УДК 004.056.5

АНАЛИЗ АТАК НА ЛОКАЛЬНО-ВЫЧИСЛИТЕЛЬНУЮ СЕТЬ

Клаченков Владислав Андреевич, ассистент
Минюк Ольга Николаевна, к.с.-х.н., доцент
Полесский государственный университет
Vladislav Klachenkov, assistant, klachenkov.v@polessu.by
Miniuk Volha, PhD, minuk.o@polessu.by
Polessky State Uiversity

Данная статья знакомит проведением атак в области защиты информации. Мониторинг безопасности локально-вычислительных сетей включает в себя определение и описание ряда уязвимостей характерных для объекта исследования.

Ключевые слова: *Локально-вычислительная сеть (ЛВС), атаки, отказ в обслуживании, MAC-адрес, ARP-spoofing, MitM-атака, DHCP Spoofing.*

После определения защитных мероприятий, проводимых на объекте исследования, был определен ряд уязвимостей, возможных для данного объекта, т.к. сеть построена на основе коммутаторов L2 и L3 уровня. Рассмотрим данные уязвимости более подробно:

Атака на дерево STP

Первый актуальный тип атак – это атаки на отказ в обслуживании или Dos-атака. Для организации атаки «Отказ в обслуживании» можно воспользоваться тем, что STP-совместимые устройства в момент реконфигурации работают не на пользователя, а лишь на создание Spanning

Tree дерева. Поскольку реконфигурация может быть вызвана, в том числе, появлением нового STP-совместимого устройства. Для этого необходимо имитировать появление периодически нового устройства с параметрами, которые будут лучше установившихся, что вызовет реконфигурацию одного из выборных параметров.

Выделим несколько типов атак в отказе обслуживания:

STP DoS: постоянный перебор

Данный вид атаки основан на ожидании появления STP пакета с текущим STP-root, затем по очереди перебираются значения bridge id, посылая bpdu с все меньшими значениями (id=id-1), до тех пор, пока не будет достигнуто предельное значение, вызывая, таким образом, перевыборы designated root каждым посланным пакетом. Когда будет достигнуто минимально возможное значение, необходимо подождать, пока данное значение не устареет из-за паузы, и начать этап сначала. С учетом того, что все параметры, включая время устаревания, устанавливаются в посылаемых пакетах назначенным корнем конфигурационных bpdu, можно получить ситуацию, при которой порты никогда не войдут в состояние "forwarding" пока происходит генерация фреймов, обеспечивающих отказ в обслуживании. Более того, в силу особенностей протокола состояние отказа в обслуживании будет продолжаться некоторое время, равное параметру Max Age, который можно выставлять согласно стандарту до 40 секунд.

Поскольку помимо 65535 возможных приоритетов bridge id включает в себя еще и MAC адрес, то количество времени, которое потребуется для переборки всех значений, составит:

(CurrentVictimBridgePriority-1 + VictimBridgeMAC-1)* (ListeningTime + LearningTime)= (CurrentVictimBridgePriority+VictimBridgeMAC-2)* (ListeningTime+LearningTime) = (CurrentVictimBridgePriority+VictimBridgeMAC-2)* 2*ForwardDelay ~секунд.

Для ForwardDelay значение по умолчанию составляет 15 секунд и может доходить до 30. На самом деле при зацикливании алгоритма состояние DoS может продолжаться сколь угодно долго, пока посылаются пакеты с фальшивыми BPDU.

STP DoS: алгоритм "исчезновения корня"

Данная атака основана на том, что начинается посылка BPDU с минимально возможным bridge id, то есть с максимально возможным приоритетом. Периодически перестает передавать конфигурационные bpdu для устаревания назначенного корня. Процесс является циклическим. На первый взгляд атака может казаться менее эффективной из-за существования небольшого промежутка времени, когда сеть работает. Тем не менее, в силу того, что ограничения, накладываемые спецификацией протокола, позволяют устанавливать время устаревания значений в очень широких пределах, этим методом можно достигнуть точно такой же эффективности. Описанный метод наиболее прост в реализации, поскольку не требует ни знания текущего идентификатора назначенного корня, ни каких-либо предположений относительно его величины (в отличие от предыдущего случая).

Навязывание ложного маршрута MitM-атака

Данная атака возможна в сети как минимум с двумя STP-совместимыми коммутаторами, подключенные к разным коммутаторам, т.к. есть возможность перехвата трафика между ними. Для реализации атаки в полной мере требуется два сетевых интерфейса, подключение которых необходимо осуществить так, чтобы образовать потенциальный дубликат имеющегося пути между источниками.

В принципе, задача определения мест включения в сеть, при которых будет возможна атака STP-MitM, должна поддаваться описанию через теорию графов. Для получения именно MitM, а не DoS, атакующий хост должен поддерживать работу обоих своих интерфейсов в режиме моста. Так же можно отметить, что для этого не требуется поддержка STP ОС, работающей как мост. Более того, такая полнофункциональная поддержка только повредит, т.к. принцип MitM атаки при использовании двух сетевых интерфейсов базируется на том, что атакующий может посылать BPDU пакеты от чужого имени, чтобы представить себя как наилучший путь хождения пакетов. При такой логике атаки полноценная поддержка STP только помешает атакующему, поэтому для реализации MitM необходимо отключать поддержку Spanning Tree, либо использовать OS+software, в которых нет поддержки STP. Таким образом, машина, реализующая MitM, на самом деле не нуждается в полноценной поддержке bridging'a, а может функционировать на манер концентратора, с единственным исключением – транзитный STP-траффик должен отбрасываться и

вместо него генерироваться собственный, анонсирующий себя как наиболее выгодный путь для пакетов.

Атака на таблицу MAC-адресов

Данная атака характеризуется переполнением таблицы MAC-адресов коммутатора. Иногда данную атаку называют лавинной атакой или атакой переполнения таблицы CAM. Размер таблиц MAC-адресов ограничен. Лавинные атаки используют это ограничение, "забрасывая" коммутатор ложными MAC-адресами источника до тех пор, пока таблица MAC-адресов коммутатора не заполнится.

Принцип действия:

Злоумышленник отправляет на коммутатор кадры с несуществующими, случайно сгенерированными MAC-адресами источника и назначения.

Коммутатор обновляет таблицу MAC-адресов информацией из фиктивных кадров.

Коммутатор входит в режим с пропусканием трафика.

Когда таблица MAC-адресов наполняется фиктивными MAC-адресами, коммутатор входит в так называемый режим с пропусканием трафика. В этом режиме коммутатор отправляет все кадры по широковещательной рассылке всем устройствам в сети.

Результат данной атаки: злоумышленник может видеть все рассылаемые кадры.

Атака на ARP

Данная атака, известная также под именем ARP Redirect, перенаправляет сетевой трафик от одного или более компьютеров к компьютеру злоумышленника. Выполняется в физической сети источника информации. Рассмотрим работу протокола ARP.

Протокол ARP реализует механизм разрешения IP-адресов в MAC-адреса Ethernet. Сетевое оборудование общается между собой путем обмена Ethernet-фреймов, на уровне канала данных. Для обеспечения возможности передачи этой информации необходимо, чтобы каждый сетевой интерфейс имел свой уникальный адрес в сети Ethernet, называемый MAC-адресом.

При посылке IP-пакета, отправляющий компьютер должен знать MAC-адрес получателя. Для этого в локальную сеть посылается широковещательный ARP-запрос, который опрашивает IP-адреса для определения MAC-адреса. Компьютер с соответствующим IP-адресом отвечает ARP-пакетом, содержащим запрошенный MAC-адрес. С этого момента, отправляющий компьютер знает MAC-адрес соответствующий IP-адресу назначения. Это соответствие сохраняется некоторое время в кэше (данная процедура предназначена для того, чтобы не выполнять запрос каждый раз при посылке IP-пакета).

Рассматриваемая атака изменяет кэш целевого компьютера. Злоумышленник шлет ARP-ответы целевому компьютеру с информацией о новом MAC-адресе, соответствующем, например, IP-адресу шлюза. На самом деле, этот MAC-адрес соответствует интерфейсу компьютера злоумышленника. Следовательно, весь сетевой трафик к шлюзу будет получать компьютер злоумышленника. Теперь можно прослушивать трафик, а также при желании изменять его. После этого, сетевой трафик будет направляться к реальному целевому адресу и, следовательно, никто не заметит изменений.

Атака ARP Spoofing используется в локальной сети, построенной на коммутаторах. С ее помощью можно перенаправить поток ethernet-фреймов на другие порты, в соответствии с MAC-адресом. После чего злоумышленник может перехватывать все пакеты на своем порту. Таким образом, атака ARP Spoofing позволяет перехватывать трафик компьютеров, расположенных на разных портах коммутатора.

Для реализации атаки ARP Spoofing, злоумышленник может воспользоваться генераторами ARP-пакетов, например, ARPSpoof, Nmap или Ettercap.

Подмена DNS через DHCP (DNS Spoofing and DHCP Spoofing)

Данная атака заключается в том, что злоумышленник, при наличии DHCP сервера в сети, производит атаку типа "отказ в обслуживании" на сервер, после чего DHCP сервер становится не доступным и тем самым перестает отвечать на запросы клиентов. В сети начинает работу ложный DHCP сервер, установленный, как правило, на компьютере атакующего, который раздает каждому компьютеру новые сетевые параметры, тем самым изменяет адреса в информационной сети. К новым сетевым параметрам может относиться IP-адрес самого компьютера, IP-адрес шлюза сегмента сети, IP-адрес DNS сервера и другие.

Получив новые сетевые параметры, каждый пользователь сети вводя в браузере в определенное доменное имя, будет обращаться к ложному DNS серверу. В ответ на полученный запрос сервер ответит, что данному доменному имени соответствует IP-адрес злоумышленника, на котором находится ложный сервер с копией домена.

После авторизации пользователя на ложном доменном имени у злоумышленника остаются все введенные данные.

Таким образом, рассмотрели такие атаки как, отказ в обслуживании (STP DoS: постоянный перебор, STP DoS: алгоритм "исчезновения корня"), MitM-атака, MAC-адрес, ARP-spoofing, , DHCP Spoofing, которые являются наиболее возможными атаки на локально-вычислительную сеть.

Список использованных источников

1. Возможные схемы атак [Электронный ресурс] BugTrag // Режим доступа: https://bugtraq.ru/library/books/stp/chapter06/ – Дата доступа: 10.03.2021.

2. Бондарев В.В. Анализ защищенности и мониторинг компьютерных сетей. Методы и средства: учебное пособие. – Москва : Издательство МГТУ им. Н. Э. Баумана, 2017. – 225, [3] с. : ил.

3. НПП «Учтех-Профи» – Корпоративные компьютерные сети – Теория. Часть 2 [Электронный ресурс] Теория CAN // Режим доступа: https://studfile.net/preview/5390122/ – Дата доступа: 10.03.2021.