LOYIHASI //Новости образования: исследование в XXI веке. – 2023. – Т. 1. – №. 6. – С. 378-386.

14. Ziyoda M., Nizommiddin N. RAQAMLI IQTISODIYOTDA SUN'IY INTELLEKT TEXNOLOGIYALARINI TURLI SOHALARDA AVTOMATLASHTIRISH VOSITALARI //International Journal of Contemporary Scientific and Technical Research. – 2023. – С. 246-250.

15. Ramazon, Mixliyev, and Babayarov Abdusattor. "MIKROSKOP YORDAMIDA HUJAYRALARDAGI QON VA OQ QON HUJAYRALARI SONI BO‘YICHA BEMORLARNING SOG‘LIG‘INI ANIQLASH." International Journal of Contemporary Scientific and Technical Research (2023): 133-137.

16. Javlon, Kholmatov, and Mustafoyev Erali. "STRUCTURE AND PRINCIPLE OF OPERATION OF FULLY CONNECTED NEURAL NETWORKS." International Journal of Contemporary Scientific and Technical Research (2023): 136-141.

17. Obid o’g, Assistent Salimov Jamshid, Assistent Abror Mamaraimov Kamalidin o'g, and Assistent Normatov Nizomiddin Kamoliddin o‘g. "Numpy Library Capabilities. Vectorized Calculation In Numpy Va Type Of Information." Eurasian Research Bulletin 15 (2022): 132-137.

18. Ziyoda, Maydonova, and Normatov Nizommiddin. "RAQAMLI IQTISODIYOTDA SUN'IY INTELLEKT TEXNOLOGIYALARINI TURLI SOHALARDA AVTOMATLASHTIRISH VOSITALARI." International Journal of Contemporary Scientific and Technical Research (2023): 246-250.

19. Nizomiddin, Normatov. "TA’LIMDA DASTURLASH JARAYONINI BAHOLASHGA ASOSLANGAN AVTOMATLASHTIRILGAN TIZIMNI TADBIQ ETISH." International Journal of Contemporary Scientific and Technical Research (2023): 24-28.

20. Kamoliddin o‘g’li, Normatov Nizomiddin, and Ergashev Sirojiddin Baxtiyor o‘g‘li. "ERWIN DASTURI YORDAMIDA IDEF0, IDEF3 VA DFD STANDAT DIAGARAMMALARIDAN FOYDALANIB TIZIM SIFATIDA YARATILGAN UNIVERSITETNING MONITORING BO ‘LIMI LOYIHASI." Новости образования: исследование в XXI веке 1.6 (2023): 378-386.

TARMOQ XUJUMLARINI ANIQLASH VOSITALARI TAHLILI

Qurbonaliyeva Dilshoda
Toshkent axborot texnologiyalari universiteti, O‘zbekiston
dilshodavaliyevna@gmail.com

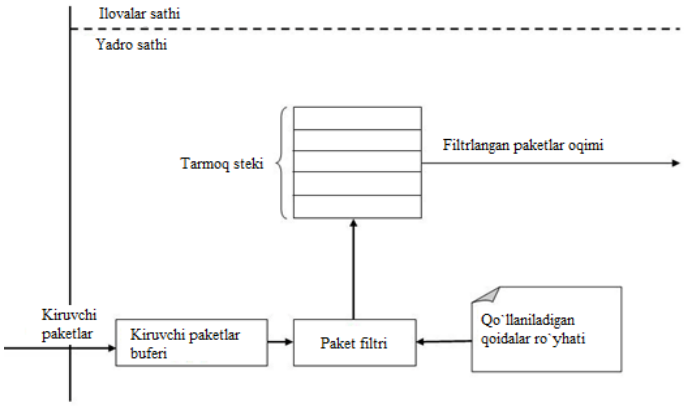
Annotatsiya. Ushbu maqolada tarmoqlararo ekranlar, tarmoq hujumlarini aniqlash va bartaraf etish tizimlari (IPS, IDS), Honeypot texnologiyalari hamda ularning avzalliklari va kamchiliklari haqida so‘z boradi.

Kalit so‘zlar. Tarmoq xavfsizligi, paketlar klassifikatsiyasi, tarmoqlararo ekranlar, IPS, IDS, Honeypot.

Tarmoq xavfsizligi bu tarmoqqa bo’ladigan xujumlar va suqulib kirishlarni monitoringlash, bartaraf etish va javob qaytarish uchun mo’ljallangan xavfsizlik siyosati, taktikasi va instrumentlarini tavsiflovchi soha hisoblanadi. U hujumlarni aniqlab, buzg’unchilarning hujumlarini yengib, tarmoqdagi faoliyatni aniqlay oladi va tarmoq o’tkazuvchanligi va blokirovkadan foydalanadi. Bunday holatda yechimlaradan biri xujumlarni bartarat etish tizimidan (IPS – Intrusion Prevention System) foydalanish, IPS - kirish ma'lumotlarini tahlil qilish orqali buzg’unchilarning mavjudligini aniqlashga imkon beradigan himoya vositasi, bu vositalar ma'lumotlar to'plamiga ega bo'lgan holda, kirish ma'lumotlar paketi namunalarini o'z ichiga olgan ma'lumotlar bazasi qoidalari va imzolari bilan taqqoslash orqali tahlil qilinadi. Bunda agar tarmoq paketlari ma’lumotlar bazasidagi qoidalarga mos kelsa tarmoq ma’muri buzg’unchilik holati haqida ogohlantirish yuboradi va aksincha [1].

Kompyuter tarmoqlaridan foydalanish tobora kengayib bormoqda. Bu biznesni tashkil qilish uchun ham, jismoniy shaxslar uchun ham ma'lumotlarni o'g'irlashga qaratilgan jiddiy tahdidlardan himoya qilish uchun juda muhimdir. Hozirgi kunda IT-bozorida ko'plab xavfsizlik yechimlari mavjud. Ulardan ba'zilari Tarmoqlararo ekran, Xujumlarn aniqlash va bartaraf etish tizimi (IDPS – Intrusion Detection Prevention System), Honeypot kabilar quyida keltirilgan va tahlil etilgan.

Tarmoqlararo ekranlar - bu ba'zi bir paketlarni boshqalarga o'tish va blokirovka qilishga imkon beradigan tashkilotning ichki tarmog'ini boshqa tarmoqlardan ajratib turuvchi apparat va dasturiy ta'minotdir. U himoya qiladigan tarmoq zonalarida o'rnatilgan ruxsatsiz yoki noqonuniy seanslarning oldini olish uchun ishlaydi. Tarmoqlararo ekranlar tashqi dunyodan ruhsat etilmagan interaktiv kirishlardan himoya qilish uchun tuzilgan [2]. Tarmoqlararo ekranlar mexanizmlar juftligi sifatida ko'rib chiqilishi mumkin: biri trafikni blokirovka qilish uchun, ikkinchisi trafikni o’tkazib yuborish uchun mavjud. Asosan, xavfsizlik devorlarining sonini kooperativ, yaxlit va chuqur tarmoq xavfsizligini himoya qilish uchun boshqariladigan tarmoqning tegishli holatiga o'rnatish mumkin. Xavfsizlik devorlarini boshqaradigan administrator tarmoqlararo ekran qoidalarini o'rnatishda ehtiyot bo'lishi kerak (1-rasm).



1.-rasm. Paketlarni filtrlash arxitekturasining sxemasi

Tarmoqlararo ekranlarning afzalliklari quyidagilardan iborat:

1. Tarmoqlararo ekranlar noqonuniy bo'lgan trafikning oldini olishi mumkin.

2. Tarmoqlararo ekranlar ushbu protokollar va xizmatlarni osonlikcha filtrlashi mumkin.

3. Tarmoqlararo ekranlar ichki tarmoq nomlarini tashqi xostlardan yashirish orqali ichki tarmoqni himoya qilishga yordam beradi.

4. Tarmoqlararo ekranlar bitta tizimda tarmoq trafigini kengaytirilgan ro'yxatga olishni jamlashi mumkin.

Tarmoqlararo ekranlarning kamchiliklari quyidagilardan iborat:

1. Tarmoqlararo ekranlar qonuniy trafikni noqonuniy trafikdan farqlash uchun qo'lda tuzilgan qoidalar to'plamidan foydalanadilar.

2. Tarmoqlararo ekranlar tarmog'i hujumiga reaktsiya berolmaydi va samarali qarshi choralarni ko'rsata olmaydi.

3. Ko'pgina tarmoqlararo ekranlar tarmoq trafigini tashkil etuvchi ma'lumot paketlarining tarkibini tahlil qilmaydi.

4. Tarmoqlararo ekranlar Intranetdan keladigan hujumlarning oldini olmaydi.

5. Tarmoqlararo ekranlar filtrlash qoidalari dastur sathidan keladigan hujumni oldini olmaydi [3].

Hujumlarni aniqlash va bartaraf etish tizimi (IDS) axborot tizimlariga hujumlarga qarshi kurashishda yordam beradi. Bunga turli xil tizimlar va tarmoq manbalaridan ma'lumot to'plash orqali erishiladi. IDS xavfsizlikning mumkin bo'lgan buzilishini aniqlash uchun kompyuter yoki tarmoq ichidagi turli sohalardagi ma'lumotlarni to'playdi va tahlil qiladi. Suqulib kirishlar tashkilot tashqarisida ham, tashkilot ichida ham hujumlarni o'z ichiga olishi mumkin [3].

IDPSning afzalliklari:

1. IDSni o'rnatish osonroq, chunki u mavjud tizimlarga yoki infratuzilmaga ta'sir qilmaydi.

2. Tarmoqqa asoslangan IDPS sensorlari TCP SYN hujumi, paketli hujum va h. kabi har qanday zararli hujum uchun paket sarlavhalarini tekshirish orqali ko'plab hujumlarni aniqlay oladi.

3. IDPS real vaqt rejimida trafikni kuzatib boradi. Shunday qilib, tarmoqqa asoslangan IDPS zararli faoliyatni ular sodir bo'lganda aniqlashi mumkin.

4. Tarmoqlararo ekranlar tashqarisida joylashtirilgan IDS sensori Tarmoqlararo ekran orqasidagi manbalarga bo’ladigan zararli xujumlarni aniqlay oladi [4].

IDPSning kamchiliklari:

1. IDPS kuchli identifikatsiya va autentifikatsiya mexanizmiga alternativa emas.

2. IDPS xavfsizlikning barcha muammolarini hal eta olmaydi.

3. Xujum aniqlangandan va xabar qilinganidan keyin uni tekshirish uchun inson aralashuvi talab qilinadi.

5. IDPS zararli faoliyatni aniqlay olmasa, soxta blokirovka qilish holatlari yuzaga keladi [3].

“Honeypot” bu axborot tizimlaridan ruxsatsiz foydalanishga bo'lgan urinishlarni aniqlash, yo'q qilish yoki biron-bir tarzda qarshi turish uchun mo'ljallangan tuzoq hisoblanadi. Odatda bu kompyuter, ma'lumotlar yoki tarmoqning bir qismi bo'lib ko'rinadigan, ammo aslida xavfsiz holatga keltirilgan va kuzatiladigan va buzg'unchilar uchun ma'lumot yoki qiymat manbai bo'lgan tarmoq saytidan iborat. “Honeypot” buzg'unchilarni qonuniy tizim ekanligiga ishontirish orqali aldaydi.

“Honeypot” afzalliklari:

1. Kichik ma’lumotlar to'plamlari: “Honeypot” faqat biror kishi yoki biror narsa ular bilan o'zaro aloqada bo'lganda ma'lumot to'playdi.

2. Yolg‘on ogohlantirishlarni darajasi pastligi: ko'pgina aniqlash texnologiyalaridagi eng katta muammolardan biri bu soxta ijobiy yoki noto'g'ri ogohlantirishlarning paydo bo'lishi. “Honeypot” bilan qilingan har qanday harakat, ta'rifiga ko'ra, ruxsatsizdir va bu hujumlarni aniqlashda juda samarali bo'ladi.

3. Salbiy holatlarni o’tkazib yuborish: An'anaviy texnologiyalarning yana bir muammosi - noma'lum hujumlarni aniqlay olmaslik.

4. Shifrlash: Hujum yoki zararli harakat shifrlanganmi yoki yo'qmi, “Honeypot” ushbu harakatni ushlaydi. Ko'proq tashkilotlar o'zlarining muhitlarida (masalan, SSH, IPSec va SSL kabi) shifrlash usullarini qabul qilar ekan, bu katta muammoga aylanadi. Asal qutilari buni amalga oshirishi mumkin, chunki shifrlangan zondlar va hujumlar “Honeypot” bilan yakunlanib, faoliyat “Honeypot” tomonidan hal qilinadi.

5. IPv6: “Honeypot” IP protokoli, shu jumladan IPv6-dan qat'i nazar, har qanday IP muhitida ishlaydi. IPv6 bu Mudofaa vazirligi kabi ko'plab tashkilotlar va Yaponiya kabi ko'plab mamlakatlar faol qabul qiladigan yangi IP standartidir. Tarmoqlararo ekranlar yoki IDPS sensorlari kabi ko'plab zamonaviy texnologiyalar IPv6-ni ishlay olmaydi.

6. Yuqori moslashuvchan: “Honeypot” juda moslashuvchan, turli xil sharoitlarda foydalanish imkoniyati bilan, ma'lumotlar bazasida joylashtirilgan Ijtimoiy himoya raqamidan tortib, kompyuterlarning butun tarmog'iga qadar.

7. Minimal manbalar: “Honeypot” hatto eng katta tarmoqlarda ham minimal resurslarni talab qiladi. Oddiy, eski Pentium kompyuteri millionlab IP manzillarni kuzatishi mumkin [4].

“Honeypot” kamchiliklari: Barcha afzalliklardan tashqari, “Honeypot”ning ham kamchiliklari bor. “Honeypot”ning asosiy kamchiliklaridan biri bu riskdir. “Honeypot” bu yomon odamlar bilan o'zaro aloqa qiladigan xavfsizlik manbai, ammo xujumchilar “Honeypot”dan boshqa zararli bo'lmagan tizimlarga hujum qilish yoki zarar etkazish uchun ham foydalanish xavfi mavjud.

Tarmoq xujumlarini aniqlash vositalarini tahlili shuni ko’rsatadiki, hozirda qo’llanilayotgan tarmoq himoyasi vositalari: tarmoqlararo ekranlar, IPS, IDS va “Honeypot” tizimlari bozorda keng tarqalgan va tarmoq xavfsizligi uchun xujumlarni o’z vaqtida aniqlash va bartaraf etish, hujum uyushtirilganlik holatlarini monitoring qilish va tahlillashda asosan xujumlarni aniqlash tizimlari qo’llaniladi.

Foydalanilgan adabiyotlar ro‘yxati:

1. World internet stats. Number of world Internet users on 30 June 2018. Available at: http://www.internetworldstats.com/stats.htm, [Accessed 20 June 2018].

2. Cavalcante, R. C., I. I. Bittencourt, A. P. Silva, M. Silva, E. Costa and R. A Survey of Security in MultiAgent Systems. Expert Systems with Applications. 2016. (39): 4835-4846.

3. K. Scarfone and P. Mell, ”Guide to Intrusion Detection and Prevention Systems (IDPS),” Gaithersburg, MD, Rep. NIST Special Publication 800-94,Feb. 2007.

4. D. Rozenblum, “Understanding Intrusion Detection System,” www.sans.org/reading_room/whitepapers/detection/understanding-intrusiondetection-systems_337, October 31, 2003.

VARIATSION KVANT ALGORITMLARINI QO‘LLASHNING SAMARADORLIGI

Istamov Ismoilzoda Uktamovich
Samarqand davlat universiteti tadqiqotchisi
Sulaymonov Mirobid Abduxolikovich
Samarqand davlat veterinariya meditsinasi, chorvachilik va biotexnologiyalar universiteti
istamovismoilzoda@gmail.com

Annotatsiya: Murakkab kvant tizimlarini simulyatsiya qilish yoki keng ko‘lamli chiziqli algebra masalalarini yechish juda yuqori hisoblash klassik kompyuterlar uchun juda qiyin. Kvant kompyuterlari va algoritmlari esa yechimni yuqori darajada aniqlikda olish imkonini bermoqda.

Parametrlashtirilgan kvant sxemasini o‘rgatish uchun klassik optimallashtiruvchidan foydalanadigan variatsion kvant algoritmlari (VKA) ushbu cheklovlarni hal qilishning ilg’or texnologiyasi sifatida paydo bo‘ldi. Kvant kompyuterlari uchun mo‘ljallangan deyarli barcha ilovalar uchun VKAlar taklif qilindi va ular kvant ustunligiga erishish uchun eng yaxshi yechimni topib berish xolati bilan afzal bo‘lib ko‘rinadi. Shunday bo‘lsa-da, muammolar, jumladan, VKAlarni o‘qitish qobiliyati, aniqligi va samaradorligi bilan bog'liq muammolar saqlanib qolmoqda. Bu ushbu tadqiqot ishida VKA sohasini ko‘rib chiqiladi, ularning qiyinchiliklarini yengish strategiyalarini muhokama qilinadi va kvant ustunligiga erishish uchun ulardan foydalanishning qiziqarli istiqbollarini ta'kidlanadi. Kvant algoritmlarini sinab ko‘rish va kvant kompyuterlari afzallik beruvchi sun’iy intellekt orqali yangi muammolarni aniqlash mumkin bo‘ladi.

Kalit so‘zlar: Kvant, variatsion kvant algoritmlari, sun’iy intellekt, machine learning, shovqinli oraliq miqyosli kvant (ShO‘MK).

Bugungi kunda variatsion kvant algoritmlari yordamida murakkab matematik hisoblashni amalga oshirish va sun’iy intellekt tezligini, samaradorligini va aniqligini oshirish orqali uni takomillashtirib bormoqda. Ushbu soha kvant hisoblashni turli xil jarayonlarni, jumladan har qanday jarayon uchun matematik modelni qurishda sun’iy intellektdan foydalanish imkonini beradi.

Kvant hisoblashlari zarur jismoniy jihozlarni yaratish uchun o‘nlab yillar davom etgan izlanishlarga turtki bo‘lgan bir qator ilovalar uchun va'da beradi. Masalan, klassik usullarga nisbatan eksponensial tezlik bilan kvant algoritmlari raqamlarni faktorlashtirishi, kvant tizimlarini taqlid qilishi yoki chiziqli tenglamalar tizimini echishi mumkin.