SUQULIB KIRISHLARNI ANIQLASH TIZIMLARI

Islomov Dostonbek Uktamjon o'g'li

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Nurafshon filiali, Axborot texnologiyalari kafedrasi assistenti, Email:islomovdostonbek97@gmail.com Tel: +99897 590 97 02

Annotatsiya

Ushbu maqolada suqulib kirishlarni aniqlash tizimlari, ularning vazifasi, arxitekturasi, turlari, ishlash funktsiyalari va ularning afzallik, kamchiliklari yoritib berilgan.

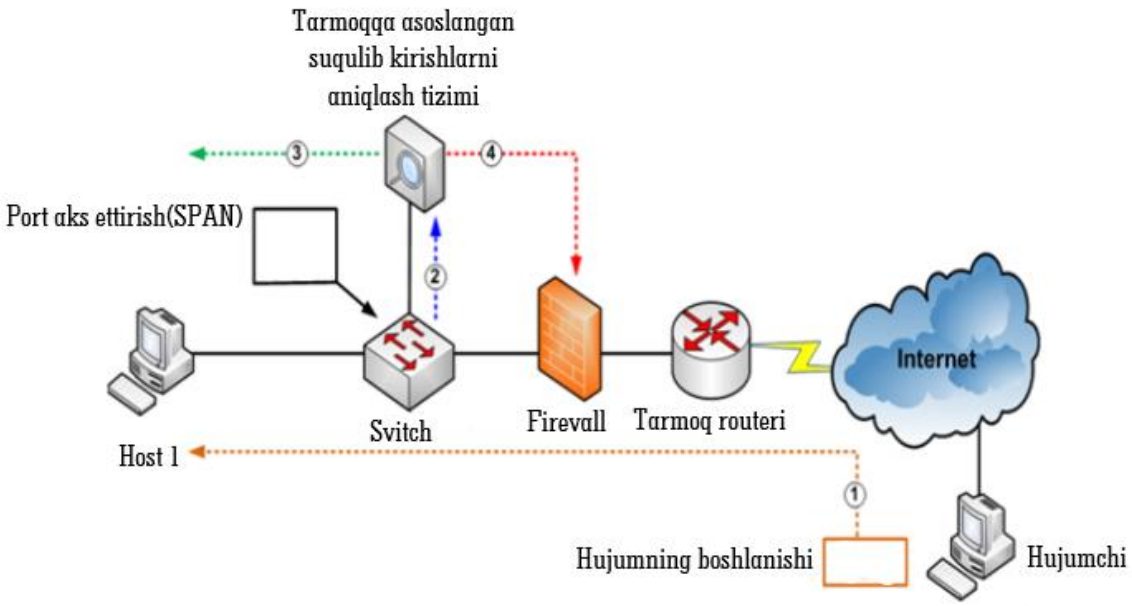
Kalit so'z Suqulib kirishlarni aniqlash tizimi, tarmoqqa asoslangan suqulib kirishlarni aniqlash tizimi, hostga asoslangan suqulib kirishlarni aniqlash tizimi.

Abstract. In this article, intrusion detection systems, their function, architecture, types, performance functions and their advantages and disadvantages are highlighted.

Key words: Intrusion detection system, network-based intrusion detection system, host-based intrusion detection system.

Tarmoqqa asoslangan suqulib kirishlarni aniqlash tizimi

Tarmoqqa asoslangan suqulib kirishlarni aniqlash tizimi(NIDS) maqsadi tizimning atribut funksiyasi va tarmoqdagi funksiya modullari kuzatiladi. Tarmoqqa asoslangan suqulib kirishlarni aniqlash tizimi(NIDS)ning nazorati qo'lda yoki avtomatik shaklga asoslangan[2]. Bu tizim xavfsizlik infratuzilmalarida sezilarli darajada foydalaniladi. Tarmoqqa asoslangan suqulib kirishlarni aniqlash tizimi(NIDS) kiruvchi va chiquvchi xavflarni nazorat qiladi, serverlarga xavfga qarshi dasturiy taminot o'rnatiladi. Bir qancha sohalarda xavfsizlikni ta'minlash juda ham zarur, misol uchun hukumat ilovalari, biznes, sanoat va ta'lim muassasalarida va boshqalar(1-rasm)[3].



1-rasm. Tarmoqqa asoslangan suqulib kirishlarni aniqlash tizimi(NIDS)ning arxitekturasi

Tarmoqqa asoslangan suqulib kirishlarni aniqlash tizimi(NIDS) belgiga asoslangan klassifikatsiyadan iborat bo‘lib, ular oldingi log fayllar yoki belgilar bilan solishtirish orqali o‘zgarishlarni aniqlaydi. Anomaliyaga asoslangan texnika, noto‘g‘ri foydalanishni shuningdek kompyuterdagi noodatiy harakatlarni aniqlaydi, keyin normal yoki hujum belgilarining evristikasiga bog‘liqligi sifatida tasniflanadi.

Tarmoqqa asoslangan suqulib kirishlarni aniqlash tizimi(NIDS) qurilmaning kiruvchi va chiquvchi paketlarini boshqaradi[4].

Tarmoqqa asoslangan suqulib kirishlarni aniqlash tizimi(NIDS) barcha tarmoq qurilmalariga va undan keladigan trafikni kuzatadi va tahlil qiladi.Tarmoqqa asoslangan suqulib kirishlarni aniqlash tizimi(NIDS) tarmoq ichidagi strategik nuqtadan (yoki bir nechta aniqlash tizimlarini o‘rnatgan bo‘lsangiz), odatda ma’lumotlarni ulash nuqtalarida ishlaydi.

Tarmoqqa asoslangan suqulib kirishlarni aniqlash tizimi(NIDS)ning afzalliklari:

- Butun tarmoq bo‘ylab suqulib kirishlarni aniqlash tizimi(IDS) xavfsizligini ta‘minlaydi.
- Bir necha strategik joylashtirilgan tarmoqqa asoslangan hujumlarni aniqlash tizimi(NIDS) korporativ tarmoqni kuzatishi mumkin.
- Tarmoqning mavjudligi yoki o‘tkazuvchanligini buzmaydigan passiv qurilma.
- Buzg‘unchilardan himoya qilishi va yashirish nisbatan oson.
- Trafik eng zaif bo‘lgan tarmoq qismlarini qamrab oladi.

Tarmoqqa asoslangan suqulib kirishlarni aniqlash tizimi(NIDS)ning kamchiliklari:

- O‘rnatish qimmat.

- Agar tarmoqqa asoslangan suqulib kirishlarni aniqlash tizimi(NIDS) keng yoki band tarmoqni kuzatishi kerak bo‘lsa, tizim past o‘ziga xoslik va vaqti-vaqti bilan sezilmaydigan buzilishdan aziyat chekishi mumkin.
- Shifrlangan trafik ichidagi tahdidlarni aniqlash muammoli bo‘lishi mumkin.
- Odatda kommutatorga asoslangan tarmoqlar uchun ideal emas[5].

Hostga asoslangan suqulib kirishlarni aniqlash tizimi

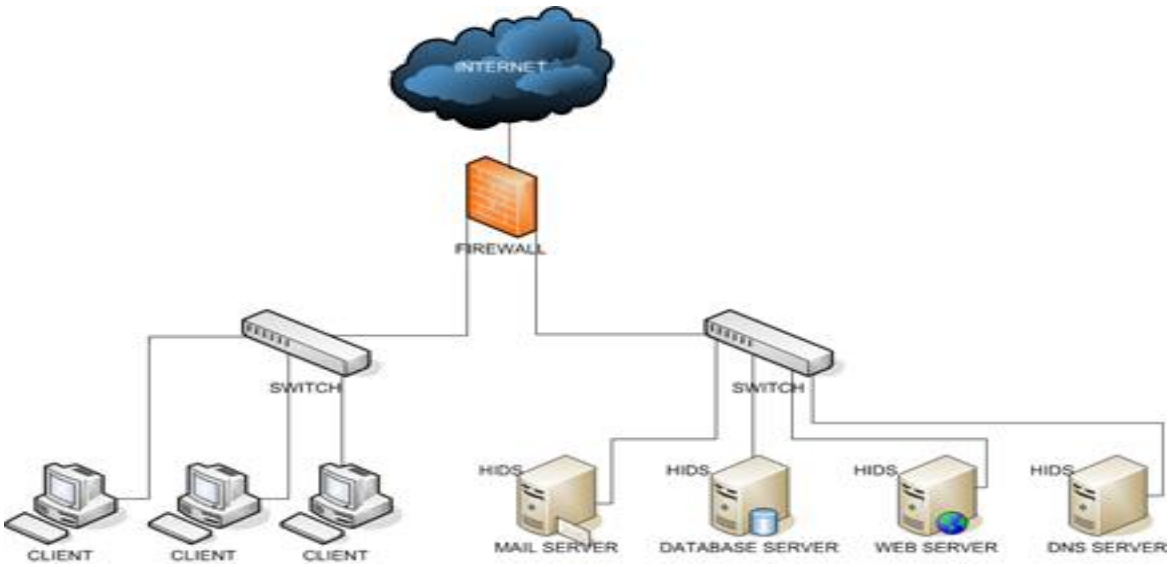
Xostga asoslangan suqulib kirishlarni aniqlash tizimi (HIDS) bu xostdagi zararli xatti-harakatlarni aniqlaydigan dasturiy ta‘minot. Shuningdek, u operatsion tizimning barcha operatsiyalarini kuzatib boradi, foydalanuvchi xatti-harakatlarini kuzatib boradi va inson yordamisiz mustaqil ishlaydi.

Xostga asoslangan suqulib kirishlarni aniqlash tizimi(HIDS) dastur darajasida ishlaydigan boshqa antivirus tizimlaridan farqli o‘laroq operatsion tizim(OS) darajasida ishlaydi. Shuningdek, u har qanday ruxsatsiz yoki shubhali faoliyatni aniqlash uchun kompyuterning operatsion tizimida ishlaydigan dasturlarning xatti-harakatlarini kuzatib boradi. Umuman olganda, ushbu turdagi himoya moliyaviy yozuvlar kabi ma’lumotlar bazalarida maxfiy ma’lumotlarga ega bo‘lgan serverlarda o‘rnatiladi. Biroq, hostga asoslangan suqulib kirishlarni aniqlash tizimi(HIDS) agent va monitor orqali ishlaydi.

Uskunalar, kataloglar va fayllardan ma’lumot to‘plash uchun agentni kuzatmoqchi bo‘lgan xostga o‘rnatilishi kerak. Shuningdek, agent ishlaydigan jarayonlar, tarmoq trafigi va boshqalardan ma’lumotlarni to‘playdi. Keyin ma’lumotlar jurnallar fayllarida shubhali hodisalarni qidiradigan monitoring dasturi tomonidan tahlil qilish uchun markaziy joyga yuboriladi. Tizimga ruxsatsiz kirish yoki kompyuterga masofadan kirish kabi hodisalar har qanday tashkilotga tahdid soladi. Bundan tashqari, fayllarni, dasturlarni, muhim tizim sozlamalarini o‘zgartirish yoki ruxsatsiz fayllarni o‘chiradi.

Bundan tashqari, u hech kim uni kirish nuqtasi sifatida ishlatmasligini ta‘minlash uchun tizimning tarmoq ulanishlarini kuzatib boradi. Keyin, monitoring dasturi suqulib kirishini aniqlaganida, xavfli hodisalarga qarshi choralar ko‘radigan ma‘murlarga ogohlantirishlar yuboradi.

Xostga asoslangan suqulib kirishlarni aniqlash tizimi(HIDS) ahamiyati log fayllardagi zararli faoliyat mavjudligini tekshiradi. Xostdagi foydalanuvchi faoliyatini nazorat qiladi. Foydalanuvchilar va voqealardan ma’lumotlarni to‘playdi. Zararli hodisalar sodir bo‘lganda administratorlarga ogohlantirish yuboriladi(2-rasm)[6].



2-rasm. Hostga asoslangan suqulib kirishlarni aniqlash tizimi(HIDS) arxitekturasi

Xostga asoslangan kirishlarni aniqlash tizimi(HIDS) ning afzalliklari.

- Asosiy qurilma va uning faoliyati (konfiguratsiya, ruxsatlar, fayllar, ro‘yxatga olish kitobi va boshqalarga o‘zgartirishlar) chuqur ko‘rinishini taklif qiladi.
- Tarmoqqa asoslangan suqulib kirishlarni aniqlash tizimi(NIDS) zararli paketga qarshi mukammal ikkinchi himoya chizig‘ini aniqlay olmaydi.
- Tizim konsolidagi fayllarga ruxsatsiz o‘zgartirishlar kabi tashkilot ichidan kelib chiqqan paketlarni aniqlashda yaxshi.
- Dasturiy ta‘minotning yaxlitligini buzishni aniqlash va oldini olishda samarali.
- Kamroq paketlar tufayli shifrlangan trafikni tarmoqqa asoslangan suqulib kirishlarni aniqlash tizimi(NIDS)ga qaraganda yaxshiroq tahlil qiladi.
- Tarmoqqa asoslangan suqulib kirishlarni aniqlash tizimi(NIDS)ni o‘rnatishdan ancha arzon.

Xostga asoslangan suqulib kirishlarni aniqlash tizimi(HIDS)ning kamchiliklari.

- Cheklangan ko‘rinish, chunki tizim faqat bitta qurilmani nazorat qiladi.
- Qaror qabul qilish uchun mavjud kontekstning kamligi.
- Yirik kompaniyalar uchun boshqarish qiyin, chunki jamoa har bir xost uchun ma’lumotlarni sozlashi va boshqarishi kerak.
- Tarmoqqa asoslangan suqulib kirishlarni aniqlash tizimi(NIDS)ga qaraganda hujumchilarga ko‘proq ko‘rinadi.
- Tarmoqni skanerlash yoki boshqa tarmoq bo‘ylab kuzatuv hujumlarini aniqlashda yaxshi emas[2].

Passiv Suqulib kirishlarni aniqlash tizimi(IDS): Passiv suqulib kirishlarni aniqlash tizimi(IDS) tarmoq ma'muri yoki foydalanuvchi harakati uchun signal ishlab chiqarish orqali hujumlarga javob beradi. Ular o‘zlari yetkazilgan zararni kamaytirishga harakat qilmaydilar yoki hujumchiga zarar etkazish yoki to‘sqinlik qilish uchun faol ravishda qidirmaydilar. Ushbu sinfdagi mavjud suqulib kirishlarni aniqlash tizim(IDS)lari: IDES (Lunt et al. 1992), GrIDS (Chen et al. 1996), NIDES (Anderson et al. 1995).

Faol suqulib kirishlarni aniqlash tizimi(IDS): Faol suqulib kirishlarni aniqlash tizimi(IDS) ma’lum harakatlarni boshlash orqali hujumlarga javob beradi. Harakat ikkita ob’ektga qarshi bo‘lishi mumkin, bu esa faol suqulib kirishlarni aniqlash(IDS)ni quyi sinflarga tasniflaydi. Bunday subektlarda bo‘lishi mumkin: Hujum tizimi: Bu sinfda suqulib kirishlarni aniqlash tizimi(IDS) hujum qiluvchi tizimni boshqarishga harakat qiladi. Suqulib kirishlarni aniqlash tizimi(IDS) bunda uning operatsion platformasidan hujum qilayotgan hujumchi tizimni olib tashlash uchun harakat qiladi. Hujum qilingan tizim: bu sinfda, IDS hujum qilingan tizimni boshqarishga harakat qiladi. Ular hujumni yumshatish uchun hujum qilingan tizim holatini o‘zgartiradilar. Ular tarmoq ulanishlarini to‘xtatishi, xavfsizlik jurnalini oshirishi mumkin yoki muammoli jarayonlarni to‘xtatish va hokazo. Mavjud faol IDS lar quyidagilar: EMERLARD (Porras and Neumann 1997), Janus (Goldberg et al. 1996), OSSEC HIDS (Hay et al. 2008), RealSecure (Internet Security Systems (ISS) 2010). Bular haqidagi muhokamalar 1-rasmda ifodalangan.

Suqulib kirishlarni aniqlash texnikalari.

Nazariy ma’lumotlarda keltirilishicha, suqulib kirishlarni aniqlash uchun turli fanlardan turli xil texnikalar qo‘llanilgan. Asosiy texnikalar *statistik usullar*, *bilimga asoslangan texnikalar* va *sun'iy intellektga (AI)* asoslangan texnikalardir. Statistikaga asoslangan IDS da tizim xatti-harakatini tasodifiy nuqtai nazardan ifodalanadi. Boshqa tomondan, bilimga asoslangan IDS usullar mavjud tizim ma’lumotlaridan (protokol spetsifikatsiyalari, tarmoq trafigining namunalari va boshqalar) da’vo qilingan xatti-harakatlarni olishga harakat qiladi. Nihoyat, Suni’y intellekt(AI)ga asoslangan IDS texnikasi belgilarni tasniflash imkonini beruvchi aniq yoki yashirin modelni o‘rnatishni o‘z ichiga oladi(Garsiya-Teodoro va boshqalar. 2009).

Ilmiy yangilik. Yangilik sifatida Anomaliyaga asoslangan suqulib kirishlarni aniqlash tizimida, suqulib kirishlar statistikasini yoritib boruvchi funktsiya qo‘shishni taklif qilar edim. Misol uchun bir oy davomida qancha ruxsatsiz suqulib kirishlar amalga oshirilgan va statistikaga asoslanib kelajakdagi ehtimoliy hujumlarni taxmin qilish va qarshi choralar ko‘rish ehtimoli bo‘ladi.

Foydalanilgan adabiyotlar ro‘yxati.

1. J. Kevric, S. Jukic, and A. Subasi, “An effective combining classifier approach using tree algorithms for network intrusion detection,” Neural Computing and Applications, pp. 1-8, 2016.

2. K. Shafi, and A.A. Hussein, “Evaluation of an adaptive genetic-based signature extraction system for network intrusion detection,” Pattern Analysis and Applications, vol. 16, no. 4, pp. 549-566, 2013.

3. N.G. Relan, and D.R. Patil, “Implementation of network intrusion detection system using variant of decision tree algorithm,” In proceedings of International Conference on Nascent Technologies in the Engineering Field (ICNTE),., 2015.

4. A.B. Ashfaq, M.Q. Ali, and S.A. Khayam, “Accuracy improving guidelines for network anomaly detection systems,” Journal in computer virology, vol. 7, no. 1, pp. 63-81, 2011.

5. https://phoenixnap.com/blog/what-is-high-availability.

6. F.L. Catherine, R. Pathak, and V. Vaidehi, “Efficient host based intrusion detection system using Partial Decision Tree and Correlation feature selection

algorithm,” In proceedings of International Conference on IEEE, Recent Trends in Information Technology (ICRTIT), 2014.