Veb saytlarga bo’ladigan DDoS xujumlarni oldini olish.

Tojidinov Azizbek Ilhomjonov o'g'li
Toshkent Axborot Texnalogiya Universiteti Farg’ona Filiali, Talaba, Farg’ona

Abdurahimov Ozodbek Azimjon o'g'li
Muhammad Al-Xorazmiy nomidagi TATU Farg‘ona filiali talabasi

Annotatsiya: Tarmoq mutasaddilari va axborot xavfsizligi bo‘yicha mutaxassislar oldida Internet-trafikni filtrlash vazifasi turibdi. Uni amalga oshirish ish stantsiyalarini viruslar bilan yuqtirishning oldini olish va xodimlar tomonidan shaxsiy maqsadlarda Internetdan noto‘g‘ri foydalanishni istisno qilish uchun zarur. Biznes foydalanuvchilarini fishing saytlari va zararli kodni o‘z ichiga olgan sahifalar ko‘rinishidagi yana bir katta muammo kutmoqda.

Kalit so’zlar: DDOS, Google Dork, Bog'lanish chuqurligi,

Kirish

Sayt tuzilishi- bu veb- saytdagi tarkibni tashkil qilish va taqdim etish usuli. Bu sahifalar bir- biri bilan qanday bog'liqligini va foydalanuvchilar saytni qanday boshqarishi mumkinligini belgilaydi. Yaxshi ishlab chiqilgan sayt strukturasi foydalanuvchilarga ma'lumotni osongina topishga yordam beradi va saytdan foydalanishning umumiy tajribasini yaxshilaydi. Foydalanuvchilar uchun navigatsiyani yaxshilaydi, saytni yanada qulay va tushunarli qiladi. Bu shuningdek, qidiruv tizimlariga sayt tarkibini yaxshiroq indekslashga yordam beradi va qidiruv natijalarida uning ko'rinishini oshiradi.

Veb- sayt tuzilishi va sahifalar o'rtasidagi munosabatlarni ko'rsatadigan diagramma. Bu saytda ma'lumotlar qanday tashkil etilganligini va foydalanuvchilar u orqali qanday harakat qilishlarini tushunishga yordam beradi. Sayt xaritasi qidiruv tizimlari tomonidan sayt mazmunini indekslash uchun Foydalaniladigan matnli fayl sifatida ham taqdim etilishi mumkin. Saytning jismoniy tuzilishini optimallashtirish

Saytning jismoniy tuzilishi veb- sayt katalogi tomonidan ko'rsatilgan tuzilmani va undagi fayllar saqlanadigan haqiqiy joyni anglatadi. Jismoniy tuzilish odatda ikki xil shaklni o'z ichiga oladi: tekis jismoniy tuzilish va daraxtning jismoniy tuzilishi. Kichik veb- sayt uchun barcha veb- sahifalar veb- saytning asosiy katalogida saqlanadi. Bu struktura tekis jismoniy tuzilishdir. Ushbu tekis jismoniy tuzilma qidiruv tizimlari uchun ideal, chunki barcha sahifalarni bir

tashrifda ko'rish mumkin. Biroq, agar veb- sayt juda ko'p sahifalarga ega bo'lsa va ildiz katalogida juda ko'p veb- sahifa fayllari mavjud bo'lsa. Ularni topish va saqlash juda qiyin bo'ladi. Shuning uchun tekis jismoniy tuzilma odatda bir necha sahifali kichik va mikrosaytlar uchun mos keladi. Kattaroq veb- saytlar ko'pincha veb- sahifalami to'g'ri saqlash uchun ikki yoki uch daraja yoki undan ko'p pastki kataloglarni talab qiladi. Bu qatlamli katalog daraxt fizik strukturasi deb ham ataladi: ya'ni ildiz katalogi bir necha kanal yoki kataloglarga bo'linadi.

Veb- saytning jismoniy tuzilishidan farqli o'laroq, veb- saytning mantiqiy tuzilmasi havola strukturasi deb ham ataladi, bu asosan veb- sahifaning ichki havolalari orqali hosil bo'lgan mantiqiy tuzilishga ishora qiladi yoki havola strukturasi deb ataladi. Mantiqiy tuzilma va jismoniy tuzilma o'rtasidagi farq shundaki, mantiqiy tuzilma veb- sayt sahifalarining munosabatlari bilan belgilanadi. Boshqa tomondan, jismoniy tuzilma veb- sayt sahifalari saqlanadigan jismoniy manzil bilan belgilanadi. Veb- saytning mantiqiy tuzilishida sahifalar orasidagi mantiqiy munosabatni tasvirlash uchun" bog'lanish chuqurligi" odatda ishlatiladi." Bog'lanish chuqurligi" manba sahifasidan maqsad sahifaga olib boradigan yo'llar sonini bildiradi. Misol uchun, agar veb- saytning A sahifasida B sahifasiga havola bo'lsa. A sahifadan B sahifaga havola chuqurligi 1 ga teng.

Agar sizning sayt zaif havolaga ega bo'lsa va veb-sayt ma'lum bir hujum turiga himoyasiz bo'lsa, ertami-kechmi sizga xakerlik hujumi sodir bo'ladi. Zaif saytni topish va uni buzish atigi bir necha daqiqada, hech qanday maxsus xakerlik vositalarisiz amalga oshirilishi mumkinligiga ishonmaydi. Masalan, 2015 yil 1 sentyabrda Google Hacking ma'lumotlar bazasida paydo bo'lgan "dork" ni ko'rib chiqing. Ochiq kataloglari bo'lgan saytlarni topishga imkon beradi, bunday kataloglarda siz nafaqat xizmat fayllari ro'yxatini ko'rish, balki ularning tarkibini, masalan, parollarni topish mumkin. Hackerning qo'lida oson o'ljaga aylanmaslik, vaziyatdan qochish juda oson. Veb-loyihalarni oldindan himoya qilish haqida o'ylang. Agar sizning sayt o'rtacha darajadan bir oz xavfsizroq CMS qutisi va standart sozlamalari mavjud bo'lsa, unda nomaqbul xakerlik muammosi sizni chetlab o'tadi.

Veb-o'rgimchaklarning bir nechtasi robots.txt yoki htaccess fayllarida keltirilgan ko'rsatmalarga amal qilishadi. Bu ikkisi juda SEO optimallashtirishning maxsus vositalari, ammo sayt yoki blog xavfsizligi nuqtai nazaridan.

Hacking kichik yoki katta bo'lsin, har qanday o'sayotgan biznesga zarar etkazishi mumkin. Hacklash usullaridan foydalangan holda siz istalgan vaqtda har qanday kompaniyaning maxfiy ma'lumotlarini o'g'irlashi, kompyuterni to'liq boshqarishi yoki hatto saytga zarar etkazishi mumkin.

Turli kompaniyalar uchun to'liq axborot xavfsizligini ta'minlash va ularga hujumlarning oldini olish uchun maxsus o'quv maktablari mavjud. Axloqiy buzish bo'yicha kurslarni o'tkazish. Qanday bo'lmasin, ular xakerlikni o'rgatishadi.

Bunday muassasalarda o'qitiladigan barcha axloqiy buzish usullari har qanday kompaniya uchun juda muhimdir. Ular uning maxfiy ma'lumotlarini o'g'irlashning oldini olishga yordam beradi. Har qanday tizimning xavfsizligini ta'minlash uchun saytni qanday qilib buzish yoki xakerlar saytni buzishda qanday usullardan foydalanish mumkinligini bilish kerak. Shunday qilib, saytni buzishning qanday usullari mavjudligini aniqlaylik.

Google Dorki - maxsus tanlangan so'rovlar, ular yordamida siz keraksiz bo'lgan fayllarni yoki sahifalarni topish mumkin, ammo baribir sayt egalari tomonidan umumiy ko'rish uchun ochilgan. Q iziquvchan krakerni uni saytlarda qiziqtirgan aniq joyga olib boradi. Biroq, ob'ektiv foydalanuvchiga buyruqlar ro'yxati hech narsa aytmaydi. Dorkovni kashf qilishda xaker uchun eng muhimi quyidagilar bo'ladi:

- zaif dasturlarni aniqlash
- oddiy foydalanuvchi ko'zidan yashirilishi kerak bo'lgan fayllar va kataloglarni qidirish
- sahifalar va xato xabarlari va tizimning boshqa kamchiliklaridan foydalanish
- Hujumni amalga oshirish uchun Internetda serverga bepul yuklab olinadigan ko'plab vositalar mavjud va bu vositalarning faqat bir nechtasi zombi tizimida ishlashi mumkin.
- Google-dan foydalanib, veb-resurs profilini osongina aniqlash mumkin: server ishlaydigan dasturlar, operatsion tizim turi va boshqalar. Bu haqda juda ko'p ma'lumotni Netcraft.com saytida topish mumkin. Ammo Dorki eng ommabop bo'lganida, hacker server qanday ishlashini aniq biladi va dasturiy ta'minotda qanday xatolar mavjudligini aniqlaydi.
- Ko'pincha ishlaydigan dasturiy ta'minot barmoq izlari kabi noyob xususiyatlarga ega. Ba'zida dastur o'zini o'zi uzib qo'yadi. Shunday qilib, mashhur dvigatellar va mavzularni ishlatadigan sayt egalari ko'pincha uning nomini satrda payqashdi. *“Tomonidan ishlab chiqilgan…”* yoki "*Sayt boshqaruvchisi* ..." Ba'zida hatto versiya raqami ham ko'rsatishni unutadi. Sahifalardagi bunday yozuvlar ommabop mavzulardan foydalanganda yoki standart ravishda serverga dastur o'rnatilganda avtomatik ravishda ro'yxatdan o'tkaziladi. Bundan tashqari, bunday chiziqlar juda tez o'chiriladi va sayt uchun hech qanday oqibatlarga olib kelmaydi. Bunday satrlarni, jumladan sharhlar va meta-teglarni qidirishda sahifalar va shablonlarni kodidan o'tib ketish juda oson. Ushbu yozuv yana paydo bo'ladimi yoki yo'qligini bilish uchun har safar mavzuni yangilab bo'lgandan keyin tekshirish kerak.

- Ko'pincha sayt sirlari teg tarkibini ochib berishi mumkin. Ushbu yozuvda ochiq ko'rsatuvchi yorliqlar mavjud emasligiga qaramasdan, qoida tariqasida, operator **sarlavha:** dasturiy ta'minotga oid matnlarni gibletlar yordamida chiqaradi. Shunday qilib, agar siz saytning egasi bo'lsangiz - tez-tez yangilab turing, yangilanishlar bekor qilinmaydi.
- DOS yoki DDOS hujumi soxta so'rovlar soni bilan server so'rovini navbatga yuborish orqali istalgan tizimni o'chirib qo'yganda eng kuchli xakerlik hujumlaridan biridir. DDOS hujumida ko'plab hujum qiluvchi tizimlar qo'llaniladi. Ko'pgina kompyuterlar bir vaqtning o'zida bitta maqsadli serverga DOS hujumlarini amalga oshiradilar. DOS hujumi bir nechta kompyuterlarni qamrab olganligi sababli, xizmatga hujum qilishni taqiqlangan rad etish deyiladi.
- Xakerlar DDOS hujumlarini boshlash uchun zombi tarmog'idan foydalanadilar. Zombi tarmog'i - bu xakerlar DOS hujum qilish vositalarini osongina o'rnatgan kompyuterlardir. Zombi tarmog'idagi ishtirokchilar soni qancha ko'p bo'lsa, hujum kuchliroq bo'ladi. Ya'ni, agar kiber-xavfsizlik xodimlari oddiygina foydalanuvchilarning IP-manzillarini blokirovka qila boshlasalar, bundan yaxshi narsa bo'lmaydi.

DDoS hujumi veb saytdagi hech qanday m’lumotlarni buzmasada, bu saytni ancha vaqtgacha to’xtatib qo’ya oladi. Bu yerda DDoS hujumlarni oldini olishning bir nechta usullari mavjud.

Onlayn biznesda to'g'ri moslashuvchanlik rejasi bo'lishi kerak. Bu DDoS hujumlarini texnik jihatdan to'xtata oladigan usullar va hujum sodir bo'lganda nima qilish kerakligi strategiyasiga ega bo'lishni anglatadi. Biznes operatsiyalarini davom ettirish va zarur bo'lgan aloqa kanallarini ochish uchun yo'l bo'lishi kerak.

Ba'zida katta DDoS hujumi xakerlar urinishlari mumkin emas. Tarmoqqa stress va uning xavfsizlik darajasini sinab ko'rish uchun mo'ljallangan kam hajmli hujumlar hollari ham mavjud. Past darajadagi hujumni aniqlash imkonini beruvchi tarmoq trafigini tushunish muhimdir. Bu yo'lda bo'lishi mumkin bo'lgan katta hujumning oldini olishga yordam beradi.

Bulutli hosting xizmatidan foydalanganda, DDoS hujumlari haqida tashvishlanish kerak deb o'ylash mumkin. Bu hatto biz aytib o'tgan kichikroq, past hajmli hujumlar ham jiddiy zarar etkazishi mumkin. Ba'zida xakerlar saytni butunlay ishdan chiqarishdan tashqari boshq maqsadlardan ham foydalanishadi. Masalan, ular sizning operatsiyalaringizga to'lov dasturini kiritish uchun kichik DDoS hujumidan shunchaki chalg‘itish uchun ham ishlatishlari mumkin. Agar siz kichikroq hujumlar, masalan, bir necha daqiqa davom etadigan hujumlardan xavotirda bo'lsangiz, ularni aniqlashga etarlicha e'tibor bermasligingiz mumkin. Tarmoqni kuzatish va

g'alati naqshlarni tan olish muhim bo'lsa- da, bu yagona himoya usuli emas. Tarmoq trafigi uchun chegarasini o'rnatish kifoya deb xato qilishingiz mumkin.

Ko'p odamlar xavfsizlik devoridan foydalanish DDoS hujumidan himoya qilish deb noto'g'ri taxmin qilishadi, ammo bu to'g'ri emas. Aslida, xavfsizlik devori hech narsaga erisha olmaydi. Xavfsizlik devorlari bilan bog'liq muammo shundaki, ular tarmoqning yuqori kuchlanish davrida haqiqiy foydalanuvchilarga ta'sir qilishi mumkin bo'lgan chegara chegaralaridan foydalanadilar. Siz doimiy foydalanuvchilarga saytni uzluksiz ko'rib chiqish imkonini beradigan yechimni xohlaysiz. Bulutli hosting yoki VPS xizmatlarini olayotganingizda, provayderingizda DDoS himoyasi rejasi mavjudligiga ishonch hosil qiling. Reja haqida bilib oling, uning muvaffaqiyat darajasi haqida so'rang va uning saytingiz uchun etarlicha yaxshi yoki yo'qligini baholang.

Foydalanilgan adabiyotlar

1. Dadakhon, T., & Sabohat, A. (2022). Developing Creative Thinking through Primary School Students Solving Problems. European Multidisciplinary Journal of Modern Science
2. Dadakhon, T. (2022). Factors that Review Students' Imagination in the Educational Process. Spanish Journal of Innovation and Integrity, 5, 551-557.
3. G'aniyev_S_K,_Karimov_M_M,_Tashiyev_K_V_Axborot_xavfsizligi_2017 Muharrir: Tex. muharrir: Musawir: Musahhih: Kompyuterda sahifalovchi: Sh.Aliyeva M.Holmuhamedov D.Azizov N.Hasanova N.Raxmatullayeva.
4. Igam berdiyev X.Z. - Toshkent davlat texnika universiteti “Boshqarishda axborot texnologiyalari” kafedrasi professori, texnika fanlari doktori; Ahmedova O.P. - “Unicon.UZ” DUK, Kriptografiya ilmiy-tadqiqot bolim i boshlig‘i, t.f.n.
5. Zhimao Lu, Houmed Mohamed *Journal of Information Security* Vol.12 No.2, April 30, 2021