**Ubuntu 14 Security Checklist**

***Made by Ardy***

---------------------------------------------------------------------------------------------------------------

This is a general OS hardening checklist for Ubuntu. There are many like it out there, but this one is mine. You may use this checklist in any way you deem fit to help you with Ubuntu, whether it be in some random high school defense competition or making your Home Ubuntu Installation a bit more secure.

Text in light blue are terminal commands.

Text that is underlined is important information.

---------------------------------------------------------------------------------------------------------------

***1: Account Management***

***2: Account Management***

***3: Files And Programs***

***3: Updates***

***3: Antivirus***

***4: SSH***

***4: VSFTPD***

***5: Samba***

***5: Services***

***6: Firewall***

**Account and User Management**

1. **Deleting Users**

* System Settings, then User Accounts
* Click the unlock symbol in the top right to make edits to the selected account.
* On the bottom left, click the “-” symbol to delete the account.

2. **Changing User Account Type**

* Unlock the Account
* Click Account type, then change as needed.

3. **Changing User Password**

10 characters, with lower/upper case, numbers, and symbols will make it better.

* Unlock the Account
* Change Password, add Passwords for EVERY account, make sure to write them down!

4. **Disabling the Guest Account**

* Open Terminal (CTRL+ALT+T)
* sudo nano /usr/share/lightdm/lightdm.conf.d/50-ubuntu.conf
* Add allow-guest=false to the end of the line, click save.

5. **Editing User Groups**

* To list all Groups: cat /etc/group
* To add a group: addgroup [groupname]
* To add a user to a group: adduser [username] [groupname]

Check /etc/sudoers.d and make sure only members of group sudo can sudo.

Check /etc/group and remove non-admins from sudo and admin groups.

* sudo userdel -r $user
* sudo groupdel $user

To be safe, just use the GUI Account management as described above to make changes if you are inexperienced with the Linux Terminal… unless you’re Zach.

6. **Password Requirements**

* Open Terminal (CTRL+ALT+T)
* Install PamCracklib with sudo apt-get libpam-cracklib
* gedit /etc/pam.d/common-password
* remember = 5 to the end of the line with pam\_unix.so
* minlen = 8 to the end of the line with pam\_unix.so
* ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 to the end of the line with pam\_cracklib.so

7. **Password History**

* Maximum Password Duration  
   - PASS\_MAX\_DAYS 7
* Minimum Password Duration  
   - PASS\_MIN\_DAYS 7
* Days set before expiration to warn Users to change their password  
   - PASS\_WARN\_AGE 14
* Save the file and close it.

8. **Setting Account Lockout Policy**

* Open Terminal (CTRL+ALT+T)
* gedit /etc/pam.d/common-auth
* Add this line to the end of the file
* auth required pam\_telly2.so deny=5 onerr=fail unlock\_time=1800
* chpasswd , then change all passwords to satisfy the new requirements.

9. **Disabling Root User**

* Open Terminal (CTRL+ALT+T)
* passwd -l root

10. **Auditing Policies**

* sudo apt-get install auditd
* Enable audits with auditctl -e 1
* gedit /etc/audit/auditd.conf

**Files and Programs**

11. **File Management**

* Delete suspicious files via the file explorer
* Use the Ubuntu Software center, go to “Installed”, and uninstall as needed.

**Updates**

12. **Enabling Automatic Updates**

* Go to System Settings
* Software and Updates
* Set Automatic updates to daily, check Important security updates as well.

13. **Updating via Terminal**

( Use sudo if needed, and remember, EVERYTHING is case sensitive!)

* CTRL+ALT+T
* sudo apt-get update
* Follow with a sudo apt-get upgrade , this may take some time so work on other things while it updates.
* Search “Software Updater” by clicking the Ubuntu icon in the top left and follow the prompts (Do this AFTER upgrading).
* A restart will most likely be needed to apply updates.

**Antivirus**

15. **Antivirus**

* sudo apt-get install clamav && sudo apt-get install clamtk
* sudo clamtk (click “Home” to scan the Home directory.)
* sudo apt-get purge johntheripper (In case it’s installed.)

**SSH**

16. **Installing Open SSH Server**

* sudo apt-get install openssh-server then sudo service ssh start

17. **Configuring SSH**

* sudo gedit /etc/ssh/sshd\_config
* Set PermitRootLogin no
* Set PermitEmptyPasswords no
* Add MaxAuthTries 3
* Set/Add PasswordAuthentication no
* Set/Add AllowGroups $SSH\_GRPS
* Set/Add X11Forwarding yes
* Set/Add LogLevel VERBOSE
* Set/Add LoginGraceTime 20
* Allow through UFW with sudo ufw allow 22
* Restart with sudo service ssh restart

**VSFTPD**

16. **Installing VSFTPD Server**

* sudo apt-get install vsftpd then sudo service vsftpd start

17. **Configuring VSFTPD**

* sudo gedit /etc/vsftpd.conf
* Set anonymous\_enable=NO
* Set local\_enable=YES
* Set write\_enable=YES
* Set chroot\_local\_user=YES
* Allow through UFW with sudo ufw allow 21
* Restart with sudo service vsftpd restart

**Samba**

16. **Installing Samba Server**

* sudo apt-get install samba then sudo service samba start

17. **Configuring Samba**

* Set password for Samba user with sudo smbpasswd -a <user\_name>
* sudo gedit /etc/samba/smb.conf
* Set hosts allow = 127.0.0.1 <other private networks>
* Set hosts deny = 0.0.0.0/0
* Set valid users = @smbusers, <admins> (in [global] tag)
* Restart with sudo service samba restart

**Services**

18. **Using Services**

Services in Ubuntu are pretty much just like the task manager in Windows. Disable suspicious services, though keep in mind which are the default OS’s.

* sudo apt-get install bum
* Run bum

To enable a service, check the box next to it. To start it, right-click and select start. A light bulb glowing on or off will indicate when the service has been stopped or disabled.

It’s a good idea to disable the following services as they are not normally used, though your needs may vary.

* Telnet
* Anonymous FTP
* Remote Process (Rexec.Rlogin, Rsh)
* Rstatd
* Finger
* Talk, Ntalk

**Firewall**

14. **UFW**

( The firewall and logging is turned off by default, turn it on with )

* sudo ufw enable
* sudo ufw logging on
* sudo ufw allow ssh (this will be useful later).

We will now install GUFW, which is a GUI version of ufw.

* sudo apt-get install gufw

To access gufw go to System Settings and click on the new “Firewall Configuration”.

A general rule of thumb is to deny incoming and allow outgoing.

If you are required to allow or deny specific ports, check the Ubuntu Docs under “ufw”.

15. **Firewall Logging**

* sudo gufw
* Click “Unlock” in the bottom-right corner.
* Click “Edit” from menu bar and then “Preferences”.
* Set the “Logging” dropdown box to “Full” and check the “Logging”, “Listening Report”, and “Show notifications” checkboxes.

**Disclaimers and Notes:**

1. Using Samba/VSFTPD may be considered as a server vulnerability, so in some cases you might be required to remove it. If you’re doing a high school security competition, installing a service such as Samba could penalize you. Could.

2. Using “sudo” will grant you permissions until your terminal process is closed, so you only need to enter “sudo” once in a terminal and your permissions will be elevated as long as that terminal is not closed.

3. Disclaimer: I may or may not have tested this checklist : )

4: Check out the Cyber Patriot Discord Server and Subreddit for some good conversation on securing systems, you might learn a thing or two.

**Special Thanks to:**

*/Kyle/*

*Zach*

*Toasty*

*ForestCorgi*

*Mat*

*“B14CKH47” (Cough, Steve, Cough.)*

*And all the other autists on Discord*