Задание по анализу защищенности с использованием Kali Linux и Damn Vulnerable Linux (DVL):

Развертывание и настройка

1. **Установка ВМ (Виртуальных Машин):**
   - **Kali Linux:** Установка виртуальной машины с Kali Linux, настройка сетевых интерфейсов, обновление системы и установка необходимых пакетов.
   - **Damn Vulnerable Linux (DVL):** Установка DVL на отдельной виртуальной машине, настройка для тестирования безопасности.

Задачи по анализу защищенности

2. **Сканирование Сети и Уязвимостей:**

   - **Инструменты: Nmap, OpenVAS**
   - **Задачи:**
     - Проведение сканирования портов и сервисов на DVL с использованием Nmap.
     - Выполнение сканирования уязвимостей на DVL с помощью OpenVAS.

3. **Пентестинг Веб-Приложений:**

   - **Инструменты: Burp Suite, OWASP ZAP**
   - **Задачи:**
     - Тестирование веб-приложений на DVL, используя инструменты перехвата и анализа трафика.
     - Выявление уязвимостей веб-приложений, таких как SQL-инъекции, XSS (Cross-Site Scripting), CSRF (Cross-Site Request Forgery).

4. **Анализ Безопасности Системы:**

   - **Инструменты: Metasploit, John the Ripper**
   - **Задачи:**
     - Использование Metasploit для эксплуатации известных уязвимостей в DVL.
     - Применение John the Ripper для взлома паролей и анализа политик безопасности паролей.

5. **Сетевая Защита и Защита От Вторжений:**

   - **Инструменты: Wireshark, Snort**
   - **Задачи:**
     - Мониторинг сетевого трафика с помощью Wireshark для обнаружения подозрительных действий.
     - Настройка и использование Snort как системы обнаружения вторжений (IDS) для мониторинга и алертинга о попытках взлома.

Заключительный Этап

6. **Отчетность и Анализ:**

- **Задача:**
  - Подготовка отчетов по каждому виду тестирования, анализ результатов и разработка рекомендаций по улучшению безопасности.