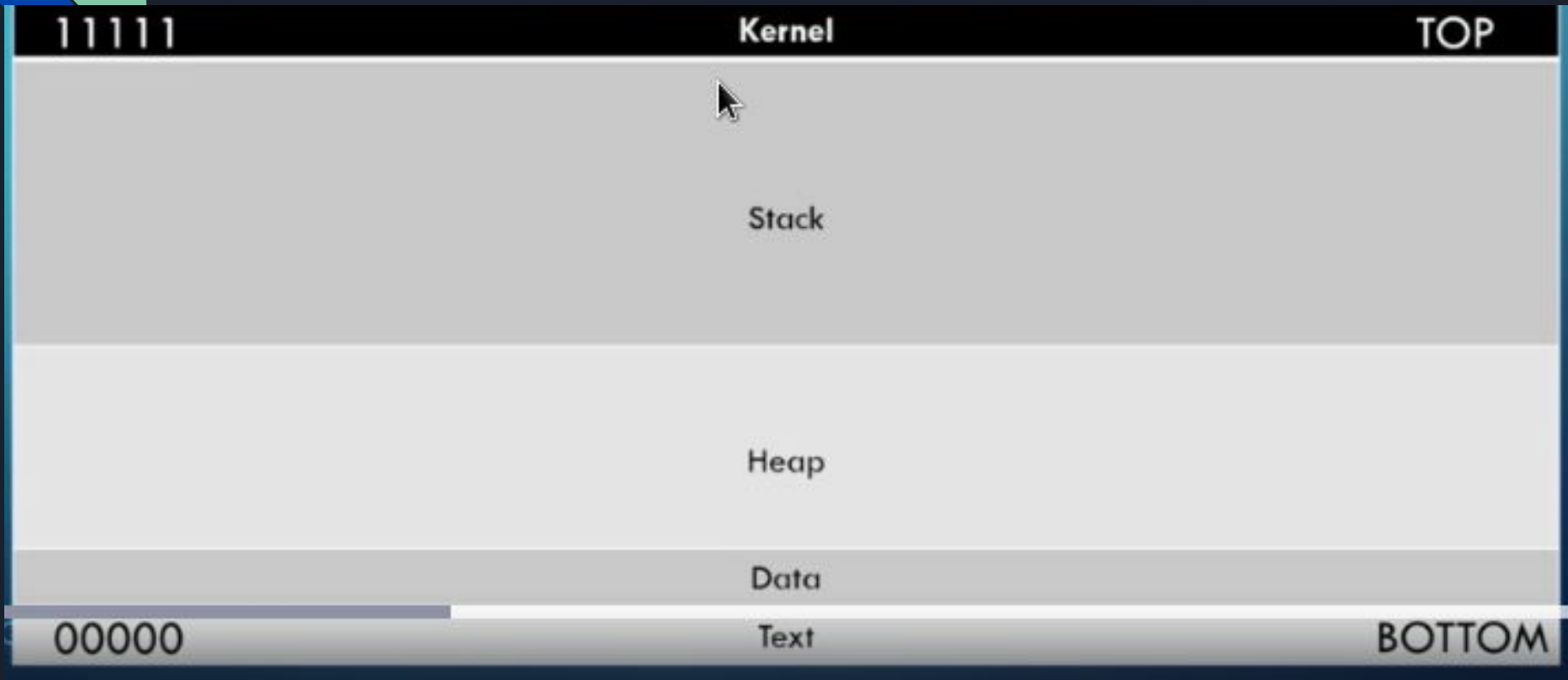


A blue parallelogram and a light green parallelogram are positioned on the left side of the slide, overlapping each other and the dark background.

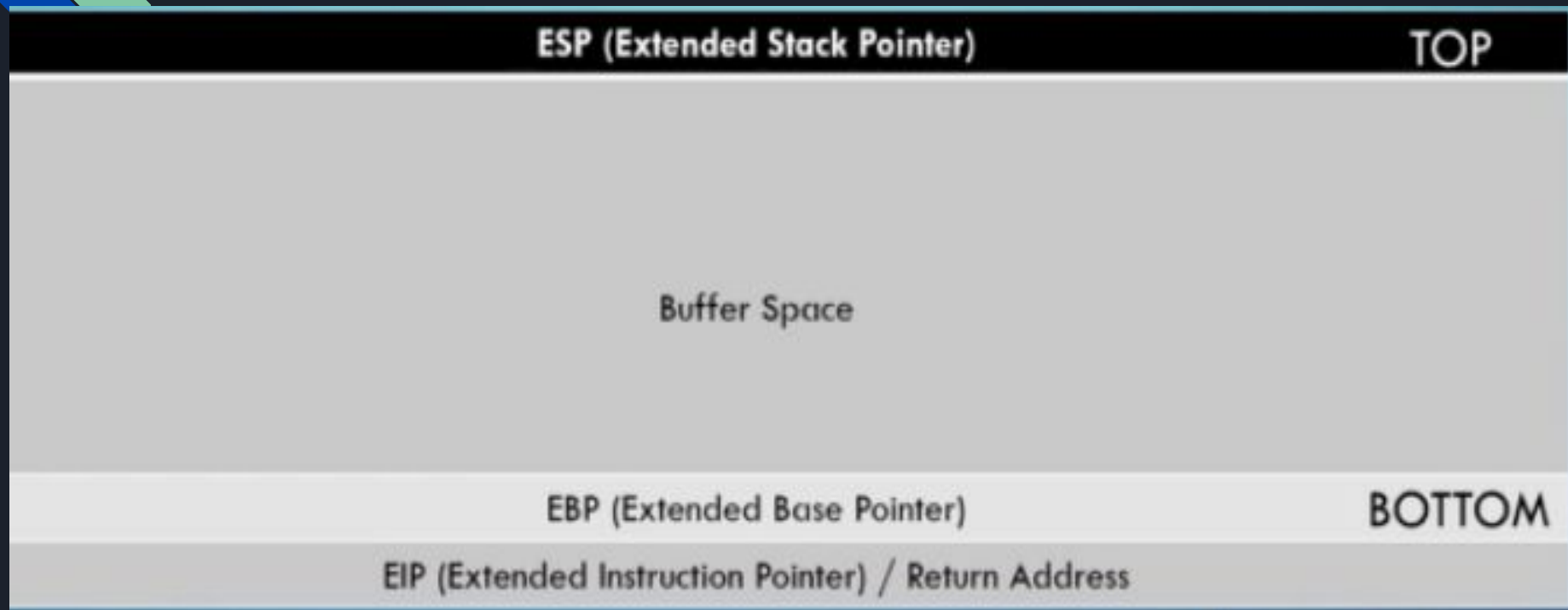
Exploit Development Level 1

@heftamayo

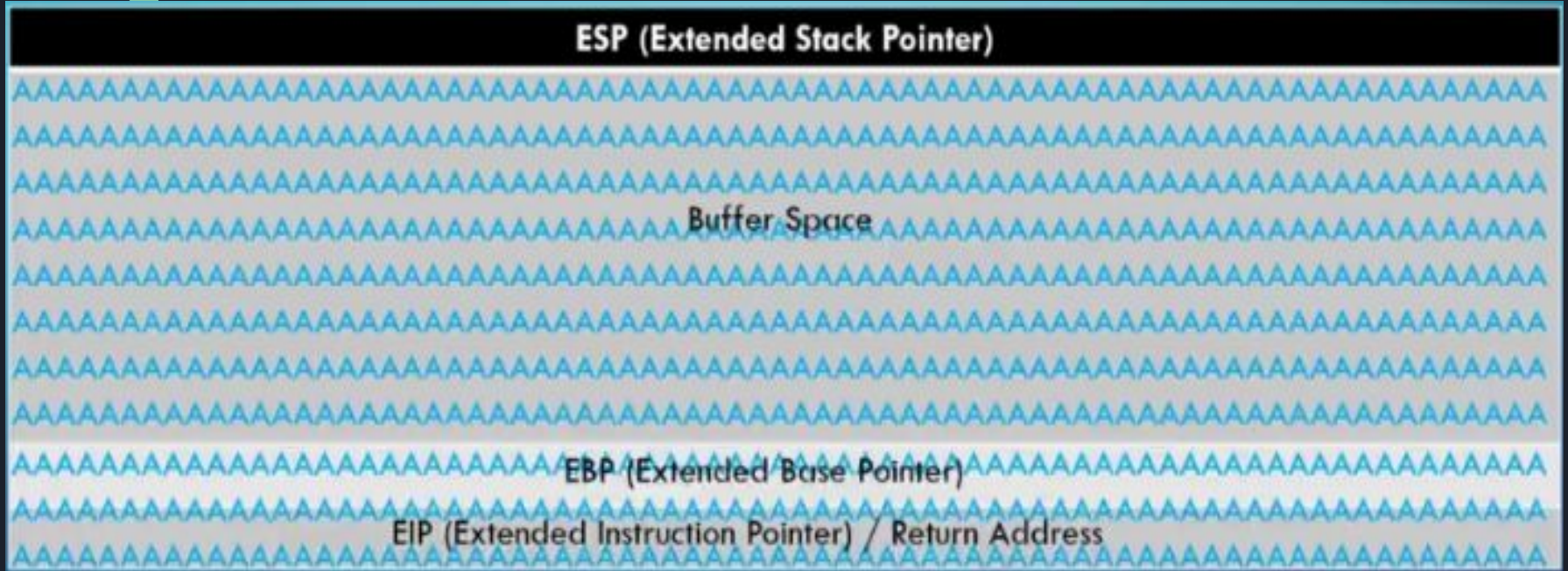
Anatomia de la RAM

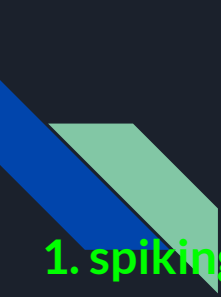


Registros asignados a la RAM



Buffer Overflow





Pasos para ejecutar un Buffer Overflow

- 1. spiking:** encontrar una vulnerabilidad en un programa
- 2. fuzzing:** enviar un grupo de caracteres para verificar si la vulnerabilidad se puede aprovechar
- 3. encontrar el offset:** si se pudo aprovechar la vulnerabilidad es debido a un punto específico (el offset)
- 4. sobrescribir el EIP:** por medio del offset con un buffer overflow
- 5. encontrar caracteres**
- 6. encontrar modulos :** items necesarios para generar el payload
- 7. escribir y enviar la reverse shell**