REDO NX Analysis with Peekaboo

`input` contains 1500 characters which will trigger the overflow in characters.

Compile NX binary.

gcc -fno-stack-protector -no-pie -o vuln vulnerable.c

~/dynamorio/build/bin64/drrun -c ~/peekaboo/peekaboo\_dr/build/libpeekaboo\_dr.so -- ../vuln < inputs/input

NX binary, peekaboo dump at PID 28511.

Compile NON-NX binary.

gcc -fno-stack-protector -z execstack -no-pie -o vuln vulnerable.c

Text

Description automatically generated

~/dynamorio/build/bin64/drrun -c ~/peekaboo/peekaboo\_dr/build/libpeekaboo\_dr.so -- ../vuln < inputs/input

NON-NX binary, peekaboo dump at PID 29335.

Extract just the instruction bytes.

~/peekaboo/read\_trace vuln-28511/28511/ | awk -F '\t ' '{print $2}' | awk -F ' ' '{print $1}' | awk NF > vuln.txt

~/peekaboo/read\_trace vuln-29335/29335/ | awk -F '\t ' '{print $2}' | awk -F ' ' '{print $1}' | awk NF > nodef\_vuln.txt

# Installation of udcli

## Inside udcli folder from https://udis86.sourceforge.net/manual/getstarted.html#building-and-installing-udis86

./configure --with-python=/usr/bin/python3.8

Text

Description automatically generated

Text

Description automatically generated