

<Write-ups>

**Kenji**

**Ringzer0ctf.com**

Catergory: Forensics

Challenge: [8] 65

“Hide my ass in my home”

root@AtomPi4:~/Downloads# tar -xvf 3d1e957be3b4880a4481d193eb563aff.tar.gz

./

./.viminfo

./.bash\_profile

./bob.tar.gz

./.bashrc

./.bash\_logout

./.mozilla/

./.mozilla/extensions/

./.mozilla/extensions/{ec8030f7-c20a-464f-9b0e-13a3a9e97384}/

./.mozilla/extensions/{ec8030f7-c20a-464f-9b0e-13a3a9e97384}/.fedora-langpack-install

./.mozilla/extensions/{ec8030f7-c20a-464f-9b0e-13a3a9e97384}/langpack-fr@firefox.mozilla.org.xpi

./.mozilla/plugins/

./index.html

./.bash\_history

./1601066\_559677267463652\_942103441\_n.jpg

./Electro - Swing || Jamie Berry Ft. Octavia Rose - Delight.mp3

./.gnome2/

./you

./.me.swp

root@AtomPi4:~/Downloads# dlist

total 10920

drwxr-xr-x 2 501 501 4096 Nov 12 2010 .gnome2

-rw-r--r-- 1 501 501 124 Jul 18 2013 .bashrc

-rw-r--r-- 1 501 501 176 Jul 18 2013 .bash\_profile

-rw-r--r-- 1 501 501 18 Jul 18 2013 .bash\_logout

drwxr-xr-x 4 501 501 4096 Jan 11 2014 .mozilla

-rw-rw-r-- 1 501 501 11311 Feb 21 2014 index.html

-rw-r--r-- 1 501 501 12288 Feb 21 2014 .me.swp

-rw------- 1 501 501 2907 Feb 21 2014 .bash\_history

-rw-rw-r-- 1 501 501 676 Feb 21 2014 you

-rw------- 1 501 501 1319 Feb 21 2014 .viminfo

-rw-r--r-- 1 root root 5505097 Feb 21 2014 'Electro - Swing || Jamie Berry Ft. Octavia Rose - Delight.mp3'

-rw-r--r-- 1 root root 20969 Feb 21 2014 1601066\_559677267463652\_942103441\_n.jpg

drwx------ 4 501 501 4096 Feb 21 2014 .

-rw-rw-r-- 1 501 501 0 Feb 21 2014 bob.tar.gz

-rw-r--r-- 1 root root 5503802 Dec 17 18:35 3d1e957be3b4880a4481d193eb563aff.tar.gz

-rw-r--r-- 1 root root 77824 Dec 17 18:52 .me.swp.swp

drwx------ 17 root root 4096 Dec 17 18:59 ..

root@AtomPi4:~/Downloads# file you

you: UTF-8 Unicode text, with very long lines

root@AtomPi4:~/Downloads# cat you

Tant qu’il existera, par le fait des lois et des mœurs, une damnation sociale créant artificiellement, en pleine civilisation, des enfers, et compliquant d’une fatalité humaine la destinée qui est divine ; tant que les trois problèmes du siècle, la dégradation de l’homme par le prolétariat, la déchéance de la femme par la faim, l’atrophie de l’enfant par la nuit, ne seront pas résolus ; tant que, dans de certaines régions, l’asphyxie sociale sera possible ; en d’autres termes, et à un point de vue plus étendu encore, tant qu’il y aura sur la terre ignorance et misère, des livres de la nature de celui-ci pourront ne pas être inutiles.

root@AtomPi4:~/Downloads# file .me.swp

.me.swp: Vim swap file, version 7.2, pid 13545, user test, host grosse-marde, file ~test/me, modified

root@AtomPi4:~/Downloads# vim .me.swp



root@AtomPi4:~/Downloads# cat .me.swp

b0VIM 7.2|▒S

U3210#"! Utad▒▒▒▒▒▒▒▒Flag-1s4g76jk89ffull of full and sunfull and i'm beautifull

NAME

vim - Vi IMproved, a programmers text editor

-r {file} Recovery mode. The swap file is used to recover a crashed

editing session. The swap file is a file with the same

filename as the text file with ".swp" appended. See ":help

recovery".

root@AtomPi4:~/Downloads# vim -r .me.swp

