- Filename: eccouncil-ceh31250-v12-6-6-1-buffer-overflows.md
- Show Name: CEHv12 (312-50)
- Topic Name: System Hacking Phases and Attack Techniques - System Hacking
- Episode Name: Buffer Overflows
  ==========

Buffer Overflows

Objectives:

- Summarize the concepts of a Buffer Overflow
- List common tools and techniques used in Buffer Overflow exploit development
- List common protections used to prevent Buffer Overflows

- What is a buffer overflow?
    - Improper memory space allocation
    - No bounds checking
    - Allows data allocated for one memory space to spill over into another
        - If this can be controlled, arbitrary code execution can be achieved
- What are the types of buffer overflows we should be aware of?
    - Heap
        - Dynamic memory allocation
            - malloc()
    - Stack
        - Static memory allocation
            - EBP
            - ESP
            - EIP
- What kind of tools are used to create a buffer overflow?
    - Network Sniffers
    - Debuggers
    - Programming languages
- Walk us through a simple buffer overflow
- How can we protect against buffer overflows?
    - DEP (Data Execution Protection)
    - ASLR (Address Space Layout Randomization)
    - Static and Dynamic code analysis
    - Safe coding practices