Impact Factor: 9.9 ISSN-L: 2544-980X

Operatsion Tizimlarda Masofadan Xavfsiz Boshqarish Texnologiyalari

Turdimatov Mamirjon Mirzayevich [1]

Annotatsiya: Ushbu maqolada tarmoq qurilmasi kommutatorlarga masofadan kirish usullari, masofaviy ish stoli protokoli, ularni boshqarish, shuningdek VPN tarmoq va SSH protokoli xususiyatlari, uning afzalliklari va kamchiliklari o'rganilgan. Natijada SSH protokoli afzalliklari, kriptotahlil nuqtai nazaridan ishonchliligi, qo'llanilgan shifrlash algoritmi va kalitlarni bardoshligi, tarmoq adminstratorini autentifikatsiya qilish jarayoni ishlab chiqildi. Laboratoriya sharoitida tarmoq qurulmasiga masofadan xavfsiz ulanish va boshqarish sinab ko'rilgan.

Kalit so'zlar: tarmoq, protokol, kommutator, SSH, autentifikatsiya, OSI modeli, xavfsiz aloqa, TCP, shifrlash , kriptografiya, RDP.

Kirish. Masofaviy kirish kompyuter, tarmoq yoki boshqa manbalarga uzoq joydan kirish imkoniyatini anglatadi. Bu foydalanuvchilarga xuddi shu joyda jismonan mavjud bo'lgandek ishlash imkonini beradi.

Masofaviy kirishning asosiy tushunchalaridan biri masofaviy ish stoli protokoli (Remote Desktop Protocol (RDP)) - bu Microsoft tomonidan ishlab chiqilgan xususiy protokol bo'lib, foydalanuvchilarga tarmoq ulanishi orqali boshqa kompyuterga ulanish imkonini beradi. Masalan, ko'pincha korporativ tizimlarda axborot xavfsizligi tahdidlari va zaif tomonlarini tavsiflash va tahlil qilishga bag'ishlangan bo'ladi. Tahdidlar va zaifliklarni tasniflash muammosi ochiq tizimlarning o'zaro bog'lanishi (RM ISO/OSI) uchun mos yozuvlar modeliga muvofiq ishlar ustida tadqiqotlar olib borilgan[1-3]. Misol tariqasida, tarmoq hujumlari tarmoq aloqa protokollari zaifliklaridan foydalanadigan tahdid amalga oshirilgan darajada tahlil qilingan[3].

Odatda masofaviy texnik yordam va virtual ish joylari uchun ishlatiladi.

Adabiyotlar tahlili va metodologiya.

Korxona va tashkilotlarda axborot xavfsizligini ta'minlashning zamonaviy usullari bilan chet el olimlaridan Mark Ciampa, Tim Boyles, Emad S. Hassan, Joseph Migga Kizza rus olimlaridan V.F.Shangin, Д.А.Боротник, Е.Л.Кротова O.Kazarin, A.A.Biryukov, B.Xorev, N.G.Miloslavskaya, M.Yu.Senatorov va boshqalar, o'zbek olimlaridan P.F.Xasanov, Z.Karimov, S.K.Ganiyev, A.A.Ganiyev, Z.T.Xudoyqulov, F.M.Muxtarov, Sh.A.Umarovlar tadqiqotlar olib borishmoqda[8-10].

Bu erda asosan xavfsizlik masalasi birinchi o'rinda turadi RDP shifrlash va kuchli autentifikatsiya usullari yordamida himoyalanishi mumkin. Masalan, virtual shaxsiy tarmoq (VPN) xavfsizroq tarmoq, masalan, internet orqali xavfsiz, shifrlangan ulanishni yaratadi va uzoq joylardan korporativ tarmoqqa xavfsiz kirishni ta'minlash uchun ishlatiladi. Uning afzalliklari VPN-lar masofaviy foydalanuvchi va tarmoq o'rtasida uzatiladigan ma'lumotlarni shifrlash orqali ma'lumotlar maxfiyligi va xavfsizligini ta'minlaydi[4].

Buni xosil qilish uchun xavfsiz qobiq (SSH) yaratish zarur. SSH - bu himoyalanmagan tarmoq orqali tarmoq xizmatlarini xavfsiz ishlatish uchun kriptografik tarmoq protokoli bo'lib, u tez-tez xavfsiz masofaviy kirish va boshqa xavfsiz tarmoq xizmatlari uchun ishlatiladi. Xususiyatlaridan biri SSH kuchli autentifikatsiya va xavfsiz bo'lmagan kanal orqali xavfsiz aloqani ta'minlaydi [3].

[1] Texnika fanlari nomzodi, dotsent, Muhammad al-Xorazmiy nomidagi TATU Farg'ona filiali "Axborot xavfsizligi"kafedrasi dotsenti. Fasg'ona,O'zbekiston

Masofaviy kirish dasturlaridan TeamViewer, AnyDesk, LogMeIn va boshqalarni olish mumkin. Bu vositalar foydalanuvchilarga dunyoning istalgan nuqtasidan masofaviy kompyuterga kirish va boshqarish imkonini beradi. Ular ko'pincha fayl uzatish, chat funksiyalari va ko'p platformali yordamni ta'minlaydi.

Bulutga asoslangan xizmatlardan foydalanishda, foydalanuvchilar istalgan joydan bulutda joylashgan resurslarga kirishlari va ularni boshqarishlari mumkin. Masalan, amazon Web Services (AWS), Google Cloud Platform (GCP) va Microsoft Azure kabi bulutli xizmatlar virtual mashinalar va boshqa resurslarga masofadan kirishni taklif qiladi. Uning afzalliklari kengaytirilishi, moslashuvchanligi va jismoniy jihozlarga bo'lgan ehtiyojning kamayishiga olib keladi.

Xavfsizlik masalalari autentifikatsiya ko'p faktorli autentifikatsiya (MFA) kabi kuchli autentifikatsiya usullari masofaviy kirishni ta'minlash uchun juda muhimdir.

Biznesning uzluksizligi xodimlar kutilmagan holatlar tufayli ofisga jismoniy kirish imkoniga ega bo'lmasa ham, operatsiyalar davom etishini ta'minlaydi.

Masofaviy ish stoli protokoli- remote desktop protocol (RDP) mijoz-server arxitekturasidan foydalanadi, bunda mijoz tomoni ilovasi RDP ruxsati yoqilgan tarmoq orqali kompyuterning maqsadli IP-manzilini yoki xost nomini belgilash uchun ishlatiladi. RDP masofaviy ruxsati yoqilgan maqsadli kompyuter server hisoblanadi. Shuni ta'kidlash kerakki, RDP sukut bo'yicha mantiqiy portni tinglaydi. Shuni yodda tutishimiz kerakki, IP-manzil tarmoqdagi kompyuter uchun mantiqiy identifikator sifatida ishlatiladi va mantiqiy port dasturga tayinlangan identifikator hisoblanadi. Oddiyroq qilib aytganda, biz tarmoq quyi tarmog'ini shahardagi ko'cha (korporativ tarmoq), shu ko'chadagi uy sifatida xostga tayinlangan ushbu kichik tarmoqdagi IP manzil va mantiqiy portlarni deraza-eshiklar sifatida ko'rib chiqishimiz mumkin[5].

So'rov (paket ichida inkapsullangan) IP manzili orqali maqsadli kompyuterga yetib borgach, so'rov ushbu so'rovda ko'rsatilgan port (paket ichidagi sarlavha sifatida kiritilgan) asosida kompyuterda joylashgan dasturga yo'naltiriladi. IP-manzillash va protokol inkapsulyatsiyasi tarmoqqa kirish modulida batafsil yoritilgan. Tarmoq nuqtai nazaridan, ushbu modulda biz faqat har bir kompyuterda tarmoq orqali muloqot qilish uchun tayinlangan IP-manzil borligini va maqsadli kompyuterlarda joylashgan ilovalar ma'lum mantiqiy portlarni tinglashini tushunishimiz kerak.

Yuqoridagi masalani amaliy echimi sifatida Linux yoki Windows bilan ishlaydigan hujum xostidan Windows tizimiga ulanish uchun RDP dan foydalanishimiz mumkin. Agar biz Windows xostiga ulansak, biz Remote Desktop Connection(mstsc.exe) deb nomlangan o'rnatilgan RDP mijoz dasturidan foydalanamiz. Asosiy foydalanishni ko'rish uchun quyidagilarni bajarishimiz kerak, masalan tizimda “Уаленный рабочий стол” ni ishga tushiramiz, so’ngra

RDP ni tezkor chiqarish uchun klaviaturadan win+R bosiladi va **mstsc** yoziladi va enter bosiladi. So’ngra kerakli komputerlar IP adreslariga bog’lanib ishni davom ettirish mumkin.

Buning ishlashi uchun maqsadli Windows tizimida masofaviy kirishga allaqachon ruxsat berilishi kerak. Odatda Windows operatsion tizimlarida masofaviy kirishga ruxsat berilmaydi, lekin HTB Akademiyasi jamoasi VPN orqali Akademiya laboratoriyalariga ulangandan so'ng RDP kirishiga ruxsat berish uchun Windows tizimiga maqsadli sozladi.

Masofaviy ish stoli ulanishi bizga ulanish profillarini saqlashga ham imkon beradi. Bu IT administratorlari orasida keng tarqalgan odat, chunki bu masofaviy tizimlarga ulanishni qulayroq usuli.

Ko'pgina boshqa Masofaviy ish stoli mijoz ilovalari mavjud, ulardan ba'zilari ushbu maqolada keltirilgan masofaviy ish stoli mijozlari deb nomlangan. Biz ushbu moduldagi har bir masofaviy ish stoli mijoz ilovasini qamray olmaymiz.

Masalan, xfreerdp dan foydalanishni ko’rib chiqamiz.

Linux-ga asoslangan hujum uyasidan biz Windows tizimiga masofadan kirish uchun xfreerdp deb nomlangan vositadan foydalanishimiz mumkin. Foydalanish qulayligi, xususiyatlar to'plami, buyruq qatori yordam dasturi va samaradorligi tufayli biz bir nechta modullarda xfreerdpdan

foydalanayotganimizni sezish mumkin. Biz asosan Pwnbox-dan foydalanib buyruq satrida xfreerdp buyruqlarini nusxalashimiz va joylashtirishimiz mumkin, shuning uchun Remote Desktop Protocol (RDP) Microsoft tomonidan ishlab chiqilgan xususiy protokol bo'lib, foydalanuvchilarga tarmoq ulanishi orqali boshqa kompyuterga ulanish imkonini beradi. Ushbu protokol masofaviy foydalanuvchiga masofaviy kompyuterga xuddi uning oldida o'tirgandek kirish va boshqarish imkonini beradi.

Natija. Demak, RDPning ba'zi asosiy jihatlarini keltirib o’tamiz. Masalan, RDP ning asosiy xususiyatlari Grafik interfeys mavjud, ya’ni RDP foydalanuvchiga mahalliy sichqoncha va klaviatura yordamida masofaviy ish stoli bilan o'zaro aloqa qilish imkonini beruvchi grafik interfeysni taqdim etadi.

Displey chiqishini masofaviy kompyuterdan mahalliy qurilmaga uzatadi va masofaviy boshqaradi. Foydalanuvchilar ilovalarni ishga tushirish, fayllarni boshqarish va tizim sozlamalarini sozlash kabi vazifalarni masofaviy kompyuterda bajarishi mumkin. U bir nechta masofaviy seanslarni qo'llab-quvvatlaydi, bu turli foydalanuvchilarga bir vaqtning o'zida bir xil masofaviy qurilmaga ulanish imkonini beradi.

Xavfsizligini saqlash masalasi RDP mijoz va masofaviy kompyuter o'rtasida uzatiladigan ma'lumotlarni himoya qilish uchun kuchli shifrlashdan foydalanadi, bu esa maxfiy ma'lumotlarning himoyalanganligini ta'minlaydi.

Autentifikatsiya esa faqat vakolatli foydalanuvchilar masofaviy kompyuterga kirishini ta'minlash uchun turli xil autentifikatsiya usullarini qo'llab-quvvatlaydi.

Yana Active Directory kabi Windows autentifikatsiya mexanizmlari bilan integratsiyalanadi. Resurs almashishi mahalliy va uzoq kompyuterlar o'rtasida printerlar, drayvlar va almashish buferi kabi resurslarni almashish imkonini beradi va foydalanuvchilar mahalliy qurilmalarni (masalan, USB drayvlar) masofaviy seansga yo'naltirishlari mumkin.

Ta'lim tizimida o'qituvchilar masofadan turib dasturlarni namoyish qilishlari yoki talabalarga amaliy mashg'ulotlar o'tkazishlari mumkin. Tavsiya sifatida xavfsizlik devori qoidalari va tarmoq xavfsizlik guruhlarini sozlash orqali RDP serverlariga kirishni cheklang, hamda kirish nazoratini RDP ruxsatiga ega bo'lgan foydalanuvchilar sonini cheklang va sessiya o'rnatishdan oldin foydalanuvchilarni oldindan autentifikatsiya qilish uchun tarmoq darajasidagi autentifikatsiyadan (NLA) foydalanishlari mumkin.

Monitoring olib boring, ya’ni har qanday noodatiy harakatlar yoki ruxsatsiz kirish urinishlari uchun jurnalga yozishni yoqing va RDP ulanishlarini kuzatib boring.

Xulosa. Ma'lumki, tarmoq qurilmalariga ulanish va masofadan boshqarishda 100% xavfsizlikka erishib bo‘lmaydi. Ammo turli xil xavfsizlik usuillari, protokollaridan samarali foydalanish orqali tarmoq xavfsizlikka tahdidlar ehtimolini sezilarli darajada kamaytirish mumkin.

Yuqorida ilmiy tadqiqot ishida tarmoq qurilmalariga, jumladan kommutatorga masofandan bog‘lanishda administrator ma’lumotlarini xavfsizligini ta’minlash SSH protokoli orqali bajarilishi samarali ekanligini ko’rsatdi. Tarmoq qurilmalrini boshqarish uchun SSH protokolidan foydalanishni Cisco kompaniyasi ham tavsiya etgan[6,7].

Tajribalar ko’rsatadiki, masofaviy ish stoli protokoli kompyuterlarga masofadan kirish va boshqarish uchun mustahkam va keng qo'llaniladigan yechim. Uning xususiyatlari va imkoniyatlari uni masofaviy ishlashdan tortib IT boshqaruvigacha bo‘lgan turli ilovalarni ideal boshqaradi. Xavfsizlik va ishlash bo'yicha eng yaxshi amaliyotlarni tatbiq etish orqali tashkilotlar xavfsizlikni ta'minlash bilan birga mahsuldorlik va moslashuvchanlikni oshirish uchun RDP dan foydalanishlari mumkin.

Bu erda masofaviy kirish asosan shaxslar va tashkilotlar uchun moslashuvchanlik va samaradorlikni oshiradigan kuchli qobiliyatdir. Xavfsizlik va ishlashning eng yaxshi amaliyotlarini tushunish va amalga oshirish orqali masofaviy kirish zamonaviy ish muhitlari uchun xavfsiz va samarali yechim bo'lishi mumkin. Bu imkoniyat Xfreerdp Windows uchun ishlab chiqilmagan bo'lsa-da, siz uni WSL

orqali yoki uni manbadan kompilyatsiya qilish orqali ishlatishingiz mumkin. WSL dan foydalanish odatda osonroq va soddaroq, ayniqsa Xming kabi X serverlari mavjudligi bilan manbadan kompilyatsiya qilish ko'proq mahalliy tajribani beradi, lekin ko'proq qadamlar va sozlashni talab qiladi.

ADABIYOTLAR

1. R.X.Djurayev, Sh.Yu.Djabbarov, B.M.Umirbekov. Tarmoq protokollari. T.: «Aloqachi», 2018, 144 b.
2. Д.А.Боротник, Е.Л.Кротова. Настройка безопасного удаленного управления маршрутизатором Cisco с помощью протокола SSH.[Elektron resurs]. URL: https://cyberleninka.ru/article/n/nastroyka-bezopasnogo-udalennogo-upravleniya-marshrutizatorom-cisco-s-pomoschyu-protokola-ssh.
3. M.M. Turdimatov, J.B. Mirzayev. Tarmoq qurilmasi kommutatorga masofadan xavfsiz boshqarishni nazoratlash usullari. FarPI ilmiy - texnika, jurnali. Farg'ona- 2023, T.27. maxsus. son №2.
4. M.M. Turdimatov. Buzish va himoyalash prinsiplari. O'quv qo'llanma . Farg'ona "ClassiC" nashriyoti -2023 yil. 250 b.
5. S.K.Ganiyev, A.A.G aniyev, Z.T.Xudoyqulov. Kiberxafsizlik asoslari: o'quv qo'llanma, -T.: "Nihol print" OK, 2021. - 224 b.
6. С.К. Ганиев, З.Т. Худойкулов, Н.Б. Насруллаев. Основы кибербезопасности: учебное пособие, -Т.: «Mahalla va oila nashriyoti», 2021. -240 с.
7. В.Ф.Шангин. "Информационная безопасность компьютерых систем и сетей", Учебное пособие. Изд. дом "Форум" ИНФРА-М.:2018 г.
8. Руководство Cisco по усилению защиты устройств Cisco IOS [Электронный ресурс]. – 2013. – 28 июля. – URL: http://www.cisco.com/cisco/web/support/RU/106/1068/1068484_21.pdf (дата обращения: 16.04.2016).
9. М.М. Турдиматов. Замонавий дастурий воситалар асосида криптография фанини ўзлаштириш усуллари. ФарПИ илмий-техника журнали. Фарғона-2022. Том 26. №1.99-104 бетлар.
10. M.M. Turdimatov. Kriptografik transformatsiyalarning zamonaviy usullari. Международная научно-техническая конференция «Практическое применение технических и цифровых технологий и их инновационных решений», ТАТУФФ, Фергана, 4 мая 2023 г. 127-131с.
11. Sh.Umarov, M.Turdimatov, A.Abduqodirov, M.Khusanova. Research on properties of crypto stability criteria of the hash function algorithm. AIP Conf. Proc. 3244, 030004 (2024). https://doi.org/10.1063/5.0241424.
12. F.Muxtarov, X Sadirova. Korxonada axborot xavfsizligini ta'minlashning zamonaviy usullari. Engineering problems and innovations, 2023.
13. F.Muxtarov. Axborot xavfsizligida veb-filtrlashning vazifalari va muammolari. Research and implementation, 2023.