Installing with curl vuln and vuln.c to wsl environment.

Running checksec on vuln.

No canary, just NX, must be easy.

Looking at vuln.c

Creating a python program.

Adding 100 to the buffer injection.

Adding 104

dmesg | tail

108

dmesg | tail

112

dmesg | tail

116

dmesg | tail

Getting win address using readelf -s vuln | grep win.

Win takes args so args must be passed with hex values like in code whereas arg1 is CAFEF00D and arg2 is F00DF00D