Mostafa Fatayri   
202101056

Canary Stack protection is a security mechanism used mainly to detect and prevent any king of stack buffer overflow exploits. When a function is called , a canary value will be placed on the stack just before the return address .Before the function returns , the canary value is checked, if it has been overwritten , thus the program will recognize this as an attack and will directly aborts the execution . if not the program will continue .

This mechanism is benefitable due to the fact that most buffer overflow attacks involve overwriting the return address on the stack to redirect the programs into malicious codes. Having a canary before the return address will fake the return address and any attack on the return address will be directed to the canary keeping the return address safe in place that is why it is very useful and a good technique . however u can still by pass a canary even through

Stack leak , guess the value …

it was called this way due to the term canary in this context is analogy to the “ canary in a coal mine” . Through out history , miners used canaries as an precaution for presence of toxic gases , if the canary showed signs of distress , this well indicate that the environment was unsafe. In the context of Computer Security , it was a similar process , if the canary address was change , then definitely the return address has been change as well .

Reference :

https://youtu.be/N7kGd76evsM?si=GYBlK6JmucAr-gm2