IP-spoofing

Черкасов Денис Юрьевич / Cherkasov Denis Yurievich
студент
Иванов Вадим Вадимович / Ivanov Vadim Vadimovich
студент
Кафедра компьютерной и информационной безопасности,
Институт кибернетики,
Московский институт радиотехники электроники и автоматики,
Федеральное государственное бюджетное образовательное
учреждение высшего образования
Московский технологический университет,
г. Москва

IP-spoofing

Преступники уже давно используют тактику маскировки своей личности — от сокрытия псевдонимов до блокировки идентификатора вызывающего. Неудивительно, что преступники, которые реализуют свои гнусные действия в сетях и компьютерах, используют такие методы. IP-спуфинг является одной из наиболее распространенных форм онлайнового камуфляжа. При IP-спуфинге злоумышленник получает несанкционированный доступ к компьютеру или сети путем «подмены» IP-адреса этого компьютера, указывая на то, что вредоносное сообщение поступило с доверенного компьютера. В этой статье мы рассмотрим концепции IP-спуфинга: почему это возможно, как это работает, для чего оно используется и как защититься от него.

История

Концепция IP-спуфинга первоначально обсуждалась в академических кругах в 1980-х годах. В то время это было теоретической дискуссией, пока Роберт Моррис, сын которого написал первый компьютерный червь, не обнаружил слабости в системе безопасности TCP-протокола. Стивен Белловин подробно рассмотрел проблему уязвимости в безопасности набора протоколов TCP / IP. Печально известная атака Кевина Митника на машине Цутому Симомура использовала методы IP-спуфинга и прогнозировала последовательности TCP. Хотя популярность таких атак уменьшилась, спуфинг еще активно реализуется.

Техническая дискуссия

Чтобы полностью понять, как осуществляются эти атаки, необходимо изучить структуру набора протоколов TCP / IP.

Интернет-протокол — IP-адрес

Интернет-протокол (IP) — это сетевой протокол, работающий на уровне 3 (сети) модели OSI, без установления соединения, то есть отсутствует информация о состоянии транзакции, которая используется для маршрутизации пакетов по сети. Кроме того, не существует метода, гарантирующего правильную доставку пакета в пункт назначения.

```
0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version|  IHL  |Type of Service|          Total Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Identification        |Flags|      Fragment Offset    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time to Live |    Protocol   |         Header Checksum       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Source Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination Address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

IP PACKET HEADER

Изучая заголовок IP-пакета, мы видим, что первые 12 байтов (или верхние 3 строки заголовка) содержат различную информацию о пакете. Следующие 8 байтов (следующие 2 строки) содержат IP-адреса источника и назначения. Используя один из нескольких инструментов, злоумышленник может легко изменить эти адреса — в частности, поле «адрес источника». Важно отметить, что каждая дейтаграмма отправляется независимо от всех остальных из-за строения IP.

Протокол управления передачей — TCP

IP можно рассматривать как оболочку маршрутизации для 4 уровня (транспорт), которая содержит протокол управления передачей (TCP). В отличие от IP, TCP ориентирован на соединение. Это означает, что участники сеанса TCP должны сначала создать соединение, используя трехстороннее рукопожатие (SYN-SYN / ACK-ACK), затем обновить друг друга через последовательности и подтверждения. Этот «разговор» обеспечивает надежную передачу данных, отправитель получает подтверждения от получателя после каждого обмена пакетами.

```
0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Source Port          |       Destination Port        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Sequence Number                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Acknowledgment Number                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Data |           |U|A|P|R|S|F|                               |
| Offset| Reserved  |R|C|S|S|Y|I|            Window             |
|       |           |G|K|H|T|N|N|                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Checksum            |         Urgent Pointer        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             data                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

TCP PACKET HEADER

Заголовок TCP сильно отличается от заголовка IP. Мы имеем дело с первыми 12 байтами TCP-пакета, которые содержат информацию о порте и последовательности. Подобно IP-дейтаграмме, TCP-пакеты могут управляться с помощью программного обеспечения. Исходный и конечный порты обычно зависят от используемого сетевого приложения (например, HTTP через порт 80). Для понимания спуфинга важно обращать внимание на номера последовательности и подтверждения. Данные, содержащиеся в этих полях, обеспечивают надежную доставку пакетов, определяя, нужно ли повторно отправлять пакет. Номер последовательности — это номер первого байта в текущем пакете, который имеет отношение к потоку данных. Номер подтверждения, в свою

очередь, содержит значение следующего ожидаемого порядкового номера в потоке. Это соотношение подтверждает, что надлежащие пакеты были получены. Этот протокол совсем не похож на IP, поскольку состояние транзакции тщательно контролируется.

Последствия проектирования TCP / IP

У нас есть обзор форматов TCP / IP, давайте рассмотрим последствия. Очевидно, что очень легко маскировать адрес источника, манипулируя IP-заголовком. Этот метод используется по очевидным причинам и применяется в нескольких описанных ниже атаках. Другим следствием, специфичным для TCP, является прогнозирование последовательности номеров, что может привести к захвату сеанса. Этот метод основан на IP-спуфинге, поскольку создается сессия, хотя и ложная.

Спуфинг-атаки

Существует несколько вариантов атак, которые успешно используют IP-спуфинг. Хотя некоторые из них относительно стары, другие очень уместны в отношении текущих проблем безопасности.

Спуфинг «не вслепую»

Этот тип атаки происходит, когда злоумышленник находится в той же подсети, что и жертва. Номера последовательности и подтверждения можно получить, устраняя потенциальную сложность их расчета. Захват сеанса достигается путем искажения потока данных установленного соединения, а затем восстановления его на основе правильной последовательности и номеров подтверждения с атакующей машины. Используя эту технику, злоумышленник может эффективно обойти любые меры аутентификации, предпринятые для построения соединения.

Спуфинг «вслепую»

Это более сложная атака, поскольку номера последовательностей и подтверждения недоступны. Несколько пакетов отправляются на целевую машину, чтобы перебирать порядковые номера. Сегодня большинство ОС реализуют генерацию случайных порядковых номеров, что затрудняет их точное прогнозирование. Однако если номер последовательности был скомпрометирован, данные могут быть отправлены на целевое устройство. Несколько лет назад многие машины использовали службы аутентификации на основе хоста. Грамотно созданная атака может слепо встраивать требуемые данные в систему (новую учетную запись пользователя), предоставляя полный доступ злоумышленнику, который выдавал себя за доверенный хост.

Атака «Man In the Middle»

Известная также как атака типа «человек посередине» (MITM). В этих атаках враждебная сторона перехватывает связь между двумя дружественными сторонами. Вредоносный хост затем управляет потоком связи и может устранить или изменить информацию, отправленную одним из исходных участников, не зная ни исходного отправителя, ни получателя. Таким образом, злоумышленник может обмануть жертву в раскрытии конфиденциальной информации путем «подмены» личности оригинального отправителя, которому предположительно доверяет получатель.

Атака, направленная на получение отказа в обслуживании

IP-спуфинг применяется в одной из самых сложных атак для защиты — «отказ в обслуживании» или DoS. Поскольку хакеры имеют дело только с потреблением полосы пропускания и ресурсов, им не нужно беспокоиться о правильном завершении транзакций. Скорее они хотят наводнить жертву как можно большим количеством пакетов за короткий промежуток времени. Когда в атаке участвует несколько взломанных хостов, принимающих все отправленные

поддельные трафики, практически невозможно это быстро заблокировать.

Неправильные представления об IP-спуфинге

Хотя некоторые из описанных выше атак немного устарели, например, захват сеанса для служб проверки подлинности на основе хоста, IP-спуфинг по-прежнему распространен в сканировании сети, а также наводнениях отказа в обслуживании. Однако этот метод не предоставляет анонимный доступ в Интернет, что является распространенным заблуждением для тех, кто не знаком с этой практикой. Любое подобное подталкивание за пределами простых наводнений относительно продвинуто и используется в очень конкретных случаях, таких как уклонение и захват соединений.

Защита от спуфинга

Существует несколько мер предосторожности, которые можно принять для ограничения рисков IP-спуфинга в вашей сети, таких как фильтрация на маршрутизаторе, шифрование и аутентификация. Внедрение шифрования и аутентификации уменьшит вероятность подмены. Понимание того, как и почему используются атаки с использованием спуфинга, в сочетании с несколькими простыми методами предотвращения, может помочь защитить вашу сеть от этих вредоносных методов клонирования и взлома.