Домашнее задание

Дисциплина	Технологии детектирования атак и управления инцидентами
Тема	Тестирование внешнего периметра и веб-ресурсов
Форма проверки	**Самопроверка. Студент выполняет задание и самостоятельно проверяет его с помощью чек-листа**
Имя преподавателя	Дмитрий Курамин
Время выполнения	120 минут
Цель задания	1. Научиться получать из открытых источников информацию о сетевой инфраструктуре компании. 2. Познакомиться с инструментами автоматизированного и ручного выявления уязвимостей веб-приложений
Инструменты для выполнения ДЗ	Google Документы, ASN Lookup, Censys, smap, RiskIQ, gowhitness, LeakCheck
Правила приёма работы	1. Выполните все предлагаемые этапы задания. 2. Загрузите файл с отчётом на Google Диск и прикрепите ссылку на файл с выполненным заданием в LMS. Важно: убедитесь, что по ссылке есть доступ. Название файла должно содержать фамилию и имя студента, номер ДЗ
Критерии оценки	**Задание считается выполненным, если:** ● прикреплена ссылка на файл с выполненным заданием; ● доступ к материалам открыт; ● выполнены требования чек-листа самопроверки. **Задание не выполнено, если:** ● файл с заданием не прикреплён или отсутствует доступ по ссылке
Дедлайн	Срок сдачи — 7 дней, т. е. до следующего вебинара

Описание задания

Перед выполнением задания посмотрите запись лекции по теме 4 «Тестирование внешнего периметра и веб-ресурсов».

Этап 1
Выберите любую организацию для анализа.

Этап 2
Используя инструмент ASN Lookup, или любой аналогичный инструмент на ваше усмотрение, выполните поиск IP-адресов выбранной организации.
Результаты поиска занесите в отчёт (этап 7).

Этап 3
Используя собранные на втором этапе диапазоны IP-адресов, найдите:

- хосты, доступные в интернете, с помощью инструмента Censys;
- доступные сетевые устройства с помощью инструмента smap.

Результаты поиска занесите в отчёт (этап 7).

Пример поискового запроса:
10.11.0.0/16
ip: 10.11.0.0/16
Важно: *без регистрации Censys обрабатывает только 10 запросов в день с одного IP-адреса. При регистрации — 250 запросов в месяц.*

Этап 4
Используя основной домен организации, найдите поддомены с помощью сервиса RiskIQ.
Результаты поиска занесите в отчёт (этап 7).

Этап 5
Воспользуйтесь инструментом gowhitness для сбора скриншотов об анализируемой организации.
Пример команды: gowhitness -D ./task.sqlite3 scan --cidr=10.11.12.0/24
Пример команды экспорта результатов: gowhitness -D ./task.sqlite3 report export -f ./result.zip
Результаты поиска занесите в отчёт (этап 7).

Этап 6
Используя сервис LeakCheck, попробуйте найти утечки учётных записей электронной почты сотрудников анализируемой организации, если у вас есть данные электронной почты. Если нет данных электронной почты сотрудников, то проверьте свой или любой интересующий вас адрес электронной почты на утечки.
Важно: *для работы с инструментом LeakCheck нужна регистрация.*
Результаты поиска занесите в отчёт (этап 7).

Этап 7
Подготовьте краткий отчёт по сбору данных. Отчёт выполняется в Google Документе.
В отчёте вы можете использовать следующие таблицы.

Таблица 1 — Перечень обнаруженных открытых портов

№п/п	Хост/Порт	Протокол	Сервис	Баннер
Пример	*127.0.0.1/25*	*tcp*	*smtp*	*Microsoft Exchange smtpd*

Таблица 2 — Перечень обнаруженных утечек учётных записей электронной почты

№п/п	Обнаруженные адреса электронной почты	Источник утечки	Дата последней утечки

Чек-лист самопроверки

Критерии выполнения задания	Отметка о выполнении
Выбрана организация для анализа	
Выполнен поиск диапазонов IP-адресов организации	
Найдены доступные в интернете хосты и внесены в отчёт	
Найдены доступные сетевые устройства и внесены в отчёт	
Найдены поддомены организации и внесены в отчёт	
Выполнен сбор скриншотов об анализируемой организации, скриншоты представлены в отчёте	
Найдены скомпрометированные учётные записи или проверен свой адрес электронной почты на утечки, заполнена таблица 2 в отчёте	
Подготовлен краткий отчёт по сбору данных в Google Документе	
Файл доступен для просмотра другим пользователям, название файла содержит фамилию и имя студента, номер ДЗ	
В LMS прикреплена ссылка на файл	