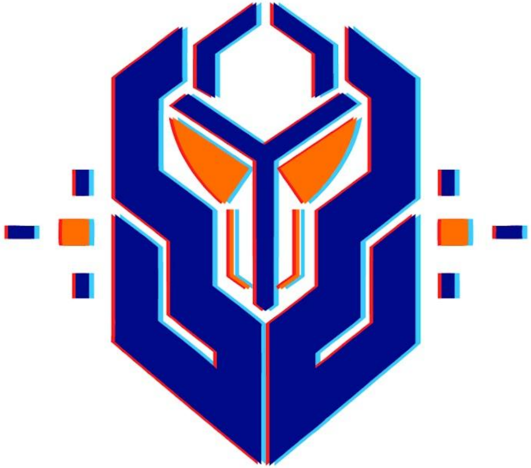
CWL
CyberWarFare Labs

A BRIEF OVERVIEW OF STACK-BASED BUFFER OVERFLOW

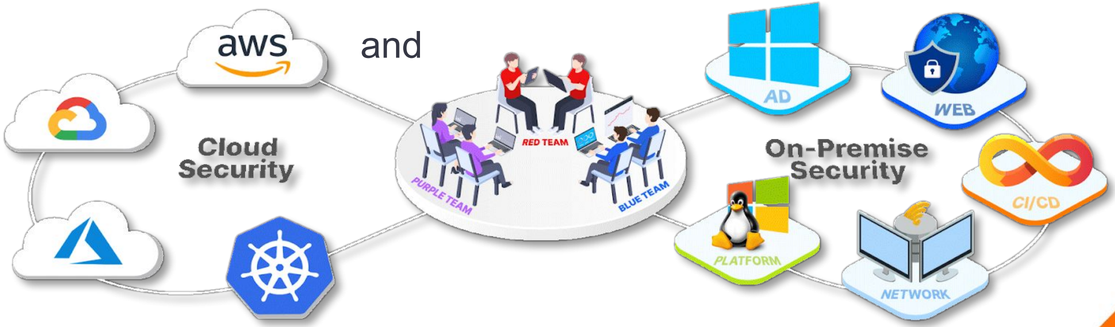


CyberWarFare Labs

CW Labs is a renowned UK based Ed-tech company specializing in cybersecurity cyber range labs. They provide on-demand educational services and recognize the need for continuous adaptation to evolving threats and client requirements.

The company has two primary divisions :

1. **Cyber Range Labs**
2. **Up-Skilling Platform**



INFINITE LEARNING EXPERIENCE

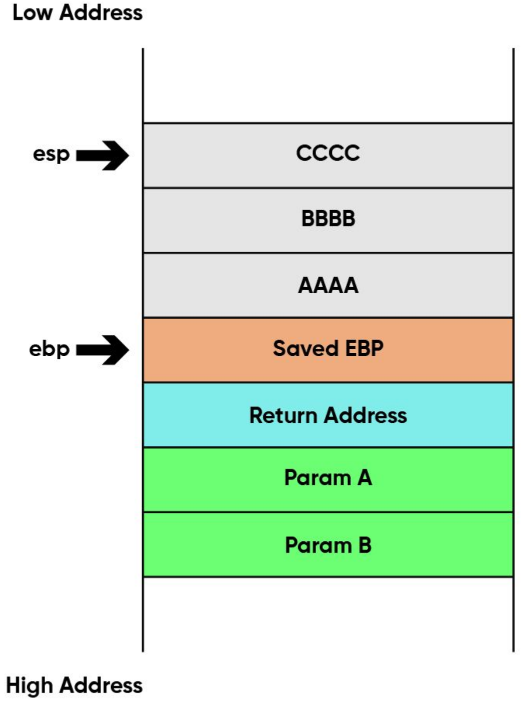
John Sherchan

Red Team Security Researcher at CW Labs

He is a Red Team Security researcher, bringing over 5+ years of experience in Reverse Engineering, Malware Analysis/Development, and Source Code Reviewing, with a specialization in Windows Internals (User and Kernel Modes). Demonstrating an advanced understanding, he has successfully reversed multiple Antivirus (AV) and Endpoint Detection and Response (EDR) systems to comprehend its architecture. Committed to advancing cybersecurity, his additional interests include PWNing Active Directory, conducting Adversary emulation/simulation, writing rootkits, crafting exploits, and strategically overcoming challenges.

STACK

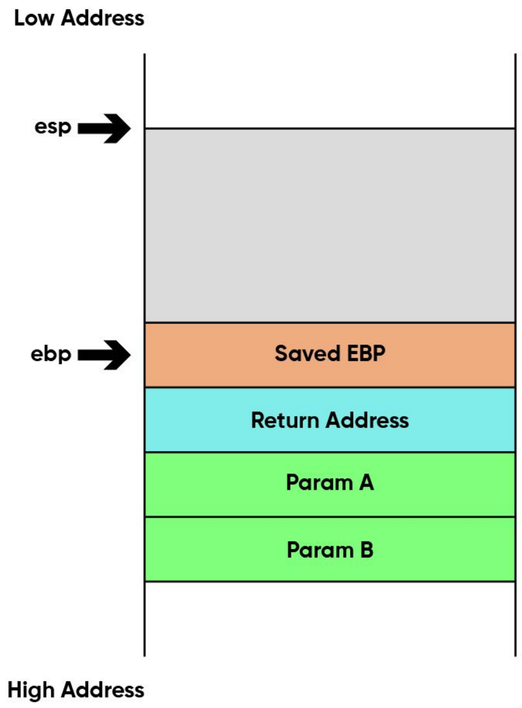
- Block of memory that holds temporary data
  - Operates in LIFO (Last In, First Out) principal
- Grows and shrinks dynamically during program execution
  - Grows towards the lower address (higher -> lower)
- Each function call creates the stack frame, containing parameters, local variables and return address

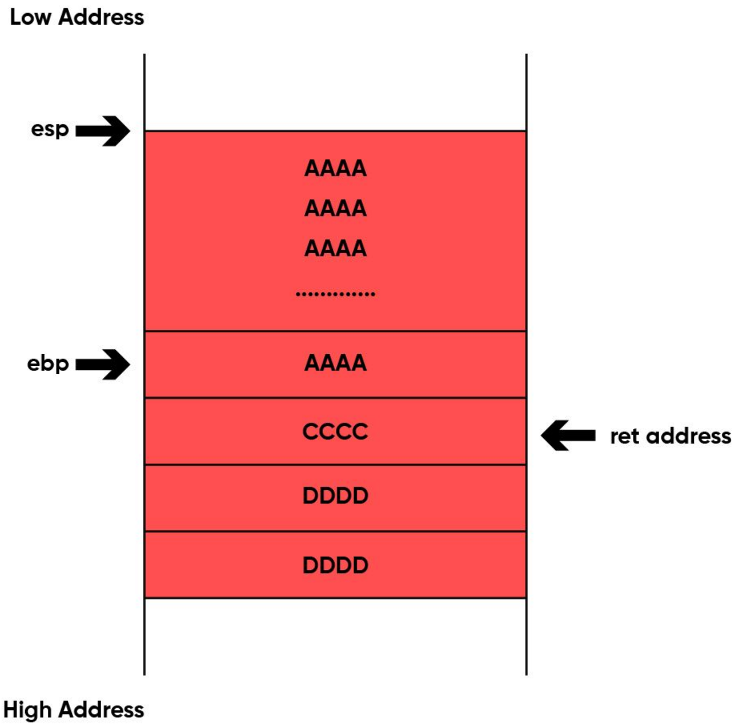

Low Address
esp
CCCC
BBBB
AAAA
ebp
Saved EBP
Return Address
Param A
Param B
High Address

Stack Based Overflow

- A flaw in software that occurs when more data is written to a buffer on the stack than it can hold,
    - resulting in the overwriting of adjacent memory, including other variables and the return address.

- If exploited correctly and all required conditions are met
    - attacker can overwrite the EIP (Instruction Pointer) register
        - potentially redirecting program execution to malicious code.


Low Address
esp
ebp
Saved EBP
Return Address
Param A
Param B
High Address


Low Address
esp
AAAA
AAAA
AAAA
....
ebp
AAAA
CCCC
ret address
DDDD
DDDD
High Address

Functions in C that may lead to overflow

- Some trivial ‘C’ functions that may lead to overflow
    - gets
    - strcpy
    - strcat
    - memcpy
    - memmove
    - sprintf

Stack Based Overflow Steps (no-mitigations)

- Figure out the vulnerable code location
- Find the offset to the return address
- Craft the payload that'll overwrite the return address with the stack location where the shellcode lies
- Send the crafted buffer to program

CWL
CyberWarFare Labs

CERTIFIED EXPLOIT DEVELOPMENT PROFESSIONAL (CEDP) COURSE

GET **80%** OFF

GUARANTEED OFFER ACCESS TO WEBINAR ATTENDEES ONLY!

Get Flat 80% OFF on Certified Exploit Development Professional [CEDP] Course!

All you need to do is ace our quiz with a score of at least 80%.

Once you qualify, you'll automatically receive an email with the discount code for 80% off the CEDP course.

Don't miss out on this amazing opportunity to advance your expertise in exploit development.

Best of luck!

Learn More : https://cyberwarfare.live/product/certified-exploit-development-professional-cedp/

Find the labs here:

https://drive.google.com/file/d/1xrR3xrRVd4v-IrpKOVQhD3bDljYWVMCU/view

CWL
CyberWarFare Labs

Thank You

For Professional Red Team / Blue Team / Purple Team,
Cloud Cyber Range labs / Courses / Trainings, please contact

info@cyberwarfare.live

To know more about our offerings, please visit:

https://cyberwarfare.live