UDK 004.72

ZAMONAVIY TARMOQ XAVFSIZLIGINI TA'MINLASHDA CISCO PACKET TRACER DASTURINI IMKONIYATLARI

Namangan muhandislik-qurilish instituti

“Axborot tizimlari va texnologiyalari” kafedrasi katta o’qituvchisi

t.f.f.d(PhD). Xaydarov Kamoliddin Sayfullayevich

Annotatsiya: Ushbu maqolada Cisco Packet Tracer dasturining imkoniyatlaridan foydalanib, zamonaviy tarmoq xavfsizligini ta'minlashda qo'llaniladigan usullar va amaliyotlar keng yoritiladi. Tarmoq xavfsizligini mustahkamlashda dastur orqali amalga oshirilgan sinovlar, monitoring vositalari va xavfsizlik siyosati texnologiyalarining qo'llanishi batafsil tahlil qilinadi.

Kalit so’zlar: Cisco Packet Tracer, tarmoq xavfsizligi, DDoS, phishing, ransomware, tarmoq topologiya, Router, switch, ACL, VLAN, NAT, Man-in-the-Middle, Simulyatsiya.

ОБЕСПЕЧЕНИЕ СОВРЕМЕННОЙ СЕТЕВОЙ БЕЗОПАСНОСТИ С ПОМОЩЬЮ CISCO PACKET TRACER

Аннотация: В данной статье подробно рассматриваются методы и практики обеспечения современной сетевой безопасности с использованием возможностей программы Cisco Packet Tracer. Анализируются тесты, проведенные с использованием программы, инструменты мониторинга и применение технологий политики безопасности для повышения уровня сетевой безопасности.

Ключевые слова: Cisco Packet Tracer, сетевая безопасность, DDoS, фишинг, программы-вымогатели, топология сети, маршрутизатор, коммутатор, ACL, VLAN, NAT, атака типа Человек посередине, симуляция.

ENSURING MODERN NETWORK SECURITY USING CISCO PACKET TRACER

Abstract: This article provides a detailed overview of the methods and practices for ensuring modern network security using the capabilities of Cisco Packet Tracer. It analyzes the tests conducted through the program, monitoring tools, and the application of security policy technologies to enhance network security.

Keywords: Cisco Packet Tracer, network security, DDoS, phishing, ransomware, network topology, router, switch, ACL, VLAN, NAT, Man-in-the-Middle attack, simulation.

Kirish: Zamonaviy dunyoda raqamli texnologiyalar hayotimizning ajralmas qismiga aylangan. Shu bilan birga, tarmoq xavfsizligi masalalari global miqyosda muhim ahamiyat kasb etmoqda. Har bir tashkilot yoki shaxs uchun ma'lumotlarni himoya qilish zaruriyati yuqori darajaga chiqdi. Bugungi kunda turli xil kiberhujumlar, xususan, DDoS (Distributed Denial of Service), phishing (firibgarlik orqali ma'lumot o'g'irlash), va ransomware (ma'lumotlarni shifrlab qo'yish orqali tovlamachilik) kabi xavflar tarmoq infratuzilmasini doimiy ravishda tahdid ostida ushlab turadi. Bu esa tarmoq muhandislarini zamonaviy xavfsizlik texnologiyalarini o'rganishga va ularni samarali qo'llashga undamoqda.

Tarmoq xavfsizligini ta'minlashda Cisco Packet Tracer dasturi katta imkoniyatlarga ega bo'lib, foydalanuvchilarga virtual muhitda tarmoq yechimlarini loyihalash, sinab ko'rish va o'rganish imkonini beradi. Ushbu dastur nafaqat tarmoq muhandislarining bilim va ko'nikmalarini oshirish uchun platforma sifatida, balki murakkab tarmoq xavfsizligi strategiyalarini rejalashtirish va amalga oshirish uchun ham qo'llaniladi.

Ushbu maqolada Cisco Packet Tracer dasturining imkoniyatlaridan foydalanib, zamonaviy tarmoq xavfsizligini ta'minlashda qo'llaniladigan usullar

va amaliyotlar keng yoritiladi. Tarmoq xavfsizligini mustahkamlashda dastur orqali amalga oshirilgan sinovlar, monitoring vositalari va xavfsizlik siyosati texnologiyalarining qo'llanishi batafsil tahlil qilinadi.

Cisco Packet Tracer dasturi orqali tarmoq xavfsizligi loyihalarini amalga oshirishda quyidagi yondashuvlar qo'llanildi:

Tarmoq topologiyasini yaratish: Router, switch va boshqa qurilmalarni joylashtirish. Tarmoq topologiyasini yaratish dastlabki qadam bo'lib, bunda tarmoqning umumiy tuzilishi rejalashtiriladi. Cisco Packet Tracer yordamida router va switchlar bir-biriga ulangan, ish stansiyalari va serverlar bilan bog'langan holda virtual tarmoq tuzilishi yaratiladi. Har bir qurilmaning vazifalari aniqlanadi va ular o'rtasida trafik oqimlari belgilab olinadi.

Xavfsizlik siyosatini qo'llash: ACL (Access Control List), VLAN va NAT kabi texnologiyalarni sozlash. ACL (Access Control List): ACL yordamida tarmoq trafikiga ruxsat berish yoki uni bloklash bo'yicha qoidalar o'rnatiladi. Cisco Packet Tracer dasturida ACL sozlamalari tarmoqdagi kiruvchi va chiquvchi trafikni boshqarish imkonini beradi. Masalan, ma'lum IP manzildan kelayotgan trafikni bloklash yoki faqat kerakli portlarga ruxsat berish orqali tarmoq xavfsizligini oshirish mumkin.

VLAN (Virtual Local Area Network): VLAN texnologiyasi tarmoqni segmentatsiya qilish imkonini beradi. Cisco Packet Tracer orqali VLAN sozlash yordamida bir xil fizik tarmoq ichida turli bo'limlar yoki guruhlarni ajratish va izolyatsiya qilish amalga oshiriladi. Bu usul xavfsizlikni oshirish bilan birga, tarmoq resurslarini samarali boshqarish imkonini beradi.

NAT (Network Address Translation): NAT texnologiyasi orqali ichki tarmoqdagi IP manzillar tashqi tarmoqdan yashiriladi. Cisco Packet Tracer yordamida NAT sozlash orqali tarmoq xavfsizligini mustahkamlash va ichki manzillarni tashqi tahdidlardan himoya qilish mumkin.

Tahdidlarni simulyatsiya qilish: Tarmoqqa hujumlarni o'xshatib ko'rish. Cisco Packet Tracer dasturi yordamida tarmoqni turli xil kiberhujumlarga nisbatan qanday munosabat bildirishini sinab ko'rish mumkin. DDoS hujumlari: Paketlarni haddan tashqari ko'p yuborish orqali tarmoqni ishdan chiqarishga qaratilgan hujumlarni simulyatsiya qilish va bu kabi holatlarga qarshi himoya choralarini sinash. Man-in-the-Middle (MITM): Trafikni o'g'irlash yoki o'zgartirishni o'xshatib ko'rish orqali xavfsizlik protokollarining samaradorligini baholash. Zararli dastur trafikini aniqlash: Nomaqbul paketlarni tarmoqdan olib tashlashga qaratilgan siyosatlarni sinovdan o'tkazish.

Monitoring va diagnostika: Paketlarning oqimini tahlil qilish va zaifliklarni aniqlash. Monitoring va diagnostika tarmoq xavfsizligini ta'minlashning ajralmas qismidir. Cisco Packet Tracer ushbu jarayonlarni amalga oshirish uchun quyidagi vositalarni taqdim etadi:

Paketlar analizatori: Tarmoq orqali o'tayotgan paketlarning xatti-harakatlarini kuzatish va ularni tahlil qilish imkonini beradi. Ushbu vosita orqali tarmoqdagi noto'g'ri konfiguratsiyalar yoki zaifliklarni aniqlash mumkin.

Log yozuvlari: Router va switch loglarini o'rganish orqali kutilmagan hodisalarni aniqlash va ular yuzasidan chora ko'rish. Trafik oqimini monitoring qilish: Real vaqt rejimida tarmoqdagi trafik hajmi va uning oqimini kuzatish, muhim segmentlarda tahlillar o'tkazish imkonini beradi.

Ushbu metodologiya yordamida turli xil xavfsizlik choralari sinovdan o‘tkazilib, tarmoqni optimallashtirish imkoniyatlari o'rganildi.

Natijalar:

ACL yordamida trafikni boshqarish. Cisco Packet Tracer orqali ACL sozlamalari orqali tarmoqda ruxsat berilgan va taqiqlangan trafik tahlil qilindi. Ushbu jarayon natijasida kiruvchi va chiquvchi trafikning nazorati mustahkamlandi, bu esa nomaqbul kirishlarni bloklash imkonini berdi.

VLAN va izolyatsiya. Tarmoq xavfsizligini oshirish maqsadida VLAN segmentatsiyasi amalga oshirildi. Bu usul yordamida bir tarmoqdagi turli bo'limlar o'rtasida trafik izolyatsiya qilinib, potentsial xavflar kamaytirildi.

NAT orqali IP-manzilni yashirish. NAT (Network Address Translation) yordamida ichki IP-manzillarni tashqi dunyodan yashirish amalga oshirildi. Bu, o'z navbatida, kiberhujumlarning oldini olishda muhim rol o'ynadi.

Simulyatsiya orqali hujumlarni aniqlash. Packet Tracer yordamida DDoS va boshqa kiberhujumlar simulyatsiya qilindi. Ushbu tajribalar orqali xavfsizlik siyosatidagi zaifliklar aniqlanib, ular bartaraf etildi.

Cisco Packet Tracer dasturi tarmoq xavfsizligi masalalarini o'rganish va amaliy sinovlar o'tkazish uchun samarali platformadir. Yuqorida keltirilgan amaliyotlar tarmoq xavfsizligini oshirishda muhim ahamiyatga ega bo'ldi. Ammo dasturda haqiqiy muhitga xos ayrim cheklovlar mavjud bo'lib, ularni hisobga olish zarur.

Xulosa: Cisco Packet Tracer tarmoq xavfsizligini ta'minlash bo'yicha ko'plab imkoniyatlarni taklif etadi. Ushbu dastur yordamida ACL, VLAN, NAT kabi xavfsizlik texnologiyalarini samarali sozlash va sinovdan o'tkazish mumkin. Ushbu vosita orqali foydalanuvchilar tarmoq xavfsizligini ta'minlashda muhim ko'nikmalarga ega bo'lishadi va murakkab muammolarni hal qilish uchun zaruriy tajribani shakllantiradilar. Biroq, Cisco Packet Tracer asosan o'quv va sinov muhiti sifatida ishlab chiqilgan bo'lib, haqiqiy tarmoq muhitlarining barcha murakkabliklarini aks ettirishga cheklovlarga ega. Shuning uchun, tarmoq xavfsizligini ta'minlashda dasturdan olingan natijalar haqiqiy muhitda qo'llashdan oldin qo'shimcha sinovlardan o'tkazilishi zarur. Kelajakda Cisco Packet Tracer imkoniyatlarini yanada kengaytirish va uni real muhitga yaqinroq qilib yaratish uchun quyidagilar amalga oshirilishi mumkin. Bunday o'zgarishlar Cisco Packet Tracer’ni nafaqat o'quv muhiti uchun, balki haqiqiy

tarmoq xavfsizligini rejalashtirish va boshqarishda ham muhim vosita sifatida foydalanish imkonini beradi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Sayfullayevich, X. K., & Qizi, A. H. R. (2024). CISCO MARSHRUTIZATORINI SOZLASH VA ISHLASH JARAYONINI TEKSHIRISH. Механика и технология, 4(17), 260-263.
2. Mulayam Singh. CISCO PACKET TRACER LABS // BookRix, 2019.
3. D.X.Tojimatov. Cisco packet tracer yordamida hususiy korxonalar uchun maxsus himoyalangan tarmoq kanali ishini loyihalash // Al-Farg‘oniy avlodlari” elektron ilmiy jurnali ISSN 2181-4252 Tom: 1-Son: № 3, 2023.
4. Mamazoidova G. "Cisco packet tracer" dasturida tarmoq texnologiyalari // RESEARCH AND EDUCATION ISSN: 2181-3191.- VOLUME 3, ISSUE 3, 2024. DOI: https://doi.org/10.5281/zenodo.10897400 .
5. Olimov.M., Raxmonova M. Cisco packet tracer dasturi hamda unda ishlash // so‘ngi ilmiy tadqiqotlar nazariyasi Respublika ilmiy-uslubiy jurnali 6-jild 6-son.
6. Moxistara, R., & Olimov, M. (2023). CISCO PACKET TRACER DASTURINI SOZLASH VA AMALIYOT O’TKAZISH. Journal of new century innovations, 30(4), 151-153.