

CTF Setup & Tooling

Configuration of a CTF Environment for Windows & Linux

>_ DEV v1.3-RC1

 Ernesto Martínez García
me@ecomaikgolf.com
ecomaikgolf#3519

 Graz University of Technology

 LosFuzzys Beginner Trainings

 18th October 2023

 SLIDES



ls.ecomaikgolf.com/slides/ctfsetup.pdf

About

❓ Why CTF Setup & Tooling? What's all this about?

Solving Capture The Flag challenges usually require a specialized toolset

pwn

rev

crypto

stego

misc

pwntools

ghidra

sagemath

*-stego

~_(_)_/_-

Each of us have our own customized CTF setup  which we are used to

 Each of us think his setup is the best one

In this presentation we want to show how to get started  with the tools 

 In an interactive way (if people want)


 Keeping the slides as a reference for future (keep the link!)

Table of Contents


Introduction

- ▼ Different Options & Choices

Windows

- ▼ WSL2 and WSLG
- ▼ Ubuntu 22.04
-  **Checkpoint**

Linux (preferred)

-  **Checkpoint**
- ▼ Rootless Podman
- ▼ Distrobox
- ▼ BlackArch
- ▼ Tools

Introduction



Toolbox

? Which tools do I need for a CTF? How do I install them?

⚙️ PRECONFIGURED

Advantages:

- ⊕ Most of the tools bundled
- ⊕ Quick setup

Disadvantages

- ⊖ Unconvenient (no host distro)



🔧 SELF MADE

Advantages:

- ⊕ Manual installation of tools
- ⊕ Customization


Disadvantages:

- ⊖ Installation Errors



Running Mechanisms

❓ How do I run the tools? Where do I execute my environment?

 **HOST MACHINE**


Advantages:

- ⊕ Resource Sharing
- ⊕ Speed
- ⊕ No folder sharing

Disadvantages:

- ⊖ Esoteric Software
- ⊖ System Breakage

Runs directly on your computer

 **VIRTUALIZED**


Advantages:

- ⊕ Secure
- ⊕ Separate Environment
- ⊕ Snapshots

Disadvantages:

- ⊖ Performance
- ⊖ Resource Sharing

Your computer emulates another computer

 **CONTAINERIZED**

Advantages:

- ⊕ Resource Sharing
- ⊕ Separate Environment
- ⊕ Snapshots

Disadvantages:

- ⊖ Complexity

Your kernel emulates another userspace

This Presentation

? What are we going to learn in this presentation?

WSL2 + WSLG

Advantages:

- + Good Integration
- + Better than a VM
- + X11 GUI support

Disadvantages:

- Stability

CONTAINERIZED

Advantages:

- + Good Integration
- + Separate Environment
- + Resilience

Disadvantages:

- Complexity

PRECONFIGURED

Advantages:

- + Beginner Friendly
- + Easy to reinstall
- + No tinkering

Disadvantages:

- Simplicity

Windows



Enable Virtualization in BIOS/UEFI

- ❗ Very important step, required for running virtual machines
- 🔧 Go into the BIOS/UEFI and enable everything named as:
 - Intel(R) Virtualization Technology
 - Virtualization Technology
 - VT-x
 - VT-d (Directed I/O)
- 🌀 Confused? Ask a Fuzzy!
- ❓ Will this break my PC? No, and you (probably) will need it for your courses

Enable Virtualization in BIOS/UEFI

Phoenix TrustedCore(tm) Setup Utility		
Advanced		
Advanced Processor Configuration		Item Specific Help
CPU Mismatch Detection:	[Enabled]	When enabled, a VMM (Virtual Machine Monitor) can utilize the additional hardware capabilities provided by Vanderpool Technology. If this option is changed, a Power Off-On sequence will be applied on the next boot.
Core Multi-Processing:	[Enabled]	
Processor Power Management:	[Disabled]	
Intel(R) Virtualization Technology	[Enabled]	
Execute Disable Bit:	[Enabled]	
Adjacent Cache Line Prefetch:	[Disabled]	
Hardware Prefetch:	[Disabled]	
Direct Cache Access	[Disabled]	
Set Max Ext CPUID = 3	[Disabled]	

F1 Info ↑↓ Select Item -/+ Change Values F9 Setup Defaults
Esc Exit ← Select Menu Enter Select ▶ Sub-Menu F10 Save and Exit

Enable Virtualization in BIOS/UEFI



Enable Virtualization in BIOS/UEFI

The screenshot displays the ASUS UEFI BIOS Utility in Advanced Mode. The interface is dark-themed with a top navigation bar containing 'My Favorites', 'Main', 'Ai Tweaker', 'Advanced' (highlighted), 'Monitor', 'Boot', 'Tool', and 'Exit'. A status bar at the top shows the date '11/28/2017 Tuesday', time '13:48', and various utility shortcuts like 'English', 'MyFavorite(F3)', 'Qfan Control(F6)', 'EZ Tuning Wizard(F11)', 'Quick Note(F9)', and 'Hot Keys'. The main configuration area lists several settings, with 'Intel Virtualization Technology' highlighted in grey and its dropdown menu set to 'Enabled'. A red arrow points to this dropdown. Other settings include L3 Cache (6 MB), L4 Cache (Not Supported), Intel Adaptive Thermal Monitor (Enabled), Active Processor Cores (All), Limit CPUID Maximum (Disabled), Execute Disable Bit (Enabled), Hardware Prefetcher(L2 Cache) (Enabled), Adjacent Cache Line Prefetcher (Enabled), Boot performance mode (Max Non-Turbo Performance), and Dynamic Storage Accelerator (Disabled). A 'CPU Power Management Configuration' section is partially visible. On the right, a 'Hardware Monitor' panel shows CPU status (3500 MHz, 27°C), Memory status (1600 MHz, 1.500 V, 8192 MB), and Voltage status (+12V, +5V, +3.3V). An information icon at the bottom left provides details about Intel Virtualization Technology. The bottom of the screen shows 'Version 2.16.1240. Copyright (C) 2015 American Megatrends, Inc.' and 'Last Modified | EzMode(F7) | ->'. A large, semi-transparent watermark 'COMPUTER' is overlaid on the center of the screen.

ASUS UEFI BIOS Utility - Advanced Mode

11/28/2017 Tuesday 13:48 | English | MyFavorite(F3) | Qfan Control(F6) | EZ Tuning Wizard(F11) | Quick Note(F9) | Hot Keys

My Favorites Main Ai Tweaker **Advanced** Monitor Boot Tool Exit

L3 Cache 6 MB

L4 Cache Not Supported

Intel Adaptive Thermal Monitor Enabled

Active Processor Cores All

Limit CPUID Maximum Disabled

Execute Disable Bit Enabled

Intel Virtualization Technology Enabled

Hardware Prefetcher(L2 Cache) Enabled

Adjacent Cache Line Prefetcher Enabled

Boot performance mode Max Non-Turbo Performance

Dynamic Storage Accelerator Disabled

> CPU Power Management Configuration

Hardware Monitor

CPU

Frequency 3500 MHz Temperature 27°C

BCLK 100.0 MHz Vcore 1.024 V

Ratio 35x

Memory

Frequency 1600 MHz Voltage 1.500 V

Capacity 8192 MB

Voltage

+12V +5V
12.000 V 5.080 V

+3.3V
3.328 V

COMPUTER

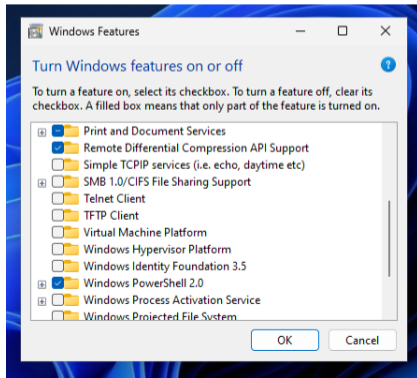
i Intel Virtualization Technology makes a single system appear as multiple independent systems to software. This allows for multiple, independent operating systems to be running simultaneously on a single system.

Version 2.16.1240. Copyright (C) 2015 American Megatrends, Inc. Last Modified | EzMode(F7) | ->

Enable Windows Virtualization

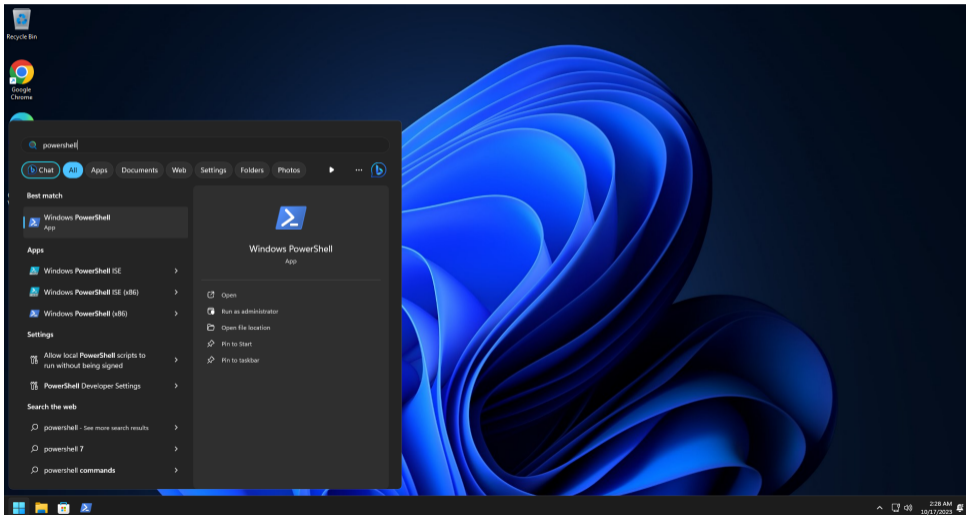
🔧 Open “Windows Features” and enable:

- Virtual Machine Platform
- Windows Hypervisor Platform
- Windows Subsystem for Linux



Install WSL2

>_ Open Poweshell



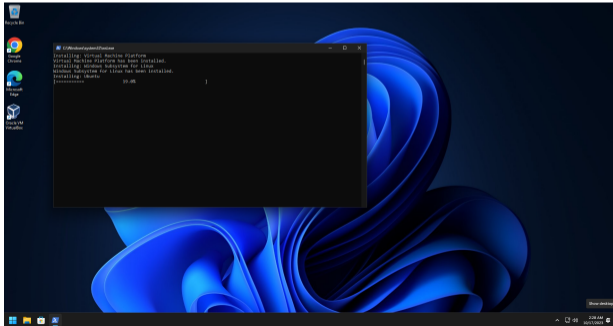
Install WSL2

🖨️ Introduce the following commands in powershell

🚀 Install Windows Subsystem for Linux

```
1 wsl --set-default-version 2
2 wsl --install
```

⚠️ Update the WSL2 Kernel (if requested) from
https://wslstorestorage.blob.core.windows.net/wslblob/wsl_update_x64.msi



Post Installation

🐧 After the installation, you should get dropped to a WSL2 shell

🔧 Now let's install the required minimum software

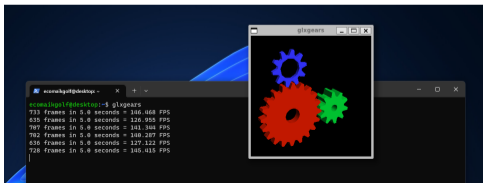
🚀 Install Required Software

- 1 `sudo apt update && sudo apt upgrade`
- 2 `sudo apt install xorg mesa-utils`

✅ Finally, let's run a sanity check

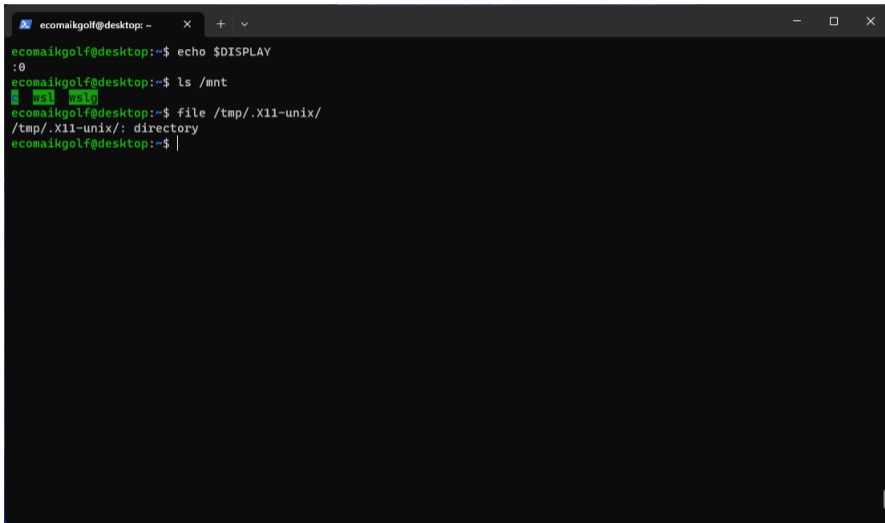
🚀 Sanity Check

- 1 `glxgears`



Additional Sanity Checks

- ❗ If it doesn't work, check that everything is correct:



```
ecomaikgolf@desktop: ~  
ecomaikgolf@desktop:~$ echo $DISPLAY  
:0  
ecomaikgolf@desktop:~$ ls /mnt  
ms1  ms1g  
ecomaikgolf@desktop:~$ file /tmp/.X11-unix/  
/tmp/.X11-unix/: directory  
ecomaikgolf@desktop:~$ |
```

Sneak Peek Final Setup

The screenshot displays a Windows desktop environment during the final setup of development tools. The taskbar at the bottom shows icons for File Explorer, Settings, and several application windows. The system tray in the bottom right corner indicates the time is 3:44 on 17/10/2023.

The primary window is **Ghidra**, showing the assembly and control flow graph for a function named `fcn.00002000`. The assembly code is as follows:

```
[0x00002000]
;--- section..init:
;--- segment.LOAD1:
fcn.00002000:
0x00002004 sub     rax, rbp, 8
0x00002008 mov     rax, qword __pmon_start__, 0x10f50
0x0000200f test    rax, rax
0x00002012 je     0x2016
```

The control flow graph shows a call to `rax` at address `0x00002014`, which then branches to `add rbp, 8` at `0x00002016`, followed by `ret` at `0x0000201a`.

Other visible windows include:

- SuperTux v0.6.3**: A game menu with options like "Start Game", "Add-ons", "Options", "Level Editor", "Credits", "Donate", and "Quit".
- About Ghidra**: Displays the Ghidra logo and version information: **Version 10.4**, **Build DEV**, **2023-Oct-01 1926 UTC**, **Java Version 21**. It also includes the Apache License text.
- About APK Studio**: Provides information about the APK Studio project, including its purpose and license.

The system tray at the bottom right shows the time as 3:44 and the date as 17/10/2023. The status bar at the bottom indicates "Running Tools: INACTIVE".

Sneak Peek Final Setup



<https://wallhaven.cc/w/135w7w>

Linux



Install Rootless Podman & Distrobox

 Introduce the following commands in bash:

Install Rootless Podman

```
1 sudo apt install podman slirp4netns fuse-overlayfs
2 sudo usermod --add-subuids 100000-165535 --add-subgids 100000-165535 <USERNAME>
```

 Podman is a container engine like docker

Install Distrobox

```
1 # Ubuntu 22.04
2 curl -s https://raw.githubusercontent.com/89luca89/distrobox/main/install | sudo sh
3 # Ubuntu 23.10
4 sudo apt install distrobox
```

 Distrobox is a wrapper over Podman/Docker to make interaction easier

Install a Linux Distribution

 Install a distribution which comes prepared for a CTF

BlackArch

```
1 distrobox create -i docker.io/blackarchlinux/blackarch:latest --name ctf
2 distrobox enter ctf
3 sudo pacman-key --init && sudo pacman-key --populate
```

 BlackArch is based on ArchLinux

Kali Linux

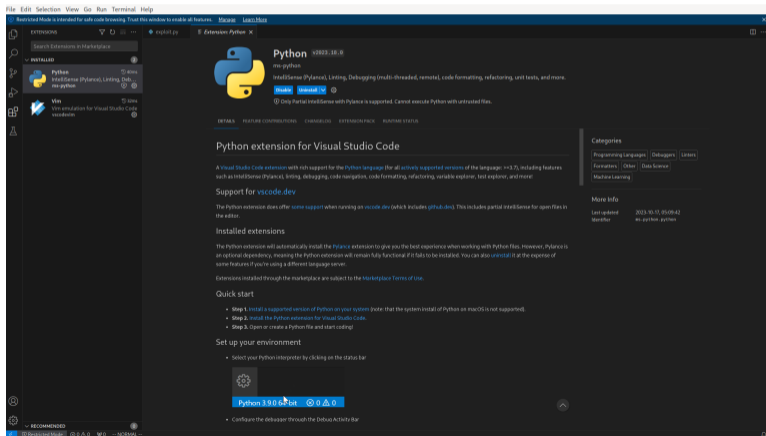
```
1 distrobox create -i docker.io/kalilinux/kali-rolling:latest --name ctf
2 distrobox enter ctf
```

 Kali Linux is based on Debian Testing

Install some Tools

🚀 Install an Editor

- 1 `sudo pacman -S vscode`
- 2 `code exploit.py`



The screenshot shows the Visual Studio Code interface with the Python extension page open in the marketplace. The left sidebar shows the 'EXTENSIONS' view with 'Python' and 'Jupyter' listed under 'INSTALLED'. The main panel displays the 'Python' extension details, including the Python logo, version '2022-10-0', and a 'Details' section with a 'Python extension for Visual Studio Code' heading. Below this, there are sections for 'Support for vscode.dev', 'Installed extensions', and 'Quick start' with a list of steps. At the bottom, there is a 'Set up your environment' section with a 'Python 3.9.0 64-bit' button and a 'Configure the debugger' link.

Install some Tools

Install pwntools

```
1 sudo pacman -S python-pwntools
```

>_ pwn version

```
[*] Pwntools v4.11.0
```

>_ python

```
Python 3.11.5 (main, Sep 2 2023, 14:16:33) [GCC 13.2.1 20230801] on linux
```

```
Type "help", "copyright", "credits" or "license" for more information.
```

```
>>> import pwn
```

```
>>> pwn.
```

```
Display all 321 possibilities? (y or n)
```

```
pwn.AppendedArgument(          pwn.atexit                pwn.default_style
pwn.BitPolynom(                pwn.attach(               pwn.defaultdict(
pwn.Buffer(                    pwn.b64d(                 pwn.depends_on_cycle(
pwn.BytesIO(                  pwn.b64e(                 pwn.dirents(
pwn.Core(                      pwn.base64                pwn.disasm(
pwn.Coredump(                 pwn.binary_ip(            pwn.division
pwn.Corefile(                 pwn.binascii              pwn.dynelf
pwn.DynELF(                   pwn.bits(                 pwn.elf
pwn.ELF(                      pwn.bits_str(             pwn.encode(
```


Install some Tools

Install binwalk

```
1 sudo pacman -S binwalk
```

>_ binwalk /bin/ls

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	ELF, 64-bit LSB shared object, AMD x86-64, version 1 (SYSV)
100461	0x1886D	Copyright string: "Copyright (C) 1996-2023 Free Software Foundation, Inc."
100616	0x18908	Copyright string: "copyright notice and this notice are preserved."
106527	0x1A01F	Unix path: /usr/share/locale
119072	0x1D120	Copyright string: "Copyright %s %d Free Software Foundation, Inc."

Install some Tools

Install yay package manager

```
1 pacman -S --needed git base-devel
2 git clone https://aur.archlinux.org/yay-bin.git
3 cd yay-bin
4 makepkg -si
```

>_ yay stego

```
6 blackarch/stepic 0.4-2 (14.0 KiB 47.7 KiB) [blackarch blackarch-stego]
  A python image steganography tool.
5 blackarch/stegseek 104.ff677b9-1 (120.5 KiB 302.0 KiB) [blackarch blackarch-stego]
  Lightning fast steghide cracker.
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/stegsolve 1.3-1 (57.8 KiB 305.0 KiB) [blackarch blackarch-stego]
  Steganography Solver.
2 blackarch/stegolego 8.85354f6-3 (6.1 KiB 39.0 KiB) [blackarch blackarch-stego]
  Simple program for using steganography to hide data within BMP images.
1 blackarch/stegosip 11.5cda6d6-1 (40.6 KiB 76.1 KiB) [blackarch blackarch-tunnel blackarch-networking
  blackarch-stego]
  TCP tunnel over RTP/SIP.
==> Packages to install (eg: 1 2 3, 1-3 or ^4)
==>
```

Reference

Create BlackArch CTF Container

```
1 distrobox create --image docker.io/blackarchlinux/blackarch:latest --name ctf
2 distrobox enter ctf
3 sudo pacman-key --init && sudo pacman-key --populate
```

Create Kali Linux CTF Container

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

Exit Container

```
1 exit # or
2 Ctrl+D # or
```

Stop Container

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

Remove Container

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

List Containers

```
1 distrobox list
```

CTF Setup & Tooling

Configuration of a CTF Environment for Windows & Linux

>_ PROD v1.3 ✓

 Ernesto Martínez García

me@ecomaikgolf.com

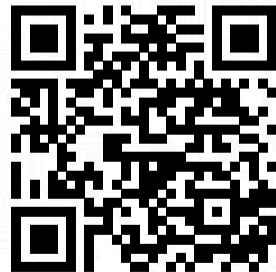
ecomaikgolf#3519

 Graz University of Technology

 LosFuzzys Beginner Trainings

 18th October 2023

 SLIDES



ls.ecomaikgolf.com/slides/ctfsetup.pdf