Lazenca Frame Faking

Frame Faking (Fake EBP)

- 가짜 스택 프레임 포인터를 만들어 프로그램의 실행 흐름을 제어하는 것
- Return Address 영역까지만 덮어쓸 수 있을 경우 사용가능
- LEAVE, RET 명령어
  - LEAVE
    - RBP 레지스터의 값을 RSP 레지스터에 저장
    - RSP 레지스터가 가리키는 Stack 영역의 값을 RBP 레지스터에 저장
  - RET
    - RSP 레지스터가 가리키는 Stack 영역의 값을 RIP 레지스터에 저장
    - JMP 명령어를 이용해 RIP에 저장된 영역으로 이동
- Stack Overflow를 이용해 Frame Pointer, Return Address 영역을 덮어 쓰고 그것을 이용하는 기법
  - Stack Overflow에 의해 Stack Data가 오염되고, 그 오염된 데이터들이 LEAVE 명령어에 의해 EBP의 값으로 들어가게 된다.
- Frame Faking 기법을 통해 ASLR (Address Space Layout Randomization) 보호기법을 우회할 수 있다.
  - ASLR : 컴파일 할 때마다 버퍼의 주소가 계속해서 바뀌는 보호 기법