HONEYNET

Xalqaro Nordik Universiteti
Sanoatni boshqarish va raqamli texnologiyalar
Kafedra o‘qituvchisi ***Sofoyeva Fotima Davlatyorovna***
Xalqaro Nordik Universiteti
1-KI-24 guruh talabasi ***Olimov Mashhurbek Otabek o’g’li***

Kalit so‘z: *Honeynet, Asal to‘rini, Honeynet-da mavjud bo‘lgan zaifliklar, Provokatsiya, Maxfiylik, qora shapka, Honeynet oldiga xavfsizlik devori*

Asalning qiymati

An'anaga ko‘ra ma'lumotlarni himoya qilish mudofaa xususiyatiga ega edi. Xavfsizlik devorlari, kirishni aniqlash tizimlari (IDS), kriptografik usullar o‘z resurslarimizni himoya qilish uchun mudofaa usulida qo‘llaniladi. Tashkilot mulkini eng yaxshi himoya qilish strategiyasi - xavfsizlik nuqsonlarini aniqlash va ularni darhol tuzatish. Ushbu yondashuvning muammosi shundaki, u dushman faol hujum qilayotgan paytda to‘liq mudofaa xususiyatiga ega. Honeynet ushbu vaziyatni o‘zgartirish uchun mo‘ljallangan bo‘lib, u sizga himoyadan faol harakatlarga o‘tishga, tashabbus ko‘rsatishga imkon beradi. Honeynetning asosiy maqsadi dushman haqida razvedka ma'lumotlarini to‘plash, uning vositalari, taktikalari va sabablarini o‘rganishdir. Bunday ma'lumotlarni to‘plash orqali siz nima tahdid qilayotganini va o‘zingizni ushbu tahdidlardan qanday qilib yaxshiroq himoya qilishni yaxshiroq tushunasiz. Axborot xavfsizligi ko‘pincha qasrni yoki partizan urushini himoya qilish kabi harbiy harakatlar bilan taqqoslanadi. Siz tanlagan o‘xshashlikdan qat'i nazar, siz har doim tashabbusni qabul qilishingiz va raqibingiz zarba berishidan oldin uni o‘rganishingiz mumkin.

Honeynet uchun mavjud bo‘lgan asosiy ma'lumot manbalaridan biri bu qora shapka suhbati, masalan, IRC (Internet Relay Chat) da. Qora qalpoqlar o‘zlarining muhitlarida erkin muloqot qilishadi, ularning motivlari, maqsadlari va “ekspluatatsiyasi” haqida gapirishadi. Honeynet yordamida biz ushbu

muzokaralarni so‘zma-so‘z muloqotlar shaklida yozib olishga muvaffaq bo‘ldik. Hatto real vaqt rejimida bizning tizimimizga hujum qilayotgan qora shapkalarning video tasvirlarini olishga muvaffaq bo‘ldik. Bu bizga qora shlyapalar jabrlanuvchini qanday nishonga olishi va hujumni amalga oshirishi haqida tasavvur beradi. “Qora qalpoqlarning motivlari va psixologiyasi” hujjati juda yorqin misoldir. Ushbu hujjat bitta mamlakatga hujum qilgan qora shapka guruhini ta'qib qilish haqida. Uch hafta davomida biz ular nafaqat buni qanday amalga oshirganlarini, balki, eng muhimi, nima uchun ekanligini aniqladik. Bunday batafsil ma'lumotlarga asoslanib, endi biz ushbu umumiy tahdiddan qanday qilib o‘zimizni himoya qilishimiz mumkinligini yaxshiroq bilib olamiz.

Honeynet shuningdek tashkilotga o‘zining xavfsizlik xavfi va zaif tomonlari haqida ma'lumot beradi. Asal to‘rini tashkiloti o‘zining kundalik ishlarida foydalanadigan tizim va dasturlardan iborat bo‘lishi mumkin. Honeynet-da mavjud bo‘lgan xatarlar va zaifliklar (ularni diqqat bilan o‘rganish va tahlil qilish mumkin) tashkilotning ish tizimidagi xatar va zaifliklarni to‘liq aks ettiradi. Masalan, kompaniya kredit kartalaridan foydalanish uchun yangi veb-server interfeysini amalga oshirishni xohlaydi. Tahlil bosqichida aniqlanmagan barcha xatar va zaifliklarni ushlab turish uchun tizimni ham, dasturni ham Honeynetning bir qismi sifatida tekshirish mumkin.

Provokatsiya - bu huquqni muhofaza qilish organlari xodimlari tomonidan qo‘llanilgan odatiy usul bo‘lib, jinoyatchini u boshqacha yo‘l tutmagan noqonuniy harakatlarga undaydi.

Maxfiylik haqida. Qo‘shma Shtatlar Adliya vazirligining kompyuter jinoyatchiligi va intellektual mulk bo‘limi tomonidan yaqinda e'lon qilingan "Jinoiy tekshiruvlarda kompyuterlarni qidirish va olib qo‘yish va elektron dalillarni olish" hujjatida ta'kidlangan ba'zi axloqiy va axloqiy ziddiyatlar mavjud (ular ichidagi kurashlar hech qachon susaymaydi).

Ma'lumotlarni boshqarish

Yuqorida aytib o‘tganimizdek, ma'lumotlar boshqaruvi ularning uzatilishini nazorat qiladi. Qora shapka bilan ish olib borganimizda, bu har doim xavfni o‘z

ichiga oladi va biz bu xavfni iloji boricha minimallashtirishimiz kerak. Biz murosaga kelgandan so‘ng, asal balchig'i Honeynetdan tashqaridagi boshqa tizimga zarar etkazish uchun ishlatilmasligiga ishonch hosil qilishimiz kerak (Honeyn ichida sodir bo‘ladigan barcha narsalar feyr-pley). Biroq, qiyinchilik shundan iboratki, qora shapka shubhali narsani sezmaydi.

Biz Honeynet-ni barcha kiruvchi va chiquvchi ulanishlarni boshqarish uchun ishlab chiqdik. Bu Honeynet oldiga xavfsizlik devorini qo‘yish orqali amalga oshiriladi, u orqali barcha tirbandliklar o‘tadi. Xavfsizlik devori Honeynet-dan Internetga qancha ulanish boshlanganligini kuzatib boradi. Muayyan pol qiymatiga erishgandan so‘ng, ekran keyingi urinishlarni bloklaydi. Bu qora shapka uchun biroz erkinlik beradi, shu bilan birga vaziyatni avtomatik ravishda nazorat ostida ushlab turadi. 5-10 ta chiquvchi ulanishga ruxsat berish boshqa tizimlarni hujumlardan himoya qilish bilan birga qora shapka baxtiga xalaqit bermasligi aniq. Bu Honeynet-ni skanerlash, o‘rganish yoki boshqa ko‘plab tizimlarga hujum qilish uchun sahna maydoni sifatida foydalanishdan himoya qiladi. Ba'zilarga bu funksiya kerak emas. Agar sizda Honeynet 24/7 rejimida kimdir nazorat qilish imkoniyatiga ega bo‘lsangiz, chiqadigan ulanishlar sonini cheklashingiz shart emas. Agar hujumning alomatlari (masalan, xizmatni rad etish) mavjud bo‘lsa, kuzatuvchi uni to‘sib qo‘yishi mumkin. Biroq, ushbu muammoni avtomatlashtirilgan tarzda hal qilish biz uchun yanada maqsadga muvofiqroq ko‘rinadi, chunki biz operator bilan tunu kun monitoring olib borolmaymiz. Bundan tashqari, yo‘riqnoma xavfsizlik devori va Honeynet o‘rtasida joylashgan. Va bu ikki sababga ko‘ra amalga oshirildi.

Xulosa

Honeynet - bu qora shapka jamoasining vositalari, taktikalari va sabablari to‘g'risida razvedka ma'lumotlarini yig'ish uchun mo‘ljallangan maxsus vosita. U chuqurchaning barcha ijobiy tomonlarini, xususan, aldanish va ogohlantirish tizimini o‘z ichiga oladi, ammo uning asosiy maqsadi o‘rganishdir. Asal qoliplari va asal qoliplari o‘rtasida ikkita asosiy farq bor. Birinchi farq shundaki, Honeynet bitta tizim emas, balki bir nechta tizim va dasturlarning tarmog'idir. Ikkinchi farq shundaki, Honeynet Internetning hamma joylarida joylashgan eng keng tarqalgan

tizimlarni o‘z ichiga oladi; o‘sha. biz tizimlarni yoki zaifliklarni taqlid qilmaymiz. Ushbu kombinatsiya Honeynetni ajoyib o‘quv vositasiga aylantiradi. Biroq, Honeynet juda katta miqdordagi ma'muriy xarajatlarni talab qiladi. Honeynet administratori buzilgan Honeynet yordamida boshqa tizimlarga hujum qilinmasligini ta'minlash uchun javobgardir

Foydalangan adabiyotlar

“Know Your Enemy: Honeynet” – The Honeynet Project kitobi

Sofoyeva, F. D. (2024). TARMOQ VA INTERNET. *Экономика и социум*, (11-1 (126)), 506-515.

https://www.honeynet.org

https://scholar.google.com/scholar?q=honeynet

Sofoyeva, F. (2024). JDK, JRE va JVM. Dasturlash muhitini tayyorlash. *Nordic_Press*, *3*(0003).