DEVELOPMENT OF METHODS AND ALGORITHMS TO PROTECT WEBSITES FROM ATTACKS SUCH AS DDOS

Kerimov Kamil Fikratovich
Sobirjonov Jakhongir Javlon oglu
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

Annotation: The article mainly provides information on websites and methods of analyzing DDOS attacks. Forming an understanding of algorithms in protecting websites from threats and security. An explanation of the anti-flood algorithm for HTTP is explained.

Keywords: Proxy server, algorithm, website, DDOS, HTTP-flood.

«VEB-SAYTLARNI DDOS KABI HUJUMLARDAN HIMOYA QILISH USULLARI VA ALGORITMLARINI ISHLAB CHIQISH»

Kerimov Kamil Fikratovich
Sobirjonov Jaxongir Javlon o'g'li
Muhammad al-Xorazmiy nomidagi Toshkent Axborot Texnologiyalari Universiteti

Annotatsiya: Maqolada asosan veb-saytlar va DDOS hujumlarini tahlil qilish usullari haqida ma'lumot berilgan. Veb-saytlarni tahdidlardan va xavfsizlikdan himoya qilishda algoritmlar tushunchasini shakllantirish. HTTP-flood ga qarshi qarshi algoritm haqida izoh berilgan.

Kalit so'zlar: proksi-server, algoritm, veb-sayt, DDOS, HTTP-flood.

KIRISH

Kiberhujumlarning eng dolzarb turlaridan biri DoS (DDoS) tipidagi hujumlar bo'lib, ularning maqsadi serverga texnik xizmat ko'rsatishni rad etishdir. Barcha foydalanuvchilar uchun, istisnosiz, bunday server foydalanuvchilari resurslardan foydalana olmaydi, chunki ular mavjud emas.

Natijada, qurilma butunlay shikastlangan bo'lishi mumkin [1].

DDoS hujumlarini amalga oshirishning ko'plab usullari orasida eng samaralisi botnet tarmog'idan yuborilgan ko'p sonli noto'g'ri so'rovlarni qayta ishlash orqali serverda joylashgan resurslarning katta ish yukini ta'minlashga qaratilgan hujumdir. Ushbu hujum ko'pincha tarmoqqa kirish imkoniga ega bo'lgan haqiqiy foydalanuvchilarning virusli qurilmalaridan uyushtiriladi, ular hatto o'z qurilmasidan har qanday hujum amalga oshirilayotganiga shubha qilmaydi. Shunday qilib, tizimga viruslar, qurtlar va "Troyan otlari" viruslarini kiritish orqali tarmoqqa ulangan himoyalanmagan qurilmalarga zararli dasturlar o'rnatiladi. Ko'p sonli tarmoq xostlarining infektsiyasi shunday sodir bo'ladi, shundan so'ng ushbu kompyuterlar ustidan nazorat tajovuzkorga o'tadi. Keyin hujum qiluvchi ob'ekt bir vaqtning o'zida infektsiyalangan tarmoqning barcha tugunlariga qandaydir buyruqni yuborishga asoslangan hujumni amalga oshiradi. Natijada, foydalanuvchi qurilmasiga o'rnatilgan dasturiy ta'minot faollashadi. Xost ma'lumotlari tajovuzkor nazorati ostida uzatiladi, shuning uchun "Xizmatni rad etish" tarqatilgan hujumning manbai bo'ladi [2].

Materiallar Va Uslublar

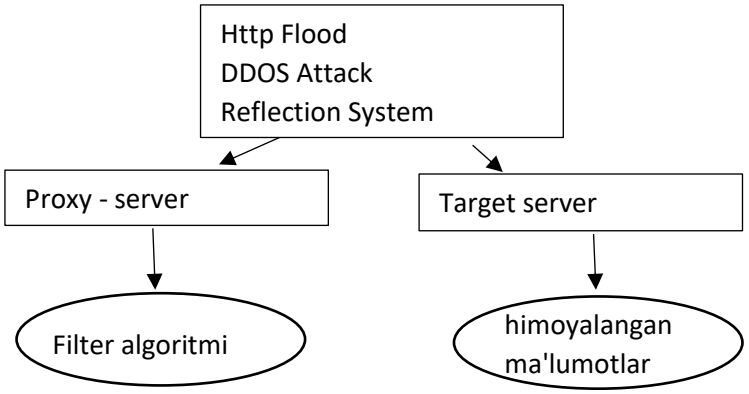
Rivojlangan hujumni aks ettirish tizimi, 1-rasmda ko'rsatilganidek, quyidagi komponentlardan iborat: kiruvchi so'rovlar uchun filtrlash algoritmini amalga oshiradigan proksi-server va hujum qilingan axborot tizimi jismoniy joylashgan maqsadli server [3].

Global Internet va proksi-server usulida so'rovlarni yuborish:

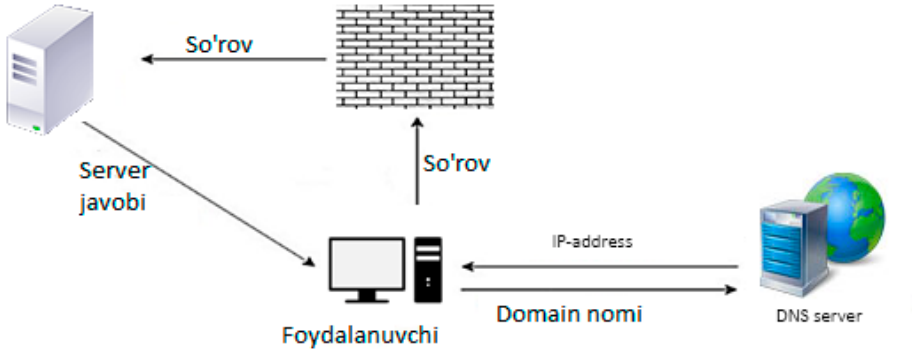
2-rasmda ko'rsatilgan HTTP proksi-server mijozlardan HTTP so'rovlarini qayta ishlash serveridir. Shunday qilib, ushbu tugun foydalanuvchi va maqsadli server o'rtasidagi oraliq aloqa bo'lib, har ikki

tomonning ko'rsatilgan xost mavjudligi to'g'risida xabardor bo'lishidan qat'i nazar. Ushbu usuldan foydalanish mijozlarga so'rovlarni yuborish va maqsadli serverdan ham, proksi-serverdan ham javob olish imkonini beradi [4].

Dastlab, so'rov yuborishda u proksi-serverga ulanadi, keyin asosiy serverga keyingi ulanish proksi-server bilan amalga oshiriladi, mijoz tomonidan talab qilinadigan resurs so'raladi va natija mijoz tomoniga qaytariladi.



1-rasm Hujumni aks ettirish tizimi ishlab chiqilishi



2-rasm Proksi-server bilan bog'liq so'rovlarni yuborish

Bundan tashqari, ba'zi hollarda mijoz tomonidan qilingan so'rov asosiy server bilan muvofiqlashtirilgan proksi-server sozlamalariga muvofiq o'zgartirilishi mumkin. Bundan tashqari, ma'lum bir konfiguratsiyaga ega proksi-texnologiyadan foydalanish kompyuter yoki axborot tizimini har xil turdagi tarmoq hujumlaridan himoya qilish imkoniyatini beradi, lekin ba'zida bu texnologiya tajovuzkorlar tomonidan maqsadli IP-manzilni yashirish yoki himoyalanmagan yoki zaif himoyalangan foydalanuvchini ma'lumotlarni ushlab turish uchun ishlatiladi.

Proksi-serverlarning barcha turlaridan ikkita turi ajralib turadi: shaffof proksi va teskari proksi.

Transparent Proxy texnologiyasi yordamida trafik marshrutizator sifatida proksi-serverga bilvosita yo'naltiriladi [5].

"Reverse Proxy" texnologiyasidan foydalanish mijoz so'rovlarini tashqi tarmoqdan mantiqiy ravishda ichki tarmoqda joylashgan serverlarga (bir yoki bir nechta bo'lishi mumkin) o'tkazish imkonini beradi. Ko'pincha, ushbu texnologiya bir qator asosiy serverlar o'rtasidagi tarmoq yukini muvozanatlash, shuningdek, L7 OSI modelining dastur darajasida xavfsizlik devori vazifasini o'taydigan ularning xavfsizligini ta'minlash uchun ishlatiladi.

So'ralgan manbaga kirishda mijoz tomonidan so'rovlar to'g'ridan-to'g'ri resurslar joylashgan asosiy serverga emas, balki proksi-serverning IP-manzili ko'rsatilgan DNS yozuvlarini o'rnatishga muvofiq proksi-serverga yuboriladi.

Mijoz tomonidan so'rov yuborilgan taqdirda, proksi-server bilan ulanish ochiladi, shundan so'ng mijoz so'rov yuboradi, so'ngra proksi-serverga o'tadi [6].

Keyin so'rovni qayta ishlash jarayoni proksi-serverda sodir bo'ladi va keyin maqsadli server bilan ulanishni ochib, mijoz so'rovini yuboring. Shundan so'ng, asosiy server mijozga ma'lumotlarni yetkazib beruvchi proksi-server so'roviga javob beradi.

Umuman olganda, proksi-server ma'lum bir protokol uchun tuzilgan mijoz qismiga ega bo'lgan ko'p funksiyali serverdir.

Veb-proksi - bu proksi-server. Server veb-serverga o'rnatilgan veb-ilova ko'rinishida anonimlikni ta'minlaydi. Bundan tashqari, so'rovlarni yuborish va axborot tizimlaridan tarkibni olish uchun oraliq vosita sifatida ishlatiladi [7].

Munozaralar Va Natijalar

Mijoz so'rovlari ular qayta ishlanadigan proksi-serverga yuboriladi, shundan so'ng mijozga javob proksi-serverda ham yaratilishi mumkin. Aks holda, mijozga o'xshash so'rov asosiy serverga yuboriladi, so'ngra javob undan mijozga uzatiladi. 3-rasmda proksi-serverli tizim sxematik tarzda ko'rsatilgan.

Ushbu tizimda proksi-server ham server, ham mijoz sifatida ishlay oladi. ATning mijoz qismidan so'rovlarni qabul qilish vaqtida u server, maqsadli serverga nisbatan esa mijoz hisoblanadi.

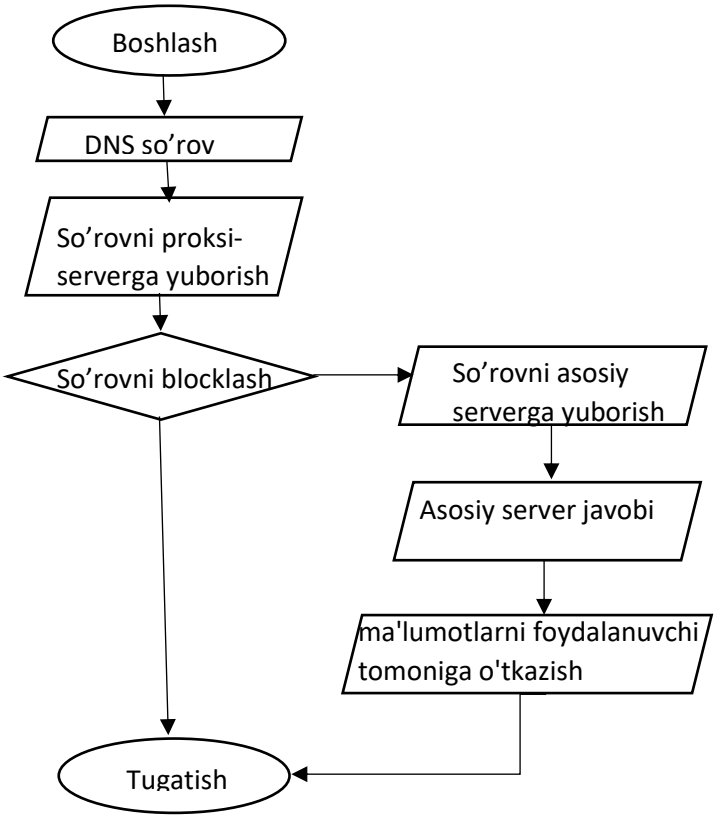
Keyinchalik, proksi-serverning jarayonini batafsilroq ko'rib chiqamiz. Dastlab, server 80 (HTTP) portida mijoz so'rovlarini qabul qilishni kutayotgan holatda. Keyin, har bir so'rov uchun so'rov qayta ishlanadigan ma'lumotlarni qayta ishlash uchun alohida oqim yaratiladi.

Proksi-serverda so'rovni qabul qilgandan so'ng, IP-manzil so'rovni yuborgan yoki uni asosiy serverga yo'naltiruvchi tomonga "Bloklangan" javobi bilan bloklanadi.

Boshqa barcha hollarda, so'rov hujjat so'raladigan masofaviy serverga yoki agar aniqlangan bo'lsa, boshqa proksi-serverga yuboriladi. Bunday holda, keshdan muvaffaqiyatsiz foydalanish (keshni o'tkazib yuborish) soni bittaga ko'payadi.

Qabul qilingan so'rovni qayta ko'rib chiqqandan so'ng, asosiy server "OK" javobini yuboradi, u avval proksi-serverga etkazib beriladi va keyinchalik mijozga uzatiladi.

Bundan tashqari, proksi-server asosiy server bilan o'zaro aloqada statistik ma'lumotlarni saqlaydi.



3-rasm Proksi-server bilan filtrlash tizimi

Agar serverdagi yuk 73% gacha oshsa, so'rovlar orasidagi vaqt proksi-serverda o'lchanadi va vaqt birligi uchun so'rovlar tezligi 1-formuladan foydalanib hisoblanadi.

$$q = \frac{C_1 * W_1 + \cdots + C_n * W_n}{t} \qquad (1)$$

bu yerda C_i - IP-manzildan t vaqt uchun so'rovlar soni; W_i - t vaqt ichida IP-manzildan so'rovlar orasidagi o'rtacha vaqt; t - so'rov chastotasi hisoblangan vaqt davri; q - vaqt birligi t uchun so'rov tezligi.

Va kelajakda, agar bitta IP-manzildan so'rovlar soni q dan 73% dan oshsa, bu IP-manzil proksi-serverda kutish vaqti bilan bloklanadi.

Xulosa

Ko'pgina dasturiy ta'minot ishlab chiqaruvchilari DDoS hujumlarini, xususan, DDoS hujumlarining eng keng tarqalgan turlari bo'lgan HTTP Flood hujumlarini aniqlay oladigan va bloklaydigan dasturiy ta'minotni ishlab chiqishdan manfaatdor. Ushbu ishda ushbu turdagi hujumlarni aniqlash va blokirovka qilish uchun ishlab chiqilgan algoritmni amalga oshiradigan va har qanday qurilmadan ishga tushirilganda foydalanish mumkin bo'lgan qulay dasturiy interfeysni amalga oshiradigan emulyatsiya dasturiy vositasini yaratishga harakat qilindi.

Ish davomida, shuningdek, eng tez-tez amalga oshiriladigan DDoS hujumlarining tasnifi amalga oshirildi, L7 so'rovlarini proksi-serverlash usuliga asoslangan tavsiya etilgan filtrlash texnikasi taqdim etildi va natijada vizual ravishda ko'rsatadigan dasturiy vosita joriy etildi. ishlab chiqilgan algoritmning samaradorligi. Biz dasturiy ta'minotning asosiy bosqichlarini ko'rsatadigan hisobotda batafsil ko'rib chiqish bilan dasturiy mahsulotni sinovdan o'tkazdik.

Adabiyotlar:

1. Telnova Yu.F. “Information systems and technologies”, M.: Unity, 2017, 544 p. (In Russian)/
2. “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.
3. Varfolomeeva A.O, Koryakovsky A.V., Romanov V.P. “Enterprise Information Systems”, M.: SIC INFRA–M, 2017, 283 p. (In Russian)
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. 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.