MAXKAMOV Anvarjon Abdujabborovich
O‘zbekiston xalqaro islom akademiyasi Zamonaviy axborot-kommunikatsiya texnologiyalari kafedrasi dotsenti, PhD

AXBOROT XAVFSIZLIGINI TA’MINLASHDA TARMOQDAGI NOQONUNIY HARAKATLARNI ANIQLASH ALGORITMLARI

АЛГОРИТМЫ ОПРЕДЕЛЕНИЯ НЕЗАКОННОЙ ДЕЯТЕЛЬНОСТИ В СЕТИ ПРИ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ALGORITHMS FOR DETERMINING ILLEGAL ACTIVITIES IN THE NETWORK IN PROVIDING INFORMATION SECURITY

Annotatsiya. *Ushbu maqolada axborot xavfsizligini ta’minlashda tarmoqdagi noqonuniy harakatlarni aniqlash algoritmlari keltirib o‘tilgan. Hozirgi vaqtda xech qaysi davlatni iqtisodiy va ijtimoiy sohalarini rivojlanishini zamonaviy axborot texnologiyalarisiz tasavvur qilib bo‘lmaydi. Shu sababdan butun dunyoda axborotga bo‘lgan talab va extiyoj ham kun sayin ortib bormoqda. Ayniqsa, axborot texnologiyalarining rivojlanib borishi ma’lumotlar xajmining ortib borishiga sabab bo‘lmoqda. Bu esa o‘z navbatida axborotga boshqacha baho berish, ya’ni unga kontent sifatida qarash va yangicha munosabatlarni yuzaga keltirish va shu qatori axborotlarga bo‘ladigan noqonuniy hujumlarni aniqlashni talab etadi. Keltirib o‘tilgan algoritmlardagi kiruvchi filtrlar tarmoq xavfsizligini oshiradi va trafik oqimini boshqarish uchun xavfsizlikni rejalashtirishda yordam beradi. Ular faqat xavfsiz va ishonchli tarmoqlarga, xostlarga yoki avtonom tizimlarga xavfsiz tarmoqqa kirish imkonini beradi, trafikni cheklash va muayyan port, xizmat, server yoki tarmoqni boshqaradigan qoidalar va siyosatlarni aniqlash uchun marshrutizatorlardan foydalanadi.*

Kalit so‘zlar: *tarmoq, filtr, axborot xavfsizligi, trafik, server, tarmoqni boshqaradigan qoidalar, tarmoq siyosati.*

Аннотация. *Алгоритмы обнаружения противоправной активности в сети упомянуты в этой статье. В настоящее время развитие экономической и социальной сферы любой страны невозможно представить без современных информационных технологий. По этой причине спрос и потребность в информации во всем мире растет с каждым днем. В частности, развитие информационных технологий является причиной увеличения объема данных. Это, в свою очередь, требует иной оценки информации, то есть рассмотрения ее как содержания и создания новых связей, а также выявления неправомерных посягательств на информацию. Входящие фильтры в вышеупомянутых алгоритмах повышают безопасность сети и помогают планировать безопасность для управления потоками трафика. Они разрешают только безопасным и надежным сетям, хостам или автономным системам доступ к защищенной сети, используя маршрутизаторы для ограничения трафика и определения правил и политик, которые управляют определенным портом, службой, сервером или сетью.*

Ключевые слова: *сеть, фильтр, информационная безопасность, трафик, сервер, сетевые правила, сетевая политика.*

Annotation*. Algorithms for detecting illegal activities in the network are mentioned in this article. Currently, the development of economic and social spheres of any country cannot be imagined without modern information technologies. For this reason, the demand and need for information in the whole world is increasing day by day. In particular, the development of information technologies is the reason for the increase in the volume of data. This, in turn, requires a different assessment of information, that is, looking at it as content and creating new relationships, as well as identifying illegal attacks on information. The inbound filters in the aforementioned algorithms increase network security and help with security planning to manage traffic flow. They allow only secure and trusted networks, hosts or autonomous systems access to a secure network, use routers to restrict traffic and define rules and policies that govern a particular port, service, server or network*

Keywords*: network, filter, information security, traffic, server, network rules, network policy.*

KIRISH

Hozirgi vaqtda xech qaysi davlatni iqtisodiy va ijtimoiy sohalarini rivojlanishini zamonaviy axborot texnologiyalarisiz tasavvur qilib bo‘lmaydi. Shu sababdan butun dunyoda axborotga bo‘lgan talab va extiyoj ham kun sayin ortib bormoqda. Ayniqsa, axborot texnologiyalarining rivojlanib

ISSN 2181-9572

borishi ma’lumotlar xajmining ortib borishiga sabab bo‘lmoqda. Bu esa o‘z navbatida axborotga boshqacha baho berish, ya’ni unga kontent sifatida qarash va yangicha munosabatlarni yuzaga keltirmoqda. Bunday sharoitda axborotni oshkor bo‘lishi, o‘g‘irlanishi yoki yo‘q qilinishi kabi holatlardan himoyalanish zarur.

ASOSIY QISM

Tarmoqdagi noqonuniy faoliyatni aniqlash murakkab vazifa bo‘lib, ko‘pincha turli xil algoritm va usullarning kombinatsiyasini talab qiladi. Tarmoqdagi noqonuniy harakatlarni aniqlash uchun bir nechta tez ishlaydigan va ommabop algoritmlarni keltirib o‘tamiz.

Imzoga asoslangan algoritm (Signature-based detection). Imzoga asoslangan aniqlash tarmoqdagi noqonuniy faoliyatni aniqlash uchun keng qo‘llaniladigan yondashuvdir. Bu tarmoq trafigini yoki fayllarni ma’lum imzolar yoki muayyan tahdidlar yoki hujumlar bilan bog‘liq naqshlar bilan solishtirishni o‘z ichiga oladi va himoyalaydi.

Trafik tahliliga asoslangan algoritm: Paketlar yoki fayllar kabi tarmoq trafigi tekshiriladi va ma’lumotlar bazasidagi imzolar bilan taqqoslanadi.

Moslash jarayoni: Algoritm kuzatilgan tarmoq trafigi va ma’lumotlar bazasidagi imzolar o‘rtasidagi moslikni tekshiradi. Agar o‘yin topilsa, bu ma’lum noqonuniy faoliyat mavjudligini ko‘rsatadi.

Ogohlantirish yoki harakat: Moslik aniqlanganda, tizim ogohlantirish yaratishi yoki shubhali trafikni bloklash, fayllarni karantin qilish yoki xavfsizlik xodimlarini xabardor qilish kabi oldindan belgilangan harakatlarni bajarishi mumkin.

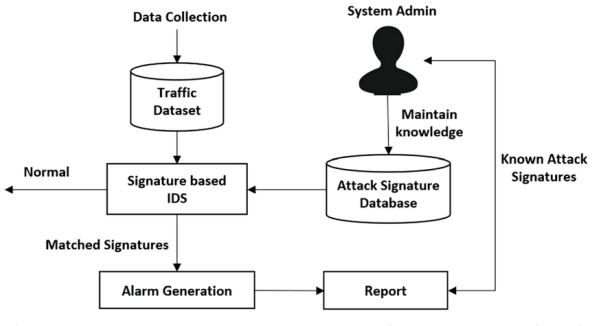
Tezlik: Imzoga asoslangan aniqlash, kuzatilgan trafikni avvaldan mavjud imzolar bazasi bilan solishtirish orqali taniqli tahdidlarni tezda aniqlashni amalga oshiradi.

Aniqlik: Imzolar ma’lum tahdidlarga xos bo‘lganligi sababli, imzoga asoslangan aniqlash past noto‘g‘ri ijobiy ko‘rsatkichlarga ega bo‘ladi, ya’ni u ma’lum noqonuniy harakatlar mavjudligini aniqlaydi.

Cheklovlar: Imzoga asoslangan aniqlash ma’lumotlar bazasida yangilangan imzolarga ega bo‘lishga asoslanadi. Mos imzolarga ega bo‘lmagan yangi yoki ilgari ko‘rilmagan tahdidlarni aniqlashda qiynalishi mumkin. Imzolar ma’lumotlar bazasini doimiy yangilash samaradorlikni saqlash uchun zarur.

Umumiy ilovalar: Imzoga asoslangan aniqlash odatda antivirus dasturlari, bosqinlarni aniqlash tizimlari (IDS) va tarmoqqa asoslangan xavfsizlik devorlarida qo‘llaniladi.

Imzoga asoslangan aniqlash ma’lum tahdidlarga qarshi samarali bo‘lsa-da, tarmoqdagi paydo bo‘lgan yoki ilgari ko‘rilmagan noqonuniy harakatlarni aniqlash uchun uni anomaliyalarni aniqlash yoki mashinani o‘rganish algoritmlari kabi boshqa aniqlash usullari bilan to‘ldirish muhim ahamiyatga egadir.



1-rasm. Imzoga asoslangan aniqlash algoritmi

Chuqur paket tekshiruvi algoritmi (Deep Packet Inspection). Deep Packet Inspection (DPI) - bu tarmoq paketlari tarkibini batafsil tahlil qilish uchun ishlatiladigan usul. Bu tarmoq trafigini chuqurroq tushunish uchun alohida paketlarning foydali yukini, sarlavhalarini va protokollarini tekshirishni o‘z ichiga oladi. DPI haqida umumiy ma’lumotni quyida keltirib o‘tamiz.

Paket tahlili: DPI odatda tarmoq qurilmalari tomonidan tekshiriladigan an’anaviy sarlavha ma’lumotlaridan tashqari tarmoq paketlarining mazmunini tekshiradi. U uzatilayotgan haqiqiy ma’lumotlarni, shu jumladan matn, tasvirlar, fayllar yoki paket yukidagi har qanday boshqa ma’lumotlarni ko‘rib chiqadi.

Protokol identifikatsiyasi: DPI HTTP, FTP, SMTP yoki DNS kabi tarmoq aloqalarida ishlatiladigan maxsus protokollarni aniqlay oladi. Bu foydalanilayotgan protokollar asosida trafikning turli hil turlarini tasniflash imkonini beradi.

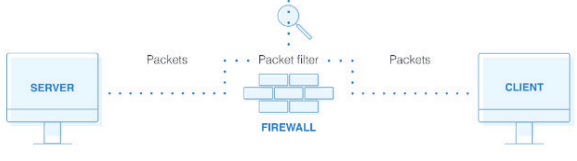
Kontentni tekshirish: DPI muayyan xatti-harakatlar yoki noqonuniy xatti-harakatlarning naqshlari, imzolari yoki ko‘rsatkichlarini aniqlash

uchun paketlardagi tarkibni tahlil qiladi. U ma’lum bo‘lgan zararli dasturlarni, shubhali buyruqlarni, maxfiy ma’lumotlarni yoki boshqa oldindan belgilangan mezonlarni qidirib topadi.

Traffic Control: DPI tahlil qilingan kontent asosida granuler trafikni boshqarish imkonini beradi. U ma’lum trafik turlarini ustuvorlashtirishi yoki ustuvorligini yo‘qotishi, muayyan protokollar yoki ilovalarni bloklashi yoki aniqlangan kontentga asoslangan xizmat sifati (QoS) siyosatini qo‘llaydi.

Tahdidlarni aniqlash: DPI zararli dasturlar, viruslar, tajovuzkorlik urinishlari, ma’lumotlarni o‘chirish yoki ruxsatsiz kirish urinishlari kabi turli xil noqonuniy harakatlar yoki xavfsizlik tahdidlarini aniqlay oladi. Paket tarkibini tekshirish orqali u zararli yoki shubhali xatti-harakatlarning ko‘rsatkichlarini aniqlaydi hamda hujumni bartaraf etadi.

Ilovalardan xabardorlik: DPI tarmoq ichida foydalaniladigan muayyan ilovalar yoki xizmatlarni aniqlay oladi, bu esa ilovalarga xos siyosatlar, ishlashni optimallashtirish yoki xavfsizlik choralarini ko‘rish imkonini beradi. Bularni quyidagi 2-rasmdan ham aniqlash mumkin.



2-rasm. Chuqur paket tekshiruvi algoritmi

DPI odatda tarmoq xavfsizligi qurilmalarida, jumladan, xavfsizlik devorlari, tajovuzlarni aniqlash va oldini olish tizimlari (IDS/IPS), tarmoq monitoringi vositalari va trafikni shakllantirish yoki o‘tkazish qobiliyatini boshqarish echimlarida qo‘llaniladi. Ammo shuni ta’kidlash kerakki, DPI maxfiylik va tarmoq betarafligi bilan bog‘liq xavotirlarni keltirib chiqaradi, chunki u tarmoq trafigini chuqur tekshirishni o‘z ichiga oladi. DPI yechimlarini amalga oshirishda tegishli himoya choralari va huquqiy va ahloqiy ko‘rsatmalarga rioya qilish zarur.

Mashinani o‘rganishga asoslangan tasnif algoritmi (Machine learning-based classification). Mashinani o‘rganishga asoslangan tasniflash ma’lumotlarni oldindan belgilangan toifalar yoki sinflarga tasniflash uchun algoritmlar va modellardan foydalanadigan usuldir. Tarmoqdagi noqonuniy faoliyatni aniqlash kontekstida mashinani o‘rganishga asoslangan tasniflash samarali yondashuv bo‘lishi mumkin. Bu qanday ishlashi haqida umumiy ma’lumotlarni quyida ko‘rib chiqiladi.

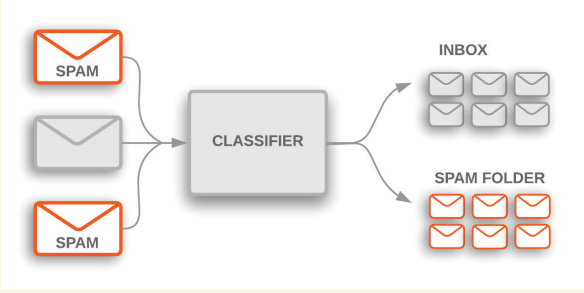
Trening ma’lumotlari: Mashinani o‘rganish modeli etiketli ma’lumotlar to‘plamidan foydalangan holda o‘qitiladi. Ma’lumotlar to‘plamida oddiy yoki noqonuniy faoliyat sifatida tasniflangan tarmoq trafigiga yoki hodisalarga misollar mavjud. Belgilangan ma’lumotlar qonuniy va noqonuniy faoliyat bilan bog‘liq bo‘lgan naqsh va xususiyatlarni o‘rganish uchun model uchun asos bo‘lib xizmat qiladi. Trafik yoki hodisalarning xususiyatlarini ifodalash uchun tarmoq ma’lumotlaridan tegishli xususiyatlar yoki atributlar olinadi. Ushbu xususiyatlar tarmoq protokollari, manba va maqsad IP manzillari, paketlar hajmi, vaqt belgilari yoki oddiy va noqonuniy harakatlarni farqlashga yordam beradigan boshqa tegishli ma’lumotlarni o‘z ichiga oladi.

Modelni o‘qitish: Olingan xususiyatlar qaror daraxti, qo‘llab-quvvatlash vektor mashinasi yoki neyron tarmoq kabi mashinani o‘rganish modelini o‘rgatish uchun hizmat qiladi. Model xususiyatlar va tegishli sinf belgilari (normal yoki noqonuniy) o‘rtasidagi naqsh va munosabatlarni aniqlashni o‘rganadi. Model o‘qitilgandan so‘ng, u tarmoq trafigining yangi, ko‘rilmagan holatlarini yoki hodisalarni oddiy yoki potentsial noqonuniy deb tasniflashi mumkin. Model olingan xususiyatlar asosida bashorat qilish uchun o‘rganilgan naqsh va qoidalarni qo‘llaydi.

Baholash va takrorlash: Mashinani o‘rganish modelining ishlashi tekshirish ma’lumotlar to‘plami yoki o‘zaro tekshirish usullari yordamida baholanadi. Agar kerak bo‘lsa, modelni takomillashtirish, giperparametrlarni sozlash yoki aniqlikni oshirish va noto‘g‘ri musbat yoki noto‘g‘ri salbiylarni minimallashtirish uchun turli xil algoritmlarni sinab ko‘rish mumkin.

Joylashtirish va monitoring: O‘qitilgan model real vaqtda tarmoq muhitida kiruvchi tarmoq trafigini yoki hodisalarini doimiy ravishda tasniflash uchun o‘rnatiladi. U noqonuniy harakatlarni kuzatish va aniqlash uchun bosqinlarni aniqlash tizimi (IDS), xavfsizlik devori yoki boshqa tarmoq xavfsizligi vositalariga birlashtirilishi mumkin.

ISSN 2181-9572



3-rasm. Mashinani o‘rganishga asoslangan tasniflash algoritmi

Mashinani o‘rganishga asoslangan tasniflash noma’lum yoki rivojlanayotgan tahdidlarni aniqlash qobiliyati, o‘zgaruvchan hujum shakllariga moslashish va doimiy o‘rganish va optimallashtirish orqali noto‘g‘ri pozitivlarni kamaytirish potentsialini o‘z ichiga olgan bir qator afzalliklarni taqdim etadi. Biroq, u haqiqiy stsenariylarda optimal ishlashni ta’minlash uchun yuqori sifatli etiketli o‘quv ma’lumotlarini, ehtiyotkorlik bilan xususiyatlarni tanlashni va modelga muntazam texnik xizmat ko‘rsatishni talab qiladi.

XULOSA

Xulosa o‘rnida shuni ta’kidlab o‘ish joizki, bugungi kunda axborot xavfsizligini ta’minlashda tarmoqdagi noqonuniy harakatlarni aniqlash juda ham dolzarb vazifaga aylanmoqda hamda katta hajmdagi ma’lumotlarni yetkazib berishda ushbu ma’lumotlarni havfsiz yetib borishini ta’minlash tarmoq xavfsizligida asosiy vositaga aylanib bormoqda. Yuqorida keltirib o‘tilgan algoritmlar asosida tarmoqdagi noqonuniy harakatlarni aniqlashda foydalanish tarmoq xavfsizligini yanada yahshiroq himoyalshga yordam beradi.

FOYDALANILGAN ADABIYOTLAR

1. Nigmatov X., Umarov A.U. “Zamonaviy axborot-kommunikatsiya texnologiyalarining aloqa kanallarida axborotlarni himoyalash”. Monografiya. “Inovatsiyon rivojlanish nashriyo-matbaa uyi”. Toshkent. 2020.144 bet.
2. Ясенев В.Н., Дорожкин А.В., Сочков А.Л., Ясенев О.В. Информационная безопасность: Учебное пособие. Нижний Новгород: Нижегородский госуниверситет им. Н.И.Лобачевского, 2017. – 198 с.
3. Maheshwari, R., & Gupta, R. K. (2014). An Efficient Methodology for Traffic Filtering Using Clustering Approach. International Journal of Scientific & Engineering Research, 5(7), 213-218.
4. Dasgupta, D., & Mahanti, A. (2017). A Survey on Traffic Filtering Techniques for DDoS Attack Mitigation. IEEE Communications Surveys & Tutorials, 19(4), 2450-2471.