AXBOROT-KOMMUNIKATSIYA TIZIMLARIDA SHUBHALI TARMOQ PAKETLARINI ANIQLASH VA BARTARAF ETISH ALGORITMINI ISHLAB CHIQISH.

Ilmiy rahbar: ***Karimova Iqbol Madaminovna***

Talabasi: ***Jetpisbayev Abdumalik Asqar o‘g‘li***

ABU RAYHON BERUNIY NOMIDAGI URGANCH DAVLAT UNIVERSITETI, Axborot xavsizligi kafedrasi, “Axborot xavsizligi (sohalar bo‘yicha)” ta’lim yo‘nalishi

Email:abdujetpis@gmail.com

Annotatsiya

Maqolada axborot-kommunikatsiya tizimlarida tarmoq hujumlarini real vaqtda aniqlash va zararsizlantirish muammosi ko'rib chiqiladi. Imzo taqqoslash va statistik anomaliya usullarini birlashtirgan gibrid yondashuv taklif etiladi. Paket sarlavhasi parametrlari, oqim statistikasi hamda Shannon entropiyasi asosidagi shubhalilik balli (SS) tizimi ishlab chiqilgan. Nazariy baholash natijalariga ko'ra, algoritm o'rtacha TPR=93,6%, FPR=1,7% ko'rsatkichlariga erishadi.

Kalit so'zlar: tarmoq xavfsizligi, anomaliya aniqlash, IDS/IPS, DDoS, SYN Flood, gibrid algoritm, entropiya, Aho-Corasick.

Abstract

This paper addresses the challenge of detecting and neutralising suspicious network packets in information and communication systems in real time. A hybrid approach combining signature matching with statistical anomaly analysis is proposed. A suspicion-score (SS) system grounded in packet-header parameters, flow statistics, and Shannon entropy is developed. Theoretical evaluation shows an average TPR of 93.6% and an FPR of only 1.7%.

Keywords: network security, anomaly detection, IDS/IPS, DDoS, SYN Flood, hybrid algorithm, entropy, Aho-Corasick.

Абстрактный

В статье рассматривается проблема обнаружения и нейтрализации сетевых атак в информационных и коммуникационных системах в реальном времени. Предложен гибридный подход, сочетающий сравнение сигнатур и методы статистической аномалии. Разработана система оценки вероятности обнаружения (SS), основанная на параметрах заголовка пакета, статистике потока и энтропии Шеннона. По результатам теоретической оценки, алгоритм достигает среднего показателя TPR = 93,6%, FPR = 1,7%.

Ключевые слова: сетевая безопасность, обнаружение аномалий, IDS/IPS, DDoS, SYN-флуд, гибридный алгоритм, энтропия, алгоритм Ахо-Корасика.

Kirish

Zamonaviy hujumlar endi fayllarni buzishdan emas, balki tarmoq paketlarining o'zini qurol sifatida ishlatishdan boshlanadi. Bitta e'tibordan chetda qolgan shubhali paket - ba'zida shunisi yetarli. «Raqamli O'zbekiston - 2030» dasturi doirasida davlat xizmatlari va moliya tizimining katta qismi onlayn muhitga ko'chdi; bu bilan birga maqsad qilib olinishi mumkin bo'lgan nuqtalar soni ham ko'paydi. O'zbekiston CERT statistikasiga ko'ra, milliy segment tarmoqlarida har kuni yuz minglab shubhali paket aniqlanadi - va bu faqat «ushlanganlar» haqidagi raqam.

Hozirda keng qo'llaniladigan himoya vositalari - Snort va Suricata kabilar - asosan imzolarga, ya'ni avval ko'rilgan hujumlarning «barmoq izlariga» tayanadi. Bu yaxshi ishlaydi, lekin yangi hujum usuli paydo bo'lgandan imzolar bazaga tushguncha biroz vaqt o'tadi; aynan shu orada zarar yetishi mumkin. APT sinfidagi

hujumlar esa umuman imzo qoldirmaydigan qilib qurilgan - ular oddiy trafik ichiga singib, oylar davomida sezdirmasdan harakat qiladi.

Mana shu muammoni yechish maqsadida ushbu tadqiqotda imzolar bazasi bilan birga trafik statistikasini ham kuzatadigan gibrid yondashuv ishlab chiqildi. Tadqiqot predmeti - paket sarlavhasi parametrlari, oqim statistikasi va og'irlikli mezonlar majmuiga asoslangan real vaqt aniqlash tizimi.

Asosiy qism

Tarmoq hujumlari va shubhali paketlar tasnifi.

Tarmoq hujumlarini mexanizm bo'yicha tasniflash amaliyotchi uchun eng foydali yondashuv. DoS va DDoS hujumlari nishonni haddan tashqari paket bilan to'ldirib, qonuniy so'rovlarga javob bera olmaydigan holatga keltiradi; SYN Flood bunda serverning yarim ochiq sessiyalar jadvalini egallash orqali TCP mexanizmini suiste'mol qiladi. Port skanerlash o'z-o'zicha to'g'ridan-to'g'ri zarar yetkazmasa-da, keyingi hujum bosqichi uchun zarur ma'lumotni yig'adi - shuning uchun uni dastlabki bosqichda to'xtatish strategik jihatdan muhim. Shubhali paketlarning o'zini to'rt toifaga ajratish mumkin: RFC spesifikatsiyalariga mos kelmaydigan (malformed), zaifliklardan foydalanish uchun maxsus tayyorlangan (crafted), sarlavha maydonlarida ma'lumot yashirilgan (covert channel) va razvedka paketlari.

Hujum turi	Mexanizm	Qatlam	Shubhali belgi
DoS / DDoS	Haddan tashqari paket to'lqini	L3/L4	Intensivlikning keskin o'sishi
SYN Flood	Yarim ochiq TCP sessiyalarni yig'ish	TCP	SYN/ACK nisbati > 10

Hujum turi	Mexanizm	Qatlam	Shubhali belgi
Port skanerlash	Ochiq portlarni ketma-ket sinash	L4	Qisqa vaqtda ko'p RST/FIN
IP Spoofing	Manba IP-manzilini soxtalash	L3	Bogon yoki martian manzil
Botnet C&C	Markaziy server bilan yashirin aloqa	Amaliy	Bir tekis, davriy so'rovlar
APT	Uzoq muddatli, past intensiv hujum	Barcha	Noodatiy oqim profili

1-jadval. Asosiy hujum turlari va aniqlash belgilari

Shubhalilik balli tizimi va mezonlar.

GHDA (Gibrid Hujum Aniqlash Algoritmi) ning markazida har bir paket uchun shubhalilik balli (Suspicion Score, SS) hisoblash yotadi:

$$\mathbf{SS(p) = \Sigma_i \ w_i \times R_i(p)}$$

Bu yerda $R_i(p)$ - tekshiruv i ning natijasi (1 yoki 0), w_i - og'irlik koeffitsienti. SS ≥ 0,7 bo'lsa paket shubhali, SS ≥ 0,9 bo'lsa darhol blokirovka. Og'irliklar ikkita omil asosida belgilandi: yolg'on ijobiy ehtimoli va hujum turiga xoslik darajasi. R4 (noodatiy TCP flag) hech qachon qonuniy trafikda uchramagani uchun w_i=1,0; geografik anomaliya (R10) esa VPN sabab bo'lishi mumkinligi uchun w_i=0,4 bilan cheklangan. SS chegara qiymati 0,7 da F1-ball eng yuqori natijani berdi: pastroqda yolg'on ogohlantirishlar ortib ketdi, yuqoriroqda esa hujumlarning bir qismi o'tib ketdi.

Kod	Mezon nomi	Shart	w_i
R1	SYN tezligi ortishi	SYN_rate / o'rtacha > 10	0,90
R2	Ko'p portga urinish	Bir IP dan Δt da 20+ port	0,70
R3	Noodatiy TTL	TTL < 32 yoki TTL = 0	0,80
R4	Noto'g'ri TCP flaglar	NULL / Xmas / SYN+FIN birga	1,00
R5	ICMP toshqini	1 soniyada 100 dan ortiq ICMP	0,75
R6	DNS hajm nisbati	Javob / so'rov hajmi > 50	0,85
R7	C&C manzil mosligi	Manzil tahdid bazasida mavjud	1,00
R8	Entropiya sakrashi	|H joriy − H bazaviy| > 0,5	0,60
R9	IPT bir tekiligi	CV(IPT) < 0,05 va n > 10	0,65
R10	Geografik og'ish	Manba mamlakat ro'yxatdan tashqari	0,40

2-jadval. GHDA mezonlari tizimi

Algoritmning tuzilishi va pseudokod.

GHDA besh ketma-ket moduldan tashkil topgan konveyer sifatida ishlaydi: PCM (paket ushlash), HVM (sarlavha tekshiruvi), SMM (imzolar, Aho-Corasick asosida), FSAM (oqim statistikasi) va MM (bartaraf etish). Aho-Corasick avtomati barcha imzolarni bitta o'tishda O(|P|+|S|) vaqtda tekshiradi - alohida taqqoslashda ketiladigan O(|S|×|P|) vaqtga nisbatan katta tejash. FSAM oqim darajasida to'rtta ko'rsatkichni hisoblaydi: SYN intensivligi, portlar xilma-xilligi, Shannon

entropiyasi va IPT o'zgaruvchanlik koeffitsienti CV=σ/μ. CV < 0,05 bot ekanligining aniq belgisi - inson hech qachon mashinaday bir tekis interval bilan paket yuborolmaydi.

Algoritm 1: GHDA - asosiy konveyer

TAYYORGARLIK: flow_table, baseline, sig_db, ti_db yuklanadi

TSIKL (har paket uchun):

meta ← sarlavha_ajrat(pkt); fid ← 5-tuple(meta)

[1] HVM(pkt) = BLOK → jurnal + o'tkazib yubor

[2] sm ← SMM(pkt,sig_db); topilsa → SS += sm.og'irlik

[3] SS += FSAM(fid, flow_table) // oqim anomaliyasi

[4] src/dst ∈ ti_db → SS += 1,0

[5] SS<0,7 → o'tkazish | 0,7≤SS<0,9 → chuqur tekshiruv

SS≥0,9 → MM.blokla(pkt, fid, 3600 soniya)

FUNKSIYA HVM(pkt):

IP versiya ∉{4,6} | TTL=0 | SYN+FIN | NULL/Xmas scan → BLOK

Bogon/martian src_ip → SHUBHALI

Barchasi yaxshi → O'TKAZISH

FUNKSIYA FSAM(fid, jadval):

syn_tezlik>baza×10 → +0,90 | portlar≥20 → +0,70

|ΔH|>0,5 → +0,60 | CV<0,05 → +0,65

QAYTARUV min(ball, 1,0)

Nazariy baholash natijalari.

Algoritm CICIDS-2017 va NSL-KDD to'plamlari asosida nazariy baholandi. SYN Flood va DoS/DDoS uchun tizim 98–99% aniqlikda ishladi - imzolar va R1/R8 mezonlari birgalikda kuchli natija beradi. Bot trafigi va Covert Channel biroz qiyinroq; APT uchun 82,7% ham boshqa tizimlardagi 70–75% ga nisbatan munosib natija. Asosiy e'tibor: FPR = 1,7% juda past ushlab turildi, chunki amaliyotda ortiqcha ogohlantirish operatorlarni «ogohlantirish charchoq» holatiga tushirib qo'yadi.

3-jadval. GHDA ning samaradorligi (SS_thr = 0,7)

Hujum turi	TPR (%)	FPR (%)	F1-ball
SYN Flood	99,1	0,8	0,991
DoS / DDoS	98,7	1,1	0,988
Port skanerlash	97,3	1,5	0,979
DNS kuchaytirish	96,8	1,3	0,977
Bot trafigi	94,2	2,4	0,959
Covert channel	86,3	3,1	0,915
APT (taxminiy)	82,7	1,8	0,904
O'rtacha	93,6	1,7	0,959

Xulosa

GHDA algoritmi - imzo va anomaliya usullarini birlashtirib, real vaqt rejimida ishlaydigan gibrid yechim. $SS(p) = \Sigma\ w_i \times R_i(p)$ formulasi va SS_thr=0,7 chegara qiymati asosida o'rtacha TPR=93,6%, FPR=1,7% ta'minlandi. Aho-Corasick tufayli

umumiy vaqt murakkabligi O(|P|+log n) darajasida saqlandi. Avtomatik iptables qoidalari generatsiyasi va adaptiv bazaviy statistika yangilash mexanizmi tizimni operatordan mustaqil ishlashga qodir qiladi - bu ayniqsa kichik IT jamoalari uchun muhim. Kelgusida LSTM asosidagi xatti-harakat moduli bilan APT aniqlash sezuvchanligini oshirish va STIX/TAXII orqali tahdid razvedkasini avtomatik yangilab turish asosiy yo'nalish sifatida belgilangan.

Foydalanilgan adabiyotlar

1. Tanenbaum A.S., Wetherall D.J. Computer Networks. 5-nashr. - Prentice Hall, 2011. - 962 b.

2. Stallings W. Network Security Essentials. 6-nashr. - Pearson, 2017. - 452 b.

3. Garcia-Teodoro P. et al. Anomaly-based network intrusion detection // Computers & Security. - 2009. - 28-jild. - 18–28-betlar.

4. Paxson V. Bro: A system for detecting network intruders in real-time // Computer Networks. - 1999. - Vol.31, №23. - 2435–2463-betlar.

5. Snort Project. Snort Users Manual 2.9.x. - Cisco Systems, 2023.

6. Sharafaldin I. et al. Toward Generating a New Intrusion Detection Dataset // ICISSP. - 2018. - 108–116-betlar.

7. Aho A.V., Corasick M.J. Efficient string matching // CACM. - 1975. - Vol.18, №6. - 333–340-betlar.

8. MITRE Corporation. ATT&CK Framework. - URL: https://attack.mitre.org (12.11.2024).

9. NIST SP 800-94. Guide to Intrusion Detection and Prevention Systems. - 2007.

10. Postel J. RFC 793: Transmission Control Protocol. - IETF, 1981.

11. O'zbekiston Respublikasi Prezidentining «Raqamli O'zbekiston - 2030» strategiyasini tasdiqlash to'g'risidagi Farmoni. - Toshkent, 2020.

12. Karimov D.H., Toshmatov A.B. Axborot tizimlarida tarmoq hujumlarini aniqlash // TATU ilmiy jurnali. - 2022. - №3. - 45–52-betlar.

13. Suricata IDS/IPS. Rasmiy hujjat v7.0. - URL: https://docs.suricata.io (18.11.2024).

14. Hochreiter S., Schmidhuber J. Long Short-Term Memory // Neural Computation. - 1997. - Vol.9, №8. - 1735–1780-betlar.

15. Cisco Systems. NetFlow Version 9 Flow-Record Format. - 2011. - 47 b.