Linux for CTFs

Nathan Huckleberry

Why run Linux?

Many CTF challenges are much easier on linux

- Most existing CTF tools are written for linux
- Scripting languages are way more convenient in linux
- Installing software/dependencies is much easier in linux
- Binary exploitation is impossible on windows/mac
- Reverse engineering is hard on windows/mac
- Forensics is hard on windows
- Crypto is inconvenient on windows

Options for running a Linux device

Windows Subsystem for Linux (WSL)

VM

Dual Boot

WSL

Linux VM built-in to Windows

Easy to set up

Compatible with almost anything you need to do

Recommended for Windows users

VM

Slightly harder to setup than WSL

Not many advantages over WSL

Dual Boot

Install Linux directly onto your computer

Choose between Linux/Windows on boot

Fairly hard to set up

Recommended if you're an upperclassman

Installing WSL

Navigate to Settings > Apps > Programs and Features

Click Turn Windows features on or off

Check Windows Subsystem for Linux

Check VirtualMachinePlatform

Restart

Installing WSL

Open Powershell as Administrator

Run wsl --set-default-version 2

If you get an invalid command line error, you need to update Windows

Your Windows version must be Build 18362.1049 or higher to use WSL2

Windows version can be checked using winver

Installing WSL

Open the Microsoft store and install Ubuntu

Setting up VM on MacOS

Install Parallels

File > New

Click Ubuntu

Programs to Install

Reversing

ghidra

cutter

binwalk

Pwn

pwntools

ropgadget

gef

onegadget

Crypto

sagemath

Networking

wireshark

Utilities

git

bless

netcat

Utility

netcat - tool for making raw connections to ports

git - version control system, useful to download tools

bless - gui hex editor

```
$ sudo apt update

$ sudo apt install git netcat bless
```

Reversing

cutter - nice ui for reversing

binwalk - looks for files inside of other files

ghidra - decompiler released by the NSA

```
$ sudo apt update

$ sudo apt install cutter binwalk


$ sudo apt install git

$ cd /tmp

$ git clone https://github.com/bkerler/ghidra_installer

$ cd ghidra_installer

$ ./install-ghidra.sh
```

Pwn

pwntools - python framework for exploits

ropgadget - automate finding gadgets for rop

gef - theme for gdb

onegadget - tool for finding 'one-gadgets' in libc

```
$ sudo apt-get update

$ sudo apt-get install python3 python3-pip
python3-dev git libssl-dev libffi-dev
build-essential

$ python3 -m pip install --upgrade pip --user

$ python3 -m pip install --upgrade pwntools --user

$ python3 -m pip install capstone --user

$ python3 -m pip install ropgadget --user

$ sudo apt install gdb

$ sh -c "$(wget http://gef.blah.cat/sh -O -)"

$ sudo apt-get install rubygems

$ gem install one_gadget
```

Crypto

sagemath - giant math library, useful for hard crypto

```
$ sudo apt install sagemath sagemath-jupyter
```

Networking

wireshark - program for capturing packets and viewing network data

```
$ sudo apt install wireshark
```

```
// if that didn’t work try this instead:

// sudo add-apt-repository universe

// sudo apt install wireshark
```