EOC
EUROASIAN
ONLINE
CONFERENCES

ENGLAND
CONFERENCE

INTERNATIONAL CONFERENCE ON MULTIDISCIPLINARY STUDIES AND EDUCATION



Google Scholar zenodo OpenAIRE doi digital object identifier

INTERNATIONAL CONFERENCE ON MULTIDISCIPLINARY STUDIES AND EDUCATION: a collection scientific works of the International scientific conference – London, England, 2026. Issue 5

Languages of publication: Uzbek, English, Russian, German, Italian, Spanish

The collection consists of scientific research of scientists, graduate students and students who took part in the International Scientific online conference **«INTERNATIONAL CONFERENCE ON MULTIDISCIPLINARY STUDIES AND EDUCATION»**. Which took place in London 2026.

Conference proceedings are recommended for scientists and teachers in higher education establishments. They can be used in education, including the process of post - graduate teaching, preparation for obtain bachelors' and masters' degrees. The review of all articles was accomplished by experts, materials are according to authors copyright. The authors are responsible for content, researches results and errors.

Lokal Tarmoqlarda Axborot Xavfsizligi: ARP Spoofing va MITM Hujumlarining Mexanizmlari hamda Amaliy Tahlili

Behzod Sobirjonov Qahramonivich
FarDu Axborot tehnologiyalari kafedrasi o‘qituvchisi
behzodbekqahramonovich@gmail.com
Qodiraliyev Jahonmurod Davronbek o'g'li
FarDu Axborot tizimlari va texnologiyalari
yo‘nalishi 2-bosqich talabasi
jahonmurod004@gmail.com

ANNOTATSIYA. Ushbu maqolada lokal hisoblash tarmoqlarining fundamental zaifliklaridan biri bo‘lgan ARP protokoli va unga asoslangan Man-in-the-Middle (MITM) hujumlari tadqiq etiladi. Maqolada kiberjinoyatchilar tomonidan ma’lumotlar oqimini tutib qolish va trafikni manipulyatsiya qilishda foydalaniladigan ARP spoofing mexanizmlari tahlil qilingan. Shuningdek, ushbu tahdidlarga qarshi zamonaviy himoya usullari bo‘yicha tavsiyalar berilgan.
Kalit so‘zlar: Kiberxavfsizlik, ARP Spoofing, MITM, OSI modeli, Lokal tarmoq, Paketlarni tutib qolish, Tarmoq xavfsizligi.
АННОТАЦИЯ. В данной статье исследуются механизмы работы атак ARP-spoofing и Man-in-the-Middle (MITM), основанных на фундаментальных уязвимостях протокола ARP в локальных сетях. В работе анализируются методы перехвата потоков данных и манипулирования трафиком, используемые киберпреступниками. Также даются рекомендации по современным методам защиты и стратегиям мониторинга против подобных сетевых угроз.
Ключевые слова: Кибербезопасность, ARP Spoofing, MITM, модель OSI, локальная сеть, перехват пакетов, сетевая безопасность.
ANNOTATION. This article examines the mechanisms of ARP spoofing and Man-in-the-Middle (MITM) attacks based on the fundamental vulnerabilities of the ARP protocol in local area networks. The paper analyzes the methods used by cybercriminals to intercept data flows and manipulate traffic. It also provides recommendations on modern defense methods and monitoring strategies against such network threats.
Keywords: Cybersecurity, ARP Spoofing, MITM, OSI model, Local Area Network (LAN), Packet sniffing, Network security.

Tarmoq Protokollaridagi "Ishonch" Muammosi

Zamonaviy kompyuter tarmoqlari ma’lumot almashish samaradorligiga asoslangan, biroq ko‘pgina fundamental protokollar, jumladan ARP (Address Resolution Protocol), xavfsizlik funksiyalarini hisobga olmagan holda ishlab chiqilgan. Lokal tarmoq ichidagi qurilmalar bir-biriga "ko‘r-ko‘rona" ishonishi kiberjinoyatchilar uchun keng imkoniyatlar ochadi. ARP spoofing va MITM hujumlari aynan shu ishonch zanjirini buzishga qaratilgan eng xavfli hujum turlaridan hisoblanadi.

1. ARP Spoofing Mexanizmi: Manzilni Soxtalashtirish

ARP protokoli IP-manzilni qurilmaning jismoniy (MAC) manziliga bog‘lash vazifasini bajaradi. Uning asosiy zaifligi — autentifikatsiyaning mutlaqo yo‘qligidir.

Ishlash tamoyili: Hujumchi tarmoqqa soxta ARP xabarlarini yuboradi. Natijada, nishon hisoblangan kompyuter (qurbon) va tarmoq shlyuzi (router) o‘zining ARP-jadvalini noto‘g‘ri ma’lumot bilan yangilaydi.

Natija: Qurbonning kompyuteri routerning MAC-manzili sifatida hujumchining qurilmasini taniydi. Shu tariqa, barcha ma'lumotlar oqimi bevosita jinoyatchining qurilmasi orqali o‘ta boshlaydi.

2. MITM (Man-in-the-Middle): O‘rtadagi Odam Hujumi

ARP spoofing muvaffaqiyatli amalga oshirilgandan so‘ng, hujumchi MITM holatiga o‘tadi. Bu bosqichda u ikki tomon o‘rtasidagi "shaffof ko‘prik"ka aylanadi.

Trafikni tutib qolish (Sniffing): Wireshark yoki Ettercap kabi vositalar yordamida shifrlanmagan (HTTP, FTP, Telnet) paketlar ichidagi login va parollar ko‘riladi.

Ma’lumotlarni manipulyatsiya qilish: Hujumchi nafaqat ma’lumotni kuzatadi, balki uni o‘zgartirishi ham mumkin. Masalan, foydalanuvchi yuklab olayotgan faylni zararli dastur (Malware) bilan almashtirib qo‘yish.

SSL Stripping: HTTPS orqali shifrlangan aloqani oddiy HTTP rejimiga tushirish orqali maxfiy ma’lumotlarni ochiq holda qo‘lga kiritish.

3. Hujumni Amalda Bajarishning Strukturaviy Bosqichlari

Kiberxavfsizlik mutaxassislari tarmoqni testdan o‘tkazishda odatda quyidagi algoritmdan foydalanadilar:

Tarmoq skanerlash: Nmap yordamida tarmoqdagi faol qurilmalar va shlyuz (gateway) manzili aniqlanadi.

IP-Forwarding yoqish: Hujumchi o‘z qurilmasini ma’lumotni to‘xtatib qo‘ymasdan, o‘zi orqali o‘tkazib yuborishi (router vazifasini bajarishi) uchun sozlaydi.

Spoofing jarayoni: Arpspoof yoki Bettercap kabi utilitalar yordamida qurbon va router o‘rtasida "zaharlangan" ARP paketlari yuboriladi.

Tahlil va Eksfiltratsiya: Tutib olingan trafik tahlil qilinib, kerakli maxfiy ma’lumotlar ajratib olinadi.

4. Strategik Himoya: ARP Hujumlaridan Saqlanish

Lokal tarmoqni bunday tahdidlardan himoya qilish uchun ko‘p bosqichli chora-tadbirlar talab etiladi:

A) Texnik va Apparat darajasidagi himoya:

Statik ARP jadvallari: Muhim qurilmalar (serverlar, routerlar) uchun ARP yozuvlarini qo‘lda kiritish. Bu avtomatik yangilanish orqali keladigan soxta ma’lumotlarni bloklaydi.

Dynamic ARP Inspection (DAI): Professional switchlarda (masalan, Cisco) qo‘llaniladi; u soxta ARP xabarlarini aniqlaydi va filtrlaydi.

Port Security: Switch portlariga faqat aniq MAC-manzilli qurilmalarning ulanishini cheklash.

B) Dasturiy va Tizimli himoya:
VPN-dan foydalanish: Hatto ARP spoofing sodir bo‘lganda ham, trafik shifrlangan bo‘lgani sababli hujumchi ma’lumotlarni o‘qiy olmaydi.
IDS/IPS tizimlari: Tarmoqdagi shubhali faollikni nazorat qiluvchi va administratorni ogohlantiruvchi tizimlarni joriy etish.
HTTPS Everywhere: Har doim xavfsiz protokollardan foydalanish va brauzerlardagi sertifikat xatoliklariga e’tiborli bo‘lish.
Xulosa. ARP spoofing va MITM hujumlari tarmoq arxitekturasidagi fundamental bo‘shliqlardan foydalanadi. Amaliyot shuni ko‘rsatadiki, texnik himoya vositalari bilan bir qatorda, tarmoq administratorlarining muntazam monitoring olib borishi va foydalanuvchilarning kiber-savodxonligi xavfsizlikning asosi hisoblanadi. Lokal tarmoq har doim "xavfsiz zona" bo‘lib qolishi uchun har bir qurilmaning tarmoqdagi xatti-harakati qat’iy nazorat qilinishi shart.

Foydalanilgan adabiyotlar

1. Tanenbaum, A. S. (2021). Computer Networks. Pearson.
2. Erickson, J. (2008). Hacking: The Art of Exploitation. No Starch Press.
3. Cisco Systems. Understanding Dynamic ARP Inspection (DAI) - Technical Guide 2024.
4. OWASP Foundation. Man-in-the-Middle Attack (MITM) Prevention Cheat Sheet.