DDOS HUJUMLARINI ANIQLLASH ALGORITIMLARI VA DASTURIY TA'MINOTINI ISHLAB CHIQISH

Raxmonov Furqatbek Davlatjon o'g'li
Toshkent Milliy Universiteti "Axborot xavfsizligi" yo'nalishi 1-bosqich magistranti

Annotatsiya: *DDos (Distributed Denial of Service) hujumlari DoS va DDoS hujumlarini amalga oshirish texnologiyalari juda xilma-xildir, manbadagi oddiy ommaviy axborotdan tortib, ma'lum zaif yoki uzoq muddatli sayt skriptlariga hujum qiluvchi "aqlli" DoSa texnikasigacha. Kiberjinoyatchilar ko'pincha server dasturiy ta'minotidagi zaifliklardan foydalanadilar.*

Kalit so’zlar: *DDOS, DoS, provayder, algoritim, dastur, botnet, sayt, server, MAC, ICMP, ICMP, SYN.*

KIRISH

Server dasturiy ta'minotining eski versiyalari bir nechta zaifliklarga, jumladan DoS va DDoS hujumlariga nisbatan zaiflikka moyil. Ushbu zaifliklardan foydalanadigan ekspluatatsiyalar DoS va DDoS hujumlarini tashkil qilish uchun ishlatiladi. Aqlli DDoSa texnikasi, shuningdek, hosting provayderlari tomonidan belgilangan chegaralardan oshib, xizmat hujumini rad etishdir. Deyarli barcha xosting provayderlarida bir martalik qo'ng'iroqlar soni kabi hujjatsiz xizmat cheklovlari mavjud. fayl tizimi serverlar, protsessorga yukni cheklash va boshqalar. Ushbu ma'lumotlar bilan tajovuzkor sayt yoki serverga hujumni boshqaradi, uning maqsadi ushbu chegaralardan oshib ketishdir. DDoS hujumi (Distributed Denial of Service) DoS hujumining bir turi. Bunday hujumni juda ko'p sonli kompyuterlar uyushtirmoqda. Shu sababli, hatto Internet-kanallarining katta o'tkazish qobiliyatiga ega bo'lgan bunday serverlar ham hujumga moyil.

NATIJALAR VA MUHOKAMA

Ammo DDoS hujumi har doim ham kimningdir yomon niyati tufayli sodir bo'lmaydi. Ba'zida bu ta'sir tasodifan sodir bo'lishi mumkin. Bu, masalan, juda mashhur veb-resursdagi havola (havola) serverda joylashgan saytga joylashtirilgan bo'lsa sodir bo'lishi mumkin. Bu hodisa splashdot effekti deb ataladi.

Siz bilishingiz kerakki, DDoS hujumi deyarli har doim tijorat maqsadlarida amalga oshiriladi, chunki uni tashkil qilish juda ko'p vaqt va moddiy xarajatlarni talab qiladi, buni tan olishingiz kerak, hamma ham qila olmaydi. Ko'pincha, DDoS hujumini tashkil qilishda botnet deb ataladigan maxsus kompyuter tarmog'idan foydalaniladi.

Botnet nima? Botnet - bu maxsus turdagi viruslar bilan zararlangan kompyuterlar tarmog'idir. Barcha zararlangan kompyuterlar masofadan turib kiberjinoyatchilarga tegishli, ko'pincha bu kompyuterlarning egalari DDoS hujumida qatnashayotganliklarini bilishmaydi ham. Kompyuterlar ma'lum bir virus yoki o'zini foydali deb ko'rsatuvchi dastur bilan zararlanadi. Keyin, ushbu dastur yordamida kompyuterga zararli kod o'rnatiladi, u

"ko'rinmas" deb ataladigan rejimda ishlaydi, shuning uchun antiviruslar buni sezmaydilar. Muayyan nuqtada botnet egasi ushbu dasturlarni faollashtiradi va kiberjinoyatchilar tomonidan hujumga uchragan serverga so'rovlar yuborishni boshlaydi.

DDoS hujumini amalga oshirishda kiberjinoyatchilar ko'pincha "DDoS klasteri" deb ataladigan narsadan foydalanadilar. DDoS klasteri shaxsiy kompyuter tarmog'ining shunday maxsus uch bosqichli arxitekturasidir. Bunday tuzilmada odatda DDoS hujumining boshlanishini bildiruvchi bir yoki bir nechta boshqariladigan konsollar mavjud.

Keyin bu signal asosiy kompyuterlarga uzatiladi (host kompyuterlar konsollar va agent kompyuterlar o'rtasidagi vositachilarga o'xshaydi). Agent kompyuterlar serverga hujum qiladigan kompyuterlardir. Ko'pincha asosiy kompyuterlar va agent kompyuterlarning egalari hujumda ishtirok etayotganliklarini ham bilishmaydi.

DDoS himoyasi boshqacha bo'lishi mumkin. Buning sababi, bu hujumlarning turlarining o'zlari farq qiladi. To'rtta asosiy tur mavjud: UDP toshqini, TCP toshqinlari, TCP SYN toshqinlari va ICMP toshqinlari. Agar tajovuzkorlar ushbu usullarning barchasini yoki bir nechtasini birlashtirsa, DDoS hujumi yanada xavfli bo'ladi.

Ushbu turdagi hujumdan himoya qilishning universal usuli hali ixtiro qilinmagan. Ammo bir nechta oddiy qoidalarga rioya qilsangiz, unda hujum xavfi deyarli nolga kamayishi mumkin. Dasturiy ta'minotning zaif tomonlarini yo'q qilish kerak, shuningdek, resurslarni ko'paytirish, shuningdek ularni tarqatish kerak. Kompyuterda ushbu turdagi hujumlardan himoya qilish uchun dasturlar to'plami bo'lishi kerak (hech bo'lmaganda minimal).

Havaskor kiberjurnalistlar orasida uchraydigan keng tarqalgan xatolardan biri bu Internet-resurslarga hujumlar turlari bo'yicha chalkashlikdir. Masalan, DoS va DDoS bir xil narsa emas. Qisqartmalar faqat bitta harf bilan farq qilsa-da, uning orqasida katta faktik farq bor.

Bugungi kunda DoS hujumi haqida yozish juda kam uchraydi (Xizmatni rad etish) beri bu hujumlar samaradorligi pastligi sababli amalda qo'llanilmaydi. Biroq, zamonaviy xizmat kiberhujumlarini rad etishning markazida aynan DoS sxemasi yotadi.

DoS hujumi - bu bitta qurilmadan (IP-manzil) "qurbon" resursiga (masalan, veb-sayt) "axlat" trafigini yaratish. Maqsad, ikkinchisining ishiga to'sqinlik qilish uchun "jabrlanuvchi" ning hisoblash va boshqa vakolatlarini tugatishdir.

Chunki Internet, kompyuter texnikasi va tarmoq uskunalari jadal rivojlanmoqda, kuchga ega bo'lib, bitta DoS hujumining hajmi har qanday muhim manbani blokirovka qilish uchun juda kichik bo'lib qoldi. Shu sababli, xakerlar DoS hujumini kuchaytirishning eng aniq usulini topdilar: uni bir vaqtning o'zida bir nechta qurilmalardan (IP-manzillar) o'tkazish. Xizmatni rad etish bo'yicha taqsimlangan (yoki ommaviy) kiberhujum - DDoS (Taqsimlangan xizmat ko'rsatishni rad etish)... Uni filtrlash ancha qiyin va quvvat 1 ts ga yetishi mumkin.

Bundan tashqari, DoS hujumi boshlanganda uni qaytarish oson: zararli trafik paketlari kelayotgan IP-ni hisoblang va unga kiring. Va hujum bir nechta IP-manzillardan kelganda,

vazifa yanada qiyinlashadi. Misol uchun, resursni himoya qilish uchun siz qonuniy ravishda hujum qiluvchi IP manzillari "bog'langan" bir mamlakatdan kelgan barcha so'rovlarni bloklashingiz mumkin, ammo u erdan qonuniy foydalanuvchilarga saytga kirish taqiqlanadi.

Qaysidir ma'noda, agar biz DDoS ta'rifi haqida gapiradigan bo'lsak, bu DoS hujumining kichik turi bo'lib, u sxemani o'zgartirish orqali paydo bo'lgan, ammo bunday hujumlarning boshqa shakllari mavjud emas va birinchisi xakerlar arsenalidan ikkinchisini siqib chiqargan. . Shuning uchun, aksariyat hollarda DDoS hujumi yoki rus tiliga tarjimasi - xizmat ko'rsatishni rad etish hujumini qo'llash to'g'riroq bo'ladi.

Bunday hujumning sxemasi uchta asosiy elementdan iborat: boshqaruv mashinasi, undan boshqaruv signallari konsolga yuboriladi, bu orqali signallar millionlab foydalanuvchi qurilmalariga (buzilgan yoki zararli kod bilan zararlangan) tarqatiladi. Aynan shu qurilmalar botlar deb ataladi. Agar ilgari bular asosan shaxsiy kompyuterlar bo'lsa, bugungi kunda botnet hujumi marshrutizatorlar, videoregistratorlar, smartfonlar va boshqalar - Internetga ulanish uchun interfeysga ega bo'lgan har qanday qurilma yordamida amalga oshirilishi mumkin. Bot foydalanuvchisi ko'pincha undan noqonuniy harakatlar uchun foydalanilayotganini bilmaydi.

Bugungi kunda Internetda bepul kirishda siz 15-20 dollarlik bema'ni to'lov evaziga istalgan saytning DDoS testini tashkil qilish bo'yicha ko'plab takliflarni topishingiz mumkin. Bunday "xakerlar" odatda katta kiberhujumni tashkil qilish uchun kuchli server yoki botnetga (buzilgan qurilmalar tarmog'iga) ega emaslar va bunday pul uchun har qanday vakolatli tizim ma'muri boshqarishi mumkin bo'lgan maksimal DoS miqdori amalga oshiriladi.

Biroq, DoS ning ahamiyatini e'tiborsiz qoldirmaslik kerak - ularda yangi hujumchilar mashq qiladilar va bunday holatlar kamdan-kam hollarda tekshirilganligi sababli ko'pchilik jazosiz qoladi.

DoS va DDoS hujumlari serverning hisoblash resurslariga tajovuzkor tashqi ta'sirlar yoki ish stantsiyasi, ikkinchisini muvaffaqiyatsizlikka olib kelish maqsadida o'tkazilgan. Muvaffaqiyatsizlik deganda biz mashinaning jismoniy ishdan chiqishini emas, balki uning resurslarining vijdonli foydalanuvchilar uchun mavjud emasligini - tizimning ularga xizmat ko'rsatmasligini nazarda tutamiz (D g'alati o f S xizmat, bu DoS qisqartmasi).

Agar bunday hujum bilan amalga oshirilsa yagona kompyuter, u DoS (DoS) deb tasniflanadi, agar bir nechta bo'lsa - DDoS (DDoS yoki DDoS), ya'ni “D taqsimlangan D g'alati o f S xizmat "- xizmatni rad etish uchun taqsimlangan eskalatsiya. Keyinchalik, hujumchilar nima uchun bunday harakatlarni amalga oshirishlari, ular nima, ular hujum qilinganlarga qanday zarar etkazishi va ikkinchisi o'z resurslarini qanday himoya qilishi mumkinligi haqida gapiraylik.

Hujumlar korxonalar va veb-saytlarning korporativ serverlariga, kamroq - jismoniy shaxslarning shaxsiy kompyuterlariga qaratilgan. Bunday harakatlarning maqsadi, qoida tariqasida, bitta - hujumga uchraganlarga iqtisodiy zarar etkazish va soyada qolish. Ba'zi hollarda DoS va DDoS hujumlari serverni buzish bosqichlaridan biri bo'lib, axborotni

o'g'irlash yoki yo'q qilishga qaratilgan. Aslida, har qanday shaxsga tegishli biznes yoki veb-sayt kiberjinoyatchilar qurboniga aylanishi mumkin.

DoS va DDoS hujumlari ko'pincha insofsiz raqobatchilarning tashabbusi bilan amalga oshiriladi. Shunday qilib, shunga o'xshash mahsulotni taklif qiladigan onlayn-do'konning veb-saytini "to'ldirish" orqali siz vaqtincha "monopolist" bo'lishingiz va uning mijozlarini o'zingiz uchun olishingiz mumkin. Korporativ serverni “qo‘yish” orqali raqobatchi kompaniya ishini buzish va shu orqali uning bozordagi o‘rnini pasaytirish mumkin.

Katta zarar etkazishi mumkin bo'lgan keng ko'lamli hujumlar odatda professional kiberjinoyatchilar tomonidan katta pul evaziga amalga oshiriladi. Lekin har doim emas. Homebrew havaskor xakerlari ham sizning resurslaringizga hujum qilishlari mumkin - qiziqish tufayli va ishdan bo'shatilgan xodimlar orasidan qasos oluvchilar va shunchaki hayot haqidagi qarashlaringiz bilan o'rtoqlashmaydiganlar.

Ba'zan ta'sir qilish tovlamachilik maqsadida amalga oshiriladi, tajovuzkor esa hujumni to'xtatish uchun resurs egasidan ochiqchasiga pul talab qiladi.

Davlat kompaniyalari va taniqli tashkilotlar serverlariga yuqori malakali xakerlarning anonim guruhlari tomonidan mansabdor shaxslarga ta’sir o‘tkazish yoki jamoatchilik noroziligiga sabab bo‘lish maqsadida tez-tez hujum qilinadi. Hujumlar qanday amalga oshiriladi.

DoS va DDoS hujumlarining ishlash printsipi serverga maksimal darajada (xakerning imkoniyatlari imkon qadar) protsessorning hisoblash resurslarini, operativ xotirani yuklaydigan, aloqa kanallarini yopib qo'yadigan katta ma'lumot oqimini yuborishdan iborat. disk maydonini to'ldiradi. Hujum qilingan mashina kiruvchi ma'lumotlarni boshqara olmaydi va foydalanuvchi so'rovlariga javob berishni to'xtatadi.

Yagona DOS hujumlarining samaradorligi unchalik yuqori emas. Bundan tashqari, shaxsiy kompyuterdan hujum tajovuzkorni aniqlash va qo'lga olish xavfini tug'diradi. Zombi tarmoqlari yoki botnetlardan tarqatilgan hujumlar (DDoS) ancha katta foyda keltiradi.

Zombi tarmog'i (botnet) - bu bir-biri bilan jismoniy aloqasi bo'lmagan kompyuterlar guruhi. Ularni barchasi hujumchi nazorati ostida ekanligi birlashtiradi. Boshqarish troyan dasturi yordamida amalga oshiriladi, bu hozircha hech qanday tarzda o'zini namoyon qilmasligi mumkin. Hujumni amalga oshirayotganda, xaker zararlangan kompyuterlarga qurbonning veb-sayti yoki serveriga so'rov yuborishni buyuradi. Va u hujumga dosh berolmay, javob berishni to'xtatadi.

To'fon, oddiy so'z bilan aytganda, semantik yukni ko'tarmaydigan ma'lumotdir. DoS / DDoS hujumlari kontekstida toshqin - bu qabul qiluvchi tugunni qayta ishlashga majbur bo'lgan u yoki bu darajadagi bo'sh, ma'nosiz so'rovlarning ko'chkisi. Suv toshqinidan foydalanishning asosiy maqsadi aloqa kanallarini to'liq yopish, tarmoqli kengligini maksimal darajada to'yintirishdir.

Suv toshqini turlari:

MAC toshqini - tarmoq kommunikatorlariga ta'sir qilish (ma'lumotlar oqimlari bilan portlarni blokirovka qilish).

ICMP suv toshqini - jabrlanuvchini zombi tarmog'i yordamida xizmat aks sadosi so'rovlari bilan to'ldirish yoki hujum qilingan xost "nomidan" so'rovlarni yuborish, shunda barcha botnet a'zolari bir vaqtning o'zida unga aks-sado javobini yuborishadi (Smurf hujumi).

ICMP suv toshqinining alohida holati bu ping toshqinidir (serverga ping so'rovlarini yuborish).

SYN toshqini - Jabrlanuvchiga bir nechta SYN so'rovlarini yuborish, ko'p sonli yarim ochiq (mijoz tasdiqlanishi kutilayotgan) ulanishlarni yaratish orqali TCP ulanish navbatini to'ldirish.

UDP toshqin - Smurf hujumlari sxemasi bo'yicha ishlaydi, bu erda ICMP paketlari o'rniga UDP datagramlari yuboriladi.

HTTP toshqin - serverni ko'plab HTTP xabarlari bilan to'ldirish. Murakkab variant - bu HTTPS toshqinidir, u erda uzatilgan ma'lumotlar oldindan shifrlangan va hujum qilingan xost uni qayta ishlashdan oldin uni shifrini ochishi kerak.

FOYDALANILGAN ADABIYOTLAR RO’YHATI :

1. Yasnitsky D.L. "Development of method for the early detection and reflection of distributed denial of service attacks." Master's certification work. Kharkov: KNURE, 2016, 356 p.

2. Varfolomeeva A.O, Koryakovsky A.V., Romanov V.P. “Enterprise Information Systems”, M.: SIC INFRA–M, 2017, 283 p. (In Russian)

3. “The basic model of threats to the security of personal data during their processing in personal data information systems. Ministry of Telecom and Mass Communications of the Russian Federation”. Moscow, 2010. [Electronic resource]. URL: http://minsvyaz.ru/ common/upload/publication/1410084of.pdf.

4. Galatenko V.A. “The basics of information security”. INTUIT. RU "Internet University of Information Technologies", 2016, 208 p.

5. Medvedovsky I.D., Semyanov P V., Leonov D.G. “Attack on the Internet”. Publishing house DMK, 2009, 332 p.

6. Skudis E. “Opposition to hackers”, M.: DMK Press, 2013, 506 p.

7. Telnova Yu.F. “Information systems and technologies”, M.: Unity, 2017, 544 p. (In Russian)/