СОФИЙСКИ УНИВЕРСИТЕТ “СВЕТИ КЛИМЕНТ ОХРИДСКИ”
ФАКУЛТЕТ ПО МАТЕМАТИКА И ИНФОРМАТИКА

гл. ас. Стела Иванова Русева

ИЗГРАЖДАНЕ НА СИСТЕМА ЗА ЗАЩИТА ОТ DDOS АТАКИ

АВТОРЕФЕРАТ

на дисертационен труд
за получаване на образователна и научна степен
“Доктор”
по научна специалност 01.01.12
“Информатика- Компютърни мрежи и архитектури”

Научен ръководител:
професор д-р Нина Василевна Синягина

София
2012

1. Обща характеристика на дисертационния труд

1.1. Актуалност

В периода на активно развитие и внедряване в ежедневието на информационните технологии важна роля има надеждността на компютърните системи, осигуряващи достъпа до информацията и нейното съхраняване. Но едновременно с растежа на важността на информацията растат и загубите, понесени вследствие на кражба, разрушение или отсъствие на достъп до една или друга информация. Атаката, довеждаща до невъзможност за получаване на информация или до невъзможност за по-нататъшна работа на компютърните системи без претоварване, се нарича "атака отказ от обслужване" - DoS (Denial of Service). Този род атаки препятстват или напълно блокират отговорите от услугите на законните потребители.

Атаките DoS винаги са злонамерени и към настоящия момент съществува огромно количество готови средства за реализирането им даже от непрофесионалисти. На практика е много по-лесно да се наруши работата на мрежата или системата, отколкото да се получи неоторизиран достъп. Атаката “отказ от обслужване” съществено е променила Интернет, показвайки слабостите в защитата на използваните технологии.

Характерна особеност на DoS и DDoS (Distributed- разпределени DoS) атаките е, че без предварителна подготовка предотвратяването им е невъзможно. Още по-неприятен факт е, че даже в случай на предварителна подготовка, противодействието им е трудно реализуемо. За съжаление повечето сървъри в Интернет не са защитени добре със защитна стена или с по-сложна защита от типа на предотвратяване на атаките. Необходима е система за анализ на аномалиите на база на изкуствения интелект, използваща математически алгоритми за решаване на проблема с претоварване на мрежата. На практика това са разработки на множество институти, години практическо изучаване на DDoS атаките и резултати от

десетки дисертации. Защитата от DDoS е сложна програма, изискваща висока концентрация на последните постижения в областта “анализ на трафика”, която в автоматичен режим реагира на атаката. Методите на атаката могат да се променят динамично и системата следва да проследи и предприеме съответните мерки.

Независимо от това че съществуват голямо количество изследвания и разработки в света, в повечето случаи те не се предоставят на широката публика, липсват публикации за конкретните разработки. Готовите продукти на различните фирми обикновено са недостъпни за използване за условията в България поради високата си цена. Основно това се отнася за обикновени потребители, използващи сървъри на базата на GNU/Linux.

Разнообразието от заплахи, застрашаващи потребителя, работещ в мрежата, е огромно. Част от тях представляват плащане за използването на сложни информационни технологии, уязвими за външни въздействия, друга част е свързана с човешката дейност.

1.2. Цел и задачи на дисертационния труд

Поради изложените причини в настоящия дисертационен труд се поставя следната **цел**:

Изследване на методи и начини за защита на компютърна система от DDoS атаки, които позволяват получаване на оптимална сигурност и достъпност на ресурсите.

За реализация на поставената цел се формулират следните конкретни **задачи**:

1. Определяне на оптимална конфигурация на системата за защита от DDoS атаки.
2. Създаване на модел на система за защита, описващ взаимодействието на сървъра и клиентите.
3. Разработка на алгоритми и програмна реализация на системата за защита.

4. Имплементация на комплекс от програмни средства, предпазващи от DDoS атаки и експериментална верификация на създадените средства.

1.3. Кратка анотация на дисертационния труд

Представената дисертация се състои от четири глави.

В първата глава се прави обзор на различните видове атаки “отказ от обслужване” с описание на начина на функционирането им, както и на метода за тяхното откриване и блокиране. Представено е състоянието на проблема и е предложена класификация на този род атаки. Показани са най-перспективните разработки в областта ”защита на компютърните мрежи”, свързана с противоборството с DDoS атаки.

Във втората глава е представен разширен анализ на подходите за изграждане на система за защита. Избрана е x86 архитектура, ОС GNU/Linux (CentOS 6), HTTP сървър Apache2.2, PHP5.3, MySQL5.0, мрежов филтър netfilter.

В третата глава е представен модел на системата, описващ взаимодействието на сървъра с клиентите, отчитащ характеристиките на компютърната мрежа и на защитавания сървър. Представен е и модел, отчитащ загубата на пакети в мрежата, причинена от TCP SYN атака.

В четвъртата глава е направено описание на програмната реализация на система за защита, получила името Ruslan (събирателно от трите имена на автора: **Rus**eva Ste**la** Iva**n**ova). Определени са компонентите, алгоритмите, конфигурацията на елементите и настройката на параметрите, позволяващи оптимална защита на уеб сървър от DDoS атаки. Представена е експериментална проверка и анализ на получените резултати.

Към дисертацията е приложен списък с цитирани източници (литература и онлайн адреси) и списък с авторските публикации.

2. Съдържание на дисертационния труд

2.1. Глава първа- Атаки от типа DoS и DDoS

В първата глава е представена е класификация на известните видове DDoS атаки и методи за борба. Направен е обзор на съвременните методи и средства за защита на компютърни системи и мрежи и констатация на постиженията в противоборството срещу DDoS атаките. Дефинирани са базовите функции, които една система за защита от DDoS атаки трябва да предоставя.

Причини за използване на атаки от типа DoS

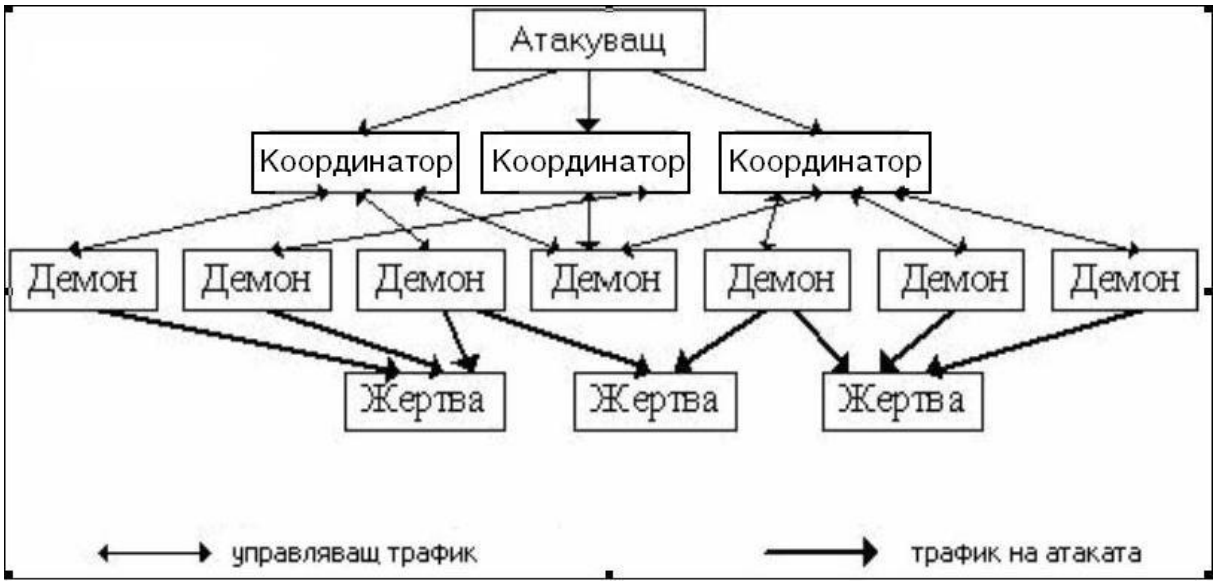
- лошо конфигурирани хостове;
- използване на известните грешки в програмното осигуряване.

По същество атаката DoS нарушава или напълно блокира обслужването на легитимните потребители на мрежите, системите или на други ресурси.

DDoS атаките се отличават принципно от DoS. С появата им се променя и концепцията за провеждане на атаките и в повечето случаи съществуващите средства за откриване като IDS (Intrusion Detection System) се оказват безсилни. Атаките са вече на три нива. Както се вижда от фиг. 1.1., злосторникът директно не взаимодейства с жертвата. Той действа с помощта на координатори (master) и демони (daemon). Координаторите обикновено са няколко и са разположени на хостове с голям трафик (с широк канал в Интернет). В случай на увеличаване на предаваната (приеманата) информация остават незабелязани. Друг важен момент е, че често пъти са сървъри (постоянно са включени), а за отстраняване на координатора е необходим рестарт на компютъра. След установяването на един или няколко координатора следва установяването на демоните. Демон е програма от тип троянски кон, която се установява

на чужда машина, често пъти с използване на известните грешки в програмното осигуряване. След установяването на машините на демоните те се свързват с един от координаторите и получават от него команди. В този случай за прекратяване на атаката е необходима неутрализацията на демоните. Проблем е, че компютърът, на който е установен демонът, нищо не подозира. Единственият възможен вариант е прехващане на управлението над координатора, но това е реализирано в по-новите версии на програмното осигуряване за реализация на разпределени атаки. Демонът след старта на атаките може повече да не се подчинява на командите на координатора. Последното увеличава вероятността за успешната реализация на атаката. Но има и минус за хакера, понеже в този случай той няма да може повторно да използва тази мрежа от демони за по-следваща атака.

Ако при DoS атаката е достатъчно добавянето на едно правило за филтрация на пакетите на защитна стена, то при разпределените атаки е необходимо тези правила да са няколко хиляди (атаката се реализира едновременно от няколко хиляди демона). Повечето защитни стени не са способни да обработват толкова голям брой правила.



Фигура 1.1. DDoS атака

Атакуващият получава достъп до множество хостове, работещи в Интернет, често пъти използвайки автоматизирани програми, известни като автомаршрутизатори, и установява програмно осигуряване на DDoS (такова съществува в много варианти). Това програмно осигуряване позволява на атакуващият отдалечено да управлява този хост в качеството на демон (подчинен на атакуващия). От управляващия хост атакуващият информира демоните за хоста-цел и насочва атаката. Хиляди хостове могат да бъдат контролирани от една точка. Времето за стартиране, времето за спиране, адресът на целта и типът на атаката- всичко това се предава от координатора на демона посредством Интернет. Използваната за тази цел една машина може да създаде трафик няколко мегабайта. Няколко стотин машини могат да създадат трафик няколко гигабайта. Отчитайки този факт, лесно се разбира колко разрушителна може да бъде тази внезапна висока активност за практически всякаква разрушителна цел.

Видове атаки от типа (D)DoS

Броят на средствата, предназначени за реализация на DDoS атаки, нараства ежемесечно, поради което, да се представи пълният им обзор, е невъзможно. Затова ще се ограничим с представянето на основния инструментариум: TFN; Trinoo; Stacheldraht; TFN2K; WinTrinoo; запълване канала на жертвата; недостиг на ресурси на жертвата; грешки в програмирането; маршрутизация и атаки на DNS сървър; атака Smurf; атака с помощта на препълване с TCP SYN пакети; DNS атаки; препокриване на фрагментите на IP пакетите; Stream и raped атаки; паника на ядрото и др.

DDoS атаките могат условно да се категоризират в три големи групи:

- атаки с голям брой формално коректни, но възможно, фалшифицирани пакети, насочени към изтощаване на ресурсите на хост или мрежа;
- атаки със специално конструирани пакети, предизвикващи общ срив на системата поради грешки в програмите;
- атаки с фалшифицирани пакети, предизвикващи изменения в конфигурацията и/ или състоянието на системата, което води до невъзможност за предаване на данни, блокиране на съединението или рязко намаляване на ефективността му.

Разработени са различни схеми за класификация на механизмите за защита от DDoS атаки. Те структурират предметната област на DDoS и облекчават търсенето на начина за защита.

Организацията CERT (Computer Emergency Response Team) е разработила редица препоръки и изисквания към потребители и доставчици на Интернет с цел предотвратяване на DDoS атаките и минимизация на последствията от тях.

Програмно-апаратни средства за защита от DDoS атаки:

- FloodGuard;
- Arbor Peakflow SP;
- Cisco Guard, Cisco Traffic Anomaly Detector, Anomaly Guard Module и Traffic Anomaly Detector Module;
- хибридни системи за откриване на атаките (Prelude IDS);
- виртуални системи за откриване на атаките;
- многослойни системи (multitiered IDS); шлюзови (gateway IDS);

- системи с контрол на състоянието (stateful IDS); основани на спецификации (specification-based IDS) или на стека (stack-based IDS).

Общият подход за защита от DDoS атаките включва реализацията на следните елементи:

1) защита от DDoS атаки;
2) откриване на атаката;
3) определяне на източника на атаките;
4) противодействие на атаката.

Изводи

1. Практически всеки сървър (HTTP, FTP, DNS, SMTP, POP3, бази данни, системи за търсене) е уязвим за DDoS атаки. Ефективно противодействие на този род атаки до настоящия момент не е открито и специалистите се ограничават единствено с даване на препоръки.
2. През последните години тенденцията е в посока, че все по-малко знания и навици са необходими за реализация на този род атаки и следователно все повече знания и умения е наложително да владее системният администратор за да защити мрежата си.
3. Да се предотвратят DDoS атаките, не е лесна задача поради трудности, свързани с откриването им. Констатирането на началото на атаките от този род, сравнено с нормалната работа на сървъра, се определя от огромен брой фактори, които е нереално да бъдат отчетени с единствен алгоритъм за реализация на защитата.

4. Към настоящия момент най-добрата техника за защита е готовността за такава атака. Много е важно да има план за реагиране на DDoS.

2.2. Глава втора- Методи и средства на защита на HTTP сървър

В тази глава са разгледани особеностите на уеб сървър от гледна точка на средства за противодействие на DDoS атаки. Определени са базови защитни механизми и методи за изграждане на защитната система.

С цел да се проведе прецизно изследване на системата, изграждаща защитата от атаките, авторът избира за целта LAMP сървър.

Обемът на паметта е един от най-важните ресурси на сървъра. Често пъти администраторите залагат на базовите параметри, зададени от разработчиците, но обикновено това се оказва недостатъчно.

От способностите на администратора да се ориентира в аспектите на управлението на паметта зависи производителността, устойчивостта и работоспособността на системата.

Сървърът поддържа множество броячи (няколко стотин, в зависимост от процесора, обема на паметта, хард диска) и следи за непривишавена на квоти.

Тук възниква проблема с точно заделяне на памет.

Операционната системата полага усилия да използва икономично цялата налична оперативна памет. Ако паметта не е заета с процеси, тя се пренасочва за буферизация (кеширане) на данни.

За виртуализация на LAMP стека е избрана технологията OpenVZ. Тя се използва най-масово в уеб хостинга.

Програмата **sysctl** и командата **ulimit** чрез управлението на параметрите на ядрото на ОС позволяват ограничаването на системните

ресурси. Това може да помогне в ситуациите, когато например се пускат прекалено много процеси и системата не отговаря на заявките или когато зададените по премълчаване параметри са недостатъчни за ефективната работа на приложението.

За да бъде осигурена защитата от DDoS атаките трябва да бъдат извършени редица изминения в параметрите на ОС Linux, позволяващи преконфигуриране на ядрото и на TCP/IP стека.

Разгледани са параметрите на IP протокол, TCP протокол, netfilter.

Основни правила за защита на системите

- Редовна проверка на системите за наличие на уязвимости. За целта се използват множество експлойти (exploit) и техни архиви в Интернет. Инсталиране на всички необходими кръпки и обновления.
- Изключване на всички ненужни услуги.
- Осигуряване на филтрация за пакети, чиито IP адреси на източника са неверни.
- Оптимизиране на структурата на маршрутизация в мрежата. Задаване на списъци за ограничаване на достъпа до маршрутизатора, реализиращ пакетен филтър.
- Използване на защита на няколко нива срещу отдалечените атаки.
- Осъществяване на мониторинг и незабавно реагиране на всякакви подозрителни действия (промяна на IP или MAC адреса и т.н.).

Средства за противодействие на атаката

За решаване на проблема се предлага да бъдат използвани следните подходи:

1) На нивото на сървъра;
2) На ниво услуги на сървъра;
3) На нивото на мрежата;

4) На ниво доставчик;
5) На апаратно ниво;
6) На ниво администратори на сървъра;
7) Комбинирано използване на всички системи.

Най-простото решение за блокиране на атаката е забраната за преминаването на трафика между двете мрежи. Но това ще доведе до невъзможността за достъп до услугите на сървъра, с което се възпрепятства нормалната му работа. Затова този метод се използва единствено при някои видове атаки, основно построени на база на протокола ICMP.

Втори подход за блокиране на DDoS атаките е филтрация на трафика на база IP адреси на злосторниците. Този вариант е най-ефективният от всички, но работи единствено в случай, ако съществува уверенност, че IP адресът на източника в пакета, съдържащ признаци за атаката, принадлежи действително на злосторника и не е подменен от него. Понеже проследяването на всеки уникален адрес не е проста задача, изискват се определени изчислителни ресурси, затова по-практично решение е филтрация на трафика на база диапазон от адреси. Макар че в този случай е реално блокирането на оторизирани потребители, намиращи се в един диапазон със злосторниците. Въпреки това този метод "има право на живот".

Друг вариант за блокиране на DDoS атаките позволява задържане на трафика и пропускане от време на време на неголеми фрагменти от входящия поток в защитаваната мрежа. И макар че в тези пропуснати пакети е възможно да се намира и враждебен трафик, намаленият обем на трафика няма да позволи падането (излизането от строя) на защитаваните сървъри. Този метод е особено ефективен при наводняване на сървъра с TCP SYN пакети и подобните им атаки.

Следващият възможен вариант за предотвратяване нарушаването на работоспособността на сървъра е аналогичен на този, който се използва от класическите средства за откриване на мрежови атаки. Това средство за блокиране на DDoS атаките е филтрация на трафика на базата на предварително зададени признаци (порт на източника, време на живот (TTL- time to live), идентификатор на пакета и т.н.).

Изводи

1. Да се създаде абсолютно защитена мрежа, е невъзможно до момента, до който вероятността от взлом на системата за защита не достигне нулева стойност (и обратното - докато надеждността на защитата не достигне единица). Последното е възможно единствено в случай, че се отстрани от процеса на създаване на защитното средство или механизъм (както и от създаване на системата по принцип) човешкият фактор, явяващ се главна причина за всички грешки. Във всяка ситуация винаги присъства човешкият фактор, който внася в изглеждащата стройна система всевъзможни проблеми, нарушаващи трудно намерения паритет между отбраната и нападението. Явно е, че на съвременния етап на развитие на науката и информационните технологии това е невъзможно.

2. Надеждността даже на суперзащитената система може да бъде сведена до нулата чрез некачествена или неграмотна настройка. Всяка система изисква квалифициран персонал, не само знаещ, но и умеещ грамотно да настройва средствата за защита. Това допълнително доказва необходимостта от обучение.

3. Несвоевременното реагиране (или неговото отсътствие) на опитите за проникване в корпоративната мрежа също я правят незащитена.

4. Предотвратяването на DDoS атаките е сложна задача. Практически тя се решава единствено чрез отхвърлянето на части от данните, пристигащи към сървъра, при което отхвърлянето следва да работи и

преди сървъра (по маршрута към него). Такава схема има сериозни недостатъци: необходима е координацията на действията Интернет доставчика, което не винаги е възможно; съществува вероятност да бъдат отхвърлени данни на легитимните потребители, неучастващи в атаките.

5. Проблемът DDoS може да бъде решен единствено чрез всеобщи усилия и по-строги стандарти за безопасност. На първо място, администраторите и домашните потребители са длъжни в еднаква степен да са сигурни, че техните компютри са защитени. Демоните, използвани в DDoS атаките, са продукт от работата на програми, които сканират хиляди хостове, като разбиват уязвимите от тях и установяват съответното програмно осигуряване. Инсталирането на последните кръпки, спирането работата на ненужните услуги, използването на базова защитна стена за филтрация ще помогне на съответния хост да не се превърне в жертва и участник в такива атаки. Желателна е редовна проверка на собствените хостове за наличие на уязвимости.

2.3. Глава трета- Изграждане на математически модел, описващ взаимодействието на сървъра с клиентите

В тази глава се разглежда модел за взаимодействие на сървъра с клиентите, като за входните параметри за този модел се приемат характеристиките на сървъра и пропускателната способност на комуникационния канал, а изходният параметър представлява признак за присъствие или отсъствие на TCP SYN атака.

След проведен анализ на съществуващите направления в съвременната наука в областта на моделиране на наводняване в компютърните мрежи авторът избира в качеството на математически апарат теорията на системите за масово обслужване (СМО), спецификата на която добре подхожда за решаването на поставената задача.

Под система за масово обслужване се разбира съвкупност от обслужващи устройства и обслужвани заявки на клиенти.

Максималният брой на заявките, които могат да се обслужат едновременно, определят пропускателната способност на системата за обслужване.

Характерно за една СМО е, че заявките постъпват нерегулярно.

Поради случайни фактори, броят на заявките за даден интервал от време е случайна величина. Времето за обслужване- също.

В теорията на масовото обслужване се приема, че входящият поток от заявки е разпределен по Поасонов закон за разпределение. Поасоновият поток напълно се определя с параметъра интензивност на потока λ. На практика λ се изчислява статистически.

Математическият апарат на теорията за масово обслужване позволява да се определят основните параметри на системата: среден брой заети устройства, вероятност за отказ при обслужването на заявките, средна дължина на опашката, средно време за престой на заявката в опашката и други.

Означаваме с μ интензивността на потока за обслужване, т.е. среден брой заявки, обслужвани за единица време.

Средният брой заети устройства се изчислява съгласно следната зависимост:

$$N = \sum_{k=1}^{n} k \cdot p_k = p_0 \sum_{k=1}^{n} \frac{\alpha^k}{(k-1)!} = \alpha(1 - p_n), \qquad (3.3)$$

където n е броят на устройствата в системата,

$\alpha = \lambda / \mu$ - коефициент за натоварване или капацитет (тази величина показва средния брой заявки, пристигащ за средното време за обслужване на една заявка),

λ - интензивност на потока от заявки,

p_k - вероятност в системата да се намират точно k заявки.

$$P_k = \frac{\frac{\alpha^n}{k!}}{\sum_{i=0}^{n} \frac{\alpha^i}{i!}} \qquad (3.4)$$

Представените съотношения позволяват определянето на средния брой заявки, намиращи се в системата за масово обслужване.

Разглеждаме множеството TCP SYN пакети, постъпващи в сървъра, в качеството на входящ поток от заявки.

В нормален режим на работа в отговор на всеки получен TCP SYN пакет сървърът е длъжен да изпрати TCP SYN+ACK пакет. От това, че съществува взаимно еднозначно съответствие между входящия и изходящия пакет, следва еквивалентност на потоците. В качеството на заявки в СМО ще разглеждаме изпращаните от сървъра SYN+ACK пакети. Под множество от обслужващи устройства разбираме ресурсите на сървъра, предназначени за съхраняване на параметрите на TCP съединението. В тази интерпретация обслужването на заявките означава резервиране на съответстващи ресурси или до успешно установяване на TCP съединението (получаване на ACK пакета, който е длъжен да бъде получен), или до изтичане на зададеното за сървъра време.

За този модел признакът за наличие на TCP SYN атака се явява рязкото нарастване на броя на заявките в СМО. Подложен на въздействието на атаките, сървърът заделя съответните ресурси, които остават заети в течение на зададеното време. За съвременните операционни системи и мрежови технологии времето (от десетки секунди до няколко минути) е достатъчно, за да бъдат заети всички достъпни ресурси на сървъра, предназначени за съхраняване на параметрите на TCP съединението. За разглеждания модел това означава рязко нарастване на заетите обслужващи устройства.

Авторът предлага представянето на ресурсите на сървъра в качеството му на система от обслужващи устройства. Параметрите на TCP съединението се съхраняват в съответстващ буфер [53], който може да се представи във вид на масив с размер L, елементите на който съхраняват параметрите на TCP съединението. Последните могат да се разделят на три типа: съдържащи параметрите на установените съединения, на полуотворените съединения и тези на свободните ресурси. Нека B е броят на отворените в дадения момент TCP съединения. Тогава $n = L - B$ е броят на елементите от втория и третия тип, съвкупността на които ще се разглежда в качеството на множество от обслужващи прибори на СМО. При това заетите с обслужване на заявките устройства са елементи от втория тип.

Модел, отчитащ загубата на пакети в мрежата

При условие че при клиента е реализиран коректно TCP протокол, появата на полуотворени съединения, които не са установени в течение на интервала време $T_{пр}$, се обяснява със загубата на SYN+ACK или на ACK пакет. Затова към заявките от втория тип ще се отнасят заявките, за които TCP съединението се намира в полуотворено състояние по-дълго от $T_{пр}$. Означаваме с s и l броят на съединенията от първия и от втория тип съответно.

Ще определим съотношенията, описващи състоянието на такава система. Средният брой на полуотворените съединения е:

$$N = s + l = \alpha_1 + \alpha_2 = \frac{\lambda_1}{\mu_1} + \frac{\lambda_2}{\mu_2} \qquad (3.9)$$

Средният брой на полуотворените съединения е случайна величина, равна на сумата на двете случайни величини с Поасонов закон за разпределение. Първата от тях описва средния брой полуотворени

съединения, които не представляват заплаха като TCP SYN атака. Втората съставна представлява полуотворените съединения, които няма да бъдат установени и след зададен интервал от време ще бъдат изтрити, като до тогава ще заемат ресурси на сървъра. Както беше отбелязано, увеличаването на броят на такива съединения е признак за TCP SYN атака. Затова е целесъобразно да се разглежда СМО само от втория тип. Ще разглеждаме системата, в която постъпват като заявки не всички SYN+ACK пакети, за които сървърът очаква ACK пакет, а само тези, за които времето на очакване превишава праговата стойност $T_{пр}$. Очевидно, че при нормална работа (отсъствие на TCP SYN атака) за всяка такава заявка е бил загубен SYN+ACK или ACK пакет. Интензивността на постъпване на такива заявки се определя от следващото съотношение:

$$\lambda_2 = \lambda \cdot P_{по} \ , \tag{3.10}$$

където:

λ – интензивност на постъпващите на входа на мрежовата карта на сървъра TCP SYN пакети,

$P_{по}$ – вероятността за поява на полуотворено съединение, което няма да бъде установено.

Параметърът $P_{по}$ зависи от качеството на работа на мрежата, което се характеризира с вероятността за загуба на пакета в мрежата ($P_{зп}$). Нека събитието A да представлява загуба на SYN+ACK пакет, а събитието B да представлява загуба на ACK пакет.

Понеже събитието B може да настъпи само тогава, когато не е настъпило събитието A (ACK пакетът може да бъде изпратен единствено след получаването на SYN+ACK пакета), тогава неговата вероятност ще е равна на:

$$P(B) = P(\overline{A}) \cdot P_{зп} = (1 - P_{зп}) \cdot P_{зп} \tag{3.12}$$

Ще разгледаме събитието C, изразяващо се в появата на полуотворено съединение от втория тип:

$$P_{по} = P(C) = P(A+B) = P(A) + P(B) = \\ = P_{зп} + (1 - P_{зп}) \cdot P_{зп} = P_{зп} + P_{зп} - P_{зп}^2 = 2P_{зп} - P_{зп}^2 \quad (3.13)$$

От съотношенията (3.10) и (3.13) намираме интензивността на потока от заявки от втория тип:

$$\lambda_2 = \lambda \cdot P_{по} = \lambda \cdot (2P_{зп} - P_{зп}^2) \quad (3.14)$$

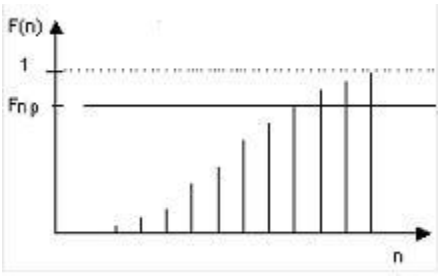
В съвременните ОС ядрото изпраща няколко копия SYN+ACK пакети до тогава, докато не бъде получен ACK пакет. Означаваме броят на тези копия с N_{SA}. Тогава интересуващото ни събитие се изразява в това, че за нито едно от копията на SYN + ACK пакет няма да бъде получен съответен ACK пакет и отношението (3.14) приема вида:

$$\lambda_2 = \lambda \cdot P_{по}^{N_{SA}} = \lambda \cdot (2P_{зп} - P_{зп}^2)^{N_{SA}} \quad (3.15)$$

Средният брой на заявките, намиращи се в СМО за обслужване, се определя от формулата:

$$l = \frac{\lambda_2}{\mu_2} = \frac{\lambda \cdot P_{зп}^{N_{SA}}}{\mu_2} = \frac{\lambda (2P_{зп} - P_{зп}^2)^{N_{SA}}}{\mu_2} \quad (3.16)$$

където: μ_2 е зададено време на сървъра за установяване на TCP съединение.



Фигура 3.4. Закон за разпределение на Поасонова СВ при $\lambda > 10$

За да се определи дали има или няма TCP SYN атака, разглеждаме стойността на функцията на разпределение, която се определя с формулата:

$$F(n) = \sum_{i=1}^{n} p(i) \qquad (3.17)$$

При използване на модела, за признак за TCP SYN атака се приема превишаването на стойността на функцията за разпределение от текущия брой полуотворени съединения l на някаква прагова стойност $F_{пр}$, която ще съответства на вероятността за вярно откриване на TCP SYN атака.

Изводи

1. Решение относно начало на атаката се приема тогава, когато реалният брой на полуотворени на сървъра съединения излиза от рамките на допустимия интервал.

2. Една част от параметрите могат да се определят посредством протоколния стек TCP/IP на защитавания сървър, а другата част- след статистическа обработка на реални получени стойности.

3. Описаният математически модел: позволява откриването на атаката, устойчив е към рязкото нарастване на интензивността на входящия поток от заявки за сървъра, отчита характеристиките на мрежата и на защитавания сървър.

2.4. Глава четвърта- Ruslan- система за защита от DDoS атаки

В глава четвърта се представят детайлно отделните модули на разработената от автора система за защита от DDoS атаки Ruslan. Предлага се решение за целите на дисертационния труд.

Конфигурация на HTTP сървъра, използвана за изследването е:

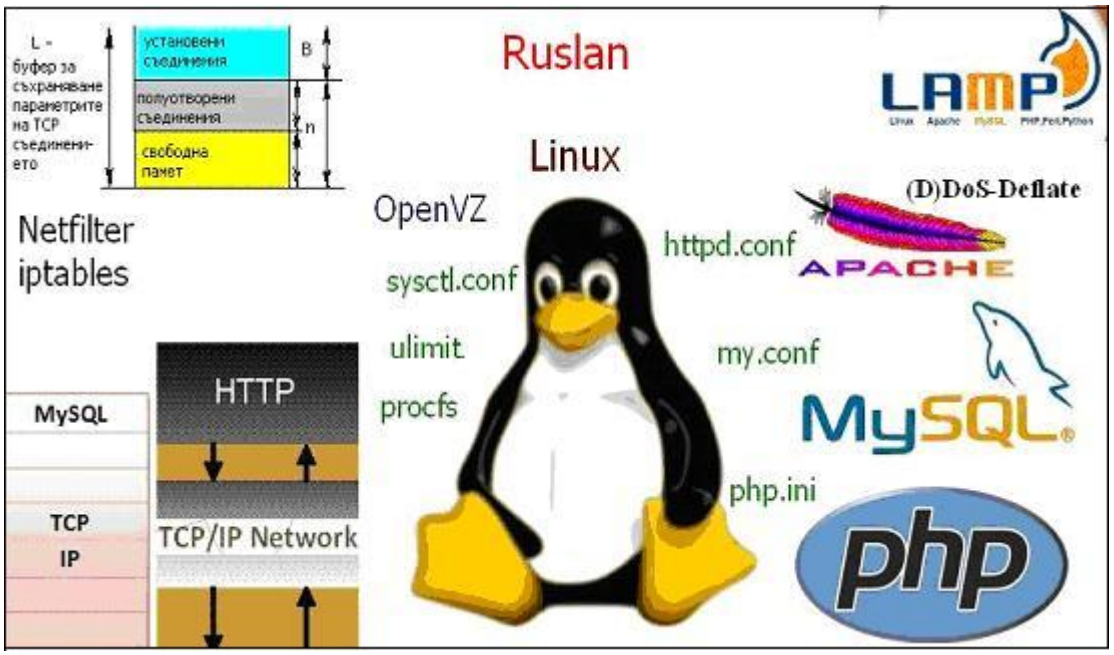
Процесор: Intel Core i3-2120 CPU, 3.30 GHz, 3M Cache

Скорост на процесора: 3.30 GHz

RAM памет: 8 GB

Мрежова карта: 3Com Typhoon (3CR990-TX-97) at MMIO 0xecf80000, 00:01:03:e6:65:e9

ОС: CentOS Linux release 6.0 ; Linux version 2.6.32-71.29.1.el6.i686 gcc version 4.4.4 20100726.



Фигура 4.1. Система за защита от DDoS атаки Ruslan

Параметри на ядрото на ОС

Преглеждат се въведените стойности на променливите та TCP/IP стека и на Netfilter с командата:

cat /etc/sysctl.conf

Увеличаваме максималните размери на буферите на TCP на 16MB:

net.core.rmem_max = 16777216

net.core.wmem_max = 16777216

Увеличиваме размера на опашката на полуотворените съединения:

net.ipv4.tcp_max_syn_backlog=4096

Параметърът tcp_synack_retries управлява броя на препредаванията в ОС Linux. По премълчаване е 5, което означава изтриване на полуотворено съединение след 3 минути. Настройваме предаването да се реализира на

третата секунда и пълното време за съхраняване на полуотворените съединения в опашката да е 9 секунди:

net.ipv4.tcp_synack_retries=1

Разрешаване поддръжка на голям прозорец на TCP протокол (според RFC1323- високопроизводителен TCP протокол):

net.ipv4.tcp_window_scaling = 1

Променяме алгоритъма за обработка на ситуацията претоварване:

net.ipv4.tcp_congestion_control=htcp

Използване на ulimit за контрол на ресурсите на сървъра

ulimit -n 512	макс. брой отворени файлове
ulimit -v 100000	макс. размер на използваната виртуална памет 100 MB
ulimit -c 0	забрана за създаване на файлове за ядрото

Защита от DDoS в конфигурацията на Apache

TimeOut – следва да се зададе възможно най-малка стойност за тази директива (на HTTP сървъра, който е подложен на DDoS атака).

KeepAliveTimeout директвата – също следва да се намали стойността и (или) напълно да се изключи.

Стойностите на различни времеви директиви могат да бъдат представени по следния начин: LimitRequestBody, LimitRequestFields, LimitRequestFieldSize, LimitRequestLine, LimitXMLRequestBody- следва коректно да са настроени за ограничаване на потреблението на ресурси, свързани със заявки на клиентите.

В този случай е задължително да се използва директивата AcceptFilter.

Установяване на модул за уеб сървър Apache- mod_dosevasive.

Извършена е промяна на параметрите по следния начин:

apache (httpd.conf)

При конфигурирането се добавят следните правила:

<IfModule mod_evasive20.c>

DOSHashTableSize 3097

DOSPageCount 6

DOSSiteCount 100

DOSPageInterval 2

DOSSiteInterval 2

DOSBlockingPeriod 600

</IfModule>

Timeout 20

MaxKeepAliveRequests 15

KeepAliveTimeout 2

MinSpareServers 3

MaxSpareServers 64

StartServers 1024

MaxClients 2500

MaxRequestsPerChild 100000

MaxConnPerIP 25

Конфигуриране на iptables

ANTI - SYN FLOOD:

iptables -A INPUT -p tcp --dport 80 --syn -m limit --limit 1/s -j ACCEPT

Блокиране на стадий SYN (не повече от 10 SYN):

iptables -A INPUT -p tcp --syn --dport 80 -m iplimit --iplimit-above 10\

-j DROP

проверка "New not syn:"

iptables -A bad_tcp_packets -p tcp --dport 80 !--syn -m state --state NEW \

-j LOG --log-prefix "New not syn:"

iptables -A bad_tcp_packets -p tcp --dport 80 !--syn -m state --state NEW \

-j DROP

ANTI - PING OF DEAD:
iptables -A INPUT -p icmp --icmp-type echo-request -m limit--limit 1/s \
-j ACCEPT
При условие, че 400 заявки вече са минали, следващите се отхвърлят, ако са повече от 300 в секунда:

iptables –A INPUT -p tcp --dport 80 -m state \

--state NEW -m limit -limit 300/second -limit-burst 400 -j DROP

Максимум 10 едновременни съединения към порт 80 от едно IP:

iptables -A INPUT -p tcp --dport 80 -m iplimit --iplimit-above 10 -j DROP

Лимит - 12 съединения в секунда за интерфейса eth0, като максимално допустимият брой е 24:

iptables --new-chain car

iptables --insert OUTPUT 1 -p tcp --destination-port 80 -o eth0 --jump car

iptables --append car -m limit --limit 12/sec --limit-burst 24 --jump RETURN

iptables --append car --jump DROP

20 съединения с мрежа от клас C:

iptables -I INPUT -p tcp --dport 80 -m iplimit --iplimit-above 20 --iplimit-mask\
24 -j DROP

Изтриване на подправени пакети, маркирани като Bad Guy.

Изтриване на известни вируси и скенери на портове.

Авторът е направил редица експерименти за оценка на отказите от обслужване със (и без) използването на защитната система Ruslan, следствие от наводняване на уеб сървър с TCP SYN пакети.

Авторът свързва в една локална мрежа с помощта на 16 портов суич уеб сървър и 15 машини, които се ползват както за атакуващи, така и за клиенти в експеримента.

Конфигурация на хостовете (клиенти и атакуващи) взаимодействащи с HTTP сървъра

Процесор: Intel® Celeron® 2.00 GHz

Скорост на процесора: 2.00 GHz

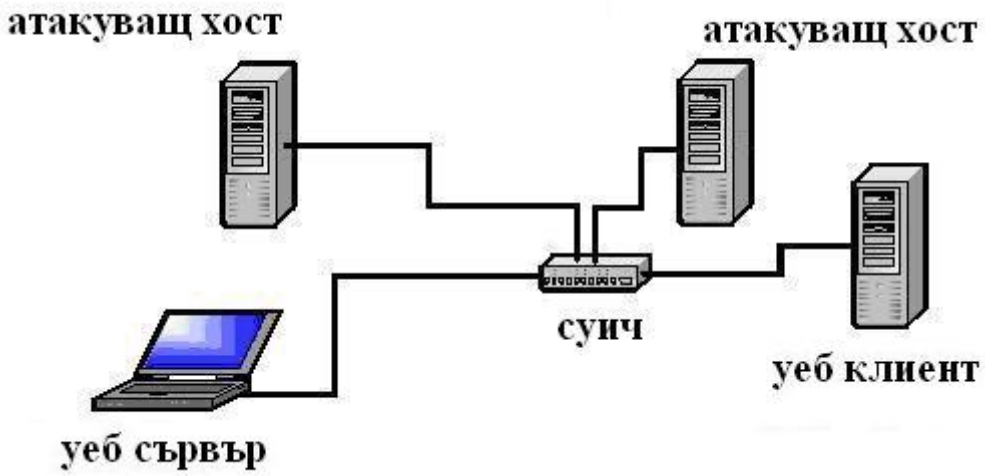
RAM памет: 512 MB

Мрежова карта: 100Mb/s Ethernet

ОС: CentOS Linux release 6.0; Linux version 2.6.32-71.29.1.el6.i686

gcc version 4.4.4 20100726.

. . . . . .



Фигура 4.4. Топология на експерименталната мрежа

Компютрите, определени като атакуващи хостове, генерират TCP SYN пакети, с което се симулира SYN наводняване. За целта се използва програма, която без защитата на системата Ruslan изпраща към уеб сървъра от един единствен хост, като уеб сървърът регистрира, че получава 47 хиляди пакета в секунда, успявайки да отговори само с 11 хиляди пакета в секунда. Това доказва, че системата има ресурс да отговори на по-малко от една четвърт от получените заявки. Когато атакуват два хаста, пак се изчерпват ресурсите - приема 32 хиляди и връща 7 хиляди. Това показва, че е налице изчерпване на ресурсите на системата, имаме работещо TCP SYN наводняване (DDoS атака).

При използването на защитната система Ruslan се прави анализ на влиянието на параметъра “размер на опашката на полуотворените съединения”:

net.ipv4.tcp_max_syn_backlog (B), който по подразбиране приема стойност 1024B.

Таблица 4.1. Влияние на параметъра размер на опашката на полуотворените съединения

net.ipv4. tcp_max_syn_backlog, B	1024	2048	4096	8192
вход. трафик, packets/ sec изход. трафик, packets/ sec	16000 4400	20000 5000	25000 5500	25000 5500

При наводняване с пакети и с увеличаване на този буфер системата успява да поеме за обработка по-голям трафик, т.е. тя разполага с по-голям ресурс за справяне с атаката и реално успява да обслужва по-голям трафик. След като имаме еднотипни данни при стойности на параметъра 4096 и 8192, стига се до извода, че не се налага повече да се увеличава буфера. Затова впоследствие е избрана стойността:
net.ipv4.tcp_max_syn_backlog=4096.

Ще направим анализ на влиянието на параметъра net.ipv4.tcp_synack_retries при използване на защита с Ruslan.

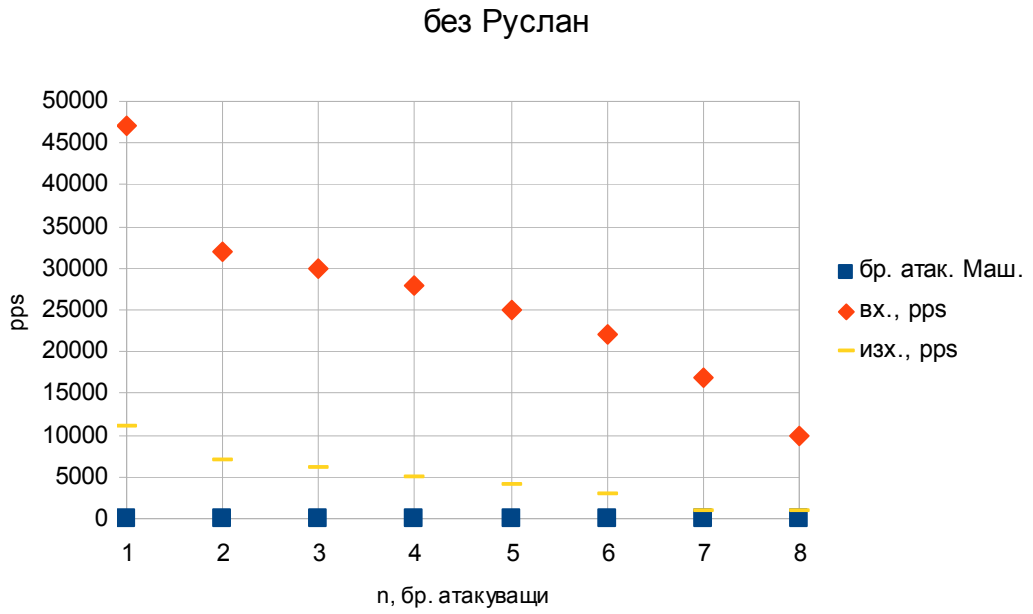
Параметърът tcp_synack_retries управлява броя на повторните предавания, като задава времето за съхраняване на полуотворените съединения в буфера. По подразбиране е 5 броя, което означава изтриване на полуотворено съединение след 3 минути.

Таблица 4.3. Влияние на параметъра, управляващ броя на препредаванията

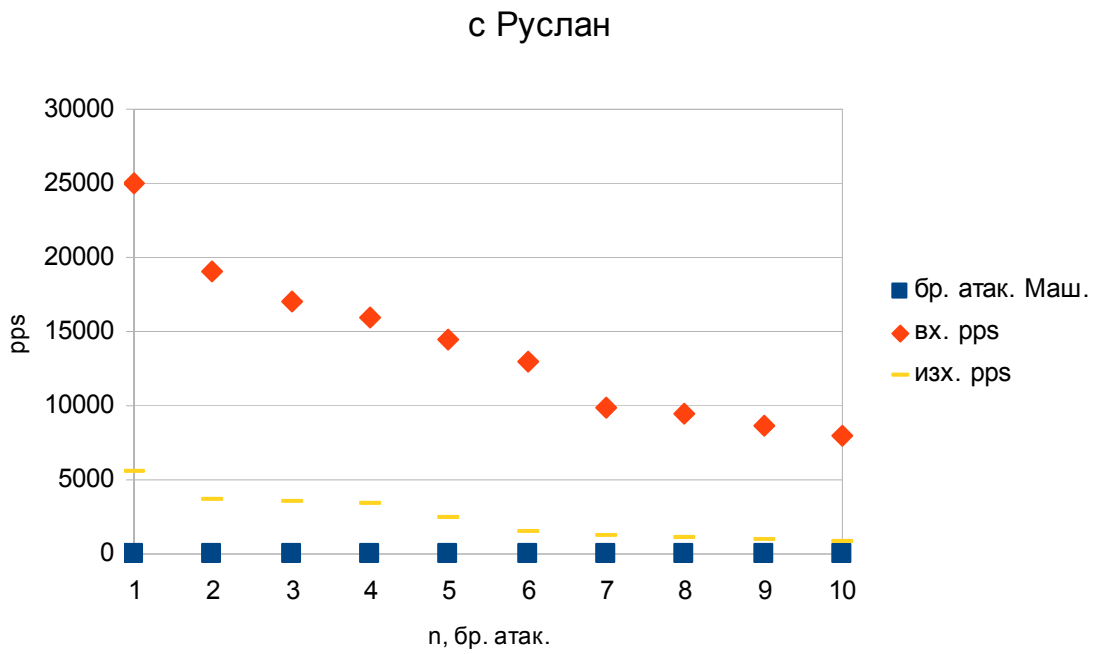
net.ipv4.tcp_synack_retries, s	5	4	3	2	1
вход. трафик, packets/ sec изход. трафик, packets/ sec	21000 4500	22000 4650	23000 4800	24000 5000	25000 5500

Извършва се настройка предаването да се реализира на третата секунда и пълното време за съхраняване на полуотворените съединения в опашката да е 9 секунди. При наводняване с пакети и намаляването на броя на препредаванията, което води до намаляване на времето за съхранение на полуотворените съединения в опашката, се стига до извода, че системата успява да поеме за обработка по-голям трафик. Затова впоследствие е избрана стойността net.ipv4.tcp_synack_retries=1.

Експериментално се получава, че без защита сървърът става неработоспособен при атакуване от 7 хоста, а с използване на Ruslan продължава да е работоспособен дори при атака от всички 15 машини.



Фигура 4.5. Генериран входящ и изходящ трафик на уеб сървъра без система за защита Ruslan



Фигура 4.6. Генериран входящ и изходящ трафик на уеб сървъра със система за защита Ruslan

Изводи

1. Базови елементи на системата за защита Ruslan са параметрите на ядрото на ОС, TCP/IP стека, скрипт за iptables.

2. Силно изразена е зависимостта на параметрите, настройвани за защита, от характеристиките на уеб сървъра (процесор, памет, ОС, пропускателна способност на комуникационния канал).

3. Използването на Ruslan успява да запази работоспособността на уеб сървъра при максимално възможното спрямо пропускателната способност на комуникационните линии и устройства наводняване на атакуваната с фалшиви заявки система. Без помощта на Ruslan уеб сървърът спира да обслужва клиентите при много по-ниски нива на входящия поток от заявки.

3. Приноси

Научно-приложни приноси на дисертацията:

1. Извършена е класификация и анализ на известните видове DDoS атаки и методи за борба с тях.

2. Дефинирани са базовите променливи за конфигуриране на защитните механизми за LAMP сървър за противодействие на DDoS атаките, като са определени средствата за противодействие на DDoS атаките и нивата на защита за уеб сървър. Изследвани са методите за изграждане на противодействаща система срещу DDoS атаките.

3. Създаден е модел на системата, описващ взаимодействието на сървъра с клиентите, отчитащ характеристиките на компютърната мрежа и на защитавания сървър. С помощта на математическия апарат на теорията на системите за масово обслужване са определени допустимите интервали за броя на полуотворени TCP съединения на сървъра. Описаният математически модел позволява откриването на атаката и е устойчив към рязкото нарастване на интензивността на входящия поток от заявки за сървъра, при което се отчитат характеристиките на мрежата и на защитавания сървър.

4. Разработена е система за защита Ruslan, целяща преодоляване на DDoS атаките. Системата променя параметри на ядрото на ОС, основни конфигурационни файлове, съдържа допълнителни модули.

5. Експериментално е доказана стабилната работа на системата Ruslan при реално проведени DDoS атаки, потвърдена е способността й за запазване на работоспособността на уеб сървъра.

4. Публикации свързани с дисертационния труд

1. Nina Siniagina, Stela Ruseva, Defence mechanisms against computer attacks “Distributed denial of service” type, International conference Policy and Models for R&D Management in Support of Defence Industrial Transformation, Sofia, June 28-29, 2007, pp. 155- 166.

2. Stela Ruseva, Distributed attacks denial of service type. Nature of these attacks and Defense against them, ComputerScience'08 conference, Kavala, Greece, September 17-20, 2008, pp. 225- 231.

3. Стела Русева, Информационна сигурност и системи за защита от атаки, Международна научна конференция „Мениджмънт и качество” 2009- Юндола, 16-18 октомври, стр. 76- 84.

4. Нина Синягина, Стела Русева, Изследване на методите за защита на електронна поща, Computer & Communications Engineering №2, 2010, София, стр. 21- 27.

5. Стела Русева, Защита на компютърни мрежи от DDoS атаки, 120 г. СУ „Св. Климент Охридски”- Годишник на СУ „Св. Климент Охридски”, стр. 121- 127.

6. Стела Русева, Защита на WEB сървър, Международна научна конференция „Мениджмънт и качество” 2010 - Юндола, 8-10 октомври, стр. 69- 75.

Creating of system for protection against DDoS attacks

Summary

There has been made a review of different types of DDoS attacks and description of the way they function, as well as the method for their detection and blocking. The condition of the problem is presented and a classification for these kinds of attacks is suggested. The most prospective research in the field of protection for computer networks connected with defense against DDoS attacks has been shown.

There has also been presented an extended analysis of the approach towards creating of a system for protection. LAMP architecture for the server has been chosen. Methods and ways for building of a protective system against DDoS attacks have been described.

In the dissertation there has been made a model of the system which describes the interaction between the server and the clients and which accounts for the characteristics of the computer network and the server under protection. A model, counting for loss of packets in the network due to a TCP SYN attack, has been shown.

A system for protection Ruslan has been developed, aiming at overcoming the DDoS attacks. It changes parameters of the OS core and basic configuration files. The system contains additional modules. It has a stable performance under real conditions - DDoS attacks. Its ability to keep the performance of the web server has been proved.