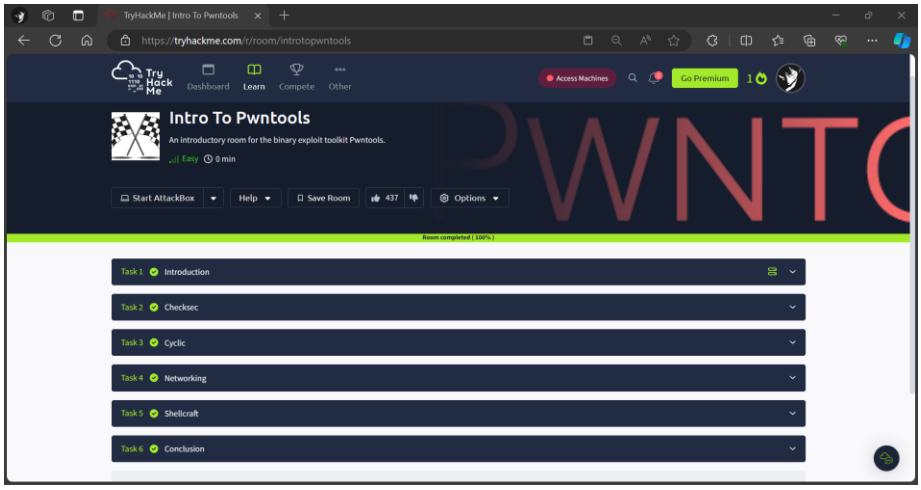
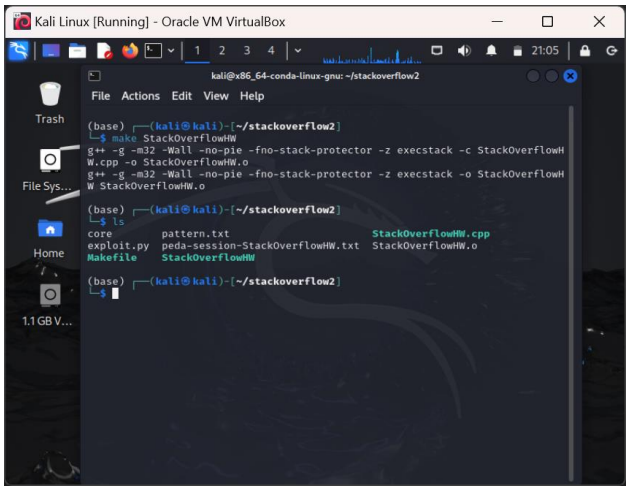
Stack Overflow Exploitation using Python Pwntools

1. TryHackMe

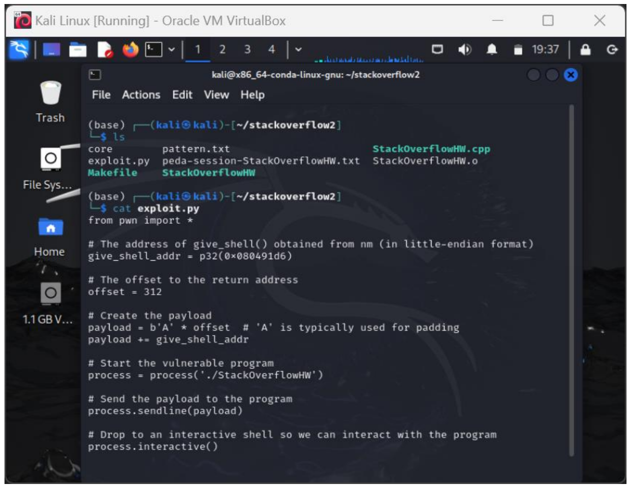


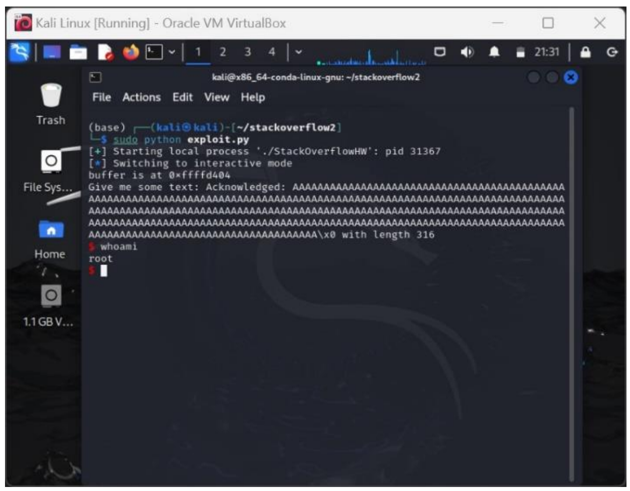
2. StackOverflowHW Executable
    a. Compile the program as x86 binary, disabling all countermeasures, using a Makefile.



    b. Write python code using the Pwntools module to force the program to execute the give_shell function and remote root shellcode to exploit the program.

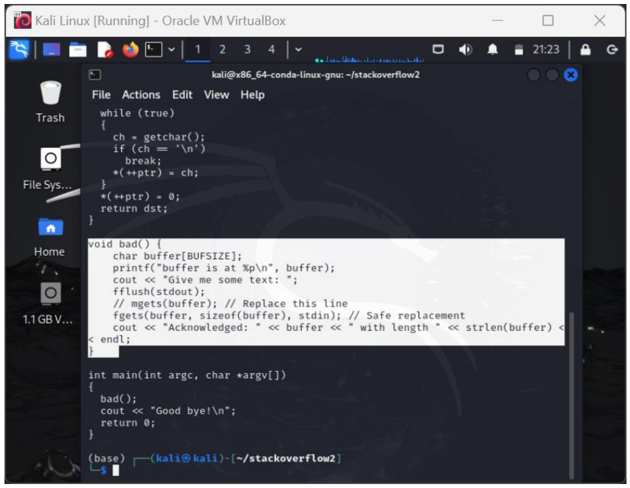
I wrote a python script like the example in TryHackMe that uses Pwntools to create a payload that redirects the flow of the program to the give_shell function. Next, I executed ‘sudo python exploit.py’ to spawn remote root shellcode.

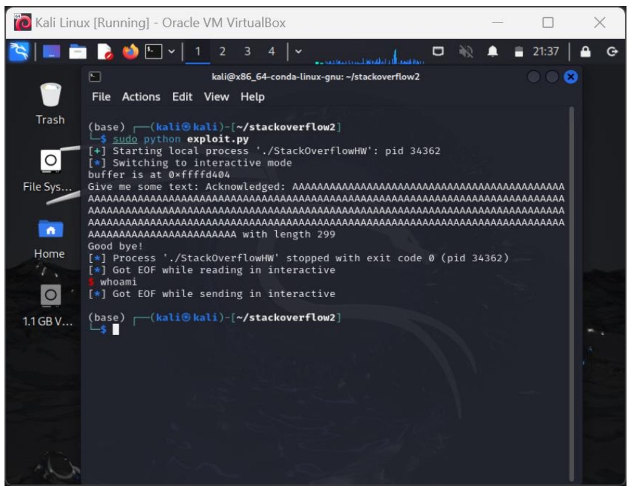




c. Patch the vulnerability in the program.

I replaced mgets with fgets (which includes boundary checking), passing it the buffer alongside its size and stdin. However, this time when I executed the exploit with the same command as before, no remote root shellcode was spawned.





d. Turn on the countermeasures and relaunch the exploit.

I modified the Makefile to comment out the countermeasures, executed make commands and a command to execute the exploit and just as before no remote root shellcode was spawned.