ШИФР УЧАСТНИКА _____

Всероссийская олимпиада школьников

МУНИЦИПАЛЬНЫЙ ЭТАП, 2024-2025 учебный год

Профиль «Информационная безопасность»

Задание практического тура

10-11 КЛАСС

Участнику предоставляется компьютер с установленным приложением Wireshark и файл: **ИБ практика 10-11 классы Идентификация подозрительных пакетов.pcap**

ЗАДАНИЕ:

0. Откройте файл в Wireshark, проанализируйте сетевые пакеты и ответьте на вопросы:

1. Найдите и перечислите все типы протоколов, которые используются в захваченном трафике (например, TCP, UDP, ICMP и пр.).

2.1. Определите, сколько подозрительных пакетов было захвачено, которые могут указывать на возможные атаки.

2.2. Определите, в чем заключалась кибератака и чем она опасна.

3. Определите, на какой компьютер производилась атака? Укажите его:

3.1. MAC-адрес

3.2. ip-адрес

3.3. порт, на который производилась атака

4. Подготовьте отчет с описанием обнаруженных подозрительных действий и рекомендациями по их предотвращению.

5. Какие ещё виды атак на протокол TCP Вы знаете? В чем они заключаются?

(Запишите ответы на следующей странице и передайте эксперту)

Шифр участника _____

Всероссийская олимпиада школьников

МУНИЦИПАЛЬНЫЙ ЭТАП, 2024-2025 учебный год

Профиль «Информационная безопасность»

Критерии оценки практического тура

10-11 КЛАСС

№	Критерии оценки практического тура	Кол-во баллов	Факт. кол-во баллов
1	**Правильный ответ:** В захваченном трафике используются 6 видов протоколов: ARP, ICMP, ICMPv6, MDNS, SSDP, TCP ***За каждый правильно определенный протокол начисляется по 1 баллу***	0-6 баллов	
2.1	**Правильный ответ:** Из записанных 906 пакетов 598 пакетов содержали SYN-запросы (запросы на подключение по протоколу TCP) в течение короткого времени от разных источников. ***За правильное определение числа подозрительных пакетов начисляется 1 балл; если нет – 0 баллов***	0-1 балл	
2.2	***За правильное «по смыслу» описание угрозы кибератаки начисляется 10 баллов.*** Пример: •«Принцип атаки заключается в том, что злоумышленник посылает огромное количество запросов установки соединения на атакуемый сервер. Сервер, видя сегменты с флагом SYN, выделяет необходимые ресурсы для поддержания соединения и отправляет в ответ сегменты с флагами SYN и ACK, переходя в состояние SYN-RECEIVED (такое состояние еще называют полуоткрытым соединением). •При этом злоумышленник игнорирует SYN+ACK пакеты цели, не высылая ответные пакеты, либо подделывает заголовок пакета таким образом, что ответный SYN+ACK отправляется на несуществующий адрес. В очереди подключений появляются полуоткрытые соединения, ожидающие подтверждения от клиента. •По истечении определенного тайм-аута эти подключения отбрасываются. Задача злоумышленника заключается в том, чтобы поддерживать очередь заполненной таким образом, чтобы не допустить новых подключений. •Из-за этого клиенты, не являющиеся злоумышленниками, не могут установить связь, либо устанавливают её с существенными задержками.» ***За неполное, фрагментарное описание начисляется 5 баллов.*** Пример: «SYN — разновидность сетевых атак типа отказ от обслуживания, которая заключается в отправке большого количества SYN-запросов в достаточно короткий срок» ***Если нет описания – 0 баллов***	0-10 баллов	

Шифр участника _____

3.1	**Правильный ответ:** MAC-адрес: eth.addr == 78:8c:b5:d7:18:a2 ***За правильное определение начисляется 1 балл; если нет – 0***	0-1 балл	
3.2	**Правильный ответ:** ip-адрес: ip.dst == 192.168.88.5 ***За правильное определение начисляется 1 балл; если нет – 0***	0-1 балл	
3.3	**Правильный ответ:** Порт: tcp.dstport == 80 ***За правильное определение начисляется 1 балл; если нет – 0***	0-1 балл	
4	***За наличие развернутого отчета и рекомендаций участника начисляется 10 баллов.*** Пример развернутого отчета и рекомендаций: «Использовать SYN-cookie. Когда к нам приходит SYN-запрос мы не создаем новое соединение, а отправляем SYN-ACK-ответ клиенту, где в поле Sequence Number кодируем данные о данном соединении. Если мы получаем ACK ответ от клиента, то из поля Acknowledgment Number восстанавливаем данные о соединении. Данный метод хорош тем, что мы более не будем выделять ресурсы, как только к нам придет SYN-запрос. Но есть и очевидный минус: если наш пакет затеряется, или подвергнется искажению, то мы не сможем отправить его повторно, так как информацию о соединении мы условились не сохранять.» ***За наличие краткого отчета и рекомендаций участника начисляется 5 баллов.*** Пример краткого отчета и рекомендаций: «Во-первых, можно увеличить количество полуоткрытых TCP-соединений и уменьшить время, в котором сокет может пребывать в состоянии SYN-RECEIVED» ***Если нет отчета и рекомендаций – 0 баллов***	0-10 баллов	
5	***За наличие дополнительных примеров кибератак на протокол TCP начисляется 5 баллов.*** Примеры описаний: TCP reset. Атака, при которой злоумышленник отправляет TCP-сегмент с флагом RST одному из участников соединения, что трактуется модулем TCP, как аварийное закрытие соединения. TCP hijalking. Атака, при которой злоумышленник вклинивается в соединение, маскируя свои пакеты под пакеты законного пользователя, тем самым поставляя жертве собственные данные. Повторение TCP сегментов. Атака, при которой злоумышленник перехватывает весь траффик, исходящий с одного источника, а затем, инициируя соединение, повторяет их вновь. ***Если нет дополнительных примеров – 0 баллов***	0-5 баллов	
	ИТОГО	**35**	