**МИНОБРНАУКИ РОССИИ**

**Федеральное государственное автономное образовательное  
 учреждение высшего образования   
«Южный федеральный университет»**

**Институт высоких технологий и пьезотехники**



Кафедра информационных и измерительных технологий

Направление: 09.03.03 "Прикладная информатика"

**Компьютерная безопасность и защита информации Отчёт по лабораторной работе №5**

**«Виды кибер-атак в сети интернет»**

Выполнил студент группы 4.6

Кузин М.А.

Принял

Сажин С. Л.

**Ростов-на-Дону**

**2022**

**Цель работы:**

Изучить основные виды кибер-атак в сети интернет, их характеристики и способы защиты от них.

**Ход работы:**

***Выключение сети***

Атака проводится на провода в сети и источники питание, т.е. на системы энергоснабжения.

Уровень угрозы – 1.

Влияет на доступность сети пользователю.

Для защиты нужно достаточно контролировать энергоснабжение. Только распределенная, и даже индивидуальная система генерации электроэнергии исключают возможность воздействия кибератак на систему энергоснабжения. Если у каждого есть свой собственный источник генерации электроэнергии, никакие кибератаки не могут привести к сбоям подачи электроэнергии и потребитель энергетически независим. Также необходим опытный сисадмин.

***Перехват DHCP***

Как правило для проведения такой атаки сначала происходит истощение DHCP основного сервера путем большого количество рассылок. После происходит подмена DHCP сервера и все пакеты данных проходят через шлюз злоумышленника.

Лишает конфиденциальность пользователя.

Уровень атаки – 2.

Избегать данных атак можно конфигурируя оборудование самостоятельно, а также проверкой изменения ip-адресов.

***Перехват routing***

Атака идет на отправляемые пакеты.

Лишает конфиденциальности пользователя.

Уровень атаки – 2.

Избежать можно проверкой сертификатов.

***MITM https***

Вид атаки в криптографии и компьютерной безопасности, когда злоумышленник тайно ретранслирует и при необходимости изменяет связь между двумя сторонами, которые считают, что они непосредственно общаются друг с другом.

Лишает конфиденциальность пользователя.

Уровень атаки – 6.

Что можно предпринять:

* Анализируйте текущие WI-FI
* Проверять свою сеть на наличие вирусов-вымогателей.
* Использовать анализатор трафика для целей защиты.
* Анализировать активность сети.

Из признаков данной атаки можно отметить:

* Неожиданное или повторное отключение
* Странные адреса в адресной строке браузера
* Незащищенный WI-FI

Для предотвращения:

* Подключайтесь только к защищенным WI-FI
* Подключайтесь только к HTTPS
* Используйте DNS поверх HTTPS
* Используйте VPN для шифрования трафика
* Используйте менеджер паролей
* Используйте многофакторную аутентификацию
* Следуйте принципам «нулевого доверия»
* Осуществляйте мониторинг активности сети

***Шторм***

Атака на сервер.

Лишает доступа пользователя к серверу.

Уровень атаки – 6.

Необходимо отметить, что в существующем стандарте сети Internet IPv4 пет приемлемых способов надежно обезопасить операционную систему от этой удаленной атаки. К счастью, взломщик не сможет получить несанкционированный доступ к вашей информации, а только "съест" вычислительные ресурсы вашей системы и нарушит ее связь с внешним миром.

***Подмена сервера http***

Подмена сервера доменных имен (DNS) — это кибератака, с помощью которой злоумышленник направляет трафик жертвы на вредоносный сайт (вместо легитимного IP-адреса). Злоумышленники используют метод «отравления» кэша DNS для перехвата интернет-трафика и кражи учетных данных или конфиденциальной информации. Отравление кэша DNS и подмена DNS — тождественные понятия, часто используемые как синонимы. Хакер хочет обманом заставить пользователей ввести личные данные на небезопасном сайте. Как ему этого добиться? С помощью отравления кэша DNS. Для этого хакер подменяет или заменяет данные DNS для определенного сайта, а затем перенаправляет жертву на сервер злоумышленника вместо легитимного сервера. Таким образом хакер добивается своей цели, ведь перед ним открываются широкие возможности: он может совершить фишинговую атаку, украсть данные или даже внедрить в систему жертвы вредоносную программу.

Атака на места хранения данных, ведущих к реальному серверу.

Лишает конфиденциальности пользователя.

Уровень атаки – 4.

Избежать можно наличием бэкапов и сверки данных с ними. В случае пользователя нужно быть внимательным и вводить свои данные только после проверки данных сайта.

***Social engineering***

Атака производится на человека, который сам раскрывает данные, либо предоставляет доступ к сервису.

Лишает конфиденциальность сервиса и его пользователя.

Избегать можно будучи бдительным, а также проводя работу с персоналом.

***Sql injection***

Атака на базу данных, которая позволит выполнить некоторое действие, которое не планировалось создателем скрипта.

Лишает конфиденциальности пользователя.

Уровень атаки – 5.

Избегать можно протестировав фильтр запросов.

***SSH exploit***

Использование уязвимостей ОС.

Нарушает целостность системы.

Уровень атаки – 2.

Для предотвращение данной атаки нужно обновлять ОС, использовать различные пароли.

**Вывод:**

В ходе лабораторной работы были изучены основные виды кибер-атак в сети интернет, их характеристики и способы защиты от них.