Уязвимости протоколов TCP/IP и атаки, основанные на них.
Vulnerabilities of TCP/IP protocols and attacks based on them.

Андреев М. А. 011гр.

Многие протоколы стека TCP/IP создавались в те времена, когда мало кто задумывался о безопасности и сохранности передаваемых данных. Наиболее популярные атаки, такие как DNS и ARP Spoofing базируются на неточностях в RFC и недостатках реализации протоколов в программном обеспечении сетевых устройств и ошибках при их конфигурировании. Рассмотрим наиболее известные типы атак: IP, ARP и DNS Spoofing (подмена сетевой информации) и DoS атаки.

1 ARP Spoofing (Подмена ARP информации)

Как известно, ARP предназначен для разрешения MAC адреса по известному IP адресу. Каждый компьютер хранит в кэше таблицу соответствия MAC и IP адресов — ARP таблица. Если при обращении к другому компьютеру он не находит соответствующей записи, то высылается ARP запрос. Кроме того ARP таблица периодически обновляется(с периодичностью около 1 минуты). Когда компьютер получает ARP ответ, он обновляет ARP кэш с новой IP/MAC ассоциацией. Существует уязвимость в ARP протоколе: большинство операционных систем обновят свою ARP таблицу, если получат ответ, независимо от того, отправляли ли они запрос или нет.

ARP spoofing состоит в том, что посылая специально сконструированные ложные ARP ответы, можно убедить целевой компьютер отправлять кадры, предназначенные компьютеру A, к компьютеру B. При этом, если все сделано как следует, то A даже не будет знать, что произошло перенаправление. Такой процесс обновления ARP таблицы целевого компьютера получил название "отравления". Естественно эта атака может быть проведена только в сети, построенной на коммутаторах.

С помощью ARP подмены можно осуществлять активное прослушивание сетевого трафика, перехватывать сессии, проводить DoS атаки. Рассмотрим атаку man-in-the-middle. Атакующий компьютер "внедряется"в поток данных между компьютерами жертв. Для этого он отравляет их ARP таблицы, рекламируя себя как соответствующий компьютер жертвы. Пусть X — хакер и V1, V2 — компьютеры жертв, тогда V1 связывает IP адрес V2 с MAC адресом X и аналогично для V2. При этом X должен перенаправить трафик, так чтобы факт перехвата не был замечен. Особенно эта атака интересна тем, что можно отравить ARP кэш маршрутизатора по умолчанию и тем самым перехватывать весь интернет трафик жертвы. Другой вариант перехвата интернет трафика: рассылание ARP ответов с установленным широковещательным MAC адресом маршрутизатора по умолчанию. Как побочный эффект при MiM атаке, если хакер перед отключением забыл восстановить правильные MAC адреса жертв, их машины начинают рассылать кадры с несуществующими MAC адресами (что-то вроде DoS атаки). Используя атаку, подобную MiM можно, например, перехватить telnet сеанс после того, как

целевой компьютер зарегестрировался как администратор на удаленном компьютере. Возможна ситуация, когда какой-нибудь пользователь, подменяя маршрутизатор, выдает фальшивое приглашение telnet администратору сети с просьбой ввести имя и пароль доступа.

Эта атака ограничена сегментом локальной сети, тем не менее она может быть удачным дополнением, если атакующий уже выявил слабые места в системе безопасности и получил контроль над одним из компьютеров в сегменте.

Существует немало программ, позволяющих осуществлять подобные атаки, например, Ettercap, который позволяет также прослушивать SSH сессии, ARPoison и Parasite.

2 IP Spoofing

Эта атака базируется на предсказуемости некоторых операционных систем при выборе номера последовательности TCP (линейно или в зависимости от времени) и заключается в подмене IP адреса источника доверенным адресом. При этом, поскольку был изменен исходящий адрес, хакер не получает пакеты, т. к. они отправляются машине, адрес которой он использовал. Поэтому эта атака называется еще слепой подменой (Blind Spoofing). Тем не менее существует два способа получения пакетов, хотя они и трудно выполнимы:

- Маршрутизация от источника (Source Routing): позволяет определять маршрут для ответных пакетов. Маршрут представляет собой последовательность IP адресов, среди которых хакер может указать подконтрольный ему маршрутизатор. В настоящее время большинство маршрутизаторов отбрасывают пакеты с маршрутизацией от источника.

- Перенаправление. Если маршрутизатор использует RIP, то можно изменить таблицу маршрутизации, посылая фиктивные RIP пакеты с необходимой маршрутной информацией, так чтобы новый путь проходил через управляемый хакером маршрутизатор.

К этой атаке чувствительны следующие службы: RPC (Remote Procedure Call), X Window, R службы (такие как rlogin, rsh) и любые службы, использующие IP адрес для аутентификации. Одна из наиболее известных атак была проведена в 1944 г. Кевином Митником [Kevin Mitnick] против Цутому Шимомура [Tsutomu Shimomura]. Эта атака включала в себя следующие шаги:

- Выявление IP адреса доверенной машины, например, используя rpcinfo.

- Проведение DoS атаки против доверенного компьютера, используя smurfing или SYN Flooding. Иначе компьютер пошлет TCP RST, что разорвет соединение.

- Угадывание порядкового номера TCP подтверждения. Именно этот пункт наиболее трудно выполнить, поэтому атаки возможны только на те системы, в которых номер подтверждения выбирается линейно или зависимости от времени.

- Собственно атака заключается в установлении TCP соединения с желаемым портом. Как известно TCP соединение устанавливается в три этапа: на первом атакующий шлет от имени доверенного компьютера запрос на соединение (SYN=x), на втором удаленный компьютер шлет обратно подтверждение на IP адрес доверенного компьютера (SYN=y, ACK=x+1), на третьем злоумышленник отсылает ответ (ACK=y+1).

Теперь, после того как соединение установлено, хакер может послать команду сервису rsh на получение дополнительных прав доступа (например, echo ++ » /.rhosts). Для этого он отсылает пакет с установленным флагом TCP PSH, полученные данные передаются протоколу rsh, после чего он может уже без подмены адресов обращаться к серверу по rsh или rlogin.

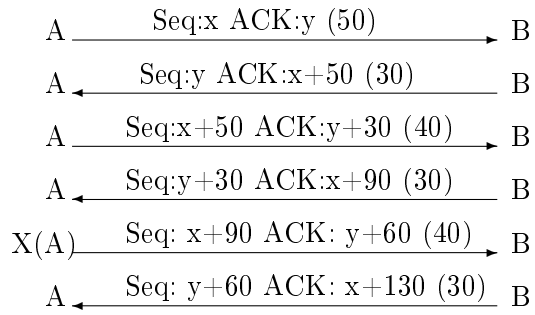
Для реализации этих атак можно воспользоваться следующими программами: Mendax, spoofit.h, ipspoof, hunt, dsniff.

3 Перехват TCP сеанса.

Перехват TCP сеанса заключается в десинхронизации атакующем TCP соединения между сервером и клентской машиной. Для того, чтобы понять как происходит перехват рассмотрим сначала более подробно процесс установления соединения и обмена пакетами. Во первых как выбирается ISN (initial sequence number). При загрузке ISN устанавливается равным 1, затем ISN увеличивается на 128000 каждую секунду, поэтому ISN повторяется каждые 9.32 часа, если не было установлено соединение. Всякий раз когда происходит соединение ISN увеличивается на 64000. Инициализация соединения осуществляется тройным рукопожатием: клиент и сервер обмениваются начальными номерами последовательности. После того как соединение установлено каждая сторона имеет свой номер последовательности и номер подтверждения принятия TCP соединения, совпадающий с номером последовательности другой стороны (все номера увеличены на единицу). Сервер принимает пакет, если его порядковый номер лежит внутри (ACK-SRV, ACK-SRV+WND-SRV), где WND-SRV — размер скользящего окна (аналогично для клиента). Если это не так, то он отбрасывается и отсылается ACK пакет с ожидаемым значением. Следует отметить, что номер последовательности меняется в соответствии с количеством переданных байт.

Атака проводится следующим образом. Пусть между машинами A и B установлено соединение и хакер X имеет возможность прослушивать весь трафик между A и B.

Пусть хакер установил, что A успешно зарегистрировал сеанс telnet на компьютере B. Тогда X решает рассинхронизировать сеанс между ними. Для этого он шлет пакет с адресом источника A и ожидаемым B номером подтверждения, этот пакет принимается B, что позволяет A выполнить команду в telnet сеансе (флаг PUSH установлен).



A в ответ на подтверждение со стороны B ложного пакета шлет пакет с недействительным номером последовательности в результате чего B отбрасывает пакет и генерирует ACK с требуемым номером. В ответ A шлет свой ACK и так далее. Эта ситуация называется "штормом подтверждений"(ACK Storm). Т. к. ACK пакеты не содержат полезной информации, то при их потере они не будут заново переданы и т. к. TCP использует IP с не нулевой потерей пакетов, то эта ситуация затухнет сама собой. Впрочем можно использовать подмену ARP информации (ARP spoofing): X подменяет MAC адрес A на свой в ARP таблице машины B так, чтобы фактически пакеты от B шли не к A, а к X.

4 DNS Spoofing

DNS spoofing заключается в подмене DNS информации, содержащейся в ответе на DNS запрос. Целью атаки является изменение записи в кэше целевого DNS сервера, связывающего DNS имя с ложным IP адресом. Для того чтобы провести такую атаку необходимо каким-то образом предугадать правильный ID запроса. Если атака проводится внутри локальной сети, то не составляет труда прослушивать трафик. В противном случае все гораздо сложнее. Существует несколько способов:

1. Произвольно проверить все возможные значения 16 битового поля ID.
2. Послать 200–300 запросов для того, чтобы увеличить шансы в нахождении хорошего ID.
3. Использовать уязвимости, найденные в BIND и позволяющие предсказать ID.

Рассмотрим случай легкого предсказания ID. Пусть ns.target.com целевой DNS сервер, www.spoofed.com — DNS имя для подмены (например, имя какого-нибудь банка или организации). У хакера должна быть возможность прослушивать пакеты, идущие от произвольного DNS (в этом примере, ns.bla.com), для этого он должен контролировать DNS (ns.attacker.com), авторитетный для домена attacker.com. Атака включает в себя следующие шаги:

- Запрашиваем у ns.target.com IP адрес (random).bla.com
- ns.target.com отсылает ответ ns.attacker.com, в котором кроме всего прочего есть ID, сгенерированный ns.target.com
- Хакер прослушивает ns.attacker.com и узнает ID
- Он подменяет IP адрес www.spoofed.com на подконтрольный. Для этого он посылает DNS запрос на разрешение имени www.spoofed.com ns.target.com. Затем как можно быстрее шлет ложные DNS ответы с измененным на какой-то свой IP адресом www.spoofed.com и IP адресом источника, подмененным на адрес одиного из DNS серверов домена spoofed.com.

Поскольку хакер знает предыдущий ID он шлет ответы с ID, увеличивающиеся на 1, т. к. возможно сервер ответил на запросы других клиентов. Этот прием значительно увеличивает вероятность угадывания ID.

Если атака удалась, кэш целевого сервера будет содержать запись, связывающую адрес www.spoofed.com с фальшивым IP адресом злоумышленника, на котором может быть размещена копия сайта, с помощью которой он может красть конфиденциальные сведения.

Рассмотрим два типа DoS атак: SYN, UDP flooding и smurfing.

5 SYN, UDP flooding

SYN наводнение является одной из самых популярных среди DoS атак. Суть атаки заключается в том, чтобы открыть как можно больше TCP соединений на компьютере жертвы (сервер) и оставить их в полуоткрытом состоянии. Для этого он отсылает жертве большое количество пакетов, с установленным флагом SYN. Для каждого полученного запроса сервер выделяет ресурсы, и когда они заканчиваются, он перестает отвечать на новые запросы. Существует максимально возможный предел для количества одновременно обрабатываемых запросов SYN. Этот предел называется backlog. Если произошло превышение лимита, то протокол TCP начинает отбрасывать новые запросы на соединение. В операционной системе Windows 2000 для отслеживания запросов к приложениям, использующим Windows

Sockets, TCP использует функцию listen(). Одним из параметров, передаваемых в эту функцию, является backlog, определяющий длину очереди незавершенных запросов. В спецификации Windows Socket 1.1 максимально возможное значение для backlog равно 5. В Windows NT 3.51 backlog может иметь максимальное значение равное 100 запросов. NT 4.0/2000 Server допускается до 200 запросов. Обычно в качестве адреса отправителя злоумышленник указывает несуществующий адрес (например, 0.0.0.0). В этом случае IP будет указывать на недостижимость получателя. TCP проигнорирует этот факт, т. к. будет считать, что эта ошибка должна быть исправлена IP, например с помощью перемаршрутизации. Пользователь, компьютер которого подвергся подобной атаке, может обнаружить этот факт с помощью команды netstat -n -p tcp. Вывод этой команды обнаружит большое число незавершенных TCP соединений (состояний SYN_RECEIVED).

Аналогичный тип атаки может быть осуществлен и с помощью бессеансового режима UDP. Атакующий шлет огромное количество UDP пакетов, направленных на одну или несколько целевых машин. Такая атака даже более эффективна, чем SYN наводнение, т. к. UDP трафик имеет больший приоритет. Кроме того в TCP предусмотрена возможность замедления скорости передачи трафика (уменьшение окна) в случае, если возникают задержки при подтверждении приема пакетов. UDP не обладает таким механизмом, поэтому он может занять всю полосу пропускания, почти ни чего не оставив TCP.

6 Smurfing

Если предыдущие атаки были нацелены на отказ в обслуживании одного или нескольких машин, то с помощью этой атаки можно вывести из строя всю сеть. Для ее проведения используется ICMP. Злоумышленник шлет направленный широковещательный ICMP ECHO запрос с адресом источника целевой машины. В ответ многие сетевые устроства пошлют пакеты ICMP ECHO REPLY. Вообще говоря, т. к. атака smurf была придумана сравнительно давно, многие производители включили в свои операционные системы защиту, препятствующую услужливому реагированию на такие запросы. В частности Windows 2000, Windows NT и Windows 98 не откликаются на широковещательный ICMP ECHO запрос.

7 Заключение

С развитием программного обеспечения все больше атак уходят в прошлое, тем не менее многие атаки, например ARP spoofing, довольно трудно отследить даже используя системы обнаружения вторжений (IDS). Кроме того развитие инфраструктуры и Web служб создает дополнительные возможности для хакеров

использовать ошибки в коде их реализации, что связано с сжатыми сроками выполнения и все увеличивающейся сложностью.

Использованные ссылки:

1. Simple Active Attack Against TCP Laurent Joncheray: www.insecure.org/stf/iphijack.txt

2. DNS ID Hacking ADM Crew: packetstorm.securify.com/groups/ADM/ADM-DNS-SPOOF/ADMID.txt

3. THE LATEST IN DENIAL OF SERVICE ATTACKS: "SMURFING"DESCRIPTION AND INFORMATION TO MINIMIZE EFFECTS Craig A. Huegen: http://www.pentics.net/denial-of-service/white-papers/smurf.html

4. IP-spoofing Demystified by daemon9 / route / infinity for Phrack Magazine: http://www.networkcommand.com/docs/ipspoof.txt

5. External attacks Eric Detoisien: http://www.security-labs.org/index.php3?page=456