Напад со преплавување со UDP пакети

Елена Ристеска[1], Митко Богдановски[2]

[1] Европски Универзитет – Скопје, Р. Македонија, risteska.elena@live.eurm.edu.mk

[2] Воена академија – Скопје, Р. Македонија, mitko.bogdanoski@eurm.edu.mk

***Апстракт*—Преголемиот замав на користењето на Интернет доведе до големи промени на начинот на живеење, промена на навиките и начинот на функционирање на институциите. Покрај предностите и благодетите кои ни ги нуди Интернетот, неговото проширување во сите сфери претставува и опасност. Имено, недоволната сигурност на мрежите и несигурноста на податоците и информациите кои се наоѓаат на Интернет, доведуваат до последици.**

Denial-of-service (DoS) нападите влијаат на мрежата на тој начин што ја оневозможуваат достапноста на одредени ресурси на Интернет. Во овој труд наш интерес се нападите со преплавување со UDP пакети. Во овој труд ќе бидат разгледани карактеристиките на овој вид напад, ќе рагледаме неколку начини за реализирање на напад, откривање и заштита од ваков напад.

***Клучни зборови*— DoS, напад, UDP преплавување**

I. Вовед

Појавата на Интернетот направи голема револуција во светот и најде своја примена во сите области од животот, почнувајќи од образованието, здравството, финансиите, банкарството, бизнисот итн. Преголемиот замав на користењето на Интернет доведе до големи промени на начинот на живеење, промена на навиките и начинот на функционирање на институциите. Покрај предностите и благодетите кои ни ги нуди Интернетот, неговото проширување во сите сфери претставува и опасност. Имено, недоволната сигурност на мрежите и несигурноста на податоците и информациите кои се наоѓаат на Интернет доведуваат до сериозни последици. Користењето на Интернетот се зголемува со експоненцијална брзина. Како и организациите, владите, така и граѓаните ја зголемуваат довербата во оваа технологија. За жал, со зголемувањето на бројот на хостови, бројот на напади на Интернет се зголемува неверојатно брзо [1].

Блокирањето на достапноста на некоја Интернет услуга може да предизвика големи финансиски загуби, како во случај на напад кој овозможува корисниците да имаат слаба конекција до важни веб сајтови за трговија како Yahoo, Amazon, eBay, E*Trade, Buy.com, ZDNet и CNN. Овие напади, чија цел е да го блокираат компјутерскиот систем или услугите се наречени DoS напади [2]. Нападите од овој вид се многу штетни, па дури и катастрофални, а тоа е и причината на голем број истражувачи и инженери за долгогодишните обиди и напори за спречување на овие напади, како и намалување на последиците од нив.

Трудот е организиран на следниот начин: во втората глава ќе зборуваме за општата поделба на нападите и ќе биде дадени опис на секој од нив, во третата глава ќе ги објасниме нападите на преплавување, во следната глава ќе илустрираме некои од алатките кои се користат за вакви напади, во петтата глава ќе разгледаме неколку можни решенија за заштита од напади со преплавување со UDP пакети, во шестата глава ќе разгледаме резултати од неколку изведени експерименти за детекција на UDP напади со преплавување и на крај во последната секција ќе кажеме краток заклучок на досегашните достигнување при решавање на овој проблем.

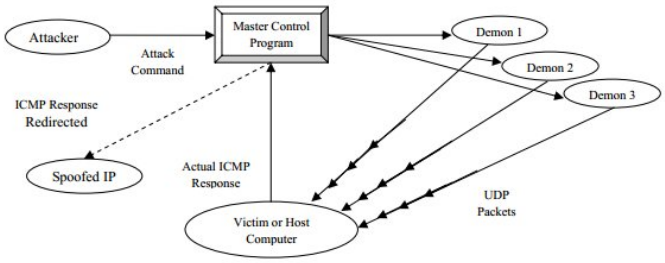
II. Видови напади

Denial-of-service (DoS) нападите влијаат на мрежата на тој начин што ја оневозможуваат достапноста на одредени ресурси на Интернет. Во зависност од начинот на дејствување постојат повеќе поделби на овие напади.

- DoS напад имаме кога еден напаѓач прави одредена услуга да биде недостапна за корисниците. Начините за извршување на вакви напади се многубројни но, најчесто се основаат на пропусти или недостатоци во дизајнот. Вообичаено, напаѓачите немаат доволно пропусен опсег и ресурси за да извршат ефективен напад со преплавување или flood attack.
- Distributed Denial-of-Service (DDoS) напад имаме кога повеќе системи ги преплавуваат ресурсите на одреден систем. При реализирањето на овој тип на напад на мрежа на компјутери, кои се поврзани на Интернет, пред нападот се инсталира malware софтвер.
- Distributed Reflection Denial of Service (DRDoS) нападот вклучува испраќање на лажни барања до голем број на компјутери кои ќе одговорат на барањето. Изворната адреса на пакетите со барања е поставена на жртвата. Овој напад резултира со илјадници одговори на системот на жртвата кои предизвикуваат прекин или трошење на ресурси [3].

A. Опис на нападите

DDoS нападите ги прават ресурсите недостапни за корисниците. Тоа значи дека напаѓачот сака да им оневозможи на корисниците пристап до сајтови или услуги на Интернет. Овој напад се случува кога повеќе системи (напаѓачи) - го преплавуваат пропусниот опсег на целниот систем со податочни пакети. DDoS нападите предизвикаа внимание во Февруари 2000, кога некои сајтови како yahoo.com, CNN.com беа паднати од ваков напад. Исто така, не можеме да не го споменеме нападот на преплавување на сајтови во Естонија во 2007-та година со кој беа нападнати сајтовите на парламентот, банките, разни министерства итн. После тоа, во јули 2009 со овој напад беа нападнати повеќе сајтови во Јужна Кореа, USA, Twitter, Facebook, Live journal, Google. Во јануари 2012 година се случи најголемиот DDoS напад во историјата од група наречена „Анонимуси“. Овој напад во кој учествуваа 5,635 хостови беше насочен кон сајтови на владата на САД, а основна причина беше исклучувањето на сајтот на Megaupload.

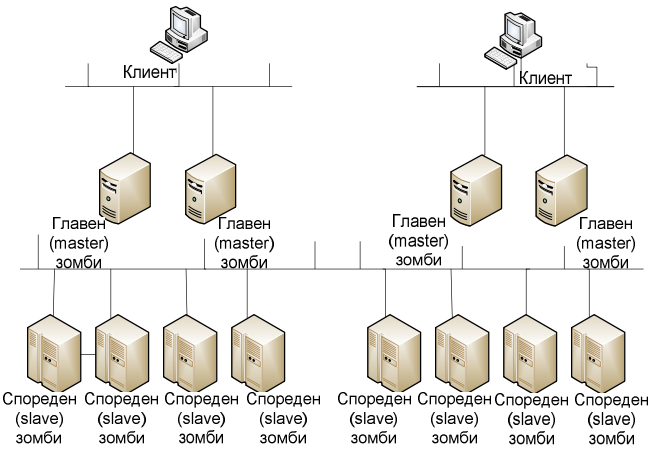


Слика 1. Механизми за UDP Floof напад [4]

Компоненти кои се вклучени во DDoS нападот се: Жртва или Хост Компјутер, Вистински напаѓач, Master Control Program и Демони – клиенти (Слика 1). Жртва е компјутерот кој е избран за напаѓање, напаѓач е мајсторскиот ум кој работи со метод и стратегија за напад. Работи под заштита од Master Control Program, која го прави тежок за да се трага по него. Master Control Program работи како интерфејс - помеѓу реалниот напаѓач и напаѓачките демони и исто така се однесува како штит за напаѓачот, примајќи наредби од реалниот напаѓач и давајќи инструкции на демоните под негова контрола за напаѓање на жртвата. Демоните се користат за директен напад на хост системот. Демоните најчесто имаат задача да ја нападнат жртвата и истовремено да ја преплават. Очигледно е дека учеството на различни работни компоненти го прави тешко заштитувањето на жртвата или хост компјутерот од овие напади [4].

Во DDoS напад со преплавување посебни системи наречени - „зомби“ го преплавуваат системот со IP сообраќај (Слика 2). Големиот број на пакети кои се испратени од „зомбите“ до системот на жртвата го успоруваат, системот прекинува да работи или го презаситуваат пропусниот опсег на мрежата.

Flood нападите може да се направат со UDP, со ICMP или TCP пакети.



Слика 2. Напад со Дистрибуирано Одбивање на Услуга (DDoS) [5]

III. Видови напади со преплавување

A. Напад со преплавување со UDP пакети (UDP flood attack)

User Datagram Protocol (UDP) е поврзувачки протокол кој функционира така што пакетите се праќаат преку UDP, при што не постои директна комуникација помеѓу двата уреди, испраќачот и примачот. Кај овој протокол не постојат механизми за контрола на протокот помеѓу испраќачот и примачот и адаптирање кон промените на мрежата.

UDP Flood нападот користи користи UDP пакети со што се постигнува загрозување на пропусниот опсег на мрежата. Преголемиот број на испратени UDP пакети до системот кој претставува жртва на ваков напад, можат да ја презаситат мрежата и да го исцрпат пропусниот опсег кој што е достапен за услуги. За да се одреди бараната апликација, системот на жртвата ги обработува пристигнатите податоци. Во случај на отсуство на бараната апликација на бараната порта, системот-жртва испраќа порака до испраќачот со информација дека дестинациијата не е достапна. Со цел да се прикрие идентитетот на напаѓачот, напаѓачот најчесто имитира IP адреса на изворот на пакетите за напад.

Еден лажен UDP пакет може да учествува во напад на проток кој никогаш не завршува. На пример, доколку напаѓачот испрати пакет до жртва претставувајќи се како да е од друга жртва. Првата жртва испраќа пакет до втората, на што следи ист пдгпвпр и од втората жртва. Двете жртви на ваков напад испраќаат ехо барања кои нема да завршат сè додека не се стопираат од некој надворешен ентитет.

За да се овозможи опција за заштита од UDP flood, потребно е да се постави праг, кој се повикува во случај на надминување на овој праг. Вредноста на овој праг вообичаено е 1000 пакети во секунда.

B. Напад со преплавување со TCP-SYN пакети (TCP-SYN flood attack)

Во текот на нападот со преплавување со TCP-SYN пакети, напаѓачкиот систем испраќа TCP-SYN барање со маскирана IP адреса на изворот кон жртвата. Овие SYN

барања се појавуваат како легитимни. Маскираната адреса се однесува на клиент кој не постои. Оттука, конечната ACK порака никогаш нема да биде испратена на серверот кој е жртва. Ова резултира во зголемен број на полу-отворени конекции на страната на жртвата. Резервниот дел од редот на чекање се користи за чување на овие полу-отворени конекции. Овие полу-отворени конекции ги поврзуваат ресурсите на серверот. Оттука, не може да се направат нови (легитимни) конекции што резултира во DOS или DDoS. Серверот-жртва не е во можност да одговори на барањата за Domain Name System (DNS) услугата кои доаѓаат од легитимните корисници [6].

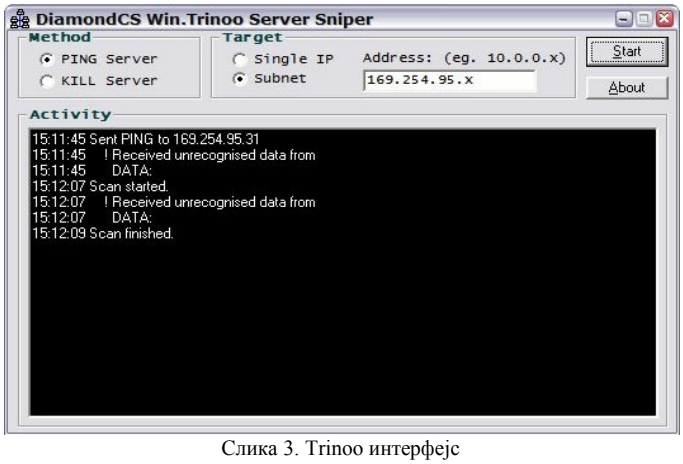
C. ICMP напад со преплавување (ICMP flood attack)

Internet Control Message Protocol (ICMP) пакетите се креирани за управување со карактеристиките на мрежата, лоцирање на мрежната опрема и одредување на изворот и дестинацијата. ICMP flood нападот се појавува кога се испратени голем број на ICMP_ECHO_REPLAY пакети на системот. Во овој случај системот треба да одговори и настанува заситување на сообраќајот [7].

IV. АЛАТКИ ЗА DOS/DDOS НАПАДИ

Постојат многубројни алатки за DDoS - напади. Повеќето од нив се разликуваат во механизмот на комуникација помеѓу управувачите (handlers) и агентите.

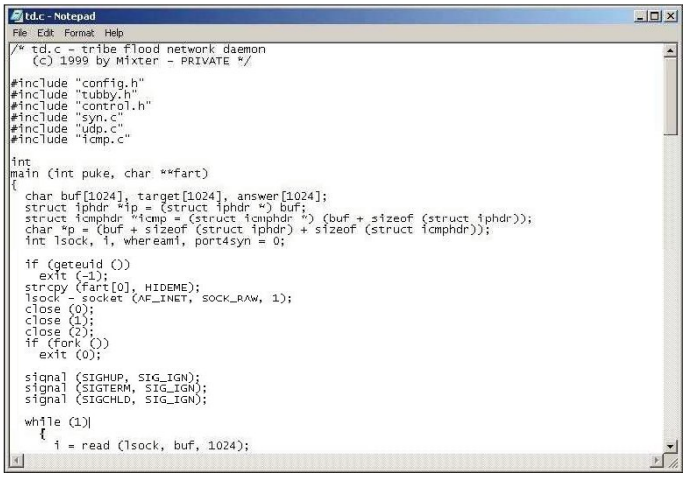
Една алатка која се користи за UDP flood е Trinoo (Слика 3). Оваа алатка е дистрибуирана за напади од различни извори. Мрежата се состои од мал број сервери и голем број клиенти. Напаѓачот ја користи мрежата trinoo поврзувајќи се на еден сервер и давајќи му инструкции да започне напад на некоја IP адреса. Серверот ја дава инструкцијата на клиентите (демоните), кои треба да извршат напад на соодветните IP адреси.



Слика 3. Trinoo интерфејс

Trinoo генерира UDP пакети со одредена големина на порти по случаен избор на една или повеќе целни адреси за време на определен интервал за напад [8].

Друга алатка за UDP Flood напади е Trible Flood Network (TFN), која е многу слична на претходната (Слика 4).



Слика 4. TFN интерфејс

Оваа алатка обезбедува мрежа која извршува различни напади, како ICMP, или TCP SYN flood, кои можат да се извршат од повеќе извори кон една или повеќе цели. Комуникацијата помеѓу серверот и клиентот се одвива преку ICMP echo пакети на одговор [9].

Stacheldraht е алатка која претставува комбинација на карактеристиките на претходните две алатки, trinoo и TFN (Слика 5). Алатката користи енкриптирана комуникација помеѓу напаѓачот и управувачите (handlers), и овозможува автоматско ажурирање на агентите, што значи дека при приклучување на агентот или при поврзување на Интернет ќе се инсталираат датотеки кои напаѓачот ги поставил на некој сервер [10].

```
trying to connect...
connection established.
---------------------------------------
enter the passphrase :
---------------------------------------
entering interactive session.
******************************
   welcome to stacheldraht
******************************

stacheldraht(status: a!0 d!0)>.help
available commands in this version are:
-----------------------------------------------------
.mtimer    .mudp   .micmp   .msyn  .mack  .mnul  .msort
.mstream   .mhavoc .mrandom .mip   .mfdns
.showalive .madd   .mlist   .msadd .msrem .help
.setusize .setisize .mdie  .sprange .mstop  .killall
.showdead .forceit  .left
-----------------------------------------------------
stacheldraht(status: a!0 d!0)>.mudp 192.168.0.119
mass udp bombing
1 floodrequests were sent to 1 bcasts.
stacheldraht(status: a!0 d!0)>
```

Слика 5. Стартување на UDP Flood напад со Stacheldraht

Shaft е алатка која има слични карактеристики како Trinoo, Stacheldraht и TFN. Со оваа алатка можат да се извршат следните напади: UDP, TCP-SYN и ICMP flooding. Shaft спречува откривањето од страна на Instrusion Detection System поради тоа што има способност за вклучување на портите и IP адресата на управувачот (handler) во реално време, за време на нападот [11,12].

Сите овие алатки може да се најдат на Интернет. Иако

алатките за ваков напад се разликуваат една од друга по начинот на кој функционираат сепак, нивната единствена намена е да го преплават системот на жртвата со зголемување на сообраќајот.

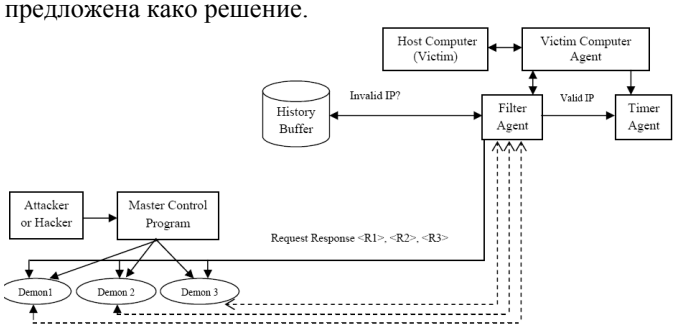
V. ЗАШТИТА ОД UDP НАПАДИ НА ПРЕПЛАВУВАЊЕ (UDP FLOOD ATTACK)

Направени се големи напори за решавање на нападите кои спаѓаат во категоријата на DDoS напади, меѓутоа, сè уште не е најдено единствено решение кое целосно ќе се справи со овие напади.

Во делот кој следи ќе бидат објаснети одредени истражувања поврзани со одредување на ефектите на UDP нападите со преплавување, како и истражувања поврзани со развој на одредени механизми за детектирање и отстранување на ефектите на овие напаи.

Авторите на [13] извршиле експеримент за проценка перформансите на Ботнет мрежа. Во експериментот е направена симулација на Ботнет мрежа во NS2. Во експериментот е направен UDP flood напад, при што системот врз кој е вршен експериментот се состои од 17 јазли: 6 бот јазли, 3 јазли кои се жртви на нападот, 1 јазол за сервер, 6 нормални јазли и 1 јазол кој работи како botmaster. Добиен е следниот резултат: пред да се изврши UDP flood напад, брзината на пренос е 2 MB, после извршениот напад перформансите на мрежата се намалалуваат 1.5, 1.3, 1.2, 1.4 MB.

Во [4] е предложено едно можно решение за заштита од UDP flood напади. Имено, се работи за една рамка која се состои од повеќе комппоненти. Предложената рамка има задача да ги открие UDP flood нападите и со тоа да го заштити компјутерот кој е потенцијална жртва на напад. Решението кое е понудено во [4] се состои од следните компоненти: Victim Computer Agent (VCA), Filter Agent (FA) кој содржи и бафер во кој се чуваат невалидните IP адреси и Timer Agent (TA). При секоја комуникација се проверува дали IP адресата се наоѓа во баферот. Доколку не се наоѓа таму, тогаш барањето може понатаму да се процесира. Адресата се проверува три пати и доколку нема никаков одговор тогаш се става во баферот на невалидни адреси. На Слика 6 е прикажана рамката која е предложена како решение.



Слика 6. Поглед на предложената рамка за заштита од UDP напади [4]

Авторите на [14] во својот труд ги изложуваат предностите и недостатоците на алатките кои се користат за управување со безбедноста, анализирање на сообраќајот, откривање на аномали и сл. Во Табела 1 (Додаток) се илустрирани карактеристиките на секоја од алатките, кои проблеми ги идентификуваат и предлог на можни решенија за нив, доверливост на алатките и нивните ограничувања и слабости. Во табелата ќе прикажеме мал извадок од [13], кој се однесува на анализа на алатките за DDoS напади.

Авторите на [15] во својот труд презентираат класификатор на UDP flood напад. Како крутериум за разликување на DDoS сообраќајот од нормалниот сообраќај ја користат претпоставката за пропорционална стапка на пакети за нормален UDP сообраќај. Експериментот е тестиран на големи корпорации како универзитети, финансиски институци итн. Резултатите покажуваат индиција за користење на алгоритмот за класификација за откривање на напади.

Сличен експеримент за откривање на UDP flood напади направиле авторите на [16], кои висината на стапката на влезниот сообраќај ја поставуваат на многу повисоко ниво од стапката на излезниот сообраќај, како и пропорцијата на искористливост на протоколот која од страна напаѓачот е многу повисока во однос на другите протоколи во сообраќајот. Авторите на [16] предлагаат систем за детекција на UDP напад, кој се заснова на анализа на брзината на сообраќај базирајќи се на разменетиот протокол. Дефинирана е стапка на сообраќај на следниот начин:

$$Traffic(T) = Traffic(IN) / Traffic(out) \quad (1)$$

- каде *Traffic(IN)* е број на влезни пакети во секунда и *Traffic (OUT)* е број на излезни пакети во секунда. Пропорцијата на искористливост на протоколот ја пресметуваат на следниот начин:

$$IN_p(UDP) > \left(IN_p(ICMP) + IN(TCP)\right)$$
$$(OUT_p(ICMP) > OUT_p(TCP)) \quad (2)$$
$$OUT_p(ICMP_{type}) == 3$$

каде - IN_p е пропорција на влезен сообраќај, OUT_p е пропорција на излезен сообраќај. Бројот 3 во формулата за излезен сообраќај е поради пораките кои го информираат клиентот за недостапност на дестинацијата - ICMP Destionation Unreachable (код 3).

DDoS нападите можат да се откријат со анализа на некои карактеристики на IP ниво, како филтрирање на IP, IP следење, IP логирање, обележување на пакети, информации во IP заглавието, статистики за патот, вредности на TTL, набљудување на протокот и сл. На транспортното ниво, за разликување на напад од нормален сообраќај, може да се врши анализа на различни пакети (ICMP, UDP, TCP-SYN). Можно е обезбедување на заштита и на апликациско ниво, како на пример анализа на HTTP сесија. Сепак, сè уште не постојат решенија за комплетна заштита од ваквиот вид на напади. Некои од решенијата кои ни се понудени би можеле да имаат ефект

само доколку доследно се следат инструкциите за нивно имплементирање и доколку се искористи комбинација на повеќе предложени механизми за заштита од овие напади.

VI. Заклучок

Овој труд е даден преглед на различните видови DDoS напади со преплавување, а посебно се концентрира на UDP нападите со преплавување. Опишани се неколку од многуте алатки кои можат да се искористат за извршување на овој тип на напад. На крај е даден опис на дел од предложените мерки за заштита од ефектите на овој напад.

DDoS нападите можат да се откријат со анализа на некои карактеристики на IP ниво, како филтрирање на IP, IP следење, IP логирање, обележување на пакети, информации во IP заглавието, статистики за патот, вредности на TTL, набљудување на протокот и сл. На транспортното ниво, за разликување на напад од нормален сообраќај, може да се врши анализа на различни пакети (ICMP, UDP, TCP-SYN). Можно е обезбедување на заштита и на апликациско ниво, како на пример анализа на HTTP сесија. Сепак, сè уште не постојат решенија за комплетна заштита од ваквиот вид на напади. Некои од решенијата кои ни се понудени би можеле да имаат ефект само доколку доследно се следат инструкциите за нивно имплементирање и доколку се искористи комбинација на повеќе предложени механизми за заштита од овие напади.

Истражувачите даваат многу големи напори за да изнајдат решение за заштита од мрежните напади. Сепак, сè уште не е најдено единствено решение кое целосно ќе се справи со овие напади. Инженерите, исто така, вложуваат многу но, од друга страна, ги имаат напаѓачите кои ги бараат најдобрите техники за напад, и имаат пристап кон алатките со кои на многу едноставен начин може да извршат еден ваков напад.

Прилог

Табела 1: Резиме на различни алатки за анализа на сообраќајот и зголемување на безбедноста

Библиографија

[1] B. B. Gupta, R. C. Joshi и Manoj Misra*: Distributed Denial of Service Prevention Techniques*, International Journal of Computer and Electrical Engineering, Vol. 2, No. 2, April, 2010 1793-8163.

[2] M. Albuz: Internet Denial of Service Attacks and Defense Mechanisms, Department of Computer Science, University of Pittsburgh.

[3] P. Suwala and N. Wieczorek: *Defense against DoS, flooding attacks*, Linköpings universitetet, Sweden.

[4] A. Singhi and D. Junea*: Agent Based Preventive Measure for UDP Flood Attack in DDoS Attacks*, Institute of Computer Technology & Business Management M.M.University, Mullana ,Haryana, India.

[5] Е. Конеска, Ј. С. Костадиновска, М. Богданоски, С. Гелев, ,DoS Напади кај безжичните мрежи и методи за намалување на нивните ефекти", CITYR, јуни 11-13, 2010, Охрид, Р. Македонија

[6] H. Wang, D. Zhang, and K. G. Shin, "Detecting SYN flooding attacks", in Proceedings of Annual Joint Conference of the IEEE Computer and Communications Societies(INFOCOM), volume 3, pages 1530-1539, June 23-27 2002

[7] M. Bogdanoski and A. Risteski, "Wireless Network Behavior under ICMP Ping FloodDoS Attack and Mitigation Techniques", International Journal of Communication Networks and Information Security (IJCNIS), Vol. 3, No. 1, April 2011

[8] Staff.washington.edu/dittrich/misc/trinoo.analysis.txt

[9] Staff.washington.edu/dittrich/misc/tfn.analysis.txt

[10] Staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt

[11] Staff.washington.edu/dittrich/misc/shaft.analysis.txt

[12] S. Dietrich, N. Long and D. Dittrich: *Analyzing Distributed Denial Of Service Tools: The Shaft Case*, New Orleans, Louisiana, USA, December 3– 8, 2000.

[13] S. Singh and M. Gyanchandani: *Analysis of Botnet Behavior Using Queuing Theory*, International Journal of Computer Science & Communication,Vol. 1, No. 2, July-December 2010, pp. 239-241.

[14] F. Ullah and W. Tariq: *Operating System Based Analysis of Security Tools for Detecting Suspicious Events in Network Traffic*, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 2, November 2011, ISSN (Online): 1694-0814

[15] A. G. Bardas, L. Zomlot and S. C. Sundaramurthy: *Classification of UDP Traffic for DDoS Detection.*

[16] Z. Ihsan, M. Y. Idris, K. Hussain, D. Stiawan and K. M. Awan: *Protocol Share Based Traffic Rate Analysis (PSBTRA) for UDP Bandwidth Attack*, Faculty of Computer Science and Information System, Universiti Teknologi Malaysia, Skudai, 81310, Johor. Malaysia.

ПРИЛОГ

ТАБЕЛА 1
РЕЗИМЕ НА РАЗЛИЧНИ АЛАТКИ ЗА АНАЛИЗА НА СООБРАЌАЈОТ И ЗГОЛЕМУВАЊЕ НА БЕЗБЕДНОСТА[1]

Автор	Име на алатка	Резиме	Идентификуван проблем	Решенија	Користени податоци	Имплемен-тиран	Ограничувања
G.H.kim& E . H. Spafford 1995	Tripwire	алатка за проверка на интегритет на датотеки и откривање напади	Leakage attack & denial of service attack	да се насетат овластените модификации	да	да	Напаѓачот може да одреди која порта се користела како tripwire
K.Lakkaraju, W.Yurick& A.J. Lee 2003	NVisionIP	Алатка за графичка репрезентација на класа B IP мрежа	системски напади, напад на злоупотреба на основната порта и DoS напад	намалување на аномалии и ненадејно известување	да	да	зависност од Instrusion detection систем и log фајловите може да бидат модифицирани
J.Mcpherson, Kliu. Ma, P.Krystosk, T.Bartoletti& M.Christensen 2004	PortVis	Алатка за сумирање на информации на активноста на секоја TCP порта	Напад на основна порта или црви, DDoS и TTL напад	Слика од сообраќајот и важни карактеристики (број на порта, време, протокол итн.)	да	да	Комплексна конфигурација и тежок за користење
N. Patwari, Alfred O&A.Pacholski 2005	Manifold learning based	Алатка за визуелизација на аномаличен сообраќај во Abilene (internet 2 backbone)	DDoS напади slammer напад на црви	развој на сензори за статистики и димензии	да	да	зависност од платформа и многу комплексни одржувања
Daniel A. Keim, F.Mansmann, J.Schneidewind& T.Schreck 2006	Radial traffic analyzer	Скалабилна алатка за визуелизација на анализите на нивото на пакети	Идни или неидентификувани напади, out ring напад, DoS напад, црви и вируси	Архитектура базирана на TCP/IP моделот	да	да	----------

[1] Operating System Based Analysis of Security Tools for Detecting Suspicious Events in Network Traffic, **Fasee Ullah and Waqas Tariq,** IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 2, November 2011, страна 3-4

UDP FLOODING ATTACK

Summary

Elena Risteska[1], Mitko Bogdanoski[2]

[1] Europian University – Skopje, R. Macedonia, risteska.elena@live.eurm.edu.mk

[2] Military academy – Skopje, R. Macedonia, mitko.bogdanoski@eurm.edu.mk

***Abstract* – Excessive use of the Internet has led to major changes in lifestyle, change habits and way of functioning of institutions. Despite the advantages and benefits that Internet offer, its expansion in all spheres is also a danger. The lack of security of networks and uncertainty of data and information found on the Internet, leading to serious consequences.**

Denial-of-service (DoS) attacks affecting the network, thus limiting the availability of certain resources on the Internet. The interest of our paper are UDP flooding attacks. We will consider the characteristics of this type of attack, and examine several mechaniusms for detection and protection against this attack.

***Клучни зборови* – Denial-of-service (DoS), attack, UDP flooding**