МИНОБРНАУКИ РОССИИ

Федеральное государственное автономное образовательное

учреждение высшего образования

«Южный федеральный университет»

Институт высоких технологий и пьезотехники

Лабораторная работа

По теме «Виды кибер-атак»

По дисциплине «Компьютерная безопасность»

Выполнил:

Студент 4 курса бакалавриата 6 группы

Едленко С.А.

Проверил:

Сажин С. Л.

Ростов-на-Дону

2022 г.

Таблица 1 – план информационных атак и уровень классификации osi, на которые атака была нацелена.

|  |  |  |  |
| --- | --- | --- | --- |
| Уровень классификации osi | Название атаки или описание | Поврежденные составляющие инф. безопасности | Способы защиты |
| L1 | Выключение питания | Доступность | Охрана значимых узлов электропроводов |
| L2 | Перехват DHCP | Конфиденциальность | включение на всех коммутаторах функции DHCP snooping |
| L3 | Перехват routing | Конфиденциальность | Осуществление технологии шифрования на 3 уровне, таких как IPSec |
| L5 | MITM https | Конфиденциальность | Подключайтесь только к защищенным маршрутизаторам Wi-Fi или используйте зашифрованное соединение вашего оператора беспроводной связи. Подключайтесь к маршрутизаторам, которые используют протокол безопасности WPA2. Он не обеспечивает абсолютной безопасности, но всё же это лучше, чем ничего.  Используйте VPN для шифрования трафика между конечными точками и сервером VPN (в корпоративной сети или в интернете). Если трафик зашифрован, «человеку посередине» сложнее его перехватить или изменить.  Используйте сквозное шифрование для электронной почты, чата и видеосвязи (Zoom, Teams и т. д.)  Обновляйте систему для защиты от вредоносных программ  Используйте менеджер паролей, чтобы защитить свои пароли и предотвратить их повторное использование.  Подключайтесь только к HTTPS-соединениям, используйте плагин браузера для контроля выполнения этого правила.  Используйте многофакторную аутентификацию везде, где это возможно.  Используйте DNS поверх HTTPS — технологию, которая защищает вас от перехвата DNS путем шифрования ваших DNS-запросов.  Следуйте принципам «нулевого доверия», чтобы создать внутренние барьеры для доступа к данным, которые не позволяют злоумышленникам свободно перемещаться по сети, даже если они проникнут внутрь. |
| L2 | Атака шторм | Доступность | сегментирования сети посредством VLAN  использовать протоколы FHRP и U-образную топологию на уровне доступа |
| L7 | Подмена сервера HTTP | Конфиденциальность | Проверка валидности сертификатоа |
| L8 | Соц. Инженерия |  | Подготовка сотрудников к подобному виду атак |
| L7 | SQL injection | Целостность | Не использовать динамических запросов к базе. Не использовать пользовательских данных в запросах |
| L7 | SSH exploit (RND) | Конфиденциальность | Изучение уязвимостей используемых решений и предотвращение возможности их использования |

**Вывод:** в ходе лабораторной работы были изучены различные виды кибер-атак, их характеристики и способы защиты от них.