TARMOQLARARO EKRANLARNING ISHLASH XUSUSIYATLARI

Ilmiy rahbar: i.f.d., PhD ***F.T.Jumayev***
Kompyuter tizimlari va ularning dasturiy ta'minoti
yo'nalishi magistranti ***Sottorov Baxtiyor Ravshan o'g'li***

Annotatsiya: Ushbu maqolada tarmoqlararo ekranlarning ishlash xususiyatlari va tarmoq trafiklari tahlili keltirilgan.
Kalit so'zlar: tarmoqlararo ekranlarning ishlash xususiyatlari, tarmoq trafiklari tahlili, yolg'on obyekt

Barcha hujumlar internet ishlashi prinsiplarining qandaydir chegaralangan soniga asoslanganligi sababli masofadan bo'ladigan namunaviy hujumlarni ajratish va ularga qarshi qandaydir kompleks choralarni tavsiya etish mumkin. Bu choralar, haqiqatdan, tarmoq xavfsizligini ta'minlaydi. Internet protokollarining mukammal emasligi sababli tarmoqdagi axborotga masofadan bo'ladigan asosiy namunaviy hujumlar quyidagilar:

- tarmoq trafigini tahlillash;
- tarmoqning yolg'on obyektini kiritish;
- yolg'on marshrutni kiritish;
- xizmat qilishdan voz kechishga undaydigan hujumlar.

Tarmoq trafigini tahlillash. Serverdan Internet tarmog'i bazaviy protokollari FTP (Fayllarni uzatish protokoli) va TELNET (Virtual terminal protokoli) bo'yicha foydalanish uchun foydalanuvchi identifikatsiya va autentifikatsiya muolajalarini o'tishi lozim. Foydalanuvchini identifikatsiyalashda axborot sifatida uning identifikatori (ismi) ishlatilsa, autentifikatsiyalash uchun parol ishlatiladi. FTP va TELNET protokollarining xususiyati shundaki, foydaluvchilaming paroli va identifikatori tarmoq orqali ochiq, shifrlanmagan ko'rinishda uzatiladi. Demak, internet xostlaridan foydalanish uchun foydalanuvchining ismi va parolini bilish kifoya. Axborot almashinuvida Internetning masofadagi ikkita uzeli almashinuv axborotini paketlarga ajratadi. Paketlar aloqa kanallari orqali uzatiladi va shu paytda ushlab qolinishi mumkin. FTP va TELNET protokollarining tahlili ko'rsatadiki, TELNET parolni simvollarga ajratadi va parolning har bir simvolini mos paketga joylashtirib, bittalab uzatadi, FTP esa, aksincha, parolni butunligicha bitta paketda uzatadi. Parollar shifrlanmaganligi sababli paketlaming maxsus skaner-dasturlari yordamida foydalanuvchining ismi va paroli bo'lgan paketni

ajratib olish mumkin. Shu sababli, hozirda ommaviy tus olgan ICQ (Bir lahzali almashish xizmati) dasturi ham ishonchli emas. ICQning protokollari va axborotlarni saqlash, uzatish formatlari ma'lum va demak, uning trafigi ushlab qolinishi va ochilishi mumkin. Asosiy muammo almashinuv protokolida. Bazaviy tatbiqiy prokollarning TCP/IP oilasi ancha oldin (60-yiIlaming oxiri va 80-yillarning boshi) ishlab chiqilgan va shundan beri umuman o'zgartirilmagan. O'tgan davr mobaynida taqsimlangan tarmoq xavfsizligini ta'minlashga yondashish jiddiy o'zgardi. Tarmoq ulanishlarini himoyalashga va trafikni shifrlashga imkon beruvchi axborot almashinuvining turli protokollari ishlab chiqildi. Ammo bu protokollar eskilarining o'rnini olmadi (SSL bundan istisno) va standart maqomiga ega bo'lmadi. Bu protokollarning standart bo'lishi uchun esa tarmoqdan foydalanuvchilarning barchasi ularga o'tishlari lozim. Ammo, internetda tarmoqni markazlashgan boshqarish bo'lmaganligi sababli, bu jarayon yana ko'p yillar davom etishi mumkin. Tarmoqning yolg'on obyektini kiritish. Har qanday taqsimlangan tarmoqda qidirish va adreslash kabi "nozik joylari" mavjud. Ushbu jarayonlar kechishida tarmoqning yolg'on obyektini (odatda bu yolg'on xost) kiritish imkoniyati tug'iladi. Yolg'on obyektning kiritilishi natijasida adresatga uzatmoqchi bo'lgan barcha axborot aslida niyati buzuq odamga tegadi. Taxminan, buni tizimingizga, odatda elektron pochtani jo'natishda foydalanadigan provayderingiz server adresi yordamida kirishga kimdir uddasidan chiqqani kabi tasavvur etish mumkin.

Tarmoqlararo ekranlarning ishlash xususiyatlari. Tarmoqlararo ekran (TE) - *Brandmauer* yoki *firewall sistemasi* deb ham ataluvchi tarmoqlararo himoyaning ixtisoslashtirilgan kompleksi. Tarmoqlararo ekran umumiy tarmoqni ikki yoki undan ko'p qismlarga ajratish va ma'lum paketlarini chegara orqali umumiy tarmoqning bir qismidan ikkinchisiga o'tish shartlarini belgilovchi qoidalar to'plamini amalga oshirish imkonini beradi.
Odatda, bu chegara korxonaning korporativ (lokal) tarmog'i va Internet global tarmoq orasida o'tkaziladi. Tarmoqlararo ekranlar garchi korxona lokal tarmog'i ulangan korporativ intratarmog'idan qilinuvchi hujumlardan himoyalashda ishlatilishi mumkin bo'lsa-da, odatda ular korxona ichki tarmog'ini Internet global tarmoqdan suqilib kirishdan himoyalaydi. Aksariyat tijorat tashkilotlari uchun tarmoqlararo ekranlarning o 'rnatilishi, ichki tarmoq xavfsizligini ta'minlashning zaruriy sharti hisoblanadi. Ruxsat etilmagan tarmoqlararo foydalanishga qarshi ta'sir ko'rsatish uchun tarmoqlararo ekran ichki tarmoq hisoblanuvchi tashkilotning

himoyalanuvchi tarmog'i va tashqi g ‘anim tarmoq orasida joylanishi lozim . Bunda bu tarmoqlar orasidagi barcha aloqa faqat tarmoqlararo ekran orqali amalga oshirilishi lozim. Tashkiliy nuqtayi nazaridan tarmoqlararo ekran himoyalanuvchi tarmoq tarkibiga kiradi. Ichki tarmoqning ko‘pgina uzellarini birdaniga himoyalovchi tarmoqlararo ekran quyidagi ikkita vazifani bajarishi kerak:
- tashqi (himoyalanuvchi tarmoqqa nisbatan) foydalanuvchilarning korporativ tarmoqning ichki resurslaridan foydalanishini chegaralash. Bunday foydalanuvchilar qatoriga tarmoqlararo ekran himoyalovchi ma’lumotlar bazasining serveridan foydalanishga urinuvchi sheriklar, masofadagi foydalanuvchilar, xakerlar, hatto kompaniyaning xodimlari kiritilishi mumkin;
- himoyalanuvchi tarmoqdan foydalanuvchilarning tashqi resurslardan foydalanishlarini chegaralash. Bu masalaning yechilishi, masalan, serverdan xizmat vazifalari talab etmaydigan foydalanishni tartibga solishga imkon beradi.

Hozirda ishlab chiqarilayotgan tarmoqlararo ekranlarning tavsiflariga asoslangan holda, ulami quyidagi asosiy alomatlari bo‘yicha turkumlash mumkin:
OS1 modeli sathlarida ishlashi bo ‘yicha.
- paketli filtr (ekranlovchi marshrutizator - screening router);
- seans sathi shlyuzi (ekranlovchi transport);
-tatbiqiy sath shlyuzi (application gateway);
- ekspert sathi shlyuzi (stateful inspection firewall).
Ishlatiladigan texnologiya bo 'yicha:
- protokol holatini nazoratlash (Stateful inspection);
- vositachilar modullari asosida (proxy);
Bajarilishi bo 'yicha:
- apparat-dasturiy;
- dasturiy;
Ulanish sxemasi bo 'yicha;
- tarmoqm umumiy himoyalash sxemasi;
- tarmoq segmentlari himoyalanuvchi berk va tarmoq segmentlari himoyalanmaydigan ochiq sxema;
- tarmoqning berk va ochiq segmentlarini alohida himoyalovchi sxema.
Trafiklarni filtrlash Axborot oqimlarini filtrlash, ularni ekran orqali, ba’zida qandaydir o‘zgartirishlar bilan o ‘tkazishdan iborat. Filtrlash, qabul qilingan xavfsizlik siyosatiga mos keluvchi, ekranga oldindan yuklangan qoidalar asosida

amalga oshiriladi. Shu sababli, tarmoqlararo ekranni axborot oqimlarini ishlovchi filtrlar ketma-ketligi sifatida tasavvur etish qulay.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

1. Аверченков В.И. Системы защиты информации в ведущих зарубежных странах: Учебное пособие. – Брянск, 2007.
2. Алферов А.П., Зубов А.Ю., Кузьмин А.С, Черемушкин А.В. Основы криптографии: Учебное пособие. – М., 2002
3. Арипов М. , Пудовченко Ю. Е., Арипов М. Основы Интернет. – Т., 2003.
4. Безбогов А.А. Методы и средства защиты компьютерной информации. Учебное пособие. – Тамбов, 2006.
5. Давыдов А.С., Маслова Т.В. Информационные технологии в деятельности органов внутренних дел: Учебное пособие. – Челябинск, 2007.
6. Зайцев А.П., Голубятников И.В., Мещеряков Р.В. Программноаппаратные средства обеспечения информационной безопасности: Учебное пособие. – М., 2006.
7. Информационные технологии управления в органах внутренних дел: Учебник / Под ред. доцента Ю.А. Кравченко. – М., 1998.
8. Мельников В.П. и др. Информационная безопасность и защита информации: Учебое пособие. – М., 2008.
9. Казиев В.М. Введение в правовую информатику. – http://www. intuit.ru.