KIBERHUJUMLARNI OLDINI OLISH UCHUN HONEYPOT TEXNOLOGIYASINING AFZALLIKLAR

Omonov Fayziddin Komil o'g'li
Toshkent axborot texnologiyalari universiteti telekommunikatsiya texnologiyalari fakulteti
Abduraxmonova Dilnoza Alisher qizi
Oriental uneversteti Pedagogika va psixologiya yo'nalishi 2-kurs talabasi

Annotatsiya: *Mazkur maqolada kiber xujumlarni oldini olish uchun honeypot texnologiyasining afzalliklar, tarmoq xavfsizligini ta'minlovchi vositalar, honeypotlarni jismoniy yoki virtual ekanligiga qarab farqlash mumkinligi haqida ma'lumotlar berilgan.*

Kalit So'zlar: *Axborot, Internet, honeypot, DMZ, TCP/IP, simulyatsiya.*

Abstract: *This article provides information on the advantages of honeypot technology to prevent cyber attacks, tools that ensure network security, and how honeypots can be distinguished based on whether they are physical or virtual.*

Key Words: *Information, Internet, honeypot, DMZ, TCP/IP, simulation.*

Аннотация: *В этой статье представлена информация о преимуществах технологии приманки для предотвращения кибератак, инструментах, обеспечивающих безопасность сети, и о том, как можно отличить приманки в зависимости от того, являются ли они физическими или виртуальными.*

Ключевые Слова: *информация, Интернет, приманка, DMZ, TCP/IP, моделирование.*

KIRISH

Axborot, Internet va kompyuter xavfsizligida aksariyat foydalanuvchilar tahdid, zaiflik va hujum tushunchalaridan tez-tez foydalanadilar. Biroq, aksariyat foydalanuvchilar tomonidan ularni almashtirish holatlari kuzatiladi.

Honeypot ozi nima? Birinchidan, honeypot kompyuter tizimidir. Unda xuddi haqiqiy kompyuter kabi fayllar, kataloglar mavjud. Biroq, kompyuterning maqsadi xakerlarni ularning xatti-harakatlarini kuzatish va kuzatish uchun unga tushishga jalb qilishdir. Shunday qilib, biz uni haqiqiy tizimga o'xshash soxta tizim sifatida belgilashimiz mumkin. Ular boshqa xavfsizlik tizimlaridan farq qiladi, chunki ular nafaqat ma'lum bir muammoga bitta yechim topadilar, balki turli xil xavfsizlik muammolarini qo'llashlari va ularga bir nechta yondashuvlarni topishlari mumkin. Masalan, ular buzilgan tizimdagi zararli harakatlarni qayd qilish uchun ishlatilishi mumkin, shuningdek, foydalanuvchilar uchun yangi tahdidlarni o'rganish va bu muammolardan qanday qutulish bo'yicha g'oyalarni yaratish uchun ishlatilishi mumkin.

ADABIYOTLAR VA METADOLOGIYA

Mokubening so'zlariga ko'ra, I. & Adams M. (2007: p.322) biz honeypotlarni maqsadlari va o'zaro ta'sir darajasiga ko'ra ajratishimiz mumkin. Asal idishlarining maqsadlariga nazar tashlaydigan bo'lsak, ikkita turdagi honeypot borligini ko'rishimiz mumkin, ular tadqiqot asallari va ishlab chiqarish asallari.

Yolg‘on nishonlar yoki tuzoqlar (honeypot). Tarmoq xavfsizligini ta’minlovchi ushbu vositadan niyati buzuq tomonidan yolg‘on nishonlarni aniqlash, hamda buzib ochish usullarini tadqiqlash maqsadida hujumni yuzaga keltirishga urinishda foydalaniladi.

Yolg‘on nishonlarni tasniflashda alomatsifatida ularning interaktivligi ishlatiladi, ya’ni quyidagi tuzoqlar farqlanadi:

- interaktiv tuzoqlar;
- interaktivlik darajasi past tuzoqlar;
- interaktivlik darajasi yuqori tuzoqlar.

Interaktivlik darajasi past tuzoqlar bitta tarmoq servisining, masalan, FTP-servisning emulyatsiyasi bo‘lishi mumkin. Joylashtirilishining va nazoratlanishining osonligi bunday tuzoqlarning afzalligi hisoblansa, kamchiligi sifatida ular yordamida ko‘pincha faqat hujum faktining aniqlanishini ko‘rsatish mumkin.

NATIJALAR

Interaktivlik darajasi yuqori tuzoqlarni to‘laqonli operatsion tizimga va servislar naboriga ega virtual mashina sifatida tasavvur etish mumkin. Bunday tuzoqlar niyati buzuq xususida ancha ko‘p axborotni yig‘ishga imkon beradi (ayniqsa, u bilan intellektual teskari bog‘lanish tashkil etilgan bo‘lsa).

Honeypot bu tajovuzkorlar e'tiborini chalg'itish bo'lib, tajovuzkorlar tarmoqdan ma'lumotlarni sindirish va olishga muvaffaq bo'lgan deb o'ylashlari uchun, aslida ma'lumotlar muhim emas va joylashuvi izolyatsiya qilingan. Axborot tizimidagi harakatlardan ruxsatsiz foydalanishni tuzoqqa tushirish yoki rad etish usuli. Honeypotning bir turi asaldir. Asal o'zaro ta'siri past bo'lgan honeypot bo'lib, u yuqori shovqin turlariga nisbatan kichikroq xavfga ega, chunki honeypot bilan o'zaro ta'sir to'g'ridan-to'g'ri haqiqiy tizimni o'z ichiga olmaydi. Mikrotikda honeypot va xavfsizlik devori, xavfsizlik devorini amalga oshirish maqsadi ishlatiladi. Honey tomonidan yaratilgan faoliyat hisobotlarini ko'rish uchun ma'muriy vosita sifatida foydalanish mumkin va administratorlar tarmoq xavfsizligi siyosatlarini aniqlashda yordam berish uchun jurnallarda saqlanadigan hisobotlarni ham ko'rishlari mumkin. Honeypotlarini joylashtirish hiyla tizimi tashkilot tarmog'iga tashqi yoki ichki hujumlarni kuzatish uchun mo'ljallanganligiga bog'liq; shuning uchun u xavfsizlik devori oldida, qurolsizlantirilgan zonada (DMZ) yoki xavfsizlik devori orqasida o'rnatilishi mumkin.

Honeypotlarni jismoniy yoki virtual ekanligiga qarab farqlash mumkin:

Jismoniy honeypots: o'z IP-manziliga ega haqiqiy mashina, bu mashina tizim tomonidan modellashtirilgan xatti-harakatlarni simulyatsiya qiladi. Ko'pincha bu usul yangi mashinalarni sotib olishning yuqori narxi, ularga texnik xizmat ko'rsatish va ixtisoslashtirilgan uskunani sozlash bilan bog'liq murakkablik kabi qo'llanilmaydi.

Virtual honeypots: bu turdagi honeypotlardan foydalanish tarmoqqa turli xil operatsion tizimlardan xostlarni o'rnatish va simulyatsiya qilish imkonini beradi, ammo buning uchun maqsadli operatsion tizimning TCP/IP-ni simulyatsiya qilish kerak. Bu usul tez-tez uchraydi.

Honeypotlarni joylashtirish (foydalanish/harakat) va ishtirok etish darajasiga qarab tasniflanishi mumkin. Joylashtirishga ko'ra, honeypotlarni quyidagilarga ajratish mumkin:

- honeypotlarni ishlab chiqarish
- honeypotlarni tadqiq qilish

Ishlab chiqarish honeypots foydalanish oson, faqat cheklangan ma'lumotlarni ushlaydi va birinchi navbatda korporatsiyalar tomonidan qo'llaniladi. Ishlab chiqarish honeypotlari umumiy xavfsizlik holatini yaxshilash uchun tashkilot tomonidan boshqa ishlab chiqarish serverlari bilan ishlab chiqarish tarmog'iga joylashtiriladi. Odatda, ishlab chiqarish honeypotlari past o'zaro ta'sirli honeypotlar bo'lib, ularni joylashtirish osonroq. Ular xujumlar yoki tajovuzkorlar haqida ko'proq ma'lumot beradilar.

Turli tarmoqlarni nishonga olgan qora shlyapalilar hamjamiyatining motivlari va taktikasi haqida ma'lumot to'plash uchun tadqiqot honeypots yuritiladi. Bu honeypots ma'lum bir tashkilotga bevosita qiymat qo'shmaydi; Buning o'rniga ular tashkilotlar duch keladigan tahdidlarni o'rganish va ushbu tahdidlardan qanday qilib yaxshiroq himoya qilishni o'rganish uchun ishlatiladi. Tadqiqot honeypots joylashtirish va saqlash, keng ma'lumot olish uchun murakkab va asosan tadqiqot, harbiy yoki hukumat tashkilotlari tomonidan qo'llaniladi.

Dizayn mezonlariga ko'ra, asal qozonlarini quyidagilarga ajratish mumkin:

- toza honeypotlari
- yuqori shovqinli honeypotlari
- past o'zaro ta'sirli honeypotlari

XULOSA

Sof honeypotlar to'liq ishlab chiqarish tizimlaridir. Buzg'unchining faoliyati honeypotning tarmoqqa havolasida o'rnatilgan xato kran yordamida nazorat qilinadi. Boshqa dasturlarni o'rnatish shart emas. Sof honeypot foydali bo'lsa ham, himoya mexanizmlarining yashirinligi yanada boshqariladigan mexanizm bilan ta'minlanishi mumkin.

FOYDALANGAN ADABIYOTLAR:

1. P. Owezarski, “Unsupervised classification and characterization of honeypot attacks,” in Proceedings of 10th International Conference on Netw and Service Management (CNSM) and Workshop, pp. 10–18, Rio de Janeiro, Brazil, November 2014. View at: Publisher Site Google Scholar

2. 2.S. Dowling, M. Schukat, and E. Barrett, “Improving adaptive honeypot functionality with efficient reinforcement learning parameters for automated malware,”Journal of Cyber Security Technology, vol. 2, no. 2, pp. 75–91, 2018. View at: Google Scholar

3. 3.I. M. M. Matin and B. Rahardjo, “Malware detection using honeypot and machine learning,” inProceedings of 2019 7th International Conference on Cyber and IT Service Management (CITSM), pp. 1–4, Bandung Institute of Technology, Bandung, Indonesia, November 2019.View at:Google Scholar

4. 4.L. Spitzner,Honeypots: Tracking Hackers, Addison-Wesley, Clemson, SC, USA, 2003