Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Факультет компьютерных систем и сетей

Кафедра электронных вычислительных машин

Системное программное обеспечение локальных компьютерных сетей

Изучение протокола ICMP и особенностей его программирования, изучение протокола IP

Лабораторная работа №1

Выполнил:
студент гр. 850503
Басько А.С.

Проверил:
Смирнов Ю.В.

Минск 2022

Вопросы:

1. Объяснить работу программы traceroute

Для определения промежуточных маршрутизаторов traceroute отправляет целевому узлу серию ICMP-пакетов (по умолчанию 3 пакета), с каждым шагом увеличивая значение поля TTL на 1. Первая серия пакетов отправляется с TTL, равным 1, и поэтому первый же маршрутизатор возвращает обратно ICMP-сообщение «time exceeded in transit», указывающее на невозможность доставки данных. Traceroute фиксирует адрес маршрутизатора, а также время между отправкой пакета и получением ответа (эти сведения ыводятся на монитор компьютера). Затем traceroute повторяет отправку серии пакетов с TTL, равным 2, что заставляет первый маршрутизатор уменьшить TTL пакетов на единицу и направить их ко второму маршрутизатору. Второй маршрутизатор, получив пакеты с TTL=1, так же возвращает «time exceeded in transit».

Процесс повторяется до тех пор, пока пакет не достигнет целевого узла. При получении ответа от этого узла процесс трассировки считается завершённым.

На оконечном хосте IP-датаграмма с TTL = 1 не отбрасывается и не вызывает ICMP-сообщения типа срок истёк, а должна быть отдана приложению. Достижение пункта назначения определяется следующим образом: отсылаемые traceroute датаграммы содержат UDP-пакет с заведомо неиспользуемым номером порта на адресуемом хосте. Номер порта будет равен 33434 + (максимальное количество транзитных участков до узла) — 1. В пункте назначения UDP-модуль, получая подобные датаграммы, возвращает ICMP-сообщения об ошибке «порт недоступен». Таким образом, чтобы узнать о завершении работы, программе traceroute достаточно обнаружить, что поступило ICMP-сообщение об ошибке этого типа

2. Объяснить механизм действия smurf атаки. Какие угрозы она несет? Способы защиты?

Атака Smurf или ICMP-флуд — один из самых опасных видов DoS-атак, так как у компьютера-жертвы после такой атаки произойдет отказ в обслуживании практически со 100 % гарантией. Злоумышленник использует широковещательную рассылку для проверки работающих узлов в системе, отправляя ping-запрос. Требуется несколько участников — это усиливающая сеть. В ней по широковещательному адресу злоумышленник отправляет поддельный ICMP пакет. Затем адрес атакующего меняется на адрес жертвы. Все узлы пришлют ей ответ на ping-запрос. Поэтому ICMP-пакет, отправленный злоумышленником через усиливающую сеть, содержащую 200 узлов, будет усилен в 200 раз. Для такой атаки обычно выбирается большая сеть, чтобы у компьютера-жертвы не было никаких шансов.

Защититься от smurf-атаки, можно блокируя направленный широковещательный трафик, поступающий в сеть. Входную фильтрацию можно использовать для проверки всех входящих пакетов. Им будет отказано

или разрешен вход в систему на основании легитимности заголовка их пакета.

3. Объяснить назначение полей заголовка протокола IP

Поле Номер версии (Version), занимающее 4 бит, указывает версию протокола IP.

Поле Длина заголовка (IHL) IP-пакета занимает 4 бит и указывает значение длины заголовка, измеренное в 32-битовых словах. Обычно заголовок имеет длину в 20 байт (пять 32-битовых слов), но при увеличении объема служебной информации эта длина может быть увеличена за счет использования дополнительных байт в поле Опции (IP Options). Наибольший заголовок занимает 60 октетов.

Поле Тип сервиса (Type of Service) занимает один байт и задает приоритетность пакета и вид критерия выбора маршрута. Первые три бита этого поля образуют подполе приоритета пакета (Precedence), Приоритет может иметь значения от самого низкого - 0 (нормальный пакет) до самого высокого - 7 (пакет управляющей информации).

Поле Общая длина (Total Length) занимает 2 байта и означает общую длину пакета с учетом заголовка и поля данных. Максимальная длина пакета ограничена разрядностью поля, определяющего эту величину, и составляет 65 535 байт, однако в большинстве хост-компьютеров и сетей столь большие пакеты не используются.

Поле Идентификатор пакета (Identification) занимает 2 байта и используется для распознавания пакетов, образовавшихся путем фрагментации исходного пакета. Все фрагменты должны иметь одинаковое значение этого поля.

Поле Флаги (Flags) занимает 3 бита и содержит признаки, связанные с фрагментацией. Установленный бит DF (Do not Fragment) запрещает маршрутизатору фрагментировать данный пакет, а установленный бит MF (More Fragments) говорит о том, что данный пакет является промежуточным (не последним) фрагментом. Оставшийся бит зарезервирован.

Поле Смещение фрагмента (Fragment Offset) занимает 13 бит и задает смещение в байтах поля данных этого пакета от начала общего поля данных исходного пакета, подвергнутого фрагментации. Используется при сборке/разборке фрагментов пакетов при передачах их между сетями с различными величинами MTU. Смещение должно быть кратно 8 байт.

Поле Время жизни (Time to Live) занимает один байт и означает предельный срок, в течение которого пакет может перемещаться по сети. Время жизни данного пакета измеряется в секундах и задается источником передачи.

Идентификатор Протокол верхнего уровня (Protocol) занимает один байт и указывает, какому протоколу верхнего уровня принадлежит информация, размещенная в поле данных пакета (например, это могут быть сегменты протокола TCP, дейтаграммы UDP, пакеты ICMP или OSPF).

Значения идентификаторов для различных протоколов приводятся в документе RFC «Assigned Numbers».

Контрольная сумма (Header Checksum) занимает 2 байта и рассчитывается только по заголовку. Поскольку некоторые поля заголовка меняют свое значение в процессе передачи пакета по сети (например, время жизни), контрольная сумма проверяется и повторно рассчитывается при каждой обработке IP-заголовка. Контрольная сумма - 16 бит - подсчитывается как дополнение к сумме всех 16-битовых слов заголовка. При вычислении контрольной суммы значение самого поля «контрольная сумма» устанавливается в нуль. Если контрольная сумма неверна, то пакет будет отброшен, как только ошибка будет обнаружена.

Поля IP-адрес источника (Source IP Address) и IP-адрес назначения (Destination IP Address) имеют одинаковую длину - 32 бита - и одинаковую структуру.

Поле Опции (IP Options) является необязательным и используется обычно только при отладке сети.