Spicy Dressing

By: Clemence Yi

[Commands to use](#_3znysh7)

[List of Software](#_gmcio6gu1y53)

[Removal](#_68yye9ehg7pm)

[README Dependent](#_hm3ibrlm9hau)

[List of Media File Types](#_3dy6vkm)

[Configuration Files](#_g3xt9j10jrlc)

[sshd\_config](#_gztzqwk0wvuk)

[lightdm.conf](#_xxmm0k7lgars)

[common-password](#_6cw1ls114xb7)

[common-auth](#_tekfogg7nph1)

[login.defs](#_7i8f436mq4ff)

[sysctl.conf](#_in8rpv64ej06)

[Firewall Security](#_j2dfkhydhflv)

[System Software and Settings](#_l8pb68buzjy3)

# **Commands to use**

|  |  |  |
| --- | --- | --- |
| Function | Command(s) | Notes |
| Add a user | sudo adduser <username>  sudo useradd <username> | Both commands do the same thing, but **adduser** requires a password |
| Delete a user | sudo deluser <username>  sudo userdel <username> | Does the same thing |
| Remove admin privileges | sudo deluser <username> sudo | The **sudo** part is the group |
| Change password | chpasswd <username> | The prompt will ask for a new password |
| Update | sudo apt-get update | Good idea to do this after System Settings are updated |
| Upgrade | sudo apt-get upgrade –y | This command will take a lot of time. Best left for last! |
| Remove software | sudo apt-get remove <package> -y  sudo apt-get purge <package> -y  sudo apt-get autoremove –y | See [**List of Software**](#_gmcio6gu1y53) |
| Firewall | sudo apt-get install ufw –y  sudo ufw enable | Will easily get points |
| Install a software | sudo apt-get install <package> -y | See [**List of Software**](#_gmcio6gu1y53) |
| Start a service | sudo service <service> start | Will start the service specified |
| Remove a service | sudo service <service> stop | Will stop the service specified |
| Find media files | find . | grep [.]<media file extension> | Will look for the media file type requested; see [**List of Media File Types**](#_3dy6vkm) |
| Copy a file | sudo cp <filename> <location> | Copies a file to the location requested |
| Remove a file or directory | sudo rm <file or directory name> | If you want to remove a directory, add **–r** before the directory name |
| Remove root login | sudo passwd -l root | No comment |
| View every single package | dpkg -l less | Watch out for a distressingly long list of packages |
| Edit a config file | sudo nano <filename> | Either navigate to the directory the file is in, or put the path with the file name |
| Check the status of services | sudo service --status-all | Make sure the necessary services are running |
| Change permissions of a file | sudo chmod <3 digit number> <filename> | |  |  | | --- | --- | | Octal | File Mode | | 0 | --- | | 1 | --x | | 2 | -w- | | 3 | -wx | | 4 | r-- | | 5 | r-x | | 6 | rw- | | 7 | rwx |   R means read  W means write  X means execute  Each digit is a different permission group. |

# **List of Software**

## **Removal**

The following software is potentially malicious and should be removed:

* bind9
* telnet\*
* iodine
* kismet
* john
* medusa
* hydra
* fcrackzip
* ayttm
* empathy
* logkeys
* vino
* tightvncserver
* rdesktop
* remmina
* vinagre
* netcat\*
* rsync

Command to delete them all: **sudo apt-get purge bind9 telnet\* iodine kismet john medusa hydra fcrackzip ayttm empathy logkeys vino tightvncserver rdesktop remmina vinagre netcat\* rsync -y && sudo apt-get remove bind9 telnet\* iodine kismet john medusa hydra fcrackzip ayttm empathy logkeys vino tightvncserver rdesktop remmina vinagre netcat\* rsync -y && sudo apt-get autoremove -y**

*One Ring to rule them all, One Ring to find them,*

*One Ring to bring them all and in the darkness bind them*

Wait a sec. Let’s make that more relevant!

*One Command to rule them all, One Command to find them,*

*One Command to bring them all and in the darkness bind them*

That’s better.

## **README Dependent**

The following software may or may not be removed. The removal or installation of the following is dictated by the README.

* apache2
* nginx
* vsftpd
* openssh-server
* samba
* mysql\*
* postfix
* mongodb
* mariadb
* sqlite

# **List of Media File Types**

The README states that any non-work related media files are prohibited. The most common file types are here:

* .mp3
* .mp4
* .wav
* .jpg
* .png
* .m4a
* .m4b
* .aif
* .iff
* .m3u
* .mid
* .mpa
* .wma
* .3g2
* .3gp
* .asf
* .avi
* .flv
* .m4v
* .mov
* .mpg
* .rm
* .srt
* .swf
* .vof
* .wmv
* .gif

Find and remove with this command: **find . -name “\*.extension” -delete**

# Configuration Files

There are many configuration files that may give points during the competition.

These may be some of them.

* SSH config
  + /etc/ssh/sshd\_config
* Lightdm config
  + /etc/lightdm/lightdm.conf
* Password configs
  + /etc/pam.d/common-password
  + /etc/pam.d/common-auth
* Password expiration information
  + /etc/login.defs
* Networking
  + /etc/sysctl.conf
* FTP config
  + /etc/vsftpd.conf
* Samba config
  + /etc/samba/smb.conf
* Ufw config
  + /etc/ufw.conf
* Sudo perms
  + /etc/group
* Check for hidden users
  + /etc/passwd
* Redirects
  + /etc/hosts
* Encrypted passwords
  + /etc/shadows

## sshd\_config

Change **PermitRootLogin** and **PermitEmptyPasswords** to **no**.

## lightdm.conf

If the file exists, simply change **allow-guest=true** to **false**, and if the file doesn’t exist, add these lines:

* **[SeatDefaults]**
* **user-session=ubuntu**
* **greeter-session=unity-greeter**
* **allow-guest=false**

## common-password

Add these lines:

* **password requisite pam\_cracklib.so retry=3 minlen=8 difok=3 reject\_username minclass=3 maxrepeat=2 dcredit=-1 ucredit=-1 lcredit=-1 ocredit=-1**
* **password sufficient pam\_unix.so nullok use\_authtok sha512 shadow remember=7**

## common-auth

Add this line:

* **auth optional pam\_tally.so deny=5 unlock\_time=900 onerr=fail audit even\_deny\_root\_account silent**

## login.defs

Change the following values.

|  |  |  |
| --- | --- | --- |
| Line | Before | Change to |
| PASS\_MAX\_DAYS | 99999 | 15 |
| PASS\_MIN\_DAYS | 0 | 6 |
| PASS\_WARN\_AGE | 7 | 9 |

## sysctl.conf

Do not uncomment any lines, it is easier to just add them to the end of the file.

* **net.ipv4.tcp\_syncookies = 1**
* **net.ipv4.tcp\_syn\_retries = 2**
* **net.ipv4.tcp\_synack\_retries = 2**
* **net.ipv4.tcp\_max\_syn\_backlog = 4096**
* **net.ipv4.conf.all.secure\_redirects = 0**
* **net.ipv4.conf.all.send\_redirects = 0**
* **net.ipv4.conf.default.send\_redirects = 0**
* **net.ipv4.conf.all.accept\_redirects = 0**
* **net.ipv4.conf.default.accept\_redirects = 0**
* **net.ipv4.conf.all.secure\_redirects = 0**
* **net.ipv4.conf.default.secure\_redirects = 0**
* **net.ipv4.conf.all.rp\_filter = 1**
* **net.ipv4.conf.default.rp\_filter = 1**
* **net.ipv4.conf.all.send\_redirects = 0**
* **net.ipv4.conf.default.send\_redirects = 0**
* **net.ipv4.conf.all.accept\_source\_route = 0**
* **net.ipv4.conf.default.accept\_source\_route = 0**
* **kernel.exec-shield = 1**
* **kernel.randomize\_va\_space = 2**

# Firewall Security

|  |  |  |
| --- | --- | --- |
| **Function** | **Command** | **Notes** |
| **Allow access through a port** | sudo ufw allow [port/protocol]  sudo ufw allow from [ip address] | No comment |
| **Deny access through a port** | sudo ufw deny [port/protocol]  sudo ufw deny from [ip address] | No comment |
| **Configure defaults** | sudo ufw default allow outgoing  sudo ufw default deny incoming | No comment |
| **List all rules** | sudo ufw status verbose | No comment |

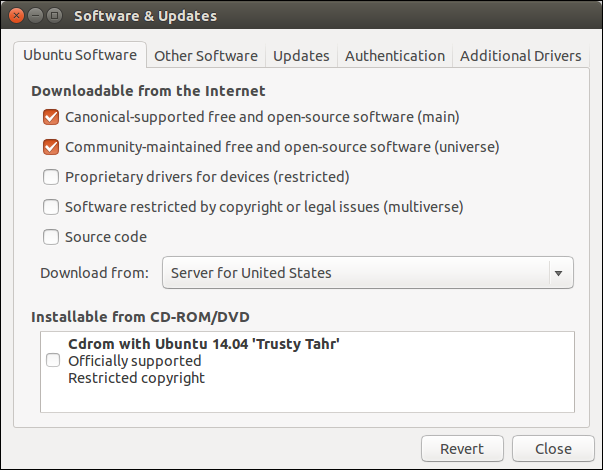
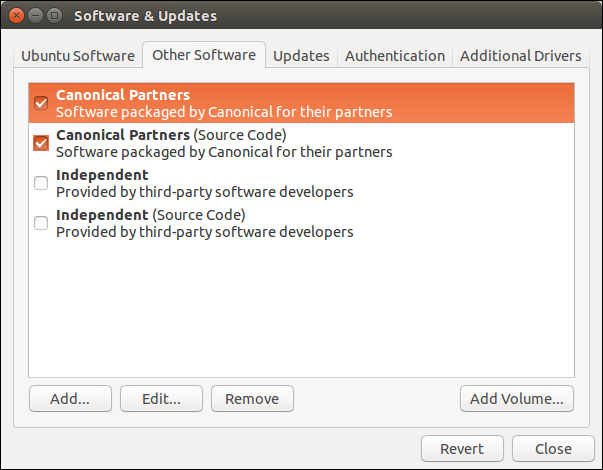
nmap -v localhost

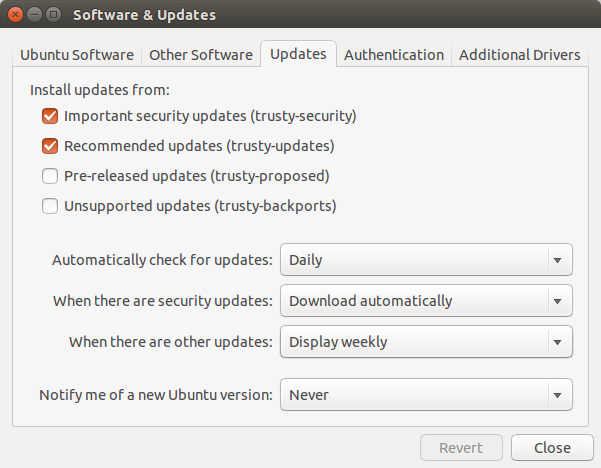
Ports

* ftp 21
* ssh 22
* http 80
* samba 445
* mysql 3306

# System Software and Settings

Under system settings, go to the Software and Updates section. Update the settings to match these pictures:





* nmap -v localhost
* Ports
  + ftp 21
  + ssh 22
  + http 80
  + samba 445
  + mysql 3306
* https://www.digitalocean.com/community/tutorials