Bajaruvchi: Hasanov Kamol

Axborot tizimlarining matematik va Dasturiy ta'mi-noti yo'nalishi Axborot tizimlari Oraliq Nazorat Bilet №24

1. IDS va IPS tizimi, Brandmauerlar
2. Aloqa kanallarida axborot xafsizligi

Javoblar

① Intrusion Detection System (IDS):

Tajovuzkorlar sizning tarmog'ingizdagi ma'lumotlar-ga kirish yoki o'zlash uchun ma'lumot kiber-hujumdagi foydalanayotganligini ko'rsatuv-chi belgilarni aniqlash uchun tarmoq trafik-ini tahlil qilish va nazorat qilish.
IDS tizimlari xavfsizlik siyosatini buzish, zararli dastur va port skanerlari kabi bir nechta xatti-harakatlarni aniqlash uchun joriy tarmoq faoliyatini ma'lumot bo'lgan tahdidlar bazasi bilan taqqoslaydi.

Intrusion Prevention Systems (IPS): Tarmoq-
-ning xavfsizlik devori bilan bir xil hud-
-udida, tashqi dunyo va ichki tarmoq o'rtasida
yashaydi. IPS xavfsizlik profiliga asoslangan
holda tarmoq ~~tar~~ trafigini faol ravishda
rad etadi agar bu paket ma'lumot xav-
-fsizlik tahdidini bildirsa.

IDS va IPS tarmoq infratuzilmasining
ikkala qismidir. IPS va IPS tarmoq pak-
-etlarini kiberhujumlarning ma'lum imzolari
o'z ichiga olgan kiber tahdidlar bazasi
bilan taqqoslaydi va mos keladigan paket-
-larni belgilaydi. Ularning asosiy farqi
shundaki, IPS - bu monitoring tizimi, IPS
-bu boshqarish tizimi. IPS hech qanday
tarzda tarmoq paketlarini o'zgartirmay
-di, IPS esa paketning tarkibiga qarab
Paketni etkazib berishga to'siqlik qiladi.
masalan, xavfsizlik devori IP-manzil
ozgali trafikni qanday qilib olishni

oladi. Ko'pgina IDS / IPS sotuvchilari ushbu ikkita o'xshash tizimlarning funk-siyalarini bitta birlikka birlashtirgan Unified Threat Management (UTM) texnologiyasi yaratish uchun xavsizlik devorlari bilan yangi IPS tizimlar-ini birlashtirdilar. Ba'zi tizimlar IPS va IPS funksiyalarini bitta birlikd ta'minlaydi. Ikkala IDS / IPS ham tarmoq paketlarini o'qiydi va tarkibini ma'lum tahdidlar ma'lumotlar bazasi bilan taqqos-laydi. Ularning orasidagi asosiy farq key-inchalik nima bilishidir. IPS - bu o'z - o'zidan chora ko'rmaydigan aniqlash va nazorat qilish vositalaridir. IPS - qaid-alari to'plami asosida paketni qabul qil-adigan yoki rad etadigan boshqaruv tizimi.

IPS inson yoki boshqa tizim nati-jalarini ko'rib chiqishi va unda kerak

qanday choralar ko'rishini talab qilish kerak, bu har kuni ishlab chiqarilgan tarmoq trafigi miqdoriga qarab doimiy ish bo'lishi mumkin. IDS ólimdan keyin CSIRT-ni xavf-sizlik bilan bog'liq hodisalarni tekshirish jarayonida foydalanish uchun yaxshiroq tibbiy variantni yaratadi.

Boshqa tomondan, IPS ning maqsadi xavfli paketlarni ushlash va ularni maqsa-dga yetmasdan tashlab yuborishdir. Bu IDS dan kora passivroq, shunchaki ma'lumot-lar bazasini tahdid ma'lumotlari bilan muntazam yangilash turishni talab qiladi.

IPS va IPS kiberhujum ma'lumotlar bazalari kabi samaralidir. Yovvoyi tabiat-da yangi hujum sodir bo'lganda va yoki hujum haqida ma'lumotlar bazasida bol-maganida ularni yangilab turish va gólda turatishlar kiritishga tayyor bo'ling.

Nima uchun IDS va IPS kiberxavfsizlik uchun juda muhimdir.

Byudjet cheklovlari bilan va korporativ siyosat bilan kurashishni davom ettirish paytida xavfsizlik guruhlari ma'lumotlar bazalashi va muvofiqlik gardmlari tobora ~~sa~~ osib borayotgan tahdidga duch kelmoqda-lar. IDS / IPS texnologiyasi kiberxavfsizlik strategiyasining o'ziga xos va muhim-ishlarini gamrab oladi.

Avtomatlashtirish. IDS / IPS tizimlari atolan oddiy, bu ularni barcha kiberxavfsizlik sfokchida foydalanish uchun ideal nomzodlarga aylantiradi. IPS, taemog cheklangan resurs talabiga ega bolgan tahdidlardan himoyalanganligini kafolatlik bilan ta'minlaydi.

Muvofiqlik: Muvofiqlikning bir gismi kopincha ma'lumotlarni himoya gilish

uchun texnologiyalar va tizimlarga mablag' kiritganingizni isbotlashni talab qiladi.

IPS / IPS uchimini tatbiq etish muvofiqlik varag'idagi katakchani tekshiradi va NDH xavfsizligi bo'yicha biz qator boshqaruv elementlariga murojaat qiladi. Eng muhimi, auditorlik ma'lumotlari muvofiqliklariga ~~muroj~~ tekshirishning qimmatli qismidir. Siyosat ijrosi IPS / IPS tarmoq darajasida ichki xavfsizlik siyosatini amalga oshirishga yordam beradigan tarzda sozlanishi mumkin. Masalan, faqat bitta VPN-ni qo'llab-quvvatlasangiz, boshqa VPN-trafikni bloklovka qilish uchun IPS-dan foydalanishingiz mumkin.

Tarmoqlararo ekran - brandmauer yoki firewall sistemasi (TE) deb ham ataluvchi tarmoqlararo himoyaning ixtisoslashtirilgan kompleksi. Tarmoqlar ekran umumiy tarmoqni ikki yoki undan ko'p kismlarga

ajratish va ma'lumot paketlarini chegara orqali umumiy tarmoqning bir qismida ekranlash amalga oshirish shartlarini belgilovchi qoidalar to'plamini amalga oshirish imkoniyatini beradi. Odatda, bu chegara korxonaning korporativ tarmog'i va Internet global tarmoq orasida o'rnatiladi. Tarmoqlararo ekranlar gardi korxona lokal tarmog'i ulangan korporativ intratarmoqida kelishuvchi xavfsizlikdan himoyalashda ishlatilishi mumkin bulsada, odatda ular korxona ichki tarmog'ini Internet global tarmoqdan sukutda kirishda himoyalaydi. Aksariyat tijorat tashkilotlari uchun tarmoqlararo ekranlarning o'rnatilishi ichki tarmoq xavfsizligini ta'minlashning zaruriy sharti hisoblanadi. Tarmoqlararo ekranlar tarmoqlararo aloqa xavfsizligini OSI modelining turli sathlarida modellaydi. Bunda etalon modelning turli sathlarida bajariladi.

gan ximoya funksiyalari bir-biridan jiddiy farqlanadi. Shu sababli, tarmoqlararo ekranlar komplektini, xar bir OSI modelining alohida satixiga muljallangan, bulinmaydigan ekranlar majmui kurinishida tasavvur etish mumkin.

② OSI modelida o'zaro aloqa vositalari yettita darajaga bölinishadi. dasturiy, taqdim etish, seans, transport tarmoq, kanal va fizik. Eng yuqori daraja dasturiy. Bu darajada foydalanuvchi dasturlar bilan ma'lumot almashtadi. Eng quyi daraja esa - fizik. Bu daraja quzilmalar öztasidagi signal almashinuvini ta'minlaydi.

Aloqa kanallari orqali ma'lumot almashinuvi ma'lumotning yuqori darajadan past darajaga uzatish, keyin aloqa liniyalari orqali transportirovka qilish, va nihoyat mijoz kompyuterida ma'lumotni quyi

darajada yuqori darajaga uzatish ozgali amalga oshiriladi.

Tarakli moslikni ta'minlash uchun kompyuter tarmoqlari arxitekturasining har bir darajasida maxsus standart protokollari mavjud. Ular bitta darajada turgan, lekin tarmoqning turli xil uzellarida joylashgan tarmoq komponentlari o'zaro almashtiradigan xabarlari kelma-ketligi va formatini aniqlaydigan tartiblangan qoidalar to'plamini o'zida mujassamlashtiradi.

TCP/IP steki o'zaro aloqa qiluvchi protokollarning butun bir to'plamini o'zida mujassamlashtiradi. Ular eng muhimi internetda bir kompyuterdan ko'plab oraliq tarmoqlar, shlyuzlar va marshrutizatorlar ozgali boshqa kompyuterga marshrut qidirish va shu marshrutlar

Bo'yicha ma'lumotlar bloklarini uzatish uchun javob beradigan IP protokoli va ma'lumotni ishchi jetkazib berish, xatosizlik va uzatilgan ma'lumotni to'g'ri tartibda qabul qilib olish uchun javob beradigan TCP protokollari hisoblanadi.

Tarmoq texnologiyasining keng kolamda qo'llanishi natijasida umumiy resurslardan foydalanish imkonini beruvchi lokal tarmoqga kompyuterlar birlashtirildi. Klient-server texnologiyasining tatbiq etilishi esa bu tarmoqni taqsimlangan hisoblash muhitiga aylantirdi. Tarmoqning xavfsizligi undagi barcha kompyuterlarning va tarmoq qurilmalarining xavfsizligi bilan aniqlash.

Buzg'unchi tarmoqning biror-bir tashkilot etuvchisining ishini buzish orqali butun tarmoqni obro'sizlantirishi mumkin.

Zamonaviy telekommunikatsiya texnologiyalari lokal tarmoqlarni global tarmoqqa - Internet-ga ulash imkonini berdi, rivojlanishi xavf-sizlikni ta'minlashni dolzarb masalaga aylantirdi va Internetga ulangan tarmoq va tizimlarda, qanday ma'lumotlarga ishlov berilishidan qatiy nazar, xavfsizlik vositalari bo'lishini taqozo etadi. Chunki, Internetning imkoniyatlaridan foydalanib buzg'unchi xavfsizlikni buzishni buzishni global masshtabda olib borishi mumkin. Internetga ulangan kompyuter tajovuz obyekti bo'lsa, hujumni amalga oshirayotgan shaxsga uning qayerda joylashgani katta ahamiyatga ega emas.

TCP/IP model Protocols and services

Application	HTTP, FTP, Telnet, NTP, DHCP, Ping	Application Presentation Session
Transport	TCP, UDP	Transport
Network	IP ARP ICMP, IGMP	Network
Network Interface	Ethernet	Data link Physical