# Linux Privacy Setup Toolkit - Complete Guide

## Table of Contents



## Overview

The Linux Privacy Setup Toolkit is a comprehensive bash script designed to transform your Linux system into a privacy-focused, security-hardened machine. Unlike basic privacy guides that suggest installing a VPN and calling it a day, this toolkit implements multiple layers of protection at the system level.

### Why This Tool Exists

Most privacy tutorials are scattered across outdated blog posts, broken GitHub repositories, and forum threads from years ago. This toolkit consolidates the best privacy practices into a single, automated setup process that:

- **Actually works** - Tested on major Linux distributions
- **Explains what it's doing** - No black box operations
- **Asks for permission** - You control what gets installed
- **Provides ongoing tools** - Not just a one-time setup

### Philosophy

Privacy isn't about becoming invisible - it's about making surveillance expensive and difficult. This toolkit raises the cost of tracking you by implementing multiple layers of protection that work together to scatter your digital footprint instead of serving it up on a silver platter.

## What This Tool Does

## 🔥 UFW Firewall Configuration

**Problem Solved**: Your system accepts incoming connections by default, creating attack vectors.

**What It Does**:

- Resets UFW to clean state
- Sets default policy to deny all incoming connections
- Allows only essential outgoing connections (DNS, HTTP, HTTPS, NTP, SSH)
- Enables comprehensive logging
- Creates a restrictive security perimeter around your system

## 🌐 DNS Encryption Setup

**Problem Solved**: DNS requests leak your browsing history to your ISP in plain text.

**What It Does**:

- Configures systemd-resolved for DNS over HTTPS (DoH) and DNS over TLS (DoT)
- Uses Cloudflare (1.1.1.1) and Google (8.8.8.8) as encrypted DNS providers
- Enables DNSSEC for cryptographic validation of DNS responses
- Prevents DNS hijacking and manipulation
- Hides your browsing patterns from network-level surveillance

## 🌍 Browser Privacy Hardening

**Problem Solved**: Default browser settings leak massive amounts of data through tracking, fingerprinting, and telemetry.

**What It Does**:

- Installs Firefox (if not present)
- Creates comprehensive privacy configuration (`user.js` file)
- Disables tracking protection, social media tracking, and fingerprinting
- Blocks WebGL, WebRTC, and Web Audio API (common fingerprinting vectors)
- Disables telemetry, health reports, and data submission to Mozilla
- Configures strict cookie policies and referrer headers
- Prevents DNS prefetching and connection prediction

## 🗂️ Metadata Removal Tools

**Problem Solved**: Files contain hidden metadata that can reveal sensitive information about you, your devices, and your activities.

**What It Does**:

- Installs `mat2` and `exiftool` for comprehensive metadata removal
- Creates a convenient `strip-metadata` command for easy use
- Removes EXIF data from images, document properties, GPS coordinates, camera information, and timestamps
- Provides both GUI-friendly (mat2) and command-line (exiftool) options

## 🏖️ Application Sandboxing

**Problem Solved**: Malicious or compromised applications can access your entire file system and personal data.

**What It Does**:

- Installs and configures Firejail for application sandboxing
- Creates isolated environments for applications with restricted file system access
- Automatically sandboxes common applications using `firecfg`
- Prevents applications from accessing private directories, devices, and system files
- Implements security profiles that drop capabilities and restrict network protocols

## 🔒 System Hardening

**Problem Solved**: Default Linux configurations prioritize usability over security, leaving unnecessary attack surfaces.

**What It Does**:

- Disables unnecessary services (Bluetooth, CUPS printing, Avahi/Zeroconf)
- Configures kernel parameters to prevent common attack vectors
- Enables Address Space Layout Randomization (ASLR) at maximum level
- Restricts access to kernel pointers and system logs
- Hardens network stack against IP spoofing, redirect attacks, and broadcast pings
- Enables TCP SYN cookies to prevent SYN flood attacks
- Protects against hardlink and symlink attacks

## 📊 Privacy Auditing

**Problem Solved**: Privacy is an ongoing process, but most people set it up once and never check again.

**What It Does**:

- Creates a `privacy-audit` command for regular system checks
- Monitors firewall status, DNS configuration, and running services
- Checks browser privacy configurations
- Verifies sandboxing and metadata tools are working

- Provides regular health checks for your privacy setup

# Prerequisites

## System Requirements

- Linux distribution (Ubuntu, Debian, Fedora, or Arch-based)
- Non-root user account with sudo privileges
- Internet connection for downloading packages
- At least 100MB free disk space

## Supported Distributions

- **Ubuntu** 18.04+ and derivatives (Pop!_OS, Linux Mint, etc.)
- **Debian** 10+ and derivatives
- **Fedora** 30+ and derivatives (CentOS Stream, Rocky Linux, etc.)
- **Arch Linux** and derivatives (Manjaro, EndeavourOS, etc.)

## What You Should Know Before Running

- This script makes system-level changes
- Some configurations may break certain applications or workflows
- You'll be prompted before each major change
- A backup of important configurations is recommended
- Some changes require a system reboot to take full effect

# Installation

## Step 1: Download the Script

```
# Create the file manually
nano privacy-toolkit.sh
```

## Step 2: Make Executable

```
chmod +x privacy-toolkit.sh
```

## Step 3: Verify Script Integrity (Recommended)

```
# Check the script content before running
less privacy-toolkit.sh
```

```
# Look for suspicious commands or unexpected network calls
grep -n "curl\|wget\|nc\|telnet" privacy-toolkit.sh
```

# Usage

## Basic Usage

```
./privacy-toolkit.sh
```

The script runs interactively, presenting you with options and asking for confirmation before making changes.

## What to Expect During Setup

1. **Welcome Screen**: Overview of what the toolkit will do
2. **System Detection**: Automatic detection of your Linux distribution
3. **Dependency Check**: Verification and installation of required tools
4. **Interactive Configuration**: Step-by-step setup with user confirmation
5. **Summary Report**: Overview of changes made and next steps

## Sample Session Flow

```
╔═══════════════════════════════════════════╗
║          Privacy Setup Toolkit v1.0.0          ║
╚═══════════════════════════════════════════╝

This toolkit will help configure privacy and security
settings on your Linux system. Each step will ask for
your confirmation before making changes.

Ready to begin privacy setup?
Continue? [y/N]: y

[2025-01-15 10:30:00] Detected distribution: ubuntu 22.04
Checking dependencies...
Missing dependencies: ufw apparmor-utils
Install missing dependencies?
Continue? [y/N]: y

=== Configuring UFW Firewall ===
Configure UFW firewall with restrictive default rules?
Continue? [y/N]: y
✓ UFW firewall configured successfully

=== Configuring Encrypted DNS ===
Configure DNS over HTTPS (DoH) using systemd-resolved?
```

```
Continue? [y/N]: y
✓ Encrypted DNS configured successfully

[... continues for each component ...]
```

# Detailed Feature Breakdown

## UFW Firewall Configuration

**Technical Details**:

```
# Default policies applied
sudo ufw default deny incoming    # Block all incoming connections
sudo ufw default allow outgoing   # Allow all outgoing connections

# Specific rules created
sudo ufw allow ssh                # SSH access (port 22)
sudo ufw allow out 53             # DNS queries
sudo ufw allow out 80             # HTTP traffic
sudo ufw allow out 443            # HTTPS traffic
sudo ufw allow out 123            # Network Time Protocol
```

**What This Protects Against**:

- Unauthorized network services accessing your machine
- Network-based attacks and port scanning
- Malware attempting to establish backdoor connections
- Data exfiltration through unexpected network channels

**Potential Issues**:

- May block legitimate services you run locally
- Gaming or peer-to-peer applications might need additional rules
- Some development tools may require port exceptions

## DNS Encryption Configuration

**Technical Details**: The toolkit configures `/etc/systemd/resolved.conf`:

```
[Resolve]
DNS=1.1.1.1#cloudflare-dns.com 8.8.8.8#dns.google
DNSOverTLS=yes
DNSSEC=yes
FallbackDNS=1.0.0.1#cloudflare-dns.com 8.8.4.4#dns.google
Cache=yes
Domains=~.
```

**What This Protects Against**:

- ISP monitoring of your web browsing through DNS logs
- DNS hijacking and redirection attacks
- Man-in-the-middle DNS manipulation
- DNS cache poisoning attacks

**How It Works**:

- DNS queries are encrypted using TLS before leaving your system
- DNSSEC verifies the authenticity of DNS responses
- Multiple providers ensure redundancy and reliability
- Local caching improves performance while maintaining privacy

## Browser Privacy Hardening

**Key Privacy Settings Applied**:

```
// Disable tracking and fingerprinting
user_pref("privacy.trackingprotection.enabled", true);
user_pref("webgl.disabled", true);
user_pref("geo.enabled", false);

// Prevent data collection
user_pref("datareporting.healthreport.uploadEnabled", false);
user_pref("toolkit.telemetry.enabled", false);

// Harden network behavior
user_pref("network.http.referer.XOriginPolicy", 2);
user_pref("network.dns.disablePrefetch", true);
```

**Fingerprinting Vectors Blocked**:

- **WebGL fingerprinting**: Graphics card and driver information
- **Canvas fingerprinting**: Unique rendering characteristics
- **Audio fingerprinting**: Audio processing differences
- **Font fingerprinting**: Installed system fonts
- **Geolocation**: Physical location data
- **WebRTC**: IP address leakage

**Trade-offs**:

- Some websites may not function correctly
- Media-rich content might have degraded performance
- Online services might request additional verification

## Metadata Removal Tools

**What Gets Removed**:

- **EXIF data from images**: Camera model, GPS coordinates, timestamps, camera settings
- **Document metadata**: Author names, creation/modification dates, revision history, comments
- **Audio/Video metadata**: Recording device, location, duration, bitrate information
- **Office document properties**: Company information, user names, document statistics

**Usage Examples**:

```
# Remove metadata from a single file
strip-metadata photo.jpg

# Remove metadata from multiple files
strip-metadata *.jpg *.png *.pdf

# Check metadata before removal
exiftool photo.jpg
mat2 --show document.pdf
```

**Important Notes**:

- Always keep backups of original files
- Some metadata removal may affect file functionality
- Certain file formats may not support all metadata removal options

## Application Sandboxing with Firejail

**How Sandboxing Works**: Firejail creates isolated environments for applications using Linux namespaces and seccomp filters:

```
# Automatic sandboxing setup
sudo firecfg  # Creates symbolic links for automatic sandboxing

# Manual sandboxing examples
firejail firefox                    # Run Firefox in sandbox
firejail --private vlc movie.mp4    # Run VLC with private home directory
firejail --net=none libreoffice     # Run LibreOffice without network access
```

**Security Features**:

- **Filesystem isolation**: Applications can't access unauthorized directories
- **Network filtering**: Control which applications can access the internet
- **Capability dropping**: Remove dangerous system capabilities from processes

- **Resource limiting**: Prevent applications from consuming excessive system resources

**Default Restrictions**:

- No access to `/boot`, `/lib`, `/usr` directories
- Private `/tmp` directory
- Restricted device access
- No root privileges within sandbox

## System Hardening Parameters

**Network Security Hardening**:

```
# Prevent IP spoofing
net.ipv4.conf.all.accept_source_route = 0

# Disable ICMP redirects
net.ipv4.conf.all.accept_redirects = 0

# Enable SYN cookies (DDoS protection)
net.ipv4.tcp_syncookies = 1

# Log suspicious packets
net.ipv4.conf.all.log_martians = 1
```

**Memory Protection**:

```
# Maximum ASLR (Address Space Layout Randomization)
kernel.randomize_va_space = 2

# Hide kernel pointers
kernel.kptr_restrict = 2

# Restrict kernel logs
kernel.dmesg_restrict = 1
```

**Process Protection**:

```
# Protect against hardlink attacks
fs.protected_hardlinks = 1

# Protect against symlink attacks
fs.protected_symlinks = 1

# Disable core dumps for SUID processes
fs.suid_dumpable = 0
```

# Post-Setup Commands

After running the toolkit, you'll have access to several new commands:

## Privacy Audit Command

```
privacy-audit
```

**What it shows**:

- Current firewall status and rules
- DNS configuration and servers
- Active network services and listening ports
- Browser privacy configurations
- Sandboxing status and active processes
- Metadata removal tool availability

**Example output**:

```
=== Privacy Configuration Audit ===
Date: 2025-01-15 14:30:00

🔥 Firewall Status:
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)

🌐 DNS Configuration:
DNS Servers: 1.1.1.1#cloudflare-dns.com
             8.8.8.8#dns.google

📊 Listening Services:
tcp    LISTEN    0    128    127.0.0.1:631    *:*
tcp    LISTEN    0    128    [::1]:631        [::]:*

🌍 Browser Configuration:
Firefox profiles found:
  - /home/user/.mozilla/firefox/abc123.default/user.js

🏖️ Sandboxing:
Firejail installed: ✓
Active sandbox processes:
  None currently running

🗂️ Metadata Tools:
```

```
mat2: ✓
exiftool: ✓
```

## Metadata Stripping Command

```
# Strip metadata from files
strip-metadata photo1.jpg photo2.jpg document.pdf

# Works with wildcards
strip-metadata *.jpg *.png *.pdf

# Check what metadata exists first
exiftool -all photo.jpg
mat2 --show document.pdf
```

## Sandboxed Application Launching

```
# Applications are automatically sandboxed after firecfg
firefox                    # Launches in sandbox automatically
vlc                        # Launches in sandbox automatically

# Manual sandboxing with custom options
firejail --private firefox                    # Private home directory
firejail --net=none libreoffice               # No network access
firejail --read-only=~ evince document.pdf    # Read-only home directory
```

# Security Considerations

## What This Toolkit Can and Cannot Do

✅ **What It Protects Against**:

- Network-level surveillance and traffic analysis
- Basic browser fingerprinting and tracking
- Metadata leakage from files
- System-level attacks through network services
- Application-level data exfiltration
- DNS monitoring and manipulation

❌ **What It Cannot Protect Against**:

- Advanced persistent threats (APTs) with zero-day exploits
- Physical access to your device
- Social engineering attacks
- Malware that exploits unknown vulnerabilities

- Government-level surveillance with legal access
- Your own poor security practices (weak passwords, etc.)

## Additional Security Recommendations

**Password Security**:

- Use a password manager (KeePassXC, Bitwarden)
- Enable two-factor authentication wherever possible
- Use unique, strong passwords for every account

**System Updates**:

```
# Keep your system updated
sudo apt update && sudo apt upgrade          # Ubuntu/Debian
sudo dnf update                              # Fedora
sudo pacman -Syu                            # Arch
```

**Disk Encryption**: If you haven't already, enable full disk encryption:

- Use LUKS during Linux installation
- Consider encrypting external drives
- Enable encrypted swap

**Additional Privacy Tools to Consider**:

- **VPN**: While not a magic bullet, still useful for some threat models
- **Tor Browser**: For truly anonymous web browsing
- **Signal**: For private messaging
- **ProtonMail**: For private email
- **Veracrypt**: For encrypted file containers

## Understanding Your Threat Model

Before relying solely on this toolkit, consider:

**Who are you protecting against?**

- Casual data harvesting by tech companies
- Network-level surveillance by ISPs
- Local network attackers (coffee shop WiFi)
- Government surveillance
- Criminal hackers

**What are you protecting?**

- Browsing habits and personal interests
- Personal files and documents
- Communication with others
- Financial and business information
- Political or activist activities

**What are the consequences of failure?**

- Embarrassment or social consequences
- Financial loss
- Professional damage
- Legal troubles
- Physical safety concerns

# Troubleshooting

## Common Issues and Solutions

### Firewall Blocks Legitimate Services

**Problem**: UFW blocks a service you need (gaming, development server, etc.) **Solution**:

```
# Allow specific ports
sudo ufw allow 8080                    # Allow port 8080
sudo ufw allow from 192.168.1.0/24     # Allow local network
sudo ufw allow out on tun0             # Allow VPN interface

# Check current rules
sudo ufw status numbered

# Delete unwanted rules
sudo ufw delete [number]
```

### DNS Resolution Issues

**Problem**: Websites don't load or load very slowly **Solution**:

```
# Check DNS status
systemd-resolve --status

# Flush DNS cache
sudo systemd-resolve --flush-caches

# Test DNS resolution
nslookup google.com
dig google.com
```

```
# Temporary fallback to regular DNS
sudo systemctl stop systemd-resolved
echo "nameserver 8.8.8.8" | sudo tee /etc/resolv.conf
```

### Browser Compatibility Issues

**Problem**: Websites break or don't function correctly **Solution**:

1. Create a separate browser profile for problematic sites
2. Temporarily disable strict privacy settings
3. Use a different browser for specific tasks
4. Whitelist specific sites in uBlock Origin or similar extensions

### Application Sandboxing Problems

**Problem**: Sandboxed applications can't access needed files **Solution**:

```
# Check sandbox status
firejail --list

# Create custom profile
firejail --profile=custom_app --read-write=~/Documents app_name

# Disable sandboxing for specific app
sudo rm /usr/local/bin/app_name  # Remove firejail symlink
```

### System Performance Issues

**Problem**: System feels slower after applying hardening **Solution**:

1. Check system resources: `htop`, `iotop`
2. Review firewall logs: `sudo ufw status verbose`
3. Monitor DNS resolution times: `dig google.com`
4. Disable unnecessary hardening if needed

## Getting Help

### Log File Analysis

Check the toolkit log file for errors:

```
# Log files are created in /tmp/ with timestamp
ls -la /tmp/privacy_toolkit_*.log
```

```
# View the most recent log
tail -f /tmp/privacy_toolkit_$(date +%Y%m%d)*.log
```

### System Status Commands

```
# Check firewall
sudo ufw status verbose

# Check DNS
systemd-resolve --status

# Check running services
systemctl list-units --type=service --state=running

# Check network connections
ss -tuln

# Check sandboxed processes
firejail --list
```

# Advanced Customization

## Customizing Firewall Rules

**Adding Application-Specific Rules**:

```
# Gaming applications
sudo ufw allow out 3478:3480/udp    # Discord voice
sudo ufw allow out 7777:7784/tcp    # Steam
sudo ufw allow out 27000:27100/tcp  # Steam games

# Development tools
sudo ufw allow 3000                 # React dev server
sudo ufw allow 8080                 # Common dev port
sudo ufw allow from 192.168.1.0/24  # Local network access
```

**Creating Service-Specific Profiles**:

```
# Create work profile
sudo ufw allow out 443 comment 'HTTPS for work'
sudo ufw allow out 993 comment 'IMAP SSL for email'
sudo ufw allow out 25 comment 'SMTP for email'

# Create gaming profile
sudo ufw allow out 3478:3480/udp comment 'Discord'
sudo ufw allow out 7777:7784/tcp comment 'Steam'
```

## Customizing DNS Configuration

**Using Alternative DNS Providers**: Edit `/etc/systemd/resolved.conf`:

```
[Resolve]
# Quad9 (privacy-focused)
DNS=9.9.9.9#dns.quad9.net 149.112.112.112#dns.quad9.net

# OpenDNS (with filtering)
DNS=208.67.222.222#opendns.com 208.67.220.220#opendns.com

# AdGuard (with ad blocking)
DNS=94.140.14.14#adguard-dns.com 94.140.15.15#adguard-dns.com
```

## Advanced Browser Hardening

**Creating Multiple Browser Profiles**:

```
# Create work profile
firefox -P work -no-remote

# Create personal profile
firefox -P personal -no-remote

# Create high-security profile
firefox -P secure -no-remote
```

**Additional Privacy Extensions**:

- **uBlock Origin**: Advanced ad and tracker blocking
- **ClearURLs**: Remove tracking parameters from URLs
- **Decentraleyes**: Protect against tracking via CDNs
- **Cookie AutoDelete**: Automatically delete cookies
- **Multi-Account Containers**: Isolate browsing contexts

## Custom Sandboxing Profiles

**Creating Application-Specific Profiles**:

```
# Custom profile for document editing
cat > ~/.config/firejail/libreoffice-custom.profile << EOF
include libreoffice.profile
caps.drop all
private-cache
private-dev
private-tmp
```

```
read-only ${HOME}/Templates
read-write ${HOME}/Documents
EOF

# Use custom profile
firejail --profile=libreoffice-custom libreoffice
```

## System Hardening Customization

**Additional Kernel Parameters**: Add to `/etc/sysctl.d/99-privacy-hardening.conf`:

```
# Additional network hardening
net.ipv4.tcp_timestamps = 0
net.ipv4.tcp_sack = 0
net.ipv4.tcp_window_scaling = 0

# Additional memory protection
kernel.exec-shield = 1
kernel.randomize_va_space = 2

# Process restrictions
kernel.yama.ptrace_scope = 1
```

# Frequently Asked Questions

## General Questions

**Q: Will this break my existing applications?** A: The toolkit is designed to minimize breakage, but some applications may need adjustment. Each change asks for your permission, and you can skip components that might interfere with your workflow.

**Q: How much will this slow down my system?** A: Performance impact is minimal. DNS encryption adds a small delay to initial connections, and sandboxing has negligible overhead. Most users won't notice any difference.

**Q: Can I undo these changes?** A: Most changes can be reverted:

- Firewall: `sudo ufw reset`
- DNS: Edit `/etc/systemd/resolved.conf`
- Browser: Delete `user.js` files
- Sandboxing: `sudo firecfg --clean`
- System hardening: Remove files from `/etc/sysctl.d/`

## Technical Questions

**Q: Why not use a VPN instead?** A: VPNs are useful but not sufficient alone. This toolkit addresses system-level privacy issues that VPNs can't solve, like browser fingerprinting, metadata leakage, and local application security.

**Q: Is this better than using Tails or Qubes?** A: Different tools for different needs:

- **Tails**: Best for temporary, anonymous sessions
- **Qubes**: Best for high-security compartmentalization
- **This toolkit**: Best for hardening your daily-use Linux system

**Q: Why systemd-resolved instead of other DNS solutions?** A: Systemd-resolved is already present on most modern Linux systems, supports DoH/DoT out of the box, and integrates well with existing network management tools.

## Privacy Questions

**Q: How does this compare to using Tor?** A: This toolkit hardens your regular browsing, while Tor provides anonymity through routing. Use both for different purposes:

- **This toolkit**: Daily browsing with improved privacy
- **Tor**: Anonymous browsing when identity protection is critical

**Q: Will this protect against government surveillance?** A: This toolkit provides protection against casual surveillance and data harvesting. For protection against targeted government surveillance, you need additional operational security measures beyond technical tools.

**Q: What about mobile devices?** A: This toolkit is Linux-specific. For mobile privacy:

- **Android**: Use LineageOS, F-Droid apps, and privacy-focused ROMs
- **iOS**: Limited options due to Apple's restrictions

## Troubleshooting Questions

**Q: What if I can't connect to certain websites?** A: Try these steps:

1. Check if it's a DNS issue: `nslookup website.com`
2. Temporarily disable firewall: `sudo ufw disable`
3. Test with a different browser or profile
4. Check browser console for specific errors

**Q: How do I know if everything is working correctly?** A: Use the built-in audit command:

```
privacy-audit
```

This will show you the status of all privacy components.

**Q: What should I do if I suspect my privacy setup has been compromised?** A:

1. Run `privacy-audit` to check configuration integrity
2. Review firewall logs: `sudo journalctl -u ufw`
3. Check for unexpected network connections: `ss -tuln`
4. Consider running from a live USB if compromise is suspected

---

# Conclusion

The Linux Privacy Setup Toolkit provides a solid foundation for digital privacy, but remember that privacy is an ongoing process, not a one-time setup. Regular audits, system updates, and staying informed about new privacy threats are essential for maintaining your digital security.

This toolkit raises the bar for surveillance by implementing multiple layers of protection, making you a harder target while maintaining system usability. Combined with good security practices and awareness of your threat model, it provides a strong foundation for digital privacy on Linux.

For the most current version of this documentation and the toolkit itself, check for updates regularly and consider contributing to the project if you find improvements or encounter issues.