**Лабораторная работа №2 – «Анализ защищенности»**

**2 балла**

*Часть 1. Разведка + поиск уязвимостей*

1. На отдельной виртуальной машине развернуть два различных уязвимых веб-сервера (примеры: https://github.com/digininja/DVWA, https://github.com/OWASP/Vulnerable-Web-Application, интересная CTF-задача на Web или Infra, уязвимая версия CMS / ПО для системного администрирования, мониторинга, прочего корпоративного назначения – по вопросу выбора можно уточнить у преподавателя). Основное требование: уязвимости на разворачиваемых сервисах должны быть различны. Вместо одного из веб-серверов может быть развернут другой уязвимый сервис (по согласованию).
2. Провести активное сканирование сервера с помощью различных инструментов (netcat, nmap, httprint, hping3, nikto, OWASP Amass, OWASP ZAP, p0f, sqlmap, acunetix, openvas, nessus, nuclei и т. п.) для определения операционной системы, версий установленного ПО и поиска уязвимых сервисов.
3. Проэксплуатировать найденные уязвимости сервисов.
4. В отчете описать результат проведения разведки, шаги, которые привели к обнаружению уязвимого сервиса, а также шаги эксплуатации и необходимые меры по устранению уязвимости на уровне сервиса.

*Часть 2. Анализ критичности и описание рекомендаций по повышению уровня защищенности*

1. Описать потенциальный ущерб, к которому может привести раскрытие или злонамеренное использование информации, полученной в результате анализа защищенности сетевого узла.
2. Сформулировать рекомендации по повышению защищённости конкретного сервиса, а также сетевого узла.
3. Ответить на вопрос – применение каких средств защиты информации позволило бы противодействовать:
    a. Эксплуатации уязвимости злоумышленником;
    b. Закреплению злоумышленника на сетевом узле / в рамках сервиса;
    c. Потенциальному продвижению злоумышленника по корпоративной сети.

В ходе анализа критичности необходимо сделать упор на назначение развернутого сервиса: как именно он применялся бы в корпоративной среде, к чему привела бы его компрометация с точки зрения бизнес-процессов.