# CTF Setup & Tooling

## Configuration of a CTF Enviroment for Windows & Linux

>_ DEV v1.3-RC1


Ernesto Martínez García[1]

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` | ¯_(ツ)_/¯ |

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

# 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 enviroment?

| HOST MACHINE | VIRTUALIZED | CONTAINERIZED |
|---|---|---|
| **Advantages:**<br>+ Resource Sharing<br>+ Speed<br>+ No folder sharing | **Advantages:**<br>+ Secure<br>+ Separate Enviroment<br>+ Snapshots | **Advantages:**<br>+ Resource Sharing<br>+ Separate Enviroment<br>+ Snapshots |
| **Disadvantages:**<br>− Esoteric Software<br>− System Breakage | **Disadvantages:**<br>− Performance<br>− Resource Sharing | **Disadvantages:**<br>− Complexity |
| Runs directly on your computer | Your computer emulates another computer | 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 Enviroment
- Resilience

**Disadvantages:**

- Complexity

### PRECONFIGURED

**Advantages:**

- Beginner Friendly
- Easy to reinstall
- No tinkering

**Disadvantages:**

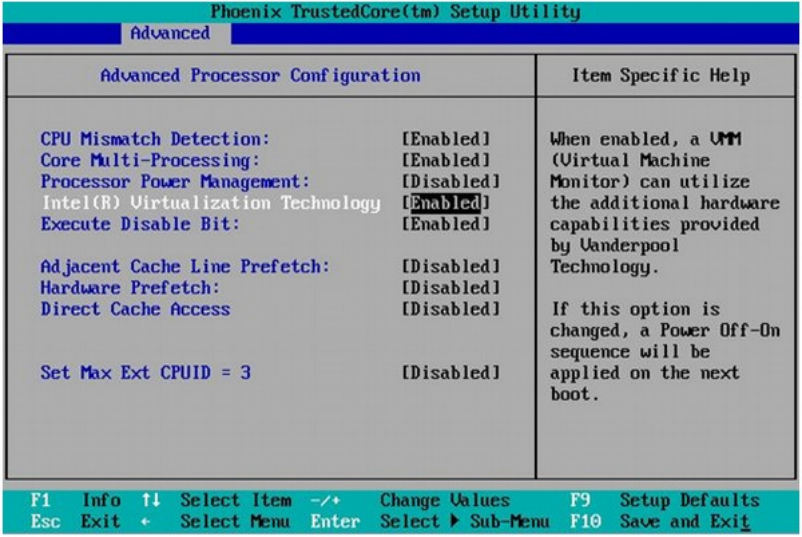
- Simplicity

Windows

# Enable Virtualization in BIOS/UEFI

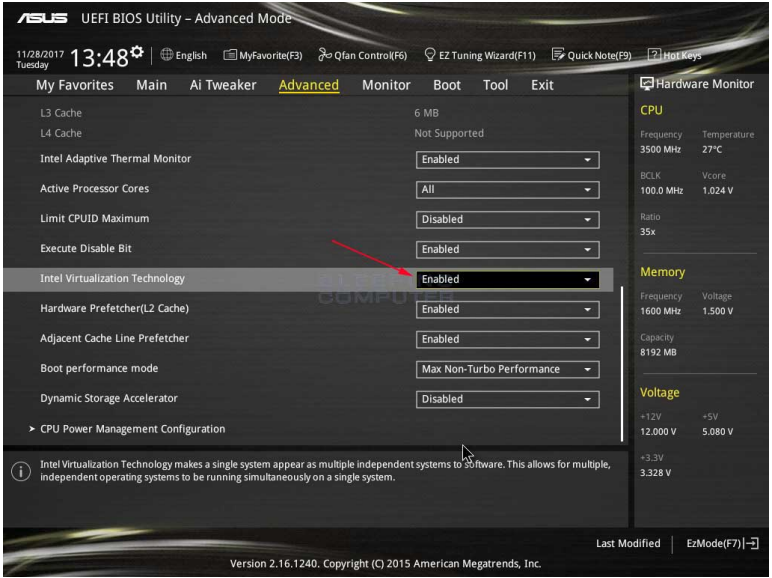
- Very important step, required for running virtual machines
- Go into the BIOS/UEFI and enable everything named as:
  - `Intel(R) Virtualization Technology`
  - `Virtualization Technology`
  - `VT-x`
  - `VT-d (Directed I/O)`
- Confused? Ask a Fuzzy!
- Will this break my PC? No, and you (probably) will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

# Enable Virtualization in BIOS/UEFI



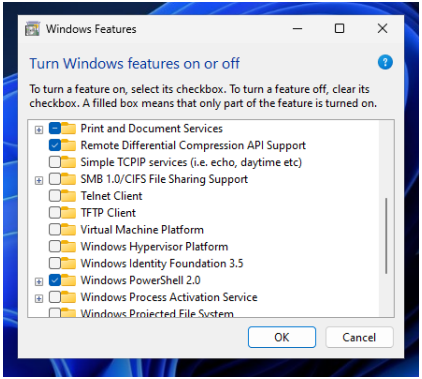
# Enable Virtualization in BIOS/UEFI

# Enable Virtualization in BIOS/UEFI



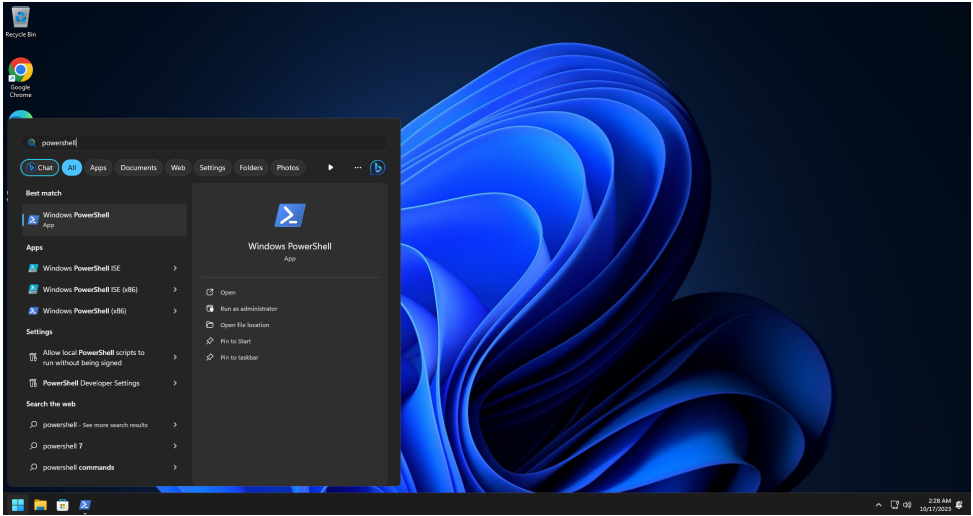
# Enable Windows Virtualization

- Open “Windows Features” and enable:
  - Virtual Machine Platform
  - Windows Hypervisor Platform
  - Windows Subsystem for Linux



# Install WSL2

>_ Open Poweshell



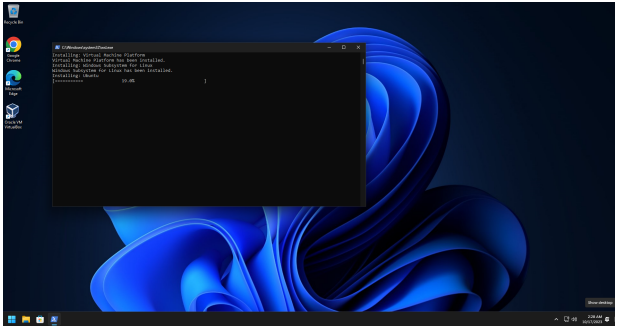
# Install WSL2

Introduce the following commands in powershell

**Install Windows Subsystem for Linux**

```
wsl --set-default-version 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

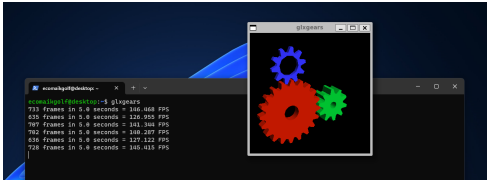
**Install Required Software**

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

- Finally, let's run a sanity check

**Sanity Check**

```
glxgears
```

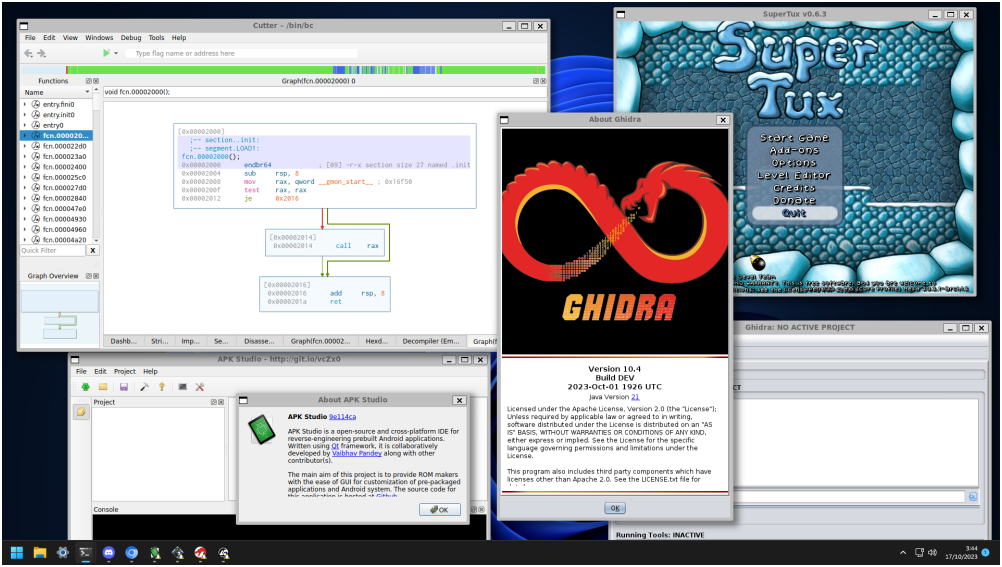


# Additional Sanity Checks

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

```
ecomaikgolf@desktop: ~
ecomaikgolf@desktop:~$ echo $DISPLAY
:0
ecomaikgolf@desktop:~$ ls /mnt
c  wsl  wslg
ecomaikgolf@desktop:~$ file /tmp/.X11-unix/
/tmp/.X11-unix/: directory
ecomaikgolf@desktop:~$
```

# Sneak Peek Final Setup



# Sneak Peek Final Setup

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

# Linux

# Install Rootless Podman & Distrobox

Introduce the following commands in bash:

Install Rootless Podman

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

Podman is a container engine like docker

Install Distrobox

```bash
# Ubuntu 22.04
curl -s https://raw.githubusercontent.com/89luca89/distrobox/main/install | sudo sh
# Ubuntu 23.10
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

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

BlackArch is based on ArchLinux

Kali Linux

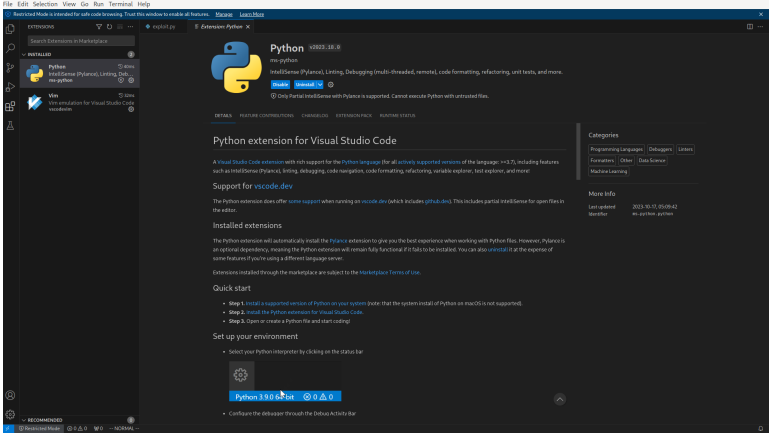
```
distrobox create -i docker.io/kalilinux/kali-rolling:latest --name ctf
distrobox enter ctf
```

Kali Linux is based on Debian Testing

# Install some Tools

**Install an Editor**

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



# Install some Tools

Install pwntools

```
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

```
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

```
pacman -S --needed git base-devel
git clone https://aur.archlinux.org/yay-bin.git
cd yay-bin
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 stegonography 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

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

### Create Kali Linux CTF Container

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

---

### Exit Container

```
exit    # or
Ctrl+D  # or
```

### Remove Container

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

### Stop Container

```
distrobox stop <name>
```

### List Containers

```
distrobox list
```

# CTF Setup & Tooling

## Configuration of a CTF Enviroment for Windows & Linux

>_ PROD v1.3 ✔


Ernesto Martínez García[1]

me@ecomaikgolf.com

ecomaikgolf#3519

Graz University of Technology


LosFuzzys Beginner Trainings

18th October 2023

SLIDES

ls.ecomaikgolf.com/slides/ctfsetup.pdf