Windows Virtual Machine Setup

Foreword

In this document I explain in a few easy steps on how to setup the windows virtual machine on p3ng0s and how to use it accordingly for building C# programs and cloning a windows environment from an exploited machine. You will also be able to boot from a plugged in USB drive. In the future there will also be a network boot option available currently it does not work (11 Jan 2024).

Note that currently the supported architecture is x86_64 but I am also working on aarch64 support.

Setup

Requirements

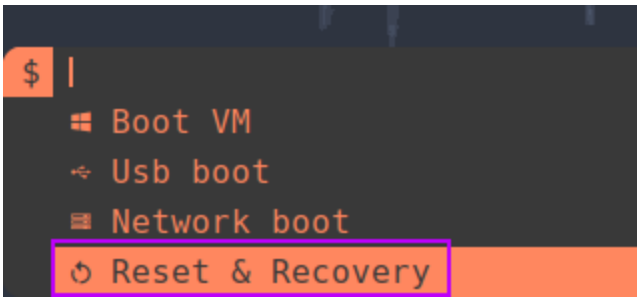
- Windows Virtio-Drivers

```
https://fedorapeople.org/groups/virt/virtio-win/direct-downloads/stable-virtio/virtio-win.iso
```

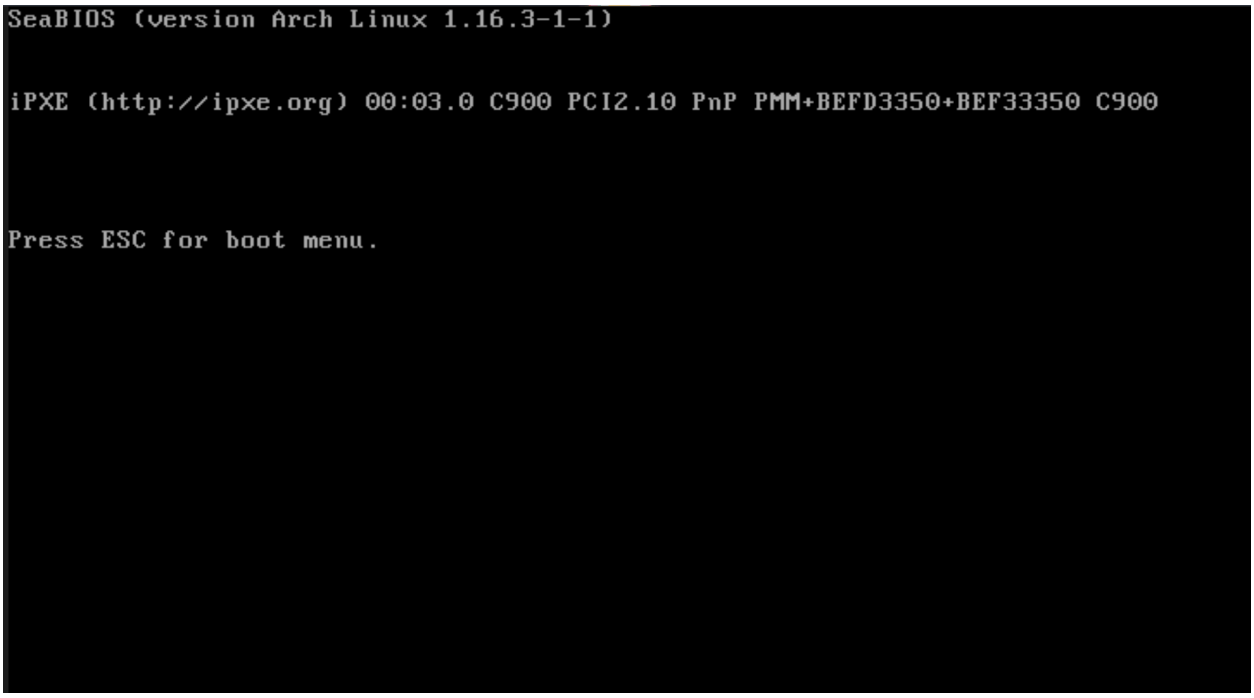
- windows 10 ISO
- qemu packages

Install of windows

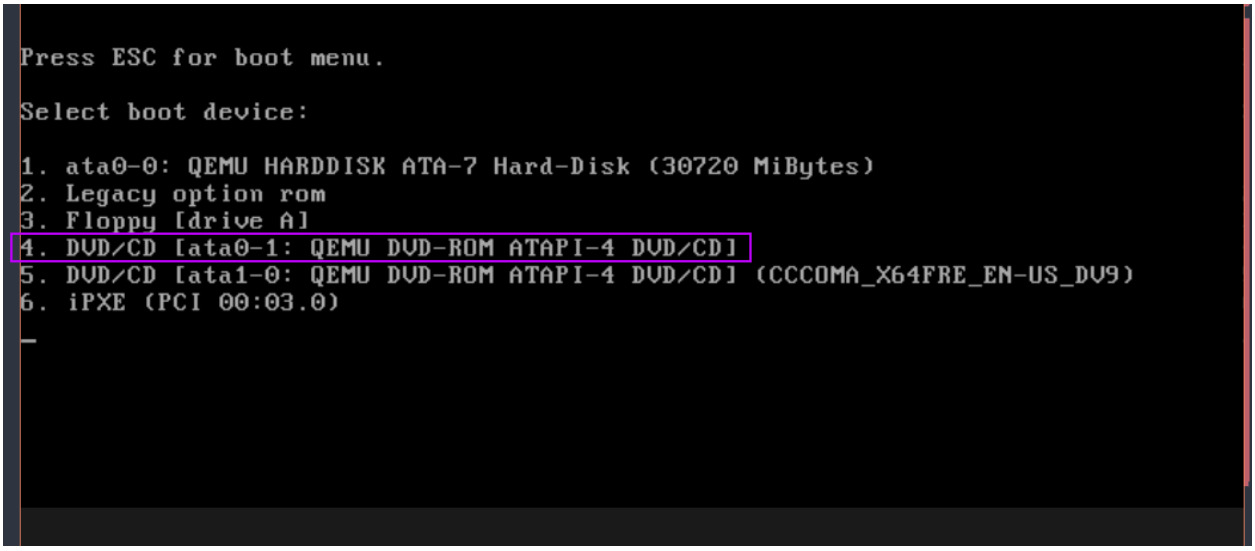
The installation of windows is quite straight forward and follows the same principle as any other installs. As long as you have the correct files in the correct folder everything should work fine! Inside of your $HOME folder you should save the Windows.iso file as the following: Win10_22H2_English_x64v1.iso I might change this name in the future so that it is more congruent. After that you can run the dmenu_win script by pressing the MOD+v (By default MOD→ Alt) shortcut on your keyboard:



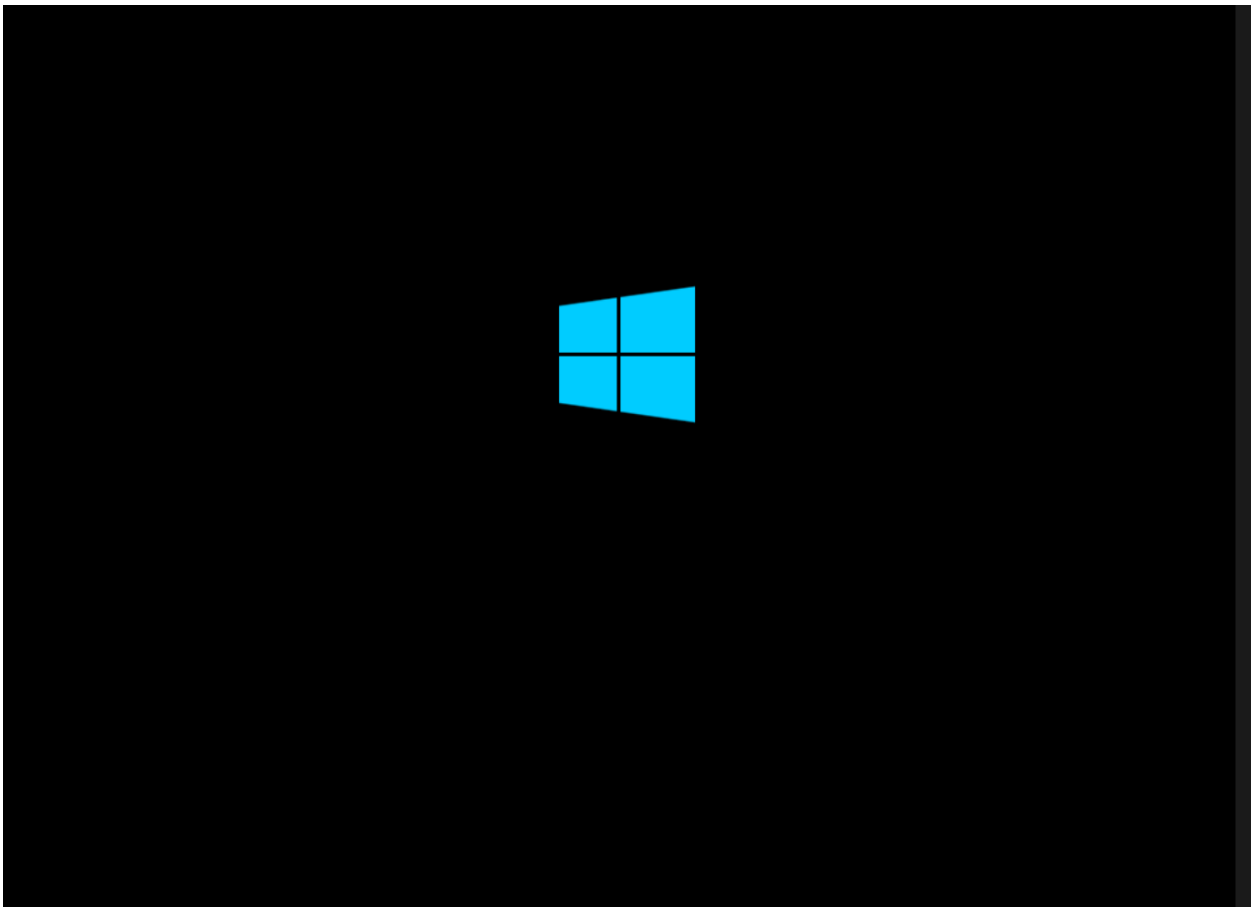
From there you can just proceed by selecting the Reset & Recovery option which will launch the creation with the .iso loaded:



You will then need to press ESC to actually boot from the .iso file select option 4:

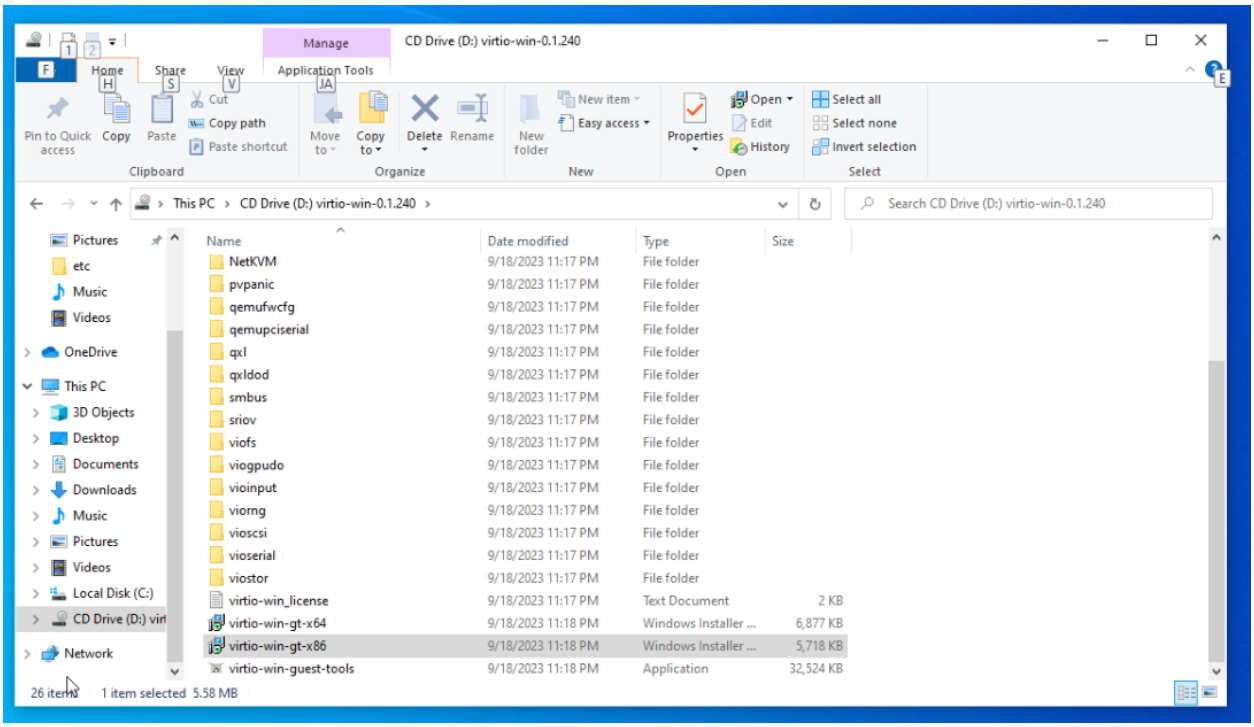


You should now be booted inside of the normal windows ISO install! It does take a bit of time to boot on first setup so if you get a blinking cursor at the top of the screen just wait for about 10 minutes to be sure it isn't just slow :)



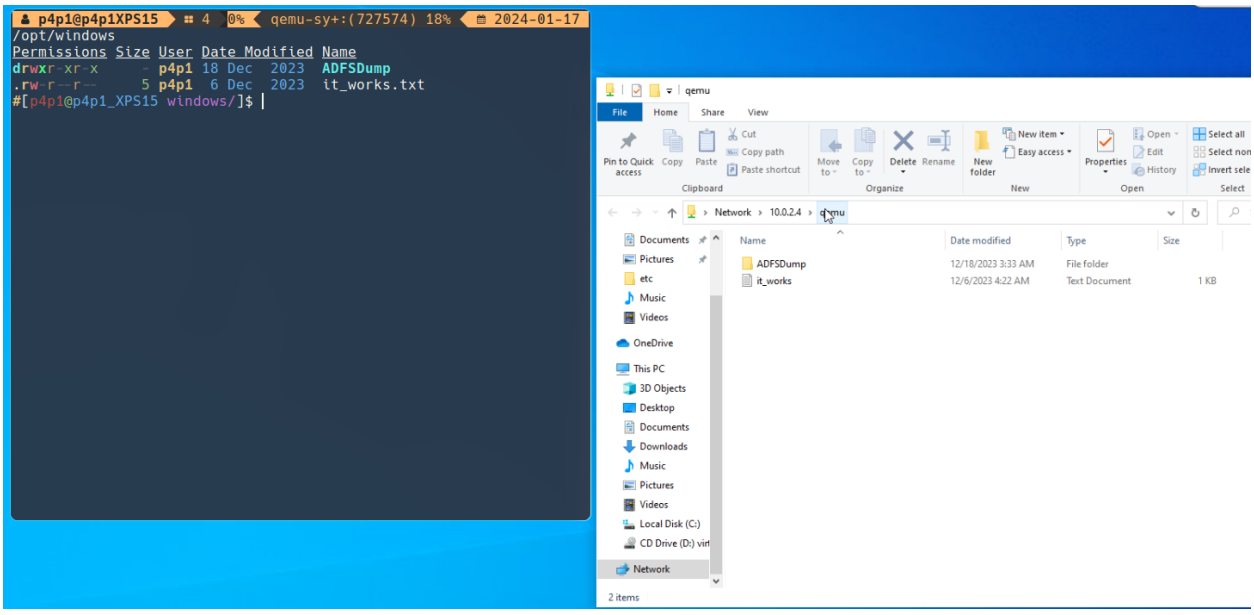
Drivers and shared folders

Now you will want to install drivers for maximum support with your machine and just so that everything runs smoothly. To do so login to your windows VM and select the following:



The D drive should have the virtio drivers and you can run the virtio-win-gt-x86 exe file!

The shared folder is made as a SMB file share located on the following link: \\10.0.2.4\qemu

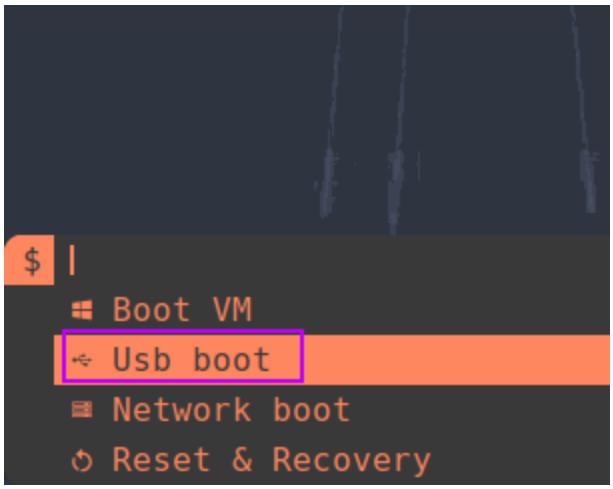


That is directly mapped to the /opt/windows/ folder inside of your p3ng0s installation!

Other Features

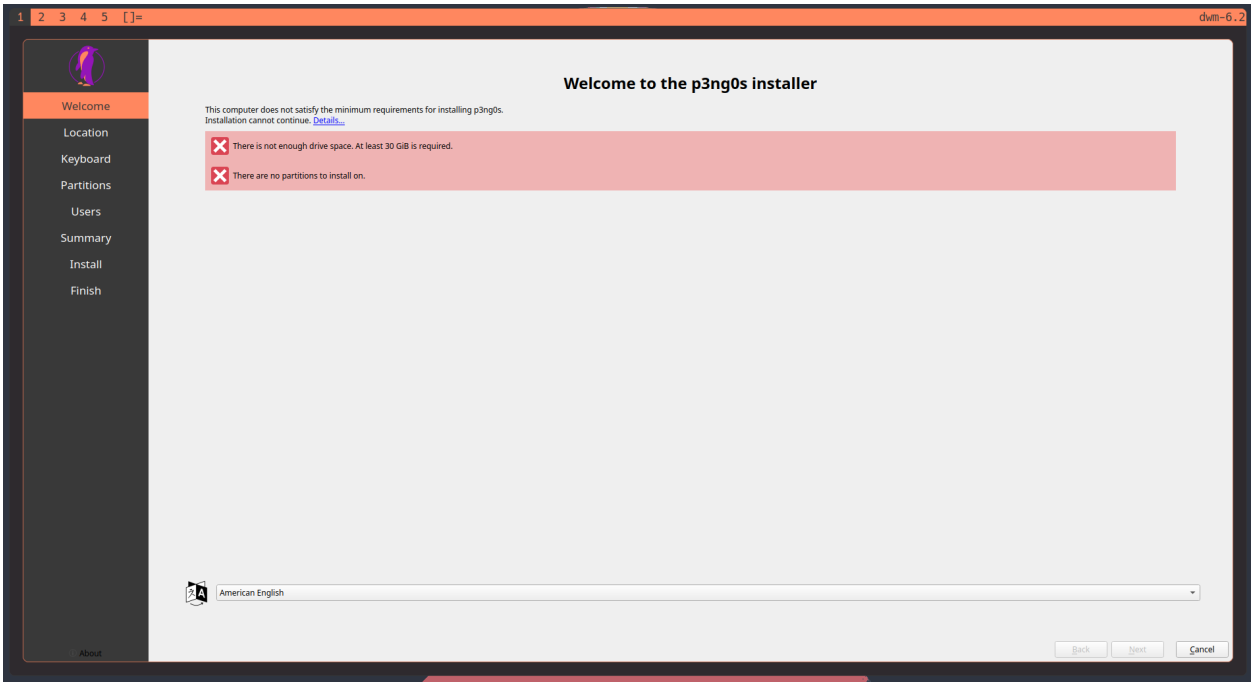
Live USB Boot

A great feature of the windows VM toolset on p3ng0s is the support of running live USB directly from the machine to do that plugin in you flash drive and select the boot from USB option:



You will then be prompted to select the drive you wish to boot form:

From there it will take a few seconds but you should be booting into your USB drive / Hard Drive that is plugged in to your machine:



Useful windows tools list

Here is a collection of windows tools that can be interesting to install on your windows machine. This is mainly for me since I always forget the windows tools but maybe someone else out there can find this toolbox usefull as well:

oxid.it - Cain & Abel

oxid.it web site

https://web.archive.org/web/20190101122212/http:/www.oxid.it/cain.html

Immunity Debugger

The best of both worlds

https://www.immunityinc.com/products/debugger/

Chocolatey - The package manager for Windows

Chocolatey is software management automation for Windows that wraps installers, executables, zips, and scripts into compiled packages. Chocolatey integrates w/SCCM, Puppet, Chef, etc.

https://chocolatey.org/