TARMOQ TRAFIGIDA SHUBHALI PAKETLARNI ANIQLASH ALGORITMI VA STRUKTURASI

G‘ulomov Sh.R
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
Kiberxavfsizlik fakulteti dekani, PhD, dotsent.
sherhisor30@gmail.com,

Annotatsiya. *Ushbu maqolada tarmoq trafigini filtirlash orqali shubhali paketlarni aniqlash algoritmi ishlab chiqilgan. IP manzillarining oq va qora ro‘yxatlarining umumlashtirilgan sxemasi keltirilgan. Taklif qilinyotgan fishing hujumlarini aniqlash algoritmining blok sxemasi qanday vazifalarni bajarishi va qanday natijaga olib kelishi keltirilgan. Tadqiqot natijalariga ko‘ra Fishingni aniqlash algoritmi qaror qabul qilish uchun giperhavolalar xususiyatlarini tahlil qiladi. Taklif etilgan algoritm va struktura qurilgan bosqichlarni amalga oshirish hisobida giperhavola funksiyalaridan foydalanib veb-sahifaning qonuniyligini tekshirish imkon beradi.*

Kalit so‘zlar: *Paketlar, qora yo‘yxat, oq ro‘yxat, tarmoq traffigi, MAC, IP, fishing, URL, DNS.*

1. KIRISH

Shubhali paketlarni kuzatish ro‘yxatlari tarmoqdagi turli tahdidlar va zararli harakatlar haqidagi ma’lumotlarni o‘z ichiga olgan maxsus ma’lumotlar bazalaridir. Ushbu ro‘yxatlar muntazam ravishda yangilanadi va yangi ma’lum tahdidlar, zararli IP manzillar, domenlar, fayl xeshlari va zararli faoliyatning boshqa xususiyatlari to‘g‘risidagi ma’lumotlarni o‘z ichiga oladi. Ular zamonaviy kibertahdidlar haqida qimmatli ma’lumotlarni taqdim etadi va tashkilotlarga ehtiyot choralarini ko‘rishda va har xil turdagi hujumlarga qarshi turishda yordam beradi.

Shubhali paketlarni kuzatish ro‘yxati ikkiga bo‘linadi: qora va oq ro‘yxatlar.

2. QORA RO‘YXAT

Qora ro‘yxatda ma’lum bo‘lgan zararli IP manzillar, domenlar, URL manzillar va kiberhujumlar bilan bog‘liq bo‘lgan boshqa tarmoq xususiyatlari mavjud.

Qora ro‘yhat to‘plami. A to‘plam nazorat qilmoqchi bo‘lgan zararli yoki keraksiz elementlar ro‘yxati hisoblanadi. To‘plamdagi elementlar sifatida xeshlar yoki noyob identifikatorlar ko‘rsatilishi mumkin.

Universal to‘plam. U universal to‘plami tarmoq yoki qora ro‘yxat ishlayotgan muhitda mavjud bo‘lishi mumkin bo‘lgan barcha mumkin bo‘lgan elementlarni ifodalaydi. Ushbu to‘plam barcha mumkin bo‘lgan IP manzillarni, domen nomlarini, xeshlarni va boshqalarni o‘z ichiga oladi.

Mansublikni tekshirish. Element qora ro‘yxatning bir qismi yoki yo‘qligini aniqlash uchun mansublik testi operatsiyasidan foydalaniladi. Misol uchun, x elementi berilgan bo‘lsa, u qora ro‘yxat to‘plamiga ($x \in A$) yoki qora ro‘yxat to‘plamining to‘ldiruvchisiga ($x \notin A$) tegishli ekanligini tekshirish mumkin bo‘ladi.

Qora ro‘yxatni yangilash. Qora ro‘yxatni yangilash A to‘plamiga yangi elementlarni qo‘shishni (masalan, yangi tahdidlar aniqlanganda) va A to‘plamidan elementlarni olib tashlashni (masalan, tahdid muvaffaqiyatli zararsizlantirilgandan yoki ahamiyatsiz bo‘lganidan keyin) o‘z ichiga oladi.

To‘plamlar ustida amallar. To‘plam operatsiyalari birlashma ($A \cup B$), kesishish ($A \cap B$) va farq ($A \backslash B$) kabi standart to‘plam amallarini o‘z ichiga oladi, bu yerda $B -$ boshqa elementlar to‘plamidir.

Mantiqiy ifodalar. Mantiqiy ifodalar murakkab shartlarni aniqlash uchun mantiqiy operatsiyalardan foydalanadi. Misol uchun, element qora ro‘yxatning bir qismi ekanligini va ma’lum bir tahdid toifasiga tegishli ekanligini tekshiradigan ifoda yaratish mumkin (misol, «$x \in A\ AND\ category(x) ='$ zararli dastur′»)).

3. OQ RO‘YXAT

Oq ro‘yxatda ishonchli IP manzillar, domenlar, URL manzillar va boshqa xususiyatlar mavjud. Ular ishonchli trafik manbalarini yaratishga yordam beradi va ma’lum yaxshi resurslarning oq ro‘yxatini taqdim etadi.

Oq ro‘yxat to‘plami (S). (S) to‘plami ishonchli yoki ruxsat etilgan elementlarning ro‘yxati. Bular IP manzillar, domen nomlari, xeshlar yoki ishonchli deb hisoblangan boshqa xususiyatlar bo‘lishi mumkin.

Universal to‘plam. U universal to‘plami oq ro‘yxat ishlaydigan tarmoq yoki muhitda mavjud bo‘lishi mumkin bo‘lgan barcha mumkin bo‘lgan elementlarni ifodalaydi. Ushbu to‘plam barcha mumkin bo‘lgan IP manzillarni, domen nomlarini, xeshlarni va boshqalarni o‘z ichiga oladi.

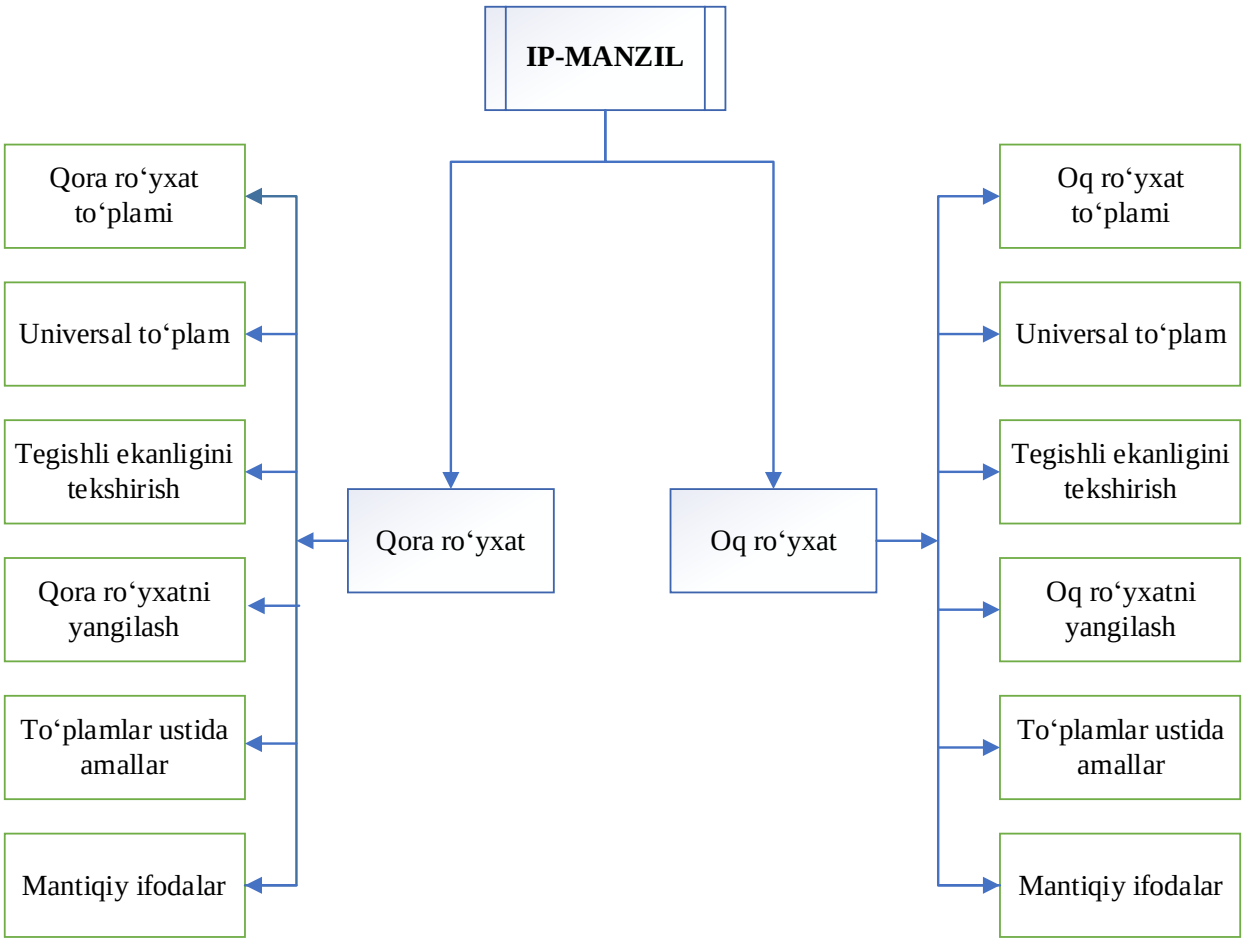
Mansublikni tekshirish. Element oq ro‘yxatning bir qismi yoki yo‘qligini aniqlash uchun mansublik testi operatsiyasidan foydalanishimiz mumkin. Masalan, x elementi berilgan bo‘lsa, u oq ro‘yxat to‘plamiga ($x \in K$) yoki oq ro‘yxat to‘plamining to‘ldiruvchisiga ($x \notin K$) tegishli ekanligini tekshirish mumkin.

Oq ro‘yxatni yangilash. Oq ro‘yxatni yangilash K to‘plamiga yangi elementlarni qo‘shishni (masalan, yangi ishonchli resurslarni qo‘shganda) va K to‘plamidan elementlarni olib tashlashni (masalan, agar resurs endi ishonchli bo‘lmasa) o‘z ichiga oladi.

To‘plamlar ustida amallar. To‘plam operatsiyalari birlashma ($K \cup D$), kesishish ($K \cap D$) va farq ($K \backslash D$) kabi standart to‘plam amallarini o‘z ichiga oladi, bu yerda $D -$ boshqa elementlar to‘plamidir.

Mantiqiy ifodalar. Mantiqiy ifodalar murakkab vaziyatlarni aniqlashda ishlatiladi. Misol uchun, element oq ro‘yxatning bir qismi ekanligini va ma’lum bir ishonchli manba toifasiga tegishli ekanligini tekshiradigan ifoda yaratish mumkin (misol, «$x \in W\ AND\ category(x) = 'ishonchli'$»).

1-rasmda IP manzillarining oq va qora ro‘yxatlarining umumlashtirilgan sxemasi taqdim etilgan.



1-rasm. IP manzillarining oq va qora ro‘yxatlarining umumlashtirilgan sxemasi

Quyida tarmoq trafigidagi shubhali paketlarni kuzatishning strukturasi taklif etiladi. Shubhali paketlarni kuzatish strukturasi quyidagi bosqichlardan iborat:

4. YUMSHATISH BOSQICHI

Yumshatish bosqichi quyida keltirilgan beshta jadvaldan iborat.

1. Qora ro‘yxat jadvali buzg‘unchining MAC manzilini bloklaydi.

2. Oq ro‘yxat jadvali paketning manba MAC manzilini tekshiradi. Agar mos yozuv bo‘lsa, paket yo‘naltiriladi. Aks holda, SYN paketi tekshirish-sinxronlash jadvaliga joylashtiriladi, ACK paketi tekshirishni tasdiqlash jadvaliga joylashtiriladi va paketning qolgan qismi o‘chiriladi.

3. Yo‘naltirish jadvali paketlarni tegishli chiqish portiga yo‘naltiradi.

4. Sinxronizatsiyani tekshirish jadvali agar paket 256 ta yozuvdan biriga mos

kelsa, SYN va ACK paketlari sinxronlashtiriladi va buzgg‘unchi aniqlanadi.

5. Tasdiqlash jadvali paketning ACK raqamini tekshiradi. Agar ACK raqami to‘g‘ri bo‘lsa, buzg‘unchi aniqlangan hisoblanadi. Aks holda, paket tashlab yuboriladi.

5. ANIQLASH BOSQICHI

Registrlarda qiymatlarni saqlash uchun xesh-jadval va jadvaldagi slotda esa kalit va qiymat mavjud. Kalit ikkita maydonni saqlaydi: IP va MAC manzillar, qiymat esa hisoblagichni saqlaydi. Aniqlash bosqichi ikkita asosiy harakatni amalga oshirish moduliga bo‘linadi: Slotga qo‘shish va slotni tozalash modullari.

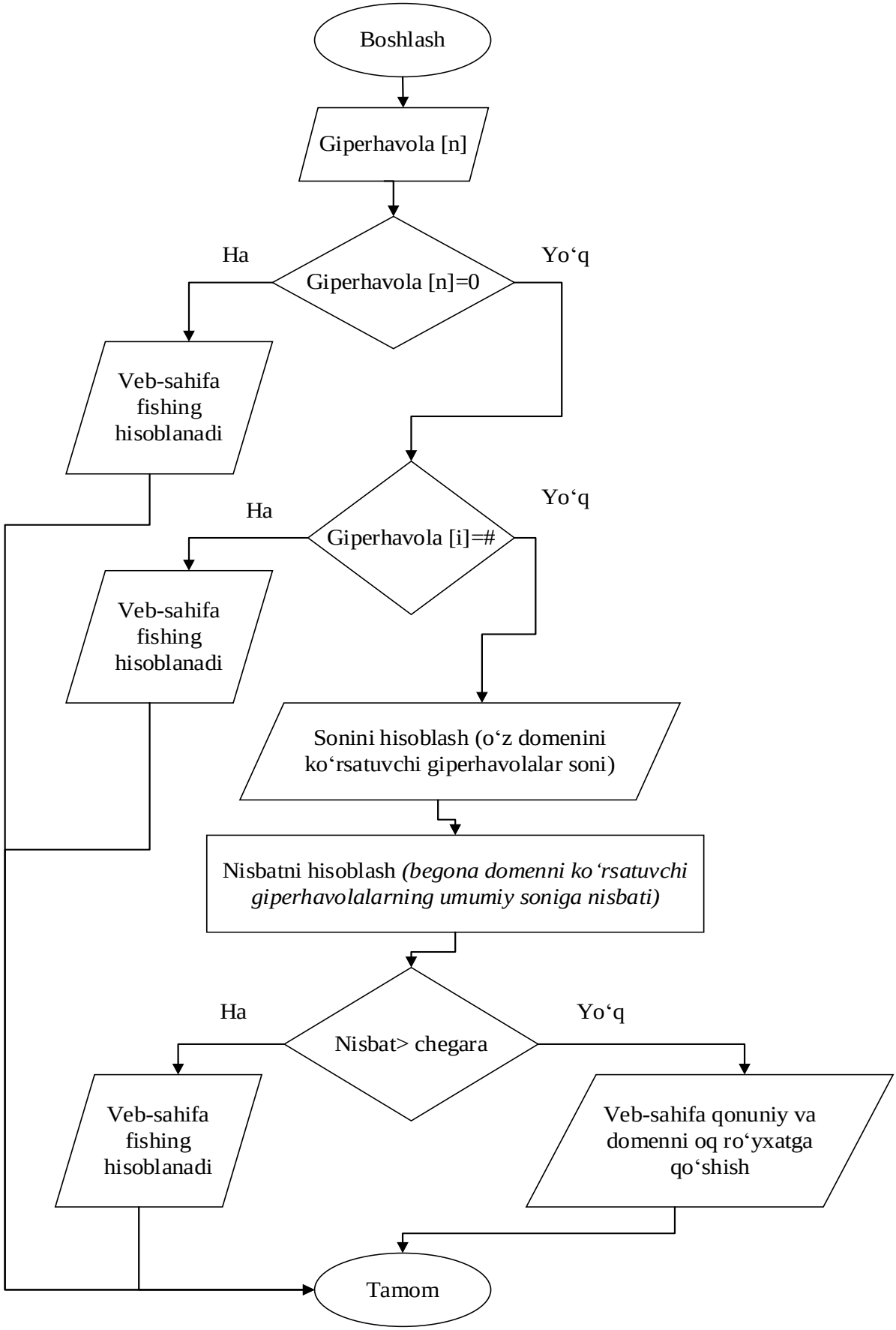
Slotga qo‘shish moduli. Kalit sifatida paketning manba IP va MAC manzillaridan foydalanib, k indeksga mos keladigan k ni olish uchun turli xesh-funksiyalar yordamida hisoblab chiqiladi. Agar kalit xesh-jadvalda mavjud bo‘lmasa, k sloti bo‘sh slot mavjudligini tekshiradi, agar bo‘sh slot bo‘lmasa, paket mijozga qaytariladi; aks holda kalit (manba IP manzili, manzil MAC manzili) saqlanadi va kalit hamda hisoblagich 1 ga o‘rnatiladi. Bundan tashqari, agar kalit xesh-jadvalda mavjud bo‘lsa, hisoblagich 1 ga oshiriladi va hisoblagich T chegarasidan oshib ketganligi tekshiriladi. Chegara T ulanishining buzilishiga ruxsat berilganligini bildiradi. Agar hisoblagich chegaradan oshib ketgan bo‘lsa, kommutator kontrollerga xulosa ma’lumotlarini yuboradi va keyin kontroller kalitning MAC manzilini qora ro‘yxat jadvaliga qo‘shadi.

Slotni tozalash moduli. Slotni tozalash bosqichi kirish elementi kaliti yordamida kirish mumkin bo‘lgan k slotlar sonini oladi. Keyin u kalit xesh-jadvalida mavjudligini tekshiradi.

5. FISHING HUJUMLARINI ANIQLASH BOSQICHI

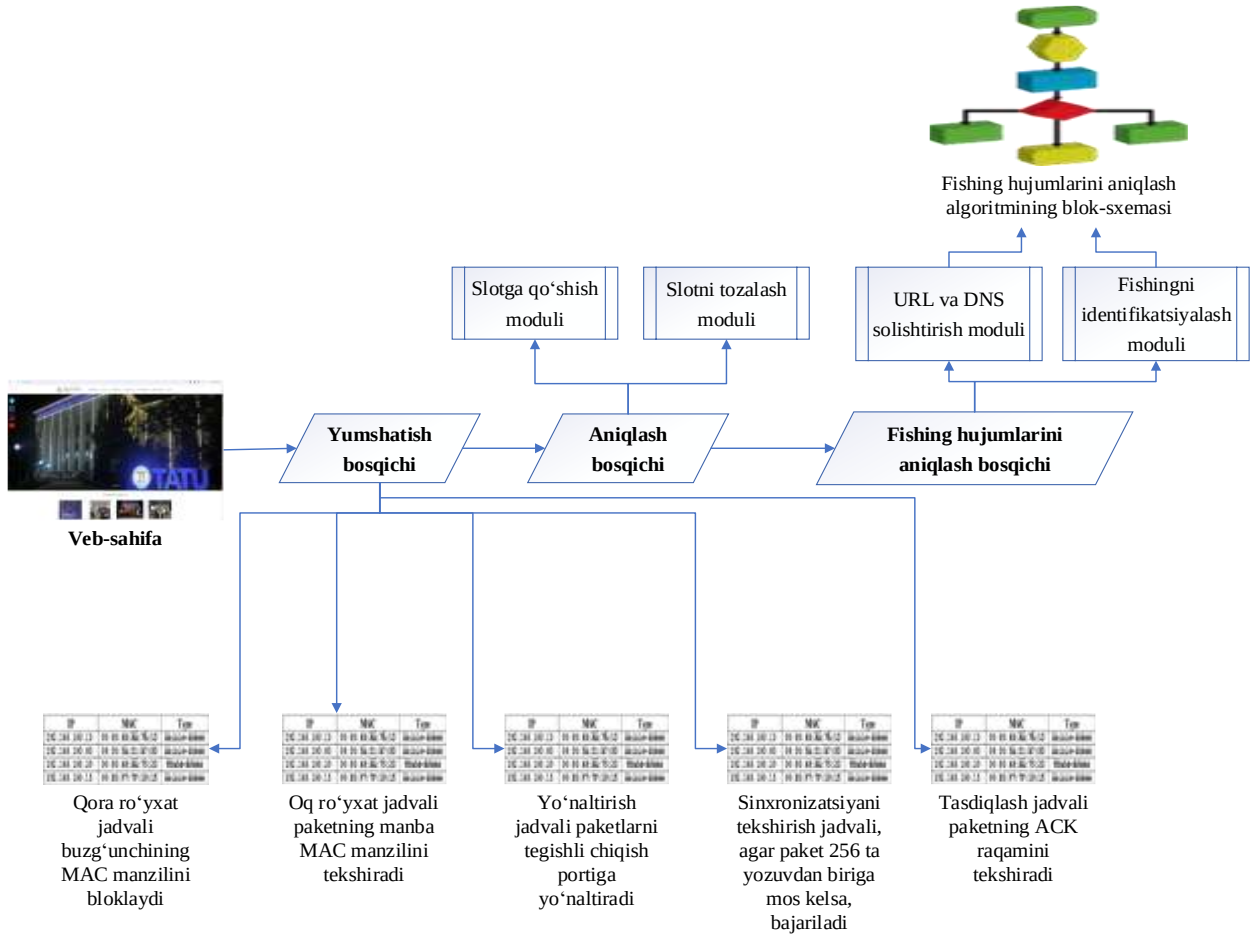
Fishing hujumini aniqlash bosqichi ikkita modulga bo‘lingan. Birinchi modul URL va DNS solishtirish moduli bo‘lib, unda ish vaqtini oshirish va yolg‘on xabarlarni kamaytirish uchun foydalaniladigan oq ro‘yxat mavjud. 2-rasmda fishing hujumlarini aniqlash algoritmining blok sxemasi taklif etilgan.

Oq ro‘yxat ikkita parametrni qo‘llab-quvvatlaydi: domen nomi va mos keladigan IP manzil. Har safar foydalanuvchi veb-saytga kirganda, tizim joriy veb-saytning domen nomi bilan oq ro‘yxatga mos kelishini tekshiradi. Agar joriy veb-sayt domeni oq ro‘yxatga mos kelsa, tizim qaror qabul qilish uchun IP manzilni moslashtiradi. Agar foydalanuvchi oq ro‘yxatga kiritilgan veb-saytga kirsa, DNS poisoning hujumini tekshirish uchun tegishli domenning IP manzilini moslashtiradi. Oq ro‘yxat noldan boshlanadi. Bu shuni anglatadiki, dastlab ro‘yxatda hech qanday domen bo‘lmaydi va foydalanuvchi yangi veb-sahifalarga kirishi bilanoq oq ro‘yxat o‘sish tartibida to‘ldirilishni boshlaydi. 3-rasmda tarmoq trafigida shubhali paketlarni kuzatish strukturasi taklif qilingan. Oq ro‘yxat ikkita parametrni qo‘llab-quvvatlaydi: domen nomi va mos keladigan IP manzil. Har safar foydalanuvchi veb-saytga kirganda, tizim joriy veb-saytning domen nomi bilan oq ro‘yxatga mos



2-rasm. Fishing hujumlarini aniqlash algoritmining blok sxemasi

kelishini tekshiradi. Agar joriy veb-sayt domeni oq ro‘yxatga mos kelsa, tizim qaror qabul qilish uchun IP manzilni moslashtiradi. Agar foydalanuvchi oq ro‘yxatga kiritilgan veb-saytga kirsa, DNS poisoning hujumini tekshirish uchun tegishli domenning IP manzilini moslashtiradi. Oq ro‘yxat noldan boshlanadi. Bu shuni anglatadiki, dastlab ro‘yxatda hech qanday domen bo‘lmaydi va foydalanuvchi yangi veb-sahifalarga kirishi bilanoq oq ro‘yxat o‘sish tartibida to‘ldirilishni boshlaydi. 3-rasmda tarmoq trafigida shubhali paketlarni kuzatish strukturasi taklif qilingan.



3-rasm. Tarmoq trafigida shubhali paketlarni kuzatish strukturasi

Foydalanuvchi veb-saytga kirganida, ikkita imkoniyat mavjud: yoki foydalanuvchi veb-saytga birinchi marta kirayapti yoki u allaqachon veb-saytga kirib bo‘lgan. Agar foydalanuvchi saytga birinchi marta kirsa, sayt domeni oq ro‘yxatda bo‘lmaydi. Bunday holda ikkinchi modul ishlashni boshlaydi, Fishingni identifikatsiyalash moduli veb-sahifaning fishing ekanligini tekshiradi va veb-sahifadan giperhavolalarni qabul qiladi va giperhavolalarni fishingni aniqlash algoritmiga yo‘naltiradi. Fishingni aniqlash algoritmi qaror qabul qilish uchun giperhavolalar xususiyatlarini tahlil qiladi. Qonuniyligini tekshirgandan so‘ng, agar sayt fishing bo‘lsa, tizim foydalanuvchini ogohlantiradi. Bundan tashqari, agar sayt qonuniy bo‘lsa, tizim oq ro‘yxatdagi domenni yangilashga imkon beradi.

7. XULOSA

Tarmoq trafigidagi shubhali paketlarni aniqlash bo‘yicha taklif etilgan algoritm va struktura qurilgan bosqichlarni amalga oshirish hisobida giperhavola funksiyalaridan foydalanib veb-sahifaning qonuniyligini tekshirish va domenlarni soxta fishing hujumlardan, hamda onlayn tahdidlar va nol hujumlardan himoya qilishga imkon beradi.

ADABIYOTLAR

1. M. Snehi and A. Bhandari, “Vulnerability retrospection of security solutions for software-defined cyber-physical system against DDoS and IoT-DDoS attacks,” Comput. Sci. Rev., vol. 40, 2021, Art. no. 100371.
2. G‘ulomov Sh.R. Veb-hujumlardan trafikni veb-filtrlash arxitekturasi. Multidisciplinary Scientific Journal. September, 2023, 229-239 стр.
3. K. Chen et al., “SDNShield: NFV-based defense framework against DdoS attacks on SDN control plane,” IEEE/ACM Trans. Netw., vol. 30, no. 1, pp. 1–17, Feb. 2022.
4. Gulomov Sherzod Rajaboevich, Mirzaeva Malika Bakhadirovna, Iminov Abdurasul Abdulatipovich. Port-Knocking Method for Enhancing Network Security. 2022 International Conference on Information Science and Communications Technologies (ICISCT) | 978-1-6654-7229-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICISCT55600.2022.10146918
5. R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, S. Garg, and M. M. Hassan, “A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network,” J. Parallel Distrib. Comput., vol. 164, pp. 55–68, 2022.
6. Gulomov Sherzod Rajaboevich, Abdurakhmonov Abduaziz Abdugafforovich, Azizova Zarina Ildarovna. Development a Model of a Network Attack Detection in Information and Communication Systems. Journal of Advances in Information Technology Vol. 13, No. 4, August 2022 (Scopus indexed), P: 312-319
7. J. Gardiner, A. Eiffert, P. Garraghan, N. J. P. Race, S. Nagaraja, and A. Rashid, “Controller-in-the-middle: Attacks on software defined networks in industrial control systems,” in Proc. 2th Workshop CPSIoT Secur. Privacy, 2021, pp. 63–68.
8. Гуломов Ш.Р., Насруллаев Н.Б., Абдурахмонов А.А., Азизова З.И. Оценка и применение алгоритмов машинного обучения для систем обнаружения и предотварешение вторжений. Муҳаммад ал-Хоразмий авлодлари илмий-амалий ва ахборот-таҳлилий журнал. № 4 (14), декабр 2020 й. Б.21-27
9. V. Tolpegin, S. Truex, M. E. Gursoy, and L. Liu, “Data poisoning attacks against federated learning systems,” in Proc. Eur. Symp. Res. Comput. Secur., 2020, pp. 480–501.