ISSN 2181-3187

KOMPYUTER TARMOQLARI VA TARMOQ XAVFSIZLIGI

Xoliqulova Zarina Ikromovna
Uchquduq tuman Kasb-hunar maktabi
Maxsus fan (Kompyuter tarmoqlari va administratorlash)

ANNOTATSIYA

Ushbu maqolada kompyuter tarmoqlari, ularning tarkibiy qismlari va tasnifi tasvirlangan. Tarmoqlar mahalliy yoki keng bo'lishi mumkin, shuningdek, avtobus, halqa, yulduz va uyali kabi turli topologiyalarni o'z ichiga olishi mumkin. Matnda, shuningdek, axborot xavfsizligidagi zaiflik, tahdid va hujum tavsifi berilgan. Mijoz-server tarmoqlaridan foydalanishning afzalligi tasvirlangan, ammo ularning zaif nuqtasi butun tizimning ishdan chiqishiga olib kelishi mumkin bo'lgan serverdir. Matnda Internet, Intranet va Extranet kabi tarmoqlar ham tilga olinadi.

Kalit so‘zlar: tarmoq, tarmoq topologiyalari, OSI modeli, TCP/IP modeli, tarmoq vositalari. zaiflik, tahdid, hujum, ichki tahdid, tashqi tahdid, razvedka hujumlari, kirish hujumlari, zararli hujumlar, xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari.

KIRISH

Kompyuter tarmoqlari resurslarni almashish maqsadida bir necha kompyuterlarning birlashuvidan iborat. Fayllar, dasturlar, printerlar, modemlar va har qanday tarmoq uskunasi birgalikda foydalaniluvchi yoki taqsimlanuvchi resurslar bo‘lishi mumkin. Kompyuterlarni birlashtirish uchun ma’lumotlarni uzatuvchi turli xil vositalardan foydalaniladi: aloqa kanallari, telekommunikatsiya vositalari, retranslyatorlar va h. Mos tarmoq servislaridan foydalanish orqali turli xil tarmoq resurslarini taqdim etish vazifasi yuklatilgan tarmoq kompyuteri server deb ataladi. Tarmoq resurslaridan va turli tarmoq servislaridan foydalanish maqsadida serverga so‘rov yuboruvchi tarmoq qurilmalari mijozlar deb ataladi. Avtonom ishlovchi yoki mijoz sifatida tarmoqqa ulangan kompyuterni, odatda, ishchi stansiyasi deb atashadi.

ADABIYOTLAR TAHLILI VA TADQIQOT METODIKASI

Kompyuter tarmoqlarini quyidagicha tasniflash mumkin: - xududiy alomat bo‘yicha; - ma’murlash usuli bo‘yicha; - topologiya bo‘yicha. Hududiy alomat bo‘yicha lokal (LAN, Local Area Network) va global (WAN, Wide Area Network) hisoblash tarmoqlari farqlanadi. Global hisoblash tarmog‘i katta geografik muhitni qamrab olgan va tarkibida aloqaning magistral liniyalari yordamida birlashtirilgan ko‘plab hisoblash tarmoqlari va masofadagi kompyuterlar bo‘lgan hududiy taqsimlangan tizimdan iborat. Megapolis va region doirasida tashkil etilgan tarmoqlar mos holda shahar tarmog‘i (MAN, Metropolitan Area Network) va shaxsiy tarmoq (PAN, Personal Area Network) deb yuritiladi. Eng mashhur global tarmoq Internet

ISSN 2181-3187

TCP/IP protokollari steki bazasiga asoslangan megatarmoq hisoblanadi. Ba'zi adabiyotlarda "korporativ tarmoq" iborasi ishlatiladi. Bu ibora orqali turli texnik, dasturiy va informatsion prinsiplarda qurilgan bir necha tarmoqlarning birlashmasi tushuniladi. Megatarmoq Internet foydalanuvchilarini birlashtirish uchun ishlatiluvchi global tarmoq Ekstranet (extranet) deb yuritiladi. TCP/IP protokoli bazasida amalga oshirilgan, ammo megatarmoq Internetdan ajratilgan tarmoq Intranet (Intranet) deb ataladi. "Mijoz-server" tarmoqlarida markazlashgan arxitektura hisobiga ma'murlash va masshtablash funksiyalarini, xavfsizlikni va tiklanishni ta'minlash osongina amalga oshiriladi. Ammo, bunday tarmoqlarning zaif joyi (barcha markazlashgan tizimlardagi kabi) server hisoblanadi. Serverning buzilishi butun tizimning ishdan chiqishiga olib keladi. Undan tashqari, "mijoz-server" tarmoqni qurish uchun serunum kompyuter va mos operatsion server muhiti talab etiladi. Mos holda, bunday tarmoqlar professional tarmoq ma'muriga ega bo'lishi shart. Tarmoq topologiyasi bo'yicha umumiy shinali (bus), xalqasimon (ring), yulduzsimon (star), uyali (mesh) va aralash topologiyali tarmoqlar farqlanadi.

"Umumiy shina" topologiyasi bitta chiziq bo'yicha yotqizilgan tarmoqdan iborat. Kabel bitta kompyuterdan keyingi kompyuterga, so'ngra undan keyingisiga o'tadi Shinaning har bir uchida terminator (signalning akslanishini istisno qiluvchi) bo'lishi lozim. Shinaning bir uchi yerga ulanishi kerak. Shinali topologiya "passiv" hisoblanadi, chunki kompyuterlar signallarni regenerasiyalamaydi. Signal so'nishi muammosini hal etishda tarkorlagichlardan foydalaniladi. Shinaning uzilishi butun tarmoq ishlashining buzilishiga sabab bo'ladi (signalning akslanishi hisobiga). "Xalqasimon" topologiyada har bir kompyuter boshqa ikkita kompyuter bilan ulangan va signal aylana bo'yicha o'tadi. Xalqasimon topologiya "aktiv" hisoblanadi, chunki har bir kompyuter keyingi kompyuterga signal regeneratsiyalaydi. Topologiyaing kamchiligi sifatida masshtablashning murakkabligini hamda umumiy shina topologiyasidagidek uzilish sodir bo'lganida tarmoqning ishdan chiqishini va axborotning sust himoyalanganligini ko'rsatish mumkin. "Yulduzsimon" topologiya har bir kompyuterni markaziy konsentrator bilan ulash orqali tashkil etiladi. Ushbu topologiyaning afzalligi uzilishlarga barqarorligi (faqat bitta kompyuter uziladi), kompyuterlarni qo'shish imkoniyatining kamchiligi sifatida konsentratorga xarajatni ko'rsatish mumkin. "Uyali" topologiyada har bir kompyuter boshqalari bilan ulangan. Shu tufayli ulanishlarning uzilishiga eng yuqori barqarorlikka erishiladi. Topologiyaning kamchiligi sifatida kabelli ulanishlarga xarajatni ko'rsatish mumkin.

MUHOKAMA VA NATIJALAR

Tarmoq xavfsizligi muammolari. Axborot, Internet va kompyuter xavfsizligida aksariyat foydalanuvchilar tahdid, zaiflik va hujum tushunchalaridan tez-tez foydalanadilar. Biroq, aksariyat foydalanuvchilar tomonidan ularni almashtirish holatlari kuzatiladi. Zaiflik - "portlaganida" tizim xavfsizligini buzuvchi kutilmagan

ISSN 2181-3187

va oshkor bo‘lmagan hodisalarga olib keluvchi kamchilik, loyihalashdagi yoki amalga oshirishdagi xatolik. Taxdid (axborot xavfsizligiga taxdid) - axborot xavfsizligini buzuvchi bo‘lishi mumkin bo‘lgan yoki real mavjud xavfni tug‘diruvchi sharoitlar va omillar majmui. Hujum - bosqinchining operatsion muhitini boshqarishiga imkon beruvchi axborot tizimi xavfsizligining buzilishi. Hozirda tarmoq orqali amalga oshiriluvchi masalalarning ortishiga quyidagi omillar sabab bo‘lmoqda: Qurilma yoki dasturiy vositaning noto‘g ‘ri sozlanishi. Xavfsizlik bo‘shliqlari, odatda, tarmoqdagi qurilma yoki dasturiy vositalarning noto‘g‘ri sozlangani bois vujudga keladi. Masalan, noto‘g‘ri sozlangan yoki shifrlash mavjud bo‘lmagan protokoldan foydalanish tarmoq orqali yuboriluvchi maxfiy ma’lumotlarning oshkor bo‘lishiga sababchi bo‘lishi mumkin. Foydalanuvchilarning e’tiborsizligi. Eng oxirgi tarmoq foydalanuvchilarining e’tiborsizligi tarmoq xavfsizligiga jiddiy ta’sir qilishi mumkin. Inson harakatlari natijasida ma’lumotlarning yo‘qolishi, sirqib chiqishi kabi jiddiy xavfsizlik muammolari paydo bo‘lishi mumkin. Foydalanuvchilarni qasddan qilgan harakatlari. Xodim ishdan bo‘shab ketgan bo‘lsada, taqsimlangan diskdan foydalanish imkoniyatiga ega bo‘lishi mumkin. U mazkur holda tashkilot maxfiy axborotini chiqib ketishiga sababchi bo‘lishi mumkin. Bu holatga foydalanuvchilarning qasddan qilgan harakatlari sifatida qaraladi. Tarmoq xavfsizligiga tahdid turlari. Tarmoqqa qaratilgan tahdidlar odatda ikki turga ajratiladi. - ichki tahdidlar; - tashqi tahdidlar. Ichki tahdidlar. Kompyuter yoki Internetga aloqador jinoyatchiliklarning 80% ini ichki hujumlar tashkil etadi. Bu hujumlar tashkilot ichidan turib, xafa bo‘lgan xodimlar yoki g‘araz niyatli xodimlar tomonidan amalga oshirilishi mumkin. Ushbu hujumlarning aksariyati imtiyozga ega tarmoq foydalanuvchilari tomonidan amalga oshiriladi. Tashqi tahdidlar. Tashqi hujumlar tarmoqda allaqachon mavjud bo‘lgan zaiflik natijasida amalga oshiriladi. Hujumchi shunchaki qiziqishga, moddiy foyda yoki tashkilotni obro‘sini tushirish uchun ushbu hujumlarni amalga oshirishi mumkin. Mazkur holda hujumchi yuqori malakali va guruh bo‘lib hujumni amalga oshirishi mumkin. Tizimlashmagan tashqi tahdidlar odatda malakali bo‘lmagan shaxslar tomonidan turli tayyor buzish vositalari va skriptlar (senariylar) yordamida amalga oshiriladi. Ushbu hujum turlari odatda shaxs tomonidan o‘z imkoniyatini testlash yoki tashkilotda zaiflik mavjudligini tekshirish uchun amalga oshiriladi.

Tarmoqqa qaratilgan hujumlar sonini ortib borishi natijasida tashkilotlar o‘z tarmoqlarida xavfsizlikni ta’minlashda qiyinchiliklarga duch kelishmoqda. Bundan tashqari, hujumchilarning yoki xakerlarning tarmoqqa kirishning yangidan - yangi usullaridan foydalanishlari, ular motivlarining turlichaligi bu murakkablikni yanada oshiradi. Tarmoq hujumlari odatda quyidagicha tasniflanadi.

XULOSA

Xulosa qilib aytganda, razvedka hujumlari asosiy hujumni oson amalga oshirish maqsadida tashkilot va tarmoq haqidagi axborotni to‘playdi va bu hujumchilarga

ISSN 2181-3187

mavjud bo‘lishi mumkin bo‘lgan zaifliklarni aniqlash imkonini beradi. Razvedka hujumining asosiy maqsadi quyidagi toifaga tegishli ma’lumotlarni yig‘ish hisoblanadi: - tarmoq haqidagi; - tizim haqidagi; - tashkilot haqidagi. Razvedka hujumlarining quyidagi turlari mavjud: Aktiv razvedka hujumlari. Aktiv razvedka hujumlari asosan portlarni va operaesion tizimni skanerlashni maqsad qiladi. Buning uchun, hujumchi maxsus dasturiy vositalardan foydalangan holda, turli paketlarni yuboradi. Masalan, maxsus dasturiy vosita router va 137 tarmoqlararo ekranga boruvchi barcha IP manzillarni to‘plashga yordam beradi. Passiv razvedka hujumlari. Passiv razvedka hujumlari trafik orqali axborotni to‘plashga harakat qiladi. Buning uchun hujumchi sniffer deb nomlanuvchi dasturiy vositadan foydalanadi. Bundan tashqari, hujumchi ko‘plab vositalardan foydalanishi mumkin. Foydalanilgan adabiyotlar

FOYDALANILGAN ADABIYOTLAR

1. Turdimatov M., Mirzaev J. Ахборотни ҳимоялашда ёпиқ виртуал қобиғини лойихалашни математик модели //Science and innovation. – 2022. – Т. 1. – №. A6. – С. 430-436.
2. Jurayev N. M., Xomidova N. Y., Yuldasheva X. X. Security analysis of urban railway systems: the need for a cyber-physical perspective //Cutting edge-science. – 2020. – Т. 206.
3. Nabijonov, R., & Ergasheva, A. (2023). Masofaviy o‘qitish tizimlarini ta’lim sifatini oshirishdagi o‘rni. Engineering Problems and Innovations. извлечено от https://fer-teach.uz/index.php/epai/article/view/44
4. Nabijonov, R., & Ergasheva, A. (2023). Media portallar yaratishda vue.js operatorlari tahlili. Engineering Problems and Innovations. извлечено от https://fer-teach.uz/index.php/epai/article/view/52
5. Nabijonov, R., & Ergasheva, A. (2023). Deykstra-Prim algoritmini amaliy tahlil qilish. Engineering Problems and Innovations. извлечено от https://fer-teach.uz/index.php/epai/article/view/71