Example:

$ ./gen\_mkr1.py

=== Preparing task for [Mykola ILIN], port 10100, flag hvost{CGLlORK4}bobra

gcc -Wno-implicit-function-declaration -static -no-pie -fno-stack-protector -o out/10100/10100\_ILIN\_Mykola out/10100/10100\_ILIN\_Mykola.c && strip -s out/10100/10100\_ILIN\_Mykola

/usr/bin/ld: /tmp/ccfgriXd.o: in function `main':

10100\_ILIN\_Mykola.c:(.text+0x16b): warning: the `gets' function is dangerous and should not be used.

Target OS:  
Ubuntu 20.04 x64 192.168.1.20

Install:

$ sudo apt-get install -y xinetd

<https://www.cyberciti.biz/faq/linux-how-do-i-configure-xinetd-service/>

Prepare:

$ sudo mkdir bv\_mkr1 && sudo cd bv\_mkr1 && sudo mkdir 10100

$ scp C:/Users/lol19/Desktop/10100\_ILIN\_Mykola.secret sam@192.168.1.20:/home/sam

$ scp C:/Users/lol19/Desktop/10100\_ILIN\_Mykola sam@192.168.1.20:/home/sam

$ sudo cp 10100\_ILIN\_Mykola.secret /bv\_mkr1/10100 && sudo cp 10100\_ILIN\_Mykola /bv\_mkr1/10100

$ sudo chmod ugo+rwx /bv\_mkr1/10100/10100\_ILIN\_Mykola.secret && sudo chmod ugo+rwx /bv\_mkr1/10100/10100\_ILIN\_Mykola

Compile:

$ gcc -Wno-implicit-function-declaration -static -no-pie -fno-stack-protector -o 10100\_ILIN\_Mykola 10100\_ILIN\_Mykola.c && strip -s 10100\_ILIN\_Mykola

Configure xinetd:

$ sudo useradd bv\_mkr1

$ sudo nano /etc/xinetd.d/bv\_mkr1

service ILIN\_Mykola

{

type = UNLISTED

protocol = tcp

socket\_type = stream

port = 10100

wait = no

server = /usr/bin/setarch

server\_args = -R /usr/sbin/chroot --userspec=bv\_mkr1 /bv\_mkr1/10100 ./10100\_ILIN\_Mykola

user = root

}

$ sudo /etc/init.d/xinetd restart

Connect from target:

$ nc localhost 10100

Connect from hacker:

$ nc 192.168.1.20 10100

Test:

$ sudo apt install python3-pip

$ pip3 install pwn

$ python3 10100\_pwn.py

# Pasha:

$ ssh -p 4444 student@62.216.54.74

123QWer45

$ scp -P 4444 C:/Users/lol19/Desktop/10100.zip student@62.216.54.74:/home/student

$ nc 62.216.54.74 10100

$ objdump -d -j .text -M intel /bv\_mkr1/10100/10100\_ILIN\_Mykola > dis.txt

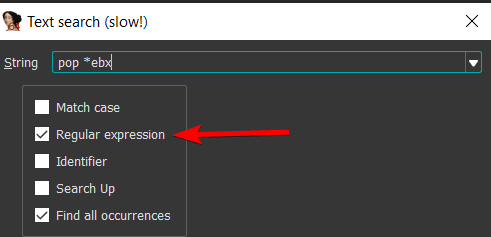
# Find gadgets (IDA):

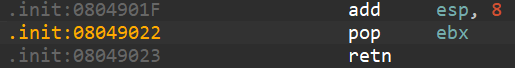
.text:08058BB8 pop ebx

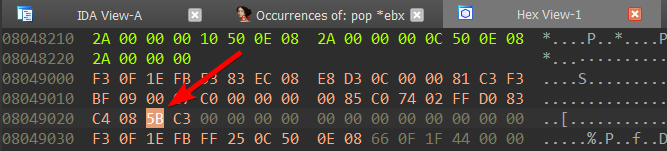
.text:08058BB9 pop esi

.text:08058BBA retn

Search regex: pop \*ebx







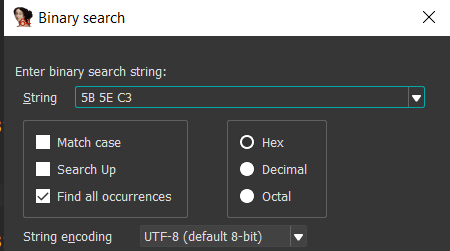
5B is opcode

Do these actions for the rest instructions:

pop \*esi 5E

retn C3

Search for opcode sequence:5B 5E C3



# Find gadgets (Cutter):

Assume you want to find "pop edi; pop ebp; ret":

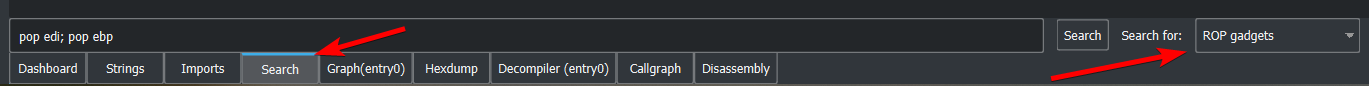
0x08058bb8 pop ebx

0x08058bb9 pop esi

0x08058bba ret

Search in ROP gadgets:

pop edi; pop ebp



# Ropper (Kali):

$ sudo apt install ropper

$ scp C:/Users/lol19/Desktop/10101\_YAKOBCHUK\_Dmytro sam@192.168.1.18:/home/sam

$ ropper -f 10101\_YAKOBCHUK\_Dmytro --nocolor > gadgets.txt

$ cat gadgets.txt | grep "pop ebx; pop esi; ret"

# Amd64:

# Kali:

$ scp C:/Users/lol19/Desktop/10100\_ILIN\_Mykola sam@192.168.1.18:/home/sam/mkr1

$ scp C:/Users/lol19/Desktop/10100\_ILIN\_Mykola.secret sam@192.168.1.18:/home/sam/mkr1

$ sudo chmod ugo+rwx 10100\_pwn.py

$ cat /dev/null > 10100\_pwn.py && nano 10100\_pwn.py

# WSL 2:

PS> wsl

$ cd Desktop/10100

$ ./10100\_ILIN\_Mykola

$ python3 10100\_pwn.py

> wsl hostname -I

$ scp C:/Users/lol19/Desktop/10100\_ILIN\_Mykola sam@172.20.166.189:/home/sam/mkr1

$ scp C:/Users/lol19/Desktop/10100\_ILIN\_Mykola.secret sam@172.20.166.189:/home/sam/mkr1

$ scp C:/Users/lol19/Desktop/10100\_ILIN\_Mykola.secret sam@172.20.166.189:/home/sam/mkr1

$ gdb -q 10100\_ILIN\_Mykola

gef➤ br \*0x401eff

gef➤ c

gef➤ set $rax=0x539

Debub programmatically:

<https://www.youtube.com/watch?v=CWxDhp0OFzI>

<https://halb.it/posts/pwntools-gdb/>

<https://github.com/Gallopsled/pwntools-tutorial/blob/master/debugging.md>

$ gdb -p 87997

For WSL:

<https://allthingsreversed.io/making-pwnlib-gdb-attach-work-under-wsl2/>

<https://www.youtube.com/watch?v=tFVmCwL30Q8>

Keep wsl run:

<https://superuser.com/questions/1762286/windows-terminal-run-a-command-when-starting-wsl-and-keeping-the-shell-open>

<https://stackoverflow.com/questions/72778785/keep-windows-terminal-tab-open-after-invoked-wsl-command>

IDA remote debug:  
$ ./linux\_server64

Options:

/mnt/c/Users/lol19/Desktop/10100/10101\_YAKOBCHUK\_Dmytro

/mnt/c/Users/lol19/Desktop/10100

DWORDS:

x/5000x $esp

$ gdb -q 10101\_YAKOBCHUK\_Dmytro -x breaks32.gdb

$ scp C:/Users/lol19/Desktop/10100/10126\_ZELENIN\_Vladyslav sam@192.168.1.20:/home/sam/mkr1