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

Кузьменко П.М.

Проверил:

Сажин С. Л.

Ростов-на-Дону

2022 г.

**Цель работы:** изучить различные виды кибер-атак, их характеристики и способы защиты от них

**Ход работы:**

Таблица 1 – Выявленные атаки.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№** | **Название атаки** | **На что идет атака** | **Влияние на** | **Уровень** | **Как избежать** |
| **1** | Выключение сети | Сеть инфраструктуры | Работоспособность сети | Физический (1) | Обезопасить доступ к кабелям сети |
| **2** | Перехват DHCP | Элементы сети (компьютеры) | *Для пользователя:* ни на что  *Для сети:* адрес сервера переназначен на адрес злоумышленника | Канальный (2) | Не допускать включение новых устройств в сеть.  Проверять Boot Request’ы при включении сети через WireShark |
| **3** | Перехват routing | Трафик сети | *Для пользователя:* ни на что  *Для сети:* весь трафик становится читаемым, передача данных в открытом виде может быть опасна | Сетевой (3) | Следить за элементами узлами, через который протекает весь трафик.  Шифровать весь поток данных |
| **4** | MITM https | Каналы передачи | Для пользователя: ни на что  Для сети: весь трафик проходит через дополнительный узел сети, тем самым асимметричное шифрование теряет свой смысл | Сеанс (5) | Внедрить подписанный сертификат.  Объяснить пользователям, что принимать другие сертификаты нельзя |
| **5** | Шторм атака | Сеть инфраструктуры | Работоспособность сети (пропускная способность сети снижается: всё не отвечает) | Канальный (2) | Правильно настроить порты в сети.  Ограничить максимальный трафик для пользователя.  Отслеживать трафик и своевременно блокировать подозрительные IP. |
| **6** | Подмена сервера http | Элементы сети (компьютеры) | *Для пользователя:* ни на что  *Для сети:* адрес сервера переназначен на адрес злоумышленника | Прикладной (7) | Своевременно отслеживать сетевой трафик |
| **7** | Social engineering | Пользователь | Безопасность всей информации | - | Нанимать грамотных сотрудников.  Все передачи важных данных осуществлять только при ведении документации |
| **8** | SQL injection | База данных | База данных | Прикладной (7) | Переписать систему с учетом SQL-инъекций |
| **9** | SSH exploit | Трафик сети | *Для пользователя:* ни на что  *Для сети:* злоумышленник способен управлять устройствами в сети | Прикладной (7) | Использовать другие алгоритмы, с большей вариацией ключей |

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