Домашнее задание

Дисциплина	Технологии детектирования атак и управления инцидентами
Тема	Введение в тестирование на проникновение и детектирование атак
Форма проверки	Проверяет преподаватель
Имя преподавателя	Геннадий Шастин
Время выполнения	120 минут
Цель задания	1. Научиться составлять правила корреляции. 2. Научиться составлять составлять авторизационное письмо для пентеста
Инструменты для выполнения ДЗ	Google / Яндекс Документы, любой инструмент для составления схем, например app.diagrams.net
Правила приёма работы	1. Выполните все предлагаемые задания. 2. Загрузите файл с выполненным заданием на Google Диск и прикрепите ссылку на файл в LMS. Важно: убедитесь, что по ссылке есть доступ. Название файла должно содержать фамилию и имя студента, номер ДЗ
Критерии оценки	**Задание оценивают по 10-балльной шкале.** **Задание считается выполненным, если:** ● выполнены все предлагаемые задания; ● прикреплена ссылка на файл с выполненным заданием; ● доступ к материалам открыт. **Задание не выполнено, если:** ● файл с заданием не прикреплён или отсутствует доступ по ссылке
Дедлайн	Срок сдачи: 14 дней после вебинара

Прежде чем выполнять задание, посмотрите:

- лекции по теме 1 «Детектирование атак» (обратите внимание на разобранные примеры правил корреляции), теме 2 «Законодательное обеспечение пентеста» (обратите внимание на раздел 2);
- запись вебинара 1 «Введение в тестирование на проникновение и детектирование атак».

Описание заданий

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.

Нужно

Разработать правило корреляции для выявления двух одновременных сессий одного и того же пользователя из разных локаций.

Важно: чтобы составить схему правила корреляции, вы можете воспользоваться app.diagrams.net

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.

Важно: чтобы составить схему правила корреляции, вы можете воспользоваться app.diagrams.net

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 2022 года).

Нужно

Составить и отправить заказчику на подписание авторизационное письмо для начала работы в указанную дату.

Критерии оценки задания

Задания	Критерии оценки	Максимальный балл
Задание 1	Оценивают точность идентификации сессий пользователя, оптимальность и универсальность предложенного алгоритма, рекомендации для дальнейших действий	3
Задание 2	Оценивают точность выявления использования протоколов FTP и Telnet, оптимальность и универсальность предложенного алгоритма, рекомендации для дальнейших действий	3
Задание 3	Оценивают: - полноту информации о предполагаемой работе; - точность и полноту контактной информации; - стиль и оформление авторизационного письма; - корректность, полнота и правильность формулировок	2
Итого		8 баллов

Максимально по этим критериям можно набрать 8 баллов — это соответствует пятёрке.
Преподаватель может добавить баллы и поставить 9 или 10, если работа выполнена сверх ожиданий и выходит за рамки программы.