DDoS халдлагад шинжилгээ хийх

Н.Угтахбаяр[1], Б.Дөлгөөн, Ш.Содбилэг[2]
Монгол Улсын Их Сургууль, Мэдээллийн Технологийн сургууль
Холбооны Технологийн Тэнхим
ugtakhbayar@num.edu.mn[1], sdblg@num.edu.mn[2]

***Хураангуй* - Энэхүү судалгааны ажлын хүрээнд сүлжээ болон системийн үйл ажиллагааг доголдуулах зорилготой DDOS халдлагын шинж чанарыг туршилтын систем дээр судлах, системд үзүүлэх нөлөөллийг тодорхойлохыг зорьсон.**

Түлхүүр үгс – DDoS; халдлага; Weka;

I. Удиртгал

Дэлхий дахинд цахим хэрэглээ асар хурдацтай нэмэгдэж буйтай холбогдуулан түүнийг ашигласан халдлагуудын тоо, төрөл асар их нэмэгдэж байгаа. Үүний нэг жишээ болох DDoS халдлагыг илрүүлэх ажлууд маш ихээр хийгдэж байгаа бөгөөд энэ нь техник, технологийн хөгжлийг дагаад асар хурдацтай өөрчлөгдөж байгаа мөн интернэт хэрэглэгчдийн тоо олон болсон тул энэхүү халдлагад bot болох хэрэглэгчдийн тоо мөн өссөн. Өнөөдрийн байдлаар DDOS халдлагыг төгс илрүүлэх, түүнээс бүрэн хамгаалах систем байхгүй байна. Халдлага эсэргүүцэх систем, Firewall, Access control list зэрэг аюулгүй байдлын системийг ашиглан энэхүү төрлийн халдлагаас сэргийлэх аргууд байдаг боловч эдгээр нь bot-ийн тоо урсгалын хэмжээ зэрэгээс хамааран DDoS-ийн халдлагыг бүрэн зогсоож чадахгүй байна. Тухайн халдлага нь ямар төрлийн системд халдаж байгаагаас шалтгаалан өөр өөр хэлбэрт байдаг. Энэ нь тухайн өртөгчийн ашиглаж буй систем, bot-ийн сүлжээг удирдах механизм зэрэг олон зүйлээс шалтгаалдаг. Мөн сүлжээний нэвтрүүлэх чадамжинд нөлөөлөх нөлөөллийг багасгах үүднээс тухайн халдлагыг илрүүлэхэд цөөн тооны параметрүүдийг ашигладаг учир энгийн урсгалыг халдлага гэж танин зогсоох, эсвэл халдлага нэгэнт болсон хойно таних зэрэг дутагдалтай талууд байсаар байна. Arbor судалгааны төвөөс гаргасан судалгаагаар [7] 2011 онтой 2012 оны DDoS халдлагыг харьцуулвал халдлагын хэмжээ 20 хувиар өссөн, пакетын хурд 11 хувиар өссөн нийт халдлагын амжилттай болсон тоо 41 хувиар өссөн гэсэн тоон үзүүлэлт байна. Иймд энэхүү төрлийн халдлагыг тодорхойлоход пакетийн тоо, хугацаа, порт, протокол, логик хаяг, оролт гаралтын пакет, пакетийн хэмжээ, bps, pps, TOS зэрэг боломжит параметруудыг ашиглан хамгийн тохиромжит байдлаар тэрхүү утгуудыг сонгохыг зорьсон. Уг ажлын давуу тал нь DDoS халдлага хийдэг ижил шинж чанартай хэд хэдэн түүл ашиглан халдлага хэрхэн хийгдэж байгааг судлаж байгаагаараа бусад судалгааны ажлуудаас ялгагдана. DDOS-ийн халдлага хийдэг маш олон түүлүүд байдаг бөгөөд эдгээрээс Hulk, LOIC, HOIC, Pyloris, Slowloris зэрэг нь дэлхий дээр хамгийн өргөн хэрэглэгддэг түүлүүд юм. [9,10]

II. Судлагдсан байдал

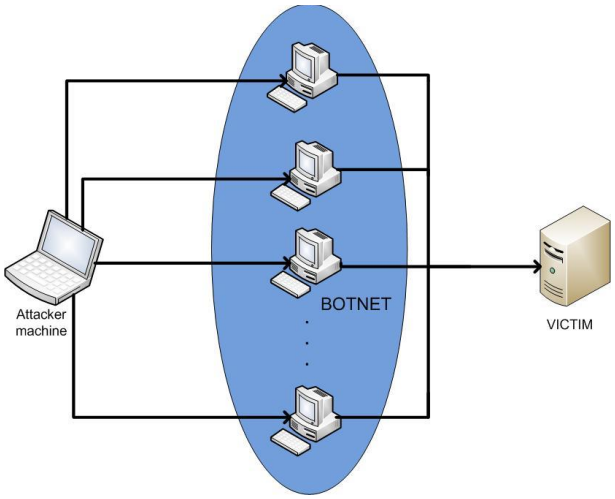
Энэ төрлийн судалгааны ажил нь аюулгүй байдлын шинжээчдийн хувьд сонирхолтой сэдвүүдийн нэг нь яах аргагүй мөн юм. DDoS-ийн халдлагыг илрүүлэхэд IP хаягийн байршил, Inline IPS, Heuristic filtering гэх мэт аргуудыг хэрэглэж байна. Esraa Alomari нар Botnet-based Distributed Denial of Service (DDOS) Attacks on Web servers: Classification and Art ажлынхаа хүрээнд зөвхөн вэбд суурилсан халдлагыг тодорхойлоход HTTP протоколд flood төрлийн халдлагууд хэрхэн нөлөөлж буйг судласан бол Sowmyadevi.K нар Detect DDoS attack using border gateways and Edge Routers ажлынхаа хүрээнд гарцын төхөөрөмж DDoS халдлагад нөлөөлөх нөлөөллийг тодорхойлжээ. Мөн эдгээр ажлуудаас гадна TCP, UDP зэрэг протоколд суурилсан, spoofing төрлүүдийн халдлагуудтай хавсарсан зэрэг олон судалгааны ажлууд хийгдсэн байна.

III. Судалгааны арга зүй

Судалгааны ажлын хүрээнд botnet ашиглан DDOS-ийн халдлагыг хийх бөгөөд энэхүү халдлагын урсгалыг tcpdump, nfdump ашиглан барьж авч эрүүл өгөгдөлтэй харьцуулан weka програм хангамжийг ашиглан анализ хийнэ.

Энэхүү ажлаа виртуал орчинд туршиж үзсэн бөгөөд халдагчийн систем нь Backtrack 5 R3, bot-уудын сүлжээ нийт 20 хэрэглэгч Windows XP SP2 /1Ghz dual core CPU, 256mb RAM, 5 GB hard, 100mbps LAN card/, өртөгч нь CentOS 6.2 /1GB ram, 40 GB hard, Core 2 (2.4Ghz) CPU/ ашигласан.

Туршилт явуулах үед сүлжээний урсгалыг netflow, tcpdump, nfdump, nfcapd ашиглан авсан. Netflow ашиглан гаргаж авсан үр дүн болон nfcapd ашиглан гаргаж авсан үр дүнгүүдийг хооронд нь харьцуулсан. МУИС-ийн сүлжээний гарцанд байрлах төхөөрөмж болох watchguard-ийн шүүлтүүр хийсэн урсгалыг ашиглан энгийн урсгалыг цуглуулсан. Дараа нь туршилтын системүүдэд botnet-ийн серверийг суулгаж backtrack систем ашиглан IRC-ээр удирдан CentOS 6.2 системд халдаж DDoS халдлага бүхий урсгалыг цуглуулсан. Хоёрдугаар алхам буюу системд DDOS халдлага хийсэн топологийг зураг 2-т харууллаа.



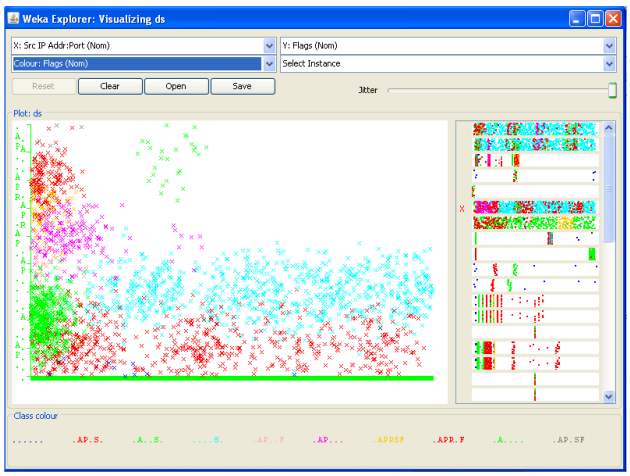
Зураг 1 CentOS системд DDoS халдлага явуулсан топологи

Уг урсгалыг барьж авахдаа CentOS систем дээр tcpdump, netflow, nfdump, nfcapd зэрэг түүлүүдийг ашигласан.

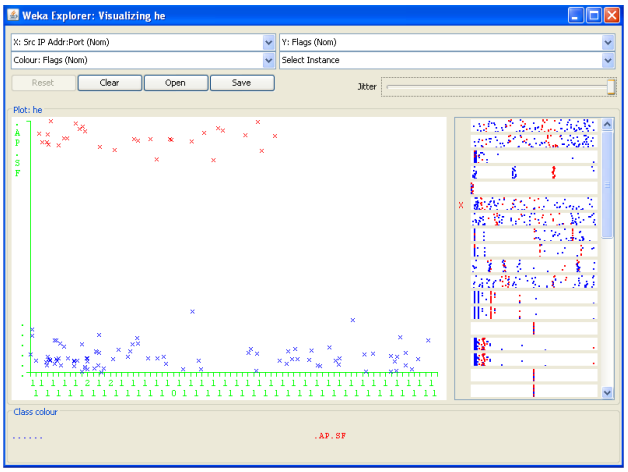
DDOS-ийн халдлага хийхэд Hulk, HOIC, LOIC түүлүүдийг ашигласан.

IV. Туршилт, Үр дүн

Туршилтын үр дүнд Hulk, HOIC, LOIC ашиглан DDOS-ийн халдлага хийх нь хоорондоо адилхан үр дүнг гаргаж байсан. Зураг 2-т DDoS-ийн халдлага хийх үеийн болон Зураг 3-т энгийн урсгалын үеийн хоорондох Flag-уудын хоорондын хамаарлыг харууллаа. Энэхүү харьцуулалтад хэвийн TCP пакет нь дамжуулалтанд ACK, PSH, FIN, SYN гэсэн дөрвөн төрлийн flag-ийг ашигладаг бол DDoS-ийн халдлагын үед flag-уудыг маш хурдан сольж буй зураглалыг харж болно. TCP Flag хурдан солигдоно гэдэг нь тухайн урсгалыг three-way handshake процессоор тодорхойлоход хүнд болж байгаа юм.

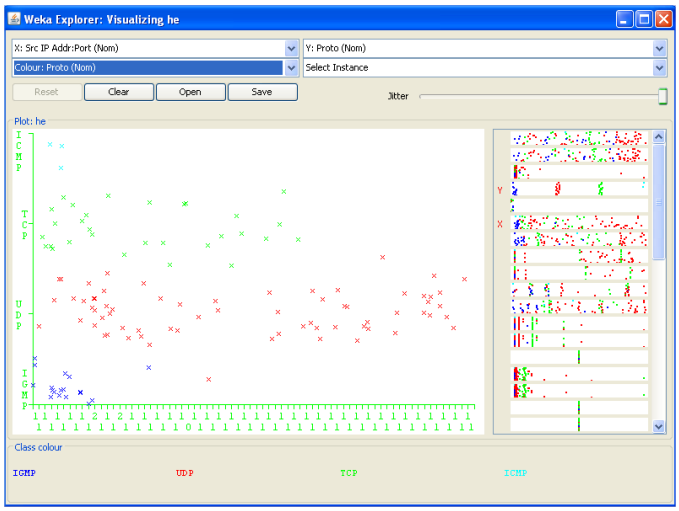


Зураг 2 DDoS-ийн халдлага хийх үеийн flag set

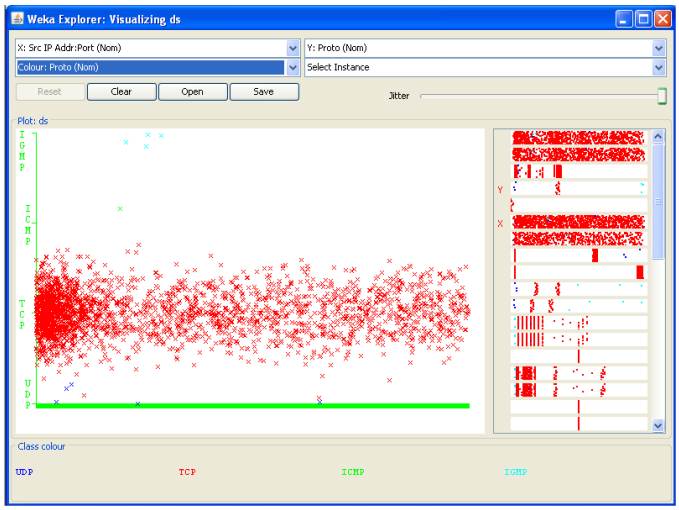


Зураг 3 Энгийн TCP урсгалын flag set

Зураг 4-д энгийн урсгалын хувьд протоколуудын пакетын хэмжээ, Зураг 5-д DDoS ашигласан үед пакетын хэмжээ хэрхэн өөрчлөгдөж буйг харууллаа. Үүний үр дүнд энгийн урсгалаас илүү DDoS халдлагын үед TCP-ийн урсгал огцом өсөж буй нь харагдаж байна. Энэ нь тухайн төхөөрөмж болон серверийн нэвтрүүлэх чадамжаас хамааран тухайн халдлагад өртөх хугацаа өөр өөр байдгыг батлан харуулж байна.



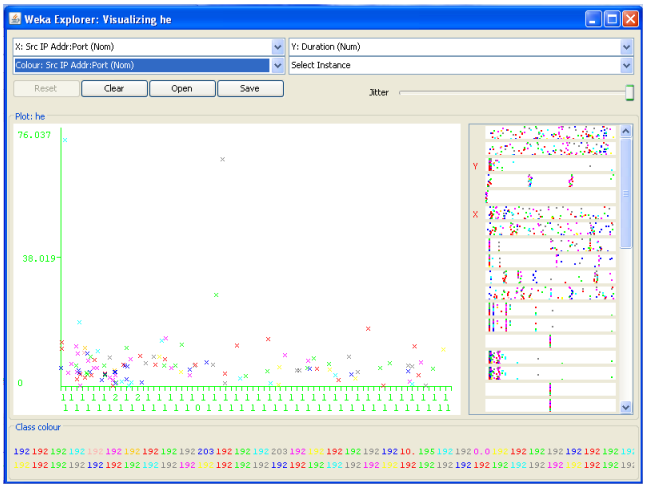
Зураг 4 Энгийн урсгалын үед протоколын хамаарал



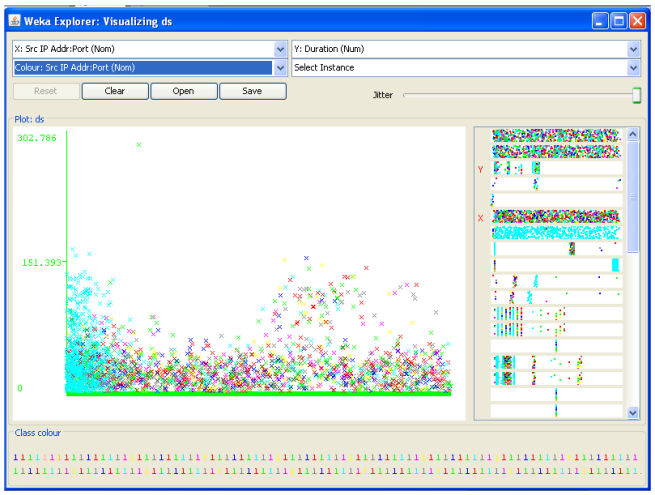
Зураг 5 DDoS халдлагын үед протоколын хамаарал

Зураг 6-д энгийн урсгалын хувьд пакетын үргэлжлэх хугацаа, Зураг 7-д DDoS ашигласан үед пакетын

үргэлжлэх хугацаа хэрхэн өөрчлөгдөж буйг харьцуулан харууллаа. Дараах зургаас харвал пакетын үргэлжлэх хугацаа нь 30 секунд орчим байхад DDoS халдлага болоход уг хугацаа 80 секунд болж өөрчлөгдөж байна. Энэ нь DDoS халдлагыг тухайн пакетийн session-ий үргэлжлэх хугацаанаас хамааруулан илрүүлэх боломжтой гэдгийг харуулж байна.

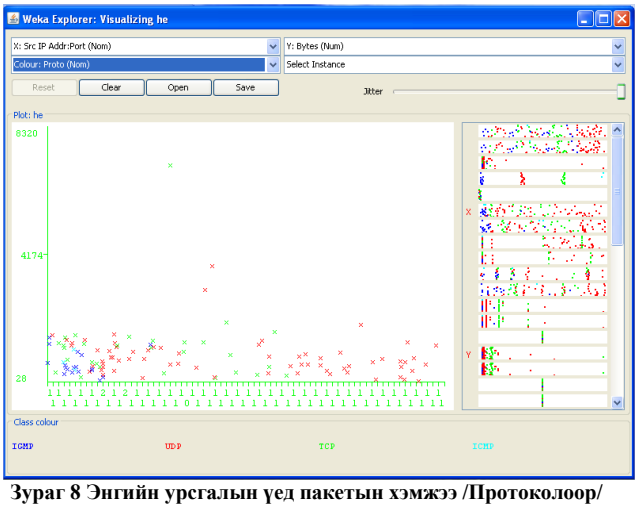


Зураг 6 Энгийн урсгалын үед пакетын үргэлжлэх хугацаа

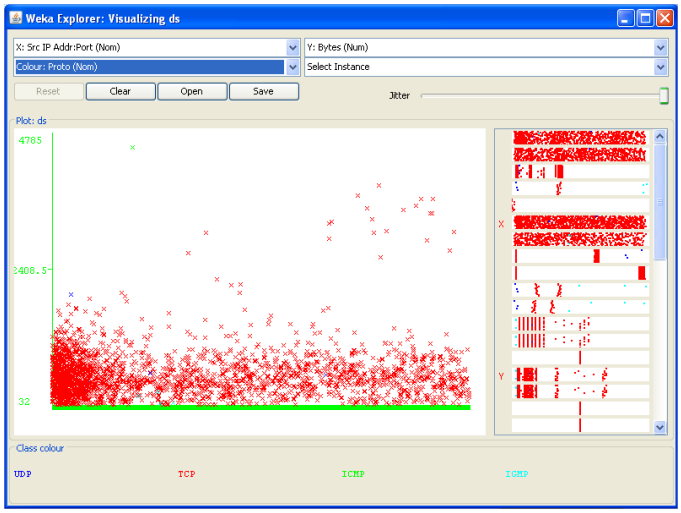


Зураг 7 DDoS халдлагын үед пакетын үргэлжлэх хугацаа

Зураг 8-д энгийн урсгалын нэг пакетын хэмжээ, Зураг 9-д DDoS ашигласан үед нэг пакетын хэмжээг харууллаа. Дараах зургаас харвал пакетын хэмжээ нь энгийн урсгалын үеийнхээс хэд дахин их байдаг нь харагдаж байна.



Зураг 8 Энгийн урсгалын үед пакетын хэмжээ /Протоколоор/



Зураг 9 DDoS халдлагын үед пакетийн хэмжээ /Протоколоор/

V. ДҮГНЭЛТ

Энэхүү судалгааны ажлын хүрээнд botnet based DDoS халдлагыг хийж эрүүл болон тухайн халдлагад өртсөн сүлжээний урсгалыг илрүүлэн тухайн хоёр урсгалыг параметрүүдээр нь харьцуулан судаллаа. Уг ажлын үр дүнд LOIC, HOIC, Hulk зэрэг түүлүүдийг ашиглан халдлага хийх үед тухайн сүлжээнд ирэх урсгалын шинж чанарт тодийлон их хэмжээний өөрчлөлт байхгүй байгааг тогтоолоо. Мөн пакетийн үргэлжлэх хугацаа, болон хэмжээ нь DDoS халдлагад чухал параметр болохыг харлаа. Уг ажлын үр дүн дээрээ тулгуурлан snort, nfsight зэрэг системүүд дээр дүрэм бичиж DDoS халдлагыг илрүүлэх улмаар тухайн халдлагыг зогсоох ажлуудыг туршиж байна.

НОМ ЗҮЙ

[1] K.Park and H.Lee, “On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denail of Service Attack,” Proc. IEEE INFOCOM, 2001.

[2] T.Peng, C.Leckie, and K.Ramamohana rao, “Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems,” ACM Computing Surveys, vol. 39, no.1, p.3, 2007.

[3] M.; Mercy Shalinie, S.; Arun Pragash, A. “IP traceback system for network and application layer attacks,” Recent Trends In Information Technology (ICRTIT), 2012 International Conference.

[4] Abraham Yaar, Adrian Perrig and Dawn Song, “StackPi: New Packet Marking and Filtering Mechanisms for DDOS and IP Spoofing Defence,” IEEE Journal On Selected Areas In Communications, vol.24, no.10, Oct. pp.1853-1863. 2006

[5] Fu-Yuan Lee, Shiuhpyng Shieh, “Defending against spoofed DDOS attacks with path fingerprint,” Computers & Security, 24, pp.571-586. 2005

[6] Feng Qiaojuan, Wei Xinhong, “A new Research on DoS/DDoS Security Detection Model,” IEEE 2nd International Conference on Computer Engineering and Technology, vol.3. 2010

[7] Arbor networks center, “DDoS attacks in 2012” report.

[8] S.M. Specht and R.B.Lee, “Distributed denial of service: Taxonomies of attacks, tools, and countermeasures,” International Workshop on Security in Parallel and Distributed Systems, 2004

[9] Jelena Mirkovic, and others "Internet denial of service: Attack and Defense Mechanisms" ISBN: 9780132704540

[10] McGraw-Hill. "Hacking exposed 6" 2009