ISSN: 2181-3906 2025

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 4 / ISSUE 4 / UIF:8.2 / MODERNSCIENCE.UZ

TARMOQ HUJUMLARINI ANIQLASH VA HIMOYALASHDA HOZIRDAKENG QO‘LLANILAYOTGAN VOSITALARNING ISHLASH STRUKTURASI HAMDA ALGORETIMLARI

Alimardon Axmedov Muhiddin o'g'li
University of Management and Future Technologies
Telekommunikatsiya injiniringi magistranti.

https://doi.org/10.5281/zenodo.15280797

Annotatsiya. *Ushbu maqolada O‘zbekiston Respublikasidagi davlat tashkilot va korxonalarida kiberxavfsizlikni ta’minlashda erishiladigan natijalarni tahlil qilish ko‘zda tutilgan. Bunda zamonaviy telekommunikatsiya tarmoqlari va axborot tizimlari orqali uzatiladigan xizmatlari uzluksizligini hamda ularning kiberxavfsizligini ta’minlash maqsadida eng zamonaviy yechimlar tahlil qilingan.*

Tadqiqot davomida davlat tashkilot va korxonalarida telekommunikatsiya infrastrukturasi apparat, dasturiy va apparatli-dasturiy vositalari xavfsizligini ta’minlash uchun axborot tizimining zamonaviy vositalar, funksional va tuzilmaviy ta’minotini monitoring qilishgacha bo‘lgan jarayonlar e’tiborga olingan.

Kalit so‘zlar: *telekommunikatsiya, tarmoq, aloqa, monitoring, server, xosting, tizim, dasturiy ta’minot, axborot tizimi, kiberxavfsizlik, kibertahdid, avtomatlashtirish, tizim samaradorligi, dasturiy vositalar, komplekslashgan axborot tizimi, Snort, Suricata.*

СТРУКТУРА РАБОТЫ И АЛГОРИТМЫ ШИРОКО ИСПОЛЬЗУЕМЫХ В НАСТОЯЩЕЕ ВРЕМЯ ИНСТРУМЕНТОВ ОБНАРУЖЕНИЯ И ЗАЩИТЫ ОТ СЕТЕВЫХ АТАК

Аннотация. *В данной статье предусмотрен анализ результатов, достигнутых при обеспечении кибербезопасности в государственных организациях и предприятиях Республики Узбекистан. При этом были проанализированы самые современные решения для обеспечения непрерывности услуг, передаваемых через современные телекоммуникационные сети и информационные системы, а также их кибербезопасности.*

В ходе исследования были рассмотрены процессы, начиная от мониторинга современного инструментального, функционального и структурного обеспечения информационной системы для обеспечения безопасности аппаратных, программных и

аппаратно-программных средств телекоммуникационной инфраструктуры в государственных организациях и на предприятиях.

Ключевые слова: *Телекоммуникации, сеть, связь, мониторинг, сервер, хостинг, система, программное обеспечение, информационная система, кибербезопасность, киберугрозы, автоматизация, эффективность системы, программные средства, комплексная информационная система, Snort, Suricata.*

THE WORKING STRUCTURE AND ALGORITHMS OF THE TOOLS CURRENTLY USED IN THE DETECTION AND PROTECTION OF NETWORK ATTACKS

Abstract. *This article provides for the analysis of the results achieved in the provision of cybersecurity in state organizations and enterprises of the Republic of Uzbekistan. In this case, the most modern solutions have been analyzed in order to ensure the continuity of services transmitted through modern telecommunication networks and information systems, as well as their cybersecurity.*

In the course of the study, the processes of telecommunication infrastructure in state organizations and enterprises, up to the monitoring of modern tools, functional and structural support of the information system, to ensure the safety of hardware, software and hardware-software tools, were taken into account.

Keywords: *telecommunications, network, communication, monitoring, server, hosting, System, Software, Information System, cyber security, cyberspace, automation, system efficiency, software tools, integrated information system, Snort, Suricata.*

Snort - bu ochiq manba asosida yaratilgan Intrusion Detection System (IDS) va Intrusion Prevention System (IPS) bo‘lib, tarmoqda kiberhujumlarni aniqlash va oldini olish uchun ishlatiladi.

Snort tarmoq trafikini real vaqtda monitoring qilish, tahdidlarni aniqlash va ogohlantirishlar yuborish imkonini beradi.

Martin Roesch tomonidan 1998-yilda ishlab chiqilgan va hozirgi kunda Cisco Systems tomonidan qo‘llab-quvvatlanadi.

Snortning emblemasi - bu cho‘chqaning chizilgan ko‘rinishi.

Emblema odatda cho‘chqa burnidan havoni kuch bilan chiqarib turgan holda tasvirlangan bo‘lib, bu uning “hiddan aniqlash” va “skanerlash” imkoniyatlarini ramziy qilib ko‘rsatadi.

Cho‘chqa bu yerda Snortning “hidsoluvchi” vazifasini ifodalaydi, ya’ni u tarmoqdagi zararli trafik yoki hujumlarni topish uchun trafigni kuzatadi.

Snort tarmoq trafikini real vaqtda kuzatadi.

Anomaliyalar va imzo asosida tahdidlarni aniqlaydi.

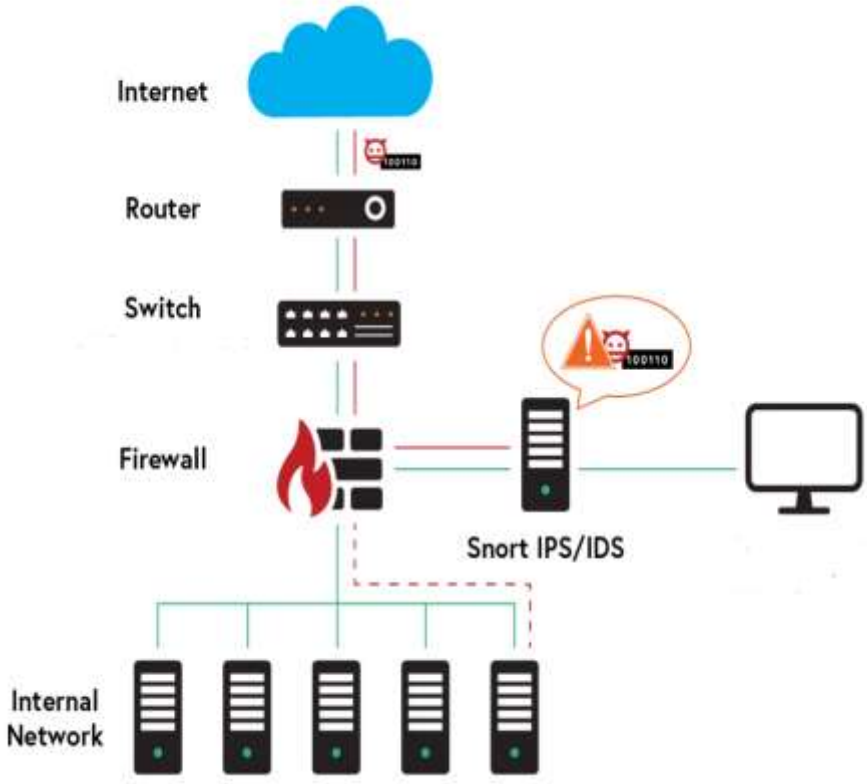
Foydalanuvchilar o‘z ehtiyojlariga mos ravishda qoidalarni yaratishi va yangilashi imkonyati.

Kiber tahdid aniqlanganda tizim administratorlariga ogohlantirish yuboradi.

Snort dastlab 2003 yilda IDS funksiyalari bilan chiqarilgan va hozirda eng ommabop IDS/IPS tizimlaridan biri hisoblanadi.

Snort millionlab foydalanuvchilar tomonidan qo‘llanilib, keng ko‘lamli xavfsizlik tahlillari va himoya choralarini ta’minlaydi.

Hujumlar va xavfsizlik hodisalari haqidagi malumotlar qaytdlarni amalga oshiradi.



1.1-rasm. Snortni real tarmoqda ishlatish sxemasi (na’muna)

Snortning asosiy funktsiyalari:

Trafikni kuzatish va tahlil qilish: Snort tarmoq orqali o‘tuvchi paketlarni tahlil qiladi va ular ichida g‘ayritabiiy yoki zararli faoliyatni aniqlaydi.

Bu signatura asosidagi qoidalar yordamida amalga oshiriladi.

Snortning asosiy versiyasi ochiq manbali bo‘lsa-da, Cisco kompaniyasi tomonidan qo‘llab-quvvatlanadigan tijorat versiyalari ham mavjud.

Cisconing Firepower platformasi, bu Snortni o‘z ichiga olgan holda tarmoq xavfsizligi yechimlarini taqdim etadi.

1.2-rasmda snortning ishlash arxitekturasi - bu tarmoq xavfsizligini ta’minlash uchun yaratilgan ochiq manba asosidagi intruzion aniqlash tizimi (IDS) va intruzion oldini olish tizimi (IPS)ning tarkibiy qismlarini va ularning o‘zaro aloqalarini ifodalaydi.

Snortning ishlash arxitekturasi quyidagi asosiy komponentlardan iborat:

Paketni ushlash moduli: Snort, libpcap yoki winpcap kutubxonalaridan foydalangan holda tarmoq paketlarini ushlaydi.

Bu modul real vaqt rejimida tarmoq trafikini to‘playdi va tahlil qiladi.

Dekoder: Ushbu komponent tarmoq paketlarini o'qiydi va ularni ko'proq tushunarli formatga o'tkazadi. Dekoder turli protokollarni, masalan, TCP, UDP, va ICMP ni tushunishga qodir.

Preprocessor*:* Ushbu modul paketlarni qo'shimcha tahlil qiladi va ularni tahdidlarni aniqlash uchun tayyorlaydi.

Preprocessor turli xil xususiyatlarni, masalan, protokolni normalizatsiya qilish, ma'lumotlarni siqish va boshqalarni qo'llaydi.

Aniqlash dvigateli*:* Bu Snortning eng muhim qismi bo'lib, o'qilgan va tayyorlangan ma'lumotlar asosida tahdidlarni aniqlash jarayonini amalga oshiradi.

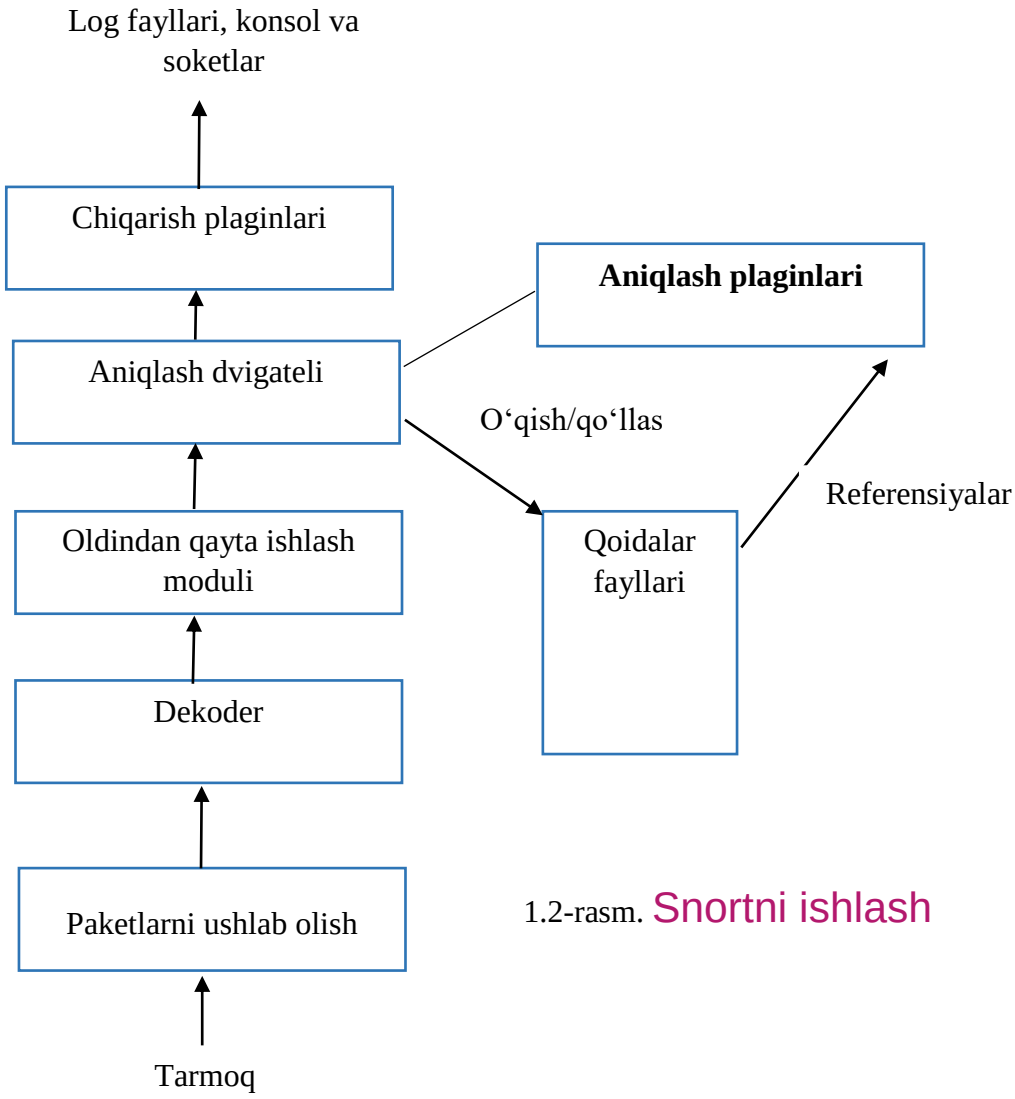
Bu yerda qoidalar fayllari yordamida shubhali xatti-harakatlar yoki trafik aniqlanadi.

Chiqish plaginlari*:* Ushbu komponentlar aniqlangan tahdidlar va ogohlantirishlar haqida ma'lumotlarni chiqazadi.

Chiqish plaginlari turli xil formatlarda, masalan, log fayllari, konsolga yoki tarmoq socketlariga chiqish imkoniyatini taqdim etadi.

ISSN: 2181-3906 2025

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 4 / ISSUE 4 / UIF:8.2 / MODERNSCIENCE.UZ



1.2-rasm. Snortni ishlash

Paketlarni chuqur tahlil qilish (Deep Packet Inspection): Snort nafaqat paketlarning header qismiga, balki ularning ma’lumotlar qismiga ham chuqur kirib boradi. Bu esa murakkab hujumlarni aniqlash imkonini beradi.

Qoida asosidagi tahlish: Snort turli qoidalarga asoslangan holda trafikni tahlil qiladi. Ushbu qoidalar tarmoqdagi zararlanish alomatlarini aniqlash uchun ishlatiladi. Masalan, qoidalar orqali ma’lum bir IP-manzilga ko‘p marta murojaat qilishni yoki ma’lum bir portga ma’lum trafikni aniqlaydi.

Qoidalarning asosiy formatlari:

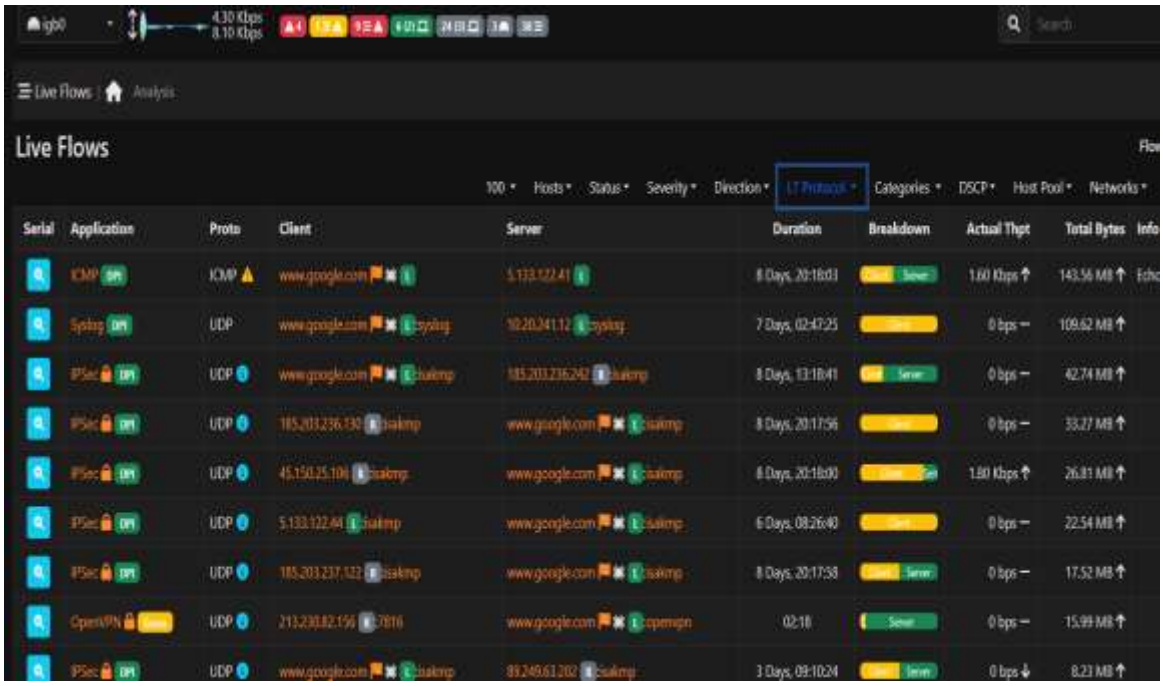
- Aloqa ma’lumotlari (IP manzillar va portlar);
- Harakatlar (alert, drop, log va boshqalar);

ISSN: 2181-3906 2025

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 4 / ISSUE 4 / UIF:8.2 / MODERNSCIENCE.UZ

- Shartlar (ma’lum protokollarga yoki paketlarning ma’lum xususiyatlariga asoslangan).

Deep Packet Inspection (DPI): Snort faqatgina paketlarning sarlavhasini emas, balki ularning ma’lu mot qismidagi kontentni ham chuqur tahlil qiladi.



1.3-rasm. Snort (Deep Packet Inspection) ishlash jarayoni

Bu texnologiya murakkab hujumlarni, masalan, shifrlangan trafikdagi zararli ma’lumotlarni aniqlash imkonini beradi.

Snort har bir trafik paketini protokollar bilan solishtiradi va signatura asosida tekshiradi.

Masalan, TCP, UDP, ICMP va boshqa protokollar bilan bog‘liq xatolar yoki hujumlar aniqlanadi.

Snort turli xil hujumlarni aniqlashda yordam beruvchi modullar bilan ham kengaytiriladi.

Masalan, preprocessor modullari yordamida tarmoqda aniq bir protokol yoki trafik turini tahlil qilishda yordam beradi.

Snortda qoidalar maxsus formatda yoziladi. Misol tariqasida Snort qoidasi shunday ko‘rinadi:

alert tcp any any -> 192.168.1.1 80 (msg:”HTTP traffic detected”; sid:100001;)

Bu qoida quyidagilarni anglatadi:

- alert - Bu qoidaga mos keladigan trafik aniqlanganda Snort ogohlantirish beradi.
- tcp - TCP protokolida ishlovchi trafik uchun qoida.

ISSN: 2181-3906 2025

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 4 / ISSUE 4 / UIF:8.2 / MODERNSCIENCE.UZ

- any any - Har qanday manzildan va portdan kelayotgan trafik.
- 192.168.1.1 80 - maqsadli manzil IP 192.168.1.1 va port 80 (odatda HTTP).
- msg: Bu qoidaga mos keladigan - trafik aniqlanganda qaysi xabar ko‘rsatilishi.
- sid - Bu qoidalarning unikal identifikatori.

Snortda qoidalar turli xil rule-setlar shaklida yig‘ilgan bo‘lib, ular tahdidlarni aniqlash uchun ishlatiladi:

Snort VRT (Vulnerability Research Team) qoidalari: Snortning asosiy qoidalari to‘plami.

Emerging Threats qoidalari: Bu to‘plam ochiq manbali bo‘lib, keng jamoa tomonidan qo‘shib boriladi.

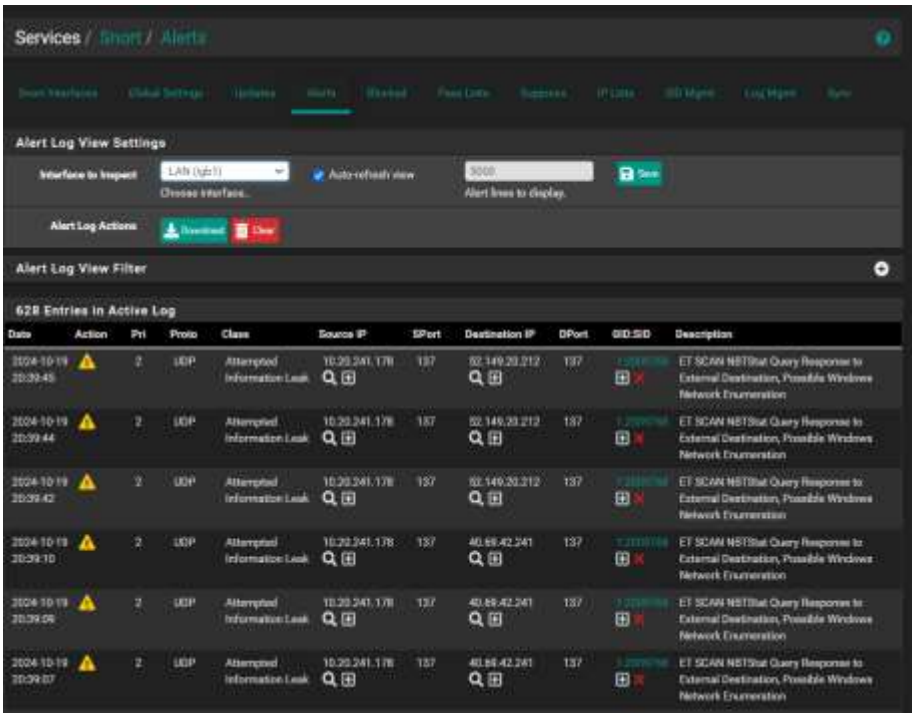
Uch rejimda ishlash imkoniyati:

Sniffer rejimi- tarmoqdan o‘tayotgan trafikni shunchaki o‘qib, konsolda aks ettiradi.

Paket yozuvchi rejim (Packet logger) - trafikni diskka yozib boradi, keyinchalik tahlil qilish uchun.

Hujumni aniqlash rejimi (Network Intrusion Detection): tarmoq trafigini real vaqt rejimida qoidalar bilan solishtirib, tahdidlarni aniqlaydi va ogohlantirishlar chiqaradi.

IDS va IPS rejimlarida ishlashi: IDS rejimida Snort faqat tarmoqda hujumlarni kuzatadi va ular haqida ogohlantiradi.

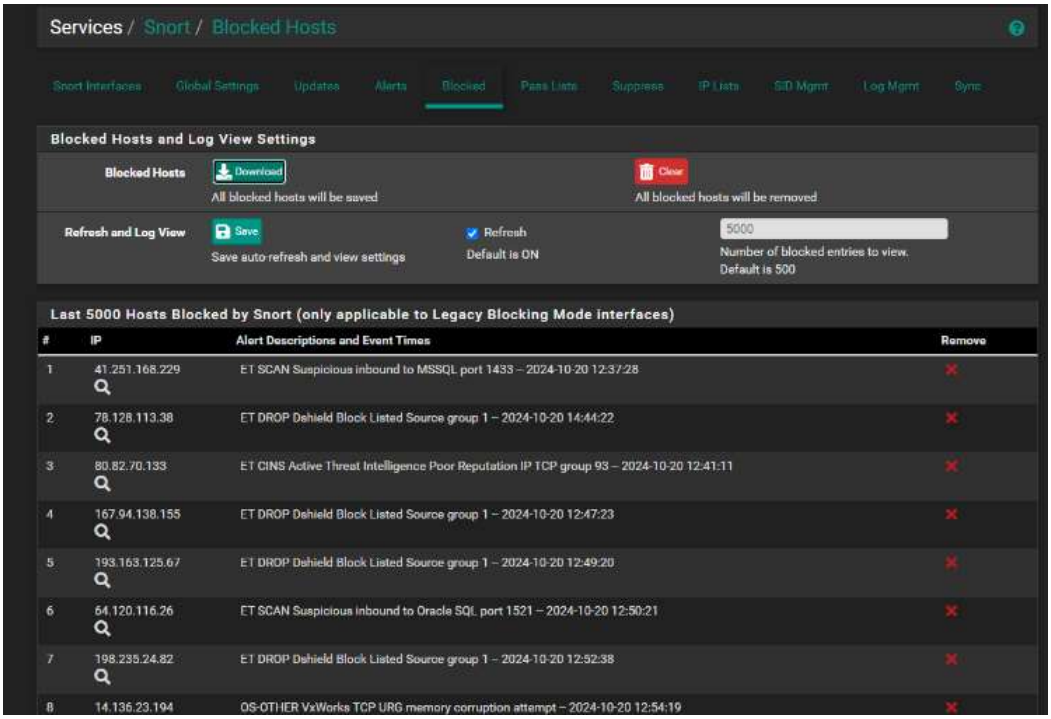


1.4- rasm. Snort kiber hujumlarni aniqlash jarayoni

ISSN: 2181-3906 2025

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 4 / ISSUE 4 / UIF:8.2 / MODERNSCIENCE.UZ

IPS rejimida esa Snort tarmoq orqali o‘tuvchi zararli trafikni to‘xtatish yoki bloklash imkoniyatiga ega.



1.5- rasm. Snort kiber hujumlarni bloklash jarayoni

Quyida Snortning ishlash algoritmlari va ular asosidagi matematik yondashuvlar:

Snortning birinchi vazifasi tarmoqdan kelayotgan paketlarni qabul qilish va ularni tahlil qilishdir. Snort har bir paketni TCP/IP stekiga muvofiq ravishda tahlil qiladi.

Matematik jihatdan bu jarayon:

Agar tarmoqdan kelsa, P_i paket quyidagicha yozilishi mumkin:

$$Pi=(H_i, D_i);$$

bu yerda:

H_i - paketning header (sarlavha) qismi,

D_i - paketning payload (ma’lumot qismi).

Snort ushbu bosqichda paketning $\{H_i\}$ qismidan manzil va protokol kabi asosiy ma’lumotlarni oladi.

Qoida asosidagi tahlil:

Snort qoidalar asosida paketlarni tahlil qiladi. Har bir qoidalar to‘plami quyidagicha bo‘ladi:

$$R_j=(M_j, Aj);$$

bu yerda:

M_j - qoidaning *match* qismi, ya'ni paketning qaysi qismlarini solishtirish kerakligi haqida shartlar,

A_j - qoidaga mos kelganda bajariladigan amallar (alert, drop, log va boshqalar).

Qoida mosligini tekshirish:

Paketni qabul qilgandan keyin, Snort paketning ba'zi qismlarini qoidalar bilan solishtiradi. Har bir qoidaga mos kelishi quyidagicha matematik ifoda bilan yoziladi:

$$\text{If } M_j(H_i, D_i) = \text{True then apply } A_j;$$

Bu yerda, *True* bo'lganda qoidaga mos keladi va natijada belgilangan amal bajariladi (masalan, ogohlantirish berish yoki paketni bloklash).

Paketlarni chuqur tahlil qilish (Deep Packet Inspection - DPI)

Snort faqatgina paketning header qismini emas, balki *payload* qismiga ham kirib, undagi ma'lumotlarni tahlil qiladi. Bu jarayon bir nechta bosqichlarga bo'linadi:

Signatura tekshiruvi: Paketning ma'lum bir signaturaga mosligini tekshirish.

Protokol tahlili: Paket protokol qoidalariga muvofiqligini tekshirish.

Matematik ifodasi:

Agar $\{S_k\}$ qoidalar to'plami bo'lsa, har bir paket uchun signatura tekshiruvi quyidagicha bo'ladi:

$$\text{If } D_i \in S_k \text{ then alert!;}$$

Bu yerda, D_i paketning payload qismi va S_k belgilangan signatura (zararli ma'lumotlar). Agar paket signaturaga mos kelsa, tizim ogohlantirish beradi.

Bu yerda, D_i paketning payload qismi va S_k belgilangan signatura (zararli ma'lumotlar). Agar paket signaturaga mos kelsa, tizim ogohlantirish beradi.

Trafikni normal tahlil qilish (anomaly detection)

Qo'shimcha mexanizmlar orqali Snort tarmoq trafigidagi anomal holatlarni ham aniqlaydi. Bu yondashuvda tarmoq trafigining odatdagi xulq-atvori kuzatilib, g'ayritabiiy o'zgarishlar qayd etiladi.

Matematik jihatdan:

Agar T tarmoq trafigining odatdagi statistikasini ifodalasa, har qanday anomaliya aniqlanishi uchun ushbu statistikadan farq qilishi kerak:

$$\text{If } |T_{normal} - T_{current}| > \epsilon \text{ then anomaly!;}$$

Bu yerda ϵ - aniqlik darajasini belgilovchi chegaraviy qiymat, Tnormal esa odatiy tarmoq trafigi. Agar joriy trafik odatdagidan farqli bo‘lsa, tizim anomaliyani qayd qiladi.

Qoida moslik qidirish algoritmi:

Snort o‘zining qoida bazasidan paketlarni moslashtirish uchun qidirish algoritmlaridan foydalanadi. Odatda Snort *AC (Aho-Corasick)* kabi qidirish algoritmlaridan foydalanadi. Bu algoritm qoidalardagi belgilarni tezkor qidirish uchun ishlatiladi.

Aho-Corasick algoritmi matnni belgilangan qoidalar bilan solishtirish uchun avtomat o‘rnatadi. Har bir qoidani tekshirish uchun algoritmda:

$$f(P)=\text{qoidalar bilan qidirilayotgan qism}$$

bu yerda, P paketning ma'lum qismi va algoritm paketni ma’lum signatura bilan solishtiradi.

Agar paket qoidaga mos kelsa yoki anomaliya aniqlansa, Snort quyidagi natijalardan birini amalga oshiradi:

Alert (Ogohlantirish): Hujum haqida ogohlantirish chiqarish.

Drop: Zararli trafikni bloklash yoki rad etish.

Matematik ifodasi:

$$\text{If } A_j \text{ is alert, then generate alert message;}$$

Snort ishlashida qoidalarga mos paketlarni qidirish, chuqur tahlil qilish va anomaliyalarni aniqlash matematik algoritmlar yordamida amalga oshiriladi. Ushbu algoritmlar tarmoq trafigini kuzatib borish va tahdidlarni aniqlash uchun asosiy yondashuv hisoblanadi.

Suricata - bu ochiq manba kodiga ega bo‘lgan tarmoq xavfsizligi tizimi bo‘lib, u tarmoq trafigini monitoring qilish, tahlil qilish va hujumlarga qarshi himoya qilish uchun ishlatiladi.

Suricata asosan IPS (Intrusion Prevention System) va IDS (Intrusion Detection System) funksiyalarini bajaradi va tarmoqda yuz berayotgan har qanday shubhali faoliyatni aniqlash va bloklashga qaratilgan.

Suricataning emblemasi - surikat (meerkat) hayvonining chizilgan tasviri bilan bog‘liq. Surikat, o‘zining qo‘riqlash va ogohlik fazilatlari bilan tanilgan kichik yirtqich hayvon bo‘lib, bu Suricata dasturining tarmoq xavfsizligini kuzatish va tahdidlarni tezda aniqlash qobiliyatini ramzi hisoblanadi.

Suricata emblemasida ko‘pincha surikat oldinga qaragan holda tik turgan tarzda tasvirlanadi, bu uning doimiy kuzatuvchanligini va xavfsizlikni ta’minlashda hushyorligini ifodalaydi.

Suricata 2010-yil 3-dekabrda ishlab chiqarilgan. Ushbu loyiha o‘zining birinchi versiyasi bo‘lgan Suricata 1.0 ni chiqarish bilan boshlandi.

Suricata dasturi Open Information Security Foundation (OISF) tomonidan ishlab chiqilgan, va uning maqsadi tarmoq xavfsizligi va hujumlarni aniqlash tizimlarini yangilash edi.

1.6-rasmda Suricataning mantiqiy ishlash algoritmi quyidagicha bosqichlardan iborat bo‘ladi:

***Boshlanish**:* Konfiguratsiya fayllarini o‘qish va buyruq qatoridagi variantlarni tahlil qilish orqali dastlabki sozlamalar amalga oshiriladi.

***Paketlarni paketlar havzasidan olish**:* Suricata tarmoqdan trafikni qabul qiladi va har bir paketni bosqichma-bosqich tahlil qilish uchun paketlar havzasiga joylashtiradi.

***Dekodlash**:* Paketning keyingi protokolini aniqlash uchun uni dekodlash bosqichi amalga oshiriladi. Bu qadamda paketning ichki protokol tuzilmalari ochiladi va yangilanadi.

Qoidalarni filtrlash va tekshirish: Qoidani ishga tushirishdan oldin, qoida filtrlanadi va ro‘yxatdan keyingi imzolar olinadi. Sarlavha mosligini tekshirish orqali qoidaga muvofiqligi baholanadi.

Aniqlash: Agar sarlavha mos kelsa, qoidaning qolgan qismini tekshirish davom ettiriladi. Boshqa imzolar mavjud bo‘lsa, ular bilan moslik tekshiriladi.

Natijalar va ichki tuzilmalarni ishga tushirish: Log fayllariga mos yozuvlar qo‘shilib, ichki tuzilmalar yangilanadi.

Ishchilar tizimlarini yaratish: Jarayonning so‘nggi bosqichida ishchi tizimlar yaratilib, uzluksiz ishlash uchun Suricata tizimi ishga tushadi.

Ushbu bosqichlar orqali Suricata tarmoqdagi tahdidlarni aniqlash va ularning oldini olishga qaratilgan jarayonni samarali amalga oshiradi.

Suricata turli protokollarni, jumladan, HTTP, FTP, SMTP, DNS va boshqalarni tahlil qiladi. Bu orqali tarmoq trafigini chuqur tahlil qilish imkonini beradi.

Suricata, tarmoqning tezligini oshirish va ko‘p foydalanuvchiga xizmat ko‘rsatish uchun ko‘p ip (multi-threading) texnologiyasidan foydalanadi.

IDS va IPS sifatida Suricata real vaqt rejimida hujumlarni aniqlash va ularni oldini olishga qodir.

***Dekodlash**:* Paketning keyingi protokolini aniqlash uchun uni dekodlash bosqichi amalga oshiriladi. Bu qadamda paketning ichki protokol tuzilmalari ochiladi va yangilanadi.

Qoidalarni filtrlash va tekshirish: Qoidani ishga tushirishdan oldin, qoida filtrlanadi va ro‘yxatdan keyingi imzolar olinadi. Sarlavha mosligini tekshirish orqali qoidaga muvofiqligi baholanadi.

Aniqlash: Agar sarlavha mos kelsa, qoidaning qolgan qismini tekshirish davom ettiriladi. Boshqa imzolar mavjud bo‘lsa, ular bilan moslik tekshiriladi.

Natijalar va ichki tuzilmalarni ishga tushirish: Log fayllariga mos yozuvlar qo‘shilib, ichki tuzilmalar yangilanadi.

Ishchilar tizimlarini yaratish: Jarayonning so‘nggi bosqichida ishchi tizimlar yaratilib, uzluksiz ishlash uchun Suricata tizimi ishga tushadi.

Ushbu bosqichlar orqali Suricata tarmoqdagi tahdidlarni aniqlash va ularning oldini olishga qaratilgan jarayonni samarali amalga oshiradi.

Suricata turli protokollarni, jumladan, HTTP, FTP, SMTP, DNS va boshqalarni tahlil qiladi. Bu orqali tarmoq trafigini chuqur tahlil qilish imkonini beradi.

Suricata, tarmoqning tezligini oshirish va ko‘p foydalanuvchiga xizmat ko‘rsatish uchun ko‘p ip (multi-threading) texnologiyasidan foydalanadi.

IDS va IPS sifatida Suricata real vaqt rejimida hujumlarni aniqlash va ularni oldini olishga qodir.

Suricata ochiq manba kodga ega, bu esa uni bepul ishlatish va moslash imkonini beradi.

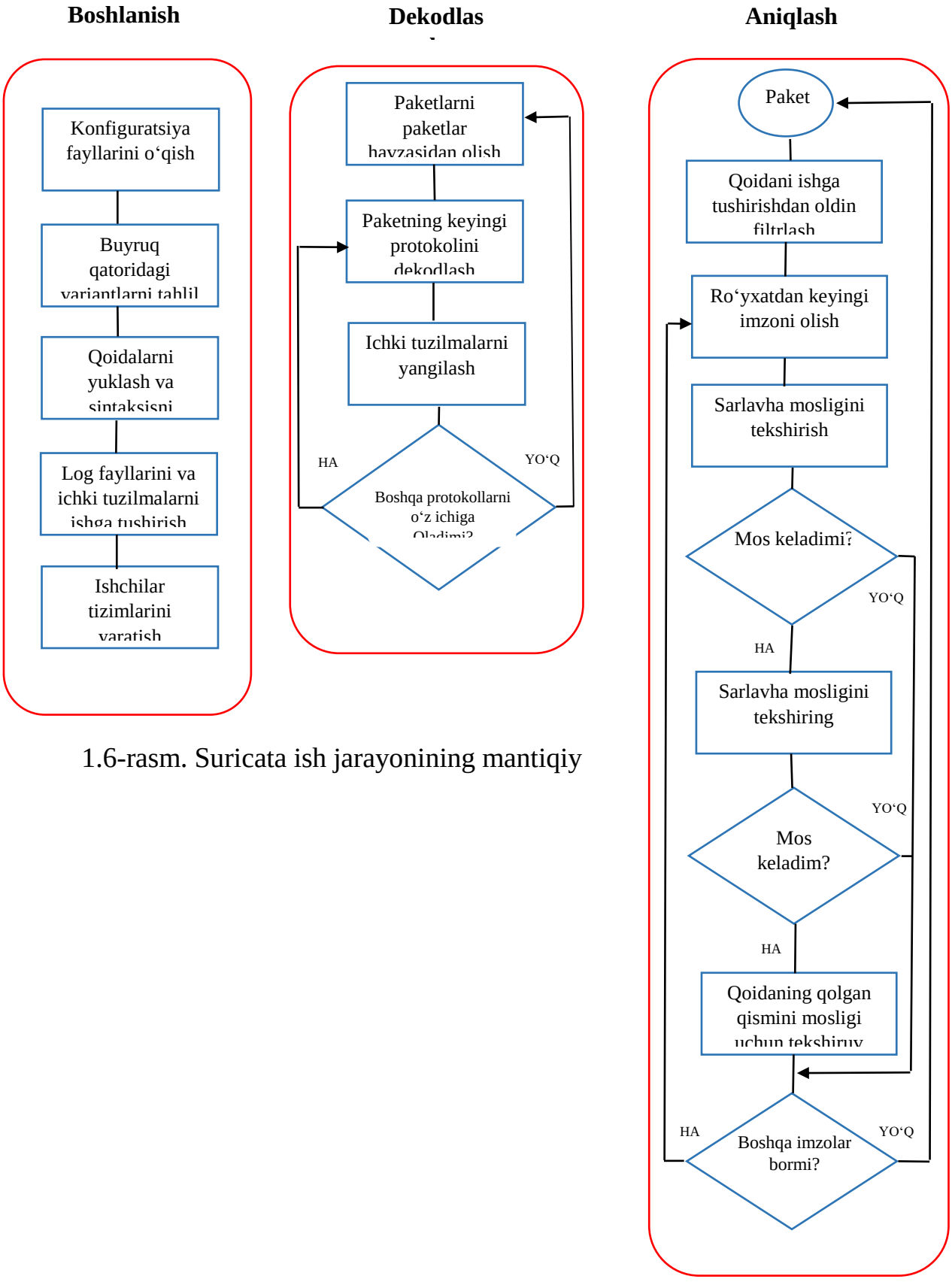
Dasturiy ta’minotni har qanday dasturchi yoki xavfsizlik mutaxassisi o‘z ehtiyojlariga mos ravishda o‘zgartirishi mumkin.

Suricata turli qo‘shimcha modullar bilan kengaytirilishi mumkin, masalan, Suricata-Update orqali qoidalar to‘plamini yangilash.

Suricata yuqori ish samaradorligi va katta hajmdagi tarmoq trafigini samarali ravishda tahlil qilish imkoniyatiga ega.

ISSN: 2181-3906 2025

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 4 / ISSUE 4 / UIF:8.2 / MODERNSCIENCE.UZ



1.6-rasm. Suricata ish jarayonining mantiqiy

Xulosa

Xulosa qilib shuni aytish mumkinki bugungi kunga kelib, nafaqat rivojlangan davlatlar qatorida O‘zbekiston ham to‘liq raqamli transformatsiya tizimini joriy etishni jadal sur’atlarda olib bormoqda. Shu bilan birga, zamonaviy telekommunikatsiya tarmoqlari xavfsizligini ta’minlashda birlamchi instrument hisoblangan monitoring qilish va markazlashgan holda boshqarishni ta’minlashga asoslangan tizim va dasturiy ta’minotlardan tashqari to‘g‘ridan-to‘g‘ri axborot va kiberxavfsizlikni ta’minlash vositalarini joriy qilish tizim xavfsizligi uchun asosiy omil bo‘lmoqda, lekin faqat shuning o‘zi yetarli emas deyish mumkin. Sabab esa bu elementlar asosida avtomatlashtirilgan va markazlashgan boshqaruv usuliga ega bo‘lgan tizimlarni joriy etishga qaratilgan chora-tadbirlarni jadallashtirilayotganligi quvonarlidir.

Zamonaviy telekommunikatsiya infratuzilmasi xafvsizligini ta’minlash maqsadida davlatning butun tarmoq infratuzilmalarini qamrab olgan yagona va markazlashgan Axborot xavfsizlik monitoring markazini joriy qilinishi telekommunikatsiya infratuzilmasi ish salohiyatini oshiribgina qolmasdan, axborot va kiberxavfsizlik talablari asosida ishlashigi ta’minlanishi olib borilgan tahlil natijalarida ham yaqqol ko‘rinish berdi. Bu yesa o‘z navbatida O‘zbekistorn Respublikasida axborot va kiberxavfsizlik salohiyatini yanada oshirish uchun bosilgan ulkan qadam bo‘ladi.

REFERENCES

1. “Security Operation Center: Building, Operating and Maintaining Your SOC” by Joseph Muniz, Gary McIntyre and Nadhem AlFardan – 2015 year.
2. “The Cybersecurity Playbook: How Every Leader and Employee Can Contribute to a Culture of Security” by Allison Cerra – 2019 year.
3. “A Taxonomy of Cyber Attacks on Machine Learning Systems” by Battista Biggio and Fabio Roli – 2018 year.
4. “A Survey on Security Information and Event Management (SIEM) Systems” by A. Khraisat et al. – 2019 year.
5. “NIST Special Publication 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations” – 2011 year.