنامه، محافظت‌های روی پشته را غیرفعال می‌کنیم که مراحل در شکل زیر آمده است.

```

fedora@localhost:/home/fedora/Desktop
File Edit View Terminal Help
[fedora@localhost ~]$ cd Desktop/
[fedora@localhost Desktop]$ su
Password:
[root@localhost Desktop]# echo "0" > /proc/sys/kernel/randomize_va_space
[root@localhost Desktop]# gcc -mpreferred-stack-boundary=2 -fno-stack-protector
-z execstack -o bufferoverflow o.c
[root@localhost Desktop]# ls
1.png  bufferoverflow  errorls.out  k  new file~  out  overflow.c~
2.png  calculator      error.txt    k~  o.c        output.out  sortls.out
asd.er  eightsort.out   error.tzt    meet  o.c~       overflow.c  sort.out
[root@localhost Desktop]# chmod u+s bufferoverflow
[root@localhost Desktop]# ls -l bufferoverflow
-rwsrwxr-x. 1 root root 5230 2015-12-17 18:42 bufferoverflow
[root@localhost Desktop]#

```

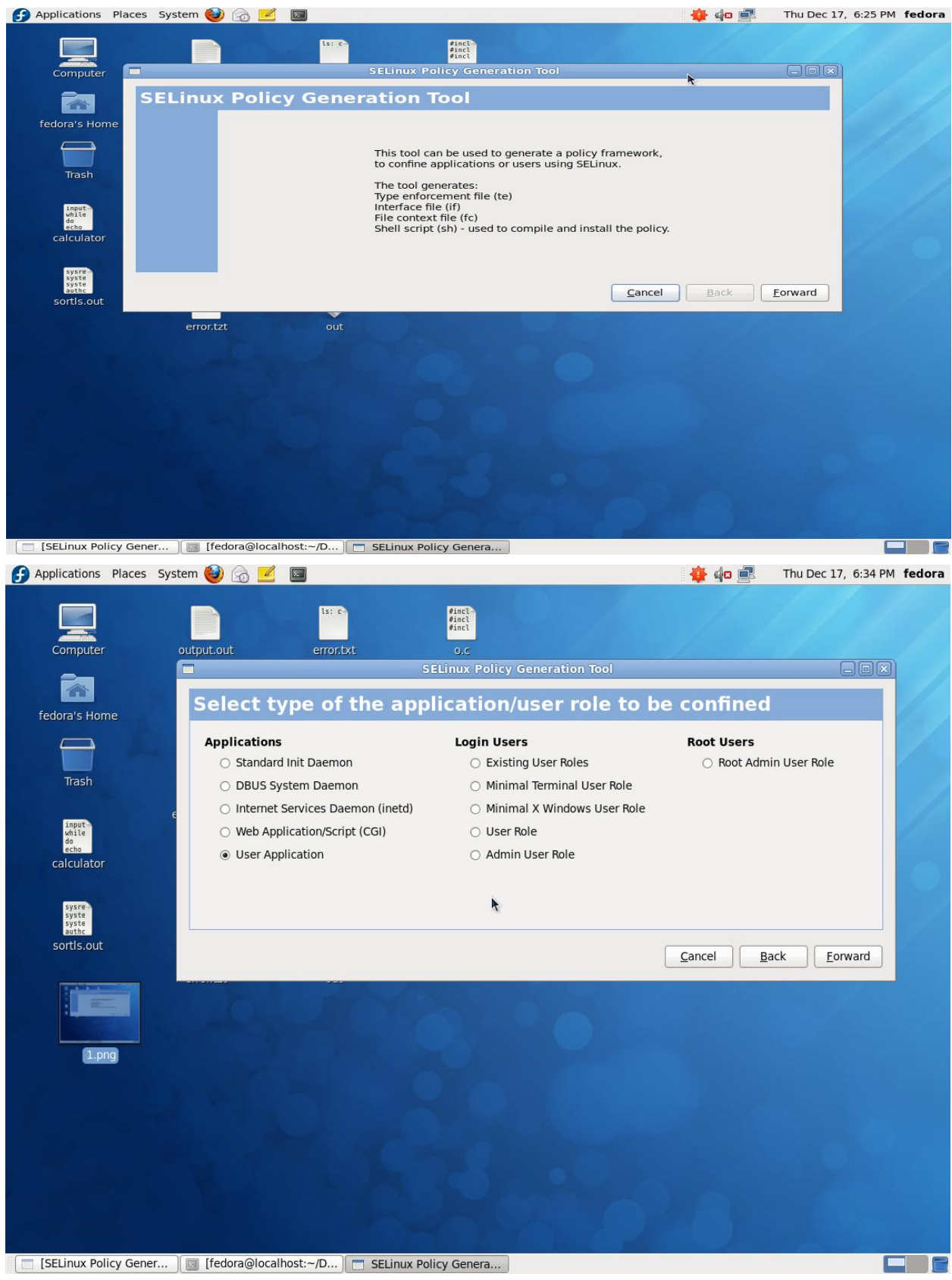
به این ترتیب، برنامه اجرایی با نام `bufferoverflow` تولید می‌شود و به محض اجرا شدن برنامه توسط کاربر غیر `root`، `shell` با دسترسی `root` به کاربر داده می‌شود.

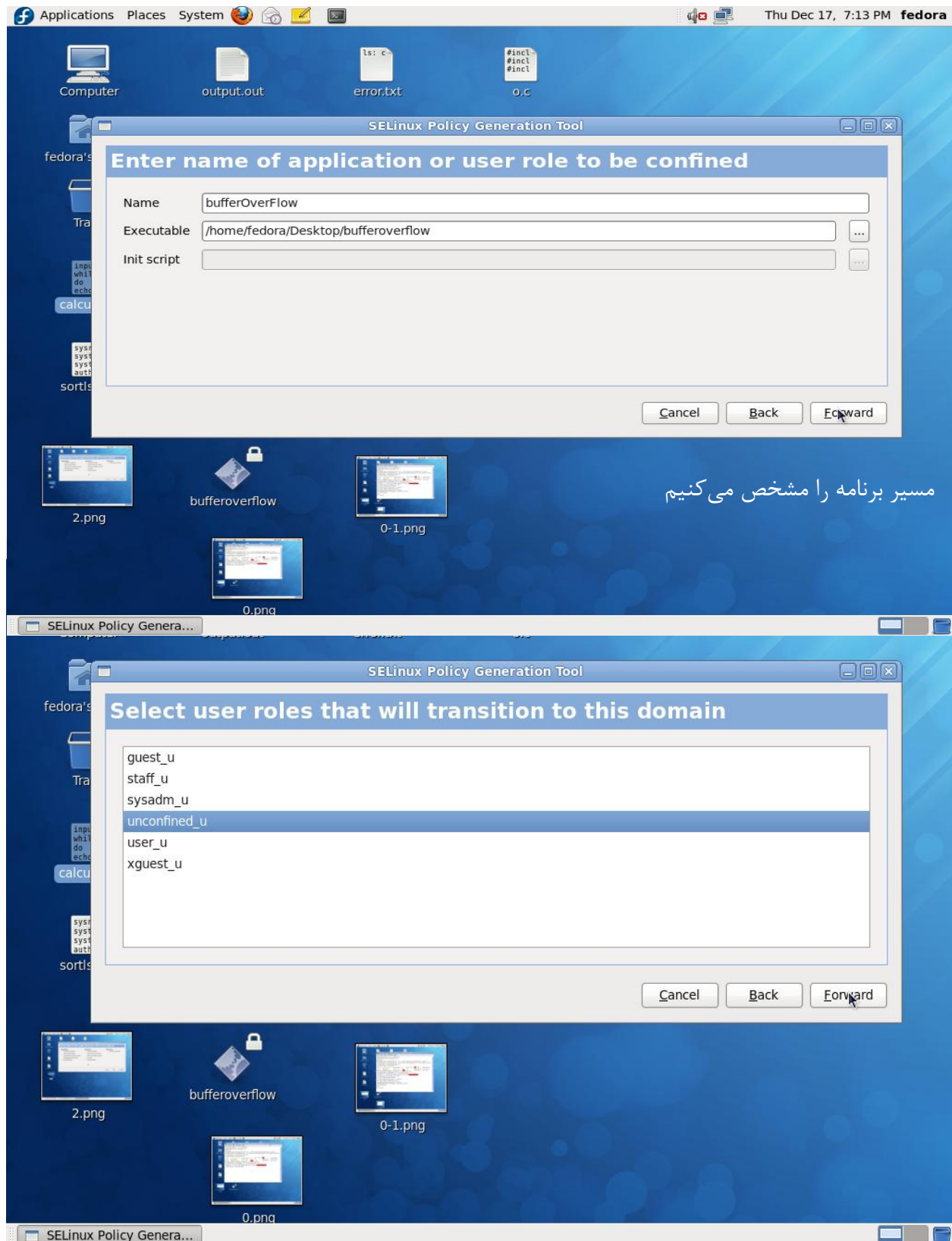
```

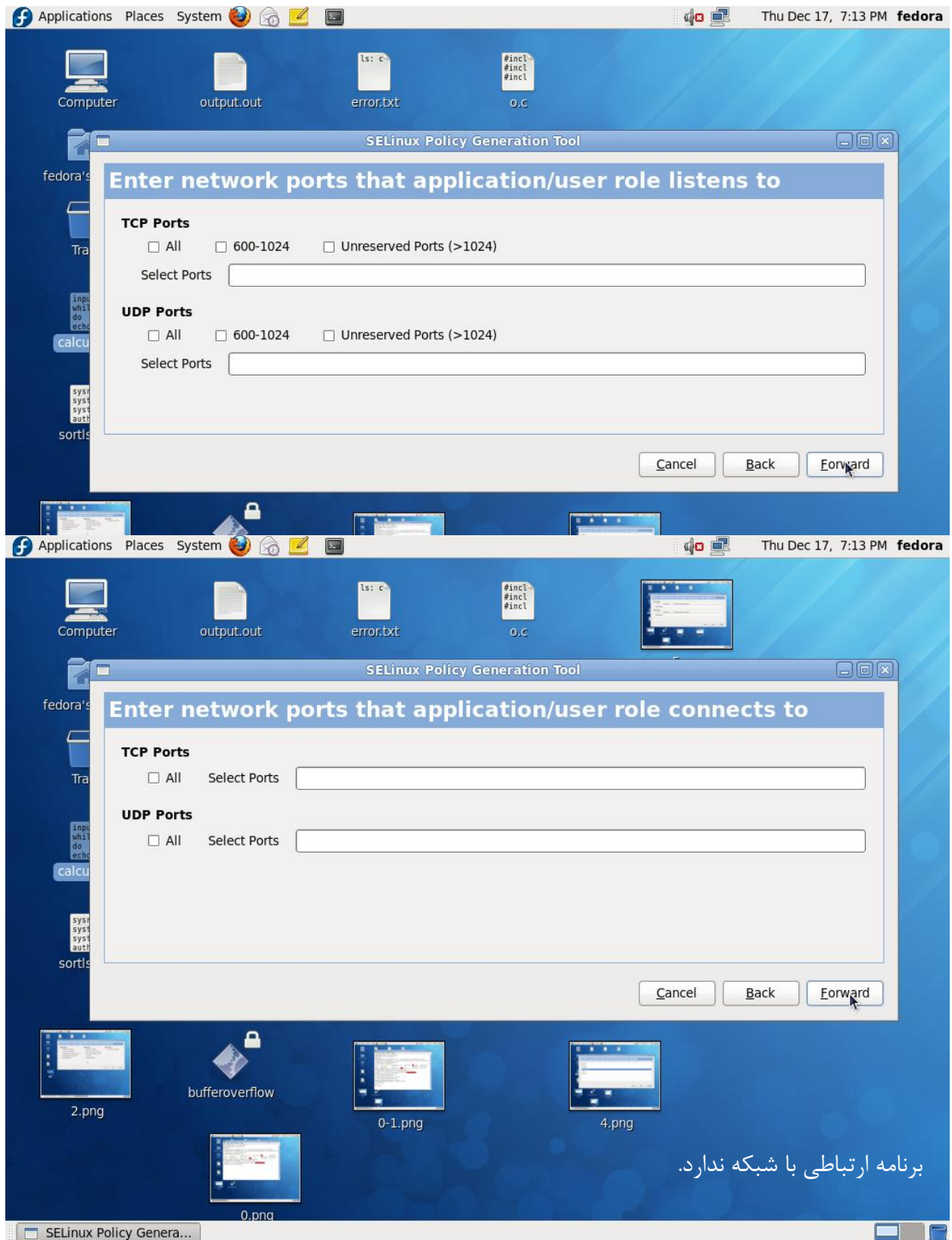
[root@localhost Desktop]# su fedora
[fedora@localhost Desktop]$ ./bufferoverflow
sh-4.0# whoami
root
sh-4.0#

```

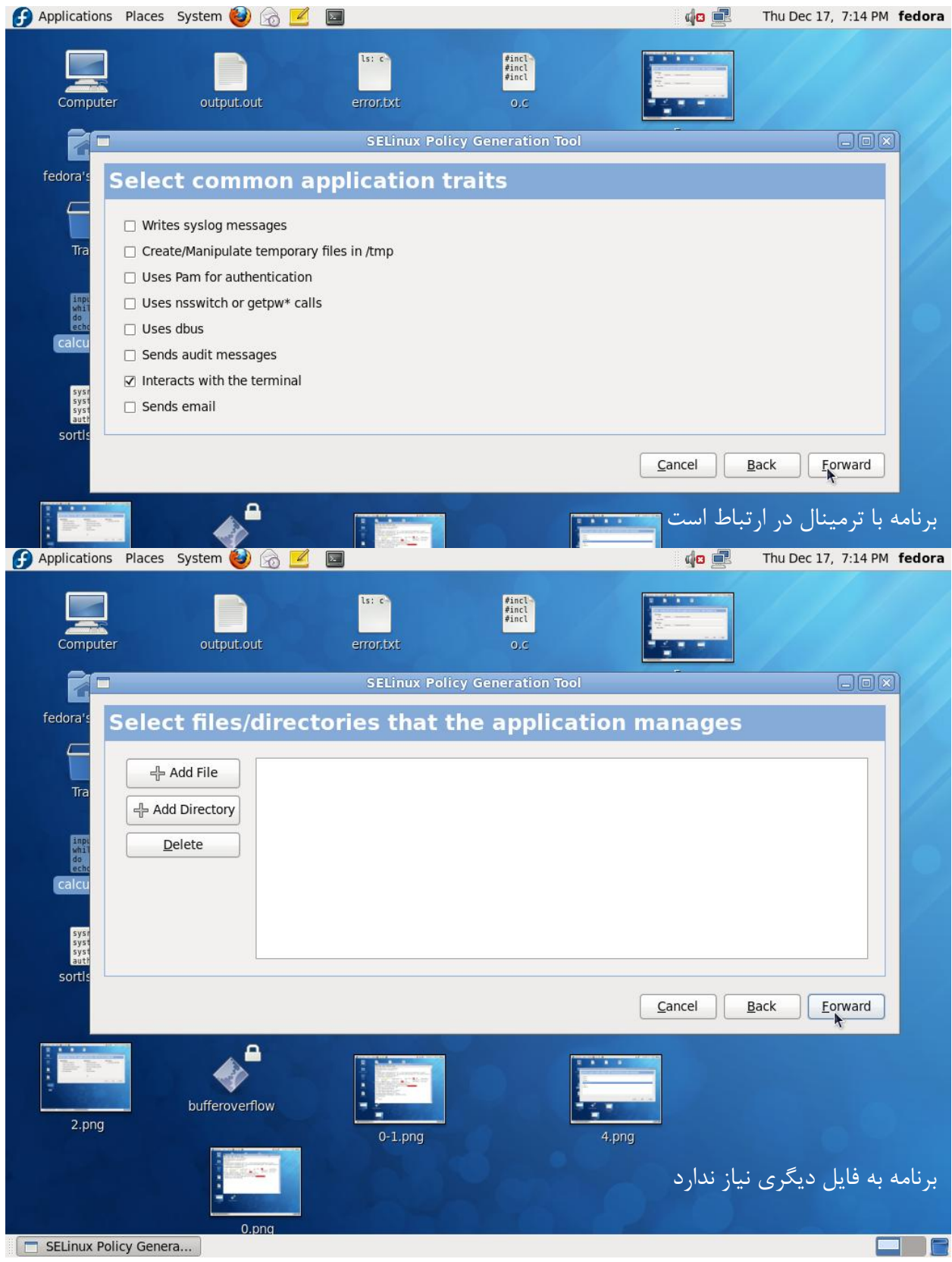
اینک نوبت تعریف خط مشی‌ها و اعمال آن توسط SELinux است. با استفاده از ابزار SELinux Policy Generation Tool، قواعد اولیه برای برنامه `bufferoverflow` تولید می‌شود. مراحل گام به گام زیر صورت گرفت:

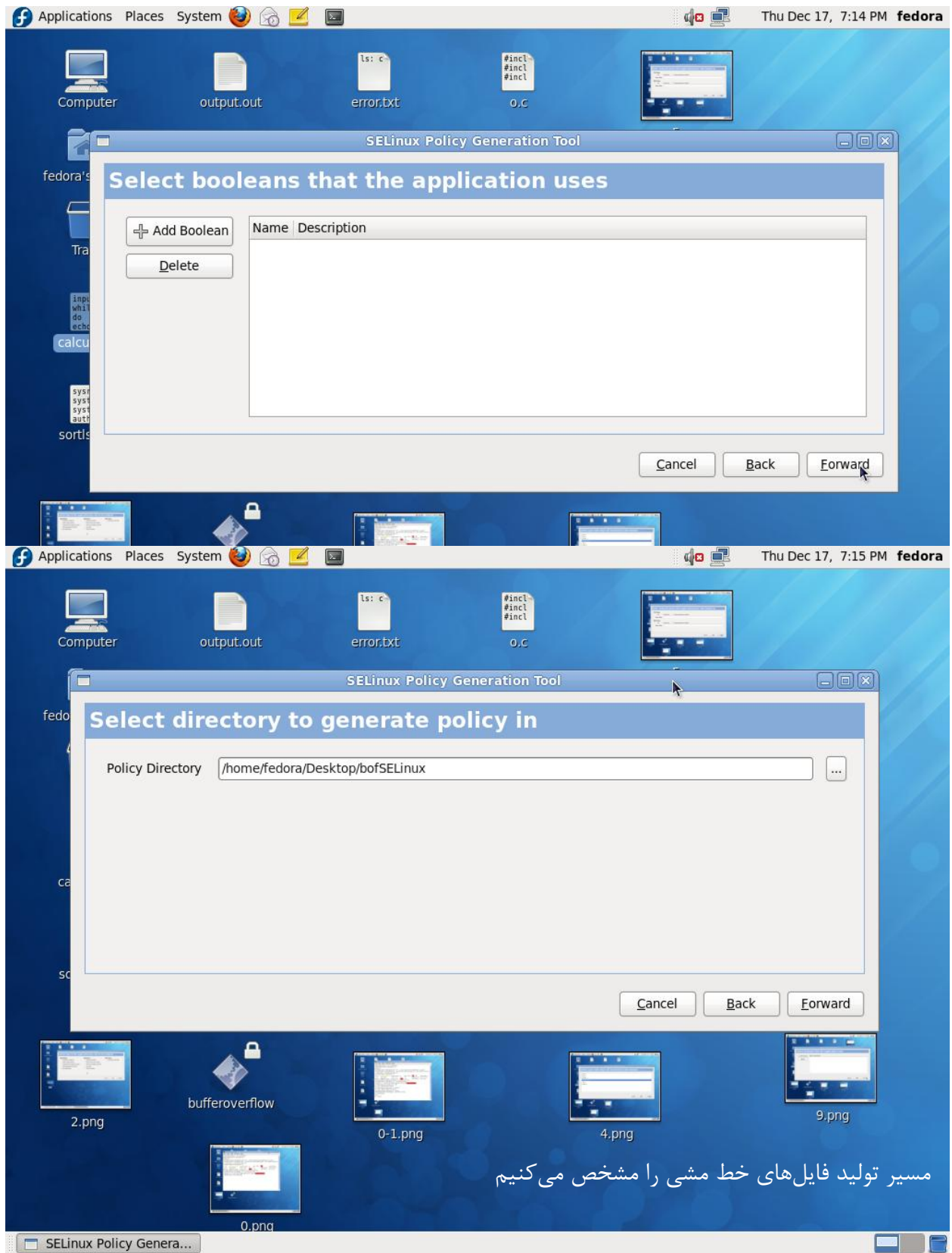


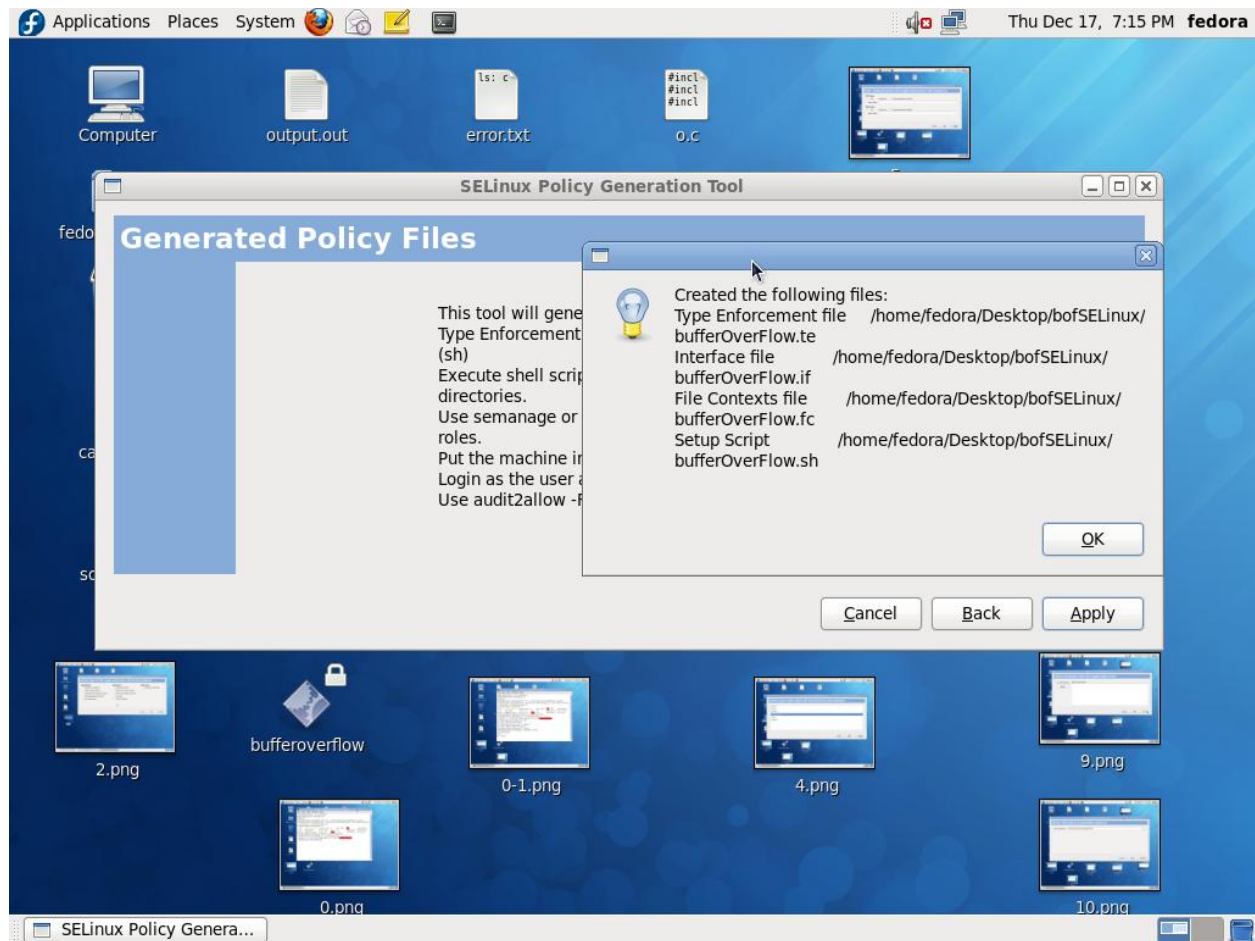




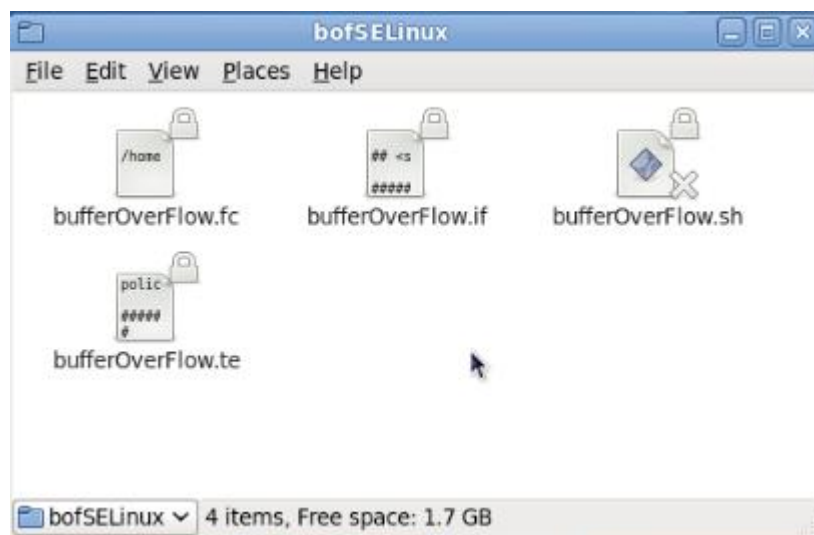
برنامه ارتباطی با شبکه ندارد.



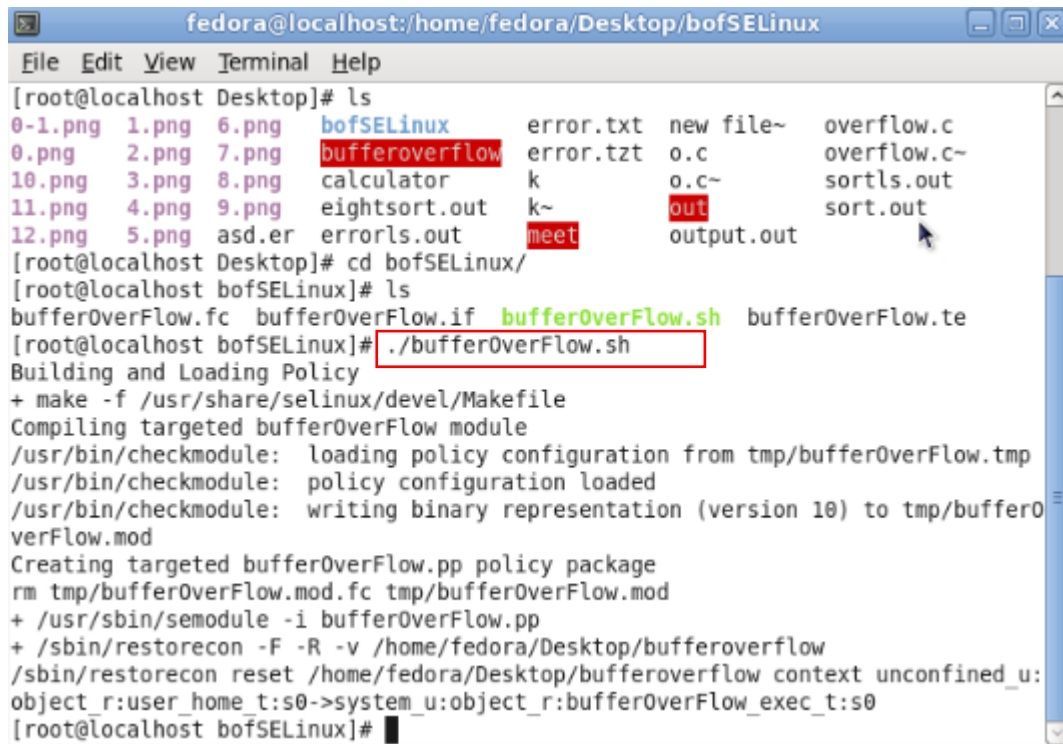




به این ترتیب، در پوشه bofSELinux، فایل‌های زیر ساخته می‌شوند:



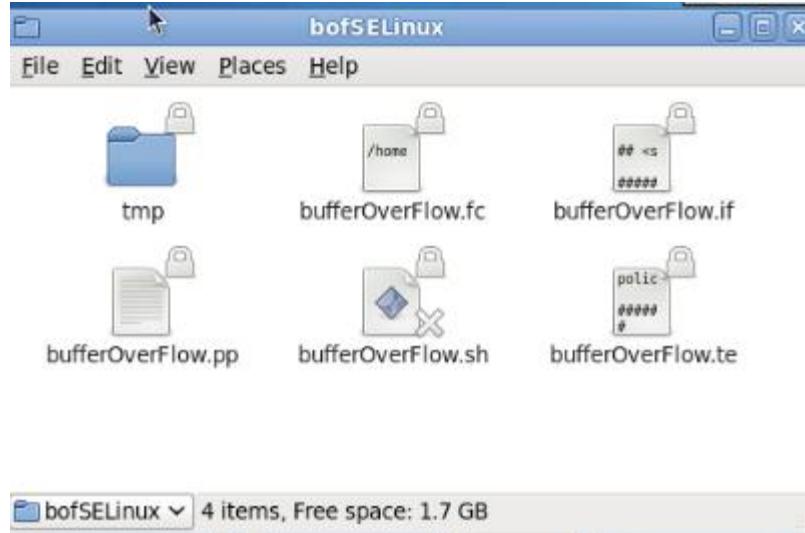
که پس از اینکه برای بار اول به شکل زیر خط مشی آپلود می‌شود، فایل‌های دیگری نیز اضافه می‌شوند:



```

fedora@localhost:/home/fedora/Desktop/bofSELinux
File Edit View Terminal Help
[root@localhost Desktop]# ls
0-1.png 1.png 6.png bofSELinux error.txt new file~ overflow.c
0.png 2.png 7.png bufferoverflow error.tzt o.c overflow.c~
10.png 3.png 8.png calculator k o.c~ sortls.out
11.png 4.png 9.png eightsort.out k~ out sort.out
12.png 5.png asd.er errorls.out meet output.out
[root@localhost Desktop]# cd bofSELinux/
[root@localhost bofSELinux]# ls
bufferOverflow.fc bufferOverflow.if bufferOverflow.sh bufferOverflow.te
[root@localhost bofSELinux]# ./bufferOverflow.sh
Building and Loading Policy
+ make -f /usr/share/selinux/devel/Makefile
Compiling targeted bufferOverflow module
/usr/bin/checkmodule: loading policy configuration from tmp/bufferOverflow.tmp
/usr/bin/checkmodule: policy configuration loaded
/usr/bin/checkmodule: writing binary representation (version 10) to tmp/bufferOverflow.mod
Creating targeted bufferOverflow.pp policy package
rm tmp/bufferOverflow.mod.fc tmp/bufferOverflow.mod
+ /usr/sbin/semodule -i bufferOverflow.pp
+ /sbin/restorecon -F -R -v /home/fedora/Desktop/bufferoverflow
/sbin/restorecon reset /home/fedora/Desktop/bufferoverflow context unconfined_u:
object_r:user_home t:s0->system_u:object_r:bufferOverflow_exec_t:s0
[root@localhost bofSELinux]#

```



حال می‌خواهیم با توجه به اصل حداقل دسترسی (least privilege)، قاعده‌ها را به فایل خط مشی اضافه کنیم.

مراحل زیر را انجام می‌دهیم:

- دستور `setenforce 0` را به منظور `permissive` کردن حالت اعمال SELinux اجرا می‌کنیم. (برای اطمینان از تغییر وضعیت SELinux، دستور `getenforce` را استفاده می‌کنیم).

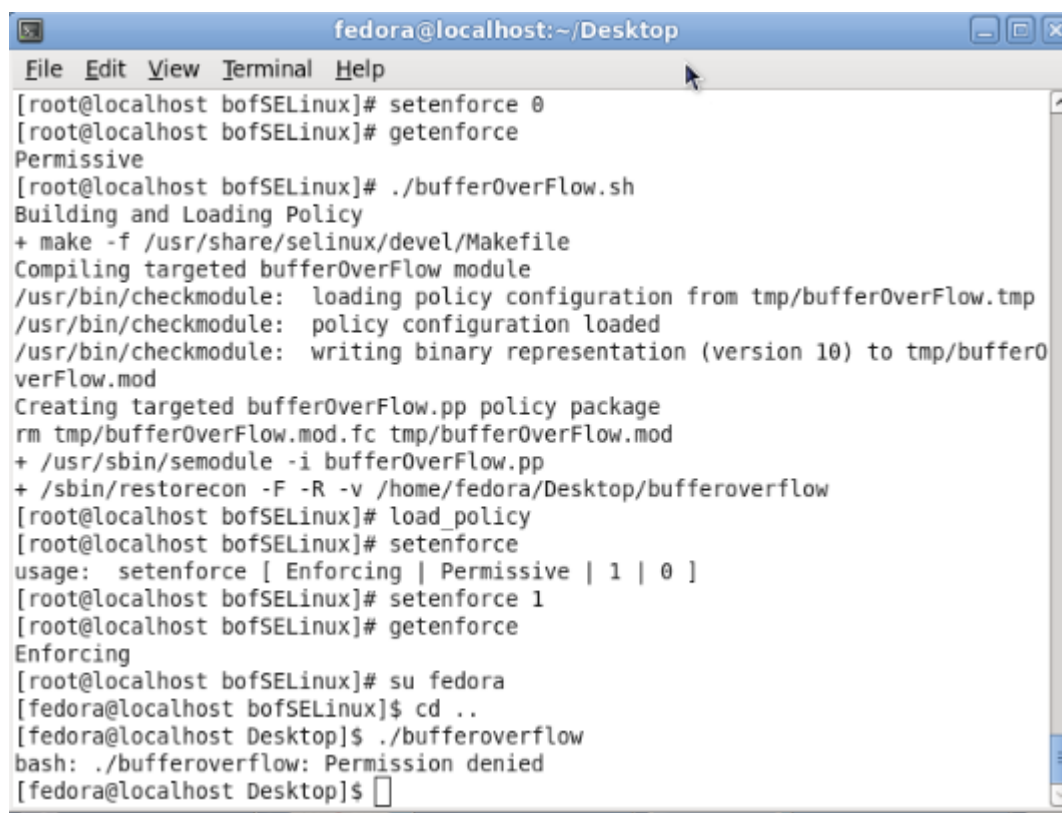
- با دستور `gedit bufferOverflow.te`، فایل خط مشی را باز کرده و تنها خطوط ابتدایی تا تعریف `type`های `bufferOverflow_t` و `bufferOverflow_exec_t` را نگه می‌داریم و بقیه خطوط را کامنت یا حذف می‌کنیم.

- با اجرای `./bufferOverflow.sh` کامپایل می‌کنیم و با دستور `load_policy`، خط مشی را بارگذاری می‌کنیم.

- اجرای `setenforce 1` برای تغییر وضعیت به حالت `enforcing`

- رفتن به حالت کاربر عادی (fedora) و اجرای برنامه `bufferoverflow`

با توجه به اینکه دسترسی‌ای تعریف نشده، اجرا با پیام `permission denied` انجام نمی‌شود (حتی دستور `ls` نیز اجازه نمایش آن فایل را نمی‌دهد).



```

fedora@localhost:~/Desktop
File Edit View Terminal Help
[root@localhost bofSELinux]# setenforce 0
[root@localhost bofSELinux]# getenforce
Permissive
[root@localhost bofSELinux]# ./bufferOverflow.sh
Building and Loading Policy
+ make -f /usr/share/selinux/devel/Makefile
Compiling targeted bufferOverflow module
/usr/bin/checkmodule: loading policy configuration from tmp/bufferOverflow.tmp
/usr/bin/checkmodule: policy configuration loaded
/usr/bin/checkmodule: writing binary representation (version 10) to tmp/bufferOverflow.mod
Creating targeted bufferOverflow.pp policy package
rm tmp/bufferOverflow.mod.fc tmp/bufferOverflow.mod
+ /usr/sbin/semodule -i bufferOverflow.pp
+ /sbin/restorecon -F -R -v /home/fedora/Desktop/bufferoverflow
[root@localhost bofSELinux]# load_policy
[root@localhost bofSELinux]# setenforce
usage: setenforce [ Enforcing | Permissive | 1 | 0 ]
[root@localhost bofSELinux]# setenforce 1
[root@localhost bofSELinux]# getenforce
Enforcing
[root@localhost bofSELinux]# su fedora
[fedora@localhost bofSELinux]$ cd ..
[fedora@localhost Desktop]$ ./bufferoverflow
bash: ./bufferoverflow: Permission denied
[fedora@localhost Desktop]$

```

حال برای اینکه مجوزهای لازم را بدانیم، از دستور `audit2allow` استفاده می‌کنیم. مراحل زیر به دفعات (بیش از ۳۰ بار!) انجام شد تا دیگر تغییری در خروجی این دستور با محتویات فایل خط مشی مشاهده نشود و برنامه به درستی کار کند.

- به حالت کاربر عادی (fedora) رفته، برنامه را در حالت `permissive` اجرا می‌کنیم.

- تغییر وضعیت به کاربر `root`

- اجرای دستور `audit2allow -a bufferoverflow` و مشاهده قاعده‌های خروجی

- اضافه کردن قواعد به فایل `bufferOverFlos.te` و ایجاد تغییرات لازم برای درست کامپایل شدن آن

- کامپایل کردن با دستور `./bufferOverFlow.sh`.

در ایجاد تغییرات لازم در فایل `te` باید دقت شود که `type`ها درست تعریف شوند و مجوز `execute_no_trans` از مجموعه مجوزهایی که وجود دارد، حذف شود. در انتهای قواعد `domain_auto-trans (unconfined_t, bufferOverFlow_t, usr_t)` را اضافه می‌کنیم.

مراحل فوق را به قدری تکرار می‌کنیم که تغییری در خروجی دستور `audit2allow` نسبت به محتویات فایل `te` مشاهده نشود. (البته که فرایند بسیار خسته‌کننده‌ای است! 😊)

بخشی از مراحل انجام‌شده در شکل‌های پایین ملاحظه می‌شود:

```

fedora@localhost:/home/fedora/Desktop
File Edit View Terminal Help

===== setfiles_t =====
allow setfiles_t bufferOverflow_exec_t:file getattr;

===== setroubleshootd_t =====
allow setroubleshootd_t bufferOverflow_exec_t:file getattr;

===== unconfined_t =====
allow unconfined_t bufferOverflow_exec_t:file { getattr execute };
[root@localhost Desktop]# setenforce 0
[root@localhost Desktop]# geten
bash: geten: command not found
[root@localhost Desktop]# getenforce
Permissive
[root@localhost Desktop]# audit2allow -a bufferoverflow

===== setfiles_t =====
allow setfiles_t bufferOverflow_exec_t:file getattr;

===== setroubleshootd_t =====
allow setroubleshootd_t bufferOverflow_exec_t:file getattr;

===== unconfined_t =====
allow unconfined_t bufferOverflow_exec_t:file { getattr execute };
[root@localhost Desktop]# █

rash. See http://projects.gnome.org/gconf/ for information. (Details - 1: Failed to get
connection to session: Did not receive a reply. Possible causes include: the remote app
lication did not send a reply, the message bus security policy blocked the reply, the re
ply timeout expired, or the network connection was broken.)
GConf Error: Failed to contact configuration server; some possible causes are that you n
eed to enable TCP/IP networking for ORBit, or you have stale NFS locks due to a system c
rash. See http://projects.gnome.org/gconf/ for information. (Details - 1: Failed to get
connection to session: Did not receive a reply. Possible causes include: the remote app
lication did not send a reply, the message bus security policy blocked the reply, the re
ply timeout expired, or the network connection was broken.)
[root@localhost bofSELinux]# setenforce 0
[root@localhost bofSELinux]# ./bufferOverflow.sh
Building and Loading Policy
+ make -f /usr/share/selinux/devel/Makefile
Compiling targeted bufferOverflow module
/usr/bin/checkmodule: loading policy configuration from tmp/bufferOverflow.tmp
/usr/bin/checkmodule: policy configuration loaded
/usr/bin/checkmodule: writing binary representation (version 10) to tmp/bufferOverflow.
mod
Creating targeted bufferOverflow.pp policy package
rm tmp/bufferOverflow.mod.fc tmp/bufferOverflow.mod
+ /usr/sbin/semodule -i bufferOverflow.pp
+ /sbin/restorecon -F -R -v /home/fedora/Desktop/bufferoverflow
[root@localhost bofSELinux]# setenforce 1
[root@localhost bofSELinux]# cd ..
[root@localhost Desktop]# su
[root@localhost Desktop]# su fedora
[fedora@localhost Desktop]$ ./bufferoverflow
Segmentation fault
[fedora@localhost Desktop]$ su
Password:
[root@localhost Desktop]# audit2allow -a bufferoverflow █

```

```
fedora@localhost:/home/fedora/Desktop/bofSELinux
File Edit View Terminal Help
GConf Error: Failed to contact configuration server; some possible causes are that you need to enable TCP/IP networking for ORBit, or you have stale NFS locks due to a system crash. See http://projects.gnome.org/gconf/ for information. (Details - 1: Failed to get connection to session: Did not receive a reply. Possible causes include: the remote application did not send a reply, the message bus security policy blocked the reply, the reply timeout expired, or the network connection was broken.)
GConf Error: Failed to contact configuration server; some possible causes are that you need to enable TCP/IP networking for ORBit, or you have stale NFS locks due to a system crash. See http://projects.gnome.org/gconf/ for information. (Details - 1: Failed to get connection to session: Did not receive a reply. Possible causes include: the remote application did not send a reply, the message bus security policy blocked the reply, the reply timeout expired, or the network connection was broken.)
GConf Error: Failed to contact configuration server; some possible causes are that you need to enable TCP/IP networking for ORBit, or you have stale NFS locks due to a system crash. See http://projects.gnome.org/gconf/ for information. (Details - 1: Failed to get connection to session: Did not receive a reply. Possible causes include: the remote application did not send a reply, the message bus security policy blocked the reply, the reply timeout expired, or the network connection was broken.)
[root@localhost bofSELinux]# setenforce 0
[root@localhost bofSELinux]# ./bufferOverflow.sh
Building and Loading Policy
+ make -f /usr/share/selinux/devel/Makefile
Compiling targeted bufferOverflow module
/usr/bin/checkmodule: loading policy configuration from tmp/bufferOverflow.tmp
/usr/bin/checkmodule: policy configuration loaded
/usr/bin/checkmodule: writing binary representation (version 10) to tmp/bufferOverflow.mod
Creating targeted bufferOverflow.pp policy package
rm tmp/bufferOverflow.mod.fc tmp/bufferOverflow.mod
+ /usr/sbin/semodule -i bufferOverflow.pp
+ /sbin/restorecon -F -R -v /home/fedora/Desktop/bufferoverflow
[root@localhost bofSELinux]#
```



```

fedora@localhost:~/Desktop
File Edit View Terminal Help
allow usr_t self:process { fork sigchld setpgid };
allow usr_t self:unix_stream_socket { create connect };
allow usr_t shell_exec_t:file { read open execute entrypoint execute_no_trans };
allow usr_t unconfined_t:fd use;
allow usr_t unconfined_t:fifo_file { read write ioctl getattr };
allow usr_t unconfined_t:process sigchld;
allow usr_t user_devpts_t:chr_file { read write ioctl getattr };
allow usr_t user_home_dir_t:dir search;
allow usr_t user_home_t:dir { write search read open getattr add_name };
allow usr_t user_home_t:file { write ioctl read create open getattr append };
allow usr_t var_run_t:dir search;
allow usr_t var_t:dir search;
#===== ROLES =====
role unconfined_r types usr_t:
[root@localhost Desktop]# setenforce 1
[root@localhost Desktop]# su fedora
[fedora@localhost Desktop]$ ./bufferoverflow
[fedora@localhost Desktop]$ su
Password:
[root@localhost Desktop]# setenforce 0
[root@localhost Desktop]# su fedora
[fedora@localhost Desktop]$ ./bufferoverflow
sh-4.0#

```

که در شکل آخر ملاحظه می‌شود که در حالت enforcing، برنامه اجرا می‌شود اما دسترسی به shell داده نمی‌شود. و در حالتی که permissive باشد، اکسپلویت اجرا می‌شود.

فایل‌های نام‌برده در این گزارش، در پیوست آمده است.