



# The BlackArch Linux Guide

<https://www.blackarch.org/>

# Contents

<b>1</b>	<b>Introduction</b>	<b>3</b>
1.1	Overview	3
1.2	What is BlackArch Linux?	3
1.3	History of BlackArch Linux	3
1.4	Supported platforms	3
1.5	Get involved	4
<b>2</b>	<b>User Guide</b>	<b>5</b>
2.1	Installation	5
2.1.1	Installing on top of ArchLinux	5
2.1.2	Installing packages	5
2.1.3	Installing packages from source	6
2.1.4	Basic Blackman usage	6
2.1.5	Installing from live-, netinstall- ISO or ArchLinux	6
<b>3</b>	<b>Developer Guide</b>	<b>7</b>
3.1	Arch's Build System and Repositories	7
3.2	Blackarch PKGBUILD standards	7
3.2.1	Groups	7
3.2.1.1	blackarch	7
3.2.1.2	blackarch-anti-forensic	7
3.2.1.3	blackarch-automation	8
3.2.1.4	blackarch-backdoor	8
3.2.1.5	blackarch-binary	8
3.2.1.6	blackarch-bluetooth	8
3.2.1.7	blackarch-code-audit	8
3.2.1.8	blackarch-cracker	8
3.2.1.9	blackarch-crypto	8
3.2.1.10	blackarch-database	8
3.2.1.11	blackarch-debugger	9
3.2.1.12	blackarch-decompiler	9
3.2.1.13	blackarch-defensive	9
3.2.1.14	blackarch-disassembler	9
3.2.1.15	blackarch-dos	9
3.2.1.16	blackarch-drone	9
3.2.1.17	blackarch-exploitation	9
3.2.1.18	blackarch-fingerprint	9
3.2.1.19	blackarch-firmware	10
3.2.1.20	blackarch-forensic	10
3.2.1.21	blackarch-fuzzer	10

3.2.1.22	blackarch-hardware	10
3.2.1.23	blackarch-honeypot	10
3.2.1.24	blackarch-keylogger	10
3.2.1.25	blackarch-malware	10
3.2.1.26	blackarch-misc	10
3.2.1.27	blackarch-mobile	11
3.2.1.28	blackarch-networking	11
3.2.1.29	blackarch-nfc	11
3.2.1.30	blackarch-packer	11
3.2.1.31	blackarch-proxy	11
3.2.1.32	blackarch-recon	11
3.2.1.33	blackarch-reversing	11
3.2.1.34	blackarch-scanner	11
3.2.1.35	blackarch-sniffer	12
3.2.1.36	blackarch-social	12
3.2.1.37	blackarch-spoof	12
3.2.1.38	blackarch-threat-model	12
3.2.1.39	blackarch-tunnel	12
3.2.1.40	blackarch-unpacker	12
3.2.1.41	blackarch-voip	12
3.2.1.42	blackarch-webapp	12
3.2.1.43	blackarch-windows	13
3.2.1.44	blackarch-wireless	13
3.3	Repository structure	13
3.3.1	Scripts	13
3.4	Contributing to repository	14
3.4.1	Required tutorials	14
3.4.2	Steps for contributing	15
3.4.3	Example	15
3.4.3.1	Fetch PKGBUILD	15
3.4.3.2	Clean up PKGBUILD	15
3.4.3.3	Adjust PKGBUILD	15
3.4.3.4	Build the package	16
3.4.3.5	Install and test the package	16
3.4.3.6	Add, commit and push package	16
3.4.3.7	Create a pull request	16
3.4.3.8	Adding a remote for upstream	16
3.4.4	Requests	17
3.4.5	General tips	17
<b>4</b>	<b>Tools Guide</b>	<b>18</b>
4.1	Coming Soon	18

# Chapter 1

## Introduction

### 1.1 Overview

○ BlackArch Linux :

- E - Π , project
- O X - BlackArch
- O Developer - Π BlackArch
- O E - M (WIP)

### 1.2 T BlackArch Linux?

T BlackArch Linux penetration testers . Π [ArchLinux](#) BlackArch .

H Arch Linux [unofficial user repository](#) BlackArch Arch Linux. T .

T [1300](#) . .

### 1.3 History of BlackArch Linux

Coming soon...

### 1.4 Supported platforms

Coming soon...



## 1.5 Get involved

M BlackArch :

Σ: <https://www.blackarch.org/>

Mail: [team@blackarch.org](mailto:team@blackarch.org)

IRC: <irc://irc.freenode.net/blackarch>

Twitter: <https://twitter.com/blackarchlinux>

Github: <https://github.com/Blackarch/>

# Chapter 2

## User Guide

### 2.1 Installation

On BlackArch, T BlackArch 2, compile sources.  
T BlackArch Arch . Λ . E ISO [Live ISO](#) section.

#### 2.1.1 Installing on top of ArchLinux

T `strap.sh` root . Δ .

```
curl -O https://blackarch.org/strap.sh
sha1sum strap.sh # should match: 86eb4efb68918dbfdd1e22862a48fda20a8145ff
sudo ./strap.sh
```

T master package list :

```
sudo pacman -Syyu
```

#### 2.1.2 Installing packages

M blackarch.

1. To list all of the available tools, run

```
pacman -Sgg | grep blackarch | cut -d' ' -f2 | sort -u
```

2. Γ ,

```
pacman -S blackarch
```

3. Γ ,

```
pacman -S blackarch-<category>
```

4. Γ ,

```
pacman -Sg | grep blackarch
```



### 2.1.3 Installing packages from source

M build BlackArch source. M PKGBUILDs [github](#). Γ build [Blackman](#) .

- Π Blackman. E BlackArch , Blackman:

```
pacman -S blackman
```

- M build Blackman:

```
mkdir blackman
cd blackman
wget https://raw2.github.com/BlackArch/blackarch/master/packages/blackman/PKGBUILD
# Make sure the PKGBUILD has not been maliciously tampered with.
makepkg -s
```

- Blackman AUR:

```
<whatever AUR helper you use> -S blackman
```

### 2.1.4 Basic Blackman usage

T Blackman , pacman. H .

- Download, compile and install packages:

```
sudo blackman -i package
```

- Download, compile and install whole category:

```
sudo blackman -g group
```

- Download, compile and install all of the BlackArch tools:

```
sudo blackman -a
```

- To list the blackarch categories:

```
blackman -l
```

- To list category tools:

```
blackman -p category
```

### 2.1.5 Installing from live-, netinstall- ISO or ArchLinux

M BlackArch Linux live- netinstall-ISOs.

Δ <https://www.blackarch.org/download.html#iso>. T ISO.

- Install blackarch-installer package:

```
sudo pacman -S blackarch-installer
```

- Run

```
sudo blackarch-install
```

# Chapter 3

## Developer Guide

### 3.1 Arch's Build System and Repositories

T PKGBUILD build scripts. T makepkg(1) . T PKGBUILD Bash.

Γ :

- [Arch Wiki: Creating Packages](#)
- [Arch Wiki: makepkg](#)
- [Arch Wiki: PKGBUILD](#)
- [Arch Wiki: Arch Packaging Standards](#)

### 3.2 Blackarch PKGBUILD standards

Γ , PKGBUILDs , AUR, . K blackarch , .

#### 3.2.1 Groups

Γ , . O "pacman -S <group name>" .

##### 3.2.1.1 blackarch

H blackarch . A .

T : T .

##### 3.2.1.2 blackarch-anti-forensic

T (forensic activities), , . П .

П: luks, TrueCrypt, Timestomp, dd, ropeadope, secure-delete





### 3.2.1.3 blackarch-automation

П .

П: blueranger, tiger, wiffy

### 3.2.1.4 blackarch-backdoor

П .

П: backdoor-factory, rrs, weevely

### 3.2.1.5 blackarch-binary

П .

П: binwally, packerid

### 3.2.1.6 blackarch-bluetooth

П Bluetooth (802.15.1).

П: ubertooth, tbear, redfang

### 3.2.1.7 blackarch-code-audit

П .

П: flawfinder, pscan

### 3.2.1.8 blackarch-cracker

П .

П: hashcat, john, crunch

### 3.2.1.9 blackarch-crypto

П , .

П: ciphertest, xortool, sbd

### 3.2.1.10 blackarch-database

П .

П: metacoretex, blindsql



### 3.2.1.11 blackarch-debugger

П .

П: radare2, shellnoob

### 3.2.1.12 blackarch-decompiler

П (compiled) .

П: flasm, jd-gui

### 3.2.1.13 blackarch-defensive

П .

П: arpon, chkrootkit, sniffjoke

### 3.2.1.14 blackarch-disassembler

П assembly .

П: inguma, radare2

### 3.2.1.15 blackarch-dos

П DoS (Denial of Service) .

П: 42zip, nkiller2

### 3.2.1.16 blackarch-drone

П drones

П: meshdeck, skyjack

### 3.2.1.17 blackarch-exploitation

П .

П: armitage, metasploit, zarp

### 3.2.1.18 blackarch-fingerprint

П .

П: dns-map, p0f, httpprint



### 3.2.1.19 blackarch-firmware

П firmware

П: None yet, amend asap.

### 3.2.1.20 blackarch-forensic

П .

П: aesfix, nfex, wyd

### 3.2.1.21 blackarch-fuzzer

П fuzz testing principle, . "" .

П: msf, mdk3, wfuzz

### 3.2.1.22 blackarch-hardware

П hardware.

П: arduino, smali

### 3.2.1.23 blackarch-honeypot

П "honeypots", . hackers.

П: artillery, bluepot, wifi-honey

### 3.2.1.24 blackarch-keylogger

П

П: None yet, amend asap.

### 3.2.1.25 blackarch-malware

П .

П: malwaredetect, peepdf, yara

### 3.2.1.26 blackarch-misc

П .

П: oh-my-zsh-git, winexe, stompy



### 3.2.1.27 **blackarch-mobile**

Π .

Π: android-sdk-platform-tools, android-udev-rules

### 3.2.1.28 **blackarch-networking**

Π IP networking.

Π: Anything pretty much

### 3.2.1.29 **blackarch-nfc**

Π nfc (near-field communications).

Π: nfcutils

### 3.2.1.30 **blackarch-packer**

Π packers.

*packers* .

Π: packerid

### 3.2.1.31 **blackarch-proxy**

Π proxy, traffic internet.

Π: burpsuite, ratproxy, sslnuke

### 3.2.1.32 **blackarch-recon**

Π .

Π: canri, dnsrecon, netmask

### 3.2.1.33 **blackarch-reversing**

A decompiler, disassembler .

Π: capstone, radare2, zerowine

### 3.2.1.34 **blackarch-scanner**

Π .

Π: scanssh, tiger, zmap



### 3.2.1.35 blackarch-sniffer

П .

: hexinject, pytactile, xspy

### 3.2.1.36 blackarch-social

П .

П: jigsaw, websploit

### 3.2.1.37 blackarch-spoof

П .

П: arpoison, lans, netcommander

### 3.2.1.38 blackarch-threat-model

П .

П: magictree

### 3.2.1.39 blackarch-tunnel

П tunnel.

П: ctunnel, iodine, ptunnel

### 3.2.1.40 blackarch-unpacker

П .

П: js-beautify

### 3.2.1.41 blackarch-voip

П VoIP.

П: iaxflood, rtp-flood, teardown

### 3.2.1.42 blackarch-webapp

П .

П: metoscan, whatweb, zaproxy



### 3.2.1.43 blackarch-windows

Π Windows wine.

Π: 3proxy-win32, pwdump, winexe

### 3.2.1.44 blackarch-wireless

Π .

Π: airpwn, mdk3, wiffy

## 3.3 Repository structure

M BlackArch git repo : <https://github.com/BlackArch/blackarch>. Υ repos : <https://github.com/BlackArch>.

M git repo, 3 :

- docs - Documentation.
- packages - PKGBUILD files.
- scripts - Useful little scripts.

### 3.3.1 Scripts

E scripts scripts/ :

- baaur - Σ AUR.
- babuild - X
- bachroot - Δ chroot .
- baclean - K .pkg.tar.xz repo.
- baconflict - Σ scripts/conflicts.
- bad-files - E .
- balock - A repo.
- banotify - E IRC push .
- barelease - E repo package.
- baright - T BlackArch copyright.
- basign - Υ .
- basign-key - Υ .



- blackman - K pacman, git (not to be confused with nrz's Blackman).
- check-groups - .
- checkpkgs - .
- conflicts -
- dbmod - T .
- depth-list - Δ .
- deptree - Δ , BlackArch.
- get-blackarch-deps - Λ BlackArch .
- get-official - Π .
- list-loose-packages - Λ .
- list-needed - Λ .
- list-removed - Λ git.
- list-tools - Λ .
- outdated - git.
- pkgmod - T Build
- pkgrel - A pkgrel .
- prep - K PKGBUILD .
- sitesync - Σ repo .
- size-hunt - K .
- source-backup - A .

## 3.4 Contributing to repository

A project BlackArch. Δ pull requests , .  
Γ , .  
. E .

### 3.4.1 Required tutorials

Π :

- [Arch Packaging Standards](#)
- [Creating Packages](#)
- [PKGBUILD](#)
- [Makepkg](#)



### 3.4.2 Steps for contributing

Γ :

1. Fork the repository from <https://github.com/BlackArch/blackarch>
2. Hack the necessary files, (e.g. PKGBUILD, .patch files, etc).
3. Commit your changes.
4. Push your changes.
5. Ask us to merge in your changes, preferably through a pull request.

### 3.4.3 Example

T BlackArch. X `yaourt` ( `pacaur`, ) `PKGBUILD nfsshell AUR` .

#### 3.4.3.1 Fetch PKGBUILD

Φ `PKGBUILD yaourt pacaur`:

```
user@blackarchlinux $ yaourt -G nfsshell
==> Download nfsshell sources
x LICENSE
x PKGBUILD
x gcc.patch
user@blackarchlinux $ cd nfsshell/
```

#### 3.4.3.2 Clean up PKGBUILD

K `PKGBUILD` :

```
user@blackarchlinux nfsshell $ ./blarckarch/scripts/prep PKGBUILD
cleaning 'PKGBUILD'...
expanding tabs...
removing vim modeline...
removing id comment...
removing contributor and maintainer comments...
squeezing extra blank lines...
removing '|| return'...
removing leading blank line...
removing $pkgname...
removing trailing whitespace...
```

#### 3.4.3.3 Adjust PKGBUILD

Π `PKGBUILD` :

```
user@blackarchlinux nfsshell $ vi PKGBUILD
```





### 3.4.3.4 Build the package

Build the package:

```
==> Making package: nfsshell 19980519-1 (Mon Dec  2 17:23:51 CET 2013)
==> Checking runtime dependencies...
==> Checking buildtime dependencies...
==> Retrieving sources...
-> Downloading nfsshell.tar.gz...
% Total      % Received % Xferd  Average Speed   Time    Time     Time
CurrentDload  Upload    Total      Spent    Left  Speed100 29213  100 29213   0
0 48150      0 --:--:-- --:--:-- --:--:-- 48206
-> Found gcc.patch
-> Found LICENSE
...
<lots of build process and compiler output here>
...
==> Leaving fakeroot environment.
==> Finished making: nfsshell 19980519-1 (Mon Dec  2 17:23:53 CET 2013)
```

### 3.4.3.5 Install and test the package

Install and test the package:

```
user@blackarchlinux nfsshell $ pacman -U nfsshell-19980519-1-x86_64.pkg.tar.xz
user@blackarchlinux nfsshell $ nfsshell # test it
```

### 3.4.3.6 Add, commit and push package

Add, commit and push the package

```
user@blackarchlinux ~/blackarchlinux/packages $ mv ~/nfsshell .
user@blackarchlinux ~/blackarchlinux/packages $ git commit -am nfsshell && git push
```

### 3.4.3.7 Create a pull request

Create a pull request on [github.com](https://github.com)

```
firefox https://github.com/<contributor>/blackarchlinux
```

### 3.4.3.8 Adding a remote for upstream

A smart thing to do if you're working upstream and on a fork is to pull your own fork and add the main ba repo as a remote

```
user@blackarchlinux ~/blackarchlinux $ git remote -v
origin <the url of your fork> (fetch)
origin <the url of your fork> (push)
user@blackarchlinux ~/blackarchlinux $ git remote add upstream https://github.com/blackarch/blackarch
user@blackarchlinux ~/blackarchlinux $ git remote -v
origin <the url of your fork> (fetch)
origin <the url of your fork> (push)
upstream https://github.com/blackarch/blackarch (fetch)
upstream https://github.com/blackarch/blackarch (push)
```



By default, git should push straight to origin, but make sure your git config is configured correctly. This won't be an issue unless you have commit rights as you won't be able to push upstream without them.

If you do have the ability to commit, you might have more success using `git@github.com:blackarch/blackarch.git` but it's up to you.

### 3.4.4 Requests

1. Don't add **Maintainer** or **Contributor** comments to *PKGBUILD* files. Add maintainer and contributor names to the AUTHORS section of BlackArch guide.
2. For the sake of consistency, please follow the general style of the other *PKGBUILD* files in the repo and use two-space indentation.

### 3.4.5 General tips

`namcap` can check packages for errors.

## Chapter 4

# Tools Guide

Coming soon...

### 4.1 Coming Soon

Coming soon...