TARMOQLARNI MONITORING QILISH VOSITALARI (WIRESHARK, PRTG, NAGIOS)

Eshonqulov Tirkash *- dotsent,*
O'zbekiston milliy universiteti Jizzax filiali

Annotatsiya: O'zbekcha: Maqolada tarmoq monitoringi vositalari – Wireshark, PRTG va Nagios dasturlarining imkoniyatlari, afzalliklari hamda ularning ta'lim va IT sohalaridagi o'rni tahlil qilingan.

Kalit so'zlar: Tarmoq monitoringi, Wireshark, PRTG, Nagios, trafik tahlili, tizim holati, protokol, ogohlantirish, IT infratuzilma

Аннотация: В статье анализируются возможности и преимущества средств мониторинга сети – программ Wireshark, PRTG и Nagios, а также их применение в образовании и сфере ИТ.

Ключевые слова: Мониторинг сети, Wireshark, PRTG, Nagios, анализ трафика, состояние системы, протокол, оповещения, ИТ-инфраструктура

Annotation: The article analyzes the capabilities and advantages of network monitoring tools – Wireshark, PRTG, and Nagios, as well as their role in education and IT fields.

Keywords: Network monitoring, Wireshark, PRTG, Nagios, traffic analysis, system status, protocol, alerting, IT infrastructure

Zamonaviy kompyuter tarmoqlari kengayib borayotgani sari, ularni samarali boshqarish va uzluksiz ishlashini ta'minlash uchun tarmoq monitoringi vositalari tobora muhim ahamiyat kasb etmoqda. Monitoring vositalari administratorlarga tarmoqdagi muammolarni erta aniqlash, ishlash unumdorligini baholash va xavfsizlik tahdidlariga qarshi choralar ko'rish imkonini beradi.

Tarmoq monitoringi vositalari yordamida real vaqt rejimida trafikni kuzatish, qurilmalar holatini baholash, xizmatlar ishlashini nazorat qilish va ishlash samaradorligini optimallashtirish mumkin. Bunday tizimlar ayniqsa yirik korxonalar, ta'lim muassasalari va IT infratuzilmasi rivojlangan tashkilotlar uchun zarurdir.

Wireshark — bu eng mashhur va kuchli tarmoq tahlilchilardan biri bo'lib, u paket darajasida tarmoq trafigini tahlil qilish imkonini beradi. Wireshark orqali administratorlar IP paketlar, TCP ulanishlari, DNS so'rovlar kabi ma'lumotlarni chuqur ko'rib chiqishlari mumkin. Bu vosita tarmoqdagi nosozliklarni aniqlash, xavfsizlikni tekshirish va protokol analizini amalga oshirishda keng qo'llaniladi.

Wireshark bepul, ochiq manbali dastur bo'lib, turli operatsion tizimlar (Windows, Linux, macOS) uchun mavjud. Foydalanuvchilarga qulay interfeys, filtrlash imkoniyatlari va real vaqtli monitoring funksiyalari bilan jihozlangan.

PRTG Network Monitor — bu tarmoq monitoringi uchun mo‘ljallangan ko‘p funksiyali vosita bo‘lib, turli qurilma va xizmatlarning ishlash holatini markazlashgan tarzda kuzatish imkonini beradi. PRTG SNMP, WMI, NetFlow, sFlow kabi protokollarni qo‘llab-quvvatlaydi va foydalanuvchiga grafikalar, hisobotlar va ogohlantirishlar taqdim etadi.

PRTG orqali har bir sensor orqali ma’lumotlar olinadi, bu esa tarmoqning har bir komponentini chuqur nazorat qilish imkonini beradi. Masalan, serverlar yuklamasi, routerlar ishlashi, disk bo‘sh joyi yoki tarmoq trafigi haqida to‘liq ma’lumotlar olinadi.

Nagios — bu tarmoq xizmatlari, tizim resurslari va infratuzilma komponentlarini monitoring qilish uchun keng tarqalgan vosita. Nagios yordamida tizim administratorlari xizmatlarning mavjudligi, resurslar yuklamasi, log fayllar va xavfsizlik holatini avtomatik kuzatib borishlari mumkin.

Nagios kuchli plaginlar tizimiga ega bo‘lib, foydalanuvchilar tomonidan moslashtirilgan monitoring ssenariylarini yaratish imkonini beradi. Bu dasturning ochiq manbali bo‘lishi uni korxona ehtiyojlariga moslashtirishni osonlashtiradi.

Monitoring tizimlarining yana bir muhim jihati — bu ogohlantirish va hisobot tizimining mavjudligidir. Har uchala vosita (Wireshark, PRTG, Nagios) o‘zida avtomatik xabar yuborish, grafik hisobotlar tuzish va tizim holatini real vaqt rejimida aks ettirish imkoniyatlarini mujassamlashtirgan.

Statistik ma’lumotlarga ko‘ra, yirik IT tashkilotlarning 80 foizdan ortig‘i tarmoq monitoringi vositalaridan muntazam foydalanadi. Bu vositalar yirik tizimlarning barqaror va xavfsiz ishlashini ta’minlashda muhim rol o‘ynaydi.

Tarmoq monitoringi vositalarini tanlashda ularning qulayligi, qo‘llab-quvvatlanadigan protokollar soni, plaginlar mavjudligi, vizual interfeys va hisobot berish tizimi muhim mezon sifatida qaraladi.

Wireshark tarmoq protokollarini chuqur tahlil qilish uchun afzal bo‘lsa, PRTG keng qamrovli holatni nazorat qilish uchun qulay. Nagios esa kuchli plagin tizimi orqali murakkab infratuzilmani boshqarish imkonini beradi.

Bu vositalarning kombinatsiyasi esa yanada kuchli va ishonchli monitoring tizimini yaratish imkonini beradi. Masalan, Wireshark orqali tarmoqda muammolar tahlil qilinadi, PRTG holatni kuzatib boradi, Nagios esa doimiy xizmat monitoringini ta’minlaydi.

O‘quv muassasalarida bu vositalardan foydalanish informatika va axborot xavfsizligi sohalaridagi amaliy ko‘nikmalarni shakllantirishda muhim ahamiyatga ega. Talabalar tarmoqni tahlil qilish, holatini baholash va muammolarni bartaraf etish tajribasini real vositalar orqali egallaydi.

Xulosa qilib aytganda, Wireshark, PRTG va Nagios singari tarmoq monitoringi vositalari zamonaviy axborot texnologiyalari infratuzilmasining ajralmas qismiga aylangan. Ular orqali tarmoqni xavfsiz, barqaror va samarali boshqarish imkoniyati

yaratiladi.

Foydalanilgan adabiyotlar:

1. Combs, Gerald. Wireshark Network Analysis. Protocol Analysis Institute, 2020.
2. Paessler AG. PRTG Network Monitor – Official Documentation. 2023.
3. Nagios Enterprises. Nagios Core Documentation. 2022.
4. Kurose, J. F., & Ross, K. W. Computer Networking: A Top-Down Approach. Pearson, 2016.
5. Tarmoq xavfsizligi bo‘yicha o‘quv qo‘llanma. Toshkent axborot texnologiyalari universiteti, 2021.
6. O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligi – Axborot xavfsizligi hisobotlari, 2023.
7. Network Monitoring Tools – Comparative Analysis Report. Gartner, 2022.
8. Open Source Network Monitoring Tools. Linux Journal, 2020.