

Hardening of Linux

Introduction

Despite the fact that Linux is Open Source and Linux it comes as a surprise that in the default installation are some hidden trackers and spy software.

Hardening

There is a script that will remove all malware. Originally written for Linux, but it can easily adopted for other distributions.

[Ubuntu Secure](#)

This script does:

- System update and software upgrade
- Amazon & advert web apps removing
- AptUrl Removing (tool, which gives possibilities to start installation by clicking on url, can be executed with js, which is not secure)
- Guest session disable for LightDM
- Remote login disable for LightDm
- DNS encryption (dnscrypt-proxy)
I don't recommend this, hence my DNS server is not working with encryption.
`apt -y remove dnscrypt-proxy`
- FireWall (UFW)
- Antivirus (ClamAV)
- Brute Force protection (Fail2Ban)
- Basic Telemetry Removing (ZeitGeist) and unsecure libs and pre-installed software with high and potential risks

Here is a version for rpm based systems:

```
#!/bin/bash
```

```
# This script removes telemetry and enhances system security on an RPM-based Linux distribution.
```

```
# System Up to Date:
sudo dnf -y update
sudo dnf -y upgrade
# =====

# Remove any pre-installed telemetry or unwanted software (no direct equivalents for `unity-lens-shopping` and
`unity-webapps-common` on RPM-based systems):
# Remove pre-installed software that may be tracking or unwanted:
sudo dnf -y remove gnome-online-accounts
sudo dnf -y remove gnome-shell-extension-prefs
sudo dnf -y remove gnome-software
# =====

# Disable Guest session & remote login for LightDM (if LightDM is in use):
if [ -f /etc/lightdm/lightdm.conf.d/50-no-guest.conf ]; then
    sudo sh -c 'printf "[Seat:*)\nallow-guest=false\n greeter-show-remote-login=false\n" >
/etc/lightdm/lightdm.conf.d/50-no-guest.conf'
    sudo dnf -y remove lightdm-remote-session-freerdp
    sudo dnf -y remove lightdm-remote-session-uccsconfigure
fi
# =====

# Remove any equivalent telemetry-related packages:
# Note: zeitgeist is generally specific to Ubuntu/Debian, so we focus on similar tools on RPM systems.

# Remove `tracker`, a GNOME-based file indexing and search tool that collects metadata:
sudo dnf -y remove tracker
sudo dnf -y remove tracker-miners
sudo dnf -y remove tracker3
sudo dnf -y remove tracker3-miners

# Remove `gnome-usage`, a system resource monitor that could collect usage data:
sudo dnf -y remove gnome-usage

# Remove `PackageKit`, which can send data back to package servers:
sudo dnf -y remove PackageKit
# =====

# DNS encryption:
```

```
sudo dnf -y install dnscrypt-proxy
```

```
# =====
```

```
# FireWall (using firewalld):
```

```
sudo dnf -y install firewalld
```

```
sudo systemctl start firewalld
```

```
sudo systemctl enable firewalld
```

```
sudo firewall-cmd --permanent --set-default-zone=block
```

```
sudo firewall-cmd --permanent --add-service=http
```

```
sudo firewall-cmd --permanent --add-service=https
```

```
sudo firewall-cmd --reload
```

```
# =====
```

```
# ClamAV Antivirus Installation:
```

```
sudo dnf -y install clamav
```

```
sudo dnf -y install clamav-daemon
```

```
sudo systemctl enable clamav-daemon
```

```
sudo systemctl start clamav-daemon
```

```
# =====
```

```
# Fail2Ban installation (protects from brute force login):
```

```
sudo dnf -y install fail2ban
```

```
sudo systemctl enable fail2ban
```

```
sudo systemctl start fail2ban
```

```
# =====
```

```
# Remove other potentially problematic or unused packages:
```

```
# Removing `cups` if you don't need printer support:
```

```
# sudo dnf -y remove cups
```

```
# Remove `remmina` if you don't use it for remote connections:
```

```
# sudo dnf -y remove remmina
```

```
# Remove unnecessary GNOME components:
```

```
sudo dnf -y remove evolution
```

```
sudo dnf -y remove evolution-data-server
```

```
sudo dnf -y remove gvfs-fuse
```

```
sudo dnf -y remove vino # VNC server (remote desktop sharing)
```

```
sudo dnf -y remove gnome-shell-extension-background-logo # Fedora logo on desktop background
```

```
sudo dnf -y remove gnome-user-share # Potentially shares user data over the network
```

```
sudo dnf -y remove libreport-plugin-bugzilla # Automatic bug reporting to Bugzilla
sudo dnf -y remove abrt-addon-xorg # Automatic bug reporting for Xorg
sudo dnf -y remove abrt-cli # Command-line tool for automatic bug reporting
sudo dnf -y remove abrt-addon-ccpp # Automatic bug reporting for C/C++ programs
sudo dnf -y remove abrt-addon-kerneloops # Automatic bug reporting for kernel oopses
sudo dnf -y remove abrt-addon-pstoreoops # Automatic bug reporting for pstore oopses
# =====

# Autoremove unnecessary dependencies:
sudo dnf -y autoremove

# =====

# Troubleshooting:
# If the internet does not work, try restarting dnscrypt-proxy:
# sudo systemctl restart dnscrypt-proxy
# Also, the tool may use another port, detect the port in this output:
# sudo ss -ntulp
# Then add the port to firewall:
# sudo firewall-cmd --permanent --add-port=[portnumber]/tcp
# sudo firewall-cmd --reload
# =====
```

Revision #3

Created 22 January 2024 17:26:44 by Admin

Updated 14 September 2024 17:20:33 by Admin