

WEAPONIZING UBUNTU

GETTING YOUR CTF/RE VM UP AND RUNNING

- > UBUNTU 16.04 (XUBUNTU)
 - > QEMU
 - > IPYTHON
 - > ANGR
 - > PWNTOOLS
 - > PWNDG
- > LOTS OF AWESOMENESS

git.io/vPFWR

UPDATE THE OS

```
sudo apt-get update  
sudo apt-get upgrade
```

PREREQS

```
sudo apt-get install git \  
tmux \  
python-dev \  
libffi-dev \  
libssl-dev \  
build-essential \  
virtualenvwrapper
```

TOOLCHAINS

```
sudo apt-get install gdb-multiarch \  
gcc-mipsel-linux-gnu \  
gcc-arm-linux-gnueabi \  
gcc-aarch64-linux-gnu
```

LIBRARIES

```
sudo apt-get install libc6-arm64-cross \  
libc6-armel-armhf-cross \  
libc6-mips-cross
```

QEMU

```
sudo apt-get install qemu-system qemu-user-binfmt  
sudo mkdir /etc/qemu-binfmt  
sudo ln -s /usr/mipsel-linux-gnu /etc/qemu-binfmt/mipsel  
sudo ln -s /usr/arm-linux-gnueabi /etc/qemu-binfmt/arm  
sudo ln -s /usr/aarch64-linux-gnu/ /etc/qemu-binfmt/aarch64
```


TESTS

```
cat << EOF > test.c
#include <stdio.h>
int main(int argc, char **argv){
    printf("hello %d\n", argc);
}
EOF
```

TESTS

```
gcc -o test test.c
```

```
aarch64-linux-gnu-gcc -o test.aarch64 test.c
```

```
arm-linux-gnueabi-gcc -o test.arm test.c
```

```
mipsel-linux-gnu-gcc -o test.mips test.c
```

ANGR

```
deactivate  
mkvirtualenv angr  
pip install ipython angr
```

PWNTOOLS

```
deactivate
```

```
mkvirtualenv pwntools
```

```
pip install ipython pwntools
```

PWNDBG

```
git clone https://github.com/pwndbg/pwndbg  
cd pwndbg  
./setup.sh
```

RADARE2

```
git clone https://github.com/radare/radare2/
```

```
cd radare2
```

```
sys/install.sh
```

```
r2pm init
```

```
r2pm update
```

```
r2pm install r2pipe-py
```