

CTF ENVIROMENT 101

How to Build a Decent CTF Enviroment

DEV v1.3-RC1

 Ernesto Martínez García

me@ecomaikgolf.com

ecomaikgolf#3519

 LosFuzzys Beginner Training

losfuzzys.net

discord.gg/RrUKAvGB2N

 7th of June 2023

 SLIDES



ls.ecomaikgolf.com/slides/distrobox.pdf

INTRODUCTION



TOOLBOX CHOICES

PRECONFIGURED

Advantages:

All the tools just work

Quick setup

Disadvantages

A bit of bloat



Kali Linux, BlackArch, ParrotOS, etc.

SELF-MADE

Advantages:

Only tools that you need

Customization

Disadvantages:

Tool Installation Errors



Arch Linux, Ubuntu, etc... + Tools

ENVIROMENT CHOICES

HOST MACHINE

Advantages:

- Resource Sharing
- Speed
- No folder sharing

Disadvantages:

- Esoteric Software
- System Breakage

Good for:

- pwn/rev players
- crypto players

VIRTUALIZED

Advantages:

- Secure
- Separate CTF/Work
- Snapshots

Disadvantages:

- Performance
- Resource Sharing

Good for:

- pwn⁺/rev⁺ players
- malware

CONTAINERIZED

Advantages:

- Resource Sharing
- Separate CTF/Work
- Snapshots
- Speed

Disadvantages:

- idk tell me

Good for:

- misc/web players
- stego, misc, etc.

CTF READY DISTRIBUTIONS

KALI LINUX



Debian Based

apt

Battle Tested

BLACKARCH



ArchLinux Based

pacman

AUR Available

PARROT-OS



Debian Based

apt

HTB pwnbox

RUNNING METHODS

Host System ✗

Persistent USB

Live USB




Dual Boot ✗

Virtual Machine ✓

Vagrant ✓

CTF READY CONTAINERS

DOCKERHUB CONTAINERS

	kalilinux/kali-last-release SPONSORED OSS ☆	↓ Pulls 50K+
	By Kali • Updated 2 days ago Image built from the last snapshot of the official release (updated quarterly)	
	Image	
	blackarchlinux/blackarch ☆	↓ Pulls 10K+
	By blackarchlinux • Updated 20 hours ago BlackArch Linux official docker images.	
	Image	
	parrotsec/security ☆	↓ Pulls 500K+
	By parrotsec • Updated a month ago Official Parrot Security image pre-loaded with pentest tools	
	Image	

But having to work with containers can be a bit inconvenient.

DISTROBOX



DISTROBOX

Wraps docker **or** podman for maximum convenience.

FEATURES

GUI Applications

\$HOME Sharing

.desktop generation

Automatic Upgrades

Emphemeral Containers



distrobox

REQUIREMENTS

Minimum docker version 2.1.0

Minimum podman version 18.06.1

(Optional) Podman or Docker configured in rootless mode

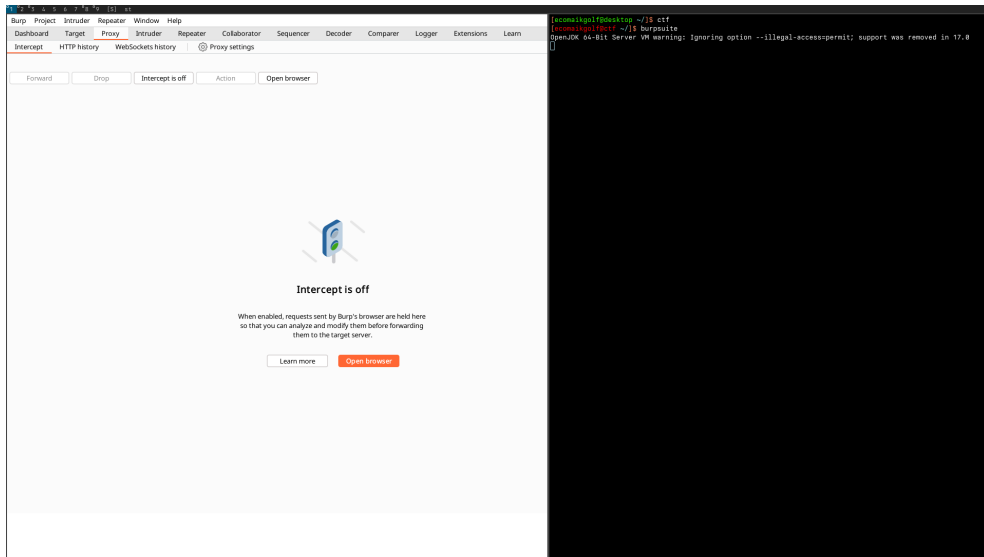
USE CASES



INSTALLING BURPSUITE FROM BLACKARCH

```
[ecomaikgolf@desktop ~/]$ distrobox enter ctf
[ecomaikgolf@ctf /home/ecomaikgolf/]$ cd
[ecomaikgolf@ctf ~/]$ yay burpsuite
5 aur/burpsuite-pro-earlyadopter 2023.4.2-1 (+1 0.43)
  An integrated platform for performing security testing of web applications (professional edition) (early adopter)
4 aur/burpsuite-cnpatch 1.0.1-1 (+1 0.00)
  Chinese patch for burpsuite community version
3 aur/burpsuite-pro 2023.4.2-1 (+8 0.05)
  An integrated platform for performing security testing of web applications (professional edition)
2 aur/burpsuite 2023.3.5-1 (+110 1.17)
  An integrated platform for performing security testing of web applications (free edition)
1 blackarch/burpsuite 1:2023.2.3-1 (550.7 MiB 560.2 MiB) [blackarch blackarch-webapp blackarch-proxy blackarch-scanner blackarch-fuzzer]
  An integrated platform for attacking web applications (community edition) + SHELLING plugin.
==> Packages to install (eg: 1 2 3, 1-3 or ^4)
==> 
```

INSTALLING BURPSUITE FROM BLACKARCH



The image shows a screenshot of the Burp Suite application interface on the left and a terminal window on the right. The Burp Suite interface displays the 'Intercept' tab, where the 'Intercept is off' button is highlighted. Below this, a message states: 'Intercept is off. When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.' There are 'Learn more' and 'Open browser' buttons. The terminal window on the right shows the following commands and output:

```
[ecomaigolf@desktop ~]$ cd /
[ecomaigolf@desktop ~]$ cd ctf
[ecomaigolf@ctf ~]$ burpsuite
OpenJDK 64-Bit Server VM warning: Ignoring option --illegal-access=permit; support was removed in 17.0
```

WEIRD CTF SOFTWARE NOT SHIPPED IN YOUR DISTRO

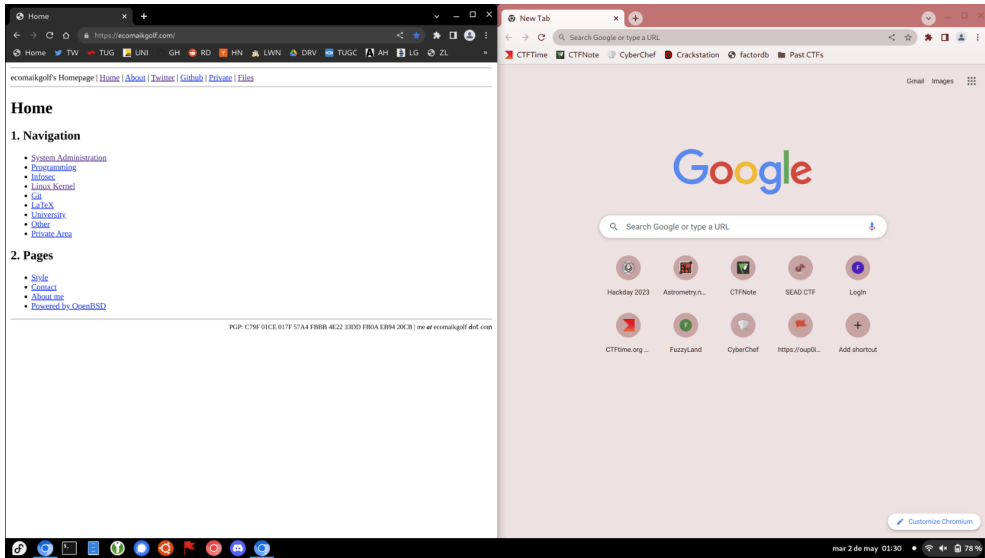
```
22 blackarch/openstego 0.8.4-1 (181.1 KiB 230.5 KiB) [blackarch blackarch-crypto blackarch-stego]
    A tool implemented in Java for generic steganography, with support for password-based encryption of the data.
21 blackarch/matroshka 58.2f820a4-2 (572.6 KiB 1.2 MiB) [blackarch blackarch-stego]
    Python steganography tool to hide images or text in images.
20 blackarch/zsteg v0.2.13.r1.gcd2588-1 (32.8 KiB 99.4 KiB) [blackarch blackarch-stego blackarch-anti-forensic]
    Detect stegano-hidden data in PNG and BMP.
19 blackarch/pngcheck 3.0.3-1 (57.8 KiB 160.4 KiB) [blackarch blackarch-stego blackarch-defensive blackarch-forensic]
    Verifies the integrity of PNG, JNG and MNG files by checking the CRCs and decompressing the image data.
18 blackarch/python-steganography 0.1.1-7 (8.4 KiB 18.8 KiB)
    Digital image steganography of encrypted text.
17 blackarch/python-stegoveritas-binwalk 2.1.2-6 (160.0 KiB 814.9 KiB)
    Binwalk release specifically for stegoveritas.
16 blackarch/python-stegoveritas-pfp 0.2.3-5 (121.2 KiB 726.4 KiB)
    An interpreter for B1B template scripts.
15 blackarch/python-stegoveritas-py010parser 0.1.10-4 (174.8 KiB 1.2 MiB)
    B1B template parser in Python.
14 blackarch/python2-steganography 0.1.1-7 (7.8 KiB 21.5 KiB)
    Digital image steganography of encrypted text.
13 blackarch/stegsolve 1.3-1 (57.8 KiB 305.0 KiB) [blackarch blackarch-stego]
    Steganography Solver.
12 blackarch/silenteye 21.e53a7ff-1 (778.6 KiB 1.2 MiB) [blackarch blackarch-stego]
    A cross-platform application design for an easy use of steganography.
11 blackarch/outguess 0.2-1 (81.1 KiB 197.0 KiB) [blackarch blackarch-crypto blackarch-misc]
    A universal steganographic tool.
10 blackarch/openpuff 4.01-3 (4.3 MiB 12.5 MiB) [blackarch blackarch-stego blackarch-windows]
    Yet not another steganography SW.
9 blackarch/snow 28120618-2 (15.9 KiB 80.0 KiB) [blackarch blackarch-crypto blackarch-misc]
    Steganography program for concealing messages in text files.
8 blackarch/stegoveritas 1.9-2 (124.4 KiB 599.7 KiB) [blackarch blackarch-stego]
    Automatic image steganography analysis tool.
7 blackarch/stegcracker 2.1.0-1 (17.5 KiB 51.6 KiB) [blackarch blackarch-stego]
    Steganography brute-force utility to uncover hidden data inside files.
6 blackarch/stegdetect 19.ac1df7a-1 (374.3 KiB 2.1 MiB) [blackarch blackarch-stego blackarch-defensive blackarch-forensic]
    An automated tool for detecting steganographic content in images.
5 blackarch/stegolego 8.88354fe-3 (6.1 KiB 39.0 KiB) [blackarch blackarch-stego]
    Simple program for using steganography to hide data within BMP images.
4 blackarch/steghide 0.5.1-10 (162.0 KiB 493.2 KiB) [blackarch blackarch-stego blackarch-anti-forensic]
    Embeds a message in a file by replacing some of the least significant bits.
3 blackarch/stegosip 11.5cda0de-1 (40.6 KiB 76.1 KiB) [blackarch blackarch-tunnel blackarch-networking blackarch-stego]
    TCP tunnel over RTP/SIP.
2 blackarch/stegseek 104.ff077b9-1 (120.5 KiB 302.0 KiB) [blackarch blackarch-stego]
    Lightning fast steghide cracker.
1 blackarch/stepic 0.4-2 (14.0 KiB 47.7 KiB) [blackarch blackarch-stego]
    A python image steganography tool.
=> Packages to install (eg: 1 2 3, 1-3 or *4)
=> []
```

Manually installing/building any uncommon tool during a CTF → errors
BlackArch/Kali packagers take care of them

WEIRD CTF SOFTWARE NOT SHIPPED IN YOUR DISTRO

```
49 blackarch/sparta 21.b0a4514-1 (265.0 KiB 816.0 KiB) [blackarch blackarch-scanner blackarch-cracker blackarch-fingerprint blackarch-networking]
    Python GUI application which simplifies network infrastructure penetration testing by aiding the penetration tester in the scanning and enumeration phase.
48 blackarch/sublist3r 138.729d649-3 (622.2 KiB 1.8 MiB) [blackarch blackarch-recon blackarch-scanner]
    A Fast subdomains enumeration tool for penetration testers.
47 blackarch/automato 33.0561b59-6 (8.1 KiB 16.7 KiB) [blackarch blackarch-automation blackarch-recon]
    Should help with automating some of the user-focused enumeration tasks during an internal penetration test.
46 blackarch/whatsmyname 2024.c71765a-1 (276.9 KiB 655.6 KiB) [blackarch blackarch-social blackarch-recon]
    Tool to perform user and username enumeration on various websites.
45 blackarch/slackpirate 142.9788be6-3 (110.1 KiB 246.7 KiB) [blackarch blackarch-social blackarch-recon]
    Slack Enumeration and Extraction Tool - extract sensitive information from a Slack Workspace.
44 blackarch/reconnoitre 441.f62afba-3 (37.0 KiB 121.4 KiB) [blackarch blackarch-recon]
    A security tool for multithreaded information gathering and service enumeration.
43 blackarch/cisco-snmp-enumeration 10.ad06f57-3 (19.6 KiB 103.0 KiB) [blackarch blackarch-automation blackarch-networking blackarch-exploitation blackarch-cracker]
    Automated Cisco SNMP Enumeration, Brute Force, Configuration Download and Password Cracking.
42 blackarch/cloudflare-enum 10.412387f-2 (4.8 KiB 35.0 KiB) [blackarch blackarch-scanner]
    Cloudflare DNS Enumeration Tool for Pentesters.
41 blackarch/gomapeenum v1.1.0.r95.g23ecc54-1 (3.3 MiB 11.5 MiB) [blackarch blackarch-cracker blackarch-recon blackarch-social blackarch-windows]
    User enumeration and password bruteforce on Azure, ADFS, OWA, O365, Teams and gather emails on LinkedIn.
40 blackarch/graphinder 1.11.6-1 (18.9 KiB 45.0 KiB) [blackarch blackarch-recon blackarch-scanner blackarch-webapp]
    GraphQL endpoints finder using subdomain enumeration, scripts analysis and bruteforce.
39 blackarch/legion 59.3c08884-1 (898.8 KiB 2.1 MiB) [blackarch blackarch-recon blackarch-automation]
    Automatic Enumeration Tool based in Open Source tools.
38 blackarch/msmailprobe 1.c01c8bf-1 (1.7 MiB 5.3 MiB) [blackarch blackarch-scanner blackarch-recon]
    Office 365 and Exchange Enumeration tool.
37 blackarch/linux-smart-enumeration 272.d69e353-1 (10.2 MiB 11.2 MiB) [blackarch blackarch-scanner]
    Linux enumeration tool for pentesting and CTFs with verbosity levels.
36 blackarch/0trace 1.5-5 (3.5 KiB 3.8 KiB) [blackarch blackarch-scanner]
    A hop enumeration tool.
35 blackarch/linenum 75.c47f9b2-1 (15.1 KiB 54.8 KiB) [blackarch blackarch-scanner blackarch-recon]
    Scripted Local Linux Enumeration & Privilege Escalation Checks
34 blackarch/python-aenum 3.1.11-1 (219.9 KiB 1.5 MiB)
    Advanced Enumerations (compatible with Python's stdlib Enum), NamedTuples, and NamedConstants.
33 blackarch/deblaze 1:1.0608dc3-2 (232.8 KiB 2.4 MiB) [blackarch blackarch-scanner]
    Performs method enumeration and interrogation against flash remoting end points.
32 blackarch/o365spray 146.a794c97-2 (145.5 KiB 675.7 KiB) [blackarch blackarch-cracker blackarch-recon blackarch-windows]
    Username enumeration and password spraying tool aimed at Microsoft O365.
31 blackarch/ad-ldap-enum 88.60bc5bb-2 (12.8 KiB 42.9 KiB) [blackarch blackarch-recon]
    An LDAP based Active Directory user and group enumeration tool.
30 blackarch/certipy 4.3.0.r0.gdcb873e-2 (202.6 KiB 1.1 MiB) [blackarch blackarch-windows blackarch-exploitation]
    Active Directory Certificate Services enumeration and abuse.
29 blackarch/crosslinked 1:19.780ad1c-1 (21.6 KiB 54.1 KiB) [blackarch blackarch-social blackarch-recon]
    LinkedIn enumeration tool to extract valid employee names from an organization through search engine scraping.
28 blackarch/social-mapper 190.92be8da-2 (2.8 MiB 3.2 MiB) [blackarch blackarch-social blackarch-recon]
    A social media enumeration and correlation tool.
```

CTF ONLY BROWSER



INSTALLATION



INSTALLING Distrobox+Rootless Podman ON UBUNTU

Installation

```
1 sudo apt-get -y update
2 sudo apt-get -y install podman
3 sudo apt-get -y install slirp4netns fuse-overlayfs
4 sudo usermod --add-subuids 100000-165535 --add-subgids 100000-165535 <USERNAME>
5 sudo apt-get -y install distrobox # Ubuntu 22.10 (old) or 23.04
6 # Other distributions: https://github.com/89luca89/distrobox#installation
```

This will install Distrobox + Rootless Podman.

Containers will run in user mode (no sudo needed).

No daemon (client/server) needed as with Docker, just uses fork+exec.

How rootless Podman Work?

<https://opensource.com/article/19/2/how-does-rootless-podman-work>

Security in Rootless Containers

<https://liu.diva-portal.org/smash/get/diva2:1711128/FULLTEXT01.pdf>

USAGE



CREATING A CTF CONTAINER

Kali Linux CTF Container

```
1 distrobox create --image docker.io/kalilinux/kali-rolling:latest --name ctf
2 distrobox enter ctf
3 sudo apt update && apt -y install kali-linux-large
```

BlackArch CTF Container

```
1 distrobox create --image docker.io/blackarchlinux/blackarch:latest --name ctf
2 distrobox enter ctf
```

Update Container Software

```
1 distrobox update <name> # Update one
2 distrobox update -a     # Update all
```

Stop Container

```
1 distrobox stop <name>
```

Remove Container

```
1 distrobox rm <name>           # Remove Container
2 distrobox rm --rm-home <name> # + $HOME if != HOST
```

List Containers

```
1 distrobox list
```

TEMPLATES & EPHEMERAL CONTAINERS

Create a CTF Container Snapshot (Template)

```
1 # Commit the state of a container
2 podman container commit -p ctf ctf-template
3 # In case you want to share it:
4 podman save ctf-template:latest | gzip > ctf-template.tar.gz
```

Create a Ephemeral CTF Container

```
1 # In case you got it shared:
2 podman load < ctf-template.tar.gz
3 # Create an ephemeral/disposable box
4 distrobox ephemeral --image localhost/ctf-template:latest
```

Usecase: Installing all the base tools you think you need and creating a template. Then instantiating a container for each CTF, install weird tools, delete container, repeat.

TEMPLATES & EPHEMERAL CONTAINERS

```
>_ podman container commit -p ctf ctf-template
```

```
Getting image source signatures
Copying blob 9c15e5285032 skipped: already exists
Copying blob 2953aa7bf21a done
Copying config e0351dc674 done
Writing manifest to image destination
Storing signatures
e0351dc6746e6a8f0f646ee7a469bb0226bc77a89f43063627bcf36b6328d4d3
```

```
>_ podman save ctf-template:latest | gzip > ctf-template.tar.gz
```

```
<empty>
```

```
>_ podman load < ctf-template.tar.gz
```

```
Getting image source signatures
Copying blob 2953aa7bf21a skipped: already exists
Copying blob 9c15e5285032 skipped: already exists
Copying config e0351dc674 done
Writing manifest to image destination
Storing signatures
Loaded image: localhost/ctf-template:latest
```

TEMPLATES & EPHEMERAL CONTAINERS

```
>_ distrobox ephemeral -image localhost/ctf-template:latest
```

```
Creating 'distrobox-LVZlZbBCPY' using image localhost/ctf-template:latest [ OK ]
```

```
Distrobox 'distrobox-LVZlZbBCPY' successfully created.
```

```
To enter, run:
```

```
distrobox enter distrobox-LVZlZbBCPY
```

```
distrobox-LVZlZbBCPY
```

```
Container distrobox-LVZlZbBCPY is not running.
```

```
Starting container distrobox-LVZlZbBCPY
```

```
run this command to follow along:
```

```
podman logs -f distrobox-LVZlZbBCPY
```

```
Starting container... [ OK ]
```

```
Installing basic packages... [ OK ]
```

```
[...]
```

```
Setting up groups... [ OK ]
```

```
Setting up users... [ OK ]
```

```
Executing init hooks... [ OK ]
```

```
Container Setup Complete!
```

RUNNING OTHER ARCHITECTURES

Install Dependencies

```
1 sudo dnf install qemu qemu-user-static qemu-user-binfmt # Tested Fedora 38
2 sudo apt install qemu qemu-user-static binfmt-support # Untested
```

Create an arm64 Ubuntu Container

```
1 distrobox create -i docker.io/arm64v8/ubuntu -n ubuntu-arm64
```

```
[ecomaikgolf@desktop ~/]$ uname -m
x86_64
[ecomaikgolf@desktop ~/]$ distrobox enter ubuntu-arm64
[ecomaikgolf@ubuntu-arm64.desktop ~/]$ uname -m
aarch64
[ecomaikgolf@ubuntu-arm64.desktop ~/]$
```

INTEGRATION WITH DESKTOP ENVIROMENTS

Create a Container Shortcut

```
1 distrobox generate-entry ctf --icon /path/icon.png
2 distrobox generate-entry --all
```

Desktop Entry

```
1 [Desktop Entry]
2 Name=Ctf
3 GenericName=Terminal entering Ctf
4 Comment=Terminal entering Ctf
5 Category=Distrobox;System;Utility"
6 Exec=/usr/bin/distrobox enter ctf
7 ...
```

Create a Container's Application Shortcut

```
1 distrobox export --bin /usr/bin/burpsuite --export-path ~/.local/bin
2 distrobox export --app <app>
```


INTEGRATION WITH DESKTOP ENVIROMENTS

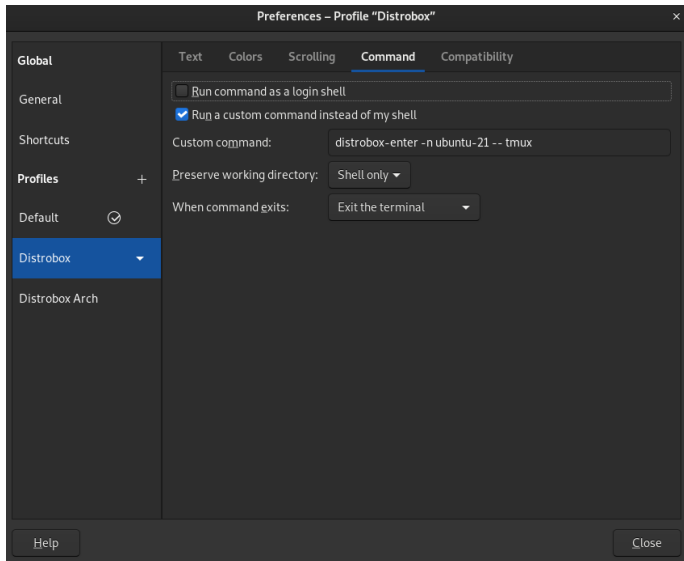
Gnome Terminal:

Multiple profiles with different background/shell/title settings.

Window Manager:

Running an entire window manager for CTFs

<https://cloudyday.tech.blog/2022/05/14/distrobox-is-awesome/>



CTF ENVIROMENT 101

How to Build a Decent CTF Enviroment

DEV v1.3-RC1

 Ernesto Martínez García

me@ecomaikgolf.com

ecomaikgolf#3519

 LosFuzzys Beginner Training

losfuzzys.net

discord.gg/RrUKAvGB2N

 7th of June 2023

 SLIDES



ls.ecomaikgolf.com/slides/distrobox.pdf