Nice script found on LinkedIN regarding the securisation of a Ubuntu machine

```
#!/bin/bash

# Update the package repository
apt-get update -y

# Install and configure the firewall (ufw)
apt-get install -y ufw
ufw default deny incoming
ufw default allow outgoing
ufw allow 22/tcp # allow incoming SSH traffic
ufw allow 80/tcp # allow incoming HTTP traffic
ufw allow 443/tcp # allow incoming HTTPS traffic
ufw enable

# Disable root login via SSH
sed -i 's/PermitRootLogin yes/PermitRootLogin no/g' /etc/ssh/sshd_config
systemctl restart ssh

# Remove unnecessary packages and services
apt-get remove -y telnet
apt-get remove -y rsh-server
apt-get remove -y rsh-client
apt-get remove -y xinetd
apt-get remove -y tftp
apt-get remove -y tftpd
apt-get remove -y talk
apt-get remove -y talkd

# Enable automatic security updates
apt-get install -y unattended-upgrades
dpkg-reconfigure --priority=low unattended-upgrades

# Remove old software packages and clean up the package cache
apt-get autoremove -y
apt-get clean -y

# Set a strong password policy
echo "password  requisite      pam_cracklib.so retry=3 minlen=8 difok=3
reject_username minclass=3 maxrepeat=2" >> /etc/pam.d/common-password
echo "password  required      pam_pwquality.so try_first_pass
local_users_only retry=3" >> /etc/pam.d/common-password

# Enable audit logging
apt-get install -y auditd
auditctl -e 1

# Disable core dumps
echo "* hard core 0" >> /etc/security/limits.conf
```

```
# Log the contents of the /etc/passwd, /etc/shadow, and /etc/group files
chmod 600 /etc/passwd
chmod 600 /etc/shadow
chmod 600 /etc/group

# Log all successful and unsuccessful login attempts
sed -i 's/\#\?\*\s+.*faillog.*/faillog\tpam_tally2\.so onerr=succeed/g'
/etc/pam.d/common-auth
sed -i 's/\#\?\*\s+.*faillog.*/faillog\tpam_tally2\.so onerr=succeed/g'
/etc/pam.d/sshd

# Enable process accounting
accton on

# Install and configure intrusion detection (fail2ban)
apt-get install -y fail2ban
cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
sed -i 's/bantime\s=\s600/bantime = 3600/g' /etc/fail2ban/jail.local
sed -i 's/findtime\s=\s600/findtime = 3600/g' /etc/fail2ban/jail.local
systemctl restart fail2ban
```

From:
https://wiki.fortier-family.com/ - **Warnaud's Wiki**

Permanent link:
https://wiki.fortier-family.com/os/ubuntu/securize

Last update: **2023/02/16 15:40**