1. **Отладчик** - инструмент для пошагового выполнения программы, анализа состояния переменных и поиска ошибок.
2. **Разница**: отладчик работает с выполняемой программой, дизассемблер преобразует машинный код в ассемблер.
3. **Типы ошибок**: логические, исключения, утечки памяти, бесконечные циклы.
4. **Точка останова** - метка, где программа приостанавливает выполнение для анализа.
5. В VS: F5 или Debug → Start Debugging.
6. **Команды**: Step Into (F11) - войти в функцию, Step Over (F10) - пропустить функцию, Continue (F5) - продолжить.
7. Через окна Locals, Autos или Watch.
8. **Watch-окно** - для отслеживания конкретных переменных/выражений.
9. Использовать трассировку и проверять состояние перед падением.
10. **Дизассемблер** - инструмент для преобразования машинного кода в ассемблер.
11. Ghidra, IDA Pro, radare2, Hopper.
12. Искать entry point или строку "main" в символах.
13. Анализируя сравнения строк и условные переходы.
14. Через импортируемые функции или секции PE/ELF.
15. Установить точку останова перед делением, проверить значение делителя.
16. Анализ дизассемблированного кода и восстановление логики.
17. По именам функций, вызовам API, строковым константам.
18. По наличию криптографических функций (AES, RSA и т.д.).
19. Анализ поведения, вызовов API, скрытых функций.
20. **Статический** - анализ без выполнения, **динамический** - во время работы.
21. Не использовать для взлома ПО, соблюдать законы об авторских правах.