Правительство Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»
(НИУ ВШЭ)

Московский институт электроники и математики им. А.Н. Тихонова

ОТЧЕТ
О ДОМАШНЕМ ЗАДАНИИ №6

по дисциплине «Технологии детектирования атак и управления инцидентами»

Студент гр. МКБ242_
_____ Макаров М.В.
«_16_» ____ноября____ 2025 г.

Москва 2025

Задание 1

Вы эксперт центра мониторинга событий информационной безопасности.

Чтобы повысить безопасность, в компании решили организовать подключение сотрудников с использованием технологии VPN. Авторизация при подключении по VPN осуществляется с использованием доменной УЗ. Так как процесс перевода сотрудников на VPN идёт не очень быстро, возникает риск, что сотрудники будут делиться своими УЗ для доступа по VPN к корпоративным ресурсам между собой, а это грубое нарушение политики ИБ компании. Вам поручили отслеживать подобные ситуации и расследовать каждый случай. Чтобы отследить эту активность, вы решаете сделать правило на SIEM-системе. В вашем распоряжении есть SIEM-система и логи VPN-сервера, также к SIEM-системе подключена база GeoIP.

Входные данные:

1. Логи VPN-сервера:
    - события **login** (вход в систему) **и keep-alive** (активная сессия)
    - user_id – имя пользователя
    - IP – ip-адресс сессии
    - timestemp – время начала сессии
2. База данных GeoIP

Основная логика правила

1. На вход подаются (анализируются) логи VPN сервера с полем **LOGIN, Result = Success** (то есть успешная установка подключения к серверу). Также анализируются записи с полем **keep-alive** (сессия активна/поддерживается)
2. Далее по двум разным веткам анализируем логи с полем **LOGIN&Result = Success** и с полем **KEEP-ALIVE –** то есть анализируем, только логи с вышеуказанными полями.
3. Если во временном промежутке 5 часов (продолжительность активного трудового дня) детектируется две и более записи с полем **LOGIN&Result = Success,** в которых поля **user** совпадают, то:
    - Если ip-адреса выявленных логов одинаковые – пропуск
    - Если ip-адреса в логах разные – проверяем адреса по базе GeoIP:
        - Если адреса принадлежат разным городам/странам – генерация инцидента ИБ
        - Если расстояние между точками >100км – генерация инцидента
        - Если расстояние между точками <100км – пропуск
4. Каждые 20 минут анализируются логи с полем **KEEP-ALIVE**
5. Если выявляются две записи с одинаковым полем **user,** а время между ними < 20 минут:
    - Если ip-адреса выявленных логов одинаковые – пропуск
    - Если ip-адреса в логах разные – проверяем адреса по базе GeoIP:
        - Если адреса принадлежат разным городам/странам – генерация инцидента ИБ
        - Если расстояние между точками >100км – генерация инцидента
        - Если расстояние между точками <100км – пропуск

Псевдокод

Для каждого события VPN (**LOGIN** или **KEEP-ALIVE**):
  Сохраняем запись {**user**, **IP**, **timestamp**}
Для каждого пользователя:
  Для каждого типа события:
    Определяем окно анализа:

- **LOGIN** → последние 5 часов
- **KEEP-ALIVE** → последние 20 минут

Находим все сессии за это окно
Если найдено >1 сессии:
  Для каждой пары сессий:
    Если **IP** одинаковые:
      Пропуск
    Иначе:
      Проверяем GeoIP(**IP**)
      Если города/страны разные или расстояние >100 км:
        Генерируем инцидент

Задание 2
Вы эксперт центра мониторинга событий информационной безопасности. В вашей компании решили повысить безопасность корпоративной сети и отказаться от использования протоколов FTP и Telnet.

Вам поручили отслеживать появление и использование подобных сервисов в сети компании. В вашем распоряжении есть SIEM-система и логи следующих устройств: NGFW (МСЭ нового поколения) и masscan (сканер портов). Masscan ежедневно сканирует всю корпоративную сеть на наличие открытых портов.

Чтобы выявить использование FTP и Telnet, вы решаете сделать правило на SIEM-системе.

Нужно
Разработать правило корреляции для выявления использования протоколов FTP и Telnet в корпоративной сети.

Входные данные

1. Логи NGFW:

    - src_ip — IP источника
    - dst_ip — IP назначения
    - dst_port — порт назначения
    - service / application — идентифицированный сервис (FTP, Telnet)
    - timestamp — время события
    - action — allow/deny

2. Результаты сканирования masscan:

    - ip — IP хоста
    - port — открытый порт
    - state — open/closed
    - timestamp — время сканирования

Основная логика правила

1. На вход правила подаются логи NGWF и результат ежедневного сканирования сети утилитой masscan. Проверка происходит каждый час.
2. Если в логах NGWF обнаруживается записи типа “dst_port=21”, “dst_port=22” или service или application = FTP или Telnet при условии, что action в поле лога = allow:
    - Генерация инцидента о фактическом использовании запрещенных сервисов
    - Иначе – пропуск
3. В то же время, если в логах утилиты masscan обнаруживается запись типа «Discovered open port 21/tcp on 192.168.1.10», которая включает в себя номер порта 21 или 23, а также статус open:
    - Генерация инцидента

Псевдокод

```
Для каждого часа:
   Получаем все новые записи логов NGWF
   Получаем новые результаты сканирования masscan

Для каждого события в логах NGWF:
   Если dst_port ∈ {21, 23} и action = allow:
      Создать инцидент «Использование запрещённого сервиса»
   Иначе если service ∈ {FTP, Telnet} или application ∈ {FTP, Telnet} и action = allow
      Создать инцидент «Использование запрещённого сервиса»
   Иначе
      Пропуск

Для каждого результата masscan:
   Если статус = open
      Если порт ∈ {21, 23}
         Создать инцидент «Обнаружен открытый запрещённый порт»
      Иначе
         Пропуск
   Иначе
      Пропуск
```

Задание 3
Вы руководитель команды пентестеров. В команде кроме вас ещё три человека: Пётр Петров (p.petrov@test.mail), Иван Иванов (i.ivanov@test.mail), Семён Семёнов (s.semenov@test.mail).
Заказчик пентеста хочет, чтобы вы приступили к работам как можно быстрее, потому что стремится закончить до конца года, а договор подписывать не меньше месяца.
Заказчик хочет, чтобы вы протестировали 2 веб-сайта (my_best_site.site и payment_system.site) и 3 внешние подсети (192.219.154.0/24, 10.234.14.0/27 и 172.20.155.0/32) и начали со следующей недели (21 ноября 2025 года).
Нужно
Составить и отправить заказчику на подписание авторизационное письмо для начала работы в указанную дату

Авторизационное письмо (для подписания заказчиком)

От:
ООО «ПентестЛаб»
Руководитель команды пентестинга: Макаров М.В.
Email: <PentestLab@gmail.com>
Телефон: <8-945-67-84-15>

Кому:
АО «WebSuite»
Email: WebMSK@gmail.com

Дата: 17 ноября 2025 г.

Авторизационное письмо на проведение тестирования на проникновение

Уважаемые коллеги,

Направляю авторизационное письмо для подписания, необходимое для начала работ по внешнему тестированию на проникновение. Документ фиксирует область работ, сроки и параметры взаимодействия. После подписания с вашей стороны мы готовы начать тестирование в согласованную дату - **21 ноября 2025 года.**

1. Область работ

Тестирование проводится в отношении следующих ресурсов вашей компании:

Веб-сайты:

- my_best_site.site
- payment_system.site

Внешние подсети:

- 192.219.154.0/24
- 10.234.14.0/27
- 172.20.155.0/32

Разрешённые виды активности:

- сканирование разрешенных подсетей
- автоматизированное и ручное сканирование уязвимостей
- тестирование веб-приложений (OWASP)
- тестирование сетевой безопасности
- эксплуатация критических уязвимостей для подтверждения рисков
- предоставление технических доказательств (PoC)
- тестирование методом black-box

Запрещённые действия (если не будут отдельно согласованы):

- DDoS, стресс-тесты
- атаки, способные нарушить доступность сервисов
- изменения конфигурации тестируемых систем
- переводы денежных средств
- разглашения персональных данных, обнаруженных в ходе работ
- разглашение результатов тестирования третьим лицам

2. Сроки проведения работ

Период действия данного разрешения:

- начало: **21 ноября 2025 года**
- окончание: **30 декабря 2025 года**

3. Информация об исполнителе

Команда пентеста:

- Макаров Максим — руководитель проекта
- Пётр Петров — p.petrov@test.mail
- Иван Иванов — i.ivanov@test.mail
- Семён Семёнов — s.semenov@test.mail

Исходящие IP-адреса исполнителя:

- 91.203.52.184
- 176.59.148.27
- 54.93.218.44
- 185.112.37.90

Контакт для экстренной связи (24/7):

- 8-800-555-35-35

4. Контакты со стороны заказчика (заполняет заказчик)

ФИО ответственного лица: _____
Телефон: _____
Email: _____

5. Подтверждение и разрешение

Настоящим документом АО «WebSuite» подтверждает, что:

- владеет или управляет указанными ресурсами
- предоставляет исполнителю ООО «ПентестЛаб» в лице руководителя Макарова М.В. право проводить тестирование на проникновение
- уполномоченный подписант имеет право оформлять подобные разрешения
- осознаёт риски, связанные с тестированием
- разрешает команде ООО «ПентестЛаб» выполнить работы в пределах указанного объёма и сроков.

Подпись заказчика

Заказчик:
_____ / <ФИО подписанта>
Должность: <должность>
Подтверждаю полномочия.
Дата: «___» _____ 2025 г.

М.П. (при необходимости)