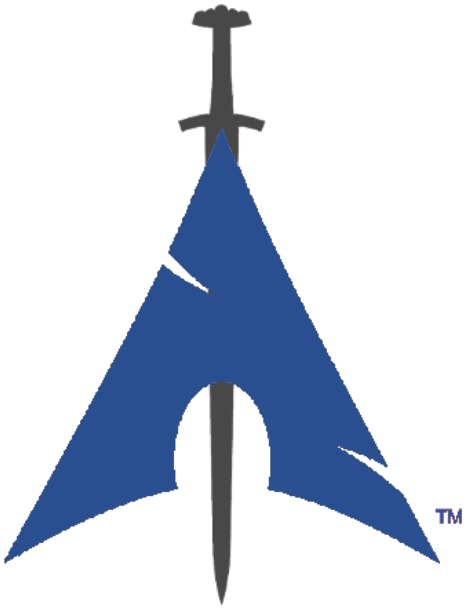

The BlackArch Linux Guide

https://www.blackarch.org/

Contents

Chapter 1

Introducere

1.1 Overview

Manualul pentru BlackArch Linux este impartit in cateva parti:

- Introducere-Ofera o previzualizare, o introducere, niste informatii in plus
- Manualul utilizatorului-Totul ce un utilizator trebuie sa stie pentru a folosi BlackArch eficient
- Manualul Dezvoltatorului-Cum sa contribui in proiect
- Manualul pentru ustensile-Explicatii clare si precise despre folosirea lor (WIP)

1.2 Ce este BlackArch Linux?

BlackArch este o distributie Linux completa pentru securitate cibernetica

Este derivata de la ArchLinux iar utilizatorii pot instala componnentele BlackArch separat

Intregul sistem este distribuit ca Arch Linux unofficial user repository deci, poti instala BlackArch intr-o instalatie ArchLinux obisnuita.Pachetele pot fi instalate separat sau pe categorii

Este continuu actualizat continand peste 2600 unelte. Toate uneltele sunt testate riguros si adaugate intr-o baza de date pentru a fi folosite la capacitate maxima

1.3 Istoria BlackArch Linux

Incurand...

1.4 Platforme Suportate

Incurand...

1.5 Ajuta-ne

Poti contacta echipa BlackArch print urmatoarele metode:

Website: https://www.blackarch.org/

Mail: team@blackarch.org

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

Twitter: https://twitter.com/blackarchlinux

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

Discord: https://discord.com/invite/xMHt8dW

Chapter 2

Manualul Utilizatorului

2.1 Instalare

Urmatoarea sectiune iti va arata cum sa instalezi BlackArch repository si cum sa instalezi pachete. BlackArch suporta ambele variante, instalarea din repository folosind pachete binare cat si compiland si instaland din sursa.

BlackArch este compatibil cu normala instalare Arch.Este exact ca un neoficial 'pachet'. Daca vrei un ISO, mai jos Live ISO section.

2.1.1 Instalarea sa pe ArchLinux

Ruleaza strap.sh ca root urmand urmatoarele instructiuni. Urmatorul exemplu

```
curl -O https://blackarch.org/strap.sh
sha1sum strap.sh # should match: d062038042c5f141755ea39dbd615e6ff9e23121
sudo chmod +x strap.sh
sudo ./strap.sh
```

Acum istaleaza o copie noua a pachetului master listeaza si sincronizeaza pachetele:

```
sudo pacman -Syyu
```

2.1.2 Instalarea pachetelor

Acum poti instala uneltele din blackarch repository.

1. Pentru a lista uneltele valabile, ruleaza

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

2. Petru a instala toate uneltele, ruleaza

   ```
   pacman -S blackarch
   ```

3. Pentru a instala o anumita categorie, ruleaza

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

4. Pentru a instala categoriile BlackArch, ruleaza

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

2.1.3 Instalarea pachetelor din sursa

Ca parte din o, poti construi pachete BlackArch din sursa. Poti gasi PKGBUILDs in github. To creeaza intregul repo, poti folosi Blackman tool.

- Prima data, trebuie sa instalezi Blackman. Daca repo-ul pentru pachetul BlackArch este configurat, poti instala Blackman:

```
pacman -S blackman
```

- Poti instala si configura Blackman din sursa:

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

- Sau poti instala BlackArch din AUR:

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

2.1.4 Folosirea simpla a lui Blackman

BlackMan e foarte usor de folosit, desi e diferent de ce te-ai fi asteptat, e diferit de pacman.

- Downloadeaza, compileaza si instaleaza pachete:

```
sudo blackman -i package
```

- Descarca, compileaza si instaleaza intreaga categorie:

```
sudo blackman -g group
```

- Descarca, compileaza si instaleaza toate uneltele BlackArch:

```
sudo blackman -a
```

- Pentru a lista categoriile BlackArch:

```
blackman -l
```

- Pentru a lista categoriile uneltelor:

```
blackman -p category
```

2.1.5 Instalarea din live-, netinstall- ISO sau ArchLinux

Poti instala BlackArch Linux din unul dintre live- neinstall-.ISO.
See https://www.blackarch.org/download.html#iso. Urmatorii pasi sunt necesari dupa boot up-ul ISO-ului

- Instalarea instalarului-blackarch:

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

- Run

```
sudo blackarch-install
```

Chapter 3

Manualul creatorului

3.1 Sistemul de construire al Arch si pachete separate

PKGBUILD sunt fisiere. Fiecare ii comunica makepkg(1) cum sa creeze un pachet. Fisierele PKGBUILD sunt scrise in Bash.

Pentru mai multe informatii, citeste (sau rasfoieste) urmatoarele:

- Arch Wiki: Crearea pachetelor
- Arch Wiki: makepkg
- Arch Wiki: PKGBUILD
- Arch Wiki: inpacetarea standard a Arch

3.2 PKGBUILD pentru standardele BlackArch

Pentru o mai buna intelegere, PKGBUILDs sunt similare cu cele AUR, cu mici diferente enumerate mai jos. Fiecare pachet trebuie sa apartina BlackArch catusi de putin.

3.2.1 Grupuri

Pentru a instala o specifica ramura de pachete rapid si usor,pachetele au fost separate in grupuri. Acestea se pot instala prin simplul 'pacman -S <group name>' pentru a instala multiple pachete

3.2.1.1 blackarch

Grupul BlackArch este baza tuturor grupurilor is este locul in care pachetele thebuie sa vie stocate. Acest lucru da voie utilizatorilor sa instaleze pachete usor Ce ar trebuie sa contina: TOTUL.

3.2.1.2 blackarch-anti-forensic

Pachetele ce sunt necesare pentru forensic, incluzand encryption, steganography, si orice ar trebuie sa modifice fisiere. Aceste unelte ar trebui sa functioneze in cazul in care doriti sa ascundeti informatii.

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

3.2.1.3 blackarch-automation

Pachete ce ar trebui folosite pentru workflow automation

Exemple: blueranger, tiger, wiffy

3.2.1.4 blackarch-backdoor

Pachete ce exploateaza sau folosesc backdoors sunt deja in sisteme vulnerabile.

Exemple: backdoor-factory, rrs, weevely

3.2.1.5 blackarch-binary

Pachete ce opereaza pe fisiere binare.

Exemple: binwally, packerid

3.2.1.6 blackarch-bluetooth

Pachete ce ataca orice are legatura cu Bluetooth standard (802.15.1).

Exemple: ubertooth, tbear, redfang

3.2.1.7 blackarch-code-audit

Pachete ce scaneaza o sursa existenta de cod in cautare de vulnerabilitati.

Exemple: flawfinder, pscan

3.2.1.8 blackarch-cracker

Pachete folosite pentru cracking cryptographic functions, ie hashes.

Exemple: hashcat, john, crunch

3.2.1.9 blackarch-crypto

Pachete ce folosesc cryptography,cu exeptia decriptarii.

Exemple: ciphertest, xortool, sbd

3.2.1.10 blackarch-database

Packages that involve database exploitations on any level.

Examples: metacoretex, blindsql

3.2.1.11 blackarch-debugger

Pachete ce dau voie utilizatorului sa vizioneza ce "face' un program intr-un anumit timp.

Exemple: radare2, shellnoob

3.2.1.12 blackarch-decompiler

Pachete ce incearca sa face reverse la un program pentru ai vedea codul sursa.

Examples: flasm, jd-gui

3.2.1.13 blackarch-defensive

Pachete ce sunt folosite pentru a apara utilizatorul de virusi si atacuri.

Exemple: arpon, chkrootkit, sniffjoke

3.2.1.14 blackarch-disassembler

Este similar cu blackarch-decompiler, si vor fi probabil multe programe ce vor ajunge in mai multe catregorii, desi aceste pachete produc assembly output

Exemple: inguma, radare2

3.2.1.15 blackarch-dos

Pachete folosite pentru D0S (Denial of Service).

Exemple: 42zip, nkiller2

3.2.1.16 blackarch-drone

Pachete ce sunt folosite pentru a folosi drone

Exemple: meshdeck, skyjack

3.2.1.17 blackarch-exploitation

Pachete ce se folosesc de vulnerabilitatiile altor programe sau servicii

Exemple: armitage, metasploit, zarp

3.2.1.18 blackarch-fingerprint

Pachete ce exploateaza echipament fingerprint biometric.

Exemple: dns-map, p0f, httprint

3.2.1.19 blackarch-firmware

Pachete ce expluateaza vulnerabilitati in firmware:

Exemple: None yet, amend asap.

3.2.1.20 blackarch-forensic

Pachhete ce sunt folosite pentru a descoperi data pe disk-uri si memorie interna.

Exemple: aesfix, nfex, wyd

3.2.1.21 blackarch-fuzzer

Pachete ce sunt folosite pentru fuzz, ie 'aruncand' valori "la nimereala" in campuri de input pentru a vedea ce se intampla.

Exemple: msf, mdk3, wfuzz

3.2.1.22 blackarch-hardware

Pachete ce exploateaza sau folosesc orice are legatura cu hardware.

Exemple: arduino, smali

3.2.1.23 blackarch-honeypot

Pachete ce au legatura cu "honeypots", ie, programe ce au tendinta sa para vulnerabile pentru a fii exploatate.

Exemple: artillery, bluepot, wifi-honey

3.2.1.24 blackarch-keylogger

Pachetele ce tin cont de functionalitatea sistemului tau.

Exemple: None yet, amend asap.

3.2.1.25 blackarch-malware

Pachete ce tin cont de malware.

Exemple: malwaredetect, peepdf, yara

3.2.1.26 blackarch-misc

Pachte ce nu se incadreaza in vreo categorie.

Exemple: oh-my-zsh-git, winexe, stompy

3.2.1.27 blackarch-mobile

Pachete ce manipuleaza platforme mobile.

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

3.2.1.28 blackarch-networking

Pachetel ce au legatura cu ip-ul.

Exemple: Cam toate

3.2.1.29 blackarch-nfc

Pachete ce se folosesc ce nfc(near-field communications).

Exemple: nfcutils

3.2.1.30 blackarch-packer

Pachete ce se folesesc de alte pachete.

packers sunt programe ce contin malware.

Exemple: packerid

3.2.1.31 blackarch-proxy

Pachete ce sunt considerate ca proxy, ie redirectionand date /trafic print internet.

Exemple: burpsuite, ratproxy, sslnuke

3.2.1.32 blackarch-recon

Pachete ce cauta vulnerabilitati. Mai mult o adunare decat un grup.

Exemple: canri, dnsrecon, netmask

3.2.1.33 blackarch-reversing

O adunare pentru dezasamblare

Exemple: capstone, radare2, zerowine

3.2.1.34 blackarch-scanner

Pachete ce cauta vulnerabilitati in sisteme specifice .

Exemple: scanssh, tiger, zmap

3.2.1.35 blackarch-sniffer

Pachete ce se concentreaza pe analizat traficul de date.

Exemple: hexinject, pytactle, xspy

3.2.1.36 blackarch-social

Pachete pentru social networking sites.

Exemple: jigsaw, websploit

3.2.1.37 blackarch-spoof

Pachete ce incearca sa faca spoof atacatorul, unde atacatorul devine o victima

Exemple: arpoison, lans, netcommander

3.2.1.38 blackarch-threat-model

Pachete ce se folosesc pentru reporting/recording o amenintare.

Exemple: magictree

3.2.1.39 blackarch-tunnel

Pachete ce sunt folosite pentru a directiona network traffic la un anumit network.

Exemple : ctunnel, iodine, ptunnel

3.2.1.40 blackarch-unpacker

Pachete ce sunt folosite pentru a extracta pre-facut malware din un executabil.

Exemple: js-beautify

3.2.1.41 blackarch-voip

Programe ce opereaza pe voip programs si protocoale.

Exemple: iaxflood, rtp-flood, teardown

3.2.1.42 blackarch-webapp

Programe ce opereaza pe internet-facing applications.

Exemple: metoscan, whatweb, zaproxy

3.2.1.43 blackarch-windows

Aceasta categorie este alcatuita de programe ce ruleaza nativ pe windows, iar noi folosim wine pentru a le folosi pe BlackArch.

Exemple: 3proxy-win32, pwdump, winexe

3.2.1.44 blackarch-wireless

Programe ce opereaza pe wireless networks la orice nivel.

Exemple: airpwn, mdk3, wiffy

3.3 Repository structure

Poti gasi intregul BlackArch repo aici: https://github.com/BlackArch/blackarch. Avem is cateva repos secundare aici: https://github.com/BlackArch.

In repo-ul principal de pe git, exista trei categorii imprtante:

- docs - Documentatie.
- packages - fisiere PKGBUILD.
- scripts - Scripturi folositoare.

3.3.1 Scripts

O referinta pentru scripturi se gaseste aici `scripts/` directory:

- baaur-Incurand, acesta va uploada fisiere pe AUR.
- babuild-Va construi un pachet.
- bachroot-Va alege un chroot pentru folosire.
- baclean-Va curata pachete vechi ca.pkg.tar.xz din repo.
- baconflict-Incurand va inlocui `scripts/conflicts`.
- bad-files-Va gasi fisiere corupte.
- balock-Va detine sau dona pachete.
- banotify-Va notifica IRC despre package pushes.