Impact Factor ISRA (India) = **1.344**
Impact Factor ISI (Dubai, UAE) = **0.829**
based on International Citation Report (ICR)

Impact Factor JIF = **1.500**
Impact Factor GIF (Australia) = **0.356**
Impact Factor SIS (USA) = **0.438**

Doi: 10.15863/TAS
International Scientific Journal
Theoretical & Applied Science

p-ISSN: 2308-4944 (print) **e-ISSN:** 2409-0085 (online)

Year: 2015 **Issue:** 01 **Volume:** 21

Published: 30.01.2015 **http://www.T-Science.org**

SECTION 4. Computer science, computer engineering and automation.

Dmitrii G. Bukhanov
engineer
Belgorod State Technological University named after V.G. Shukhov (BSTU after V.G. Shukhov), Russia
db.old.stray@gmail.com
Vladimir M. Polyakov
Ph.D., Associate Professor
Vice Rector for Academic Affairs,
BSTU after V.G. Shukhov, Russia
p_v_m@mail.ru
Dmitrii A. Uskov
Student, BSTU after V.G. Shukhov, Russia
myself.elf@gmail.com
Feras Daeef
undergraduate BSTU after V.G. Shukhov, Russia
ferasit87@gmail.com

DETECTION SYN FLOOD ATTACKS WITH WINPCAP DRIVER

Abstract: *The paper provides an overview of approaches detection SYN flood attacks in local area networks based on the method of comparing the SYN and FIN packets. An approach is proposed to counter SYN flood attacks, based on the use of low-level driver - WinPcap. The paper describes the algorithm for detecting SYN flood attack. On the basis of the proposed approach are presented experimental results that confirm its effectiveness.*

Key words: *winpcap, syn flood, detection ddos, network security.*
Language: *Russian*
Citation: Bukhanov DG, Polyakov VM, Uskov DA, Daeef F (2015) DETECTION SYN FLOOD ATTACKS WITH WINPCAP DRIVER. ISJ Theoretical & Applied Science 01 (21): 139-144. doi: http://dx.doi.org/10.15863/TAS.2015.01.21.24

ОБНАРУЖЕНИЕ SYN FLOOD АТАК С ИСПОЛЬЗОВАНИЕМ ДРАЙВЕРА WINPCAP

Аннотация: *В работе проводится обзор подходов обнаружения SYN flood атак в локальных вычислительных сетях, основанных на методе сопоставления SYN и FIN пакетов. Предлагается подход для противодействия SYN flood атакам, основанный на использовании драйвера низкого уровня – WinPcap. В работе описывается алгоритм обнаружения SYN flood атаки. На основе предложенного подхода представлены результаты эксперимента, которые подтверждают его эффективность.*

Ключевые слова: *winpcap, syn flood, обнаружение ddos, сетевая безопасность.*

Введение

В настоящее время, практически любое сетевое приложение легко можно вывести из строя. Доступным и эффективным инструментом, позволяющим злоумышленникам препятствовать деятельности или полностью блокировать работу сетевых приложений, являются DDoS-атаки (Distributed Denial of Service - "распределенная атака на отказ в обслуживании"). Принцип работы DDoS заключается в следующем: на сервер-жертву обрушивается множество ложных запросов с большого количества компьютеров. В результате сервер расходует все системные ресурсы на обслуживание этих запросов, и узел-жертва перестает принимать легитимные запросы пользователей и тем самым становится недоступным. Существующие сейчас различные виды DDoS-атак, можно классифицировать в зависимости от уровня модели OSI, на котором они проводятся. На сетевом уровне может быть эффективно реализована Winfreeze атака, использующая протокол ICMP [1]. Посылая ICMP-сообщения REDIRECT жертве, злоумышленник может вывести из строя узел локальной вычислительной сети. Также существуют DDoS атаки прикладного уровня, которые направлены на вывод из строя конкретного сетевого приложения [2]. Другой разновидностью атак, является группа атак, использующих транспортный уровень. Они являются наиболее сложным типом DDoS-атак для обнаружения. Самой распространеной из них является SYN flood атака [3]. Она заключается в использовании уязвимости протокола TCP и создании полуоткрытых

соединений на стороне сервера после второго этапа «трёхкратного рукопожатия». В этом случае сервер, в ожидании ответа от клиента, не освобождает выделенные системные ресурсы, что может привести к их исчерпанию. Своевременное выявление данной атаки позволит избежать сбоев в работе критически важных приложений на узлах локальной вычислительной сети.

В качестве способа противодействия SYN flood атакам, в данной работе предлагается использовать ограничение запросов на новые подключения от конкретного источника за определенный промежуток времени.

Основой для многих методов обнаружения SYN flood атак является сопоставление SYN-пакетов к FIN-пакетам. Авторы таких подходов предлагают накапливать информацию о входящих SYN-пакетах и оценивать ее с помощью различных статистических параметров [3, 4, 5, 6]. В роли них могут выступать следующие параметры:

– отношение количества входящих SYN-пакетов к FIN и RST-пакетам;

– отношение количества SYNACK-пакетов к клиентским ACK-пакетам;

– экспоненциально взвешенное скользящее среднее числа полученных SYN пакетов на заданном интервале;

– количество полуоткрытых соединений.

Независимо от способов хранения и состава анализируемых данных, эти методы обладают общими недостатками, которые могут существенно отразиться на качестве их применения в реальных системах. К их числу можно отнести невозможность установления источника атаки и неустойчивость к «медленной» SYN flood атаке, при которой злоумышленник постепенно увеличивает число SYN-пакетов.

Существуют методы, не использующие соответствия SYN-пактов к FIN-пакетам. В работе [7] авторы для создания средства обнаружения SYN flood атаки предлагают подход, в котором используется обнаружение пакетов 1stDP. 1stDP – это пакет, который передается в первую очередь после установки соединения. Если в течение некоторого времени не приходит 1stDP, соединение считается нелегитимным и запрещается. Данный подход имеет существенный недостаток – в нем не предусмотрена система противодействия атаке.

Существуют также методы, которые используют нейронные сети для обнаружения аномалий в сети [8,9]. Данные методы подходят для диагностирования сетей не только на наличие SYN атаки, но и других, например, атак типа Probe, U2R, R2l [10]. Данные подходы предлагают использовать для анализа не только мгновенные параметры состояния сети, но и учитывают параметры, изменяющиеся в течение длительных промежутков времени работы сети. Недостатком такого решения является необходимость проведения специальной процедуры обучения, которая требует большого количества разнородного трафика, собранного как при нормальной работе сети, так и при атаке на нее.

Анализ подходов сбора сетевого трафика

Для получения диагностической сетевой информации в операционных системах семейства Windows NT, не обязательно использовать драйверы-фильтры (например, NDIS) или использовать специальные сторонние инструменты для работы с сетевой картой. Систему получения и регистрации трафика можно разработать на базе Windows сокетов. Для этого требуется создать RAW-сокет и перевести сетевую карту в неразборчивый режим (promiscuous mode), в котором ведется прием всех пакетов, независимо от того, кому они адресованы.

Для того чтобы выполнить прием пакетов, необходимо совершить следующие действия:

WSADATA wsadata;
WSAStartup(MAKEWORD(2, 2), &wsadata); //инициализация библиотеки для работы с winsock;
SOCKET s = socket(AF_INET, SOCK_RAW, IPPROTO_IP); // создание сокета
bind(s, (SOCKADDR*)&sa, sizeof SOCKADDR); //связывание локального адреса с сокетом;
DWORD flag = TRUE;
ioctlsocket(s, SIO_RCVALL, &flag); // включение неразборчивого режима;

Режим приема всех входящих пакетов, включается указанием в качестве команды сокету константы SIO_RCVALL, которая позволяет ему принимать все IP пакеты из сети. Дескриптор сокета, переданный в функцию WSAIoctl (или ioctlsocket), должен принадлежать семейству адресов AF_INET (internetwork). Тип этого сокета должен быть SOCK_RAW и протокол – IPPROTO_IP. Сокет также должен быть связан с явным локальным интерфейсом. Далее следует бесконечный цикл, внутри которого выполняются приём и обработка всех принятых IP-пакетов.

К недостаткам сетевых сокетов Windows в системе определения SYN flood атаки, можно отнести:

– возможность «прослушивания» только трафика сетевого уровня;

– нет возможности установки низкоуровневого фильтра;

– требуются права администратора для их применения;

– нет возможности работать на канальном уровне.

Для преодоления этих недостатков при получении сетевого трафика в системе обнаружения SYN flood атак при работе с сетевой картой предлагается использовать низкоуровневый драйвер WinPcap. Его архитектура дополняет стандартные функции операционных систем семейства Windows возможностью принимать и передавать данные по сети, минуя стек протоколов операционной системы, и взаимодействовать непосредственно с сетевым адаптером.

Драйвер WinPcap состоит из трех основных элементов (рисунок 1): сетевой ловушки (network tap), пакетного фильтра (packet filter) и структуры, состоящей из двух буферов памяти. Сетевая ловушка – это петлевая функция, являющаяся частью кода драйвера. Ее вызывает драйвер сетевого адаптера, когда принимает каждый входящий пакет. Сетевая ловушка копирует поступившие пакеты и передает их копии через фильтр на прикладной уровень.

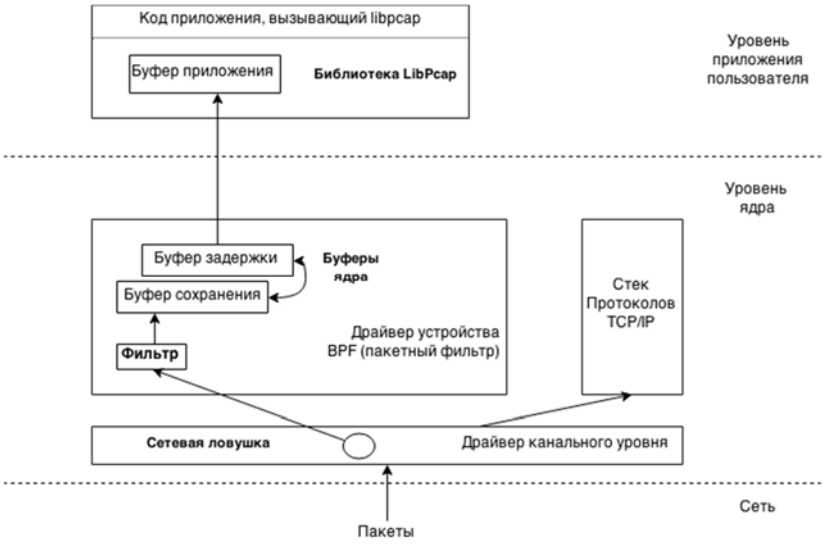

Рисунок 1 – Схема работы драйвера WinPcap.

Фильтр задаётся приложением и передается в сетевой драйвер. Драйвер назначает фильтр и два буфера на каждый процесс. Первый буфер (store buffer – буфер сохранения) используется для приема данных от адаптера, второй (hold buffer – буфер задержки) используется для копирования пакетов в приложение. Если буфер сохранения заполнен, он меняется местами с буфером задержки.

Когда пакет поступает на вход сетевого интерфейса, драйвер устройства канального уровня передает его системному стеку протоколов, а драйвер WinPcap вызывает функцию сетевой ловушки, которая передает пакет фильтру.

Обнаружение SYN flood атак

Для получения сетевого трафика предлагаемый подход обнаружения SYN flood атаки использует драйвер WinPcap. Он основан на сопоставлении каждому SYN пакету такого пакета, который покажет легитимность соединения. На рисунке 2 показана блок-схема алгоритма, описывающая работу системы обнаружения SYN flood атак.

Считается, что соединение легитимно, если на один SYN-пакет приходит одно сообщение с заполненным полем данных. Для каждого поступившего пакета с флагом SYN создается и заполняется следующая структура:

typedef struct{
char sour_mac[6]; //физические адрес отправителя;
char sour_ip[4]; //логический адрес отправителя;
short dest_port; //порт получателя;
short time; //время ожидания подтверждения соединения;
short repeat; // количество эквивалентных пакетов;
} type_knownRecord; // структура записи для каждого пакета.

Эта структура заносится в массив knownRecords. Затем, через TIMEOUT секунд,

запись удаляется из knownRecords и заносится в suspiciousRecords. При добавлении происходит пересчет числа записей в массиве suspiciousRecords, эквивалентных данной. Эквивалентными считаются записи с одинаковыми sour_ip и dest_port или одинаковыми sour_mac и dest_port. Если оказалось, что их количество больше заданного MAX_REPEATS то, это означает наличие угрозы безопасности со стороны соответствующего отправителя. В этом случае система предпринимает действия по устранению угрозы в соответствии с внутренней политикой безопасности системы.

Если пришедший пакет содержит заполненное поле данных, то производится поиск соответствующих ему записей в массиве knownRecords. В случае если такая запись найдена, то она удаляется из knownRecords.

Если в течение периода TIMEOUT не приходит сообщение, подтверждающее, что запрос пришёл от пользователя, запись попадает в список подозрительных соединений.

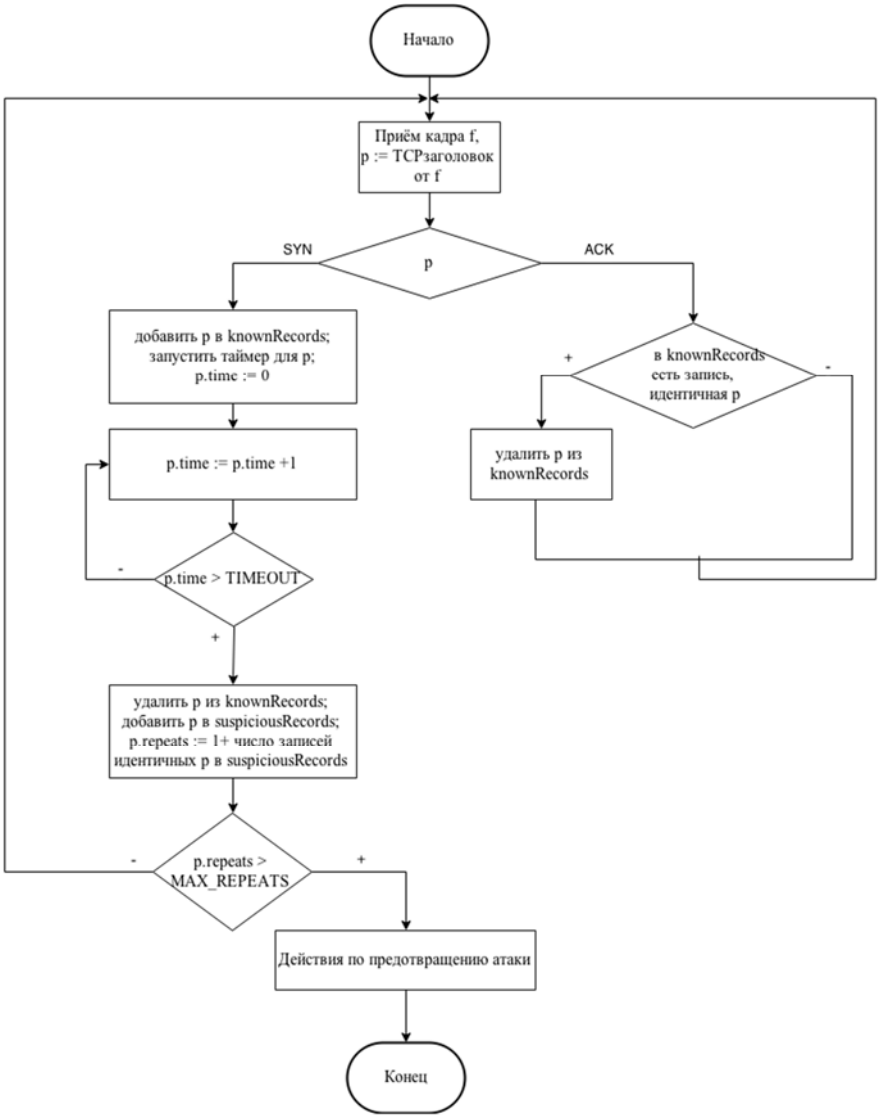

Рисунок 2 – Блок-схема алгоритма определения SYN flood атаки.

Считается, что пользователь подтвердил соединение отправкой TCP пакета с заполненным полем данных. Разработанный подход позволяет не только информировать об атаке, но и получить список подозреваемых узлов.

Экспериментальная проверка системы обнаружения SYN flood атаки

Данный подход обнаружения SYN flood атаки используется в распределенной диагностической системе на основе программных агентов. Децентрализация процесса обнаружения позволяет избавиться от ограничения на пропускную способность анализируемого канала, т.е. каждый узел диагностирует только свои соединения. Это уменьшает количество записей и объем используемой памяти для хранения списка узлов, подозреваемых в атаке. Так же это уменьшает загрузку процессора, так как диагностируется трафик меньшего объема.

Для обнаружения синтетической SYN flood атаки был проведен следующий эксперимент в изолированной компьютерной сети без случайного трафика и без доступа к сети Интернет. Для чистоты эксперимента в сети можно было контролировать все параметры. Такая среда проведения эксперимента позволяет однозначно определить следующие параметры:

– время обнаружения атаки;

– предельное допустимое количество полуоткрытых соединений;

– загруженность ЦП при определении атаки.

В ходе эксперимента на основании описанного подхода были получены следующие данные (табл. 1).

Таблица 1

Результаты работы системы обнаружения SYN flood атаки

№	Сетевой сервис (name)	Время обнаружения атаки, сек (t)	Предельно допустимое количество полуоткрытых соединений, шт (h)	Загруженность ЦП в процентах
1	Free FTP Server, FileZilla	3-5	До 10	45
2	Apache2	менее 1	До 700	67
4	Xlight FTP Server	3-5	До 10	50
6	IRC	1-2	До 80	60
7	Hub DC	3-5	До 20	55

Экспериментально показано, что применение данного подхода позволяет выявлять атаки эффективнее, создавая меньшую нагрузку на узел, по сравнению с результатами, полученными в работе [11]. Но для результативного применения описанного подхода требуется произвести более глубокий анализ архитектуры защищаемого приложения. Т.е. для каждого конкретного случая требуется найти предельно-допустимое количество полуоткрытых соединений, на основе которого вычисляется значение MAX_REPEATS. Это значение зависит от мощности узла, текущей загруженности ЦП, операционной системы, архитектуры приложения, работающего на защищаемом порту и некоторых других параметров. Результаты эксперимента показывают, что чем более интенсивная атака проводится, тем меньше требуется времени на ее выявление.

Заключение

Использование технологии WinPcap позволяет ускорить работу системы обнаружения атаки. В отличие от стандартного подхода, основанного на использовании Windows-сокетов, WinPcap позволяет получать больше параметров для диагностирования и работает не только с сетевым уровнем модели OSI, но и с канальным.

Предложенный подход позволяет противодействовать SYN flood атаке, направленной на узлы защищаемой сети, а также дает возможность определения других видов DDoS атак, например, WinFreeze.

Децентрализация анализа сетевого трафика позволяет выполнять обнаружения атаки с большей достоверностью, так как каждый агент проверяет меньший объем трафика. Это убирает ограничение системы на пропускную способность общего канала.

References:

1. Chowdhary M, Suri S, Bhutani M (2014) Comparative Study of Intrusion Detection System. International Journal of Computer and Engineering. – 2014. – Vol. 2, No. 4. – pp. 197-200.

2. Rajesh S (2013) Protection from Application Layer DDoS Attacks for Popular Websites. International Journal of Computer and Electrical Engineering. – 2013. – Vol. 5, No. 6. – pp. 555-558.
3. Wang H (2002) Detecting SYN flooding attacks / H. Wang, D. Zhang, K. G. Shin / In Proc. of INFOCOM. IEEE Communications Society. – 2002. – pp. 1530-1539.
4. Brodsky BE (1993) Nonparametric Methods in Change-Point Problems / B. E. Brodsky, B. S. Darkhovsky. – Kluwer Academic Publishers, 1993. – 210 p.
5. Siris VA (2004) Application of anomaly detection algorithms for detecting SYN flooding attacks / V. A. Siris, F. Papagalou / In Proc. of Globecom. IEEE Communications Society. – 2004. – pp. 2050-2054.
6. Haris SHC (2010) Detecting TCP SYN Flood Attack Based on Anomaly Detection / S. H. C. Haris, R. B. Ahmad, M. A. H. A. Ghani / In Proc. of Network Applications Protocols and Services. IEEE Communications Society. – 2010. – pp. 240-244.
7. Jianxi T (2013) Defending Against SYN Flood Attack under Asymmetric Routing Environment / T. Jianxi, Z. Li, Z. Zhou, Y. Rong, Y. Wei, L. Qingyun / International Workshop on Cloud Computing and Information Security. – 2013. – pp. 165-168.
8. Slepovichev II (2009) Obnaruzhenie DDoS-atak nechetkoy neyronnoy setyu / I. I. Slepovichev, P. V. Irmatov, M. S. Komarova, A. A. Bezhin / Izvestiya Saratovskogo universiteta. Seriya 8. Matematika. Mehanika. Informatika. – 2009. – Vyip. 3. – pp. 84-89.
9. Chastikova VA (2014) Obnaruzhenie DDos-atak na osnove neyronnyih setey s primeneniem metoda roya chastits v kachestve algoritma obucheniya / V. A. Chastikova, K. A. Vlasov, D. A. Kartamyishev / Fundamentalnyie issledovaniya. – 2014. – Vyip. 8-4. – pp. 829-832.
10. Golovko VA (2011) Proektirovanie intellektualnyih sistem obnaruzheniya anomaliy / V. A. Golovko, S. V. Bezobrazov / OSTIS. – 2011. – pp. 185-196.
11. Brusnikin MS (2014) Analiz effektivnosti statisticheskoy filtratsii setevogo trafika pri zaschite ot setevyih atak / M. S. Brusnikin, D. V. Paschenko / Informatsionnyie tehnologii v nauke i obrazovanii. Problemyi i perspektivyi. – 2014. – pp. 82-84.