МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
Дальневосточный федеральный университет

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

Кафедра информационной безопасности

О Т Ч Е Т

о прохождении учебной (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практики

Выполнил студент
гр. С8118-10.05.01-1СПЕЦ
_____ Башкатов М. А.
(подпись)

Отчет защищен с оценкой

_____
_____ С.С. Зотов
(подпись) (И.О. Фамилия)
« 31 » июля 2021 г.

Руководитель практики
Старший преподаватель кафедры
информационной безопасности ШЕН
_____ С.С. Зотов
(подпись) (И.О. Фамилия)

Регистрационный № _____
« 31 » июля 2021 г.

_____ Е.В. Третьяк
(подпись) (И.О. Фамилия)

Практика пройдена в срок
с « 19 » июля 2021 г.
по « 31 » июля 2021 г.
на предприятии
Кафедра информационной безопасности ШЕН ДВФУ

г. Владивосток
2021

Оглавление

Задание на практику

- Проведение исследования DDoS и способах защиты от него.

- Написание отчета по практике о проделанной работе.

Введение

Учебная (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практика проходила на кафедре информационной безопасности ШЕН ДВФУ в период с 19 июля 2021 года по 31 июля 2021 года.

Целью прохождения практики является приобретение практических и теоретических навыков по специальности, а также навыков оформления проведенного исследования в отчетной форме.

Задачи практики:

1. Ознакомиться с DDoS и статистическими данными по его атакам.

2. Ознакомиться с типами DDoS атак и защитой от них.

3. На основе полученных знаний написать отчет по практике о проделанной работе.

Основные противодействия DDoS атакам

Аннотация: В статье предоставлена информация о DDoS. Проанализирована информация о типах DDoS атак, а также предоставлена информация о всех возможных способах защиты от всех возможных атак.

Основная информация

DDoS-атака – распределенная атака, направленная на отказ в обслуживании. В результате атаки такого типа атакуемый сетевой ресурс получает лавинообразное количество запросов, которые не успевает обработать. Источником вредоносных запросов являются так называемые зомби-сети, состоящие большей частью из компьютеров обычных пользователей, в силу каких-то причин зараженных вредоносным ПО
DDoS-атака похожа на другую распространённую веб-угрозу — «Отказ в обслуживании» (Denial of Service, DoS). Единственное различие в том, что обычное распределенное нападение идет из одной точки, а DDos-атака более масштабна и идет из разных источников.

Ботнет –компьютерная сеть, состоящая из некоторого количества хостов с запущенными ботами – автономным программным обеспечением.
Доступность – состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие права доступа, могут реализовывать их беспрепятственно за удовлетворимое время.

IoT устройства – концепция вычислительной сети физических предметов, оснащѐнных встроенными технологиями для взаимодействия друг с другом или с внешней средой, рассматривающая организацию таких сетей как явление, способное перестроить экономические и общественные процессы, исключающее из части действий и операций необходимость участия человека.

Статистические данные

Рассмотрим Таблицу 1 (здесь и далее “q” обозначает номер квартала), данные собранны из официальных отчетов Kaspersky DDoS Protection, где можно наблюдать следующие скачки DDoS активности. Рассмотрим следующие события:

- 2018 год 4 квартал в США произошли промежуточные выборы;
- 2018 год 1 квартале в Россия проводились выборы президента РФ.

Эти данные явно показывают «всплески» активности DDoS атак в связи с значимыми событиями. Из чего следует, что атаки используются не только в коммерческих целях для получения материальной выгоды, но и в геополитике для достижения своих политических целей.

Таблица 1. –Процент DDoS атак на объекты информатизации стран по кварталам

	Китай	США	Гонконг	Великобритания	Канада	Вьетнам	Франция	Россия
2019 q2	63,8	17,57	4,61	1,2	0,93	0,68		
2019 q1	67,89	17,17	4,81	0,66	0,86	0,62	0,66	
2018 q4	50,43	24,9	1,84	2,18	1,94	0,85	0,93	
2018 q3	77,67	12,57	1,72	0,53	0,82	0,39	0,39	0,37
2018 q2	59,03	12,46	17,13	0,51	0,69	0,5	0,43	0,21
2018 q1	59,42	17,83	3,67	1,3	1,27	0,71	0,83	4,76
2017 q4	59,18	16	0,67	2,7	0,68	1,26	1,24	1,25
2017 q3	63,3	12,98	1,31	1,36	0,68	0,59	1,31	1,58
2017 q2	58,07	14,03	2,38	1,38	0,79		0,77	1,23
2017 q1	55,11	11,37	1,37	0,77	0,66	0,83	0,64	1,6

Влияние же на коммерческую составляющую также достаточно очевидно, помимо подрыва репутации из-за недоступности того или иного сервиса, собственники теряют прямую прибыль из-за простоя их оборудования и невозможности проводить операции.

Рассматривая данные по абсолютному количеству атак, приведенное в Таблице 2, количество атак снижается с каждым годом.

Таблица 2. –Абсолютное количество атак

2018 q3	2018 q4	2019 q1	2019 q2
46575	29161	18932	17035

В тоже время длительность атак с каждым кварталом увеличиваться, эти данные представлены в Таблице 3.

Таблица 3. –Максимальная продолжительность DDoS атаки в часах

2016 q4	2017 q1	2017 q2	2017 q3	2017 q4	2018 q1	2018 q2	2018 q3	2018 q4	2019 q1	2019 q2
92	20	77	15	46	97	58	39	89	29	09

Общая тенденция длительности всех атак приведена в Таблице 4, в ней же указаны процентные соотношения длительности атак.

Таблица 4. –Процентное соотношение продолжительности атак

	< 4	5–9	10–19	20–49	> 50	50–99	> 100	100–139	140
2019 q2	82,69	9,78	4,71	2,03	0,78	0,54	0,24	0,11	0,13
2019 q1	78,66	10,13	5,57	3,8	1,83	1,51	0,32	0,11	0,21
2018 q4	83,34	9,4	3,51	2,48	1,26	1,01	0,25	0,14	0,11
2018 q3	86,94	5,49	3,79	3,07	0,69	0,5	0,19	0,09	0,1
2018 q2	69,49	14,01	10,05	5,25	1,19	0,96	0,23	0,11	0,12
2018 q1	80,73	10,73	4,93	2,82	0,77	0,52	0,25	0,11	0,14
2017 q4	76,76	8,28	10,2	4,65	0,11	0,08	0,03	0,02	0,01
2017 q3	76,09	10,33	9,5	3,73	0,36	0,3	0,06	0,03	0,03
2017 q2	85,93	8,35	3,07	2,32	0,32	0,25	0,07	0,06	0,01
2017 q1	82,21	8,45	5,03	4,05	0,25	0,24	0,01	0,01	0

Из приведенных ниже данных видна общая тенденция. Количество атак становится меньше, а протяженность увеличивается. Одной из причин снижения количества атак является понижение интереса к криптовалюте . Причиной же повышения мощности атак стало использования серверов Memcached, о чем в первый раз было упомянуто в ноябре 2017 года. Самой мощной DDoS атакой на текущий момент является атака на американский провайдер 1,7 Тб/сек, что почти в три раза мощнее, чем предыдущий рекорд, установленный в 2016 году.

Еще одной причиной увеличения мощности стало повсеместное применение IoT устройств, используемые злоумышленниками при подключении к своим

ботнетам. Это заметно при анализе данных процентного соотношения операционных систем ботов из атакующих сетей, которые приведены на Рисунке 1.

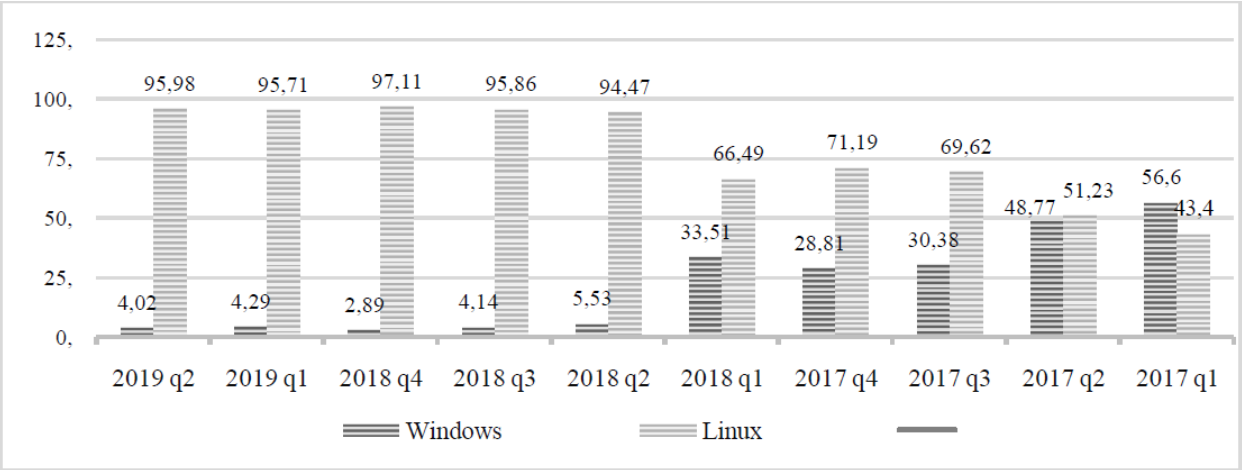

Рис. 1.– Статистика операционных систем в ботнетах

Причины уменьшения количества устройств под управлением операционной системы Windows не совсем очевидны. Это может указывать как на резкое включение большого количества устройств Linux, так и на неиспользование зараженных устройств на Windows. Последнее оставляет потенциальный риск рост мощностей атак, из-за возможного подключения дополнительных устройств.

Немалый вклад в развитие DDoS атак вносит и развитие мощностей персональных компьютеров что позволяет использовать злоумышленникам более мощные ботнеты.

Типы DDoS атак

Низкоуровневые происходят на транспортном и сетевом уровнях OSI-модели. Они используют несовершенство сетевой архитектуры. Защититься от них достаточно просто — подключите услугу, и через пару часов сервер снова будет в строю.

Высокоуровневые осуществляются на сеансовом, представительском и прикладном уровнях. Они эмулируют действия пользователей. Защититься от них сложнее, для этого понадобиться специальная настройка сервера.

Наводнения SYN атаки происходят на потребности средств сервера в предоставить огромной структуры данных памяти для аутентификации входящих SYN-пакетов. Во время атак SYN flood злоумышленник отправляет большее количество SYN-пакетов на адреса. В процессе ответа на запрос время, когда сервер отправляет информацию запроса в память стек, он будет ждать подтверждения от клиента, что отправляет запрос. Таким образом, пока запрос ожидает своего установления, он останется в памяти. Поскольку исходные адреса, используемые в атаках SYN flood, могут быть ложные, сервер не будет получать пакеты подтверждения для запросов, созданных атакой SYN flood. Каждая половина - открытое соединение останется в памяти в ожидание ответа.

Smurf атака типа ICMP Flood, где
злоумышленники используют пакеты эхо-запроса ICMP, направленные на IP широковещательные адреса из удаленных мест для генерации атаки отказа в обслуживании. В этих атаках участвует: злоумышленник, посредник и жертва. Сначала злоумышленник отправляет один пакет эхо-запроса ICMP на сетевой широковещательный адрес и запрос перенаправляется на все хосты в промежуточной сети.
Во-вторых, все хосты в промежуточной сети
отправиляют эхо-ответы ICMP для флудинга жертве. Настоящее время, smurf-атаки довольно редки в Интернете, так как защита против таких атак не составит труда.

HHTP потоп относится к атаке, которая бомбардирует веб
серверы с HTTP-запросами. HTTP-флуд - обычное дело
функция в большинстве программ ботнетов. Чтобы отправить HTTP-запрос, должно быть установлено действующее TCP-соединение, которое требуется подлинный IP-адрес. Злоумышленники могут добиться этого

используя IP-адрес бота. Более того, злоумышленники могут создавать HTTP-запросы по-разному, чтобы максимизировать силу атаки или избегая обнаружения.

Еще одна важная DDoS-атака - это атака *SIP flood* .
Широко поддерживаемый открытый стандарт настройки вызова в передача голоса по IP (VoIP) - протокол инициирования сеанса (SIP). Как правило, прокси-серверы SIP требуют общедоступного доступа в Интернет для приема запросов на установку вызова от любого клиента VoIP. Более того, для достижения масштабируемости SIP обычно реализуется поверх UDP, чтобы быть без гражданства. В одном сценарии атаки злоумышленника могут затопить SIP-прокси с множеством пакетов SIP INVITE, которые имеют поддельные исходные IP-адреса. Злоумышленники также могут запустить флуд из ботнета с использованием незарегистрированного IP-адреса источника адреса. Второй тип жертвы - получатели звонков. Они будут поражены поддельными звонками VoIP с невозможность дозвониться истинным абонентам.

Способы защиты

Защита от DoS и DDoS атак сильно зависит от модели сети и типа атаки. Было предложено несколько механизмов для решения этой проблемы. Однако у большинства из них есть слабости и терпят неудачу при атаках.

Методы *переупорядочения* и *улучшения протокола* сделают протоколы безопасности более надежными и менее уязвимыми к атакам на ресурсы жертвы.

Фильтрация входящего сетевого трафика - это механизм, предлагаемый для

предотвращать атаки, использующие поддельные адреса. Это включает настройку маршрутизаторов на отбрасывание пакетов, ложные IP-адреса. Одна из серьезных ловушек, он не может остановить атаку, которая исходит с поддельного IP-адреса изнутри сети.

Сообщения *трассировки ICMP* полезны для распознавания путь, по которому проходят пакеты через Интернет. Это требует, чтобы маршрутизатор использовал очень низкую вероятность, с которой сообщения трассировки отправляются вместе с трафиком. Следовательно, при достаточно большом количестве сообщений можно завершить маршрут, пройденный транспортным потоком во время атаки. Это позволяет локализовать агрессивный хост.

Подход к решению проблем, связанных с проверкой действительности IP-адресов при входящей фильтрации заключается в последовательном использовании маршрутизации. *IP-трассировка* предлагает надежный способ выполнения поэтапного отслеживания пакета до атакующего источника от откуда он возник. Однако для этого требуется скоординированные усилия всех маршрутизаторов в сети от жертвы к злоумышленнику, и проверка журналов пакетов.

Детерминированная маркировка пакетов (DPM) - другое средство для обнаружения DoS-атак. Он полагается на информацию вписываемой в заголовок пакета маршрутизаторами при прохождении пакета по сети.

Вероятностная маркировка пакетов (PPM) для IP-трассировки метод, который пытается улучшить DPM. Это устраняет подделку IP-адреса, позволяя каждому маршрутизатору вероятностно вписать информацию о локальном пути в пакет, который его проходит. Это позволяет хосту-жертве

локализовать атакующий источник, сохранив фиксированный размер заголовка пакетов. Механизм зависит от стабильности маршрута между злоумышленником и жертвой для локализации злоумышленника. Похожий механизм, известный как *основанный на маршрутах фильтрация пакетов*, в которой используется адреса источника и назначения в заголовке пакета для прочности маршрута.

Путем идентификатор (Pi) - отпечаток следа встроен в каждый пакет, что позволяет жертве идентифицировать пакеты проходя по тем же путям через Интернет на каждой пакетной основа, независимо от подмены IP-адреса источника. Pi позволяет жертве играть практическую роль в защита от DDoS-атаки с помощью знака Pi для отфильтрования атакующих пакетов.

PushBack подходы были предложены для извлечения сигнатуры атак путем ограничения скорости сомнительного трафика предназначенного для перегруженного сети. С момента DDoS, ход атаки не соответствует сквозному контролю потока протокола в пути, поэтому можно найти скопление пакетов с использованием статистики отбрасывания пакетов.

MULTOPS - маршрутизаторы замечают атаки на полосу пропускания, используя эвристику, основанную на скорости отправки пакетов. Путем расчета скорости пакетов по разным маршрутам. Как только это состояние нарушено, предполагается, что произошло нападение. Однако, эффективность MULTOPS снижается с рандомизированным IP исходных адресов.

D-WARD - выполняет статистическое профилирование трафика на краю сети, чтобы заметить новые типы DDoS-атак. Путем мониторинга номинального типа для каждого пункта назначения скорости прихода и отправления трафика TCP, UDP, ICMP пакетов, а также при обнаружении

любых нерегулярных асимметричных поведений двустороннего трафика на граничном маршрутизаторе подключаясь к тупиковой сети, D-WARD стремится остановить DDoS-атаки возле их источников.

Вывод

С развитием телекоммуникационных сетей DDoS атаки стали повсеместны и приносят вред как мелким предпринимателям, так и целым государствам. Подводя итог изложенному, можно констатировать тот факт, что защита информации является важной и достижимой задачей для обеспечения защиты, как коммерческих предприятий так и государственных структур. Хотя на сегодняшний день существует большое количество средств и методов обеспечения защиты от DDoS атак, подход к защите должен быть комплексным и включать в себя несколько способов защиты от них, а также организационно-техническая подготовка персонала.

Заключение

Для достижения данной цели, в процессе прохождения учебной (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практики ознакомился с DDoS атаками и основными способами противодействия им.

Также были изучены требования к написанию отчета по практике. В результате прохождения практики был составлен отчет по практике, соответствующий предъявленным требованиям.

В ходе прохождения практики все задачи были выполнены, а цель достигнута.

Список используемых источников

1. Saravanan Kumarasamy, R. Asokan «An Efficient Detection Mechanism for Distributed Denial of Service (DDoS) Attack» [Электронный ресурс] – Электрон. дан. – Режим доступа: https://arxiv.org/abs/1302.5158

2. Терновой Олег Степанович «Методика и средства раннего выявления и противодействия угрозам нарушения информационной безопасности при DDoS-атаках» [Электронный ресурс] – Электрон. дан. – Режим доступа: https://elibrary.ru/item.asp?id=20879286&

3. Артемьев Д.С., Якушина А.П. «Анализ данных по DDoS атакам» [Электронный ресурс] – Электрон. дан. – Режим доступа: https://www.elibrary.ru/item.asp?id=42794429

4. Saravanan Kumarasamy, R. Asokan, «Distributed Denial of Service (DDoS) Attacks Detection Mechanism» [Электронный ресурс] – Электрон. дан. – Режим доступа: https://arxiv.org/abs/1201.2007