SAT-2G.303-1-CST-02

System for generating of DoS network attacks

Martin Todorov, Hristo Valchanov

Система за генериране на DoS мрежови атаки

Мартин Тодоров, Христо Вълчанов

The variety of DoS attacks and their growing makes the protection of networks extremely difficult. The network protection is very important in today's Internet world. This requires the development of tools for analyzing the attacks to help in the training of specialists in network security. This paper presents the architecture and features of system for generating network DoS attacks. The system allows the implementation of several of the most popular and used DoS network attacks and helps for understanding the principles behind them.

Key words: *Computer Networks, DoS attacks, Network Security*

ВЪВЕДЕНИЕ

Мрежовите атаки за отказ на услуга (Denial of Service – DoS) имат за цел да спрат достъпа до определена услуга, а също така и да затруднят трафика в големи компютърни мрежи посредством техниката на „наводняване" (flooding) в общоприетия случай [2]. Други срещани цели на атаките са компрометиране на сигурността на система или устройство, нерегламентиран достъп до ресурсите на дадена система или отказ на достъп за регламентираните потребители. Често такъв вид атаки се организират групово (известни като разпределени - DDoS атаки) [8]. Атаки от подобен вид се считат за престъпление поради огромната вреда, която нанасят. Когато бъде стартирана такъв вид атака срещу сървър предоставящ услуга, това се отразява на цялата мрежа и трафикът заема в идеалния за атакуващия случай цялата честотна лента, което причинява проблеми за достъпа на всички потребители.

Като се вземе предвид съвременната зависимост на потребителите от Интернет като най-масовото средство за комуникация, пазаруване, трансфер на активи и предаване на ценна информация, нуждата от защита срещу всякакви опити за посегателство върху този трафик, както и осигуряването на надежден достъп до използваните ресурси и услуги е огромна. Проблемът със самата защита е повече от комплексен и включва множество политики за сигурен достъп до мрежата, използване на различни мрежови архитектури и устройства (например защитни стени), правилно конфигуриране на услугите и други. Всички тези фактори налагат задълбочено изследване и запознаване с тези атаки, за да можем да се предпазим от тях. Това, от своя страна, налага разработването на средства за анализ на атаките, които да помогнат при обучението на специалистите по мрежова сигурност [7].

Подобни средства трябва да предоставят възможности както за ефективна реализация на атаки, така и за разбиране в детайли на механизма на тяхното действие. Това ще позволи мрежовите администратори да определят как изглежда една атака, какви са нейните симптоми и какви действия трябва да се предприемат за нейното неутрализиране.

Известни са редица средства за генериране на атаки. Продуктите BackTrack Linux [1], както и Kali Linux [6], предназначени за тестване против неоторизиран достъп до системи, са реализирани като отделни дистрибуции. Това, обаче затруднява тяхното използване, както и налага отделяне на повече време за конфигурирането им. Друг недостатък е, че добре направеният графичен интерфейс, който помага за бързите и интуитивни стартирания, не позволява по-задълбочено вникване в протоколите и използваните средства за атака. Други средства, като

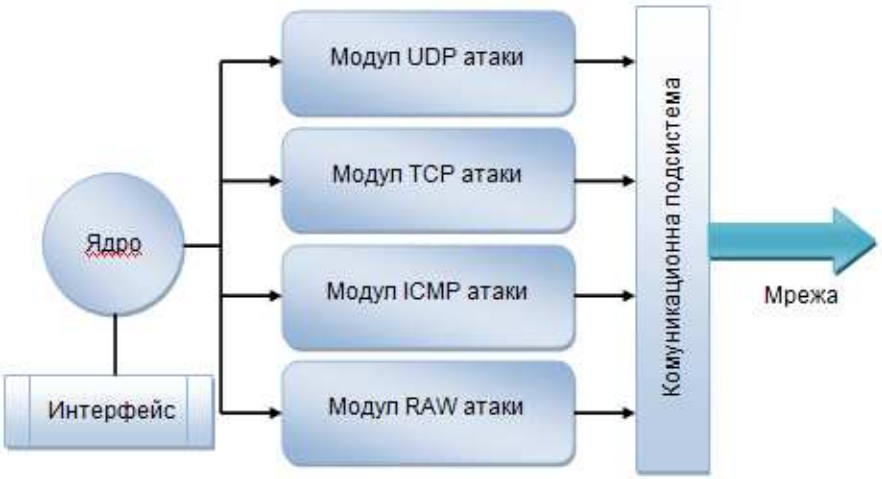
L0phtCrack [5] и Low Orbit Ion Cannon [3], които са тясно специализирани за осъществяване на неоторизиран достъп в системи, не дават разнообразие в използваните методи за атаки.

Настоящият доклад представя особеностите на система за генериране на мрежови DoS атаки, която предоставя възможност за прилагане на няколко от най-често разпространените и използвани атаки по начин, удобен за усвояване на принципите, стоящи зад тях. Системата е изключително удобна за обучение на мрежови администратори, които могат да тестват мрежата и устройствата си за пропуски в софтуера и конфигурирането им, както и за правилно структурирана топология и защита.

.

АРХИТЕКТУРА НА СИСТЕМА ЗА ГЕНЕРИРАНЕ НА АТАКИ

Архитектурата на системата за генериране на атаки има модулен характер (фиг. 1). Предимството в сравнение с представените подобни средства е постигане на гъвкава функционалност. От една страна се дава възможност за лесно модифициране на действията при генерирането на атаки, а от друга страна функционалността може да бъде разширявана чрез добавяне на нови модули, реализиращи нови атаки.



Фиг. 1. Архитектура на системата

Системата е разработена на C++ под управлението на ОС Linux.

Ядрото реализира базовата функционалност като координира работата на останалите компоненти.

Модулите за атаки реализират атаките по трите основни протоколи – UDP, TCP и ICMP [4]. Обособяването на три базови модула се определя от спецификата на формиране на пакетите за тези базови протоколи. Всеки от модулите включва отделни библиотеки, които се зареждат към ядрото на системата при нейното стартиране. Една библиотека реализира един тип атака. Необходимите библиотеки се определят от различните видове атаки, които ще се генерират за целта на тестовете, като те се указват в конфигурационен файл. Тази организация позволява постигане на гъвкавост при разширението на системата с нови функционалности. Особеност на представяната система в сравнение с подобни такива е наличието на специален RAW модул, чрез който потребителят има възможност да генерира пакети за мрежови атаки на основата на други протоколи.

Модулът за UDP атаки реализира UDP flood атака, изпращайки множество UDP пакети към определен порт на целевата машина с цел блокиране на услуга и генериране на голям трафик. Модулът TCP реализира SYN flood атака с цел заемане на ресурси от дестинацията. Модулът за ICMP генерира два типа атаки по този протокол – Ping of Death, при която се препълват буферите на приемащата

машина и Smurf атака с цел генериране на огромен трафик в определен мрежови сегмент. Модулът за RAW атаки реализира ARP Spoofing при която се подменя MAC адрес в адресната таблица.

За връзка с потребителя е разработен опростен интерфейс. Текущата реализация е конзолна с цел максимална съвместимост и може да се изпълнява под всяка Linux дистрибуция. Потребителят може да задава допълнителни параметри към генератора на атаката, като, например, размер на пакетите, брой, времетраене и др.

Комуникацията през мрежата се осъществява от комуникационната подсистема и е реализирана на базата на механизма на сокетите.

ЕКСПЕРИМЕНТАЛНИ ИЗСЛЕДВАНИЯ И РЕЗУЛТАТИ

Целта на експериментите е да се изследва функционалността на представената система в реална мрежова среда. Експериментите са проведени в локална мрежа, включваща маршрутизатори и хостове с цел доближаване до реална обстановка. Локалната мрежа е изолирана физически от останалите мрежи от гледна точка недопускане на вредно влияние по време на тестовете. Атакуващата машина е под управлението на Linux Slackware 3.10. Атакуваните машини са с операционни системи Linux и Windows 7.

Първата група тестове е за UDP атака. Атакува се машина, на която има стартиран DNS сървър (порт 53). За анализиране на получения трафик се използва програмата tcpdump. На фиг.2 е показана прехванатата комуникация на атакуваната машина.

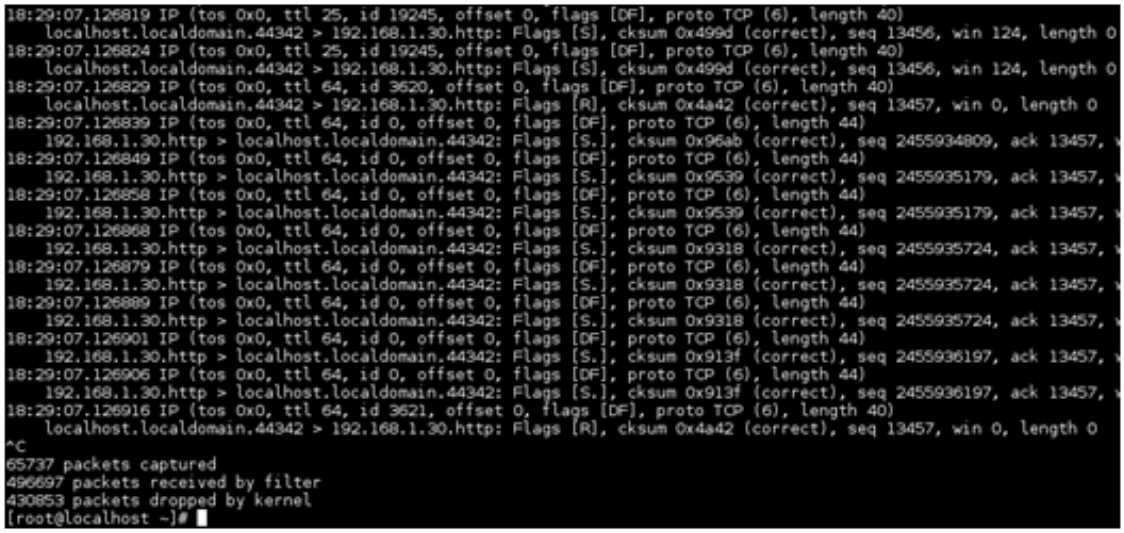
```
18:51:31.460311 IP (tos 0x0, ttl 64, id 61253, offset 0, flags [DF], proto UDP (17), length 29)
    192.168.1.24.54321 > 192.168.1.30.domain: [udp sum ok] [|domain]
18:51:31.460316 IP (tos 0x0, ttl 64, id 61254, offset 0, flags [DF], proto UDP (17), length 29)
    192.168.1.24.54321 > 192.168.1.30.domain: [udp sum ok] [|domain]
18:51:31.460323 IP (tos 0x0, ttl 64, id 61255, offset 0, flags [DF], proto UDP (17), length 29)
    192.168.1.24.54321 > 192.168.1.30.domain: [udp sum ok] [|domain]
18:51:31.460329 IP (tos 0x0, ttl 64, id 61256, offset 0, flags [DF], proto UDP (17), length 29)
    192.168.1.24.54321 > 192.168.1.30.domain: [udp sum ok] [|domain]
18:51:31.460335 IP (tos 0x0, ttl 64, id 61257, offset 0, flags [DF], proto UDP (17), length 29)
    192.168.1.24.54321 > 192.168.1.30.domain: [udp sum ok] [|domain]

3443 packets captured
177566 packets received by filter
161060 packets dropped by kernel
root@sdhx:~#
```

Фиг. 2. UDP атака към DNS сървър

Изходът от анализатора показва множеството изпратени пакети, като не е възможно всичките да бъдат обработени от ядрото.

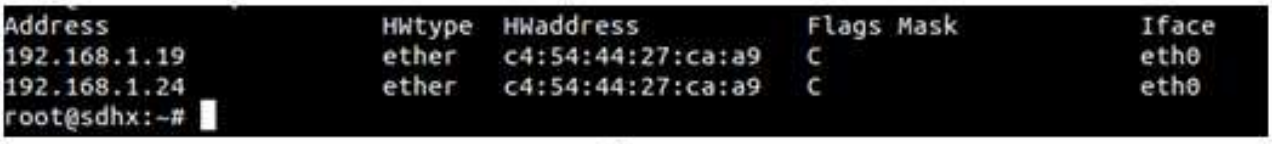
При SYN flood атаката се използва като услуга Apache HTTP сървър (фиг. 3). Характерно за този тест е, че се наблюдава и обратен трафик, с който атакуваната машина връща SYN-ACK пакети за потвърждение на отправените заявки. При опит за достъп до web страница на тази машина, изтича таймаута на браузъра, което е доказателство за ефективността на атаката.



Фиг. 3. SYN flood атака към HTTP сървър

Следващият тест е ARP Spoofing атака. При нея се изпраща като отговор фалшив MAC адрес на маршрутизатора в сегмента. На фиг.4-а е показан ARP кеша на атакуваната машина преди атаката, а на фиг.4-б – след атаката.

а)

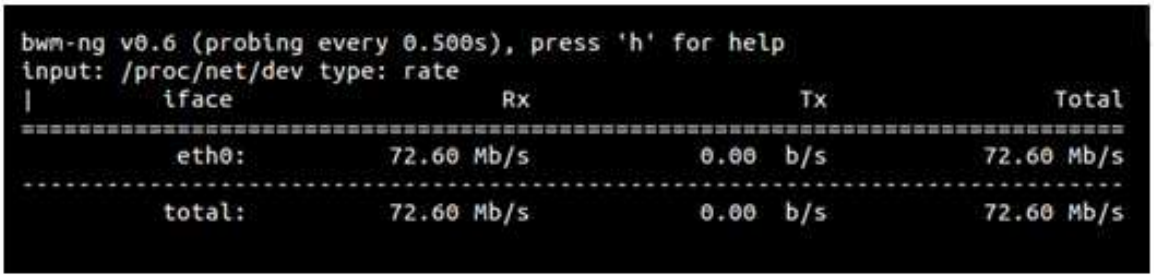


б)

Фиг. 4. ARP Spoofing атака

Резултатите показват, че MAC адресът на маршрутизатора (20:aa:4b:af:da:00) е подменен след атаката (c4:54:44:27:ca:a9) в адресната таблица. След този момент, всичкия изходящ трафик от атакуваната машина ще бъде препращан към и прехващан от атакуващата машина.

При теста с Smutf атака, атакуващата машина изпраща ICMP echo request пакети със сменен IP адрес на източника с този на атакуваната машина към броадкаст адрес на мрежа. Резултатът е пълно блокиране на мрежата на атакуваната машина поради огромния брой изпратени пакети. На фиг. 5 е показан моментният трафик на атакуваната машина. Резултатите са изведени с програмата bwm-ng и показват ефекта от атакуването ѝ – изключително голям входящ трафик в нейната мрежа.



Фиг. 5. SMURF атака

ЗАКЛЮЧЕНИЕ

Разнообразието от DoS атаки, както и постоянното им развитие прави защитата от тях изключително трудна и актуална. Поради това, с придобиването на необходимите познания върху естеството на атаките, както и върху функционалността и свойствата на системите за превенция, в повечето случаи е напълно възможно да бъде изградена достатъчно сигурна защита. Това от своя страна изисква разработването на средства, които да помогнат на специалистите по мрежова защита за постигане на ефективна превенция срещу опасностите и вредите, породени от тях.

Настоящият доклад представя архитектурата и особеностите на система за генериране на мрежови DoS атаки. Нейната архитектура има модулна структура, което позволява удобно и ефективно бъдещо разширение на нейната функционалност. Проведените експерименти показват, че предлаганата система има пълна функционалност по отношение на базовите мрежови атаки.

Цел на бъдеща работа е разработване на допълнителни компоненти за други атаки, изискващи по-специални средства за реализация, както и графичен интерфейс за по-удобно манипулиране с параметрите на атаката.

ЛИТЕРАТУРА

[1] Backtrack Linux. http://www.backtrack-linux.org/.
[2] Denial of Service Attacks. http://www.cs.utexas.edu/users/chuang/dos.html.
[3] Denial-of-Service Tools & Techniquies. http://null-byte.wonderhowto.com/how-to/hack-like-pro-denial-service-dos-tools-techniques-0165699/.
[4] Internet Engineering Task Force. http://www.ietf.org.
[5] L0pthCrack. http://sectools.org/tool/l0phtcrack/.
[6] Smeth D. *Kali Linux Cookbook*. Packt Publishing. 2013.
[7] Stallings W. *Computer Security: Principles and Practice*. Pearson, 2014.
[8] Yu Shui. *Distributed Denial of Service Attack and Defense*. Springer-Verlag. 2014.

За контакти:

Доц. д-р инж. Христо Вълчанов, Катедра “Компютърни науки и технологии”, Технически университет-Варна, тел.: 052 383 424, e-mail: hristo@tu-varna.bg

Инж. Мартин Тодоров, Катедра “Компютърни науки и технологии”, Технически университет-Варна, e-mail: sdxh19@abv.bg