INNOVATIVE WORLD
Ilmiy tadqiqotlar markazi

YANGI RENESSANS

ILMIY JURNALI

2026/4

+998335668868
www.innoworld.net

YANGI RENESSANS

ILMIY JURNALI
TO'PLAMI

3 - JILD, 4 - SON
2026

www.innoworld.net

O'ZBEKISTON-2026

Zone transfer (AXFR) hujumlari va ularning oldini olish
Атаки с переносом зоны (AXFR) и их предотвращение
Zone transfer (AXFR) attacks and their prevention

Sobirjonov Behzodbek Qahramonovich
Farg‘ona davlat universiteti Axborot texnologiyalari kafedrasi o’qituvchisi
behzodbekqahramonovich@gmail.com
Ismonaliyeva Dilbarxon Maxamadali qizi
Farg‘ona davlat universiteti Axborot tizimlari va texnologiyalari yo‘nalishi
2-kurs talabasi
dilbarxon228@gmail.com

Annotatsiya

Ushbu maqolada DNS tizimida yuzaga keladigan Zone Transfer (AXFR) hujumlari, ularning ishlash prinsiplari va keltirib chiqaradigan xavflari tahlil qilinadi. AXFR mexanizmi aslida DNS serverlar o‘rtasida ma’lumot almashish uchun mo‘ljallangan bo‘lsa-da, noto‘g‘ri sozlangan holatlarda hujumchilar tomonidan tarmoq infratuzilmasi haqida muhim ma’lumotlarni qo‘lga kiritish uchun ishlatilishi mumkin. Maqolada bunday hujumlarning oldini olish usullari, jumladan, kirishni cheklash, autentifikatsiya mexanizmlarini qo‘llash va xavfsizlik siyosatini kuchaytirish bo‘yicha tavsiyalar beriladi.

Аннотация

В данной статье рассматриваются атаки типа Zone Transfer (AXFR) в системе DNS, их принципы работы и потенциальные угрозы. Механизм AXFR предназначен для передачи зонной информации между DNS-серверами, однако при неправильной настройке он может быть использован злоумышленниками для получения конфиденциальных данных о сетевой инфраструктуре. В статье также представлены методы предотвращения подобных атак, включая ограничение доступа, использование механизмов аутентификации и усиление политики безопасности.

Abstract

This article examines Zone Transfer (AXFR) attacks in the Domain Name System (DNS), including their operational principles and associated security risks. Although AXFR is designed for legitimate data synchronization between DNS servers, improper configuration can expose sensitive network information to attackers. The paper also discusses effective mitigation strategies, such as access control restrictions, implementation of authentication mechanisms, and strengthening overall security policies.

Kalit so‘zlar: DNS, Zone Transfer, AXFR, kiberxavfsizlik, tarmoq xavfsizligi, DNS hujumlari, ma’lumotlar sizib chiqishi, autentifikatsiya, kirishni cheklash, server himoyasi.

Ключевые слова: DNS, передача зоны, AXFR, кибербезопасность, сетевая безопасность, DNS-атаки, утечка данных, аутентификация, ограничение доступа, защита сервера.

Keywords: DNS, Zone Transfer, AXFR, cybersecurity, network security, DNS attacks, data leakage, authentication, access control, server protection.

Kirish

Bugungi kunda axborot texnologiyalarining jadal rivojlanishi bilan bir qatorda kiberxavfsizlik masalalari ham tobora dolzarb ahamiyat kasb etmoqda. Internet infratuzilmasining muhim tarkibiy qismi hisoblangan DNS (Domain Name System) tizimi tarmoqda nomlarni IP-manzillarga moslashtirish vazifasini bajaradi. Shu sababli, uning xavfsizligi butun tizim barqarorligi va ishonchliligiga bevosita ta’sir ko‘rsatadi.

DNS tizimida qo‘llaniladigan Zone Transfer (AXFR) mexanizmi serverlar o‘rtasida zonalar haqidagi ma’lumotlarni uzatish uchun xizmat qiladi. Biroq, ushbu mexanizm noto‘g‘ri sozlangan holatlarda tajovuzkorlar tomonidan suiste’mol qilinishi mumkin. Natijada, ular tarmoq tuzilmasi, serverlar va boshqa muhim resurslar haqida maxfiy ma’lumotlarni qo‘lga kiritish imkoniga ega bo‘ladilar.

Shu nuqtai nazardan, Zone Transfer (AXFR) hujumlari kiberxavfsizlik sohasida jiddiy tahdid hisoblanadi. Mazkur maqolada ushbu hujumlarning mohiyati, ularning ishlash prinsiplari hamda oldini olish usullari batafsil tahlil qilinadi.

DNS (Domain Name System) tizimi internetda domen nomlarini IP-manzillarga moslashtiruvchi muhim xizmat hisoblanadi. Ushbu tizimda serverlar o‘rtasida ma’lumot almashish jarayoni Zone Transfer deb ataladi. Zone Transfer, xususan AXFR (Asynchronous Full Zone Transfer) protokoli orqali amalga oshiriladi va u bir DNS serverdan boshqasiga butun zona ma’lumotlarini uzatishga xizmat qiladi. Bu jarayon odatda asosiy (primary) va zaxira (secondary) DNS serverlar o‘rtasida ishlatiladi.

Biroq, agar AXFR mexanizmi noto‘g‘ri sozlangan bo‘lsa, ya’ni unga kirish cheklanmagan bo‘lsa, har qanday foydalanuvchi yoki hujumchi DNS serverdan to‘liq zona ma’lumotlarini so‘rab olishi mumkin. Natijada, domen ichidagi barcha subdomenlar, server nomlari, IP-manzillar va boshqa muhim ma’lumotlar oshkor bo‘ladi. Bu esa tarmoq infratuzilmasi haqida to‘liq tasavvur hosil qilish imkonini beradi va keyingi hujumlar uchun zamin yaratadi.

Zone Transfer (AXFR) hujumlari odatda razvedka (reconnaissance) bosqichida qo‘llaniladi. Hujumchilar maxsus vositalar yordamida DNS serverga AXFR so‘rov yuborib, uning javobini tahlil qiladilar. Agar server noto‘g‘ri sozlangan bo‘lsa, u barcha zona yozuvlarini qaytaradi. Bu esa ma’lumotlar sizib chiqishiga olib keladi.

Bunday hujumlarning oldini olish uchun bir qator xavfsizlik choralarini qo‘llash zarur. Avvalo, DNS serverda Zone Transfer faqat ishonchli serverlar uchun ruxsat etilishi kerak. Buning uchun IP-manzillar bo‘yicha cheklov (access control) joriy qilinadi. Shuningdek, TSIG (Transaction Signature) kabi autentifikatsiya mexanizmlaridan foydalanish orqali serverlar o‘rtasidagi almashinuvni himoyalash mumkin.

Bundan tashqari, DNS serverlarni muntazam ravishda yangilab borish, xavfsizlik sozlamalarini tekshirish va monitoring tizimlarini joriy etish ham muhim ahamiyatga ega. Tarmoq xavfsizligini ta’minlashda kompleks yondashuv zarur bo‘lib, faqat bitta choraga tayanib qolish yetarli emas.

Xulosa

Xulosa qilib aytganda, DNS tizimida qo‘llaniladigan Zone Transfer (AXFR) mexanizmi muhim funksional ahamiyatga ega bo‘lsa-da, noto‘g‘ri sozlangan holatlarda jiddiy xavfsizlik tahdidlariga olib kelishi mumkin. AXFR hujumlari orqali tajovuzkorlar tarmoq infratuzilmasi haqida batafsil ma’lumotlarga ega bo‘lib, keyingi bosqichdagi kiberhujumlarni amalga oshirishlari osonlashadi.

Shu sababli, DNS serverlarni to‘g‘ri sozlash, Zone Transfer jarayonini faqat ishonchli manbalar bilan cheklash va zamonaviy autentifikatsiya mexanizmlaridan foydalanish muhim ahamiyat kasb etadi. Bundan tashqari, tizimlarni muntazam monitoring qilish va yangilab borish orqali xavfsizlik darajasini yanada oshirish mumkin.

Foydalanilgan adabiyotlar

1. Абдуллаев А.А. Axborot xavfsizligi asoslari. — Toshkent: O‘zbekiston, 2021.
2. Рустамов Б.Т. Axborot xavfsizligi va kiberxavfsizlik. — Toshkent: Fan va texnologiya, 2022.
3. Исмоилов Ш. Kompyuter tarmoqlari va ularning xavfsizligi. — Toshkent: Innovatsion rivojlanish nashriyoti, 2020.
4. Нурмухамедов Д. Kiberxavfsizlik asoslari. — Toshkent: Yangi nashr, 2023.
5. ISO/IEC 27001 standarti bo‘yicha Axborot xavfsizligini boshqarish tizimlari haqida qo‘llanmalar.